

REF

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

SWORN STATEMENT

LOCATION: Fort Carson CID Office, Fort Carson, CO 80913

FILE NUMBER: 0327-10-CID0056

0028-10-CID221-10117

DATE: 25 Aug 2010

TIME: 1417

NAME:

SSN:

GRADE/STATUS: SFC / AD

ORGANIZATION OR ADDRESS: B Company, Division Special Troops Battalion, 4th Infantry Division, Fort Carson, CO 80902

(b)(6)(b)(7)(C)

want to make the following statement under oath:

Q: SA (b)(6)(b)(7)(C)

A: SFC (b)(6)(b)(7)(C)

Q: Where you ever assigned to Fort Huachuca?

A: I was assigned there from Jun 05 to May 23, 2008.

Q: What was your duty assignment while at Fort Huachuca?

A: I was an instructor for the first 7 months, then I was a Drill Sergeant in training, and then an AIT Platoon Sergeant in D Co, 305th MI BN.

Q: Do you know PFC MANNING?

A: Not that I know of.

Q: When was the last time you had contact with PFC MANNING?

A: I don't recall ever having contact with PFC MANNING.

Q: Are you aware of any security incidents involving PFC MANNING?

A: I am not aware of any. If he was one of my privates, I would know, if while I was there, he had a security violation.

Q: Are you aware of any disciplinary incidents involving PFC MANNING?

A: I am not aware of any. If he was one of my privates, I would know, if while I was there, he had a disciplinary violation, because then he would have stood out.

Q: What do you know about the OPSEC incident in which PFC MANNING posted YouTube videos pertaining to a SCIF?

A: I saw something online about it when the whole thing came out less than a year ago. I remember when I read the article about the incident that the time frame he did this was after left Fort Huachuca, so I figured he was not one of my privates.

Q: What do you know about an incident in which PFC MANNING stabbed/attempted to stab/assault another Soldier with a pencil?

A: Nothing, but if he was my Soldier I would definitely remember.

Q: Did PFC MANNING ever discuss the unauthorized released of classified information with you?

A: No, I don't remember a PFC MANNING.

Q: Did PFC MANNING ever mention WikiLeaks?

A: No, according to the news, that happened after I left Fort Huachuca.

Q: Did PFC MANNING ever say why he joined the Army?

A: I don't know the kid (b)(6)(b)(7)(C)

INITIALS OF PERSON MAKING STATEMENT

(b)(6)(b)(7)(C)

PAGE 1 OF 2 PAGES

DA Form 2823-E

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 177

001054
encl. 3

CASE NUMBER: 0028-10-CID221-10117

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

STATEMENT OF: (b)(6)(b)(7)(C) TAKEN AT: Fort Carson CID Office, Fort Carson, CO 80913. Date: 4

(b)(6)(b)(7)(C) Aug 10, CONTINUED:

(b)(6)(b)(7)(C): Did PFC MANNING ever mention any of his friends?

A: I don't remember kid let alone his friends.

Q: Was any documentation prepared as a result of conduct/performance/disciplinary issues?

A: According to our SOP, if a private was phased, had a security violation, was late, or any kind of performance (positive or negative), they would be counseled by their Platoon Sergeant. I do not remember any documentation for PFC MANNING.

Q: Do you have anything further to add to this statement?

A: If the news is true, I hope the dude rots, because he is making a bad name for my MOS.

Q: Do you have anything further to add to this statement?

A: No.///END OF STATEMENT///(b)(6)(b)(7)(C)

AFFIDAVIT

I (b)(6)(b)(7)(C) have read or have had read to me this statement which begins on page 1 and ends on page 2. I fully understand the contents of the entire statement made by me. The statement is true. I have initialed all corrections and have initialed the bottom of each page containing the statement. I have made this statement freely without hope of benefit or reward, without threat of punishment, and without coercion, unlawful influence or unlawful inducement.

Witness #1:

Witness #2:

Oath)

(b)(6)(b)(7)(C)

ent)

Subscribed and sworn before me, a
 person authorized by law to administer
 oaths, this 25th day of August, 2010
 at Fort Carson, CO, 80913

(b)(6)(b)(7)(C)

(Signature of Person Administering Oath)

SA (b)(6)(b)(7)(C), (b)(7)(E)

(Typed name of Person Administering

10 USC 936

(Authority to Administer Oath)

INITIALS OF PERSON MAKING STATEMENT

(b)(6)(b)(7)(C)

PAGE 2 OF 2 PAGES

SWORN STATEMENT

LOCATION: CID Office, Fort Carson, CO

FILE NUMBER: 0327-10-CID056-

DATE: 25 Jul 10 (b)(6)(b)(7)(C)

TIME: 1424 (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)

NAME: (b)(6)(b)(7)(C)

SSAN: (b)(6)(b)(7)(C)

GRADE/RANK: SFC

ORGANIZATION OR ADDRESS: A Company, 2nd Special Troops Battalion, 2 BCT, 4ID, Fort Carson, CO 80913

(b)(6)(b)(7)(C)

(b)(6)(b)(7)(C), SFC (b)(6)(b)(7)(C) would like to make the following statement under oath.

Q: SA (b)(6)(b)(7)(C)

A: SFC (b)(6)(b)(7)(C)

Q: How do you know PFC MANNING?

A: He was an AIT student at Delta Company 305th at Fort Huachuca, AZ while I was a Drill Sergeant. His face and name are familiar, but I don't recall any specific event or issue involving him.

Q: When was the last time you had contact with PFC MANNING?

A: I was at Delta Company from Feb-Sep 08. I don't remember when he was there, but during his AIT cycle. I was night Drill during May timeframe and interacted with all soldiers in all platoons such as bed checks, fireguard, etc.

Q: Are you aware of any security incidents involving PFC MANNING?

A: Yes, I saw it on the news in July 2010.

Q: Are you aware of any disciplinary incidents involving PFC MANNING?

A: No.

Q: What do you know about an OPSEC incident in which PFC MANNING posted YouTube videos pertaining to SCIF?

A: Nothing.

Q: What do you know about an incident in which PFC MANNING stabbed/attempted to stab/assaulted another soldier with a pencil?

A: Nothing, I don't remember this incident.

Q: Did PFC MANNING ever discuss the unauthorized release of classified information with you? If so, please explain.

A: No.

Q: Did PFC MANNING ever mention WikiLeaks? If so, in what context?

A: No, I didn't even know about Wikileaks until I heard it on the news.

Q: Did PFC MANNING ever say why he joined the Army? If so, why?

A: In my platoon I do a round robin with the troops and ask why they joined as an ice breaker when they arrived at Fort Huachuca; however, I don't know if he was one of my soldiers or in another platoon.

Q: Did PFC MANNING ever mention any of his friends? If so, who?

A: No.

Q: For leaders in PFC MANNING's chain of command. Was any documentation prepared as a result of conduct/performance/disciplinary issues? If so, by who, and where is that documentation located (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)

INITIALS OF PERSON MAKING STATEMENT (b)(6)(b)(7)(C)

PAGE 1 OF 2 PAGES

We documented everything regarding incidents involving students. Their files are kept in the orderly room for two years after they graduate.

Q: When were you assigned to Fort Huachuca?

A: From Feb 05- Jul 09.

Q: What was your duty assignment/unit while at Fort Huachuca?

A: I was with the NCO Academy for a year and 305th 3 1/2 years while at Fort Huachuca.

Q: Do you have anything else to add to your statement?

A: No. ///End of Statement (b)(6)(b)(7)(C)

AFFIDAVIT

I, (b)(6)(b)(7)(C) have read or have had read to me this statement which begins on page 1 and ends on page 2. (b)(6)(b)(7)(C) fully understand the contents of the entire statement made by me. The statement is true. I have initialed all corrections and have initialed the bottom of each page containing the statement. I have made this statement freely without hope of benefit or reward, without threat of punishment, and without coercion, unlawful influence or unlawful inducement.

Witness #1:

Witness #2:

(b)(6)(b)(7)(C)

Subscribed and sworn before me, a person authorized by law to administer oaths, this 25th day of August 2010, at Fort Carson, CO 80913.

(b)(6)(b)(7)(C)

(Signature of Person Administering Oath)

SA (b)(6)(b)(7)(C), (b)(7)(E)

(Typed name of Person Administering Oath)

10 U.S.C 936

(Authority to Administer Oath)

INITIALS OF PERSON MAKING STATEMENT

(b)(6)(b)(7)(C)

PAGE 2 OF 2 PAGES

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1452, 25 Aug 10, SA (b)(6)(b)(7)(C) coordinated with Ms. (b)(6)(b)(7)(C) Lockheed Martin contractor, Army CIO/G6, Office of Information Assurance and Compliance, Alexandria, VA. Ms. (b)(6)(b)(7)(C) provided this office with the following information related to the Information Awareness (IA) training taken by the user bradley.e.manning@us.army.mil:

<u>DATE</u>	<u>TYPE</u>	<u>VERIFIED BY</u>
5 Sep 08	Annual	Ft Gordon DB
31 Oct 09	Annual	Ft Gordon DB

Ms. (b)(6)(b)(7)(C) stated that there was no other training listed in the bradley.e.manning@us.army.mil user profile.////LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

SA-

(b)(6)(b)(7)(C)

DATE

25 Aug 10

EXHIBIT

179

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001058

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

For Official Use Only - Law Enforcement Sensitive

ROI NUMBER:

0224-10-CID043

PAGE 1 OF 1 PAGE

DETAILS

BASIS FOR INVESTIGATION: This office received a Request for Assistance (RFA) from the Arizona Branch CCIU Office to locate, fully ID and interview WO1 (b)(6)(b)(7)(C) A CO, 297th Military Intelligence Battalion, Fort Gordon, GA 30905 (FGGA), to determine what knowledge if any he had about PFC Bradley E. MANNING, HHC, 2nd Brigade Combat Team (BCT), 10th Mountain Division (MTNDIV), Forward Operating Base (FOB) Hammer, Iraq, wherein he claimed he had disclosed U.S. Government Classified Information to the operators of "Wikileaks", which were subsequently posted to the website.

About 0800, 26 Aug 10, SA (b)(6)(b)(7)(C) interviewed WO1 (b)(6)(b)(7)(C) who stated he remembered PFC MANNING, but did not know of any incident involving a pencil, or information being placed on YouTube about a SCIF. WO1 (b)(6)(b)(7)(C) stated he was PFC MANNING's instructor and the last time he had contact with PFC MANNING was May of 2009 when he was TDY to Fort Hood. WO1 (b)(6)(b)(7)(C) stated PFC MANNING did not disclose any information about his friends, and he was not aware of any security violation incidents which involved PFC MANNING. WO1 (b)(6)(b)(7)(C) could not provide any other information pertinent to this investigation.

About 1245, 26 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C), and briefed him on the interview of WO1 (b)(6)(b)(7)(C). SA (b)(6)(b)(7)(C) related no other investigative activity was required. All requested investigative activity has been completed by this office. No further investigative activity is anticipated.///Last Entry///

TYPED AGENT'S NAME AND SEQUENCE NUMBER:

(b)(6)(b)(7)(C), (b)(7)(E)

Special Agent

ORGANIZATION:

Fort Gordon CID Office
Fort Gordon, GA 30905

SIGNATURE:

(b)(6)(b)(7)(C)

DATE:

26 Aug 10

EXHIBIT:

180

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

1 FEB 77

ENCL 7 001059

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0289-10-CID013/ 0028-10-CID221-10117

PAGE 1 OF 1 PAGE

DETAIL

BASIS FOR INVESTIGATION: About 0900, 26 Aug 10, this office received a Request for Assistance (RFA) from the Computer Crime Investigation Unit (CCIU), Fort Belvoir, VA 22060, to locate, fully identify, interview, and if necessary, obtain a sworn statement from CPT (b)(6)(b)(7)(C) C Co., 199th IN BN, Fort Benning, GA 31905 (FBGA), regarding his past association with PFC Bradley E. MANNING, HHC, 2 BCT, 10th MTN DIV, FOB Hammer, Iraq.

About 1400, 26 Aug 10, SA (b)(6)(b)(7)(C) interviewed CPT (b)(6)(b)(7)(C) who had recently left FBGA en route to Fort Bragg, NC. CPT (b)(6)(b)(7)(C) stated he was previously assigned as the Executive Officer (XO) of A and D Co., 305th MI BN (AIT), Fort Huachuca, AZ during 2007 and 2008, but had no recollection of PFC MANNING. He also did not recall an incident of a Soldier posting videos of a SCIF to the internet, or any incident of a Soldier attempting to stab another Soldier with a pencil. ///LAST ENTRY///

TYPE AGENT'S NAME AND SEQUENCE NUMBER

(b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Fort Benning CID Office, 3rd MP Group (CID)
USACIDC, Fort Benning, GA 31905

SIGNATURE

(b)(6)(b)(7)(C)

DATE

26 Aug 10

EXHIBIT

181

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0172-10-CID452

PAGE 1 OF 2

DETAILS

About 1300, 7 Jul 10, SA (b)(6)(b)(7)(C) interviewed Mrs. (b)(6)(b)(7)(C) who provided a sworn statement where she stated she knew PFC MANNING through her husband, SSG (b)(6)(b)(7)(C) but had not stored any of PFC MANNING's personal belongings at any time. Mrs. (b)(6)(b)(7)(C) stated that she believed MSG (b)(6)(b)(7)(C) Headquarters and Headquarters Company, 2nd Brigade Combat Team, 10th Mountain Division, Fort Drum, NY 13602(FDNY) had stored the box of PFC MANNING's belongings.

About 1355, 13 Jul 10, SA (b)(6)(b)(7)(C) coordinated with Mrs. (b)(6)(b)(7)(C) (the dependent wife of MSG (b)(6)(b)(7)(C) who stated there was not a box of PFC MANNING's belongings at her off post quarters.

About 1524, 22 Jul 10, SA (b)(6)(b)(7)(C) CCIU, coordinated with SA (b)(6)(b)(7)(C) in reference further investigative activity not previously requested. SA (b)(6)(b)(7)(C) requested this office coordinate with MANNING's Chain of Command and/or DOIM to determine if MANNING signed any acceptable use policies for SIPR or NIPR networks. SA (b)(6)(b)(7)(C) further requested this office determine if MSG (b)(6)(b)(7)(C) was currently deployed to Iraq.

About 1535, 22 Jul 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C) who confirmed MSG (b)(6)(b)(7)(C) was currently deployed to Iraq. SSG (b)(6)(b)(7)(C) further related copies of nondisclosure agreements for SIPR and NIPR networks are maintained at Division G2, by Ms. (b)(6)(b)(7)(C)

About 1031, 23 Jul 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C), G-6, 10th Mountain Division, FDNY, who stated he did not have record of MANNING signing the acceptable user agreements, nor did MANNING have an account registered with the G-6 Information Assurance systems. CPT (b)(6)(b)(7)(C) further related the forward OIC of 2nd BCT Information Management took the incomplete Information Assurance documentation with him to Iraq for completion. He was supposed to upload the documentation into the DoD tracking system upon completion, but failed to do so.

About 1115, 23 Jul 10, SA (b)(6)(b)(7)(C) coordinated with Mr. (b)(6)(b)(7)(C) Mission Support Element, G-2, 10th Mountain Division, FDNY, who provided a copy of a Classified Information Nondisclosure Agreement signed by MANNING on 17 Sept 08, and a copy of a Sensitive Compartmented Information Nondisclosure Statement signed by MANNING on 22 Jan 09.

About 0955, 11 Aug 10, SA (b)(6)(b)(7)(C) submitted DA Form 4254 Request for Private Medical Information, pertaining to PFC MANNING, to Wilcox Behavioral Health Clinic personnel.

About 1215, 11 Aug 10, SA (b)(6)(b)(7)(C) conducted a re-interview of SSG (b)(6)(b)(7)(C) HHC, 2nd BCT, FDNY, in order to clarify information given in a previous statement. SSG (b)(6)(b)(7)(C) stated he allowed MANNING to use his personal laptop computer on several occasions while deployed. SSG (b)(6)(b)(7)(C)

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b)(7)(E)		ORGANIZATION 62 nd MP Det (CID), Fort Drum, NY	
SIGNATURE (b)(6)(b)(7)(C)		DATE 26 Aug 10	EXHIBIT 182

CID FORM 94 FOR OFFICIAL USE ONLY/ LAW ENFORCEMENT SENSITIVE

1 FEB 77

001061

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0172-10-CID452

PAGE 2 OF 2

DETAILS

kept his personal laptop in his supply office and only allowed himself, MANNING, and his clerk, CPL (b)(6)(b)(7)(C)(NFI) to use it. SSG (b)(6)(b)(7)(C) did not password protect his personal laptop computer and it was possible for someone to have used it without his knowledge; however, it was unlikely because if the computer was not in his or CPL (b)(6)(b)(7)(C) direct line of sight, it was secured within the supply office.

SSG (b)(6)(b)(7)(C) stated he had seen the video now known as "Collateral Murder" while assigned to the 2nd Battalion, 75th Ranger Regiment in 2006 or 2007. SSG (b)(6)(b)(7)(C) stated he had never visited the WikiLeaks website, nor had he received any emails, texts or digital media from MANNING. SSG (b)(6)(b)(7)(C) stated he had a strictly professional relationship with MANNING.

About 1610, 23 Aug 10, SA (b)(6)(b)(7)(C) obtained Behavioral Health records pertaining to MANNING from Ms. (b)(6)(b)(7)(C) Medical Support Assistant, Wilcox Behavioral Health Clinic, FDNY.

About 1045, 24 Aug 10, SA (b)(6)(b)(7)(C) obtained the originals of the Nondisclosure Agreements signed by MANNING from Ms. (b)(6)(b)(7)(C) and entered them on a DA Form 4137, Evidence/Property Custody Document.

About 1038, 26 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) who advised no further investigative assistance was required at this time.////LAST ENTRY////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

62nd MP Det (CID), Fort Drum, NY

SIGNATURE

(b)(6)(b)(7)(C)

DATE

26 Aug 10

EXHIBIT

(182)

CID FORM 94 FOR OFFICIAL USE ONLY/ LAW ENFORCEMENT SENSITIVE

1 FEB 77

001062

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

SWORN STATEMENT

File Number : 0172-10-CID452
 Location : Fort Drum, NY 13602
 Date : 7 Jul 10

Time: 1425
 Rank: FM/W

Statement of: (b)(6)(b)(7)(C)

SSN: (b)(6)(b)(7)(C)

Org/Address : (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C), (b)(6)(b)(7)(C) WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH: I met PFC MANNING about a year or so before his unit deployed. I met him through my husband. I don't really know him all that well, just from what I've talked to him while he was working Staff Duty with my husband. About 13 October 2009, I was at the company area with my husband while he was drawing his weapon for deployment. The single soldiers in the barracks were clearing the barracks rooms that day as well. I was approached by PFC MANNING who said he had a large box full of his personal belongings that he said a friend of his was going to come and pick up. PFC MANNING asked if he could store this box of his belongings at my quarters until his friend could come and pick it up. While PFC MANNING was drawing his weapon, he was approached MSG (b)(6)(b)(7)(C) who was the NCOIC of the weapons draw and barracks clearing operations. MSG (b)(6)(b)(7)(C) asked PFC MANNING if he had cleared his barracks room, PFC MANNING responded that he had cleared his barracks room, but had a box of his belongings in my car for me to store. MSG (b)(6)(b)(7)(C) requested to see the box and decided that it was not a good idea for me to store the box and that it was too big for me to have to carry. MSG (b)(6)(b)(7)(C) then transferred the box from my car to his personal car. That is the last I had seen or heard about PFC MANNING's box.

Q: SA (b)(6)(b)(7)(C)

A: MRS. (b)(6)(b)(7)(C)

Q: Is this statement in your own words, as prepared by SA (b)(6)(b)(7)(C)

A: Yes.

Q: Can you describe the box of belongings that PFC MANNING asked you to hold for him?

A: It was a brown, cardboard box. It was about 2' x 2' x 1.5' and plain. There was nothing printed on the outside.

Q: Did you inventory the box at any time?

A: No. I actually never touched the box. PFC MANNING and another soldier loaded it into my car and MSG (b)(6)(b)(7)(C) loaded it into his car.

Q: Did PFC MANNING show you what was in the box or tell you specifically what was in the box?

A: No. I don't recall whether or not if he specifically told me what was in the box. I want to say that PFC MANNING told me that he had some CD's, movies, and maybe some electronic equipment in the box that would need to be stored out of the heat.

Q: Who is MSG (b)(6)(b)(7)(C)

A: He is the NCOIC of the S-2 shop in HHC 2 BCT, my husband's unit.

Q: Did PFC MANNING observed MSG (b)(6)(b)(7)(C) remove the box from your car and put the box into his own car?

A: No, he did not. PFC MANNING was still in line waiting for weapons draw, but PFC MANNING was told by MSG (b)(6)(b)(7)(C) of the transfer of the box.

Q: Do you know if MSG (b)(6)(b)(7)(C) still has the box of PFC MANNING's belongings?

A: I have no idea. I haven't talked to MSG (b)(6)(b)(7)(C) since this incident.

Q: Do you know if MSG (b)(6)(b)(7)(C) is still a part of HHC, 2BCT?

A: He is. He was back here in the Ft. Drum area for mid-tour leave sometime in June of this year, but I think he is already back in Iraq at FOB Hammer.

Q: At any time, did PFC MANNING ever disclose to you anything regarding the dissemination of classified information (b)(6)(b)(7)(C)

INITIALS (b)(6)(b)(7)(C)

Page 1 of 2

Exhibit 183

Encl 62

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVESTATEMENT OF (b)(6)(b)(7)(C) TAKEN AT Fort Drum, NY 13602 DATED: 7 Jul 10,
CONTINUED: (b)(6)(b)(7)(C)

0172-10-CID452-

A: No.

Q: Is there anything you want to add to this statement?

A: No.///End Of Statement/ (b)(6)(b)(7)(C)

AFFIDAVIT

I, (b)(6)(b)(7)(C) HAVE READ OR HAD (b)(6)(b)(7)(C) READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 2. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(b)(6)(b)(7)(C)

(Signature of Person Making Statement)

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 7 day of July, 2010, at Fort Drum, NY 13602.

(b)(6)(b)(7)(C)

(Signature of Person Administering Oath)

SA (b)(6)(b)(7)(C), (b)(7)(E)

(Typed Name of Person Administering Oath)

10 USC § 936

WITNESS:

INITIALS

(b)(6)(b)(7)(C)

Page 2 of 2

Exhibit 183

Encl 1

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

001064

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 3 PAGES

DETAILS

About 0910, 27 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed CW2 (b)(6)(b)(7)(C) B Company, 741st Military Intelligence Battalion, 9802 Love Road, Fort Meade, MD 20755, as he was identified as having been assigned with PFC MANNING at Forward Operating Base (FOB) Hammer during the time period PFC MANNING was deployed to Iraq. CW2 (b)(6)(b)(7)(C) stated he was assigned to FOB Hammer from approximately 15 Jan 10, through sometime in July 2010; and that he was the replacement for Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) as the Officer in Charge (OIC) of Cryptologic Support Team 5 (CST5). CW2 (b)(6)(b)(7)(C) said he remembered PFC MANNING as someone who had an attitude, was 'wound-up', and/or became agitated frequently. CW2 (b)(6)(b)(7)(C) explained that the day before the incident involving PFC MANNING assaulting SPC (b)(6)(b)(7)(C) CW2 (b)(6)(b)(7)(C) said he saw PFC MANNING accidentally run into another soldier in the dining facility on FOB Hammer. CW2 (b)(6)(b)(7)(C) explained PFC MANNING nearly dumped the other soldier's tray of food onto the floor and the soldier PFC MANNING ran into was two or three times the size of PFC MANNING. CW2 (b)(6)(b)(7)(C) said PFC MANNING looked like he was about to hit the other soldier. CW2 (b)(6)(b)(7)(C) related PFC MANNING told him something to the effect that he wouldn't think twice about hitting the other soldier, which CW2 (b)(6)(b)(7)(C) explained seemed unusual given how big the other soldier was in comparison to PFC MANNING. CW2 (b)(6)(b)(7)(C) stated he did not witness the incident involving PFC MANNING and SPC (b)(6)(b)(7)(C) but did say that in a certain respect, SPC (b)(6)(b)(7)(C) may have encouraged the incident. CW2 (b)(6)(b)(7)(C) said SPC (b)(6)(b)(7)(C) was a senior Specialist (Pay Grade E-4) that tended to talk down to the personnel she supervised; which included PFC MANNING, SPC (b)(6)(b)(7)(C) (NMN) (b)(6)(b)(7)(C) and another female Private First Class who CW2 (b)(6)(b)(7)(C) couldn't immediately remember the name of. CW2 (b)(6)(b)(7)(C) said PFC MANNING often seemed to be in a hurry and mentioned he had sat next to PFC MANNING on several occasions at the FOB Hammer dining facility when no other alternate seating had been available. CW2 (b)(6)(b)(7)(C) noted in the times he had been around PFC MANNING in the dining facility, PFC MANNING appeared to have a habit of drinking two cans of Coke, then ate what CW2 (b)(6)(b)(7)(C) described as "a little", and would then grab two more cans of Coke to take back to work with him. CW2 (b)(6)(b)(7)(C) related PFC MANNING did not talk with the CST5 personnel very much, as the CST5 personnel tended to avoid all of the 2nd BCT, 10th Mountain Division soldiers; which they described as "Organics" (analysts organic to the 2nd BCT). CW2 (b)(6)(b)(7)(C) related the 2nd BCT soldiers seemed to have an attitude with the CST5 members, as the CST5 members tried to not get involved with the 2nd BCT unit issues and would often leave meetings related to 2nd BCT business. CW2 (b)(6)(b)(7)(C) said when CST5 personnel would leave in the middle of meetings, it appeared to upset the 10th Mountain Division soldiers who may have felt this was rude. CW2 (b)(6)(b)(7)(C) said he could not remember PFC MANNING ever asking him any hypothetical questions in regard to computers or computer networks. CW2 (b)(6)(b)(7)(C) mentioned PFC MANNING appeared to be friends with PFC (b)(6)(b)(7)(C) CW2 (b)(6)(b)(7)(C) said PFC (b)(6)(b)(7)(C) had already been moved out of working in the Sensitive Compartmented Information Facility (SCIF) prior to CW2 (b)(6)(b)(7)(C) arrival in Iraq, and was working in a section called 'Current Operations'. CW2 (b)(6)(b)(7)(C) explained all of the soldiers who were having various issues during the deployment were assigned to Current Operations. CW2 (b)(6)(b)(7)(C) said PFC MANNING was treated professionally during the time CW2 (b)(6)(b)(7)(C) was around with one exception. CW2 (b)(6)(b)(7)(C) related PFC MANNING seemed to have a hygiene issue, in that he was noticed by numerous unit members as having an odor. CW2 (b)(6)(b)(7)(C) related one day someone gave PFC MANNING a

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

27 Aug 10

EXHIBIT

184

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001065

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 3 PAGES

DETAILS

gift box containing 'Old Spice' bath products by leaving them on his desk. CW2 (b)(6)(b)(7)(C) stated he believed MSG (b)(6)(b)(7)(C) appeared to try to 'protect' PFC MANNING while working in the SCIF. CW2 (b)(6)(b)(7)(C) explained that after the incident involving SPC (b)(6)(b)(7)(C) PFC MANNING was removed from the SCIF and this incident was the sole reason the unit upgraded the SCIF security. CW2 (b)(6)(b)(7)(C) said the upgraded security included locks on the SCIF doors as well as the posting of guards, which CW2 (b)(6)(b)(7)(C) felt was ridiculous. CW2 (b)(6)(b)(7)(C) related that he did not know of the software application 'OTR', did not have any knowledge of anything related to the '9/11 Pager Messages' as mentioned by PFC MANNING in his Internet chats. CW2 (b)(6)(b)(7)(C) said he did remember discussing the iPhone with a member of his higher command (which was also mentioned by PFC MANNING in chat conversations in which he talked about an unidentified NSA personnel). CW2 (b)(6)(b)(7)(C) however did not think PFC MANNING would have known about his iPhone conversation(s). CW2 (b)(6)(b)(7)(C) said, when asked specific questions about things PFC MANNING mentioned in his internet chats with Mr. (b)(6)(b)(7)(C) that the only way PFC MANNING could have accessed the Joint Worldwide Intelligence Communications System (JWICS) network would have been through the National Security Agency Network (NSANet); although CW2 (b)(6)(b)(7)(C) explained that would have been highly unlikely due to: the lack of access PFC MANNING had to NSANet; that none of the CST5 personnel should have allowed PFC MANNING access to NSANet on their accounts; and the method for connecting to JWICS via NSANet is not something easily understood. CW2 (b)(6)(b)(7)(C) said he did not believe any of the Signals Intelligence (SIGINT) personnel knew how to do this. CW2 (b)(6)(b)(7)(C) said in regard to PFC MANNING's comments about allegedly tracking a Naturalized U.S. Citizen 'Off the Record', that PFC MANNING would have had to have worked with a SIGINT Analyst to have done this. CW2 (b)(6)(b)(7)(C) related PFC (b)(6)(b)(7)(C) was a SIGINT Analyst, but had already been moved to another section by the time CW2 (b)(6)(b)(7)(C) arrived in Iraq. CW2 (b)(6)(b)(7)(C) related when asked about the Foreign Intelligence Surveillance Act (FISA) and/or whether PFC MANNING had ever asked him about FISA information, CW2 (b)(6)(b)(7)(C) said he had not mentioned any FISA information to PFC MANNING, and that SSgt (b)(6)(b)(7)(C) and himself were the only two personnel he was aware of that were cleared for FISA. CW2 (b)(6)(b)(7)(C) explained the personnel that composed CST5 were: SPC (b)(6)(b)(7)(C) SSgt (b)(6)(b)(7)(C) Mr. (GS-13) (b)(6)(b)(7)(C) SSgt (b)(6)(b)(7)(C) and SrA (b)(6)(b)(7)(C) CW2 (b)(6)(b)(7)(C) explained SSgt (b)(6)(b)(7)(C) was transferred to Baghdad about four to six weeks after arriving in Iraq, and was not at FOB Hammer the majority of CW2 (b)(6)(b)(7)(C) six-month assignment in Iraq. CW2 (b)(6)(b)(7)(C) further related SrA (b)(6)(b)(7)(C) was sent back to the United States about two months into his six month tour in Iraq, due to what CW2 (b)(6)(b)(7)(C) explained were marital issues SrA (b)(6)(b)(7)(C) was experiencing. CW2 (b)(6)(b)(7)(C) related in regard to the shift work in the SCIF, that during the night shift the SCIF was generally manned by a 'skeleton crew' and did not typically include any officers on the night shift. Upon being asked, CW2 (b)(6)(b)(7)(C) explained the term 'Reflection' (which had been used by PFC MANNING in chat his Internet conversations) was used as a SIGINT term to describe intercepted conversations and/or other intelligence from secondary personnel who were not directly part of an incident or situation. CW2 (b)(6)(b)(7)(C) said he could not remember a situation in which PFC MANNING would have gone 'outside the wire' (left FOB Hammer) during the time he was in Iraq, due to the nature of his position. CW2 (b)(6)(b)(7)(C) related other personnel in PFC MANNING's unit may know more about PFC MANNING having left FOB Hammer to work with Iraqi Police units or the Iraqi Army. CW2 (b)(6)(b)(7)(C) said during the conclusion of his interview that

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

27 Aug 10

EXHIBIT

184

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 3 OF 3 PAGES

DETAILS

he believed PFC MANNING may have used some type of automated tool running in the background on his computer to harvest the data he was alleged to have compromised; and he further mentioned PFC MANNING owning an "Apple Mac Book Pro" as a personal computer. CW2 (b)(6)(b)(7)(C) could not immediately provide any additional information about PFC MANNING in relation to this investigation.

AGENTS COMMENT: SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) both discussed several things mentioned by CW2 (b)(6)(b)(7)(C) as well as the interview overall, specifically that CW2 (b)(6)(b)(7)(C) may have been the individual mentioned by PFC MANNING as the '...NSA person who would talk, and talk, and talk...'; as CW2 (b)(6)(b)(7)(C) appeared to be quite talkative and forthcoming with information. SA (b)(6)(b)(7)(C) additionally noted CW2 (b)(6)(b)(7)(C) mentioning PFC MANNING having possibly automated his harvesting of information on the Secure Internet Protocol Router (SIPR) network using an automated software tool, as this was not something which had been mentioned to CW2 (b)(6)(b)(7)(C) during the interview and not something SA (b)(6)(b)(7)(C) believed had been mentioned by the media in this case. However, SA (b)(6)(b)(7)(C) noted CW2 (b)(6)(b)(7)(C) was a Computer Network Management Technician, and consequently may have accurately guessed how PFC MANNING obtained some of the U.S. Government materials he is alleged to have unlawfully disclosed. SA (b)(6)(b)(7)(C) also noted CW2 (b)(6)(b)(7)(C) knowledge of PFC MANNING having an Apple Mac Book Pro was not something which had been mentioned during his interview and also not something which had been reported by the media, as this fact was generally unremarkable to personnel outside of this investigation. CW2 (b)(6)(b)(7)(C) also seemed to indicate, by process of elimination, that he would have been one of the only personnel knowledgeable about FISA related information after SSgt (b)(6)(b)(7)(C) was reassigned from FOB Hammer to the Baghdad area after only the first four to six weeks into SSgt (b)(6)(b)(7)(C) six month assignment in Iraq. CW2 (b)(6)(b)(7)(C) also identified his knowledge of the iPhone and having discussed this information with his senior leadership. Lastly, it was noted that during the initial portion of the interview, CW2 (b)(6)(b)(7)(C) aimed to know little about PFC MANNING; but, as the interview progressed and lasted nearly 90 minutes, CW2 (b)(6)(b)(7)(C) was able to provide a fair amount of information about PFC MANNING.

//////////////////////////////////// LAST ENTRY //////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

27 Aug 10

EXHIBIT

184

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001067
Approved

Exhibit(s) 185

Page(s) 001068 and 01068a withheld:

5 U.S.C. § 552(b)(1)

Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 186

Page(s) 001069 and 001070 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

AGENT'S INVESTIGATION REPORT

0198-10-CID045-

CID Regulation 195-1

PAGE 1 OF 3 PAGES

BASIS FOR INVESTIGATION: About 1430, 30 Aug 10, this office received a Category 1 Request For Assistance from Computer Crime Investigative Unit, Washington Metro Resident Agency, Fort Belvoir, VA 22060, to locate all personnel in PFC Bradley E. MANNING, (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2d Brigade Combat Team (BCT), 10th Mountain Division, FOB HAMMER, Iraq, chain of command while he went through Basic Training and Advanced Individual Training on Fort Leonard Wood, MO 65743 (FLWMO), from Oct 2007 through Apr 2008.

About 1432, 30 Aug 10, SA (b)(6)(b)(7)(C) this office, conducted a search of the Centralized Operations Police Suite (COPS) which revealed no incidents involving PFC MANNING, which occurred at FLWMO.

About 1530, 30 Aug 10, SA (b)(6)(b)(7)(C) coordinated with 1SG (b)(6)(b)(7)(C) C Company, 2-10 Infantry Battalion, FLWMO, who related during the time frame in question the key leaders were CPT (b)(6)(b)(7)(C) and 1SG (b)(6)(b)(7)(C). He further related he does not know where they currently PCS'd to. Furthermore, he related he was never briefed about a soldier who attempted to stab another soldier with a pencil.

About 1545, 30 Aug 10, SA (b)(6)(b)(7)(C) conducted a Department of Defense Employee Interactive Data System (DEIDS) check on the following personnel:

MAJ (b)(6)(b)(7)(C) 43rd Adjutant General Battalion, FLWMO.

1SG (b)(6)(b)(7)(C) 738th Engineer Company, Fort Bragg, NC 28307.

About 1620, 30 Aug 10, SA (b)(6)(b)(7)(C) interviewed MAJ (b)(6)(b)(7)(C) 43rd AG Battalion, FLWMO, who related he was the commander of C Company 2-10, Infantry Battalion, during January of 2008. He further confirmed his First Sergeant's name was (b)(6)(b)(7)(C) and he PCS'd to Fort Bragg, NC. He further related he does not recall an incident of a soldier trying to stab another soldier with a pencil. He stated he was in command for approximately 13 months and had numerous soldiers come through for Advanced Individual Training. Furthermore, he stated he does not remember the names of any of his former drill sergeants during that timeframe.

SA (b)(6)(b)(7)(C)
Special Agent (b)(7)(E)

Fort Leonard Wood CID Office
78th MP DET (CID), 1001st MP BN
Fort Leonard Wood, MO 65473

Signature: (b)(6)(b)(7)(C)

Date:

Exhibit:

31 Aug 10

CID Form 9

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE
Law Enforcement Sensitive

EXHIBIT 187
001071

ENCL 1

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

0028-10-CID221-10117

AGENT'S INVESTIGATION REPORT

0198-10-CID045-

CID Regulation 195-1

PAGE 2 OF 3 PAGES

About 0800, 31 Aug 10, SA (b)(6)(b)(7)(C) coordinated with Mr. (b)(6)(b)(7)(C) Human Resources Manager, 3rd Chemical Brigade, FLWMO, who provided this office with a Alpha Roster of both C Company 82nd Chemical BN and C Company 2-10 Infantry BN, FLWMO. Through a review of the list of names on the Alpha Roster the following individuals were listed: SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C); SFC (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SGT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) and SGT (b)(6)(b)(7)(C), all with C Company, 2-10 Infantry BN, FLWMO. Further, the Alpha Roster had the following names listed: SGT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) and CPT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) all with C Company, 82nd Chemical BN, FLWMO.

About 0830, 31 Aug 10, SA (b)(6)(b)(7)(C) conducted a DEIDS check on all of the above individuals which revealed the following two soldiers are still located at FLWMO:

SSG (b)(6)(b)(7)(C) A Company, 84th Chemical BN, FLWMO.

1SG (b)(6)(b)(7)(C) 2-10 Infantry BN, FLWMO.

About 0900, 31 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C) who related he was assigned as a drill sergeant during the timeframe in question. He further related he had no knowledge of a soldier trying to stab another soldier with a pencil. He further stated that if a soldier would have tried to stab another soldier the command would have notified the Military Police for actions. Furthermore, he stated he does not recall a soldier by the name of PFC MANNING.

About 0930, 31 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SPC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) S-1 Personnel, 3rd Chemical Brigade, FLWMO, who related 1SG (b)(6)(b)(7)(C) has currently PCS'd to Fort Hood, TX. He stated he cleared his unit approximately one month ago.

SA (b)(6)(b)(7)(C)
Special Agent, (b)(7)(E)

Fort Leonard Wood CID Office
78th MP DET (CID), 1001st MP BN
Fort Leonard Wood, MO 65473

Signature: (b)(6)(b)(7)(C)

Date:
31 Aug 10

Exhibit:

CID Form 94

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE
Law Enforcement Sensitive

EXHIBIT 187
001072

ENCL 1

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

AGENT'S INVESTIGATION REPORT

0198-10-CID045-

CID Regulation 195-1

PAGE 3 OF 3 PAGES

About 1050, 31 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SGT (b)(6)(b)(7)(C) S-1 Personnel, 3rd Chemical Brigade, FLWMO, who related they only keep counseling statements and disciplinary paperwork on soldiers for one year after they graduate. He further related 82nd Chemical BN was merged into 84th Chemical BN and most paperwork was destroyed during this time frame.

About 1145, 31 Aug 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) Computer Crime Investigative Unit, Washington Metro Resident Agency, Fort Belvoir, VA 22060, who required no further assistance from this office.///LAST ENTRY///

SA (b)(6)(b)(7)(C)
Special Agent, (b)(7)(E)

Fort Leonard Wood CID Office
78th MP DET (CID), 1001st MP BN
Fort Leonard Wood, MO 65473

Signature: (b)(6)(b)(7)(C)

Date:
31 Aug 10

Exhibit:

CID Form 94

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE
Law Enforcement SensitiveEXHIBIT 187
001073

ENCL 1

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1527, 25 Aug 10, SA (b)(6)(b)(7)(C) conducted a telephonic re-interview of MSG (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (2 BCT), 10th Mountain Division (10 Mtn Div), 10112 4th Armored Division Drive, Fort Drum, NY 13602 (FDNY), who stated SIPR computers used in SCIF at Forward Operating Base (FOB) Hammer, Iraq (IZ), would often "crash" due to the environmental causes and frequently needed to be either replaced or re-imaged/base-lined; however, MSG (b)(6)(b)(7)(C) could not recall whether or not PFC MANNING's computer(s) was crashed and had to be replaced or re-imaged/base-lined or otherwise repaired. MSG (b)(6)(b)(7)(C) stated he believed US Army CID agents had collected a total of three computers reportedly used by PFC MANNING; two of which were the property of 2 BCT while the other one was Theatre Provided Equipment (TPE). MSG (b)(6)(b)(7)(C) stated he believed he had originally signed for approximately 12 TPE computers at FOB Hammer, IZ. MSG (b)(6)(b)(7)(C) described the re-deployment process and stated all of the hard drives from SIPR computers were removed and stored in a Pelican-type case and the case placed in a SECRET-accredited CONEX. MSG (b)(6)(b)(7)(C) stated NIPR and SIPR computers without internal hard drives were then placed in another CONEX. MSG (b)(6)(b)(7)(C) stated none of the hard drives should have been wiped, altered, over-written, and/or modified.

About 1624, 25 Aug 10, SA (b)(6)(b)(7)(C) conducted a telephonic interview of CPT (b)(6)(b)(7)(C) Officer on Charge (OIC), S-2, HHC, 2 BCT, 10 Mtn Div, FDNY, who stated SIPR computers used in SCIF at FOB Hammer, IZ, would frequently "crash" and, as a matter of fact, his computer had to be repaired three different times while he was at FOB Hammer, IZ. CPT (b)(6)(b)(7)(C) stated Mr. (b)(6)(b)(7)(C) (later fully identified as Mr. (b)(6)(b)(7)(C)) was the System Administrator of the Distributed Common Ground System - Army (DCGS-A) systems at FOB Hammer and was in charge of the system maintenance, operations, and all of its hardware and peripherals. CPT (b)(6)(b)(7)(C) stated he believed each time his computer crashed, Mr. (b)(6)(b)(7)(C) would either wipe the hard drive and rebuild it or replace the unit. CPT (b)(6)(b)(7)(C) stated DCGS-A computers were highly temperamental and sensitive to the harsh environment. CPT (b)(6)(b)(7)(C) stated the DCGS-A computers were strictly maintained by Mr. (b)(6)(b)(7)(C) and no soldiers from the unit S-6 shop were allowed to have administrator-level privileges to the system and its hardware and peripherals. CPT (b)(6)(b)(7)(C) stated he believed there were about 10 to 12 DCGS-A computers used in the SCIF at FOB Hammer and all were stay-behind TPEs and would more than likely have been re-imaged/base-lined and re-distributed through IZ. CPT (b)(6)(b)(7)(C) further stated only two or three 2 BCT owned SIPR computers were used in the SCIF and they should be all backed up on the SIPR server and then wiped cleaned. CPT (b)(6)(b)(7)(C) stated in preparation for re-deployment, all SIPR hard drives were backed-up on the SIPR server and wiped clean and only a few SIPR computers were hand-carried back because the sensitive item CONEX had already been sealed and shipped. CPT (b)(6)(b)(7)(C) stated the hand-carried back computers should have been secured in the SECRET vault of each perspective unit. CPT (b)(6)(b)(7)(C) further mentioned it was the mission of the S-2, HHC, 2 BCT, 10th Mtn Div, while at FOB Hammer, IZ, to enable Iraqi Security Forces through the Foreign Disclosure process by providing them with the most timely, accurate, and objective intelligence so that the Iraqi Security Forces could be successful in their mission.

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

DATE

31 Aug 10

EXHIBIT

188

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001074

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

About 1700, 26 Aug 10, SA (b)(6)(b)(7)(C) conducted a telephonic interview of Mr. (b)(6)(b)(7)(C) Contractor, DCGS-A System Administrator, Camp Ramadi, IZ, who stated he was the DCGS-A system Administrator for S-2, HHC, 2 BCT, 10th Mtn Div at FOB HAMMER, IZ, for the duration of their deployment and he specifically recalled PFC MANNING's DCGS-A SIPR computer "crashed" at least twice from the time PFC MANNING started working in the SCIF to the time he was apprehended in May 2010. Mr. (b)(6)(b)(7)(C) stated Windows Explorer on his computer would frequently lock up and applications on the computer would not open. Mr. (b)(6)(b)(7)(C) stated that on one occasion, he asked PFC MANNING if he was "messing around" on the computer, to which PFC MANNING replied that he used to work at a computer repair shop (NFI) and was somewhat computer savvy, but denied having altered and/or modified his computer. Mr. (b)(6)(b)(7)(C) stated that when he re-imaged "crashed computers", he would use software to restore current settings and should it fail, he would base-line by overwriting all previously imaged settings. Mr. (b)(6)(b)(7)(C) stated there were only 10 to 12 DCGS-A SIPR computers used in SCIF at FOB Hammer, IZ, and when S-2, HHC, 2 BCT, 10 Mtn Div redeployed, the computers were more than likely wiped clean and redistributed through IZ. Mr. (b)(6)(b)(7)(C) further mentioned he believed Mr. (b)(6)(b)(7)(C) (NFI) would be able to provide further information pertaining to the current whereabouts of the DCGS-A computers.

About 1835, 31 Aug 10, SA (b)(6)(b)(7)(C) conducted a telephonic interview of SPC (b)(6)(b)(7)(C) Provost Marshal's Office (PMO), 2 BCT, 10 Mtn Div, FDNY who stated while he was giving SA (b)(6)(b)(7)(C) (US Army CID Agent) a ride to the FOB Hammer Landing Zone (LZ), he heard SA (b)(6)(b)(7)(C) mention that she had not been able to locate SPC (b)(6)(b)(7)(C) and still needed to talk to her and further take a look at her computer. SPC (b)(6)(b)(7)(C) stated he told SA (b)(6)(b)(7)(C) that he knew where SPC (b)(6)(b)(7)(C) lived and drove SA (b)(6)(b)(7)(C) to SPC (b)(6)(b)(7)(C) Place of Dwelling (POD). SPC (b)(6)(b)(7)(C) stated he walked up to SPC (b)(6)(b)(7)(C) POD and knocked on her door and was greeted by SPC (b)(6)(b)(7)(C). SPC (b)(6)(b)(7)(C) stated when he told SPC (b)(6)(b)(7)(C) there was a CID agent looking for her, her face turned red and she told him, "I only checked his (PFC MANNING's) emails...I was just being his friend." SPC (b)(6)(b)(7)(C) recalled SPC (b)(6)(b)(7)(C) was obviously nervous and concerned, but he did not think she was lying or trying to hide something. SPC (b)(6)(b)(7)(C) stated that shortly thereafter SPC (b)(6)(b)(7)(C) was interviewed by SA (b)(6)(b)(7)(C) and since that day he and SPC (b)(6)(b)(7)(C) had not had any discussion pertaining to PFC MANNING or that encounter. SPC (b)(6)(b)(7)(C) stated at no time SPC (b)(6)(b)(7)(C) told him that she had mailed any package or had done anything else other than checking PFC MANNING's e-mails nor did he tell anyone that SPC (b)(6)(b)(7)(C) had sent and/or received any package for PFC MANNING.

//////////////////////////////////LAST ENTRY//////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIG (b)(6)(b)(7)(C), (b) (7)(E)

DATE

31 Aug 10

EXHIBIT

188

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001075
Approved

(b)(6)(b)(7)(C)

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0634-10-CID034-

PAGE 1 OF 1 PAGE(S)

DETAILS

BASIS FOR INVESTIGATION: About 1255, 09 Sep 10, this office received a Request for Assistance (RFA) from the Computer Crime Investigative Unit (CCIU), Washington Metro Resident Agency (WMRA), Fort Belvoir, VA 22060 (FBVA), requesting this office locate, identify, and interview SPC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) 717th Military Intelligence (MI) Battalion (BN), Lackland Air Force Base (LAFB), San Antonio, TX 78243, with regards to PFC Bradley E. MANNING, (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division (MTN DIV), Forwarding Operating Base (FOB) Hammer, Iraq, stabbing or attempting to stab another Soldier during either Basic Training or Advanced Individual Training (AIT) with a pencil.

About 1710, 09 Sep 10, SA (b)(6)(b)(7)(C) interviewed SPC (b)(6)(b)(7)(C) who provided a sworn statement, wherein he admitted to knowing PVT MANNING, and witnessed PVT MANNING running towards PV2 (b)(6)(b)(7)(C) with his head down, and assault PV2 (b)(6)(b)(7)(C) with a wooden pencil. SPC (b)(6)(b)(7)(C) stated this incident occurred in the Squad Bay, during basic training at Fort Leonard Wood, MO, about the first of November 2007.

About 0915, 10 Sep 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) who stated that no further investigative leads needed to be completed by this office.

STATUS: Further activity by this office is not anticipated at this time. This matter is closed within the files of this office. Additional activity, if deemed necessary, will be conducted under a separate sequence. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Fort Hood CID Office
Fort Hood, TX 76544

SIGNATURE

(b)(6)(b)(7)(C)

DATE

10 Sep 10

EXHIBIT

189

FOR OFFICIAL USE ONLY - Law Enforcement Sensitive

0634-10-CID034-

SWORN STATEMENT

LOCATION: Fort Hood CID Office, Fort Hood, TX 76544 **DATE:** 09 Sep 10 **TIME:** 1710

NAME: (b)(6)(b)(7)(C)

SSN: (b)(6)(b)(7)(C)

STATUS: SPC / AD

ORGANIZATION/ADDRESS: B Company, 717 Military Intelligence Battalion, 470 Military Intelligence Brigade, Lackland Air Force Base, San Antonio, TX 78543

(b)(6)(b)(7)(C), (b)(6)(b)(7)(C) want to make the following statement under oath:

I attended basic training at Fort Leonard Wood, Missouri from October 2007 to December 2007. I was in C Company, 82nd division where I met PVT MANNING who was going to be a 35F. PVT MANNING was in the same platoon as I was and he slept two bunk beds down from me in the squad bay where we both had bottom bunk beds. Our drill sergeants were Senior Drill Sergeant SFC (b)(6)(b)(7)(C) and SSG (b)(6)(b)(7)(C). PVT MANNING was a weak willed person in my opinion, never wanting to participate in the daily activities during training. PVT MANNING was a quiet person who was easily annoyed and would usually keep to himself. PVT MANNING was a bunkmate with PVT (b)(6)(b)(7)(C). About the second week of Basic Training, there was an incident in which PVT MANNING and PVT (b)(6)(b)(7)(C) had a shouting match when PVT MANNING got upset about PVT (b)(6)(b)(7)(C) putting things on his bed. Around the 1st of November 2007, PVT MANNING was involved in an incident where he attempted to stab another Soldier possibly named PV2 (b)(6)(b)(7)(C) with a wooden pencil in the stomach about 2 to 3 times. PV2 (b)(6)(b)(7)(C) had been mocking PVT MANNING, provoking PVT MANNING for an unknown reason. PV2 (b)(6)(b)(7)(C) was a white male, possibly around six feet tall, bald, muscular build, big person. The other Soldiers in the platoon stopped the altercation, but I do not know if the Drill Sergeants ever found out about the incident. Before the completion of our basic training cycle PVT MANNING was removed from our cycle, due to lack of motivation and his low level of discipline, and set back into a later graduating class. After PVT MANNING was washed back in basic, I never saw him again until about October of 2009 when his current unit was switching locations with my unit 3 BCT, 82nd ABN DIV which was forward deployed to Bagdad, Iraq. PVT MANNING was a 35F and worked within the same SCIF as I did at the time of his arrival. PVT MANNING worked in the first section of the SCIF where the Secret Classified computers were, while I worked in the Top Secret section in the back of the SCIF. Occasionally, PVT MANNING would come to the back of the SCIF to get information about any targets and issues he was tasked to work on. (b)(6)(b)(7)(C)

Q: SA (b)(6)(b)(7)(C)

A: (b)(6)(b)(7)(C)

Q: Is the above statement typed in your own words?

A: Yes.

Q: Are you sure about the names of your Drill Instructors?

A: Yes, there was a third Drill Instructor, but I do not remember his name and I never knew any of their first names.

Q: What is PVT (b)(6)(b)(7)(C) first name?

A: I have no idea, but I am sure his last name was PVT (b)(6)(b)(7)(C)

INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

Page 1 of 4 Pages

FOR OFFICIAL USE ONLY - Law Enforcement Sensitive

EXHIBIT 190
001077
ENCL 2

FOR OFFICIAL USE ONLY – Law Enforcement Sensitive

0634-10-CID034-_____

"Statement of (b)(6)(b)(7)(C) Continued:"

LOCATION: Fort Hood CID Office, Fort Hood, TX 76544

Q: Describe PVT (b)(6)(b)(7)(C)

A: White male, Black hair, very short, maybe 4'11", I think his MOS was 88M, truck driver, very heavy facial hair, black unbrow.

Q: What was PV2 (b)(6)(b)(7)(C) first name?

A: I have no idea and I am about 80% sure his name was PV2 (b)(6)(b)(7)(C)

Q: Did you witness PVT MANNING stabbing, or attempting to stab PV2 (b)(6)(b)(7)(C)

A: Yes.

Q: Where did PVT MANNING attempt to stab PV2 (b)(6)(b)(7)(C)

A: In the Squad Bay, between the first bunk bed and the entrance/exit to the Squad Bay. There was only one entrance/exit to the squad bay.

Q: About how far away from PVT MANNING and PV2 (b)(6)(b)(7)(C) were you when this happened?

A: About 6-7 feet.

Q: What lead up to PVT MANNING attempting to stab PV2 (b)(6)(b)(7)(C)

A: PV2 (b)(6)(b)(7)(C) was the aggressor, but he was just making fun of PVT MANNING.

Q: Did PVT MANNING actually stab PV2 (b)(6)(b)(7)(C)

A: Yes, he made contact on the left side of PV2 (b)(6)(b)(7)(C) stomach.

Q: Did PV2 (b)(6)(b)(7)(C) have any clothes on at the time he was stabbed by PVT MANNING?

A: Yes, I believe it was an Army PT shirt.

Q: Was there any damage done to the Army PT shirt of PV2 (b)(6)(b)(7)(C)

A: No.

Q: What type of injury did PV2 (b)(6)(b)(7)(C) sustain?

A: None, no injury what so ever.

Q: What was PVT MANNING using to stab PV2 (b)(6)(b)(7)(C)

A: A yellow, wooden pencil and it was sharpened, but it had a dull point on it.

Q: Which hand did PVT MANNING have the pencil in?

A: His right hand.

Q: How many people did it take to stop this incident with PVT MANNING and PV2

(b)(6)(b)(7)(C)

A: It took about four people to break it up.

Q: Was anyone else injured?

A: No.

Q: Is it possible that this was a staged attack, and not intended to actually harm anyone?

A: Possibly, but PVT MANNING was very mad and charged PV2 (b)(6)(b)(7)(C) with his head down. PVT MANNING put his head into PV2 (b)(6)(b)(7)(C) stomach and was then trying to stab him with the pencil.

Q: Why was this incident not reported to the Drill Instructors?

A: Because if one person had gotten into trouble, everybody would have gotten into trouble.

Q: What is a 35F?

A: All source intelligence specialist.

Q: What is a SCIF?

A: Secret Compartmented Information Facility.

Q: Have you heard of any other incidences or problems with PVT MANNING?

A: No.

Q: How do feel that you were treated today?

INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

Page 2 of 4 Pages

FOR OFFICIAL USE ONLY – Law Enforcement Sensitive

EXHIBIT 190
001078 ac 2

FOR OFFICIAL USE ONLY - Law Enforcement Sensitive

0634-10-CID034-_____

"Statement of (b)(6)(b)(7)(C) Continued:"

LOCATION: Fort Hood CID Office, Fort Hood, TX 76544

A: Great.

Q: Is there anything else you would like to add to this statement?

A: No. ///End of Statement/// (b)(6)(b)(7)(C)

INITIALS OF PERSON MAKING STATEMENT

(b)(6)(b)(7)(C)

Page 3 of 4 Pages

FOR OFFICIAL USE ONLY - Law Enforcement Sensitive

EXHIBIT 190

001079 ENC 2

FOR OFFICIAL USE ONLY – Law Enforcement Sensitive

0634-10-CID034-_____

"Statement of (b)(6)(b)(7)(C) Continued:"

LOCATION: Fort Hood CID Office, Fort Hood, TX 76544

AFFIDAVIT

I, (b)(6)(b)(7)(C) HAVE READ (b)(6)(b)(7)(C) I HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 4 FULLY UNDERSTOOD THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(b)(6)(b)(7)(C)

WITNESSES:

Subscribed and sworn to before me, a person authorized by law
to administer oaths, on _____, 2010 at
Fort Hood (b)(6)(b)(7)(C)

ORGANIZATION AND ADDRESS

Special Agent (b)(6)(b)(7)(C), (b)(7)(E)
(Typed Name of Person Examining Sworn)

Title 10 USC, Section 936
(Authority to Administer Oath)

INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

Page 4 of 4 Pages

FOR OFFICIAL USE ONLY – Law Enforcement Sensitive

EXHIBIT 190
001080

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0010-10-CID321

PAGE 1 OF 2 PAGES

DETAILS

About 0700, 23 Aug 10, this office received a Request For Assistance under Report Of Investigation (ROI) 0028-10-CID221-10117 from the Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA, to locate and interview all cadre assigned to D Company, 305th Military Intelligence (MI) Battalion (BN), Fort Huachuca, AZ during the period when PFC Bradley MANNING, subject of ROI 0028-10-CID221-10117 was assigned to the unit for Advance Individual Training (AIT) at Fort Huachuca, AZ. Interviews were to determine if PFC MANNING posted a video to YouTube regarding Sensitive Compartmented Information Facilities (SCIFs) located on Fort Huachuca, AZ while attending AIT. Further, it was requested to determine if any record of Non-Judicial Punishment (NJP) or Uniform Code of Military Justice (UCMJ) action pertaining to PFC MANNING was available.

About 0930, 24 Aug 10, SA (b)(6)(b)(7)(C) interviewed SFC (b)(6)(b)(7)(C) D Company, 305th MI BN, Fort Huachuca, AZ regarding his knowledge of PFC MANNING's actions while attending AIT in 2008. SFC (b)(6)(b)(7)(C) related he was aware of whom PFC MANNING was, but he had been assigned to a different platoon and SFC (b)(6)(b)(7)(C) did not routinely come in contact with him. SFC (b)(6)(b)(7)(C) is aware of a video posted by PFC MANNING to YouTube but not the content; further he was aware that PFC MANNING had been required to provide an Operational Security (OPSEC) briefing to the unit as part of his punishment. SFC (b)(6)(b)(7)(C) was unaware of any NJP or UCMJ punishment given to PFC MANNING. SFC (b)(6)(b)(7)(C) provided nothing further of significance.

About 1130, 24 Aug 10, SA (b)(6)(b)(7)(C) interviewed WO1 (b)(6)(b)(7)(C) Task Force ODIN, Fort Hood, TX who was currently attending the Warrant Officer Basic Course at Fort Huachuca, AZ. WO1 (b)(6)(b)(7)(C) related he had been the assistant Platoon Sergeant for PFC MANNING during AIT. WO1 (b)(6)(b)(7)(C) related he was aware of a video posted by PFC MANNING to YouTube but not the content; further he was aware that PFC MANNING had been required to provide an Operational Security (OPSEC) briefing to the unit as part of his punishment and was also counseled for his actions by SFC (b)(6)(b)(7)(C) D Company, 305th MI BN. WO1 (b)(6)(b)(7)(C) was unaware of any NJP or UCMJ punishment given to PFC MANNING. WO1 (b)(6)(b)(7)(C) provided nothing further of significance.

About 1335, 27 Aug 10, SA (b)(6)(b)(7)(C) interviewed SFC(R) (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SFC(R) (b)(6)(b)(7)(C) related he was aware of this investigation and knew who PFC MANNING was from the unit. He was aware of the YouTube video as several soldiers had come to him to report the video. SFC(R) (b)(6)(b)(7)(C) remembered PFC MANNING had been counseled and had to provide training for the unit regarding OPSEC. SFC(R) (b)(6)(b)(7)(C) was unaware of any NJP or UCMJ punishment given to PFC MANNING. SFC(R) (b)(6)(b)(7)(C) provided nothing further of significance.

About 0930, 2 Sep 10, SA (b)(6)(b)(7)(C) interviewed SFC (b)(6)(b)(7)(C) who related he had been the Assistant Platoon Sergeant for PFC MANNING during AIT. SFC (b)(6)(b)(7)(C) related he was aware of PFC MANNING and when he had made the news for the WikiLeaks arrest, he had remembered the incident with the YouTube video during AIT and went to locate the "Smith" file containing documentation of incidents during PFC MANNING's AIT period to refresh his memory. SFC (b)(6)(b)(7)(C) learned the file had been

TYPED AGENT'S NAME AND SEQUENCE NUMBER

ORGANIZATION

Arizona Branch Office, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

DATE

10 Sep 10

EXHIBIT

191

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001081
Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0010-10-CID321

PAGE 2 OF 2 PAGES

DETAILS

destroyed approximately two months prior to the news story in accordance with the US Army's two-year retention and destruction policy. SFC (b)(6)(b)(7)(C) related his recollection of the video entailed PFC MANNING in his barracks room talking, as if to his mother, about life at AIT and he mentioned in the video that he had access to classified material during his AIT classes, which was what initiated the inquiry by his chain of command. SFC (b)(6)(b)(7)(C) is aware that PFC MANNING had been counseled regarding his actions by SFC(R) (b)(6)(b)(7)(C). Further PFC MANNING was ordered by the commander, CPT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) HHC, 22d Chemical Battalion, Aberdeen Proving Ground, MD to remove the video from the internet. SFC (b)(6)(b)(7)(C) related he had knowledge the video had been removed. SFC (b)(6)(b)(7)(C) was asked if he had any knowledge regarding a conversation intimating the chain of command should revoke PFC MANNING's security clearance and have him reclassified to another Military Occupational Specialty (MOS). SFC (b)(6)(b)(7)(C) related he overheard a conversation between SFC(R) (b)(6)(b)(7)(C) and other platoon sergeants discussing this matter but was unaware if it went any further or was presented to the chain of command as a recommendation. SFC (b)(6)(b)(7)(C) provided nothing further of significance.

About 1045, 10 Sep 10, SA (b)(6)(b)(7)(C) interviewed 1LT (b)(6)(b)(7)(C) Co E, 305th MI BN, Fort Huachuca, AZ. 1LT (b)(6)(b)(7)(C) related was the Executive Officer (XO) of the company while PFC MANNING was assigned for AIT. 1LT (b)(6)(b)(7)(C) related he could not recall if PFC MANNING had received NJP for the YouTube incident, which 1LT (b)(6)(b)(7)(C) was aware of. 1LT (b)(6)(b)(7)(C) related he had no knowledge of any documentation still existing at the unit as one of his duties was to ensure records were purged at the appropriate time as there was limited record keeping space. 1LT (b)(6)(b)(7)(C) provided nothing further of significance.

/////////////////////////////////LAST ENTRY/////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Arizona Branch Office, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

(b)(6)(b)(7)(C), (b)(7)(E)

DATE

10 Sep 10

EXHIBIT

191

OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001082
Approved

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0830, 9 Sep 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both assigned to Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, coordinated with Mr. (b)(6)(b)(7)(C) to obtain the contents of the broken open box of PFC MANNING's personal goods that (b)(6)(b)(7)(C) was storing. See AIR of the interview of Mr. (b)(6)(b)(7)(C) on 9 Aug 10. Mr. (b)(6)(b)(7)(C) signed a Consent to Search for the contents of the box. 2nd Brigade Combat Team 10th Mountain Division Fort Drum, NY(See Consent to Search for details).

Between 0830 and 1148, 9 Sep 10, SA (b)(6)(b)(7)(C) collected the box and its contents as evidence, which was documented on Evidence/Property Custody Document (EPCD), Document Number(DN) 130-10.

/////////////////////////////////LAST ENTRY/////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

WMRA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

SA- (b)(6)(b)(7)(C)

DATE

10 Sep 10

EXHIBIT

192

CID FORM 54 FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

1 FEB 77

001083
Approved

(b)(6)(b)(7)(C)

Date: 09 Sep 10	(b)(6)(b)(7)(C)	Consent To Search (USACIDC Supplement 1 to AR 190-22)		Time: 0830 EST	8:30 AM	(b)(6)(b)(7)(C)
1. Name of person consenting to the search: Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)		2. Organization and location: 167 Ames Street Rochester, NY				
3. I have been informed by the undersigned USACIDC Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law: Damage to U.S. Government Computer, 18 USC 1030(a)(5), Accessing U.S. Government Computer without and/or with Excess of Authorization, 18 USC 1030(a)(1), and Espionage, Article 106(a), UCMJ						
4. I have been requested by the undersigned USACIDC Special Agent to give my consent to a search of my person, premises, or property as indicated below. I have been advised of my right to refuse a search of my person, premises, or property. (If you <u>do not</u> give your consent, do not sign this form.)						
5. I hereby authorize the undersigned USACIDC Special Agent and/or other Authorized Law Enforcement Officials assisting the undersigned USACIDC Special Agent to conduct a search of: <i>(Initial and sign applicable blocks)</i>						
a.	My Person	Initials	Signature			
b.	My Quarters:	Initials	Signature			
Located At:						
c.	My Vehicle	Initials	Signature			
Located At:						
Described As:						
d.	Other	Initials	Signature (b)(6)(b)(7)(C)			
Located At: 167 Ames Street Rochester, NY						
Described As: Brown Box, containing multiple items, purportedly property of PFC MANNING.						
6. This written permission is given to the undersigned USACIDC Special Agent freely, voluntarily and without threats or promises of any kind:						
JA (b)(6)(b)(7)(C)		(b)(6)(b)(7)(C)		(b)(6)(b)(7)(C)		
Signature of USACIDC Special Agent		Signature of Person Granting Consent		(b)(6)(b)(7)(C)		

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0945, 10 Sep 10, SA (b)(6)(b)(7)(C), (b)(7)(E) SA (b)(6)(b)(7)(C), (b)(7)(E), and SA (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) all assigned to this office, conducted an evidence recovery scene examination of the Sensitive Item (SI) CONEX, property of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (2nd BCT), 10th Mountain Division (10th MTN DIV), Fort Drum, NY 13602 (FDNY), located at 10200 North Riva Ridge Loop, FDNY. This examination was conducted pursuant to a Search and Seizure Authorization issued by CPT (b)(6)(b)(7)(C) Military Magistrate, APO AE 09344, on 10 Sep 10.

1. Characteristics of the Scene: The SI CONEX was located in the north parking lot of HHC, 2nd BCT, 10th MTN DIV, FDNY, adjacent to the south side of North Riva Ridge Loop. The CONEX had its serial number USAU0480480 marked on all four sides of its exterior walls.

2. Condition of the Scene: The inside of the CONEX was dirty and in disarray. There were several individual storage boxes within the CONEX.

3. Factors Pertinent to Entry/Exit (E/E): The main and only E/E to the SI CONEX was facing south and locked and sealed and further showed no signs of tampering and/or foul play.

4. Scene Documentation: SA (b)(6)(b)(7)(C) prepared an evidence recovery scene sketch and took photographs of the scene using a Canon PowerShot SD1300IS digital camera (See Evidence Recovery Scene Sketch and CD for details).

5. Collection of Evidence: Between 1350-1446, 10 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one NetApp Computer Server "T Drive" containing unknown data, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 131-10.

About 1456, 10 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one Samsung Hard Disk Drive (HDD) containing PFC MANNING's profile which was documented on EPCD, DN 132-10.

Between 1601-1639, 10 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one NetApp Computer Server "T Drive" containing unknown data, which was documented on EPCD, DN 133-10.

Between 1825-2058, 10 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence 44 HDD's containing unknown data which was documented on EPCD, DN 135-10.

////////////////////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

s/ (b)(6)(b)(7)(C), (b)(7)(E)

DATE

10 Sep 10

EXHIBIT

194

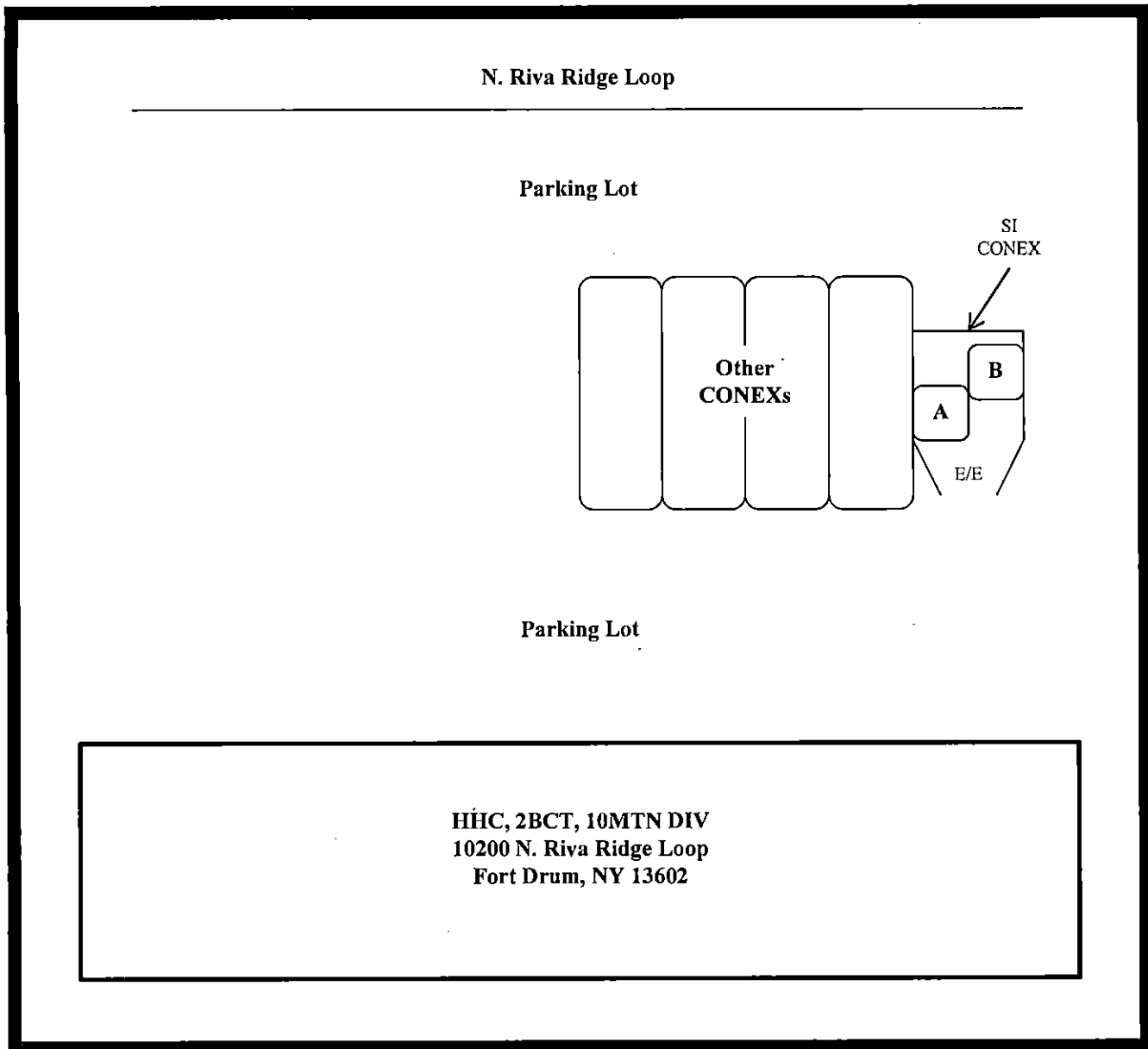
FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001085

Approved

(b)(6)(b)(7)(C)

ROUGH SKETCH DEPICTING RECOVERY SCENE

LEGEND

A- "T Drive" Computer Servers

B- (44) Hard Disk Drives

TITLE BLOCK

Case Number: 0028-10-CID221-10117

Offense: Damage to USG Computer, Accessing USG
Computer without and/or with Excess of
Authorization, and EspionageScene Portrayed: Parking lot of HHC, 2BCT, 10MTN
DIV, FDNY

Location: 10200 N. Riva Ridge Loop, FDNY

Victim: U.S. Government

Time/Date Began: 0945. 10 Sep 10

Sketched By: SA (b)(6)(b)(7)(C)

Verified By: SA (b)(6)(b)(7)(C)



NOT TO SCALE

FOR OFFICIAL USE ONLY LAW
ENFORCEMENT SENSITIVEEXHIBIT 195

001086

SI CONEX PHOTOS



FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 196
001087





APPROVED FOR TRANSPORT UNDER CUSTOMS SEAL

USA/70012-LN/03

TYPE

CMC 101

MANUF. No.

CM 31033

OWNER: PROPERTY OF U. S. ARMY

NSN: 8145-01-483-9125

CONTRACT NO. 6500502-B-1019-1309

TIMBER TREATMENT: ALL STEEL CONSTRUCTION

MANUFACTURED BY
CHARLESTON MARINE
CONTAINERS, INC.
CHARLESTON,
SC USA

CSC SAFETY APPROVAL

USA/LN/70012 10/01

DATE MANUFACTURED

IDENTIFICATION NO.

MAXIMUM GROSS WEIGHT

ALLOW STACK WT. 1.8G

RACKING TEST LOAD VALUE

DOORS/END WALL LOADING

10	/ 200
6759 KG	14940 LB
12200 KG	423280 LB
15240 KG	33600 LB
0.6P	

THIS CSC APPROVAL IS ONLY VALID FOR THE (2) UNITS
COUPLED TOGETHER WITH APPROPRIATE CONNECTIONS





PROFE

USACU0480480

F0286

Frustrate:
Bogey
L+P
L.P.
S I Z 6

WUWAA





001094

PACKING
LIST



001095





001097





ATTENTION

Before you install this unit, verify that your operating system is compatible with it. For safety considerations, read the disk drive type that came with your disk drive before you install it. You can also remove the disk drive from the unit to read the Manual Operating System Requirements label on the side of the disk drive unit.

For information about properly removing a disk drive from the unit, see the disk drive installation guide that came with your system.

1. Before you install this unit, verify that your operating system is compatible with it. For safety considerations, read the disk drive type that came with your disk drive before you install it. You can also remove the disk drive from the unit to read the Manual Operating System Requirements label on the side of the disk drive unit.

2. For information about properly removing a disk drive from the unit, see the disk drive installation guide that came with your system.



001100



NetApp

SYSTEM S/N:



300000442

Pool: X

FRAGILE



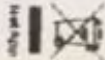
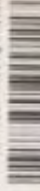
Always use proper handling techniques
when removing or installing the drive.

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed.

DRIVE S/N: VAX42E5A
NA P/N: 108-00083+A1



WARNING: Do not touch the
drive surface. Do not touch the
drive surface. Do not touch the
drive surface.

System Requirements
Fiber - Data ONTAP 6.4 for later
NetCache - Release 6.0 or later
Storage Hardware - DS14 PC
Additional product and configuration
information can be found at:
www.netapp.com

α. 1357, 10 SEP 10, (b)(6)(b)(7)(C)



Handwritten markings: 13, L, and a circled 'X'.

FIRMWARE: NA03

NA SN: VAX42E5A

PART No. 17R6349

WVN No. 20000000075E08F0

SERIAL No. 55VAX42E5A

MODEL: HUST10300FLF210

12V-0.08A 5V-1.18A

MADE IN SINGAPORE

Hitachi Global Storage Technologies

HDA REV. A

300GB 10,000rpm

10K300 Series HUST10300FLF210

HITACHI Ultrastar

CE, RoHS, and other regulatory marks.

UL N13506

12810

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

81206 5208 6111 2361

TESTED
SEP 07

N34



FRAGILE

Do not remove this item unless a bay blank or replacement module is installed.

Unlatch and wait 30 seconds for drive to spin down before removal. Place / store drive on cushioned surface.

INSERT INTO ENCLOSURE GENTLY

DRIVE SN: WAX429PA
NA PN: 108-00083-A1

Unit: 2.5" 15.2mm
Serial: 108-00083-A1

System Requirements
Fiber: Data ONTAP 6.4.4 or later
NetCache™: Release 6.0 or later
Storage Hardware: Storageshair DS147C

Additional product and configuration information can be found at:
www.netapp.com

b, 1403, 10SEP10,

(b)(6)(b)(7)(C)

FRAGILE



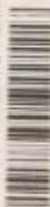
Warning: use if not returned to
Original Approved Packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX420VA
NA P/N: 108-00083+A1



Warning: Part No. 4276A-05
Serial Part No. SP-276A-05
System Requirements:
Firmware: Data ONTAP 6.4.4 or later
NetCache 11 Release 6.0 or later
Storage Hardware: Storageshair
DS14 FC
Additional product and configuration
information can be found at:
now.netapp.com

C. 1407. 10SEP10.

(b)(6)(b)(7)(C)

11

FIRMWARE: NA03



NA SN: VAX429VA



PART No. 17R6349



WWN No. 20000000875EA3D8



SERIAL No. 55VAX429VA



MODEL: HUS103030FLF210



12V±0.80A 5V±1.10A

MADE IN SINGAPORE

Hitachi Global Storage Technologies

300GB 10,000rpm
HDA REV. A

HARD DISK DRIVE
10K300 Series

HUS103030FLF210

Ultrastar™

HITACHI

CAUTION
Warranty void if any label or
screw is removed or broken or
a hole is closed.
Other patents pending
6.236.528 6.311.236
6.125.427 6.156.405 6.212.024
5.771.248 5.933.297 6.111.715
5.606.470 5.833.766 5.687.045
5.404.255 5.563.752 5.572.379
5.212.608 5.313.340 5.402.400
4.803.572 5.164.931 5.168.409

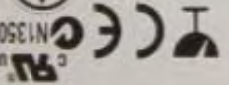
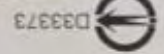
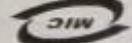
N02



12B18



E-H011-04-0050 (B)



0987



TESTED
SEP 07



N34

FRAGILE

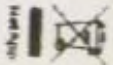


When using, hold it as required in
vertical / horizontal packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface
**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a buy-
back or replacement
module is installed

DRIVE 5.25" VAX2YMBA
NA P/N 108-00083-A1
Serial Part No. 108-00083-A1
System Requirements
Filter "Data Out" 6.4 A for later
NetCache™ Release 6.0 or later
Storage Hardware StorageShare
DS14 PC
Additional product and configuration
information can be found at:
http://netapp.com



d. 1411, 10SEP10

(b)(6)(b)(7)(C)

14 JB

FIRMWARE: NA83

NA SN: VAX2YMB4

PART No. 17R6349

WWN No. 2000000007AE5CC8

SERIAL No. 55VAX2YMB4

MODEL: HUST103030FLF210

12V=0.88A 5V=1.18A

MADE IN SINGAPORE

Hitachi Data Storage Technologies

HDA REV. A

300GB 10,000rpm

10K300 Series HUST103030FLF210

HITACHI Ultrastar™

CE

UL

13508

20

12810

NA82

4 803.572 5.154 501 5.168 405

5 212.608 5.313 540 5.402 400

5 404.266 5.963 752 5.572 378

5 506.470 5.833 786 5.587 343

5 771.248 5.833 287 5.114 715

5 125.427 5.105 405 5.212 024

5 206.028 5.211 235

CAUTION

Warning: void if any label or

mark is removed or broken or

if this is copied.

TESTED
SEP 07

NA4

INSERT INTO
ENCLOSURE
GENTLY

Do not remove this item unless a bay blank or replacement module is installed

Indefinite periods of time

DRIVE SN: VAX425TA

NA PAM 106-00083+A1



Abstract

Washing Machine

System Requirements

NotCachio™: Release 6.0 or later

Storage Hardware Storage Software DataTec

Additional product and configuration

now natapp.com

10

e, 1414, 10 SEP 10, (b)(6)(b)(7)(C)



9

FIRMWARE: NA03

NA SN: VAX425TA

PART NO: 17R6349

WWN No: 20000000007A559C6

SERIAL NO: 55VAX425TA

MODEL: HUS10300FLF210

12V=0.80A 5V=1.10A

MADE IN SINGAPORE

HDA REV. A

300GB 10,000rpm

10K300 Series HUS10300FLF210

HITACHI Ultrastar™

HARD DISK DRIVE

CAUTION

Do not remove the cover or
screw is removed or broken or
screw is covered.

4.803.572 5.154.401 5.166.408
5.212.409 5.213.340 5.402.400
5.404.205 5.563.792 5.672.279
5.606.470 5.623.796 5.687.045
5.771.248 5.903.297 6.111.715
6.125.427 6.196.409 6.212.024
6.226.528 6.311.236
Other parts pending

NO2

12B10

E-MET-04-0058 (B)

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

TESTED
SEP-07

N34

FRAGILE



Warning: do not return in
Vendor Approved Packaging

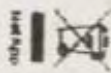
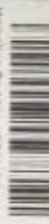
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX2R8MA

NA P/N: 108-00083 +A1



Warning: do not
insert into SP-176A-03

System Requirements

Filter: Data ONTAP 6.4.4 or later

NetCache™: Release 6.0 or later

Storage Hardware: Storageshell
DS14 FC

Additional product and configuration
information can be found at:
now.netapp.com

f.1417.10SEP10

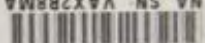
(b)(6)(b)(7)(C)

4
0
5

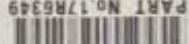
FIRMWARE: NA03



NA SN: VAXX2R8MA



PART NO: 17RB349



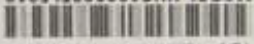
WVN NO: 20000000875E8F0B



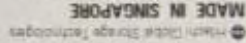
SERIAL NO: 55VAXX2R8MA



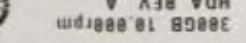
MODEL: HUST103030FLF210



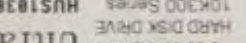
12V=0.80A 5V=1.10A



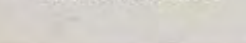
MADE IN SINGAPORE



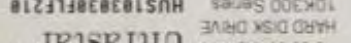
300GB 10,000rpm



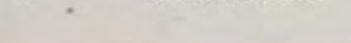
HDA REV. A



10K300 Series



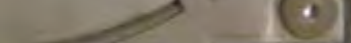
HUST103030FLF210



HITACHI Ultrastar™



HARD DISK DRIVE



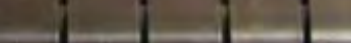
CE



20



CCC



UL



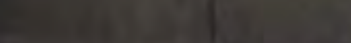
13508



SEP 07



TESTED



N34



CAUTION
Open parts pending
Warranty void if any label or
screen is removed or broken or
if tape is closed

4 803 572 8 164 901 9 168 400

5 212 609 5 913 340 5 402 400

5 404 205 5 063 752 5 572 379

5 806 470 5 833 766 5 887 045

5 771 346 5 833 297 5 111 715

5 125 427 5 136 409 5 212 004

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

6 236 528 6 211 236

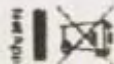
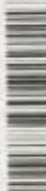
FRAGILE



Warning: use of not returned to
Vendor Approved Packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.
**INSERT INTO
ENCLOSURE
GENTLY**
Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N VAX41WLA
NA P/N 108-00083+A1



Warning: Part No. 1076488
Server Part No. 1076488
System Requirements
Filter Data OutTap 6.4 for later
NetCache™ : Release 6.0 or later
Storage Hardware : StorageShare
DS14 PC
Additional product and configuration
information can be found at:
now.netapp.com

9,1422. 10 SEP 10.

(b)(6)(b)(7)(C)



HITACHI
HARD DISK DRIVE
10K300 Series
HUS103030FL210

300GB 10,000rpm
HDA REV. A

MADE IN SINGAPORE
12V=0.80A 5V=1.10A

MODEL: HUS103030FL210

SERIAL NO. 55VAX41WLA

WVN NO. 2000000007A55ED9

PART NO. 17H6349

NA SN: VAX41WLA

FIRMWARE: NA03

CAUTION

Do not open the cover. If the cover is opened, the drive will be damaged. The drive is covered by a warranty. If the drive is damaged, the warranty will be void. The drive is covered by a warranty. If the drive is damaged, the warranty will be void.

7

S

TESTED
SEP 07

N34

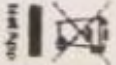
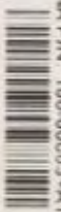
FRAGILE



Warning: until it has returned to
Manufacturer's packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.
**INSERT INTO
ENCLOSURE
GENTLY**
Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX42A3A
NA P/N: 108-00093-A1
Warning: Part No. 4276A-02
Serial Part No. 376A-02
System Requirements:
Filer: Data ONTAP 6.4.4 or later
NetCache™: Release 6.0 or later
Storage Hardware: Storageshair
DS14 FC
Additional product and configuration
information can be found at:
http://netapp.com



i, 1432.10SEP10.

(b)(6)(b)(7)(C)

5 &

FIRMWARE: NA83



NA SN: VAXX4243A



PART NO. 17R6349



WWN No. 2000000007A55F1E



SERIAL No. 55VAX4243A



MODEL: HUS10308FLF210



12V ± 0.88A 5V ± 1.10A

MADE IN SINGAPORE

Hitachi Global Storage Technologies

300GB 10,000rpm

HDA REV. A

10K300 Series

HARD DISK DRIVE

HITACHI

Ultrastar™

HUS10308FLF210

10K300 Series

HARD DISK DRIVE

HITACHI

Ultrastar™

HUS10308FLF210

10K300 Series

HARD DISK DRIVE

HITACHI

Ultrastar™

HUS10308FLF210

10K300 Series

HARD DISK DRIVE

HITACHI

Ultrastar™

HUS10308FLF210

10K300 Series

HARD DISK DRIVE

HITACHI

Ultrastar™

HUS10308FLF210

10K300 Series

HARD DISK DRIVE

HITACHI

Ultrastar™

HUS10308FLF210

10K300 Series

HARD DISK DRIVE

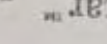
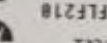
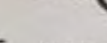
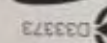
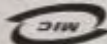
CAUTION

Warning: void if any label or
mark is removed or broken or
if this is covered.

N02



12B10



TESTED
SEP 07
0907

N34



FRAGILE



carefully seal it and returned to
Vendor Approved Packaging

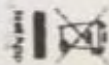
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a Day
blank or replacement
module is installed

DRIVE SAN VAX40-1VA

NA P/N 108-00083-A1



Handling and Storage
Requirements
System Requirements:
Filter: Data ONTAP 6.4 or later
NetCache 5.0 or later
Storage Hardware: StorageSPi1
DS14 FC
Additional product and configuration
information can be found at:
http://netapp.com

K.1437. 10SEP10.

(b)(6)(b)(7)(C)



3

FORMWARE: NAB3

NA SN: VAXXAHYA

PART NO: 17R0349

WVWV NO: 288888887A5508E

SERIAL NO: 55VAXXAHYA

MODEL: HUS1838FL218

12V-8.98A 5V-1.18A

MADE IN SINGAPORE

HDA REV. A

3R8GB 10,000rpm

10,000 RPM HUS1838FL218

HITACHI Ultrastar

CAUTION
Do not touch the surface of the disk.
If you touch the surface, the data may be lost.
If you touch the surface, the disk may be damaged.
If you touch the surface, the disk may be scratched.
If you touch the surface, the disk may be bent.
If you touch the surface, the disk may be broken.

12818

12818

12818

12818

12818

12818

12818

12818

12818

12818

TESTED
SEP 07

N34

FRAGILE



Always use it in its original
padding and packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX3EK0A
NA P/N: 108-00083-A1



Warning: Part No. X276A-B5
Serial Part No. SP-276A-B5
System Requirements:
Filer: Data ONTAP® 6.4.4 or later
NetCache™: Release 6.0 or later
Storage Hardware: Storageshelf
DS14 FC
Additional product and configuration
information can be found at:
now.netapp.com

1, 1441, 10SEP10.

(b)(6)(b)(7)(C)

#2

FW: NAB3

NA SN: VAX3EK0A

PART NO. 17R6349

WVN No. 2000000087A5AFE

SERIAL No. 55VAX3EK0A

MODEL HUS103030FL210

12V 8.80A 5V 1.18A

MADE IN SINGAPORE

Hitachi Global Storage Technologies

HDA REV. A

300GB 10,800rpm

10K300 Series

HARD DISK DRIVE

HUS103030FL210

Ultrastar™

HITACHI

CAUTION
Do not touch the surface of the disk or the head.
If the head is exposed, the disk may be damaged.
If the disk is damaged, the data may be lost.
If the head is exposed, the disk may be damaged.
If the disk is damaged, the data may be lost.

NO2

12B10

12B10

12B10

12B10

12B10

12B10

12B10

12B10

TESTED
SEP 07
0907

N34



m. 1444, 10SEP10

(b)(6)(b)(7)(C)



1

FIRMWARE: NAB3

Warranty void if any label or
mark is removed or broken or
a hole is drilled.

CAUTION

Overheating warning
4 803 572 5 184 301 5 188 400
5 212 508 5 313 540 5 402 400
5 404 255 5 563 752 5 572 278
5 606 470 5 633 796 5 687 040
5 771 248 5 833 297 8 111 775
8 129 407 8 198 405 8 212 004
8 226 508 8 311 298

NO2

12818

12V=0.80A 5V=1.18A
E-Mark: 04-04-0404 (M)



D33373



UL US
N13508

HITACHI Ultrastar™
HARD DISK DRIVE
10K300 Series
HUST10300FL210

300GB 10,000rpm
HDA REV. A

MADE IN SINGAPORE
Hitachi Global Storage Technologies

TESTED
SEP 07
0307

N34

FRAGILE

Unlatch and wait 30 sec for drive to spin down before removal. Place / store drive on cushioned surface.

INSERT INTO ENCLOSURE GENTLY

Do not remove this item unless a day blank or replacement module is installed.

DRIVE SN: VAX3T2H4
NA P/N: 108-00003-A1

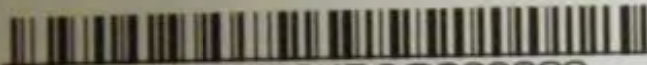
WARNING: Part No. 8726A-01
Access Point 8726A-01
System Requirements
Filter: "Data ONTAP" 6.4 for later
NetCache™ 1 Release 6.0 or later
Storage Hardware: Storageware
DS14 PC

Additional product and configuration information can be found at
now.netapp.com

N.1446.10SEP10.

(b)(6)(b)(7)(C)

<http://www.samsunghdd.com> or <http://www.samsunghdd.co.kr>



S/N: S1NSJDOQ800999

Model : HM121HJ
HDD P/N : HM121HJ/D
LBA 234,441,648 120.0GB MP2

REV. A
F/W : 2AA00_00



WARRANTY VOID IF REMOVED



KR-0H318D-39794-
882-00RR-A00

Made in Korea

DP/N 0H318D

SATA
120 GB
RPM 7200
FW : 2AA00_00

Cet appareil numérique
de la classe B est conforme
à la norme NMB-003 du Canada.

SAMSUNG



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

DO NOT COVER



P / N : 309611C0704339

1456, 10SEP10.

(b)(6)(b)(7)(C)



001127



001128







MOBILE

ATTENTION
Before you install this disk shelf, verify that your operating system is
compatible with it. To verify compatibility, read the disk shelf's
compatibility with your disk drive and/or disk shelf. You can also verify
a disk drive's compatibility with the disk shelf by reading the disk drive's
System Requirements label on the side of the disk drive's outer
shell. For information about properly connecting a disk drive to the disk
shelf, see the disk shelf installation guide that came with your
system.

ATTENTION
Before you install this disk shelf, verify that your operating system is
compatible with it. To verify compatibility, read the disk shelf's
compatibility with your disk drive and/or disk shelf. You can also verify
a disk drive's compatibility with the disk shelf by reading the disk drive's
System Requirements label on the side of the disk drive's outer
shell. For information about properly connecting a disk drive to the disk
shelf, see the disk shelf installation guide that came with your
system.

ATTENTION
Before you install this disk shelf, verify that your operating system is
compatible with it. To verify compatibility, read the disk shelf's
compatibility with your disk drive and/or disk shelf. You can also verify
a disk drive's compatibility with the disk shelf by reading the disk drive's
System Requirements label on the side of the disk drive's outer
shell. For information about properly connecting a disk drive to the disk
shelf, see the disk shelf installation guide that came with your
system.



001132



001133



001134



MODULE

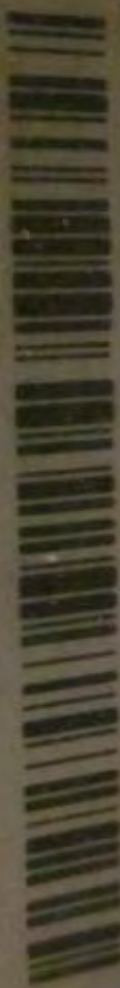
CAUTION
Before you install the disk shelf, verify that your operating system is
compatible with it. To verify compatibility, read the disk drive type
that came with your disk drive and/or disk shelf. You can also compare
System Requirements listed on the side of the disk drive cabinet.
For information about properly mounting a disk drive from the disk
shelf, see the disk shelf installation guide that came with your
system.

CAUTION
Before you install the disk shelf, verify that your operating system is
compatible with it. To verify compatibility, read the disk drive type
that came with your disk drive and/or disk shelf. You can also compare
System Requirements listed on the side of the disk drive cabinet.
For information about properly mounting a disk drive from the disk
shelf, see the disk shelf installation guide that came with your
system.

CAUTION
Before you install the disk shelf, verify that your operating system is
compatible with it. To verify compatibility, read the disk drive type
that came with your disk drive and/or disk shelf. You can also compare
System Requirements listed on the side of the disk drive cabinet.
For information about properly mounting a disk drive from the disk
shelf, see the disk shelf installation guide that came with your
system.



S/N: SHU76605001D4CA



Assembled in USA



P/N: 05-02



FRAGILE

Unlatch and wait 30 sec. for drive to spin down before removal. Place / store drive on cushioned surface.

INSERT INTO ENCLOSURE GENTLY

Do not remove this item unless a bay blank or replacement module is installed.

Warranty void if not returned in Vendor Approved Packaging

DRIVE S/N: VAX3NEHA

NA P/N: 10B-00083+A1

Hitachi Data Systems
System Requirements
Firmware: 0.4.4 or later
HostCache: Release 0.0 or later
Storage Hardware: StorageShare
OS: 4.0 or later

Additional product and configuration information can be found at:
www.hitapp.com

00, 1610, 10 SEP 10

(b)(6)(b)(7)(C)



FRAGILE



Warranty void if not returned in
Vendor Approved Packaging

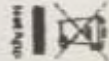
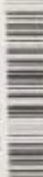
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX3MKA

NA P/N: 108-00083-A1



Warning: Do not use the drive
before the next release.
System Requirements
Firmware: Data ONTAP 6.4.4 or later
HotCache 1 Release 6.0 or later
Storage Hardware: DS147C
Additional product and configuration
information can be found at:
now.netapp.com

01, 109EP10
L167

(b)(6)(b)(7)(C)



FIRMWARE: NAB3

NA SN: VAX3MK4A

PART NO: 17R6349

WWN No: 200000000756258

SERIAL NO: 55VAX3MK4A

MODEL: HUS10300FL210

12V 0.88A 5V 1.10A

MADE IN SINGAPORE

Hitachi Data Storage Technologies

HDA REV. A

300GB 10,000rpm

10K300 Series

HARD DISK DRIVE

Ultrastar™

HUS10300FL210

CE

UL

N13508

20

033373

12010

N02

4 603 572 5 104 931 5 168 424

5 212 008 5 213 340 5 402 400

5 404 305 5 563 752 5 572 379

5 508 470 5 833 796 5 687 045

5 771 248 5 833 297 5 111 715

5 425 427 5 156 405 5 212 034

5 206 528 5 311 236

Other parts pending

CAUTION

Warning: void if any label or

sticker is removed or broken or

if tape is covered.

TESTED

SEP 07

0907

N34

FRAGILE

Unlatch and wait 30 sec for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
label unless a bay
blank or replacement
module is installed.

DRIVE 5M VAX31VMA
NA P/N 100.00003 +A1

System Requirements
Prior: 68010 or later
Firmware: 68010 or later
Storage Hardware: StorageShare
DS14 TC

Additional product and configuration
information can be found at:
www.hi3100.com

02, 1620, 10SEP10, (b)(6)(b)(7)(C)



2

FORMWARE NAB3

CAUTION
Do not touch the disk surface.
If the disk is touched, the data may be lost.
If the disk is touched, the data may be lost.

NA SN: VAXXNMA

PART NO: 17M6349

WVH NO: 20000000075E8050

SERIAL NO: 55VAXXNMA

MODEL: HUS10300FL210

12V-8.80A 5V-1.10A

MADE IN SINGAPORE

HDA REV A

10000 10,000rpm

10K300 Series HUS10300FL210

HITACHI Ultrastar™

CE

20

12810

NO2

12810

TESTED
SEP 07
0307

N34



03, 1622, 10SEP10,

(b)(6)(b)(7)(C)



3

FIRMWARE: MA03

CAUTION
Warranty void if any label is
removed or broken or
if not as shown.

Other patents pending
4K03.572 3.154.501 3.198.405
3.212.509 3.213.340 3.402.400
3.404.255 3.583.752 3.572.378
3.608.470 3.633.766 3.587.045
3.771.248 3.823.287 3.111.715
3.125.427 3.156.428 3.212.004
3.236.528 3.211.236

MADE IN SINGAPORE

12V=0.80A 5V=1.10A

MODEL: HUS183038FL210

SERIAL NO. 55VAXX2RWLA

WWN No. 2000000087566C87

PART No. 17R6349

NA SN: VAXX2RWLA

300GB 10,000rpm

HDA REV. A

MADE IN SINGAPORE

Hitachi Data Storage Technology

10K300 Series HUS183038FL210

HARD DISK DRIVE

HITACHI Ultrastar™

CE N13508

20

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

033373

TESTED
SEP 07
0007

N34

FRAGILE



Warranty void if not returned to
Vendor Approved Packaging

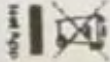
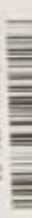
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX31NVT4

NA P/N: 108-00003+A1



Handling Precautions: 42164-01
Server Factory Settings: 01
System Requirements:
Firmware: Data ONTAP 6.4.4 or later
NetCache: Release 6.0 or later
Storage Hardware: DS147C
Additional product and configuration
information can be found at:
now.netapp.com

04, 1624, 10 SEP 10

(b)(6)(b)(7)(C)



Handwritten mark: a stylized 'H' or 'A'.

FIRMWARE: NA83

NA SN: VAX3NVT4

PART NO. 17R6349

WVN NO. 200000000756676

SERIAL NO. 55VAX3NVT4

MODEL HUST10300FLF210

12V 8.80A 5V 1.10A

MADE IN SINGAPORE

Hitachi Global Storage Technologies

HDA REV. A

300GB 10,000rpm

10K300 Series HUST10300FLF210

HITACHI Ultrastar™

HARD DISK DRIVE

UL
N13505

CE

20

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

120

TESTED
SEP 07
0907

N34

FRAGILE



Warranty void if not returned in
Vendor Approved Packaging

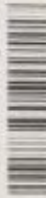
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a buy
blank or replacement
module is installed

DRIVE S/N VAX2TG6A

NA P/N 108-00083-A1



Warning: Part No. 0276A.05

Serial Part No. 0276A.05

System Requirements:

Filter: "Data OUT" 6.4.4 or later

NetCache: Release 6.0 or later

Storage Hardware: StorageShare

OS/4 PC

Additional product and configuration
information can be found at:
now.netapp.com

05, 1626, 105EP10.

(b)(6)(b)(7)(C)



5

FIRMWARE: NAB3

NA SN: VAXX2166A

PART No. 17R6349

WVN No. 20000000875664DA

SERIAL No. 55VAXX2166A

MODEL: HUST103030FLF218

12V-0.80A 5V-1.18A

MADE IN SINGAPORE

Hitachi Data Storage Technologies

HDA REV. A

300GB 10,000rpm

10K300 Series

HARD DISK DRIVE

HUST103030FLF218

Ultrastar™

HITACHI

CE N13508

20

033373



E-H011-94-005A (H)

12B10

4 800 572 5 184 801 5 188 400

5 212 806 5 213 340 5 400 400

5 404 256 5 563 752 5 572 378

5 606 470 5 833 287 5 847 715

5 771 248 5 933 287 5 947 715

5 125 427 5 156 405 5 212 024

5 206 528 5 211 236

Other patterns pending

CAUTION

Warranty void if any label or screw is removed or broken or if cover is closed

TESTED
SEP 07
0307

N34

FRAGILE



Warranty void if not returned in
Vendor Approved Packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

INSERT INTO
ENCLOSURE
GENTLY

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX32UKA

NA P/N: 108-00083-A1



Warning: Do not touch the
drive surface. Do not breathe
on the drive. Do not use the
drive in a high-temperature
environment. Do not use the
drive in a high-vibration
environment. Do not use the
drive in a high-magnetic-field
environment. Do not use the
drive in a high-electric-field
environment. Do not use the
drive in a high-radiation
environment. Do not use the
drive in a high-pressure
environment. Do not use the
drive in a high-velocity
environment. Do not use the
drive in a high-acceleration
environment. Do not use the
drive in a high-deceleration
environment. Do not use the
drive in a high-impact
environment. Do not use the
drive in a high-shock
environment. Do not use the
drive in a high-vibration
environment. Do not use the
drive in a high-magnetic-field
environment. Do not use the
drive in a high-electric-field
environment. Do not use the
drive in a high-radiation
environment. Do not use the
drive in a high-pressure
environment. Do not use the
drive in a high-velocity
environment. Do not use the
drive in a high-acceleration
environment. Do not use the
drive in a high-deceleration
environment. Do not use the
drive in a high-impact
environment. Do not use the
drive in a high-shock
environment.

01, 1629, 10SEP10

(b)(6)(b)(7)(C)



f

FIRMWARE: NA03

NA SN: VAX32UKA

PART NO. 1786349

WVN NO. 20000000075E6989

SERIAL NO. 55VAX32UKA

MODEL: HUS103030FLF210

12V=0.80A 5V=1.10A

MADE IN SINGAPORE

Hitachi Global Storage Technologies

HDA REV. A

300GB 10,800rpm

HARD DISK DRIVE 10K300 Series HUS103030FLF210

HITACHI Ultrastar™

CE RoHS

20

MIC

E-HR11-04-0050 (01)

NO2

12818

4 803 572 5 164 901 5 165 408
5 212 809 5 213 240 5 402 400
5 404 205 5 563 752 5 572 378
5 506 470 5 603 766 5 687 045
5 771 246 5 833 287 5 111 715
6 125 427 5 156 406 5 212 024
6 236 526 6 311 206

CAUTION
Warranty void if any label or
screw is removed or broken or
a hole is closed.

TESTED
SEP 07

N34

FRAGILE



Warranty void if not returned in
Vendor Approved Packaging

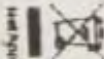
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX3EXSA

NA P/N: 108-00083-A1



WARNING: RISK OF INJURY
DANGER: RISK OF INJURY
System Requirements
Firmware: 0.4.4 or later
NetCache: 1. Release 6.0 or later
Storage Hardware: StorageShare
DS14FC
Additional product and configuration
information can be found at:
now.netapp.com

08,1631,1052P10

(b)(6)(b)(7)(C)



2

PRINTED NAME

NA SN VAXXEXSA

PART NO. 1705345

W/WN NO. 200000007A1000E

SERIAL NO. 55VAXXEXSA

MODEL HUS18300FL7210

12V-8.88A 5V-1.70A

MADE IN SINGAPORE

NOA REV. A

2000 10,000rpm

10K300 3.5" 7200

HARD DISK DRIVE

HITACHI Ultrastar™

HUS18300FL7210

10K300 3.5" 7200

2000 10,000rpm

NOA REV. A

MADE IN SINGAPORE

PART NO. 1705345

W/WN NO. 200000007A1000E

NA SN VAXXEXSA

PRINTED NAME

CAUTION

DO NOT OPEN

DO NOT TOUCH

DO NOT BREATHE

DO NOT SMOKING

DO NOT EATING

DO NOT DRINKING

DO NOT SLEEPING

DO NOT WORKING

DO NOT PLAYING

DO NOT DRIVING

DO NOT FLYING

DO NOT SWIMMING

DO NOT BOATING

DO NOT CAMPING

DO NOT HIKING

DO NOT JUMPING

DO NOT RUNNING

DO NOT SKATING

DO NOT SLIDING

DO NOT CLIMBING

DO NOT CRAWLING

DO NOT CRAWLING

DO NOT CRAWLING

DO NOT CRAWLING

TESTED
SEP 07

NS4

FRAGILE



Warranty void if not returned in Vendor Approved Packaging

Unlatch and wait 30 secs for drive to spin down before removal. Place / store drive on cushioned surface.

INSERT INTO ENCLOSURE GENTLY

Do not remove this item unless a bay, blank or replacement module is installed

DRIVE S/N: VAX3N4SA
NA P/N: 108-00083-A1



Using Part No. 4272A-05
Serial Part No. 376A-02

System Requirements
Firmware: Data ONTAP 6.4 or later
MeiCache: Release 6.0 or later
Storage Hardware: StorageShield DS14 PC

Additional product and configuration information can be found at:
now.netapp.com



NetApp

09, 1632.10SEP10,

(b)(6)(b)(7)(C)



5

FIRMWARE: MAB3

NA SN: VAX3N45A

PART No. 17M6349

WVN No. 20000000087566448

SERIAL No. 55VAX3N45A

MODEL: HUST103030FLF210

12V-0.80A 5V-1.10A

MADE IN SINGAPORE

Hitachi Data Storage Technologies

HDA REV. A

300GB 10,000rpm

10K300 Series HUST103030FLF210

HITACHI Ultrastar™

CAUTION
Warranty void if any label or
screw is removed or broken or
a hole is poked.
Other patents pending
8.236 528 8.311 298
8.125 427 8.106 405 8.212 024
8.771 048 8.933 287 8.111 715
8.808 470 8.833 768 8.687 045
8.404 255 8.963 752 8.572 379
8.212 808 8.313 340 8.402 400
8.103 572 8.164 931 8.168 409

NO2

12810

12810

EE 20 002

20

CE

UL US

TESTED
SEP 07

N34

Merchants sold if not returned in
Vendor Approved Packaging



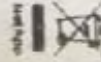
FRAGILE

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a day
blank or replacement
module is installed.

DRIVE S/N: VAX15REA
NA P/N: 108-00083-A1
Warning: Part No. 2215A-01
Store Part No. 2215A-01
System Requirements:
Fiber, Data ONTAP 6.4.4 or later
NetApp's NetApp 6.4 or later
Storage Hardware: StorSafe
OS14 FC
Additional product and configuration
information can be found at:
now.netapp.com



10.1634.10SEP10

(b)(6)(b)(7)(C)



HITACHI
HARD DISK DRIVE
10K300 Series
HUST10300FL210

300GB 10,000rpm
HDA REV. A
MADE IN SINGAPORE
12V-0.88A 5V-1.10A

MODEL: HUST10300FL210
SERIAL NO. 55VAX35NEA
WVN No. 2000000075550F5

PART NO. 17R0349
NA SN: VAX35NEA

CAUTION
Do not remove the top cover
Access is restricted to authorized personnel only

4 001 572 0 104 931 0 104 409
0 212 008 0 213 040 0 402 409
0 404 255 0 503 702 0 572 579
0 506 470 0 503 700 0 507 045
0 777 045 0 803 297 0 111 715
0 120 427 0 104 409 0 212 004

CAUTION
Do not remove the top cover
Access is restricted to authorized personnel only

FRONT VIEW: NAB3

10

TESTED
SEP 07
0007

N34

FRAGILE



Warranty void if not returned in
Vendor Approved Packaging

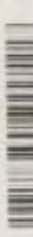
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N VAX3PRHA

NA P/N 108-00083-A1



WARNING: Part 108-00083-A1
is a Class 1 Laser Product.

System Requirements

File: Data ONTAP 6.4.4 or later

NetCache: Release 6.0 or later

Storage Hardware: StorageShield
DS14 FC

Additional product and configuration
information can be found at
now.netapp.com

11, 1635, 10SEP10.

(b)(6)(b)(7)(C)



HITACHI Ultrastar™
HARD DISK DRIVE
10K300 Series
HUS103030FLF210

300GB 10,000rpm
HDA REV. A

MADE IN SINGAPORE
12V 0.88A 5V 1.18A
E-H011-04-0058 (B)

MODEL: HUS103030FLF210
SERIAL No. 55VAX3PRHA

WVN No. 20000000875E7FAB
PART No. 17R6349

NA SN: VAX3PRHA
FIRMWARE: NA03

CAUTION
Warning: Do not touch the disk surface.
If the disk surface is scratched, the data may be lost.
If the disk surface is scratched, the data may be lost.

Other features pending
B 220 528 6 211 206
B 125 427 8 156 405 6 212 024
B 171 245 5 933 297 6 111 715
B 608 470 5 633 766 5 667 045
B 404 255 5 563 752 5 572 379
B 212 809 5 913 340 5 402 400
B 503 572 5 954 951 5 168 409

TESTED
SEP 07
N34

FRAGILE



Warranty void if not returned in
Vendor Approved Packaging

Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a bay
blank or replacement
module is installed

DRIVE S/N: VAX3MM00A

U/A P/N: 100-00003+A1



Hard Copy

Warning: Do not use
direct force on the drive

System Requirements

Filter: Data ONTAP 6.4 or later

NetCochet: Release 6.0 or later

Storage Hardware: StorageShare
DS14 FC

Additional product and configuration
information can be found at:
www.netapp.com

12. 1636, 10SEP10

(b)(6)(b)(7)(C)



12

FIRMWARE: NA03

NA 5N VAX3MMBA

PART NO. 17R6349

W/N No. 200000000756F19

SERIAL NO. 55VAX3MMBA

MODEL HUS103030FLF210

12V-8.80A 5V-1.10A

MADE IN SINGAPORE

HDA REV. A

300GB 10,000rpm

10K300 Series HUS103030FLF210

HITACHI Ultrastar™

CAUTION

Warning: void if any label or screw is removed or broken or a hole is caused.

Other permits pending
0 200 520 0 211 230
0 120 427 0 150 405 0 212 024
0 171 240 0 033 207 0 111 715
0 000 470 0 033 207 0 007 045
0 404 205 0 033 207 0 072 379
0 212 020 0 212 340 0 402 400
0 003 572 0 104 031 0 100 400

NO2

12810

0 000 000

0 000 000

0 000 000

0 000 000

0 000 000

TESTED
SEP '07
0007

N34

Warranty void if not returned in
Vendor Approved Packaging



FRAGILE

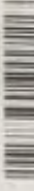
Unlatch and wait 30 secs for
drive to spin down before
removal. Place / store drive
on cushioned surface.

**INSERT INTO
ENCLOSURE
GENTLY**

Do not remove this
item unless a day
blank or replacement
module is installed

DRIVE S/N: VAX 32X6A

NA P/N: 108-00083-A1



Warning: Handle with care

System Requirements

Filter: Data Center 6.4 or later

NetCache: Release 6.0 or later

Storage Hardware: StorageShare

DS147C

Additional product and configuration
information can be found at:
<http://www.netapp.com>

13, 1639, 10SEP10

(b)(6)(b)(7)(C)

General Dynamics CHS-3 Warranty Item Cage Code: 67032
Contract No.: DAAH01-03-D-0029 Warranty Stop Date: 02/2014
Item: FFP - 300GB DRIVE (DELL 6950)
P/N: 02-2801679-1 CHS-3 Hotline: 877-247-7711

S/N: SEE VENDOR S/N

NSN:

Cheetah 15K.6

N176 D33827

Manufactured by Seagate Technology Int'l

MODEL NUMBER: *ST3300656SS*

LOT NUMBER: *R-01-0017-5*

新加坡製

MADE IN SINGAPORE

ST3300656SS

VDC AMP5 CS0 LOT
#5 1.8 NUMBER
#12 1.8

PART NUMBER: *8CH066-R50*

UIN: 5000CS00040F2200

SERIAL NUMBER: *30P0E452*

FIRMWARE HS09

THIS PRODUCT IS MANUFACTURED UNDER ONE OR MORE PATENTS OF THE UNITED STATES
OR OTHER COUNTRIES, OWNED OR LICENSED BY SEAGATE TECHNOLOGY LLC

Serial Attached SCSI (SAS)

Capacity: 300GB

RPM: 15K

Firmware: HS09

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

HAM2 6950

DRIVE 2

1825, 10JEP10,

(b)(6)(b)(7)(C)

DELL™



156585

General Dynamics CHS-3 Warranty Item Cage Code: 67032

Contract No.: DAAH01-03-D-0029

Warranty Stop Date: 02/2014

Item: FFP-300GB DRIVE (DELL 6950)

P/N: 02-2801679-1

CHS-3 Hotline: 877-247-7711

S/N: SEE VENDOR S/N

NSN:

ST3300656SS

PART NUMBER: *9CH066-850*

SERIAL NUMBER: *3Q2F6J1*

VOL AMPS CSQ LOT
+5 1.0 NUMBER
+12 1.0

UJN15000CS0004BA63D4

FIRMWARE HS09

THIS PRODUCT IS MANUFACTURED UNDER ONE OR MORE PATENTS OF THE UNITED STATES OR OTHER COUNTRIES OWNED OR LICENSED BY SEAGATE TECHNOLOGY LLC.

Serial Attached SCSI (SAS)

Capacity: 300GB

RPM: 15K

Firmware: HS09

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

MADE IN SG

DP/N 0VP778

12531-00

HAM2 6950
DRIVE 1

1852.10SEP10.

(b)(6)(b)(7)(C)

Rev A00

MADE IN MEXICO
1-888-387-4333
MS-00000-7007



(b)(6)(b)(7)(C)

033073

Fujitsu
Taiwan Ltd
13F No. 38,
Sec 1, Chung-Hua
Road, Taipei, Taiwan



MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
8 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057KS

FUJITSU LIMITED



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

2443 (R)



HDD S/N: DA03P7A057KS

2d BCT, 10th MTN DIV
SDE (P17 FINAL)
HD0 SET3

1905, 10 SEP 10

(b)(6)(b)(7)(C)

D33073

Fujitsu
Taiwan Ltd.
19F No. 39,
Sec 1, Chung-hwa
Road, Taipei, Taiwan



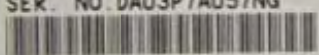
N124

WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN.

APL
NOT BE MANUFACTURED UNDER ONE
OF FOLLOWING U.S. PATENTS:
6,201,888; 6,928,876; 6,784,881;
6,189,883; 6,778,820; 6,846,882;
6,880,042; 6,981,874; 6,918,147;
6,154,888; 6,158,162; 6,181,884;
6,179,338; 6,201,870; 6,201,240;
6,300,884; 6,409,323; 6,182,814;
6,158,888; 6,942,812; 6,919,888

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
8 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057NG

FUJITSU LIMITED



This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

2443(B)



HDD S/N: DA03P7A057NG

2d BCT, 10th MTN DIV
MSG (P17 FINAL)
HD0 SET3

TO EXPOSE ADHESIVE REMOVE LINER
TO EXPOSE ADHESIVE REMOVE LINER
TO EXPOSE ADHESIVE REMOVE LINER



1914, 11 SEP 10 (b)(6)(b)(7)(C)

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057EK

APL
FAM109-001
E-104-001
E-800-003
E-870-040
E-107-004
E-107-040
E-107-004
E-107-004
E-107-004

300GB
10K RPM
Firmware 5803
DRV. Rev. A1-21



PH-0HC490-26813-7AP-6KSE
REV A00
Made in Philippines

HDD S/N: DA03P7A057EK

2d BCT, 10th MTN DIV

IOP (P17 Final)

HD1 SET 3

General Dynamics
Contract No.: DAAH01-03-D-0029
Item: DELL 300GB DRIVES
P/N: 341-2049
CHS-3 Warranty Item
Warranty Stop Date: 10/2012
CHS-3 Hotline: 877-247-7711

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

ATED

SCSI
LVD/SE

SER. NO. DA03P7904PDJ

300GB
10K RPM
Firmware 5803

DRV. Rev. A1-11

ENCLOSURE
E-H011-05-2443(B1)

20

PH-0HC490-26813-795-5YK1

REV A00 Made in Philippines

HDD S/N: DA03P7904PDJ

2d BCT, 10th MTN DIV

SDE (P17 Final)

HD4 Set 4

SET 2

1925, 10SEP10

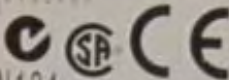
(b)(6)(b)(7)(C)

D33073

Fujitsu
Taiwan Ltd
19F No 39,
Sec 1, Chung-hwa
Road, Taipei, Taiwan



WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN



N124

MAY BE MANUFACTURED UNDER ONE
OF FOLLOWING U.S. PATENTS:
U.S. PAT. NO. 6,108,810; 6,108,811;
U.S. PAT. NO. 6,108,812; 6,108,813;
U.S. PAT. NO. 6,108,814; 6,108,815;
U.S. PAT. NO. 6,108,816; 6,108,817;
U.S. PAT. NO. 6,108,818; 6,108,819;
U.S. PAT. NO. 6,108,820; 6,108,821;
U.S. PAT. NO. 6,108,822; 6,108,823;

MODEL MAW3300NC ID:JW RoHS

Ultra320 SCSI/SCA2/LVD

FUJITSU LIMITED

PART NO. CA06550-B40300DL

+12V 1.20A --- +5V 1.00A ---

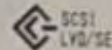
DATE 2007-10 DE REV. A

MADE IN PHILIPPINES

REV. NO. A 2 3 4 5 6 7 8 9

B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03P7A057FL



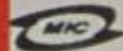
This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



011-05-2443(B)



PH-0HC490-26813-7AP-6KRW

REV A00

Made in Philippines



HDD S/N: DA03P7A057FL

001173

2d BCT, 10th MTN DIV

MSG (P17 Final)

HD0 Set 4

001174

(b)(6)(b)(7)(C)

General Dynamics

Contract No.: DAAH01-03-D-0029

Item: DELL 300GB DRIVES

P/N: 341-2049

CHS-3 Warranty Item

Warranty Stop Date: 10/2012

CHS-3 Hotline: 877-247-7711

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

ITED

SCSI
LVD/SE

B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03P7904PDY

300GB

10K RPM

Firmware 5803

DRV. Rev. A1-11

ENCLOSURE
E-H011-05-2443(B)

20

PH-0HC490-26813-795-5YKH

REV A00

Made in Philippines

HDD S/N: DA03P7904PDY

2d BCT, 10th MTN DIV
APPS2 (P17 Final)
HD0 Set 4



(b)(6)(b)(7)(C)

1930, 10 SEP 10,

General Dynamics CHS-3 Warranty Item. Cage Code: 67032
Contract No.: DAAH01-03-D-0029 Warranty Stop Date 02/2013
Item: DELL 300GB DRIVE
P/N: 341-3049 CHS-3 Hotline: 877-247-7711

S/N: SEE VENDOR S/N
NSN:

DATE 2007-12 DE REV. A
MADE IN PHILIPPINES
REV. NO. A1

SER. NO. DA03P7C05JNF

300GB
10K RPM
Firmware 5803
DRV. Rev. A1-11

300GB
10K RPM
Firmware 5803

PH-0M490-26810-70W 1602-A00
Made in Philippines
DP/N 00490

HDD S/N: DA03P7C05JNF

2d BCT, 10th MTN DIV



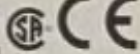
D33073

Fujitsu
Taiwan Ltd
19F No. 39
Sec. 1, Chung-hua
Road, Taipei, Taiwan



WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN.

N124



NOT BE MANUFACTURED UNDER THE
BY FOLLOWING U.S. PATENTS:
A. 5,851, 586; B. 5,851, 587; C. 5,851, 588;
D. 5,851, 589; E. 5,851, 590; F. 5,851, 591;
G. 5,851, 592; H. 5,851, 593; I. 5,851, 594;
J. 5,851, 595; K. 5,851, 596; L. 5,851, 597;
M. 5,851, 598; N. 5,851, 599; O. 5,851, 600;
P. 5,851, 601; Q. 5,851, 602; R. 5,851, 603;
S. 5,851, 604; T. 5,851, 605; U. 5,851, 606;
V. 5,851, 607; W. 5,851, 608; X. 5,851, 609;

MODEL MAW3300NC ID:JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057P5

FUJITSU LIMITED



This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



HDD S/N: DA03P7A057P5

2d BCT, 10th MTN DIV
MSG (P17 FINAL)
HD2 SET3

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

FUJITSU
TS1
19F
SCSI
ROB

MODEL PARS3000
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-840300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057N5

FUJITSU LIMITED



300GB
10K RPM
Firmware 5803
DRV. Rev. A1-21

E-H011-05-2442(B)



PH-0HC490-26813-7AP-6L18
Made in Philippines
REV A00

HDD S/N: DA03P7A057N5

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
MDC (P17 Final)
HD1 SET 3

1938, 10 SEP 10.

(b)(6)(b)(7)(C)

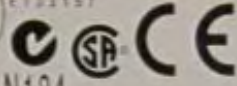
D33073

Fujitsu
Taiwan Ltd.
19F No. 39,
Sec. 1, Chung-hwa
Road, Taipei, Taiwan



WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN.

E133157



N124

MAY BE MANUFACTURED UNDER ONE
OF FOLLOWING U.S. PATENTS:
U.S. 6,821,480; U.S. 6,821,481; U.S. 6,821,482;
U.S. 6,821,483; U.S. 6,821,484; U.S. 6,821,485;
U.S. 6,821,486; U.S. 6,821,487; U.S. 6,821,488;
U.S. 6,821,489; U.S. 6,821,490; U.S. 6,821,491;
U.S. 6,821,492; U.S. 6,821,493; U.S. 6,821,494;
U.S. 6,821,495; U.S. 6,821,496; U.S. 6,821,497;
U.S. 6,821,498; U.S. 6,821,499; U.S. 6,821,500

MODEL MAW3300NC ID: JW RoHS

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

300GB
10K RPM
Firmware 5803
DRV. Rev. A1-11



MIC
E-H011-05-2443(B)



PH-0HC490-26813-76Q-5DU5

REV A00 Made in Philippines

HDD S/N: DA03P76049F4

2d BCT, 10th MTN DIV

1944, 10 SEP 10, (b)(6)(b)(7)(C)

General Dynamics CHS-3 Warranty Item
Contract No.: DAAH01-03-D-0029 Warranty Stop Date: 10/2012
Item: DELL 300GB DRIVES CHS-3 Hotline: 877-247-7711
PIN: 341-2046

S/N: SEE VENDOR S/N

NSN:

Cage Code: 67032

MODEL MAW3300NC ID: JW ReHS

Ultra320 SCSI/SCA2/LVD

FUJITSU LIMITED

PART NO. CA06550-B40300DL

+12V 1.20A --- +5V 1.00A ---

DATE 2007-09 DE: REV. A

MADE IN PHILIPPINES

REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03PT904PDP



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



HDD S/N: DA03PT904PDP

2d BCT, 10th MTN DIV
MSG (P17 FINAL)
HD5 SET3

001186

3N24

1946, 10 SEP 10

(b)(6)(b)(7)(C)

033073
Fujitsu
Taiwan Ltd
19F No 39
Sec 1, Chung-hwa
Road, Taipei, Taiwan

WARRANTY VOID IF ANY LABEL
SCREW IS REMOVED OR BROKEN

APL
NOT TO BE REPRODUCED OR
TRANSMITTED IN ANY FORM
BY ANY MEANS, ELECTRONIC
OR MECHANICAL, INCLUDING
PHOTOCOPYING, RECORDING,
OR BY ANY INFORMATION
STORAGE AND RETRIEVAL
SYSTEM, WITHOUT PERMISSION
IN WRITING FROM FUJITSU
LIMITED

RoHS
CE
SF
N124

MODEL MAW3300NC ID: JW RoHS

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

ED
SCSI
LVD/SE

300GB
10K RPM
Firmware 5803
DRV Rev. A1-11

MAC
E-H011-05-2443(B)

20

PH-0HC490-26813-76R-5EN5
REV A00
Made in Philippines

HDD S/N: DA03P76049WJ

2d BCT, 10th MTN DIV

001188

3M47

1950 10 SEP 10

(b)(6)(b)(7)(C)

General Dynamics CHS-3 Warranty Item Cage Code: 67032
Contract No.: DAAH01-03-D-0029 Warranty Stop Date 02/2013
Item: DELL 300GB DRIVE
P/N: 341-2049 CHS-3 Hotline: 877-247-7711
S/N: SEE VENDOR S/N

This medium is classified

SECRET

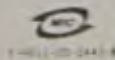
U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SECRET (1-87)

300GB
10K RPM
Firmware 5803

DRV. Rev. A1-11



PH-DHC490-26X13-TCM-7400-A00
Made in Philippines
DP/N DHC490



HDD S/N: DA03P7C05JR4

2d BCT, 10th MTN DIV

001190

3M24

1953, 10SEP10

(b)(6)(b)(7)(C)

D33073
Fujitsu
Taiwan Ltd
19F No. 39
Sec. 1, Chung-hwa
Road, Taipei, Taiwan

WARRANTY VOID IF ANY LABEL/SCREW IS REMOVED OR BROKEN. APL
NOT BY MANUFACTURED COUNTRY NOT
BY POLISHING U.S. 91004111
N. 301, 400 N. 500, 670 N. 740, 800
N. 780, 900 N. 110, 120 N. 600, 100
N. 600, 100 N. 601, 610 N. 610, 100
N. 110, 100 N. 110, 100 N. 100, 100
N. 110, 100 N. 100, 100 N. 100, 100
N. 100, 100 N. 100, 100 N. 100, 100
N. 100, 100 N. 100, 100 N. 100, 100

RoHS

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD FUJITSU LIMITED

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

SCSI LVD/SE

300GB
10K RPM
Firmware 5803
DRV. Rev. A1-11

MC
E-H011-05-2443(8)

20

PH-0HC490-26813-76R-5ELQ
REV A00
Made in Philippines

HDD S/N: DA03P76049YW

2d BCT, 10th MTN DIV



Cheetah 10K.7

RPM: 10K Capacity: 300GB

MODEL NUMBER: *ST3300007LC*

LOT NUMBER *A-81-8743-G*



MADE IN SINGAPORE

ST3300007LC

PART NUMBER *ST3300007LC*

VOC APPS CSD LOT
+5 8.6 NUMBER
+12 8.6

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

ULTRA U320 SCSI DRIVE

SG-0HC492-12531-74Q-ZM5G

Rev A00

Made in Singapore

HDD S/N: 3KR3ZM5G

100450843

1959. 10SEP10.

(b)(6)(7)(C)

001193

2d BCT, 10th MTN DIV

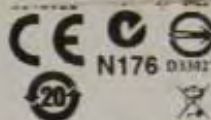
APPS2 (P17 Final)

HD0 SET 3

General Dynamics
Contract No.: DAAH01-03-D-0029
Item: DELL 300GB DRIVES
P/N: 341-2049
S/N: SEE VENDOR S/N
NSN:
CHS-3 Warranty Item
Warranty Stop Date: 10/2012
CHS-3 Hotline: 877-247-7711
Cage Code: 67032

Cneetan 10K.7

RPM: 10K Capacity: 300GB
MODEL NUMBER: *ST3300007LC*
LOT NUMBER *A-01-0911-S*



MADE IN SINGAPORE

ST3300007LC

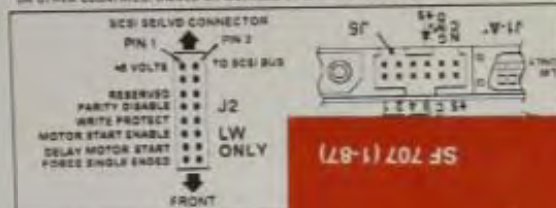
PART NUMBER *5K1005-143*

SERIAL NUMBER *3KR4DC5R*

VDC AMPS CSO LOT
+5 0.8 NUMBER
+12 0.8

FIRMWARE D784

THIS PRODUCT IS MANUFACTURED UNDER ONE OR MORE PATENTS IN THE UNITED STATES
OR OTHER COUNTRIES. OWNED OR LICENSED BY SEAGAT TECHNOLOGY LLC.



ULTRA U320 SCSI

SG-0HC492-12531-7
Rev A00

HDD S/N: 3KR4DC5R

SF 707 (1-87)

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

2001.10SERIO.

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
MDC (P17 Final)
HD0 SET 3

001196

TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE
TO EXPOSE ADHESIVE REMOVE LINE

SET 2

D33073
Fujitsu
Taiwan Ltd
15F No 33
Sec 1, Chung-Hua
Road, Taipei, Taiwan

WARRANTY VOID IF ANY LABEL
SCREW IS REMOVED OR BROKEN

UL
CE
N124

MODEL MAW3300NC ID:JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057FD

FUJITSU LIMITED
SCSI LVD/SE

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

PH-OHC490-26813-7AP-6KRY
Made in Philippines
REV A00
HDD S/N: DA03P7A057FD
2004, 10 SEP 10

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV

MSG (P17 Final)

HD2 Set 4

(b)(6)(b)(7)(C)

300GB
10K RPM
Firmware 5803
DRY Rev. A1-11
PH-0HC490-26813-7AP-6L3B
REV A00
Made in Philippines
HDD S/N: DA03P7A057KJ
3007, 10 SEP 10

MODEL MAW300NC ID: JM RoHS
Ultrastar 320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057KJ


SCSI
LVD/SE

FUJITSU LIMITED

ASL

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



2d BCT, 10th MTN DIV

SDE (P17 Final)

HD1 Set 4

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

PART NO. CA06550-840300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
9 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057EG

FUJITSU LIMITED



300GB
10K RPM
Firmware: 5803
DRV. Rev. A1-21

E-W011-07-2443181



PH-0HC490-26813-7AP-6KSF
Made in Philippines
REV A00

HDD S/N: DA03P7A057EG

2009. 10. 08. 08

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
APPS2 (P17 Final)
HD1 SET 3



Seagate

Cheetah 10K.7

RPM: 10K Capacity: 300GB

MODEL NUMBER: *ST3300007LC*

LOT NUMBER *A-01-8743-1*

ST3300007LC

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

ULTRA U320 SCSI DRIVE

SG-0HC492-12531-74L-XN25

Made in Singapore


Rev A00

HDD S/N: 3KR3XN25

2012.10SE910

(b)(6)(b)(7)(C)

105450843



2d BCT, 10th MTN DIV

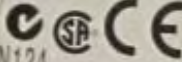
SET 2

D33073

Fujitsu
Taiwan Ltd.
19F No. 35,
Sec. 1, Chung-Hua
Road, Taipei, Taiwan

N124

WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN. APPL.



MODEL MAW3300NC ID:JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE.REV.A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057J2

FUJITSU LIMITED



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

MPC
1-05-2443(B)



PH-OHC490-26813-7AP-6K28

REV A00 Made in Philippines

HDD S/N: DA03P7A057J2

2015, 10SERIO

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
MSG (P17 Final)
HD3 Set 4

4M28

This medium is classified

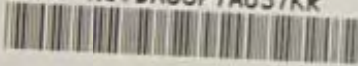
SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057KR



300GB
10K RPM
Firmware 5803

DRV. Rev. A1-11

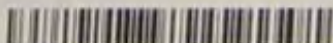


PHILIPS
E-H011-05-2443(B)



PH-0HC490-26813-7AP-6L31

Made in Philippines
REV A00



HDD S/N: DA03P7A057KR

2017. 10SEP10.

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
SDE (P17 Final)
HD2 Set 4

033073

Fujitsu
Taiwan Ltd.
19F No. 39,
Sec. 1, Chung-Hua
Road, Taipei, Taiwan



N124

WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN. APPL.

WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN. APPL.
BY FOLLOWING S.D. PARTS LIST:
A. 101 400 A. 100 870 A. 100 801
A. 100 801 A. 100 870 A. 100 801
A. 100 801 A. 100 870 A. 100 801
A. 100 801 A. 100 870 A. 100 801
A. 100 801 A. 100 870 A. 100 801
A. 100 801 A. 100 870 A. 100 801
A. 100 801 A. 100 870 A. 100 801

MODEL MAW3300NC ID:JW RoHS

Ultra320 SCSI/SCA2/LVD

FUJITSU LIMITED

PART NO. CA06550-B40300DL

+12V 1.20A --- +5V 1.00A ---

DATE 2007-10 DE REV. A

MADE IN PHILIPPINES

REV. NO. A 2 3 4 5 6 7 8 9

B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03P7A057FC



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



HDD S/N: DA03P7A057FC

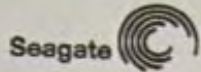
2019. 10 SEP 10.

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
SDE (P17 FINAL)
HD1 SET3

001210

TO EXPOSE ADHESIVE REMOVE LINER



Cheetah 10K.7

RPM: 10K Capacity: 300GB

MODEL NUMBER: *ST330007LC*

LOT NUMBER *A-01-0750-2*



MADE IN SINGAPORE

VOC APPS CSO LOT
+5 0.8 NUMBER
+12 0.8

ST3300007LC

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

ULTRA U320 SCSI DRIVE

SG-0HC492-12531-76A-3FD3

Made in Singapore


Rev A00

HDD S/N: 3KR43FD3

2021.10SEP10

(b)(6)(b)(7)(C)

0450049



2d BCT, 10th MTN DIV

001212

TO EXPOSE ADHESIVE REMOVE LINER

WARRANTY VOID IF ANY LABEL
SCREW IS REMOVED OR BROKEN

D33073
Fujitsu
Taiwan Ltd
19F No. 39
Sec. 1, Chung-Hua
Road, Taipei, Taiwan

UL
N124

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057NS

SCSI
LVD/SE

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

20

HDD S/N: DA03P7A057NS
2006. 10 SEP 10. (b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV
SDE (P17 FINAL)
HD5 SET3

SET 2

033073

Fujitsu
Taiwan Ltd
13F No 39
Sec 1 Chung-Hua
Road Taipei Taiwan

N124

WARRANTY VOID IF ANY LABEL
SCREW IS REMOVED OR BROKEN

APL

1 2 3 4 5 6 7 8 9

10 11 12 13 14 15 16 17 18 19 20

21 22 23 24 25 26 27 28 29 30

31 32 33 34 35 36 37 38 39 40

41 42 43 44 45 46 47 48 49 50

51 52 53 54 55 56 57 58 59 60

61 62 63 64 65 66 67 68 69 70

71 72 73 74 75 76 77 78 79 80

81 82 83 84 85 86 87 88 89 90

91 92 93 94 95 96 97 98 99 100

MODEL MAW3300NC ID:JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV A
MADE IN PHILIPPINES
REV NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9

FUJITSU LIMITED

SCSI
LVD/SE

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

PH-0HC490-26813-7AP-6L3A

Made in Philippines
REV A00

HDD S/N: DA03P7A0571E

2028. 10SEP10

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV

MSG (P17 Final)

HD4 Set 4



D33073
FUJITSU
Taiwan Ltd
19F No 39
Sec 1 Chung-hua
Road Taipei Taiwan

WARRANTY VOID IF ANY LABEL
SCREW IS REMOVED OR BROKEN.

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO CA06550-B40300DL
+12V 1.20A +5V 1.00A
DATE 2007-10 DE REV A
MADE IN PHILIPPINES
REV NO A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO DA03P7A057P6

SECRET
This medium is classified
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

HDD S/N: DA03P7A057P6
2030.1055P10

2d BCT, 10th MTN DIV
SDE (P17 FINAL)
HD2 SET3

D33073

Fujitsu
Taiwan Ltd
19F No 39,
Sec 1, Chung-hwa
Road Taipei, Taiwan



N124

WARRANTY VOID IF ANY LABEL/ SCREW IS REMOVED OR BROKEN. APL

MAY BE MANUFACTURED UNDER THE
U.S. GOVERNMENT G.P. PATENT NO.
5,231,408; 5,239,875; 5,298,481
5,768,888; 5,776,828; 5,858,288
5,888,288; 5,905,514; 5,914,247
5,928,888; 5,939,828; 5,945,828
5,958,828; 5,968,828; 5,978,828
5,988,828; 5,998,828; 6,008,828
6,018,828; 6,028,828; 6,038,828

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD FUJITSU LIMITED

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

SCSI
LVD/SE

300GB
10K RPM
Firmware 5803

MPC
E-H011-05-2443(R)

DRV. Rev A1-11

PH-OHC490-26813-721-3WYT

Made in Philippines

REV A00

HDD S/N: DA03P7203AM

2033.10SEP10

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV

WARRANTY VOID IF ANY LABEL/SCREW IS REMOVED OR BROKEN. APV

D33073
Fujitsu
Taiwan Ltd
ISF No. 39
Sec. 1, Chung-hua
Road, Taipei, Taiwan

N124

RoHS

SCSI LVD/SE

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD FUJITSU LIMITED
PART NO. C406550-R4030001

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

300GB
10K RPM
Firmware 5803
DRV. Rev. A1-21

20

E-H011-05-2442101

PH-0HC490-26813-731-4SJW
REV A00
Made in Philippines

HDD S/N: DA03P7303PGH
2055, 108EPD.

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV

P/N N6747

General Dynamics
Contract No: DDONUS
Item: 300GB SCSI RHD ASSY
P/N: C406550 B40000L
S/N: SEE VENDOR S/N
NSN: N/A
CHS-3 Warranty Item
Warranty Stop Date: 06/2012
Cage Code: 57032
CHS-3 Hotline: 877-247-7711



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

FL
TB
19
Se
RO

Model: VMB5000 1000W K0NS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-03 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
8 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7303M68

FUJITSU LIMITED



300GB
10K RPM
Firmware 5803
DRV. Rev. A1-21

E-H011-05-2443(B)



PH-OHC490-26813-73K-4YRF
Made in Philippines
REV A00

HDD S/N: DA03P7303M68
2038.10 SEP 10

2d BCT, 10th MTN DIV

SDE (P17 Final)

HD3 Set 4

SET 2

D33073

Fujitsu
Taiwan Ltd
19F No. 39,
Sec 1, Chung-Hua
Road, Taipei, Taiwan



WARRANTY VOID IF ANY LABEL/
SCREW IS REMOVED OR BROKEN.



N124

MAX. 500MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)
100MB/s (100MB/s) (100MB/s)

MODEL MAW3300NC ID:JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV.A
MADE IN PHILIPPINES

FUJITSU LIMITED



REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03P7A057FH



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



05-2443 (B)



PH-0HC490-26813-7AP-6KRL

REV A00

Made in Philippines



HDD S/N: DA03P7A057FH

2040, 10 SEP 10

(b)(6)(7)(C)

2d BCT, 10th MTN DIV

MSG (P17 Final)

HD5 Set 4

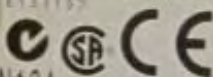
D33073

Fujitsu
Taiwan Ltd
19F No. 39,
Sec. 1, Chung-hwa
Road, Taipei, Taiwan



WARRANTY VOID IF ANY LABEL
SCREW IS REMOVED OR BROKEN

ET31152



N124

WELL BY MANUFACTURED HARDWARE
BY FOLLOWING U.S. PATENT NO.
A. 3,301, 416 A. 3,300, 410 A. 3,300, 411
A. 3,301, 412 A. 3,301, 413 A. 3,301, 414
A. 3,301, 415 A. 3,301, 416 A. 3,301, 417
A. 3,301, 418 A. 3,301, 419 A. 3,301, 420
A. 3,301, 421 A. 3,301, 422 A. 3,301, 423
A. 3,301, 424 A. 3,301, 425 A. 3,301, 426

MODEL MAW3300NC ID:JW RoHS

Ultra320 SCSI/SCA2/LVD

FUJITSU LIMITED

PART NO. CA06550-B40300DL

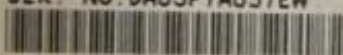
+12V 1.20A --- +5V 1.00A ---

DATE 2007-10 DE.REV.A

MADE IN PHILIPPINES

REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03P7A057EW



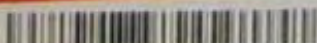
This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)



HDD S/N: DA03P7A057EW

2042, 10 SEP 10

(b)(6)(b)(7)(C)

001227

2d BCT, 10th MTN DIV

SDE (P17 FINAL)

HD4

SE 3

001228

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF-707 (1-87)

PART NO. CA06550-B403000L
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
8 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057FR

300GB
10K RPM
Firmware S803
DRV. Rev. A1-11

6-H011-05-2443181

PH-OHC490-26813-7AP-6KRK
REV A00
Made in Philippines

HDD S/N: DA03P7A057FR

2044. 10SEP10

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV

IOP (P17 Final)

HD0 SET 3

TO EXPOSE ADHESIVE REMOVE LINER



This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)



MODEL MAW3300NC ID/JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-840300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057F6

FUJITSU LIMITED



300GB
10K RPM
Firmware 5803
DRV. Rev. A1-11

E-H011-05-2442181



PH-OHC490-26813-7AP-6KS4
Made in Philippines
REV A00

HDD S/N: DA03P7A057F6

2046.10 SEP 10

(b)(6)(7)(C)

2d BCT, 10th MTN DIV

APPS1 (P17 Final)

HD0 SET 3

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

PART NO. CA06550-B40300DL

+12V 1.20A --- +5V 1.00A ---

DATE 2007-10 DE REV A

MADE IN PHILIPPINES

REV. NO. A 2 3 4 5 6 7 8 9

B 0 1 2 3 4 5 6 7 8 9

SER. NO. DA03P7A057DW

BAD

300GB

10K RPM

Firmware 5803

DRV. Rev. A1-21

E-H011-05-2443(B)

PH-OHC490-26813-7AP-6KSA

Made in Philippines

REV A00

HDD S/N: DA03P7A057DW

2009, 10SEP10

(b)(6)(7)(C)

001233

2d BCT, 10th MTN DIV

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.

SF 707 (1-87)

FUJITS
Toshiba
19F No
Sec. 1
Road.

MODE
Ultr

PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE. REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
B 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057F1

SCSI
LVD/SE

300GB
10K RPM
Firmware 5803
DRV. Rev. A1-11

MAC
E-H011-05-2443(B)

20

PH-0HC490-26813-7AP-6KRM
Made in Philippines
REV A00

HDD S/N: DA03P7A057F1
2051, 10 SEP 10.

(b)(6)(b)(7)(C)

001235

2d BCT, 10th MTN DIV
APPS1 (P17 Final)
HD1 SET 3

001236

Classified by: NSA/CSS
Manual 1-52 dtd 08 Jan 07
Declassify on 20320108

D33073

Fujitsu
Taiwan Ltd.
19F No. 39,
Sec 1, Chung-hwa
Road, Taipei, Taiwan



N124

MODEL MAW3300NC ID: JW
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300D
+12V 1.20A --- +5V 1.00A
DATE 2006-12 DE. REV. A
MADE IN PHILIPPINES
REV. NO. A ~~2~~ 3 4 5 6
 B 0 1 2 3 4 5 6
SER. NO. DA03P6C02P6F



300GB
10K RPM
Firmware 5803
DRV. Rev. A1-11



PH-OHC490-26813-6CT-3EMN

REV A00

Made in Philippines

HDD S/N: DA03P6C02P6F

2056.10SEP10.

SF 707 (1-87)

This medium is classified

SECRET

U.S. Government Property
Protect it from unauthorized
disclosure in compliance with
applicable executive orders,
statutes, and regulations.



E-H011-05-2443(B)

(b)(6)(b)(7)(C)

2d BCT, 10th MTN DIV

SDE (P17 Final)

HD0 Set 4

P/N N6747

TO EXPOSE ADHESIVE REMOVE LINER
TO EXPOSE ADHESIVE REMOVE LINER
TO EXPOSE ADHESIVE REMOVE LINER

SET 2

D33073
Fujitsu
Taiwan Ltd
19F No. 39
Sec 1, Chung-Hua
Road, Taipei, Taiwan

WARRANTY VOID IF ANY LABEL/SCREW IS REMOVED OR BROKEN

RoHS
N124

MODEL MAW3300NC ID: JW RoHS
Ultra320 SCSI/SCA2/LVD
PART NO. CA06550-B40300DL
+12V 1.20A --- +5V 1.00A ---
DATE 2007-10 DE REV. A
MADE IN PHILIPPINES
REV. NO. A 2 3 4 5 6 7 8 9
8 0 1 2 3 4 5 6 7 8 9
SER. NO. DA03P7A057NV

FUJITSU LIMITED

SCSI
LVD/SE

This medium is classified

SECRET

U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 707 (1-87)

PH-0HC490-26813-7AP-6L34
REV A00 Made in Philippines

HDD S/N: DA03P7A057NV
2058, 10SERVO (b)(6)(b)(7)(C)



2d BCT, 10th MTN DIV

MSG (P17 Final)

HD1 Set 4

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1636, 10 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one packet of paperwork pertaining to PFC MANNING's Secret Compartmented Information (SCI) Clearance, from Ms. (b)(6)(b)(7)(C) SCI Program Manager, G2, Mission Support Element, Fort Drum, NY 13602, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 134-10.

/////////////////////////////////LAST ENTRY/////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro Resident Agency
Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

10 Sep 10

EXHIBIT

197

CI OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

1 FEB 77

001241
Approved

(b)(6)(b)(7)(C)

Exhibit(s) 198

Page(s) 001242 thru 001263 referred to:

Directorate of Human Resources
Administrative Services Division
Attn: IMNE-DRM-HRR (FOIA-PA)
10720 Mt. Belvedere Blvd.
Fort Drum, New York 13602-5045

Exhibit(s) 199

Page(s) 001264 and 01264a withheld:

5 U.S.C. § 552(b)(1)

Permits withholding information that
is classified for
National Security purposes

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 5 PAGES

DETAILS

About 0730, 10 Sep 10, SA (b)(6)(b)(7)(C), (b)(7)(E) SA (b)(6)(b)(7)(C), (b)(7)(E) and SA (b)(6)(b)(7)(C), (b)(7)(E) all assigned to Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, arrived at Fort Drum, NY (FDNY), in preparation for locating and searching the Shipping Containers (Connexes) from PFC MANNING's unit to identify any computers, hard drives, and other digital media that PFC MANNING may have used while deployed to IRAQ and to seize and subsequently search the SIPR server identified as housing PFC MANNING's electronic network storage space.

About 0900, 10 Sep 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C), (b)(7)(E) WMRA, CCIU, and received a signed copy of the Search and Seizure Authorization for the shipping containers and secure storage equipment of HHC, 2nd Brigade Combat Team (2nd BCT), 10th Mountain Division (10th Mtn Div), FDNY located at 10200 North Riva Ridge Loop, FDNY,. (See Search and Seizure Authorization for details.)

About 1045, 10 Sep 10, SA (b)(6)(b)(7)(C) coordinated with SFC (b)(6)(b)(7)(C) Automations NCOIC, 2nd BCT, FDNY, who assisted in identification of items in the Sensitive Items Container. SFC (b)(6)(b)(7)(C) identified the T-Server which consisted of two rack-mountable computers and the Pelican cases which contained hard drives he said belonged to the S-2 section. SFC (b)(6)(b)(7)(C) said that the other server in the container was their portal and SQL server. He stated that PFC MANNING would not have had access to that server, as he did not have administrative privileges on the server. SFC (b)(6)(b)(7)(C) said that he needed more of his section personnel, who were currently on leave, before he could place the server back into operation to confirm that PFC MANNING never had access to the server.

Between 1238 and 1909, 10 Sep 10, SA (b)(6)(b)(7)(C) previewed the contents of the following hard drives for the presence of a user profile pertaining to PFC MANNING by connecting a write blocker to a stand-alone laptop computer capable of processing data up to the classification level of Secret:

Make	Model	Serial Number	Classification	Start Time	End Time	Results
Kanguru	QS-2 USB External	IWS128-750	UNCLASSIFIED	1238	1242	Negative
Seagate	Barracuda	3QD0JMAF	SECRET	1248	1301	Negative
Dell	ST3300656SS	3QP0F6J1	SECRET	1307	1309	Negative
Hitachi	TravelStar	7BFJ5133TH351	SECRET	1327	1328	Negative
IBM	TravelStar	46MJ6896	SECRET	1340	1345	Negative
Maxtor	MaxLine Plus II	Y65Z4XHE	SECRET	1349	1353	Negative
Maxtor	MaxLine Plus II	Y65Z4R6E	SECRET	1354	1359	Negative
Hitachi	HTS	MPCZN7Y0J40WEL	SECRET	1432	1438	Negative
Hitachi	HTS	5MHOWM5H	SECRET	1441	1448	Negative
Samsung	HM121HJ	S1NSJD0Q800999	SECRET	1451	1456	Positive
Seagate	Barracuda	4JT0B4C9	SECRET	1510	1513	Negative
Seagate	Barracuda	4JT0BFFA	SECRET	1518	1521	Negative

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGN

(b)(6)(b)(7)(C)

DATE

12 Sep 10

EXHIBIT

200

OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

1 FEB 77

001265

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

Report NUMBER

0028-10-CID221-10117

PAGE 2 OF 5 PAGES

DETAILS

Fujitsu	Unable to read	5MHONJJJ	SECRET	1526	1532	Negative
Hitachi	HTS721010	MPCZN7Y05940VL	SECRET	1534	1536	Negative
Hitachi	ONY552	070714DP1D00DFG	SECRET	1538	1542	Negative
Hitachi	Unable to read	5MHOHJL	SECRET	1544	1546	Negative
Hitachi	HTS	MPCZN7Y0J93JXL	SECRET	1548	1550	Negative
Hitachi	HTS	MPCZN7Y0J31LAL	SECRET	1551	1553	Negative
Fujitsu	MH2260BJFFS	K83CT9228ZMR	SECRET	1555	1557	Negative
Hitachi	HTC	MPCZN7Y0J1UP7L	SECRET	1558	1559	Negative
Hitachi	HTC	MPCZN7Y0J9L1PL	SECRET	1603	1604	Negative
Seagate	Momentum	5MHOTBX4	SECRET	1605	1607	Negative
Fujitsu	Unable to read	5MHOHPLB	SECRET	1609	1611	Negative
Toshiba	MK3252GSX	780CP1OUT	SECRET	1619	1624	Negative
Toshiba	MK40256AS	Z5FX1417S	SECRET	1704	1710	Negative
Hitachi	TravelStar	XKG4M38M	SECRET	1712	1714	Negative
Fujitsu	MHV2060AH	NT25T5B2P72P	SECRET	1715	1719	Negative
Fujitsu	MHV2060AH	NT25T5B2P7T4	SECRET	1745	1747	Negative
Fujitsu	MHV2060AH	NT25T5B2P8BK	SECRET	1748	1750	Negative
Fujitsu	MHV2060AH	NT25T5B2PRBT	SECRET	1753	1755	Negative
Toshiba	HDD2D14	460M09767	SECRET	1756	1757	Negative
Fujitsu	MHV2060AH	NT25T5A2M298	SECRET	1758	1759	Negative
Fujitsu	MHV2060AH	NT25ST5B2P7F2	SECRET	1800	1802	Negative
Fujitsu	MHV2060AH	NT25T5C2UD3E	SECRET	1802	1803	Negative
Seagate	Momentum	5MHONZQA	SECRET	1815	1816	Negative
Hitachi	TravelStar	BBEH4A1AH903	SECRET	1817	1818	Negative
Fujitsu	MHV2080AH	NT24T5C2FDFD	SECRET	1819	1820	Negative
Fujitsu	MHV2040AH	NT26T5B2W	SECRET	1822	1823	Negative
Hitachi	DK23CA-20	2P009DM171H1674Z	SECRET	1824	1825	Negative
Hitachi	DK23CA-20	2P009A7P28V2152Z	SECRET	1826	1827	Negative
Seagate	ST92130	DFJH058ZA	SECRET	1830	1831	Negative
Samsung	MP0603H	S03ZJ10YB48570	SECRET	1832	1833	Negative
Hitachi	DK23FB-40	BBEH4A12T145	SECRET	1834	1836	Negative
Hitachi	HTS54804OM9AT	MRI231L2GADGAB	SECRET	1841	1843	Negative
Fujitsu	MHV2060AH	NT25T612UFWJ	SECRET	1845	1848	Negative
Seagate	Momentum	3K WG2885	SECRET	1850	1853	Negative
Fujitsu	MHT2040AH	NPOET4A2UWR9	SECRET	1900	1904	Negative
Hitachi	TravelStar	MRG387K3KZB76H	SECRET	1907	1909	Negative

Between 1239 and 1959, 10 Sep 10, SA (b)(6)(b)(7)(C) reviewed the contents of the following hard drives for the presence of a user profile pertaining to PFC MANNING by connecting a write blocker to a stand-alone

TYPED AGENT'S NAME AND SEQUENCE NUMBER		ORGANIZATION	
SA (b)(6)(b)(7)(C), (b)(7)(E)		Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE		DATE	EXHIBIT
(b)(6)(b)(7)(C)		12 Sep 10	200

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001266
Approved (b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

REPORT NUMBER

0028-10-CID221-10117

PAGE 3 OF 5 PAGES

DETAILS

laptop computer capable of processing data up to the classification level of Secret (drives which were classified at higher than Secret or had an unknown classification label were previewed by connecting a write blocker to a stand-alone desktop computer capable of processing data up to the classification level of Sensitive Compartmented Information), all of which met with negative results:

Make	Model	Serial Number	Classification	Start Time	End Time	Results
Hitachi	HTS721010G9SA00	MPCZN7Y0J9JMJ	Secret	1239	1246	Negative
Hitachi	HTS721010G9SA00	MPCZN7Y0J9JPTI	Secret	1249	1251	Negative
Fujitsu	MHV2060AH	NT25T5B2P760	Secret	1254	1306	Negative
Unknown	DJSA-220	Unknown	Secret	1309	1311	Negative
Seagate	9EU132-037	6RYCS4XP	Sensitive Compartmented Information	1420	1425	Negative
Seagate	9EU132-037	6RYCTCQQ	Sensitive Compartmented Information	1428	1431	Negative
Western Digital	WD5000YS	WMANU1115162	Sensitive Compartmented Information	1434	1436	Negative
Seagate	9EU132-037	6RYCS5YS	Sensitive Compartmented Information	1437	1438	Negative
Seagate	9S1038-508	5LYCK02Z	Sensitive Compartmented Information	1445	1447	Negative
Hitachi	H7S541080G9AT00	XKG8PETM	Sensitive Compartmented Information	1448	1458	Negative
Hitachi	H7S541080G9AT00	X6G5978C	Sensitive Compartmented Information	1459	1506	Negative
Hitachi	H7S541080G9AT00	XKGPS40M	Sensitive Compartmented Information	1506	1512	Negative
Hitachi	H7S541080G9AT00	X6G64AXC	Sensitive Compartmented Information	1514	1517	Negative
Hitachi	H7S541080G9AT00	X6K333DM	Sensitive Compartmented Information	1520	1523	Negative
Hitachi	H7S541080G9AT00	XNJ0830G	Not Marked	1530	1532	Negative
Toshiba	MK8026GAX	652S0039T	Sensitive Compartmented Information	1535	1539	Negative
Seagate	ST3120022A	5JS79SF2	Sensitive Compartmented Information	1541	1543	Negative
Seagate	ST3120022A	5JS6L9RM	Sensitive Compartmented Information	1544	1545	Negative
Western	WD5000YS	WMANU1067415	Sensitive Compartmented	1546	1549	Negative

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

12 Sep 10

EXHIBIT

200

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 4 OF 5 PAGES

DETAILS

Digital			Information			
Western Digital	WD5000YS	WMANU1115513	Sensitive Compartmented Information	1550	1551	Negative
Western Digital	WD5000YS	WMANU1115082	Sensitive Compartmented Information	1552	1553	Negative
Western Digital	WD5000YS	WMANU1115233	Sensitive Compartmented Information	1554	1555	Negative
Western Digital	WD5000YS	WMANU1509514	Sensitive Compartmented Information	1556	1601	Negative
Western Digital	WD5000YS	WMANU1115222	Sensitive Compartmented Information	1602	1604	Negative
Seagate	9S1038-508	5LYCJZ85	Sensitive Compartmented Information	1606	1607	Negative
Toshiba	MK8026GAX	652S0040T	Sensitive Compartmented Information	1608	1610	Negative
Seagate	9S1038-508	5LYCK020	Not Marked	1612	1614	Negative
Seagate	ST910021AS	5MH0GZG8	Secret	1615	1617	Negative
Hitachi	HTS541080G9AT00	X6G6450C	Secret	1618	1619	Negative
Hitachi	08K0637	KCG46XTP	Secret	1910	1913	Negative
Hitachi	08K0637	K3HBYJDH	Secret	1914	1917	Negative
Hitachi	Travelstar	BBEH4A1E0409	Secret	1919	1923	Negative
Toshiba	MK3021GAS	64IG3499T	Secret	1925	1926	Negative
Fujitsu	MHV2060AH	NT25T5B2P86V	Secret	1927	1928	Negative
Hitachi	Travelstar	3TU528	Secret	1929	1930	Negative
IBM	Travelstar	46M76587	Secret	1932	1933	Negative
Toshiba	MK0321GAS	13A30404S	Secret	1934	1934	Negative
Toshiba	MK0321GAS	13A30412S	Secret	1947	1948	Negative
IBM	Travelstar	46MA6144	Secret	1949	1950	Negative
Fujitsu	MHM2200AT	01030916	Secret	1952	1953	Negative
Hitachi	Travelstar	MCE55AJ64006	Secret	1955	1956	Negative
Hitachi	Travelstar	MCE65ARB1847	Secret	1956	1957	Negative
Toshiba	MK4006MAV	39A18235P	Secret	1959	1959	Negative

About 1451, 10 Sep 10, SA (b)(6)(b)(7)(C) previewed a Samsung 2.5" SATA laptop drive, S/N: S1NSJD0Q800999. In the folder "Documents and Settings", there was a profile folder for "Bradley.Manning".

About 1456, 10 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence the Samsung 2.5" SATA laptop drive, S/N: S1NSJD0Q800999, containing a profile folder "Bradley.Manning", which was documented

TYPED AGENT'S NAME AND SEQUENCE NUMBER		ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)		Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)		DATE	EXHIBIT
		12 Sep 10	200

CID FORM 94/

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001268

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

Form NUMBER

0028-10-CID221-10117

PAGE 5 OF 5 PAGES

DETAILS

Evidence/Property Custody Document (EPCD), Document Number(DN) 132-10. (See EPCD for details).

/////////////////////////////////LAST ENTRY/////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

12 Sep 10

EXHIBIT

200

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001269
Approved

(b)(6)(b)(7)(C)

SEARCH AND SEIZURE AUTHORIZATION

For use of this form, see AR 27-10; the proponent agency is OTJAG

TO: (Name and Organization of the person to whom authorization is given)

Special Agent (b)(6)(b)(7)(C) of the United States Army Criminal Investigation Command (USACIDC)

(An affidavit) (A sworn or (unsworn) oral statement) having been made before me by Special Agent (b)(6)(b)(7)(C)
(Name of Affiant)

Washington Metro Resident Agency, Computer Crime Investigative Unit (CCIU), USACIDC, Fort Belvoir, Virginia 22060

(Organization or Address of Affiant)

(which affidavit is attached hereto and made a part of this authorization), and as I am satisfied that there is probable cause to believe that the matters mentioned in the affidavit are true and correct, that the offense set forth therein has been committed, and that the property to be seized is located (on the person) (at the place) to be searched, you are hereby ordered to search the (person) (place) known as

Shipping Containers and Secure Storage of HHC, 2nd BCT, 10th Mountain Div, 10200 N. Riva Ridge Loop, Fort Drum, NY

for the property described as electronic data and physical evidence related to the identified offenses, which may include:

computers, computer servers, hard disk drives, digital media and other U.S. Government property as specified in Attachments

A and C, which are hereby incorporated into this Search Authorization.

bringing this order to the attention of the (person searched) (person in possession, if any person be found at the place or on the premises searched). The search will be made in the (daytime) (nighttime), and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to:

Evidence Custodian, Computer Crime Investigative Unit (CCIU), 9805 Lowen Road, Bldg 193, Fort Belvoir, Virginia

(Name and Organization of Authorized Custodian)

and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 10 day of September, 2010

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL

(b)(6)(b)(7)(C)
CPT, JA

DUTY POSITION OF AUTHORIZING OFFICIAL

MILITARY MAGISTRATE

ORGANIZATION OF AUTHORIZING OFFICIAL

B CO DSTB 1AD
APO AE 09344

SIGNATURE OF AUTHORIZING OFFICIAL

(b)(6)(b)(7)(C)

DA FORM 3745, SEP 2002

DA FORM 3745-R, MAR

APD PE v1.02ES

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

00Exhibit 201

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

For use of this form, see AR 27-10; the proponent agency is OTJAG.

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

I. I.

Special Agent

(b)(6)(b)(7)(C)

Washington Metro Resident Agency

(Name)

(Organization or Address)

Computer Crime Investigative Unit (CCIU), USACIDC, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060

having been duly sworn, on oath depose and state that:

SEE ATTACHMENT A.

2. The affiant further states that:

SEE ATTACHMENT A.

3 In view of the foregoing, the affiant requests that an authorization be issued for a search of

SEE ATTACHMENT B

(the person) (and)

(the quarters or billets) (and)

and (seizure) (apprehension) of

SEE ATTACHMENT C

(the automobile)

(items/persons searched for)

TYPED NAME AND ORGANIZATION OF AFFIANT

Special Agent (b)(6)(b)(7)(C)
Washington Metro Resident Agency
Computer Crime Investigative Unit (CCIU), USACIDC

SIGNATURE OF AFFIANT

(b)(6)(b)(7)(C)

SWORN TO AND SUBSCRIBED BEFORE ME THIS 10th DAY OF September 2010 AT 5:52 (EST)

TYPED NAME, ORGANIZATION AND OFFICIAL CAPACITY OF AUTHORITY
ADMINISTERING THE OATH

(b)(6)(b)(7)(C)
CPT, JA
MILITARY MAGISTRATE

SIGNATURE OF AUTHORITY ADMINISTERING THE OATH

(b)(6)(b)(7)(C)

INSTRUCTIONS

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it has been committed. Use additional page if necessary.
2. In paragraph 2, set forth facts establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraphs 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she has plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary.
3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under certain circumstances for evidentiary matters.

ATTACHMENT A

INTRODUCTION

I make this affidavit in support of an application for a Military Magistrate Search Authorization for electronic data, computer hardware, and physical evidence relating to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information). As set forth herein, there is probable cause to believe within the U.S. Government Shipping Container(s), described as the "Sensitive Items Connex" and the "S-2 Connex", both assigned to Headquarters and Headquarters Company ("HHC"), 2nd Brigade Combat Team ("BCT"), 10th Mountain Division, Fort Drum, New York ("Fort Drum") which are presently or are to-be located within or adjacent the HHC, 2nd BCT, 10th Mountain Division main offices at 10200 North Riva Ridge Loop, Fort Drum, New York (herein "Unit Area") – and within a Secure Storage Area referred to as the "Unit Vault", also located within the Unit Area; contain evidence, fruits, and/or instrumentalities of the offenses committed by Private First Class (PFC) Bradley Edward MANNING ("MANNING") formerly assigned to HHC, 2nd BCT, 10th Mountain Division, as further described in this affidavit.

AGENT BACKGROUND

I am a Special Agent in the United States Army Criminal Investigation Command ("USACIDC") and have been so for approximately eight years. I am currently assigned to the USACIDC, Washington Metro Resident Agency, of the Computer Crime Investigative Unit ("CCIU"), located at Fort Belvoir, Virginia; where I am responsible for

the investigation of, among other things, violations pertaining to computer intrusions, denial of service attacks, and other types of malicious computer activity directed against U.S. Army and/or Department of Defense computer networks anywhere in the world. Prior to my assignment at CCIU, I was assigned as a Special Agent with USACIDC in: South Korea, where I was responsible for conducting felony investigations impacting the U.S. Army in South Korea; Fort Lewis, Washington, where I was responsible for conducting felony investigations impacting the U.S. Army in the states of Washington, Oregon, Idaho, and Montana; and concurrently with my position at CCIU, I was assigned to the Baghdad CID Battalion as a Computer Crime Coordinator where I was responsible for conducting computer forensic examinations of seized computers, cellular phones, and other digital media within Iraq, Kuwait and Afghanistan.

I have been trained in computer incident response, digital evidence acquisition, LINUX and Windows Forensic Examinations by the Department of Defense Cyber Investigations Training Academy ("DCITA"). I currently possess "Department of Defense Certified Digital Forensic Examiner" and "Department of Defense Certified Digital Media Collector" certifications. In addition to my training and experience as a criminal investigator, I have also been an employee of several commercial Information Technology companies to include: a national Internet Service Provider ("ISP"), a commercial software company specializing in law enforcement and intelligence analysis products, and several defense contracting companies where I worked as a government contractor to the Federal Bureau of Investigation, as a member of the Pentagon Joint Staff, and the Washington DC Department of Corrections. I have received training from the U.S. Army in the investigation of fraud; training from several commercial companies

in computer, computer network, and database administration; and I hold a Bachelor of Science degree in Information Technology from George Mason University, an accredited state university in Virginia.

My experience as a USACIDC Special Agent has included the investigation of cases involving violent and non-violent crimes as well as the use of computers. I have received training and gained experience in interviewing and interrogation techniques, arrest procedure, search warrant applications, the execution of searches and seizures, and other criminal laws and procedures.

As a Special Agent of the USACIDC, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice (Title 10 U.S.C. Section 47) and other applicable federal and state laws where there is a U.S. Army or Department of Defense interest. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

SOURCE OF EVIDENCE

The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals – including other law enforcement officers and particularly other USACIDC Special Agents – as well as my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and

experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

RELEVANT STATUTES

Title 18, United States Code, § 793(d) makes it unlawful to make unauthorized disclosure of national defense information. Specifically, the statute provides in pertinent part that:

Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered or transmitted . . . the same to any person not entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years, or both.

Title 18, United States Code, § 1030(a) makes it unlawful to, without authorization, obtain from a United States Government computer certain national defense information, and disclose such information. Specifically, the statute provides in pertinent part that:

Whoever – (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted . . . the same to any person not entitled to receive it [shall be

punished by a fine under this title or imprisonment for not more than ten years, or both]

The national security classification levels assigned to national security information and national defense information are defined in Executive Order No. 13526 and its predecessor orders. Information may be classified if the following conditions are met: (1) an original classification authority ("OCA") is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the United States Government; (3) the information falls within one or more of the categories set forth in the Executive Order (which includes intelligence sources and methods; cryptology; military plans; and vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security of the United States); and (4) the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage. Under the Executive Order, information may be classified "Confidential" if its unauthorized disclosure reasonably could be expected to cause damage to the national security; "Secret" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security; and "Top Secret" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

BACKGROUND AND TECHNICAL INFORMATION

The term "computer" as used in this affidavit is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any

data storage facility or communications facility directly related to or operating in conjunction with such device.

I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I am aware of the following:

a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information.

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

c. Instant Messaging (IM) is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger, etc.) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or

countries before it arrives at its final destination, even if the communicating parties are in the same state. Instant Messaging may also be commonly referred to as 'Internet Chat'.

d. The Windows User Profile is created the first time the user interactively logs-on at the computer on computers running current Microsoft Windows Operating Systems. A user profile defines customized desktop environments, such as individual display, network and printer connections settings, Favorites, Cookies and History, Start Menu, Desktop, Application Data, as well as forms the basis of a container for a user to place user created files and folders. Typically the contents of a User Profile are inaccessible by other users who do not have elevated or administrator level rights on the computer system. Consequently information related specifically to that user, such as their activities on a particular computer or network can be determined from examination of data and information contained in or related to the User's Profile.

PROBABLE CAUSE FOR SEARCH

Manning's Access To Classified Information

MANNING enlisted in the United States Army on or about October 2, 2007, and currently holds the rank of Private First Class. He received training in Intelligence Analysis, and was ultimately assigned as a U.S. Army Military Occupational Specialty ("MOS") 35F – Intelligence Analyst. MANNING was granted a U.S. Government security clearance at the "Top Secret" level as part of his position within the U.S. Army. On or about October 12, 2009, MANNING was deployed with his unit, HHC, 2nd BCT, 10th Mountain Division, to Forward Operating Base ("FOB") Hammer, located approximately 40 miles east of Baghdad, Iraq, and 70 miles west of the Iran-Iraq border.

Between October 2009 and May 2010, while assigned in Iraq and working in the role of an All-Source Intelligence Analyst, MANNING was granted access to national defense information through various U.S. Army and DoD computer network systems, including: the Non-Secure Internet Protocol Router ("NIPR") network, used for the processing of unclassified documents and unclassified communications; and the Secure Internet Protocol Router ("SIPR") network, used for the processing of classified documents and classified communications at the "Confidential" and "Secret" classification levels. MANNING also had access to a commercial, non-military, satellite-based ISP while in his living quarters on FOB Hammer, which he used with his personal laptop computer while not performing official duties. This information has been verified by statements of co-workers in MANNING's unit, by examination of various computer account and network log file systems, the forensic examination of computers used by MANNING, and by documents obtained during the course of this investigation.

Classified Material Published On The Internet

On February 18, 2010, the website WikiLeaks.org ("WikiLeaks") – which is self-described as "a multi-jurisdictional public service designed to protect whistle blowers, journalists and activists who have sensitive materials to communicate to the public" – published on their website a U.S. Department of State diplomatic cable originating from the U.S. Embassy in Reykjavik, Iceland, which was classified "Confidential". This diplomatic cable, dated January 13, 2010, related to diplomatic discussions on the topic "Icesave" between members of the U.S. Department of State, the British Foreign Service, and Icelandic Government personnel. Based on this classified document's publication on the WikiLeaks website, the U.S. Department of State's Diplomatic

Security Service initiated an investigation on February 19, 2010, to identify the person(s) who unlawfully disclosed this document.

On April 5, 2010, at the National Press Club in Washington, D.C., the founder of WikiLeaks, an Australian citizen named Julian P. Assange, held a press conference to publicly release classified video footage of United States combat operations in Iraq. The video footage, apparently taken by a U.S. Army AH-64 Apache attack helicopter engaged in combat in or around Baghdad, Iraq, depicts an air-strike conducted on July 12, 2007, during which two *Reuters* journalists, several suspected Iraqi insurgents, and several Iraqi civilians were killed or wounded. Assange released the original 38-minute-long version of the video as well as a shorter "production" version lasting approximately 18 minutes, titled "Collateral Murder", both of which were published on the Internet at the URL "www.collateralmurder.org". Due to the controversial and/or graphic nature of the video, this classified material received wide news media coverage. U.S. Department of Defense officials later confirmed that the video footage was genuine and was properly classified "Secret".

Manning Identified as Source of Classified U.S. Government Material

Between May 20, 2010 and May 26, 2010, MANNING began a series of Internet chat conversations with a civilian, Mr. (b)(6)(b)(7)(C) residing in (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) is known in the computer security community as a 'computer hacker' and has been profiled extensively in the print and on-line media. MANNING and (b)(6)(b)(7)(C) discuss a range of issues related to Classified U.S. Government material over a period of approximately 6 days; wherein MANNING admits to (b)(6)(b)(7)(C) to having unlawfully disclosed U.S. Government Classified material to the website WikiLeaks.org. During these chat conversations, which MANNING and (b)(6)(b)(7)(C) encrypted so that only they could

read the communications, MANNING detailed the specific items of Classified U.S. Government material he unlawfully disclosed to the WikiLeaks website as: a video and related documentation of a U.S. airstrike in Gharani, Afghanistan; the Apache airstrike video in Baghdad, Iraq which was publicly disclosed by WikiLeaks; an Iraq War Event Log believed to contain approximately 500,000 records; the "Gitmo Papers" relating to terror suspect detainees being held in Guantanamo Bay, Cuba; and a U.S. Department of State database containing approximately 260,000 Classified U.S. State Department internal communications, to include the Classified cable related to the topic of "Icesave" also disclosed by WikiLeaks.

(b)(6)(b)(7)(C) subsequently notified law enforcement of these chat conversations which lead to USACIDC Special Agents in Iraq apprehending MANNING on FOB Hammer on May 27, 2010. Upon MANNING's apprehension by USACIDC, MANNING invoked his legal right to counsel and declined to make any statements in relation his involvement in the unlawful disclosure of Classified U.S. Government materials. MANNING has further been held in confinement since May 27, 2010, pending a Military Courts-Martial.

At the time of MANNING's apprehension in Iraq, USACIDC Special Agents seized numerous U.S. Government and personal computers associated with MANNING on FOB Hammer, per a Military Magistrate Search Authorization. The U.S. Government computers collected as evidence included: several SIPR computers MANNING was identified as having been assigned while working in his position as an Intelligence Analyst in Iraq; several NIPR computers other personnel in MANNING's unit, to include MANNING, would have shared for work-related duties; and several personally owned computers, to include MANNING's personal laptop computer and other items of digital

media as well as those from other personnel in MANNING's unit.

Subsequent computer forensic examination of MANNING's assigned U.S. Government and personal computers by personnel assigned to CCIU, revealed evidence MANNING had unlawfully accessed and/or unlawfully possessed the Classified U.S. Government material he claimed in his Internet chats with Lamo. Further forensic examination revealed MANNING may have used his personal laptop computer and non-military, satellite-based ISP Internet connection to transmit classified documents directly or indirectly to WikiLeaks. During the course of the on-going computer forensic examination of MANNING's primary SIPR computer he was assigned for duty, which contained evidence of his access to Classified U.S. Government material believed to have been disclosed to the website WikiLeaks – the Microsoft Windows personal profile of MANNING was found to have been created on this computer in March 2010. Further forensic examination of this hard drive revealed the Microsoft Operating System installed on this computer appeared to have been installed in 2008; suggesting MANNING had not used this particular SIPR computer during his entire period of duty in Iraq and/or prior to March 2010.

Based on the time line of events set forth in this investigation to include: MANNING's own statements during his Internet chats with (b)(6)(b)(7)(C) the timing of disclosures of certain Classified U.S. Government materials to and/or by the website WikiLeaks, and the known creation/original publication dates of documents disclosed by MANNING; it is believed MANNING's activities related to the unlawful disclosure of Classified U.S. Government materials began prior to March 2010, and may have begun as early as November 2009. Based on this information it is suspected MANNING may

have been using a different U.S. Government computer(s) other than the computers identified and collected at FOB Hammer, Iraq as evidence by USACIDC Special Agents at the time MANNING was apprehended.

Subsequent interviews with personnel assigned to or supporting MANNING's unit related that it was not uncommon for computers to have mechanical problems due to the excessive heat and general dusty conditions of Iraq. Personnel interviewed specifically related they knew of several instances in which MANNING's U.S. Government computer(s) had problems requiring the attention of support personnel. Due to the seemingly insignificant and/or routine nature of these unit computer problems and lack of any reliable unit records showing repairs of computers or the use of replacement parts (such as hard drives), USACIDC Special Agents have been unable to rule-out the use of other U.S. Government computers by MANNING while assigned at FOB Hammer. Based on the workload of MANNING's unit and the need for MANNING's assigned U.S. Government SIPR computers to function for MANNING to conduct his duties, it is believed MANNING's SIPR computer which had been reportedly malfunctioning, may have been substituted for another U.S. Government computer. Based on further discussions with MANNING's unit personnel, it is possible that a computer or hard disk drive from a computer used by MANNING may have been later reissued to other personnel in MANNING's unit once the problem with that computer or hard disk drive was corrected.

In addition to MANNING's assigned U.S. Government SIPR computer's available hard disk drive storage, and possibly due to the abovementioned computer mechanical issues, MANNING was further identified as having used a "Network Share Drive" to

store files and other data as part of his duties in conducting Intelligence Analysis in Iraq. Due to the nature in which MANNING is believed to have harvested large amounts of data from U.S. Government websites and/or databases on the SIPR network, it is further believed that MANNING placed this data, temporarily, within his allocated electronic storage space, on the SIPR Network Share Drive. The computer which functioned as the provider of, and housed this electronic storage space, was a Server also assigned to HHC, 2nd BCT, 10th Mountain Division, and was present at FOB Hammer during the time MANNING's unit was deployed in Iraq. At the request of CCIU during the initial stages of this investigation, and while MANNING's unit was conducting their assigned combat mission in Iraq, HHC, 2nd BCT personnel provided a 'Logical Image' of the electronic storage space used by MANNING. This Logical Image or Logical Copy contained only the files, information and data viewable using the server's Operating System, and would not include "deleted" files, folders, information and data which could be obtained from a 'Physical Image' of the drive(s) on which this storage space resided. Due to a combination of issues related to this server's critical role for MANNING's unit, lack of a replacement server, as well as the mission critical information stored on this server; a more thorough 'Physical Copy' of this storage space and/or a computer forensic examination of this server could not readily be conducted. Further, forensic examinations of other computers used by MANNING had not identified a compelling need to conduct a more in-depth forensic analysis of this server until the time this server had already been prepared for redeployment with MANNING's unit which was returning to Fort Drum and/or it was determined it would have been logistically difficult to have collected and shipped this server to CCIU from Iraq prior to

the unit returning with the property as part of its redeployment.

Based on forensic examinations of MANNING's identified SIPR computers, it is believed additional evidence of files, information, and electronic data MANNING accessed, both while conducting his Intelligence Analysis duties and while committing the mentioned violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information), may be contained on this server and obtainable from a Physical Image of the hard disk drives on this server – providing USACIDC Special Agents a better understanding of the scope of MANNING's activities.

Additional Disclosure of Classified Materials by the Website WikiLeaks

On July 25, 2010, the WikiLeaks website in coordination with The New York Times, The Guardian (a news media publication based in London, England) and Der Spiegel Magazine (a news media publication based in Germany) published approximately 75,000 classified U.S. Government documents relating to the War in Afghanistan. According to an on-line article posted on The New York Times website on July 25, 2010:

"The articles published today are based on thousands of United States military incident and intelligence reports — records of engagements, mishaps, intelligence on enemy activity and other events from the war in Afghanistan — that were made public on Sunday on the Internet. The New York Times, The Guardian newspaper in London, and the German magazine Der Spiegel were given access to the material several weeks ago. These reports are used by desk officers in the Pentagon and troops in the field when they make operational plans and prepare briefings on the situation in the war zone..."

Further, regarding the source of the material The New York Times article relates:

"The documents — some 92,000 individual reports in all — were made available to The Times and the European news organizations by WikiLeaks, an organization devoted to exposing secrets of all kinds, on the condition that the papers not report on the data until July 25, when WikiLeaks said it intended to post the material on the Internet. WikiLeaks did not reveal where it obtained the material."

While the information reported by The New York Times identifies approximately 92,000 reports being disclosed, about 15,000 reports were not published by either the website WikiLeaks or the mentioned news media organizations due to this material believed to contain information more sensitive than in the published material. The New York Times article suggests information even more sensitive than the published Classified U.S. Government materials were obtained from WikiLeaks as the article further relates:

"We have, for example, withheld any names of operatives in the field and informants cited in the reports. We have avoided anything that might compromise American or allied intelligence-gathering methods such as communications intercepts."

The WikiLeaks website in regard to the 15,000 unpublished Classified U.S. Government documents published on its website:

"We have delayed the release of some 15,000 reports from the total archive as part of a harm minimization process demanded by our source. After further review, these reports will be released, with occasional redactions, and eventually in full, as the security situation in Afghanistan permits."

Personnel associated with the website WikiLeaks have publicly acknowledged having other Classified U.S. Government material (which are believed to have been unlawfully disclosed by MANNING) such as the Gharani, Afghanistan airstrike video and associated report; however, for reasons unknown WikiLeaks has not published this material to the public.

MANNING's Unit Redeploys From Iraq to Fort Drum

During the month of August 2010, MANNING's unit begins the process of redeploying from Iraq to Fort Drum after having completed the unit's tour of duty in Iraq. As part of this redeployment process MANNING's unit packed a specific U.S. Government Shipping Container (commonly referred to as a "Connex") with many of the unit's assigned 'Sensitive Items'. According to the DA Form 5748-R, Shipment Unit Packing List and Load Diagram, completed on August 18, 2010, by personnel assigned to MANNING's unit – this Shipping Container was packed with numerous U.S. Government: computers, of various makes and models; cryptological communication equipment; communication equipment; computer networking and peripheral hardware components; high security safes; miscellaneous paper and office supplies; office equipment; over 225 computer hard disk drives packed in boxes or with other equipment; as well as various other miscellaneous U.S. Government Property assigned to HHC, 2nd BCT, 10th Mountain Division. On these shipping documents it was further noted that several of these U.S. Government computer systems and/or equipment was identified as being Classified systems or components.

This Shipping Container, further referred to by unit personnel as the unit's "Sensitive Items Connex", was reportedly securely sealed in accordance with U.S. Army and/or Department of Defense regulations for shipping containers of this nature and was transported under U.S. Government control from Iraq to the United States by sea freight, arriving at the U.S. Port of Beaumont, Texas, on September 6, 2010. This Shipping Container was further transported under U.S. Government control by truck from Beaumont, Texas to Fort Drum, and is scheduled to arrive on or about September

9, 2010. Upon the arrival of this Shipping Container at Fort Drum and its customary processing by the Fort Drum Transportation Office, the HHC, 2nd BCT unit command has arranged for this container to be positioned within the HHC, 2nd BCT unit area; and that personnel assigned to the unit will be on hand to assist USACIDC Special Agents in opening, identifying, inventorying, and preparing the identified computers possibly used by MANNING in Iraq for examination – to determine if each identified computer may have been used by MANNING and/or be of evidentiary value to this investigation.

Additional sensitive items, to include computers and/or computer hard disk drives, similar to and/or identical to ones transported in the aforementioned connex, were reportedly hand-carried by HHC, 2nd BCT unit members redeploying from Iraq back to Fort Drum, where they were placed into a Secured Storage Space, referred to as the "Unit Vault", within the Unit Area. USACIDC Special Agents further wish to examine these items in the same manner and for the same reasons, to identify potential evidence, as the items contained in the mentioned Shipping Container.

Further, a second Shipping Container, identified as the "S-2 Connex" also contains similar and/or identical computer equipment and/or digital media, although reportedly these items have been identified for processing 'Unclassified' information. USACIDC Special Agents desire to survey these items for potential evidence; however, although it was initially reported this Shipping Container had previously arrived at Fort Drum and was located amongst four (4) other similar containers within the Unit Area – at this time the location and/or identity of this Shipping Container is unknown. Should this Shipping Container be identified and/or found to be within the Unit Area, USACIDC Special Agents would also examine these items as well. Unfortunately due to poor

documentation, the previously mentioned server believed to contain the electronic storage space used by MANNING in conjunction with his SIPR computer, appears to have been improperly identified within the HHC, 2nd BCT unit shipping documents. Consequently, HHC, 2nd BCT personnel are unsure of its specific location, but believe it is located in one of the mentioned Shipping Containers or within the Secure Storage Space within the Unit Area.

The Unit Area where the Shipping Container described as the "Sensitive Items Connex" is to be positioned; the "S-2 Connex" which was initially reported to be located within the Unit Area; and the Secure Storage Space within the Unit Area, all containing the described U.S. Government property, are further described in Attachment B.

Method of Examination of U.S. Government Computers by USACIDC Personnel While at Fort Drum

In an attempt to identify what previously unidentified computers MANNING may have used which are in possession of the U.S. Government, USACIDC Special Agents plan on identifying all computer hard disk drives found in the above described Shipping Container(s) and the Secure Storage Space within the Unit Area, and will then connect the hard disk drives using methods and procedures to forensically preserve any potential evidence on those drives, to forensic computers installed with commercially available computer forensic software. The USACIDC Special Agents will then further attempt to determine by the inspection of the electronic file system contained on each hard disk drive as to whether a Windows User Profile related to MANNING's SIPR and/or NIPR network account(s) are present on the drive(s). Should a drive be found

containing a Windows User Profile for MANNING, this will provide a strong indication this drive was once contained in or associated with a computer used by MANNING's network user account. Consequently these hard disk drive(s) will be seized, collected as evidence, and further computer forensic examination will be conducted to determine the drive's evidentiary value to this investigation as further described in Attachment C.

I have learned in my professional experience in conducting forensic examinations that intentional or unintentional data and information stored on hard disk drives and other digital media, is highly persistent and may remain on digital media, computers, and computer-related devices nearly indefinitely without concerted efforts to purge or "wipe" this data by personnel with specialized tools and/or knowledge beyond the average computer user. More specifically when data is "Deleted" by a computer user, although this data may be no longer accessible to the computer user by normal means of the Operating System - this data is not removed from the digital media it was contained on necessarily, but the space this data occupies may simply be marked as available for future data to be stored in its place by the Operating System. However, until over-written by future data it may remain fully or partially intact and can provide further evidence of criminal violations or in some cases exculpatory evidence. Consequently, although considerable time has passed since MANNING may have accessed any computers and/or hard disk drives contained in the mentioned Shipping Containers or the Secure Storage Space, the likelihood evidence related to MANNING's activities is still present should MANNING have used that given computer or hard disk drive is relatively high. This is also true of the electronic storage space on the

mentioned server, which uses the same technology, hard disk drives, in which to store information.

Requirement for Military Magistrate Search Authorization

While the aforementioned physical items USACIDC Special Agents wish to evaluate for potential evidence have been: identified as U.S. Government property and that no personal property has been identified as having been co-mingled into the identified Shipping Container(s); that the unit responsible for the property identified in the Shipping Container(s) have consented to USACIDC Special Agents inspecting the items for evidence and are cooperating in this process – the information contained on items of digital media (such as hard disk drives) may still contain personal information, documents, electronic communications between third-parties associated or not associated with MANNING, who in various circumstances may still have a limited expectation to privacy to this information stored on these computer systems, hard disk drives, and/or digital media owned by the U.S. Government. Further, although USACIDC Special Agents will attempt to quickly evaluate each item of digital media for signs of its previous use by MANNING as a practical matter to facilitate the expeditious evaluation of a large number of items – in some cases inadvertent or unavoidable viewing of personal data, third-party communications, digital photographs, and/or other electronic information which individuals, to include MANNING, may have limited privacy expectations to this data, may still occur. Further, the evaluation process mentioned herein, while minimally invasive, could be considered in a certain sense, a “search” in of itself, as the computers, hard disk drives, and other digital media to be evaluated are

not merely 'open containers' easily viewable without specialized computer forensic hardware, forensic software tools and training.

Upon the identification of any digital media located in the places to be searched, as described in Attachment B, which are believed to have been previously used by MANNING, USACIDC Special Agents will seize and further search these identified digital media items for additional evidence, fruits and instrumentalities of violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information), in accordance with the procedures specified in Attachment C.

Conclusion

Given the facts and circumstances of the incidents related to the unlawful disclosure of Classified U.S. Government material by MANNING; the identification of Classified U.S. Government materials on MANNING's personal computer; the identification MANNING may have used other computers belonging to his unit to conduct his unlawful activities; that a hard disk drive(s) from MANNING's identified SIPR computer may have been replaced with other hard disk drives due to computer mechanical failures, and that these hard disk drives may still be in the possession of MANNING's former unit; that MANNING is known to have used electronic network storage space on an identified server belonging to MANNING's former unit; that data and/or evidence on all of these items could reasonably still exist - there is probable cause to believe that additional evidence, fruits and instrumentalities of the offenses believed to have committed by MANNING to include violations of 18 U.S.C. § 793(d)

(Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information) are contained on: computers; the identified SIPR server containing the electronic storage space MANNING utilized; hard disk drives present within computers, the mentioned SIPR server, and/or as stand-alone items; and/or other digital media exists – which are further contained within the aforementioned “Sensitive Items Connex” and/or “S-2 Connex” (herein identified as U.S. Government Shipping Containers) and/or within Secure Storage Space (herein identified as the “Unit Vault”) of HHC, 2nd BCT, 10th Mountain Division, located 10200 North Riva Ridge Loop, Fort Drum, New York – and described in more detail in Attachment C.

ATTACHMENT B

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The following locations are to be searched as explained in Attachment A and reported to be located and/or are to-be located within and/or adjacent to the main office space of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, 10200 North Riva Ridge Loop, Fort Drum, New York, are described as follows:

The U.S. Government Shipping Container, Identified by Seal Number "AWBDAAA\$0F0286XX", and further described as 96 inches wide, by 96 inches tall, by 78 inches in length, 416 cubic feet, metal Tricon, container, marked with unit identification information of HHC, 2nd BCT, 10th Mountain Division (WBDAAA) – which is further referred to in Attachment A, as the "Sensitive Items Connex";

The U.S. Government Shipping Container, Identified by Seal Number Unknown, and further described as 96 inches wide, by 96 inches tall, by 78 inches in length, 416 cubic feet, Metal Tricon, container, marked with unit identification information of HHC, 2nd BCT, 10th Mountain Division (WBDAAA) – which is further referred to in Attachment A, as the "S-2 Connex"; and,

The Secure Storage Space also known as the "Unit Vault", which is described as a secure storage area for the storage of sensitive items of U.S. Government and/or Military property within the HHC, 2nd BCT, 10th Mountain Division Unit Area.

ATTACHMENT C

ITEMS TO BE SEIZED AND SEARCHED

Special Agents of USACIDC or other Army law enforcement personnel assisting USACIDC to search the location of 10200 North Riva Ridge Loop, Fort Drum, New York, and the immediate adjacent areas associated with Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division as described in Attachment B, and therein to seize and subsequently search all computer hardware and digital media having been identified as associated with or previously used by Private First Class (PFC) Bradley Edward MANNING, formerly assigned to HHC, 2nd BCT, 10th Mountain Division – specifically as it relates to information, documents, and data, both classified and unclassified, as mentioned in Attachment A, which is herein incorporated into Attachment C, in regard to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information).

Computer Hardware and Digital Media is further described as any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data processing hardware (such as "desktop computers" and self-contained "laptop", "notebook", or "netbook" computers, as well as "Smart Phones" and internet capable PDAs); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical disc storage devices such as CDs or DVDs, USB drives, flash

memory cards or similar solid-state storage media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

FURTHER SEARCH OF SEIZED COMPUTERS AND DIGITAL MEDIA ITEMS

The items seized as part of this Search Authorization, which should consist of computers, servers, hard disk drives, and/or other digital media, will have forensically sound images (digital copies) produced of the seized items as appropriate, which will in turn be searched in lieu of the original seized items as part of a digital media/computer forensic examination. The search of digital copies of the items seized is done to ensure and preserve the forensic integrity of the seized items for additional and/or future examination(s) in accordance with criminal procedure and rules of evidence. These examination(s) of seized items will be conducted by personnel assigned to the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) who are certified by the Department of Defense and/or Department of the Army to conduct such types of examinations. These personnel will use computer forensic hardware and/or software, which has been approved for use in conducting such examinations. Due to the unknown nature and/or number of items which could be seized within the scope of this Search Authorization, it is not necessarily practical or

feasible to make forensically sound images (digital copies) of seized evidence while at the search location. Subsequently, these digital copies will be produced within a reasonable amount of time, unless extended by authorization of the Military Magistrate, with the originally seized items being returned to the owner of the property in accordance with Army Regulation 195-5, "Evidence Procedures". Further, due to the unknown number of items seized, as well as the complexity of examining these items, it is also not feasible to conduct a search/forensic examination of the items while at the search location to determine their complete evidentiary value. Consequently, this search/examination activity will be completed within facilities operated by the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) and completed as expeditiously as possible.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1023, 10 Sep 10, SA (b)(6)(b)(7)(C), (b)(7)(E) SA (b)(6)(b)(7)(C), (b)(7)(E) and SA (b)(6)(b)(7)(C), (b)(7)(E) all assigned to Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, interviewed 1LT (b)(6)(b)(7)(C), HHC, 2nd Brigade Combat Team (2nd BCT), 10th Mountain Division (10th Mtn Div), Fort Drum, NY (FDNY), who stated she was currently assigned to the 2nd BCT S-2 shop and first met PFC MANNING shortly after her arrival at FDNY around June or July of 2008. 1LT (b)(6)(b)(7)(C) stated that because she had to attend training in July, 2009, away from FDNY, she departed for Forward Operating Base (FOB) Hammer, Iraq in February, 2010, several months later than the rest of the 2nd BCT. 1LT (b)(6)(b)(7)(C) stated while at FOB Hammer, PFC MANNING was a "go-to" person for computer problems and would often help other Soldiers. 1LT (b)(6)(b)(7)(C) stated the Entry and Exit (E/E) door of the Sensitive Compartmented Information Facility (SCIF) at FOB Hammer was equipped with a push-button cipher lock and its combinations would often change according to the Standing Operating Procedures (SOP) but no access logs were kept. 1LT (b)(6)(b)(7)(C) further identified the following soldiers as the ones she remembered having access to the SCIF at FOB Hammer:

1. SFC (b)(6)(b)(7)(C) Fort Drum, NY;
2. MAJ (b)(6)(b)(7)(C), 2-15th Field Artillery (2-15 FA), 2nd BCT, 10th Mountain Division (10th Mtn Div), Fort Drum, NY (FDNY);
3. 1LT (b)(6)(b)(7)(C) Military Intelligence (MI) Company (Co.), 2nd Brigade Special Troop Battalion (2nd BSTB), 10th Mtn Div, FDNY;
4. CPT (b)(6)(b)(7)(C) MI Co., 2nd BSTB, 10th Mtn Div, FDNY;
5. 1SG (b)(6)(b)(7)(C) (NFI); MI Co., 2nd BSTB, 10th Mtn Div, FDNY;
6. SPC (b)(6)(b)(7)(C) (NFI);
7. 1LT (b)(6)(b)(7)(C) Bravo (B) Co., 2nd BSTB, 10th Mtn Div, FDNY;
8. CPT (b)(6)(b)(7)(C), HHC, 2nd BCT, 10th Mtn Div, FDNY;
9. SPC (b)(6)(b)(7)(C) HHC, 2nd BCT, 10th Mtn Div, FDNY;
10. SPC (b)(6)(b)(7)(C) HHC, 2nd BCT, 10th Mtn Div, FDNY;
11. PFC (b)(6)(b)(7)(C) 2-15 FA, 2nd BCT, 10th Mtn Div, FDNY;
12. SPC (b)(6)(b)(7)(C) B Co., 2nd BSTB, 10th Mtn Div, FDNY;
13. CPT (b)(6)(b)(7)(C) (NFI), Permanent Change of Station (PCS);
14. CPT (b)(6)(b)(7)(C) 1-89th Cavalry (1-89 CAV), 2nd BCT, 10th Mtn Div, FDNY;
15. CPT (b)(6)(b)(7)(C) 2-15 FA, 2nd BCT, 10th Mtn Div, FDNY;
16. CW3 (b)(6)(b)(7)(C) FDNY;
17. WO1 (b)(6)(b)(7)(C) FDNY;
18. CW2 (b)(6)(b)(7)(C) FDNY;
19. Mr. (b)(6)(b)(7)(C) (NFI), Civilian;
20. Mr. (b)(6)(b)(7)(C) Contractor, DCGS-A System Administrator, Camp Ramadi, Iraq;
21. SSG (b)(6)(b)(7)(C) B Co., 2nd BSTB, 10th Mtn Div, FDNY;
22. SFC (b)(6)(b)(7)(C) B Co., 2nd BSTB, 10th Mtn Div, FDNY;

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E) /

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

12 Sep 10

EXHIBIT

202

1 FEB 77

OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001299
Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

23. (b)(6)(b)(7)(C) FDNY;
 24. CPT (b)(6)(b)(7)(C) FDNY; and
 25. CW2 (b)(6)(b)(7)(C) National Security Agency (NSA), Fort Meade, MD 20755
 ///////////////////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
 U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

SA (b)(6)(b)(7)(C)

DATE

12 Sep 10

EXHIBIT

202

OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

1 FEB 77

001300
 Approved _____

Exhibit(s) 203

Page(s) 001301 and 01301a withheld:

5 U.S.C. § 552(b)(1)

Permits withholding information that
is classified for
National Security purposes

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

For Official Use Only - Law Enforcement Sensitive

ROI NUMBER: 0028-10-CID221-
0084-10-CID609

PAGE 1 of 4 PAGES

DETAILS

BASIS FOR INVESTIGATION: About 1500, 7 Jul 10, this office received Category 1 Request For Assistance (RFA) 0028-10-CID221-10117, from the Washington Metro Resident Agency, Computer Crimes Investigative Unit (CCIU), 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060 (FBVA), to obtain information regarding inmate PFC Bradley E. MANNING, (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, FOB Hammer, Iraq APO AE 09308 (FHIZ), detained at the Theater Field Confinement Facility (TFCF), Camp Arifjan, Kuwait APO AE 09366 (CAKU). The requested information included the following: potential dates of transfers, whether the transfers were permanent or temporary, potential recorded phone conversations, logs of phone calls made by PFC MANNING, identification of any other means of communication accessed by PFC MANNING, inventory records of the personal belongings of PFC MANNING, potential review of PFC MANNING's personal belongings if stored in a clear container, detailed report of PFC MANNING's behavior and activities since arriving to TFCF, CAKU.

About 1500, 8 Jul 10, SA (b)(6)(b)(7)(C) coordinated with CDR (b)(6)(b)(7)(C) YN1 (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) and MAC (b)(6)(b)(7)(C) all of TFCF, CAKU. CDR (b)(6)(b)(7)(C) reported PFC MANNING was originally in General Population, but was moved and sent to Administrative Segregation once he began to act up. CDR (b)(6)(b)(7)(C) stated PFC MANNING developed relationships with a couple of the inmates, and then had a falling out, which caused PFC MANNING to act out. CDR (b)(6)(b)(7)(C) related PFC MANNING stated he was sick of the inmates "queer bashing". CDR (b)(6)(b)(7)(C) stated PFC MANNING was originally segregated into the 30 minute Check Section, but then moved to 15 minute Check Section, which was where inmates were visually checked every 30 or 15 minutes. CDR (b)(6)(b)(7)(C) stated PFC MANNING, at one point, fashioned a noose out of his bed sheets; and he was subsequently put on 24/7 Suicide Watch. CPT (b)(6)(b)(7)(C) stated CPT (b)(6)(b)(7)(C) Psychiatrist, Director of Mental Health, CAKU, CDR (b)(6)(b)(7)(C) Psychiatrist and LT (b)(6)(b)(7)(C) Clinical Psychologist, all of TFCF, were all providing mental health evaluations and counseling to PFC MANNING. CPT (b)(6)(b)(7)(C) stated PFC MANNING's condition was evaluated, and he was put on medication. CPT (b)(6)(b)(7)(C) stated TFCF, CAKU, was not equipped to provide the level of psychological care needed by PFC MANNING. CDR (b)(6)(b)(7)(C) stated this was why it was being contemplated to move PFC MANNING; but stated no decisions had been made yet. CPT (b)(6)(b)(7)(C) reported PFC MANNING was claiming to be a woman stuck in a man's body. CPT (b)(6)(b)(7)(C) stated since beginning to take the medications, PFC MANNING calmed down and even apologized to CPT (b)(6)(b)(7)(C). CDR (b)(6)(b)(7)(C) stated PFC MANNING had been under a media and communication ban; but had recently been given his glasses and re-granted his reading privileges. CDR (b)(6)(b)(7)(C) stated PFC MANNING was currently reading a novel. CDR (b)(6)(b)(7)(C) stated all inmates are allotted the privilege of utilizing the phone for 30 minutes each night; but were forbidden from discussing their cases. CDR (b)(6)(b)(7)(C) stated the calls were a privilege, logs were kept of each call and the calls themselves are monitored. CDR (b)(6)(b)(7)(C) stated PFC

TYPED AGENT'S NAME AND SEQUENCE NUMBER:

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION:

Arifjan CID Office
1156th MP DET (CID) (FWD), 11th MP BN (CID) (FWD)
Camp Arifjan, Kuwait APO AE 09366

SIGNATURE:

(b)(6)(b)(7)(C)

DATE:

16 Sep 10

EXHIBIT:

204

<h2 style="margin: 0;">AGENT'S INVESTIGATION REPORT</h2> <p style="margin: 0;"><i>CID Regulation 195-1</i></p> <p style="margin: 0;"><i>For Official Use Only – Law Enforcement Sensitive</i></p>		<p>ROI NUMBER: 0028-10-CID221-0084-10-CID609</p>	
		<p>PAGE 2 of 4 PAGES</p>	
<p>DETAILS</p> <p>MANNING called his Aunt, and requested she changed his Status on Face Book. CDR (b)(6)(b)(7)(C) stated the phone call was disconnected immediately and PFC MANNING's phone call privileges were revoked. YN1 (b)(6)(b)(7)(C) stated PFC MANNING's personal belonging were inventoried on a DA Form 1132-R, Prisoner's Personal Property List, and kept in an opaque plastic storage container on the facility. YN1 (b)(6)(b)(7)(C) stated PFC MANNING had papers on his person when he was escorted to the facility. YN1 (b)(6)(b)(7)(C) stated he did not know what was on the papers, but one paper specifically was a price list for sex change operations. CDR (b)(6)(b)(7)(C) stated PFC MANNING was visited by MAJ (b)(6)(b)(7)(C) Trial Counsel, Staff Judge Advocate, Area Support Group, CAKU, who read PFC MANNING his charges. CDR (b)(6)(b)(7)(C) stated MAJ (b)(6)(b)(7)(C) provided PFC MANNING with a copy of his Charge Sheet, but stated the Charge Sheet was later removed from PFC MANNING's possession and placed inside of his Personal Property storage container. CDR (b)(6)(b)(7)(C) stated his office would provide SA (b)(6)(b)(7)(C) with Observation Reports/Logs, Disciplinary Reports/Logs, DA Form 1132-R, Medical Records, Mental Health Records, Phone Call Logs and recordings of the phone conversations. CDR (b)(6)(b)(7)(C) requested SA (b)(6)(b)(7)(C) provide him with a written request to obtain these documents.</p> <p>AGENT'S COMMENT: SA (b)(6)(b)(7)(C) was informed the TFCF utilized a recording system which required specific software with which to listen to the recordings. CDR (b)(6)(b)(7)(C) stated he would still provide SA (b)(6)(b)(7)(C) with recordings of the conversations, but if she needed to, he would make MAC (b)(6)(b)(7)(C) available for SA (b)(6)(b)(7)(C) to review all the conversations and take notes.</p> <p>About 1700, 8 Jul 10, SA (b)(6)(b)(7)(C) submitted a DA Form 4254-R, (Request for Private Medical Information) pertaining to the medical records and mental health records of PFC MANNING, since his arrival to TFCF, CAKU. The request was denied.</p> <p>About 1450, 9 Jul 10, SA (b)(6)(b)(7)(C) coordinated with CDR (b)(6)(b)(7)(C) who stated when a Service Member was brought to TFCF, the Service Member was searched, personal property confiscated, inventoried and then stored. CDR (b)(6)(b)(7)(C) stated if the Service Member needed something out of their personal property, then a request was submitted. CDR (b)(6)(b)(7)(C) related as long as the request was reasonable, the property was supplied to the inmate, and then returned to storage at the end of use. CDR (b)(6)(b)(7)(C) stated TFCF had access to the personal property of inmates, but no real reason to access it, unless requested to do so by a granted request from an inmate.</p> <p>About 1505, 9 Jul 10, SA (b)(6)(b)(7)(C) coordinated with YN1 (b)(6)(b)(7)(C) who stated the phone log did not indicate what was said during calls, so he could not tell from the Log which day it was. YN1 (b)(6)(b)(7)(C) also stated he did not have access to the disc containing the conversations due to software restrictions.</p>			
<p>TYPED AGENT'S NAME AND SEQUENCE NUMBER:</p> <p>SA (b)(6)(b)(7)(C), (b) (7)(E)</p>		<p>ORGANIZATION:</p> <p>Arifjan CID Office 1156th MP DET (CID) (FWD), 11th MP BN (CID) (FWD) Camp Arifjan, Kuwait APO AE 09366</p>	
<p>SIGNATURE:</p> <p>(b)(6)(b)(7)(C)</p>		<p>DATE:</p> <p>16 Sep 10</p>	<p>EXHIBIT:</p> <p>204</p>

CID FORM 94

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

1 FEB 77

001303

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

For Official Use Only - Law Enforcement Sensitive

ROI NUMBER: 0028-10-CID221-
0084-10-CID609

PAGE 3 of 4 PAGES

DETAILS

About 1520, 9 Jul 10, SA (b)(6)(b)(7)(C) Coordinated with CDR (b)(6)(b)(7)(C) to inform him although the case agent had access to Central Operations Police System (COPS), she did not have access to the portion of COPS which dealt with inmates and related reports. CDR (b)(6)(b)(7)(C) reviewed the Observation Reports for PFC MANNING. CDR (b)(6)(b)(7)(C) related Regulation and SOP infractions were documented in the Observation Reports, once an inmate seeks assistance with Mental Health. CDR (b)(6)(b)(7)(C) stated this was done so there was not added stress placed upon the already fragile mental stated of inmates. CDR (b)(6)(b)(7)(C) further explained this as with most Disciplinary Reports, multiple counseling were involved, rather than when an infraction was documented through the Observation Reports. CDR (b)(6)(b)(7)(C) was able to inform SA (b)(6)(b)(7)(C) that PFC MANNING made the Face Book call to his Aunt on 7 Jun 10. CDR (b)(6)(b)(7)(C) stated from what he could see of the report, PFC MANNING informed his Aunt of his Face Book password and username.

About 1725, 9 Jul 10, SA (b)(6)(b)(7)(C) Coordinated with MAJ (b)(6)(b)(7)(C) Military Magistrate, Office of the Staff Judge Advocate (OSJA), CAKU and submitted a Affidavit Supporting request for Authorization to Search and Seize or Apprehend and a Search Authorization. MAJ (b)(6)(b)(7)(C), (b) (5)

(b) (5)
(b) (5) MAJ (b)(6)(b)(7)(C) stated TFCF personnel could conduct the search in front of SA (b)(6)(b)(7)(C) in regards to PFC MANNING's personal property. SA (b)(6)(b)(7)(C) reiterated the need to be very careful in this investigation, which was why CCIU requested this office obtain a search authorization. MAJ (b)(6)(b)(7)(C) stated she would not grant the search authorization.

About 1300, 21 Jul 10, SA (b)(6)(b)(7)(C) coordinated with CDR (b)(6)(b)(7)(C) who related the TFCF would not release any documents without a court order or an order from ARCENT directing the release.

About 1400, 21 Jul 10, SA (b)(6)(b)(7)(C) coordinated with MAJ (b)(6)(b)(7)(C) ASG Deputy Chief Judge Advocate, OSJA, CAKU and requested assistance in obtaining the records and documents from the TFCF.

About 1324, 18 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C), this office, coordinated with Petty Officer (PO) (b)(6)(b)(7)(C) Administrative office, TFCF, regarding request for documents pertaining to PFC MANNING. PO (b)(6)(b)(7)(C) recommended this issue be addressed to CPT (b)(6)(b)(7)(C)

About 1330, 18 Aug 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) made contact with CPT (b)(6)(b)(7)(C) who related he did not have the diagnosis for PFC MANNING, but only had interviews with PFC MANNING over last 10-12 days before he was returned to CONUS. CPT (b)(6)(b)(7)(C) also related Dr. (b)(6)(b)(7)(C) (NFI) was at Quantico, VA.

TYPED AGENT'S NAME AND SEQUENCE NUMBER:

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION:

Arifjan CID Office
1156th MP DET (CID) (FWD), 11th MP BN (CID) (FWD)
Camp Arifjan, Kuwait APO AE 09366

SIGN

(b)(6)(b)(7)(C)

DATE:

16 Sep 10

EXHIBIT:

204

CID FORM 94

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

001304

AGENT'S INVESTIGATION REPORT*CID Regulation 195-1**For Official Use Only - Law Enforcement Sensitive*ROI NUMBER: 0028-10-CID221-
0084-10-CID609

PAGE 4 of 4 PAGES

DETAILS

About 1000, 28 Aug 10, SA (b)(6)(b)(7)(C) coordinated with MAJ (b)(6)(b)(7)(C) who related he had copies of the paper documents produced by the TFCF.

About 1300, 28 Aug 10, SA (b)(6)(b)(7)(C) this office, coordinated with MAJ (b)(6)(b)(7)(C) and obtained copies of the documents from detention facility. (See reports pertaining to PFC MANNING for Details)

About 1400, 7 Sep 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) Chief of Military Justice, 1st Armored Division, Camp Liberty, Iraq who related SA (b)(6)(b)(7)(C) CCIU, FBVA had requested he contact this office to complete the Search Affidavit. SA (b)(6)(b)(7)(C) related he would coordinate with SA (b)(6)(b)(7)(C) or SA (b)(6)(b)(7)(C) to figure out what else needed to be accomplished.

About 2230, 7 Sep 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) who related SA (b)(6)(b)(7)(C) had set up for this office to forward the affidavit to CPT (b)(6)(b)(7)(C)

About 2245, 7 Sep 10, SA (b)(6)(b)(7)(C) forwarded the original search affidavits to CPT (b)(6)(b)(7)(C)

About 1051, 14 Sep 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) ASG Deputy Chief Judge Advocate, OSJA, (b)(6)(b)(7)(C) who related she received an email from MAC (b)(6)(b)(7)(C) Prisoner Services Branch, TFCF, (b)(6)(b)(7)(C) relating PFC MANNING's belonging were forwarded to the Quantico Confinement Facility on 30 Aug 10.

About 1859, 14 Sep 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) who related to disregard obtaining a search authorization.

About 2309, 15 Sep 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) who related nothing further was needed from this office.

About 0930, 16 Sep 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) ASG Deputy Chief Judge Advocate, OSJA, (b)(6)(b)(7)(C) and obtained a CD containing the telephone conversations and a copies of pictures of the items SPC MANNING attempted to kill himself with. (See CD and Picture for Details)

This case is closed in the files of this office. No further investigative activity is anticipated. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER:

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION:

Arifjan CID Office
1156th MP DET (CID) (FWD), 11th MP BN (CID) (FWD)
Camp Arifjan, Kuwait APO AE 09366

SIGNATURE:

(b)(6)(b)(7)(C)

DATE:

16 Sep 10

EXHIBIT:

204

CID FORM 94

FOR OFFICIAL USE ONLY

1 FEB 77

LAW ENFORCEMENT SENSITIVE

001305

EXHIBIT(s) 205

Page(s) 001306 thru 001408 referred to:

SECNAV/CNO FOIA Office
Chief of Naval Operations (DNS-36)
2000 Navy Pentagon
Washington, DC 20350-2000

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Between 1130 and 1530, 18 Sep 10, SA (b)(6)(b)(7)(C) recorded PFC MANNING's visitation period at the Marine Corps Brig - Quantico, Quantico, VA . During visiting hours, PFC MANNING had two visitors, Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C). (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) visited with PFC MANNING for approximately 2 hours 35 minutes.

Between 1125 and 1530, 19 Sep 10, SA (b)(6)(b)(7)(C) recorded PFC MANNING's visitation period at the Marine Corps Brig - Quantico, Quantico, VA . During visiting hours, PFC MANNING had two visitors, Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C). Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) visited with PFC MANNING for approximately 2 hours 50 minutes.

About 1113, 20 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one DVD which captured the recording of PFC MANNING's 18 Sep 10 and 19 Sep 10 visitation periods at the Marine Corps Brig - Quantico. The collection was documented on DA Form 4137, Evidence/Property Custody Document (EPCD), Document Number (DN) 139-10. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

20 Sep 10

EXHIBIT

206

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001409
Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1130, 16 Sep 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) Military Magistrate, 9910 Lowen Road, Building 702, Fort Belvoir, VA 22060, to obtain a Military Magistrate Search Authorization for the personal property items of PFC MANNING which had been collected in Iraq by PFC MANNING's unit. These items were subsequently turned over by PFC MANNING's unit to Military Intelligence personnel who had been conducting a parallel investigation related to PFC MANNING's activities while assigned to Forward Operating Base (FOB) Hammer, Iraq. These personal property items were further released to the Camp Liberty CID Office, Camp Liberty, Iraq, which collected these items as evidence within a sealed container. The items were subsequently forwarded to the Evidence Depository in Kuwait which supported the Camp Liberty CID Office, which in turn transferred these items to the Washington Metro Resident Agency (WMRA), CCIU, along with other evidence collected in this investigation. During the coordination, CPT (b)(6)(b)(7)(C) asked SA (b)(6)(b)(7)(C) numerous questions pertaining to the affidavit presented to her in regard to the aforementioned property. CPT (b)(6)(b)(7)(C) based on the information presented, opined there was probable cause to conduct a search of the items and granted the Military Magistrate Search Authorization.

AGENT'S COMMENT: SA (b)(6)(b)(7)(C) was on Temporary Duty (TDY) in Charlotte, NC, at the time of the coordination with CPT (b)(6)(b)(7)(C) regarding the Search Authorization. SA (b)(6)(b)(7)(C) and CPT (b)(6)(b)(7)(C) made an agreement that SA (b)(6)(b)(7)(C) would come to CPT (b)(6)(b)(7)(C) office on 20 Sep 10, upon completion of TDY, in order to provide an original signature on all documents related to the Search Authorization.

About 0945, 20 Sep 10, SA (b)(6)(b)(7)(C) met with CPT (b)(6)(b)(7)(C) to finalize the Military Magistrate Search Authorization paperwork from 16 Sep 10.

About 1133, 21 Sep 10, SA (b)(6)(b)(7)(C) contacted CPT (b)(6)(b)(7)(C) and explained that upon retrieving the Sealed Container to be searched per the Military Magistrate Search Authorization from the Evidence Depository of this office, it was found this container was not a cardboard box, but was instead a paper envelope. SA (b)(6)(b)(7)(C) noted the original container which held PFC MANNING's personal belongings was a cardboard box which had been sealed (as indicated on the evidence voucher); however, when this container was received from the Camp Liberty CID Office by the Evidence Custodian in Kuwait (which processed evidence collected at numerous CID offices located within Iraq), the items were removed from the original cardboard box and repackaged into a new container, a paper envelope. The Evidence Custodian in Kuwait, SA (b)(6)(b)(7)(C) Evidence Custodian, 11th Military Police Battalion (CID), Camp Arifjan, Kuwait, APO AE 09366, further prepared a Memorandum For Record (MFR) documenting this repackaging activity. CPT (b)(6)(b)(7)(C) related the Military Magistrate Search Authorization was still valid, even though the description of the container was different, as the scope of the Search Authorization related to the items within the 'sealed container' (the personal belongings of PFC MANNING).

About 1150, 21 Sep 10, SA (b)(6)(b)(7)(C) signed out the evidence collected on Evidence/Property Custody Document (EPCD), Document Number (DN) 111-10, which was the container holding the personal belongings of PFC MANNING which had been collected from his FOB Hammer barracks room. SA

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

21 Sep 10

EXHIBIT

207

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001410
Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

(b)(6)(b)(7)(C) as witnessed by Ms. (b)(6)(b)(7)(C) Evidence Custodian, CCIU, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060, unsealed the container and found 23 items of evidence (each sealed in their own individual containers) inside. SA (b)(6)(b)(7)(C) examined the items which appeared to be various documents PFC MANNING had authored or documents from multiple sources which had been printed and/or contained handwritten information. The documents appeared to be: notes made by PFC MANNING which, based on the context of the documents, related to an Equal Opportunity complaint(s) about soldiers assigned to PFC MANNING's unit; personal and/or official military documents related to personnel actions involving PVT (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), FOB Hammer, Iraq, which were dated December 2009; documents related to the procedures for processing U.S. Army separation actions under Army Regulation (AR) 635-200; various documents related to transgender personnel in the military; as well as a spiral notebook which contained a hand written note stating, "I may have gender identity issues." SA (b)(6)(b)(7)(C) recorded digital photographs of all items of evidence. Of all of the evidence items examined, none of these items appeared to be of immediate evidentiary value in regard to this investigation.

//////////////////// LAST ENTRY //////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

21 Sep 10

EXHIBIT

207

SEARCH AND SEIZURE AUTHORIZATION

For use of this form, see AR 27-10; the proponent agency is OTJAG

TO: (Name and Organization of the person to whom authorization is given)

Special Agent (b)(6)(b)(7)(C) of the United States Army Criminal Investigation Command (USACIDC)

(An affidavit) (A (sworn) or (unsworn) oral statement) having been made before me by

Special Agent (b)(6)(b)(7)(C)

(Name of Affiant)

Washington Metro Resident Agency, Computer Crime Investigative Unit (CCIU), USACIDC, Fort Belvoir, Virginia 22060

(Organization or Address of Affiant)

(which affidavit is attached hereto and made a part of this authorization), and as I am satisfied that there is probable cause to believe that the matters mentioned in the affidavit are true and correct, that the offense set forth therein has been committed, and that the property to be seized is located (on the person) (at the place) to be searched, you are hereby ordered to search the (person) (place) known as

Scaled Container containing the personal belongings of PFC MANNING, at 9805 Lowen Rd, Bldg 193, Fort Belvoir, VA 22060

for the property described as all papers, documents, notebooks, letters, receipts, postal forms, customs forms, and all other written

or printed material; as well as any digital media or other personal property which may contain information or data related to

postal mail and/or packages mailed by PFC MANNING and passwords used by PFC MANNING.

bringing this order to the attention of the (person searched) (person in possession, if any person be found at the place or on the premises searched). The search will be made in the (daytime) (nighttime), and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to:

Evidence Custodian, Computer Crime Investigative Unit (CCIU), 9805 Lowen Road, Bldg 193, Fort Belvoir, Virginia

(Name and Organization of Authorized Custodian)

and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 16TH day of September, 2010

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL

(b)(6)(b)(7)(C)

CPT, JA

DUTY POSITION OF AUTHORIZING OFFICIAL

MILITARY MAGISTRATE

ORGANIZATION OF AUTHORIZING OFFICIAL

OSJA FORT BELVOIR, VA

SIGNATURE (b)(6)(b)(7)(C) ICIAL

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

For use of this form, see AR 27-10; the proponent agency is OTJAG.

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

1. I, Special Agent (b)(6)(b)(7)(C), Washington Metro Resident Agency
(Name) (Organization or Address)

Computer Crime Investigative Unit (CCIU), USACIDC, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060

having been duly sworn, on oath depose and state that:

SEE ATTACHMENT A.

2. The affiant further states that:

SEE ATTACHMENT A.

3. In view of the foregoing, the affiant requests that an authorization be issued for a search of

SEE ATTACHMENT B

(the person) (and)

(the quarters or billets) (and)

SEE ATTACHMENT C

(the automobile) (

and (seizure) (apprehension) of

(items/persons searched for)

TYPED NAME AND ORGANIZATION OF AFFIANT

Special Agent (b)(6)(b)(7)(C)
Washington Metro Resident Agency
Computer Crime Investigative Unit (CCIU), USACIDC

S (b)(6)(b)(7)(C)

SWORN TO AND SUBSCRIBED BEFORE ME THIS 16TH DAY OF September 2010 AT 1130

TYPED NAME, ORGANIZATION AND OFFICIAL CAPACITY OF AUTHORITY
ADMINISTERING THE OATH

(b)(6)(b)(7)(C)

CPT, JA/ OSJA FORT BELVOIR, VA
MILITARY MAGISTRATE

SIG (b)(6)(b)(7)(C) RITY ADMINISTERING THE OATH

INSTRUCTIONS FOR

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it has been committed. Use additional page if necessary.
2. In paragraph 2, set forth facts establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraphs 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she has plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary.
3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under certain circumstances for evidentiary matters.

ATTACHMENT A

INTRODUCTION

I make this affidavit in support of an application for a Military Magistrate Search Authorization for data, information, writings, documents, receipts and U.S. Customs forms and other physical evidence in any other format relating to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information). As set forth herein, there is probable cause to believe within a sealed container, further described as a brown cardboard box, measuring approximately 12 inches by 10 inches by 5 ½ inches, and sealed with green, 2-inch adhesive (military 100-mile-and-hour) tape along all box seals (herein "Sealed Container"), and containing the personal property of Private First Class (PFC) Bradley Edward MANNING ("MANNING"), formerly assigned to Headquarters and Headquarters Company ("HHC"), 2nd Brigade Combat Team ("BCT"), 10th Mountain Division, Forward Operating Base ("FOB") Hammer, Iraq; which are presently located within the Evidence Depository, Computer Crime Investigative Unit ("CCIU"), 9805 Lowen Road, Building 193, Fort Belvoir, Virginia; contains evidence, fruits, and/or instrumentalities of the offenses committed by MANNING, as further described in this affidavit.

AGENT BACKGROUND

I am a Special Agent in the United States Army Criminal Investigation Command ("USACIDC") and have been so for approximately eight years. I am currently assigned to the USACIDC, Washington Metro Resident Agency, of CCIU, located at Fort Belvoir,

Virginia; where I am responsible for the investigation of, among other things, violations pertaining to computer intrusions, denial of service attacks, and other types of malicious computer activity directed against U.S. Army and/or Department of Defense computer networks anywhere in the world. Prior to my assignment at CCIU, I was assigned as a Special Agent with USACIDC in: South Korea, where I was responsible for conducting felony investigations impacting the U.S. Army in South Korea; Fort Lewis, Washington, where I was responsible for conducting felony investigations impacting the U.S. Army in the states of Washington, Oregon, Idaho, and Montana; and concurrently with my position at CCIU, I was assigned to the Baghdad CID Battalion as a Computer Crime Coordinator where I was responsible for conducting computer forensic examinations of seized computers, cellular phones, and other digital media within Iraq, Kuwait and Afghanistan.

I have been trained in computer incident response, digital evidence acquisition, LINUX and Windows Forensic Examinations by the Department of Defense Cyber Investigations Training Academy ("DCITA"). I currently possess "Department of Defense Certified Digital Forensic Examiner" and "Department of Defense Certified Digital Media Collector" certifications. In addition to my training and experience as a criminal investigator, I have also been an employee of several commercial Information Technology companies to include: a national Internet Service Provider ("ISP"), a commercial software company specializing in law enforcement and intelligence analysis products, and several defense contracting companies where I worked as a government contractor to the Federal Bureau of Investigation, as a member of the Pentagon Joint Staff, and the Washington DC Department of Corrections. I have received training from

the U.S. Army in the investigation of fraud; training from several commercial companies in computer, computer network, and database administration; and I hold a Bachelor of Science degree in Information Technology from George Mason University, an accredited state university in Virginia.

My experience as a USACIDC Special Agent has included the investigation of cases involving violent and non-violent crimes as well as the use of computers. I have received training and gained experience in interviewing and interrogation techniques, arrest procedure, search warrant applications, the execution of searches and seizures, and other criminal laws and procedures.

As a Special Agent of the USACIDC, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice (Title 10 U.S.C. Section 47) and other applicable federal and state laws where there is a U.S. Army or Department of Defense interest. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

SOURCE OF EVIDENCE

The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals – including other law enforcement officers and particularly other USACIDC Special Agents – as well as my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and

circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

RELEVANT STATUTES

Title 18, United States Code, § 793(d) makes it unlawful to make unauthorized disclosure of national defense information. Specifically, the statute provides in pertinent part that:

Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered or transmitted . . . the same to any person not entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years, or both.

Title 18, United States Code, § 1030(a) makes it unlawful to, without authorization, obtain from a United States Government computer certain national defense information, and disclose such information. Specifically, the statute provides in pertinent part that:

Whoever – (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or

causes to be communicated, delivered, or transmitted . . . the same to any person not entitled to receive it [shall be punished by a fine under this title or imprisonment for not more than ten years, or both . . .]

The national security classification levels assigned to national security information and national defense information are defined in Executive Order No. 13526 and its predecessor orders. Information may be classified if the following conditions are met: (1) an original classification authority ("OCA") is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the United States Government; (3) the information falls within one or more of the categories set forth in the Executive Order (which includes intelligence sources and methods; cryptology; military plans; and vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security of the United States); and (4) the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage. Under the Executive Order, information may be classified "Confidential" if its unauthorized disclosure reasonably could be expected to cause damage to the national security; "Secret" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security; and "Top Secret" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

BACKGROUND AND TECHNICAL INFORMATION

The term "computer" as used in this affidavit is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data

processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I am aware of the following:

- a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information.
- b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.
- c. Instant Messaging (IM) is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger, etc.) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the

structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are in the same state. Instant Messaging may also be commonly referred to as 'Internet Chat'.

d. Encryption refers to the practice of mathematically scrambling computer data typically as a communications and/or storage security measure – typically so only the intended parties can read or open the contents of a communication or electronic file. Unencrypted information is called “plaintext”, while encrypted information is called “cipher text”. “Decryption” is the process of converting the cipher text back into the original, readable plaintext format. The particular method used to encrypt or decrypt data, often used synonymously to describe the type of encryption, is an algorithm – which may also be described as a mathematical formula or finite sequence of instructions for conducting the encryption/decryption. The alpha-numeric or other values used as a basis to encrypt/decrypt a message is called the “key”, which is often generated from a user specified “password” comprised of letters, numbers, and special (punctuation) characters. Based on the algorithm and/or key length, to guess the password/key of an encrypted electronic file by attempting all possible combinations of values, in modern cryptography, even with the use of multiple and/or super-computers, may not be possible within a reasonable amount of time (hundreds or thousands of years).

e. Mac OS (Macintosh Operating System) “Keychain” is Apple Inc.'s password management system in Mac OS. It was introduced with Mac OS Version 8.6, and has been included in all subsequent versions of Mac OS, including Mac OS X. A

Keychain can contain various types of data: passwords (for Websites, FTP servers, SSH accounts, network shares, wireless networks, groupware applications, encrypted disk images), private keys, certificates and secure notes.

f. An Apple Disk Image is Apple Inc.'s proprietary electronic file/disk image format commonly used with the Mac OS X operating system. The file format allows secure password protection of the contents of the file as well as file compression, and hence serves both security and file distribution functions. Apple Disk Images typically have a ".dmg" file extension, although legacy Apple Disk Image files intended for Mac OS 9 and earlier generally have .smi or .img file extensions.

PROBABLE CAUSE FOR SEARCH

Manning's Access To Classified Information

MANNING enlisted in the United States Army on or about October 2, 2007, and currently holds the rank of Private First Class. He received training in Intelligence Analysis, and was ultimately assigned as a U.S. Army Military Occupational Specialty ("MOS") 35F – Intelligence Analyst. MANNING was granted a U.S. Government security clearance at the "Top Secret" level as part of his position within the U.S. Army. On or about October 12, 2009, MANNING was deployed with his unit, HHC, 2nd BCT, 10th Mountain Division, to Forward Operating Base ("FOB") Hammer, located approximately 40 miles east of Baghdad, Iraq, and 70 miles west of the Iran-Iraq border.

Between October 2009 and May 2010, while assigned in Iraq and working in the role of an All-Source Intelligence Analyst, MANNING was granted access to national defense information through various U.S. Army and DoD computer network systems, including: the Non-Secure Internet Protocol Router ("NIPR") network, used for the

processing of unclassified documents and unclassified communications; and the Secure Internet Protocol Router ("SIPR") network, used for the processing of classified documents and classified communications at the "Confidential" and "Secret" classification levels. MANNING also had access to a commercial, non-military, satellite-based ISP while in his living quarters on FOB Hammer, which he used with his personal laptop computer while not performing official duties. This information has been verified by statements of co-workers in MANNING's unit, by examination of various computer accounts and network log file systems, the forensic examination of computers used by MANNING, and by documents obtained during the course of this investigation.

Classified Material Published On The Internet

On February 18, 2010, the website WikiLeaks.org ("WikiLeaks") – which is self-described as "a multi-jurisdictional public service designed to protect whistle blowers, journalists and activists who have sensitive materials to communicate to the public" – published on their website a U.S. Department of State diplomatic cable originating from the U.S. Embassy in Reykjavik, Iceland, which was classified "Confidential". This diplomatic cable, dated January 13, 2010, related to diplomatic discussions on the topic "Icesave" between members of the U.S. Department of State, the British Foreign Service, and Icelandic Government personnel. Based on this classified document's publication on the WikiLeaks website, the U.S. Department of State's Diplomatic Security Service initiated an investigation on February 19, 2010, to identify the person(s) who unlawfully disclosed this document.

On April 5, 2010, at the National Press Club in Washington, D.C., the founder of WikiLeaks, an Australian citizen named Julian P. Assange, held a press conference to publicly release classified video footage of United States combat operations in Iraq.

The video footage, apparently taken by a U.S. Army AH-64 Apache attack helicopter engaged in combat in or around Baghdad, Iraq, depicts an air-strike conducted on July 12, 2007, during which two *Reuters* journalists, several suspected Iraqi insurgents, and several Iraqi civilians were killed or wounded. Assange released the original 38-minute-long version of the video as well as a shorter "production" version lasting approximately 18 minutes, titled "Collateral Murder", both of which were published on the Internet at the URL "www.collateralmurder.org". Due to the controversial and/or graphic nature of the video, this classified material received wide news media coverage. U.S. Department of Defense officials later confirmed that the video footage was genuine and was properly classified "Secret".

Manning Identified as Source of Classified U.S. Government Material

Between May 20, 2010 and May 26, 2010, MANNING began a series of Internet chat conversations with a civilian, Mr. (b)(6)(b)(7)(C) residing in Carmichael, California. Lamo is known in the computer security community as a 'computer hacker' and has been profiled extensively in the print and on-line media. MANNING and (b)(6)(b)(7)(C) discuss a range of issues related to Classified U.S. Government material over a period of approximately 6 days; wherein MANNING admits to (b)(6)(b)(7)(C) to having unlawfully disclosed U.S. Government Classified material to the website WikiLeaks.org. During these chat conversations, which MANNING and (b)(6)(b)(7)(C) encrypted so that only they could read the communications, MANNING detailed the specific items of Classified U.S. Government material he unlawfully disclosed to the WikiLeaks website as: a video and related documentation of a U.S. airstrike in Gharani, Afghanistan; the Apache airstrike video in Baghdad, Iraq which was publicly disclosed by WikiLeaks; an Iraq War Event Log believed to contain approximately 500,000 records; the "Gitmo Papers" relating to

terror suspect detainees being held in Guantanamo Bay, Cuba; and a U.S. Department of State database containing approximately 260,000 Classified U.S. State Department internal communications, to include the Classified cable related to the topic of "Icesave" also disclosed by WikiLeaks.

(b)(6)(b)(7)(C) subsequently notified law enforcement of these chat conversations which lead to USACIDC Special Agents in Iraq apprehending MANNING on FOB Hammer on May 27, 2010. Upon MANNING's apprehension by USACIDC, MANNING invoked his legal right to counsel and declined to make any statements in relation his involvement in the unlawful disclosure of Classified U.S. Government materials. MANNING has further been held in confinement since May 27, 2010, pending a Military Courts-Martial.

At the time of MANNING's apprehension in Iraq, USACIDC Special Agents seized numerous U.S. Government and personal computers associated with MANNING on FOB Hammer, per a Military Magistrate Search Authorization. The U.S. Government computers collected as evidence included: several SIPR computers MANNING was identified as having been assigned while working in his position as an Intelligence Analyst in Iraq; several NIPR computers other personnel in MANNING's unit, to include MANNING, would have shared for work-related duties; and several personally owned computers, to include MANNING's personal laptop computer and other items of digital media as well as those from other personnel in MANNING's unit. Of the other items of digital media seized from MANNING's personal living quarters under a Military Magistrate Search Authorization issued in Iraq, was an optical disc containing a version of the classified Video publicly released by WikiLeaks on April 5, 2010.

Subsequent computer forensic examination of MANNING's assigned U.S.

Government and personal computers by personnel assigned to CCIU, revealed evidence MANNING had unlawfully accessed and/or unlawfully possessed the Classified U.S. Government materials he claimed in his Internet chats with (b)(6)(b)(7)(C). Further forensic examination revealed MANNING may have used his personal laptop computer and non-military, satellite-based ISP Internet connection to transmit classified documents directly or indirectly to WikiLeaks.

In addition to the aforementioned evidence found on MANNING's personal laptop computer hard drive, was the Mac OS "Keychain" containing encrypted passwords related to MANNING's various accounts, as well as an encrypted file named "strongbox.dmg", which is approximately 1.5 GB in size. While CCIU forensic examiners were able to decrypt the Keychain containing numerous passwords used by MANNING for his internet, email, and other related accounts, the contents of the file "strongbox.dmg" is still presently unknown due to this file being encrypted and investigators not knowing the password to decrypt this file. It is believed this file may contain additional evidence, fruits or instrumentalities of MANNING's disclosure of Classified U.S. Government material.

Package(s) Sent by MANNING from Iraq

Based on various interviews of MANNING's unit members and/or roommate he shared his personal living quarters with at FOB Iraq, conflicting information was developed as to whether MANNING may have sent one or more packages during April 2010, to person(s) unknown. As a result of this information, the Eagle Cash Card records pertaining to MANNING's account were obtained by USACIDC Special Agents which disclosed MANNING appears to have shipped mail/package(s) from the FOB

Hammer, Iraq, APO AE 09308 Post Office on 21 Apr 10, and the transaction amount was \$13.50. Unfortunately, due to the time that had passed between MANNING's postal transaction and his apprehension, the FOB Hammer Post Office had already destroyed their copies of any receipts and/or customs forms related to this transaction.

It was later determined that when USACIDC Special Agents in Iraq conducted a search of MANNING's personal living quarters on FOB Hammer, per a Military Magistrate Search Authorization, the aforementioned optical disc containing the Classified U.S. Government Video has been found in an opened and unmailed postal service type box – which appeared to potentially have been readied for mailing.

During forensic examinations of MANNING's personal computer it was also noted that MANNING, in chat conversations, expressed frustration in regard to the time to upload files using his non-Military, satellite-based ISP while in Iraq; which was slow due to technical issues with this type of connection. Subsequently, it is unknown whether MANNING may have mailed digital media containing Classified U.S. Government material to personnel associated with the website WikiLeaks or to other person(s) which may have indirectly provided this information to WikiLeaks.

Additional Disclosure of Classified Materials by the Website WikiLeaks

On July 25, 2010, the WikiLeaks website in coordination with The New York Times, The Guardian (a news media publication based in London, England) and Der Spiegel Magazine (a news media publication based in Germany) published approximately 75,000 classified U.S. Government documents relating to the War in Afghanistan. According to an on-line article posted on The New York Times website on July 25, 2010:

"The articles published today are based on thousands of United States military incident and intelligence reports — records of engagements, mishaps, intelligence on enemy activity and other events from the war in Afghanistan — that were made public on Sunday on the Internet. The New York Times, The Guardian newspaper in London, and the German magazine Der Spiegel were given access to the material several weeks ago. These reports are used by desk officers in the Pentagon and troops in the field when they make operational plans and prepare briefings on the situation in the war zone..."

Further, regarding the source of the material The New York Times article relates:

"The documents — some 92,000 individual reports in all — were made available to The Times and the European news organizations by WikiLeaks, an organization devoted to exposing secrets of all kinds, on the condition that the papers not report on the data until July 25, when WikiLeaks said it intended to post the material on the Internet. WikiLeaks did not reveal where it obtained the material."

While the information reported by The New York Times identifies approximately 92,000 reports being disclosed, about 15,000 reports were not published by either the website WikiLeaks or the mentioned news media organizations due to this material believed to contain information more sensitive than in the published material. The New York Times article suggests information even more sensitive than the published Classified U.S. Government materials were obtained from WikiLeaks as the article further relates:

"We have, for example, withheld any names of operatives in the field and informants cited in the reports. We have avoided anything that might compromise American or allied intelligence-gathering methods such as communications intercepts."

The WikiLeaks website in regard to the 15,000 unpublished Classified U.S. Government documents published on its website:

"We have delayed the release of some 15,000 reports from

the total archive as part of a harm minimization process demanded by our source. After further review, these reports will be released, with occasional redactions, and eventually in full, as the security situation in Afghanistan permits."

Personnel associated with the website WikiLeaks have publicly acknowledged having other Classified U.S. Government material (which are believed to have been unlawfully disclosed by MANNING) such as the Gharani, Afghanistan airstrike video and associated report; however, for reasons unknown WikiLeaks has not published this material to the public.

MANNING's Personal Belongings Provided to Military Intelligence

During a subsequent parallel investigation conducted by Military Intelligence ("MI") personnel in Iraq into MANNING's activities in the unlawful disclosure of Classified U.S. Government material; MI Special Agents conducted interviews at FOB Hammer of personnel assigned to MANNING's unit. Prior to these MI personnel departing FOB Hammer for their assigned base in Iraq, personnel from MANNING's unit provided the MI Special Agents with a box containing MANNING's personal belongings which had been collected by unit personnel from MANNING's living quarters. MI Special Agents reportedly did not fully know and/or recognize what this property was until returning to their assigned office on another base within Iraq. Upon identifying the nature of this property, MI Special Agents transported these belongings to the local CID Office at Camp Liberty, Iraq; wherein the box containing MANNING's personal belongings was sealed and collected as evidence, pending the appropriate legal authority to search through the box.

Although this investigation was initially opened by the Camp Liberty CID Office, the investigation was later transferred to the WMRA, CCIU for further investigation and completion due to the technical nature of the offenses under investigation. Subsequently, the sealed container of MANNING's personal belongings was sent to the CCIU, 9805 Lowen Road, Building 193, Fort Belvoir, Virginia, via U.S. Registered Mail. This sealed container has remained in the CCIU Evidence Depository since its arrival from Iraq.

Conclusion

At the time of MANNING's apprehension on May 27, 2010, the nature and full scope of his activities in regard the unlawful disclosure of Classified U.S. Government material was not fully known. Consequently, when USACIDC Special Agents initially searched the personal living quarters of MANNING under the authority of a Military Magistrate Search Authorization, although they were able to identify obvious digital media evidence which were collected (MANNING's personal computer and optical discs found in MANNING's quarters) other items which may not have appeared to have evidentiary value at the time (books, papers, notebooks, etc.) – potentially containing passwords used by MANNING, postal receipts related to mail or packages sent by MANNING, and/or other evidence – may have been inadvertently missed. Consequently, unit personnel from MANNING's unit provided all of these personal belongings from MANNING's personal living quarters to MI Investigators which were subsequently transferred to USACIDC upon the discovery of the nature of these items.

In my training and experience as a Special Agent assigned to conduct

investigations of criminal matters involving computer and internet based systems, as well as my personal experience, I have found passwords created by computer users, both beginner and expert, are very often not combination of random characters or numbers, which may be difficult to remember; but are typically words, numbers and/or phrases which have some personal connection or meaning to the computer user creating them. Computer users will typically create passwords which contain: full or partial family member or acquaintance names; personal initials; birth dates, anniversary dates and other important dates; portions of social security, telephone, or other identifying numbers; names of places the user has traveled or lived; names of pets; characters, locations and events from books or movies; passages from religious materials; slang terms from the user's identified hobbies, social life, or communities they are involved in; as well as other favored or significant elements from the computer user's life. Further, when users do create seemingly random passwords, they may habitually use these same passwords on multiple websites, internal files, and other systems requiring passwords – out of familiarity and the ability to easily recall these previously used passwords. When users are required by certain systems to periodically change their passwords, typical computer users will often maintain the 'main body' of their original password by adding or changing one or two numbers or characters which comprise the remainder of the password – and in some cases revert back to passwords used in the past when prompted for successive password changes.

An analysis of the passwords which were discovered from decrypting the Mac OS Keychain on MANNING's personal laptop, further reinforce the above mentioned statements related to user passwords. Specifically, these passwords contained: terms

related to MANNING's personal life; terms related to places MANNING had visited recently; numbers from books MANNING is believed to have been owned and read, which had been recovered from another source of MANNING's belongings; and/or were passwords previously believed to have been used by MANNING on other computer based systems. Because USACIDC Special Agents have already obtained access to email accounts and other related computer network storage space known to have been used by MANNING, which did not reveal any identifiable passwords; that the passwords found on the Mac OS Keychain contained on MANNING's personal laptop computer did not contain the "strongbox.dmg" password; and MANNING is known to have made comments to the effect that his passwords are complicated and would be difficult to guess – it is believe MANNING may have written down any passwords he used, or that other writings or material contained in the box of his personal belongings may be able to provide investigators and/or personnel supporting this investigation information that will allow the password to be determined. Further, the identification of this password and subsequent decryption of the "strongbox.dmg" file, will allow investigators to understand the full scope of MANNING's activities.

In addition to information related to passwords, the box of personal belongings may also contain receipts, customs forms, and/or other documentation related to packages and/or mail sent by MANNING, which may further identify other personnel and/or addresses which may have been involved in the unlawful disclosure of Classified U.S. Government materials – and again, provide investigators information to identify the full scope of MANNING's activities.

Given the facts and circumstances of the incidents related to the unlawful disclosure of Classified U.S. Government material by MANNING; the identification of Classified U.S. Government materials on MANNING's personal computer; the identification MANNING may have mailed digital media to person(s) unknown directly or indirectly related to the website WikiLeaks; that MANNING is known to have used electronic file-based encryption to conceal the contents of files found on his personal computer; and that data, writings, information and/or evidence related to all of these aspects of this case could reasonably exist in the personal belongings of MANNING - there is probable cause to believe that additional evidence, fruits and instrumentalities of the offenses believed to have committed by MANNING to include violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information) are contained in the sealed container collected as evidence and presently securely stored within the Evidence Depository, CCIU, located at 9805 Lowen Road, Building 193, Fort Belvoir, Virginia - and described in more detail in Attachment C.

ATTACHMENT B

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The following locations are to be searched as explained in Attachment A and located within the Evidence Depository, CCIU, 9805 Lowen Road, Building 193, Fort Belvoir, Virginia, are described as follows:

The sealed container, described as: a brown cardboard box, measuring approximately 12 inches by 10 inches by 5 ½ inches, and sealed with green, 2-inch adhesive (military 100-mile-and-hour) tape along all box seals, containing the personal belongings of MANNING – which is further referred to in Attachment A, as the "Sealed Container".

ATTACHMENT C

ITEMS TO BE SEIZED AND SEARCHED

Special Agents of USACIDC or other Army law enforcement personnel assisting USACIDC are to search the Sealed Container, containing the personal belongings of MANNING, as described in Attachment B, and therein to are seize and subsequently further search all papers, documents, notes, forms, files, receipts, notebooks and/or other written or printed materials; as well as any digital media which may have been inadvertently overlooked, previously hidden or otherwise been not before identified – which are associated with or previously used by Private First Class (PFC) Bradley Edward MANNING, formerly assigned to HHC, 2nd BCT, 10th Mountain Division – specifically as it relates to information, documents, and data, both classified and unclassified; as well as addresses, phone numbers, names, postal tracking numbers or information, as mentioned in Attachment A, which is herein incorporated into Attachment C – in regard to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information).

Computer Hardware and Digital Media is further described as any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data processing hardware (such as "desktop computers" and self-contained "laptop", "notebook", or "netbook" computers, as well as "Smart Phones" and internet capable PDAs); internal and peripheral storage devices

(such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical disc storage devices such as CDs or DVDs, USB drives, flash memory cards or similar solid-state storage media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

FURTHER SEARCH OF SEIZED COMPUTERS AND DIGITAL MEDIA ITEMS

The items seized as part of this Search Authorization, which should consist of papers, documents, forms, receipts, notebooks, letters, and other paper-like materials; will have will have digital photographs exposed of these items to document their value as evidence. Any items found which are considered digital media, such as computers, hard disk drives, and/or other digital media, will have forensically sound images (digital copies) produced of the seized items as appropriate, which will in turn be searched in lieu of the original seized items as part of a digital media/computer forensic examination. The search of digital copies of the items seized is done to ensure and preserve the forensic integrity of the seized items for additional and/or future examination(s) in accordance with criminal procedure and rules of evidence. These examination(s) of seized items will be conducted by personnel assigned to the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit

(CCIU) who are certified by the Department of Defense and/or Department of the Army to conduct such types of examinations. These personnel will use computer forensic hardware and/or software, which has been approved for use in conducting such examinations. Consequently, this search/examination activity will be completed within facilities operated by the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) and completed as expeditiously as possible. All of the above items found to be contained inside the Sealed Container, will further be retained in accordance with Army Regulation 195-5, "Evidence Procedures".

Exhibit(s) 209 thru 222

Page(s) 001438 and 001477 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

Exhibit(s) 223

Page(s) 001478 thru 001484

Documents

SEALED

by the

U.S. District Court
for the Eastern District of New York

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Between 1100 and 1600, 25 Sep 10, SA (b)(6)(b)(7)(C) reported to the Brig, MCB Quantico, and facilitated the recording of conversations between PFC MANNING and his visitor(s) on that date. The only visitor was Ms. (b)(6)(b)(7)(C) PFC MANNING's (b)(6)(b)(7)(C)

About 1008, 27 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one (1) compact disc (CD) containing the 25 Sep 10 recording of PFC MANNING and Ms. (b)(6)(b)(7)(C) on Evidence/Property Custody Document (EPCD), Document number (DN) 144-10.

////////////////////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIC (b)(6)(b)(7)(C)

DATE

27 Sep 10

EXHIBIT

224

CID FORM 51
1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001485
Approved

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1210, 29 Sep 10, SA (b)(6)(b)(7)(C) received the results of the Department of Defense Inspector General (DOD/IG) Subpoena 2010233-10433, served on the custodian of records at Yahoo, Inc, for subscriber information regarding the email account bradass87@yahoo.com. Yahoo provided the following results:

Internal reference number: 155642

The account "bradass87@yahoo.com" was created on Wednesday, 19 Oct 2005 at 23:26:43 GMT.

Name: Mr. Bradley Manning

Address: (no street name given), Oklahoma City, OK 73162

IP address at registration: 68.12.179.192 (This IP address was registered to Cox Communications, 1400 Lake Hearn Dr., Atlanta, GA 30319)

Secondary email address: bradley.manning@cheesy-design.com (The domain cheesy-design.com was no longer valid).

Yahoo's logs showed no logins to the account within the last 90 days. See report from Yahoo.com for additional information. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION Washington Metro Resident Agency
Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

SA (b)(6)(b)(7)(C)

DATE

29 SEP 10

EXHIBIT

225

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001486

Approved

(b)(6)(b)(7)(C)

Exhibit 226

Page(s) 001487 thru 001492 referred to:

Department of Defense
Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 4 PAGES

DETAILS

About 0950, 29 Sep 10, SA (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) Digital Forensic Examiner, Digital Forensic and Research Branch, CCIU, coordinated with CPT (b)(6)(b)(7)(C) Brigade Automation Officer, S-6, Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (2nd BCT), 10th Mountain Division (10th Mtn Div), Fort Drum, NY 13602 (FDNY), to setup the servers needed to constitute the T-Drive which the unit had used while deployed to Iraq. SA (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) observed as 2nd BCT S-6 personnel (CPT (b)(6)(b)(7)(C) SGT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C); and WO1 (b)(6)(b)(7)(C) Signal Support Systems Technician, attempted to make the T-Drive functional. CPT (b)(6)(b)(7)(C) related the T-Drive consisted of three NetApp devices, two of which were the NetApp devices (labeled as T-Drive) previously collected on Evidence/Property Custody Documents (EPCD), Document Number (DN) 131-10 and 133-10. 2nd BCT personnel connected a third NetApp device which had no label to the other two devices and booted the three devices. They accessed the devices via console connected to a 2nd BCT laptop and via web interface and determined the volume was not complete. Upon opening transport cases with other servers enclosed, 2nd BCT personnel discovered another NetApp device which was also labeled T-Drive on the front. 2nd BCT personnel shut down the three NetApp devices, disconnected the device that was not labeled T-Drive, and connected the NetApp device they removed from the transport case which was labeled T-Drive. They booted the three devices and were able to verify through web interface that the file structure was complete. They were, however, unable to browse files on the device, as it was configured to only allow file access through domain controller authentication. A domain controller previously used on the same network as the T-Drive was connected to a switch with the T-Drive and a laptop. 2nd BCT personnel were still unable to access files on the T-Drive.

Between 1723 and 1743, 29 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence four servers, consisting of one DS14 MK4, NetApp brand, S/N: 30000442, purportedly the third chassis comprising the T-Drive; two Sunfire X4100, Sun Microsystems brand, S/N: 0733BD20EC and 0732BD1FEC, purportedly SIPR domain controllers; and one PowerEdge 2850, Dell brand, S/N: HBHLJ81, purportedly a SIPR domain controller, all from WO1 (b)(6)(b)(7)(C) which was documented on EPCD, DN 145-10.

About 1446, 30 Sep 10, SA (b)(6)(b)(7)(C) collected as evidence one Sunfire X4100 server, Sun Microsystems brand, S/N: 0732BD1FE0, purportedly used as a NIPR domain controller for 2nd BCT, 10th MTN DIV, FDNY, from WO1 (b)(6)(b)(7)(C) which was documented on EPCD, DN 146-10.

About 1720, 30 Sep 10, SA (b)(6)(b)(7)(C) received a signed Search Authorization, authorizing the search of hard drives contained within a plastic container belonging to 2nd BCT, from SA (b)(6)(b)(7)(C) this office, which he was sworn to by CPT (b)(6)(b)(7)(C) Military Magistrate, Fort Belvoir, VA.

Between 1014 and 1059, 1 Oct 10, SA (b)(6)(b)(7)(C) reviewed the contents of the following hard drives, property of 2nd BCT, 10th MTN DIV, FDNY, for the presence of a user profile pertaining PFC MANNING by connecting a write blocker to a stand-alone laptop computer, all of which met with negative results:

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b)(7)(E)		ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 1 Oct 10	EXHIBIT 227	

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001493

Approved _____

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 4 PAGES

DETAILS

Make	Model	Serial Number	Classification	Start Time	End Time	Results
Fujitsu	MHV2060AH	NT25T5B2PRF5	Unclassified	1014	1015	Negative
Unknown	IC25N020ATCS04-0	D9HUN9ZB	Unclassified	1017	1019	Negative
Fujitsu	MHV2060AH	NT25T612UFRK	Unmarked	1020	1022	Negative
Fujitsu	Unknown	NT25T612UMCL	Unclassified	1025	1027	Negative
Seagate	Momentus 40GB	3KW031ZM	Unclassified	1028	1029	Negative
Hitachi	Travelstar 60GB	K3GY7V2H	Unmarked	1031	1032	Negative
Seagate	Momentus 80 GB	3MH04H0G	Unmarked	1034	1036	Negative
Fujitsu	MHV2060AH	NT25T612UG22	Unmarked	1038	1039	Negative
Fujitsu	MHV2060AH	NT25T612UPU6	Unmarked	1041	1042	Negative
Fujitsu	MHV2060AH	NT25T582H023	Unmarked	1043	1045	Negative
Hitachi	DK23EA-40	MCE55A8L9862	Unmarked	1047	1048	Negative
Hitachi	DK23EA-40	MCE55A8M0110	Unmarked	1051	1053	Dead
Hitachi	DK23EA-40	MCE55A7S7388	Unmarked	1058	1059	Negative

Between 1014 and 1059, 1 Oct 10, Mr. (b)(6)(b)(7)(C) previewed the contents of the following hard drives for the presence of a user profile pertaining PFC MANNING by connecting a write blocker to a stand-alone laptop computer, all of which met with negative results:

Make	Model	Serial Number	Classification	Start Time	End Time	Results
Seagate	ST94Q11A	3KW91ZRY	Secret	1145	1152	Negative
Seagate	ST94Q11A	3KW91RQ5	Secret	1150	1151	Negative
IBM	Unknown	DMHYA6XB	Secret	1152	1153	Negative
Fujitsu	MHT2040AH	NP0ET4C39AWL	Secret	1154	1155	Negative
Unknown	Unknown	K36Y94YP	Secret	1203	1205	Negative
Unknown	Unknown	17M51533	Secret	1205	1206	Negative
IBM	Unknown	170J0745	Secret	1206	1207	Dead
IBM	Unknown	170E1835	Secret	1210	1211	Negative

About 1315, 1 Oct 10, SA (b)(6)(b)(7)(C) coordinated with MSG (b)(6)(b)(7)(C) S-2 NCOIC, HHC, 2nd BCT, 10th Mtn Div, FDNY, who identified a hard drive that was previously scanned by agents on 10 Sep 10, as a hard drive he believed PFC MANNING utilized to complete a tasking he had provided PFC MANNING. MSG (b)(6)(b)(7)(C) related the tasking was to complete a functional database of incident reports. The hard drive was used in a computer which was not connected to the SIPR network, and PFC MANNING would have subsequently used an administrative logon rather than his personal logon. MSG (b)(6)(b)(7)(C) further related that prior to deployment, PFC MANNING had SIPR access; however, he was uncertain if he had his own logon or used a general logon. He further related that he believed PFC MANNING had access to Intellilink and the 3rd BCT, 82nd Airborne DIV, Fort Bragg, NC, web database, as he was tasked with gathering information about Iraq prior to the deployment. 3rd BCT, 82nd Airborne DIV, was the unit in Iraq that 2nd BCT, 10th Mtn Div replaced. MSG (b)(6)(b)(7)(C) related that CW2 (b)(6)(b)(7)(C)

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b)(7)(E)		ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)		DATE 1 Oct 10	EXHIBIT 227

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001494

Approved

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 3 OF 4 PAGES

DETAILS

(b)(6)(b)(7)(C) Fusion OIC, S-2, HHC, 2nd BCT, 10th Mtn Div, FDNY, may have further information pertaining to PFC MANNING's access prior to deployment.

About 1345, 1 Oct 10, SA (b)(6)(b)(7)(C) interviewed CW2 (b)(6)(b)(7)(C) who provided a sworn statement wherein he detailed his knowledge of PFC MANNING's SIPR access prior to deployment and his interaction with PFC MANNING during the deployment. CW2 (b)(6)(b)(7)(C) related that PFC MANNING was assigned to conduct an Iraq country study prior to deployment.

Further, CW2 (b)(6)(b)(7)(C) detailed an instance wherein PFC MANNING stated the U.S. Flag meant nothing to him and he had no loyalties to the U.S. (See Sworn Statement.)

About 1600, 1 Oct 10, SA (b)(6)(b)(7)(C) coordinated with MSG (b)(6)(b)(7)(C) who related that the S-2 had completed going through all of their shipping containers and he could not foresee the unit finding any more hard drives that PFC MANNING may have had access to. MSG (b)(6)(b)(7)(C) went through the drives with SA (b)(6)(b)(7)(C) to determine which drives PFC MANNING definitely would not have had access to. MSG (b)(6)(b)(7)(C) was able to narrow down the number of possible drives to about 30. SA (b)(6)(b)(7)(C) also provided MSG (b)(6)(b)(7)(C) a copy of the search authorization pertaining to the drives that were searched earlier that day.

About 1945, 1 Oct 10, SA (b)(6)(b)(7)(C) met with CPT (b)(6)(b)(7)(C) Military Magistrate, FDNY, and briefed him on the aspects of this investigation. SA (b)(6)(b)(7)(C) provided a draft affidavit, attachments and search authorization.

About 2020, 1 Oct 10, SA (b)(6)(b)(7)(C) received the signed search authorization from CPT (b)(6)(b)(7)(C) authorizing the search of the remaining drives in the 2nd BCT Sensitive Compartmented Information Facility, FDNY.

Between 2244 and 2325, 1 Oct 10, SA (b)(6)(b)(7)(C) previewed the contents of the following hard drives for the presence of a user profile pertaining PFC MANNING by connecting a write blocker to a stand-alone laptop computer with its hard drive removed and booted with a boot disc, all of which met with negative results:

Make	Model	Serial Number	Classification	Start Time	End Time	Results
Unknown	IC25N060ATMR04-0	K3GS5T0H	Secret	2244	2245	Negative
Toshiba	MK4025GAS	Z5FX1427S	Secret	2248	2249	Negative
Unknown	IC25N060ATMR04-0	K3GVGAYK	Secret	2250	2255	Negative
Fujitsu	MHV2080AH	NT9AT63281DY	Unmarked	2257	2258	Negative
Hitachi	Travelstar	K3GYXTJH	Secret	2302	2303	Negative
Hitachi	DK23EA-40	MCE65APG8189	Secret	2305	2307	Negative
Hitachi	Travelstar	MCE55AN84638	Secret	2308	2309	Negative
Unknown	IC25N060ATMR04-0	K3HLNLSH	Secret	2310	2311	Negative
Hitachi	Travelstar	K3HA9WHH	Secret	2313	2316	Negative
Unknown	IC25N060ATMR04-0	KCJ3TKNH	Secret	2318	2319	Negative

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro Resident Agency
Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

1 Oct 10

EXHIBIT

227

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001495

Approved

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 4 OF 4 PAGES

DETAILS

Unknown	DK23EA-60	MCE5JAMG4246	Secret	2321	2323	Negative
Seagate	Momentum	3MH14K29	Secret	2324	2325	Negative

Between 2244 and 2325, 1 Oct 10, Mr. (b)(6)(b)(7)(C) previewed the contents of the following hard drives for the presence of a user profile pertaining PFC MANNING by connecting a write blocker to a stand-alone laptop computer with its hard drive removed and booted with a boot disc, all of which met with negative results:

Make	Model	Serial Number	Classification	Start Time	End Time	Results
Seagate	Unknown	3MH14K6C	Secret	2244	2246	Negative
Seagate	Unknown	5MH0WIJT	Secret	2245	2246	Negative
Seagate	Unknown	5MH0HQ48	Secret	2248	2249	Negative
Seagate	Unknown	5MH0ASJ6	Secret	2250	2251	Negative
Seagate	Unknown	5MH0NX7V	Secret	2251	2252	Negative
Hitachi	HT37210G9A00	MPCZN7Y0J9JMRL	Secret	2255	2259	Positive
Unknown	Unknown	5MH09QEE	Secret	2300	2301	Negative
Seagate	ST980811AS	5L8VJXF	Secret	2302	2303	Negative
Seagate	ST910021AS	5MH0SNGX	Secret	2303	2304	Negative
Seagate	Unknown	3MH15676	Secret	2307	2308	Negative
Seagate	ST980811	5LY8T8Q9	Secret	2309	2310	Negative
Toshiba	MK1251GSY	489FT0ULT	Secret	2314	2315	Negative
Unknown	Unknown	070714DP1000DGG08K6G	Secret	2317	2320	Positive
Seagate	ST9160823AS6	5NK16120	Secret	2321	2322	Negative
Hitachi	Unknown	Unknown	Secret	2323	2324	Negative
Hitachi	Unknown	Unknown	Secret	2324	2325	Negative
Hitachi	DK23EA-60	Unknown	Secret	2330	2335	Negative
Hitachi	IC25N060ATMR04	K3GBZUW1T	Secret	2335	2336	Negative
Seagate	Unknown	Unknown	Secret	2332	2338	Negative
Unknown	Unknown	Unknown	Secret	2339	2345	Negative
Unknown	08K0634	K36MZL2P	Secret	2350	2355	Dead

Between 2338 and 2345, 1 Oct 10, SA (b)(6)(b)(7)(C) collected as evidence three hard disk drives, consisting of one unknown capacity, Hitachi brand, S/N: K3HBYJDH, purportedly used by PFC MANNING under an administrative profile; one 160GB, Hitachi brand, S/N: 070714DP1D00DGG08K6G, purportedly containing a Bradley MANNING profile; and one 100GB, Hitachi brand, S/N: MPCZN7Y0J9JMRL, purportedly containing a Bradley MANNING profile, all from MSG (b)(6)(b)(7)(C) which was documented on EPCD, DN 147-10.

////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b)(7)(E)		ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 1 Oct 10	EXHIBIT 227	

SEARCH AND SEIZURE AUTHORIZATION

For use of this form, see AR 27-10; the proponent agency is OTJAG

TO: (Name and Organization of the person to whom authorization is given)

Special Agent (b)(6)(b)(7)(C) of the United States Army Criminal Investigation Command (USACIDC)

(An affidavit) (A (sworn) or (unsworn) oral statement) having been made before me by

Special Agent (b)(6)(b)(7)(C)

(Name of Affiant)

Washington Metro Resident Agency, Computer Crime Investigative Unit (CCIU), USACIDC, Fort Belvoir, Virginia 22060

(Organization or Address of Affiant)

(which affidavit is attached hereto and made a part of this authorization), and as I am satisfied that there is probable cause to believe that the matters mentioned in the affidavit are true and correct, that the offense set forth therein has been committed, and that the property to be seized is located (on the person) (at the place) to be searched, you are hereby ordered to search the (person) (place) known as

Plastic Container containing U.S. Government digital media, at 10200 N. Riva Ridge Loop, Fort Drum, New York

for the property described as U.S. Government computers, hard disk drives, and/or digital media, the property of HHC, 2nd Brigade

Combat Team, 10th Mountain Division, Fort Drum, New York, containing information or data related to the use of computers/

digital media by PFC MANNING and access to and/or disclosure of Classified U.S. Government Material (See Attachment C).

bringing this order to the attention of the (person searched) (person in possession, if any person be found at the place or on the premises searched). The search will be made in the (daytime) (nighttime), and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to:

Evidence Custodian, Computer Crime Investigative Unit (CCIU), 9805 Lowen Road, Bldg 193, Fort Belvoir, Virginia

(Name and Organization of Authorized Custodian)

and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 30 day of September, 2010

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL

(b)(6)(b)(7)(C)

CPT, JA

DUTY POSITION OF AUTHORIZING OFFICIAL

MILITARY MAGISTRATE

ORGANIZATION OF AUTHORIZING OFFICIAL

OSJA FORT BELVOIR, VA

SIGNATURE OF AUTHORIZING OFFICIAL

(b)(6)(b)(7)(C)

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

For use of this form, see AR 27-10; the proponent agency is OTJAG.

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

1. I, Special Agent (b)(6)(b)(7)(C), Washington Metro Resident Agency
(Name) (Organization or Address)

Computer Crime Investigative Unit (CCIU), USACIDC, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060

having been duly sworn, on oath depose and state that:

SEE ATTACHMENT A.

2. The affiant further states that:

SEE ATTACHMENT A.

3. In view of the foregoing, the affiant requests that an authorization be issued for a search of

SEE ATTACHMENT B

(the person) (and)

(the quarters or billets) (and)

SEE ATTACHMENT C

(the automobile) (

and (seizure) (apprehension) of

(items/persons searched for)

TYPED NAME AND ORGANIZATION OF AFFIANT

Special Agent (b)(6)(b)(7)(C)
Washington Metro Resident Agency
Computer Crime Investigative Unit (CCIU), USACIDC

(b)(6)(b)(7)(C)

SWORN TO AND SUBSCRIBED BEFORE ME THIS 30th DAY OF September 2010 AT 1704

TYPED NAME, ORGANIZATION AND OFFICIAL CAPACITY OF AUTHORITY
ADMINISTERING THE OATH

(b)(6)(b)(7)(C)

CPT, JA/ OSJA FORT BELVOIR, VA
MILITARY MAGISTRATE

SIGNATURE OF AUTHORITY ADMINISTERING THE OATH

(b)(6)(b)(7)(C)

INSTRUCTIONS FOR

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it has been committed. Use additional page if necessary.

2. In paragraph 2, set forth facts establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraphs 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she has plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary.

3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under certain circumstances for evidentiary matters.

ATTACHMENT A

INTRODUCTION

I make this affidavit in support of an application for a Military Magistrate Search Authorization for electronic data, computer hardware, and physical evidence relating to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information). As set forth herein, there is probable cause to believe within a plastic portable 'Pelican' brand shipping container, the property of the U.S. Government, and assigned to Headquarters and Headquarters Company ("HHC"), 2nd Brigade Combat Team ("BCT"), 10th Mountain Division, Fort Drum, New York ("Fort Drum"), presently located within the Headquarters Building of the 2nd BCT, 10th Mountain Division at 10200 North Riva Ridge Loop, Fort Drum, New York; contain evidence, fruits, and/or instrumentalities of the offenses committed by Private First Class (PFC) Bradley Edward MANNING ("MANNING") formerly assigned to HHC, 2nd BCT, 10th Mountain Division, as further described in this affidavit.

AGENT BACKGROUND

I am a Special Agent in the United States Army Criminal Investigation Command ("USACIDC") and have been so for approximately eight years. I am currently assigned to the USACIDC, Washington Metro Resident Agency, of the Computer Crime Investigative Unit ("CCIU"), located at Fort Belvoir, Virginia; where I am responsible for the investigation of, among other things, violations pertaining to computer intrusions, denial of service attacks, and other types of malicious computer activity directed against

U.S. Army and/or Department of Defense computer networks anywhere in the world. Prior to my assignment at CCIU, I was assigned as a Special Agent with USACIDC in: South Korea, where I was responsible for conducting felony investigations impacting the U.S. Army in South Korea; Fort Lewis, Washington, where I was responsible for conducting felony investigations impacting the U.S. Army in the states of Washington, Oregon, Idaho, and Montana; and concurrently with my position at CCIU, I was assigned to the Baghdad CID Battalion as a Computer Crime Coordinator where I was responsible for conducting computer forensic examinations of seized computers, cellular phones, and other digital media within Iraq, Kuwait and Afghanistan.

I have been trained in computer incident response, digital evidence acquisition, LINUX and Windows Forensic Examinations by the Department of Defense Cyber Investigations Training Academy ("DCITA"). I currently possess "Department of Defense Certified Digital Forensic Examiner" and "Department of Defense Certified Digital Media Collector" certifications. In addition to my training and experience as a criminal investigator, I have also been an employee of several commercial Information Technology companies to include: a national Internet Service Provider ("ISP"), a commercial software company specializing in law enforcement and intelligence analysis products, and several defense contracting companies where I worked as a government contractor to the Federal Bureau of Investigation, as a member of the Pentagon Joint Staff, and the Washington DC Department of Corrections. I have received training from the U.S. Army in the investigation of fraud; training from several commercial companies in computer, computer network, and database administration; and I hold a Bachelor of

Science degree in Information Technology from George Mason University, an accredited state university in Virginia.

My experience as a USACIDC Special Agent has included the investigation of cases involving violent and non-violent crimes as well as the use of computers. I have received training and gained experience in interviewing and interrogation techniques, arrest procedure, search warrant applications, the execution of searches and seizures, and other criminal laws and procedures.

As a Special Agent of the USACIDC, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice (Title 10 U.S.C. Section 47) and other applicable federal and state laws where there is a U.S. Army or Department of Defense interest. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

SOURCE OF EVIDENCE

The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals – including other law enforcement officers and particularly other USACIDC Special Agents – as well as my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing

probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

RELEVANT STATUTES

Title 18, United States Code, § 793(d) makes it unlawful to make unauthorized disclosure of national defense information. Specifically, the statute provides in pertinent part that:

Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered or transmitted . . . the same to any person not entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years, or both.

Title 18, United States Code, § 1030(a) makes it unlawful to, without authorization, obtain from a United States Government computer certain national defense information, and disclose such information. Specifically, the statute provides in pertinent part that:

Whoever – (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted . . . the same to any person not entitled to receive it [shall be punished by a fine under this title or imprisonment for not more than ten years, or both . . .]

The national security classification levels assigned to national security information and national defense information are defined in Executive Order No. 13526 and its predecessor orders. Information may be classified if the following conditions are met: (1) an original classification authority ("OCA") is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the United States Government; (3) the information falls within one or more of the categories set forth in the Executive Order (which includes intelligence sources and methods; cryptology; military plans; and vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security of the United States); and (4) the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage. Under the Executive Order, information may be classified "Confidential" if its unauthorized disclosure reasonably could be expected to cause damage to the national security; "Secret" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security; and "Top Secret" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

BACKGROUND AND TECHNICAL INFORMATION

The term "computer" as used in this affidavit is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in

conjunction with such device.

I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I am aware of the following:

a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information.

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

c. Instant Messaging (IM) is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger, etc.) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are

in the same state. Instant Messaging may also be commonly referred to as 'Internet Chat'.

d. The Windows User Profile is created the first time the user interactively logs-on at the computer on computers running current Microsoft Windows Operating Systems. A user profile defines customized desktop environments, such as individual display, network and printer connections settings, Favorites, Cookies and History, Start Menu, Desktop, Application Data, as well as forms the basis of a container for a user to place user created files and folders. Typically the contents of a User Profile are inaccessible by other users who do not have elevated or administrator level rights on the computer system. Consequently information related specifically to that user, such as their activities on a particular computer or network can be determined from examination of data and information contained in or related to the User's Profile.

PROBABLE CAUSE FOR SEARCH

Manning's Access To Classified Information

MANNING enlisted in the United States Army on or about October 2, 2007, and currently holds the rank of Private First Class. He received training in Intelligence Analysis, and was ultimately assigned as a U.S. Army Military Occupational Specialty ("MOS") 35F – Intelligence Analyst. MANNING was granted a U.S. Government security clearance at the "Top Secret" level as part of his position within the U.S. Army. On or about October 12, 2009, MANNING was deployed with his unit, HHC, 2nd BCT, 10th Mountain Division, to Forward Operating Base ("FOB") Hammer, located approximately 40 miles east of Baghdad, Iraq, and 70 miles west of the Iran-Iraq border.

Between October 2009 and May 2010, while assigned in Iraq and working in the role of an All-Source Intelligence Analyst, MANNING was granted access to national defense information through various U.S. Army and DoD computer network systems, including: the Non-Secure Internet Protocol Router ("NIPR") network, used for the processing of unclassified documents and unclassified communications; and the Secure Internet Protocol Router ("SIPR") network, used for the processing of classified documents and classified communications at the "Confidential" and "Secret" classification levels. MANNING also had access to a commercial, non-military, satellite-based ISP while in his living quarters on FOB Hammer, which he used with his personal laptop computer while not performing official duties. This information has been verified by statements of co-workers in MANNING's unit, by examination of various computer account and network log file systems, the forensic examination of computers used by MANNING, and by documents obtained during the course of this investigation.

Classified Material Published On The Internet

On February 18, 2010, the website WikiLeaks.org ("WikiLeaks") – which is self-described as "a multi-jurisdictional public service designed to protect whistle blowers, journalists and activists who have sensitive materials to communicate to the public" – published on their website a U.S. Department of State diplomatic cable originating from the U.S. Embassy in Reykjavik, Iceland, which was classified "Confidential". This diplomatic cable, dated January 13, 2010, related to diplomatic discussions on the topic "Icesave" between members of the U.S. Department of State, the British Foreign Service, and Icelandic Government personnel. Based on this classified document's publication on the WikiLeaks website, the U.S. Department of State's Diplomatic Security Service initiated an investigation on February 19, 2010, to identify the

person(s) who unlawfully disclosed this document.

On April 5, 2010, at the National Press Club in Washington, D.C., the founder of WikiLeaks, an Australian citizen named Julian P. Assange, held a press conference to publicly release classified video footage of United States combat operations in Iraq. The video footage, apparently taken by a U.S. Army AH-64 Apache attack helicopter engaged in combat in or around Baghdad, Iraq, depicts an air-strike conducted on July 12, 2007, during which two *Reuters* journalists, several suspected Iraqi insurgents, and several Iraqi civilians were killed or wounded. Assange released the original 38-minute-long version of the video as well as a shorter "production" version lasting approximately 18 minutes, titled "Collateral Murder", both of which were published on the Internet at the URL "www.collateralmurder.org". Due to the controversial and/or graphic nature of the video, this classified material received wide news media coverage. U.S. Department of Defense officials later confirmed that the video footage was genuine and was properly classified "Secret".

Manning Identified as Source of Classified U.S. Government Material

Between May 20, 2010 and May 26, 2010, MANNING began a series of Internet chat conversations with a civilian, Mr. (b)(6)(b)(7)(C) residing in (b)(6)(b)(7)(C). (b)(6)(b)(7)(C) is known in the computer security community as a 'computer hacker' and has been profiled extensively in the print and on-line media. MANNING and (b)(6)(b)(7)(C) discuss a range of issues related to Classified U.S. Government material over a period of approximately 6 days; wherein MANNING admits to (b)(6)(b)(7)(C) to having unlawfully disclosed U.S. Government Classified material to the website WikiLeaks.org. During these chat conversations, which MANNING and (b)(6)(b)(7)(C) encrypted so that only they could read the communications, MANNING detailed the specific items of Classified U.S.

Government material he unlawfully disclosed to the WikiLeaks website as: a video and related documentation of a U.S. airstrike in Gharani, Afghanistan; the Apache airstrike video in Baghdad, Iraq which was publicly disclosed by WikiLeaks; an Iraq War Event Log believed to contain approximately 500,000 records; the "Gitmo Papers" relating to terror suspect detainees being held in Guantanamo Bay, Cuba; and a U.S. Department of State database containing approximately 260,000 Classified U.S. State Department internal communications, to include the Classified cable related to the topic of "Icesave" also disclosed by WikiLeaks.

(b) (6), (b) (7)(C) subsequently notified law enforcement of these chat conversations which lead to USACIDC Special Agents in Iraq apprehending MANNING on FOB Hammer on May 27, 2010. Upon MANNING's apprehension by USACIDC, MANNING invoked his legal right to counsel and declined to make any statements in relation his involvement in the unlawful disclosure of Classified U.S. Government materials. MANNING has further been held in confinement since May 27, 2010, pending a Military Courts-Martial.

At the time of MANNING's apprehension in Iraq, USACIDC Special Agents seized numerous U.S. Government and personal computers associated with MANNING on FOB Hammer, per a Military Magistrate Search Authorization. The U.S. Government computers collected as evidence included: several SIPR computers MANNING was identified as having been assigned while working in his position as an Intelligence Analyst in Iraq; several NIPR computers other personnel in MANNING's unit, to include MANNING, would have shared for work-related duties; and several personally owned computers, to include MANNING's personal laptop computer and other items of digital media as well as those from other personnel in MANNING's unit.

Subsequent computer forensic examination of MANNING's assigned U.S. Government and personal computers by personnel assigned to CCIU, revealed evidence MANNING had unlawfully accessed and/or unlawfully possessed the Classified U.S. Government material he claimed in his Internet chats with (b)(6)(b)(7)(C). Further forensic examination revealed MANNING may have used his personal laptop computer and non-military, satellite-based ISP Internet connection to transmit classified documents directly or indirectly to WikiLeaks. During the course of the on-going computer forensic examination of MANNING's primary SIPR computer he was assigned for duty, which contained evidence of his access to Classified U.S. Government material believed to have been disclosed to the website WikiLeaks – the Microsoft Windows personal profile of MANNING was found to have been created on this computer in March 2010. Further forensic examination of this hard drive revealed the Microsoft Operating System installed on this computer appeared to have been installed in 2008; suggesting MANNING had not used this particular SIPR computer during his entire period of duty in Iraq and/or prior to March 2010.

Based on the time line of events set forth in this investigation to include: MANNING's own statements during his Internet chats with (b)(6)(b)(7)(C) the timing of disclosures of certain Classified U.S. Government materials to and/or by the website WikiLeaks, and the known creation/original publication dates of documents disclosed by MANNING; it is believed MANNING's activities related to the unlawful disclosure of Classified U.S. Government materials began prior to March 2010, and may have begun as early as November 2009. Based on this information it is suspected MANNING may have been using a different U.S. Government computer(s) other than the computers

identified and collected at FOB Hammer, Iraq as evidence by USACIDC Special Agents at the time MANNING was apprehended.

Subsequent interviews with personnel assigned to or supporting MANNING's unit related that it was not uncommon for computers to have mechanical problems due to the excessive heat and general dusty conditions of Iraq. Personnel interviewed specifically related they knew of several instances in which MANNING's U.S. Government computer(s) had problems requiring the attention of support personnel. Due to the seemingly insignificant and/or routine nature of these unit computer problems and lack of any reliable unit records showing repairs of computers or the use of replacement parts (such as hard drives), USACIDC Special Agents have been unable to rule-out the use of other U.S. Government computers by MANNING while assigned at FOB Hammer. Based on the workload of MANNING's unit and the need for MANNING's assigned U.S. Government SIPR computers to function for MANNING to conduct his duties, it is believed MANNING's SIPR computer which had been reportedly malfunctioning, may have been substituted for another U.S. Government computer. Based on further discussions with MANNING's unit personnel, it is possible that a computer or hard disk drive from a computer used by MANNING may have been later reissued to other personnel in MANNING's unit once the problem with that computer or hard disk drive was corrected.

In addition to MANNING's assigned U.S. Government SIPR computer's available hard disk drive storage, and possibly due to the abovementioned computer mechanical issues, MANNING was further identified as having used a "Network Share Drive" to store files and other data as part of his duties in conducting Intelligence Analysis in Iraq.

Due to the nature in which MANNING is believed to have harvested large amounts of data from U.S. Government websites and/or databases on the SIPR network, it is further believed that MANNING placed this data, temporarily, within his allocated electronic storage space, on the SIPR Network Share Drive. The computer which functioned as the provider of, and housed this electronic storage space, was a Server also assigned to HHC, 2nd BCT, 10th Mountain Division, and was present at FOB Hammer during the time MANNING's unit was deployed in Iraq. At the request of CCIU during the initial stages of this investigation, and while MANNING's unit was conducting their assigned combat mission in Iraq, HHC, 2nd BCT personnel provided a 'Logical Image' of the electronic storage space used by MANNING. This Logical Image or Logical Copy contained only the files, information and data viewable using the server's Operating System, and would not include "deleted" files, folders, information and data which could be obtained from a 'Physical Image' of the drive(s) on which this storage space resided. Due to a combination of issues related to this server's critical role for MANNING's unit, lack of a replacement server, as well as the mission critical information stored on this server; a more thorough 'Physical Copy' of this storage space and/or a computer forensic examination of this server could not readily be conducted. Further, forensic examinations of other computers used by MANNING had not identified a compelling need to conduct a more in-depth forensic analysis of this server until the time this server had already been prepared for redeployment with MANNING's unit which was returning to Fort Drum and/or it was determined it would have been logistically difficult to have collected and shipped this server to CCIU from Iraq prior to the unit returning with the property as part of its redeployment.

Based on forensic examinations of MANNING's identified SIPR computers, it is believed additional evidence of files, information, and electronic data MANNING accessed, both while conducting his Intelligence Analysis duties and while committing the mentioned violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information), may be contained on this server and obtainable from a Physical Image of the hard disk drives on this server – providing USACIDC Special Agents a better understanding of the scope of MANNING's activities.

Additional Disclosure of Classified Materials by the Website WikiLeaks

On July 25, 2010, the WikiLeaks website in coordination with The New York Times, The Guardian (a news media publication based in London, England) and Der Spiegel Magazine (a news media publication based in Germany) published approximately 75,000 classified U.S. Government documents relating to the War in Afghanistan. According to an on-line article posted on The New York Times website on July 25, 2010:

"The articles published today are based on thousands of United States military incident and intelligence reports — records of engagements, mishaps, intelligence on enemy activity and other events from the war in Afghanistan — that were made public on Sunday on the Internet. The New York Times, The Guardian newspaper in London, and the German magazine Der Spiegel were given access to the material several weeks ago. These reports are used by desk officers in the Pentagon and troops in the field when they make operational plans and prepare briefings on the situation in the war zone..."

Further, regarding the source of the material The New York Times article relates:

"The documents — some 92,000 individual reports in all —

were made available to The Times and the European news organizations by WikiLeaks, an organization devoted to exposing secrets of all kinds, on the condition that the papers not report on the data until July 25, when WikiLeaks said it intended to post the material on the Internet. WikiLeaks did not reveal where it obtained the material."

While the information reported by The New York Times identifies approximately 92,000 reports being disclosed, about 15,000 reports were not published by either the website WikiLeaks or the mentioned news media organizations due to this material believed to contain information more sensitive than in the published material. The New York Times article suggests information even more sensitive than the published Classified U.S. Government materials were obtained from WikiLeaks as the article further relates:

"We have, for example, withheld any names of operatives in the field and informants cited in the reports. We have avoided anything that might compromise American or allied intelligence-gathering methods such as communications intercepts."

The WikiLeaks website in regard to the 15,000 unpublished Classified U.S. Government documents published on its website:

"We have delayed the release of some 15,000 reports from the total archive as part of a harm minimization process demanded by our source. After further review, these reports will be released, with occasional redactions, and eventually in full, as the security situation in Afghanistan permits."

Personnel associated with the website WikiLeaks have publicly acknowledged having other Classified U.S. Government material (which are believed to have been unlawfully disclosed by MANNING) such as the Gharani, Afghanistan airstrike video and associated report; however, for reasons unknown WikiLeaks has not published this material to the public.

MANNING's Unit Redeploys From Iraq to Fort Drum

During the month of August 2010, MANNING's unit began the process of redeploying from Iraq to Fort Drum after having completed the unit's tour of duty in Iraq. As part of this redeployment process MANNING's unit packed a specific U.S. Government Shipping Container (commonly referred to as a "Connex") with many of the unit's assigned 'Sensitive Items'. According to the DA Form 5748-R, Shipment Unit Packing List and Load Diagram, completed on August 18, 2010, by personnel assigned to MANNING's unit – this Shipping Container was packed with numerous U.S. Government: computers, of various makes and models; cryptological communication equipment; communication equipment; computer networking and peripheral hardware components; high security safes; miscellaneous paper and office supplies; office equipment; over 225 computer hard disk drives packed in boxes or with other equipment; as well as various other miscellaneous U.S. Government Property assigned to HHC, 2nd BCT, 10th Mountain Division. On these shipping documents it was further noted that several of these U.S. Government computer systems and/or equipment was identified as being Classified systems or components.

This Shipping Container, further referred to by unit personnel as the unit's "Sensitive Items Connex", was reportedly securely sealed in accordance with U.S. Army and/or Department of Defense regulations for shipping containers of this nature and was transported under U.S. Government control from Iraq to the United States by sea freight, arriving at the U.S. Port of Beaumont, Texas, on September 6, 2010. This Shipping Container was further transported under U.S. Government control by truck from Beaumont, Texas to Fort Drum, and arrived at Fort Drum, New York on or about

September 9, 2010. Upon the arrival of this Shipping Container at Fort Drum and its customary processing by the Fort Drum Transportation Office, the HHC, 2nd BCT unit command arranged for this container to be positioned within the HHC, 2nd BCT unit area. The unit Command further arranged for unit personnel to be on hand to assist USACIDC Special Agents in opening, identifying, inventorying, and preparing the identified computers and/or hard disk drives for examination – to determine if each may have been used by MANNING and/or be of evidentiary value to this investigation.

On September 10, 2010, USACIDC Special Agents from CCIU, under the authority of a Military Magistrate issued Search Authorization by CPT (b)(6)(b)(7)(C) Military Magistrate, B Company, Division Special Troops Battalion, 1st Armor Division, Camp Liberty, Iraq, searched the aforementioned connexes for the items mentioned. In addition to the computers and/or hard disk drives from the connex, additional sensitive items, to include computers and/or computer hard disk drives (similar to and/or identical to ones transported in the aforementioned connex) which had been hand-carried by HHC, 2nd BCT unit members redeploying from Iraq back to Fort Drum, were also examined. These items had been placed into a Secured Storage Space, referred to as the "Unit Vault", within the Unit Area. Further, a second Shipping Container, identified as the "S-2 Connex" was also found to contain similar and/or identical computer equipment and/or digital media, although reportedly these items have been identified for processing 'Unclassified' information. All of the aforementioned connex and non-connex items were included as items to be searched/examined in the above mentioned Military Magistrate Search Authorization. Upon completion of the examination/search, several identified computers and/or hard disk drives were collected as evidence.

Additional Computers and/or Hard Disk Drives Identified

Upon USACIDC Special Agents returning to Fort Belvoir with computers and/or hard disk drives identified and collected at Fort Drum, it was determined one of the major items that was collected – which was related to the Server and/or Network Storage Space identified that MANNING utilized – needed to be physically connected to computers/servers at Fort Drum which were not believed to be of evidentiary value and were not collected as evidence, in order to conduct an examination of the items that were collected at Fort Drum. Due to this technical problem, on September 28, 2010, USACIDC Special Agents returned to Fort Drum with the collected evidence (related to the Server and/or Network Storage Space MANNING used) in order to physically connect this item of evidence with other computers which had been deployed in Iraq; to complete the examination of the collected evidence.

During the completion of this technical/investigative effort, HHC, 2nd BCT, 10th Mountain Division personnel identified additional computer hard disk drives that had not been previously identified to USACIDC Special Agents in their previous examinations/searches of connex items and other Information Technology equipment returned from Iraq and/or possibly used by MANNING. These previously unidentified items (which consisted of more computer hard disk drives) were found in a connex which had been located within a motor pool assigned to HHC, 2nd BCT. The hard disk drives were stored in a plastic portable 'Pelican' brand shipping container which was removed from the connex by Staff Sergeant (b)(6)(b)(7)(C) on September 30, 2010. (b)(6)(b)(7)(C) secured the container and its contents (hard disk drives) in the 2nd BCT Headquarters, located at 10200 N. Riva Ridge Loop, Fort Drum, New York, which is their present location. It was

noted that during the previous search of connexes and other locations by USACIDC Special Agents at Fort Drum, on or about September 10, 2010, that HHC, 2nd BCT unit personnel who would have been more knowledgeable about the recently identified additional computer hard drives, were on block leave due to their deployment and were physically unavailable to assist investigators at that time.

**Method of Examination of U.S. Government Computers by USACIDC Personnel
While at Fort Drum**

In an attempt to identify what previously unidentified computers MANNING may have used which are in possession of the U.S. Government, USACIDC Special Agents plan on: identifying all computer hard disk drives found in the above described Shipping Container; and they will then connect the hard disk drives using methods and procedures to forensically preserve any potential evidence on those drives, to forensic computers installed with commercially available computer forensic software. The USACIDC Special Agents will then further attempt to determine by the inspection of the electronic file system contained on each hard disk drive as to whether a Windows User Profile related to MANNING's SIPR and/or NIPR network account(s) are present on the drive(s). Should a drive be found containing a Windows User Profile for MANNING, this will provide a strong indication this drive was once contained in or associated with a computer used by MANNING's network user account. Consequently these hard disk drive(s) will be seized, collected as evidence, and further computer forensic examination will be conducted to determine the drive's evidentiary value to this investigation as further described in Attachment C.

I have learned in my professional experience in conducting forensic examinations that intentional or unintentional data and information stored on hard disk drives and other digital media, is highly persistent and may remain on digital media, computers, and computer-related devices nearly indefinitely without concerted efforts to purge or "wipe" this data by personnel with specialized tools and/or knowledge beyond the average computer user. More specifically when data is "Deleted" by a computer user, although this data may be no longer accessible to the computer user by normal means of the Operating System - this data is not removed from the digital media it was contained on necessarily, but the space this data occupies may simply be marked as available for future data to be stored in its place by the Operating System. However, until over-written by future data it may remain fully or partially intact and can provide further evidence of criminal violations or in some cases exculpatory evidence. Consequently, although considerable time has passed since MANNING may have accessed any computers and/or hard disk drives contained in the mentioned Shipping Container, the likelihood evidence related to MANNING's activities is still present should MANNING have used that given computer or hard disk drive is relatively high.

Requirement for Military Magistrate Search Authorization

While the aforementioned physical items USACIDC Special Agents wish to evaluate for potential evidence have been: identified as U.S. Government property and that no personal property has been identified as having been co-mingled into the identified Shipping Container; that the unit responsible for the property identified in the Shipping Container have consented to USACIDC Special Agents inspecting the items for evidence and are cooperating in this process – the information contained on items of

digital media (such as hard disk drives) may still contain personal information, documents, electronic communications between third-parties associated or not associated with MANNING, who in various circumstances may still have a limited expectation to privacy to this information stored on these computer systems, hard disk drives, and/or digital media owned by the U.S. Government. Further, although USACIDC Special Agents will attempt to quickly evaluate each item of digital media for signs of its previous use by MANNING as a practical matter to facilitate the expeditious evaluation of a large number of items – in some cases inadvertent or unavoidable viewing of personal data, third-party communications, digital photographs, and/or other electronic information which individuals, to include MANNING, may have limited privacy expectations to this data, may still occur. Further, the evaluation process mentioned herein, while minimally invasive, could be considered in a certain sense, a "search" in of itself, as the computers, hard disk drives, and other digital media to be evaluated are not merely 'open containers' easily viewable without specialized computer forensic hardware, forensic software tools and training.

Upon the identification of any digital media located in the places to be searched, as described in Attachment B, which are believed to have been previously used by MANNING, USACIDC Special Agents will seize and further search these identified digital media items for additional evidence, fruits and instrumentalities of violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information), in accordance with the procedures specified in Attachment C.

Conclusion

Given the facts and circumstances of the incidents related to the unlawful disclosure of Classified U.S. Government material by MANNING; the identification of Classified U.S. Government materials on MANNING's personal computer; the identification MANNING may have used other computers belonging to his unit to conduct his unlawful activities; that a hard disk drive(s) from MANNING's identified SIPR computer may have been replaced with other hard disk drives due to computer mechanical failures, and that these hard disk drives may still be in the possession of MANNING's former unit; that data and/or evidence on all of these items could reasonably still exist - there is probable cause to believe that additional evidence, fruits and instrumentalities of the offenses believed to have committed by MANNING to include violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information) are contained on: computers; hard disk drives present within computers and/or as stand-alone items; and/or other digital media exists – which are contained in a plastic shipping container previously shipped in a connex assigned to HHC, 2nd BCT, 10th Mountain Division, now located at 10200 North Riva Ridge Loop, Fort Drum, New York – and described in more detail in Attachment C.

ATTACHMENT B

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The following locations are to be searched (as explained in Attachment A): the main office space of the 2nd Brigade Combat Team (BCT) Headquarters Building, 10th Mountain Division, 10200 North Riva Ridge Loop, Fort Drum, New York; and more specifically a plastic portable 'Pelican' brand shipping container formerly located within a U.S. Government shipping container (connex) assigned to HHC, 2nd BCT, 10th Mountain Division, Fort Drum, New York.

ATTACHMENT C

ITEMS TO BE SEIZED AND SEARCHED

Special Agents of USACIDC or other Army law enforcement personnel assisting USACIDC to search a plastic portable 'Pelican' brand container, located at 10200 North Riva Ridge Loop, Fort Drum, New York, as described in Attachment B, and therein to seize and subsequently search all computer hardware and digital media having been identified as associated with or previously used by Private First Class (PFC) Bradley Edward MANNING, formerly assigned to HHC, 2nd BCT, 10th Mountain Division – specifically as it relates to information, documents, and data, both classified and unclassified, as mentioned in Attachment A, which is herein incorporated into Attachment C, in regard to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information).

Computer Hardware and Digital Media is further described as any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data processing hardware (such as "desktop computers" and self-contained "laptop", "notebook", or "netbook" computers, as well as "Smart Phones" and internet capable PDAs); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical disc storage devices such as CDs or DVDs, USB drives, flash memory cards or similar solid-state storage media, and other memory storage devices);

peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

FURTHER SEARCH OF SEIZED COMPUTERS AND DIGITAL MEDIA ITEMS

The items seized as part of this Search Authorization, which should consist of computers, hard disk drives, and/or other digital media, will have forensically sound images (digital copies) produced of the seized items as appropriate, which will in turn be searched in lieu of the original seized items as part of a digital media/computer forensic examination. The search of digital copies of the items seized is done to ensure and preserve the forensic integrity of the seized items for additional and/or future examination(s) in accordance with criminal procedure and rules of evidence. These examination(s) of seized items will be conducted by personnel assigned to the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) who are certified by the Department of Defense and/or Department of the Army to conduct such types of examinations. These personnel will use computer forensic hardware and/or software, which has been approved for use in conducting such examinations. Due to the unknown nature and/or number of items which could be seized within the scope of this Search Authorization, it is not necessarily practical or feasible to make forensically sound images (digital copies) of seized evidence while at

the search location. Subsequently, these digital copies will be produced within a reasonable amount of time, unless extended by authorization of the Military Magistrate, with the originally seized items being returned to the owner of the property in accordance with Army Regulation 195-5, "Evidence Procedures". Further, due to the unknown number of items seized, as well as the complexity of examining these items, it is also not feasible to conduct a search/forensic examination of the items while at the search location to determine their complete evidentiary value. Consequently, this search/examination activity will be completed within facilities operated by the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) and completed as expeditiously as possible.

SWORN STATEMENT

For use of this form, see AR 190-45; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.

1. LOCATION 2nd BCT HQ, Fort Drum, NY 13602	2. DATE (YYYYMMDD) 20b/10/01	3. TIME 1530	4. FILE NUMBER 0028-10-CID221-10117
5. LAST NAME, FIRST NAME, MIDDLE NAME (b)(6)(b)(7)(C)	6. SSN (b)(6)(b)(7)(C)	7. GRADE/STATUS CW2	

8. ORGANIZATION OR ADDRESS
Headquarters and Headquarters Company, 2nd Brigade Combat Team 10th Mountain Division, Fort Drum, NY 13602

9. (b)(6)(b)(7)(C), WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

I met and worked with Bradley Manning prior to the deployment as well as throughout the deployment. Prior to the deployment PFC Manning was responsible for getting together an Iraq country brief so that he would grasp a better working knowledge on the country of Iraq and their cultures as well as building an informative product to help out his fellow soldiers in their transition into the country of Iraq. This study covered religion, race, agriculture, culture practice, economic, and extremist groups that operate within the country of Iraq. His access was not limited to NIPR but the request was to keep it unclassified for distribution to others outside the shop as well. When we deployed we took all computers with us with the exception of one and that was never a SIPR computer. That computer was left behind with SSC (b)(6)(b)(7)(C) PFC Manning did make random and reoccurring visits down to Syracuse leaving him subject to finding random rides back up to Fort drum.

Upon arrival to Iraq the shop was split apart into day, night, current operations, and a small group was sent to other FOB's for random Intelligence tasks. PFC Manning, SPC Manning at the time, only operated in the day and night shift position within the SCIF. His access was limited to SIPR and NIPR throughout his stay in Iraq. Although his clearance authorized it he was only read on to actual missions that were higher classified but never was allowed access to JWICS or the SIGINT platform that they were utilizing. PFC Manning was part of a three man night shift for the majority of his deployment and was supervised from SPC (b)(6)(b)(7)(C) as well as SPC (b)(6)(b)(7)(C) during the beginning of the deployment. The beginning of the deployment was very hectic but around December I recognized PFC Manning's trips to the smoke area seem to be a little concerning. He would walk forcefully to the bunker at the smoke pit and chain smoke two cigarettes and walk at a quick pace back to the office. Sometimes he would stare off into the bliss and others it would seem as though he would hold a conversation or debate with himself. I approached him a few times about it, even inviting him to come and hang out with others while out there. Checking to see the stress was getting to him, or if anything else was bothering him. He denied both the invite and that anything was bothering him at all. He did accept invitations to walk and talk to the coffee shop every now and then. He shared some concerns about his life, and that he had nowhere to go right now. This conversation was brought up in the office as we were all talking about why we joined or stayed in the Army. When it came around to PFC Manning he said that the US Flag meant nothing to him and he had no loyalties to our country. When asked why he would join our Military he said because he had no choice. He said he lost his job, was homeless and the only thing that was available to him at the time was the US Army. I was concerned not for his patriotism but for him because that could be signs of depression or anger issues. He assured me that it was anger it was just him being honest. PFC Manning continued work in that shop for five more months without any issues other than the smoking routine which was always bothersome. However, when he returned from leave he seemed rejuvenated as most soldiers do. Everything seemed normal until the day he punched SPC (b)(6)(b)(7)(C).

Q: SA (b)(6)(b)(7)(C)

A: CW2 (b)(6)(b)(7)(C)

Q: Did PFC MANNING's smoking routine change when he returned from leave?

A: His smoking routine stayed the same, but his attitude changed. He started talking a lot more when he came back from leave and seemed better. He seemed happier.

10. EXHIBIT	11. INITIALS OF PERSON MAKING STATEMENT (b)(6)(b)(7)(C)	PAGE 1 OF 2 PAGES
-------------	--	-------------------

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF _____ TAKEN AT _____ DATED _____"

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE INDICATED.

STATEMENT OF (b)(6)(b)(7)(C) TAKEN AT Fort Drum, NY DATED 2010/10/01 (b)(6)(b)(7)(C)

9. STATEMENT (Continued)

Q: Did you ever observe PFC MANNING taking information out of the SCIF?

A: No.

Q: Did you observe PFC MANNING bring any CDs into the SCIF?

A: Yes. Everyone brought in music CDs to play.

Q: Do you remember anything specific about the CDs PFC MANNING brought into the SCIF?

A: No.

Q: What were the standard procedures as to what could be brought into and out of the SCIF?

A: No removable media, cell phones or re-writeable CDs were allowed. Most of the CDs I saw appeared to be factory CDs.

Q: Did anyone check to see if the CDs brought into the SCIF were re-writeable?

A: Yes, we did random checks.

Q: Were re-writeable CDs ever found during the random checks?

A: No.

Q: Was it policy that CDs had to be factory CDs?

A: No, it was not policy. The only policy was that they could not be re-writeable.

Q: Was PFC MANNING ever caught with any unauthorized items in the SCIF?

A: No. He actually showed more concern about other people who had unauthorized items than most of the people in the SCIF.

Q: Do you have anything else to add to your statement?

A: No.///END OF STATEMENT/// (b)(6)(b)(7)(C)

AFFIDAVIT

I, (b)(6)(b)(7)(C), HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1, AND ENDS ON PAGE 2. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT MORE OF BENEFIT OR DAMAGE WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE (b)(6)(b)(7)(C)

(Signature of Person Making Statement)

WITNESSES:

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 1st day of October, 2010 at Fort Drum, NY

(b)(6)(b)(7)(C)

(Signature of Person Administering Oath)

ORGANIZATION OR ADDRESS

SA (b)(6)(b)(7)(C), (b)(7)(E)

(Typed Name of Person Administering Oath)

ORGANIZATION OR ADDRESS

5 USC 303

(Authority To Administer Oaths)

INITIALS OF PERSON MAKING STATEMENT

(b)(6)(b)(7)(C)

PAGE 2 OF 2 (b)(6)(b)(7)(C)

SEARCH AND SEIZURE AUTHORIZATION

For use of this form, see AR 27-10; the proponent agency is OTJAG

TO: (Name and Organization of the person to whom authorization is given)

Special Agent (b)(6)(b)(7)(C) of the United States Army Criminal Investigation Command (USACIDC)

(An affidavit) (A (sworn) or (unsworn) oral statement)

having been made before me by

Special Agent (b)(6)(b)(7)(C)

(Name of Affiant)

Washington Metro Resident Agency, Computer Crime Investigative Unit (CCIU), USACIDC, Fort Belvoir, Virginia 22060

(Organization or Address of Affiant)

(which affidavit is attached hereto and made a part of this authorization), and as I am satisfied that there is probable cause to believe that the matters mentioned in the affidavit are true and correct, that the offense set forth therein has been committed, and that the property to be seized is located (on the person) (at the place) to be searched, you are hereby ordered to search the (person) (place) known as

Sensitive Compartmented Information Facility containing U.S. Govt Digital Media, 10200 N. Riva Ridge Loop, Fort Drum, NY

for the property described as U.S. Government hard disk drives, and/or digital media, the property of HHC, 2nd Brigade Combat

Team, 10th Mountain Division, Fort Drum, New York, containing information or data related to the use of computers/digital

media by PFC MANNING and access to and/or disclosure of Classified U.S. Government Material (See Attachment C).

bringing this order to the attention of the (person searched) (person in possession, if any person be found at the place or on the premises searched). The search will be made in the (daytime) (nighttime), and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to:

Evidence Custodian, Computer Crime Investigative Unit (CCIU), 9805 Lowen Road, Bldg 193, Fort Belvoir, Virginia

(Name and Organization of Authorized Custodian)

and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 1 day of October, 2010

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL

CPT (b)(6)(b)(7)(C)

DUTY POSITION OF AUTHORIZING OFFICIAL

Military Magistrate

ORGANIZATION OF AUTHORIZING OFFICIAL

SJA office of 10th MTN

SIGNATURE OF AUTHORIZING OFFICIAL

(b)(6)(b)(7)(C)

(b)(6)(b)(7)(C)

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

For use of this form, see AR 27-10; the proponent agency is OTJAG.

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

1. I, Special Agent (b)(6)(b)(7)(C), Washington Metro Resident Agency
(Name) (Organization or Address)

Computer Crime Investigative Unit (CCIU), USACIDC, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060

having been duly sworn, on oath depose and state that:

SEE ATTACHMENT A.

2. The affiant further states that:

SEE ATTACHMENT A.

3. In view of the foregoing, the affiant requests that an authorization be issued for a search of

SEE ATTACHMENT B

(the person) (and)

(the quarters or billets) (and)

SEE ATTACHMENT C

(the automobile) (

and (seizure) (appreh)

(items/persons searched for)

Search and Seizure

TYPED NAME AND ORGANIZATION OF AFFIANT

Special Agent (b)(6)(b)(7)(C)
Washington Metro Resident Agency
Computer Crime Investigative Unit (CCIU), USACIDC

SIGNATURE OF AFFIANT

(b)(6)(b)(7)(C)

SWORN TO AND SUBSCRIBED BEFORE ME THIS

1st

DAY OF

October

2010

AT

2020

TYPED NAME, ORGANIZATION AND OFFICIAL CAPACITY OF AUTHORITY
ADMINISTERING THE OATH

CPT (b)(6)(b)(7)(C)

SIGNATURE OF AUTHORITY ADMINISTERING THE OATH

(b)(6)(b)(7)(C)

INSTRUCTIONS FOR

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it has been committed. Use additional page if necessary.
2. In paragraph 2, set forth facts establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraphs 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she has plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary.
3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under certain circumstances for evidentiary matters.

ATTACHMENT A

INTRODUCTION

I make this affidavit in support of an application for a Military Magistrate Search Authorization for electronic data, computer hardware, and physical evidence relating to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information). As set forth herein, there is probable cause to believe within the Sensitive Compartmented Information Facility ("SCIF") assigned to the 2nd Brigade Combat Team ("BCT"), 10th Mountain Division, Fort Drum, New York ("Fort Drum"), located at 10200 North Riva Ridge Loop, Fort Drum, New York; contains evidence, fruits, and/or instrumentalities of the offenses committed by Private First Class (PFC) Bradley Edward MANNING ("MANNING") formerly assigned to Headquarters and Headquarters Company ("HHC"), 2nd BCT, 10th Mountain Division, as further described in this affidavit.

AGENT BACKGROUND

I am a Special Agent in the United States Army Criminal Investigation Command ("USACIDC") and have been so for approximately three years. I am currently assigned to the USACIDC, Washington Metro Resident Agency, of the Computer Crime Investigative Unit ("CCIU"), located at Fort Belvoir, Virginia; where I am responsible for the investigation of, among other things, violations pertaining to computer intrusions, denial of service attacks, and other types of malicious computer activity directed against U.S. Army and/or Department of Defense computer networks anywhere in the world. Prior to my assignment at CCIU, I was assigned as a Special Agent with USACIDC in:

Fort Bragg, NC, where I was responsible for conducting felony investigations and a Computer Crime Coordinator where I was responsible for conducting computer forensic examinations of seized computers, cellular phones, and other digital media impacting the U.S. Army in North Carolina, South Carolina, Georgia and Virginia; within Iraq, Kuwait and Afghanistan.

I have been trained in computer incident response, digital evidence acquisition, Windows Forensic Examinations by the Department of Defense Cyber Investigations Training Academy ("DCITA"). I currently possess "Department of Defense Certified Digital Forensic Examiner" and "Department of Defense Certified Digital Media Collector" certifications. In addition to my training and experience as a criminal investigator, I have also received a Bachelor of Science from Liberty University, Lynchburg, Virginia.

My experience as a USACIDC Special Agent has included the investigation of cases involving violent and non-violent crimes as well as the use of computers. I have received training and gained experience in interviewing and interrogation techniques, arrest procedure, search warrant applications, the execution of searches and seizures, and other criminal laws and procedures.

As a Special Agent of the USACIDC, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice (Title 10 U.S.C. Section 47) and other applicable federal and state laws where there is a U.S. Army or Department of Defense interest. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in

that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

SOURCE OF EVIDENCE

The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals – including other law enforcement officers and particularly other USACIDC Special Agents – as well as my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

RELEVANT STATUTES

Title 18, United States Code, § 793(d) makes it unlawful to make unauthorized disclosure of national defense information. Specifically, the statute provides in pertinent part that:

Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered or transmitted . . . the same to any person not entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years, or both.

Title 18, United States Code, § 1030(a) makes it unlawful to, without authorization, obtain from a United States Government computer certain national defense information, and disclose such information. Specifically, the statute provides in pertinent part that:

Whoever — (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted . . . the same to any person not entitled to receive it [shall be punished by a fine under this title or imprisonment for not more than ten years, or both]

The national security classification levels assigned to national security information and national defense information are defined in Executive Order No. 13526 and its predecessor orders. Information may be classified if the following conditions are met: (1) an original classification authority ("OCA") is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the United States Government; (3) the information falls within one or more of the categories set forth in the Executive Order (which includes intelligence sources and methods; cryptology; military plans; and vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security of the United States); and (4) the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational

terrorism, and the OCA is able to identify or describe the damage. Under the Executive Order, information may be classified "Confidential" if its unauthorized disclosure reasonably could be expected to cause damage to the national security; "Secret" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security; and "Top Secret" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

BACKGROUND AND TECHNICAL INFORMATION

The term "computer" as used in this affidavit is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I am aware of the following:

a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information.

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area

network, wireless and numerous other methods.

c. Instant Messaging (IM) is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger, etc.) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are in the same state. Instant Messaging may also be commonly referred to as 'Internet Chat'.

d. The Windows User Profile is created the first time the user interactively logs-on at the computer on computers running current Microsoft Windows Operating Systems. A user profile defines customized desktop environments, such as individual display, network and printer connections settings, Favorites, Cookies and History, Start Menu, Desktop, Application Data, as well as forms the basis of a container for a user to place user created files and folders. Typically the contents of a User Profile are inaccessible by other users who do not have elevated or administrator level rights on the computer system. Consequently information related specifically to that user, such as their activities on a particular computer or network can be determined from examination of data and information contained in or related to the User's Profile.

PROBABLE CAUSE FOR SEARCH**Manning's Access To Classified Information**

MANNING enlisted in the United States Army on or about October 2, 2007, and currently holds the rank of Private First Class. He received training in Intelligence Analysis, and was ultimately assigned as a U.S. Army Military Occupational Specialty ("MOS") 35F – Intelligence Analyst. MANNING was granted a U.S. Government security clearance at the "Top Secret" level as part of his position within the U.S. Army. On or about October 12, 2009, MANNING was deployed with his unit, HHC, 2nd BCT, 10th Mountain Division, to Forward Operating Base ("FOB") Hammer, located approximately 40 miles east of Baghdad, Iraq, and 70 miles west of the Iran-Iraq border.

Between October 2009 and May 2010, while assigned in Iraq and working in the role of an All-Source Intelligence Analyst, MANNING was granted access to national defense information through various U.S. Army and DoD computer network systems, including: the Non-Secure Internet Protocol Router ("NIPR") network, used for the processing of unclassified documents and unclassified communications; and the Secure Internet Protocol Router ("SIPR") network, used for the processing of classified documents and classified communications at the "Confidential" and "Secret" classification levels. MANNING also had access to a commercial, non-military, satellite-based ISP while in his living quarters on FOB Hammer, which he used with his personal laptop computer while not performing official duties. This information has been verified by statements of co-workers in MANNING's unit, by examination of various computer account and network log file systems, the forensic examination of computers used by MANNING, and by documents obtained during the course of this investigation.

Classified Material Published On The Internet

On February 18, 2010, the website WikiLeaks.org ("WikiLeaks") – which is self-described as "a multi-jurisdictional public service designed to protect whistle blowers, journalists and activists who have sensitive materials to communicate to the public" – published on their website a U.S. Department of State diplomatic cable originating from the U.S. Embassy in Reykjavik, Iceland, which was classified "Confidential". This diplomatic cable, dated January 13, 2010, related to diplomatic discussions on the topic "Icesave" between members of the U.S. Department of State, the British Foreign Service, and Icelandic Government personnel. Based on this classified document's publication on the WikiLeaks website, the U.S. Department of State's Diplomatic Security Service initiated an investigation on February 19, 2010, to identify the person(s) who unlawfully disclosed this document.

On April 5, 2010, at the National Press Club in Washington, D.C., the founder of WikiLeaks, an Australian citizen named Julian P. Assange, held a press conference to publicly release classified video footage of United States combat operations in Iraq. The video footage, apparently taken by a U.S. Army AH-64 Apache attack helicopter engaged in combat in or around Baghdad, Iraq, depicts an air-strike conducted on July 12, 2007, during which two *Reuters* journalists, several suspected Iraqi insurgents, and several Iraqi civilians were killed or wounded. Assange released the original 38-minute-long version of the video as well as a shorter "production" version lasting approximately 18 minutes, titled "Collateral Murder", both of which were published on the Internet at the URL "www.collateralmurder.org". Due to the controversial and/or graphic nature of the video, this classified material received wide news media coverage. U.S. Department of Defense officials later confirmed that the video footage was genuine and

was properly classified "Secret".

Manning Identified as Source of Classified U.S. Government Material

Between May 20, 2010 and May 26, 2010, MANNING began a series of Internet chat conversations with a civilian, Mr. (b)(6)(b)(7)(C) residing in Carmichael, California. Lamo is known in the computer security community as a 'computer hacker' and has been profiled extensively in the print and on-line media. MANNING and (b)(6)(b)(7)(C) discuss a range of issues related to Classified U.S. Government material over a period of approximately 6 days; wherein MANNING admits to (b)(6)(b)(7)(C) to having unlawfully disclosed U.S. Government Classified material to the website WikiLeaks.org. During these chat conversations, which MANNING and (b)(6)(b)(7)(C) encrypted so that only they could read the communications, MANNING detailed the specific items of Classified U.S. Government material he unlawfully disclosed to the WikiLeaks website as: a video and related documentation of a U.S. airstrike in Gharani, Afghanistan; the Apache airstrike video in Baghdad, Iraq which was publicly disclosed by WikiLeaks; an Iraq War Event Log believed to contain approximately 500,000 records; the "Gitmo Papers" relating to terror suspect detainees being held in Guantanamo Bay, Cuba; and a U.S. Department of State database containing approximately 260,000 Classified U.S. State Department internal communications, to include the Classified cable related to the topic of "Icesave" also disclosed by WikiLeaks.

(b)(6), (b)(7)(C) subsequently notified law enforcement of these chat conversations which lead to USACIDC Special Agents in Iraq apprehending MANNING on FOB Hammer on May 27, 2010. Upon MANNING's apprehension by USACIDC, MANNING invoked his legal right to counsel and declined to make any statements in relation his involvement in the unlawful disclosure of Classified U.S. Government materials. MANNING has further

been held in confinement since May 27, 2010, pending a Military Courts-Martial.

At the time of MANNING's apprehension in Iraq, USACIDC Special Agents seized numerous U.S. Government and personal computers associated with MANNING on FOB Hammer, per a Military Magistrate Search Authorization. The U.S. Government computers collected as evidence included: several SIPR computers MANNING was identified as having been assigned while working in his position as an Intelligence Analyst in Iraq; several NIPR computers other personnel in MANNING's unit, to include MANNING, would have shared for work-related duties; and several personally owned computers, to include MANNING's personal laptop computer and other items of digital media as well as those from other personnel in MANNING's unit.

Subsequent computer forensic examination of MANNING's assigned U.S. Government and personal computers by personnel assigned to CCIU, revealed evidence MANNING had unlawfully accessed and/or unlawfully possessed the Classified U.S. Government material he claimed in his Internet chats with (b)(6)(b)(7)(C). Further forensic examination revealed MANNING may have used his personal laptop computer and non-military, satellite-based ISP Internet connection to transmit classified documents directly or indirectly to WikiLeaks. During the course of the on-going computer forensic examination of MANNING's primary SIPR computer he was assigned for duty, which contained evidence of his access to Classified U.S. Government material believed to have been disclosed to the website WikiLeaks – the Microsoft Windows personal profile of MANNING was found to have been created on this computer in March 2010. Further forensic examination of this hard drive revealed the Microsoft Operating System installed on this computer appeared to have been installed in 2008;

suggesting MANNING had not used this particular SIPR computer during his entire period of duty in Iraq and/or prior to March 2010.

Based on the time line of events set forth in this investigation to include: MANNING's own statements during his Internet chats with (b)(6)(b)(7)(C) the timing of disclosures of certain Classified U.S. Government materials to and/or by the website WikiLeaks, and the known creation/original publication dates of documents disclosed by MANNING; it is believed MANNING's activities related to the unlawful disclosure of Classified U.S. Government materials began prior to March 2010, and may have begun as early as November 2009. Based on this information it is suspected MANNING may have been using a different U.S. Government computer(s) other than the computers identified and collected at FOB Hammer, Iraq as evidence by USACIDC Special Agents at the time MANNING was apprehended.

Subsequent interviews with personnel assigned to or supporting MANNING's unit related that it was not uncommon for computers to have mechanical problems due to the excessive heat and general dusty conditions of Iraq. Personnel interviewed specifically related they knew of several instances in which MANNING's U.S. Government computer(s) had problems requiring the attention of support personnel. Due to the seemingly insignificant and/or routine nature of these unit computer problems and lack of any reliable unit records showing repairs of computers or the use of replacement parts (such as hard drives), USACIDC Special Agents have been unable to rule-out the use of other U.S. Government computers by MANNING while assigned at FOB Hammer. Based on the workload of MANNING's unit and the need for MANNING's assigned U.S. Government SIPR computers to function for MANNING to

conduct his duties, it is believed MANNING's SIPR computer which had been reportedly malfunctioning, may have been substituted for another U.S. Government computer. Based on further discussions with MANNING's unit personnel, it is possible that a computer or hard disk drive from a computer used by MANNING may have been later reissued to other personnel in MANNING's unit once the problem with that computer or hard disk drive was corrected.

In addition to MANNING's assigned U.S. Government SIPR computer's available hard disk drive storage, and possibly due to the abovementioned computer mechanical issues, MANNING was further identified as having used a "Network Share Drive" to store files and other data as part of his duties in conducting Intelligence Analysis in Iraq. Due to the nature in which MANNING is believed to have harvested large amounts of data from U.S. Government websites and/or databases on the SIPR network, it is further believed that MANNING placed this data, temporarily, within his allocated electronic storage space, on the SIPR Network Share Drive. The computer which functioned as the provider of, and housed this electronic storage space, was a Server also assigned to HHC, 2nd BCT, 10th Mountain Division, and was present at FOB Hammer during the time MANNING's unit was deployed in Iraq. At the request of CCIU during the initial stages of this investigation, and while MANNING's unit was conducting their assigned combat mission in Iraq, HHC, 2nd BCT personnel provided a 'Logical Image' of the electronic storage space used by MANNING. This Logical Image or Logical Copy contained only the files, information and data viewable using the server's Operating System, and would not include "deleted" files, folders, information and data which could be obtained from a 'Physical Image' of the drive(s) on which this storage

space resided. Due to a combination of issues related to this server's critical role for MANNING's unit, lack of a replacement server, as well as the mission critical information stored on this server; a more thorough 'Physical Copy' of this storage space and/or a computer forensic examination of this server could not readily be conducted. Further, forensic examinations of other computers used by MANNING had not identified a compelling need to conduct a more in-depth forensic analysis of this server until the time this server had already been prepared for redeployment with MANNING's unit which was returning to Fort Drum and/or it was determined it would have been logistically difficult to have collected and shipped this server to CCIU from Iraq prior to the unit returning with the property as part of its redeployment.

Based on forensic examinations of MANNING's identified SIPR computers, it is believed additional evidence of files, information, and electronic data MANNING accessed, both while conducting his Intelligence Analysis duties and while committing the mentioned violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information), may be contained on this server and obtainable from a Physical Image of the hard disk drives on this server – providing USACIDC Special Agents a better understanding of the scope of MANNING's activities.

Additional Disclosure of Classified Materials by the Website WikiLeaks

On July 25, 2010, the WikiLeaks website in coordination with The New York Times, The Guardian (a news media publication based in London, England) and Der Spiegel Magazine (a news media publication based in Germany) published approximately 75,000 classified U.S. Government documents relating to the War in

Afghanistan. According to an on-line article posted on The New York Times website on July 25, 2010:

"The articles published today are based on thousands of United States military incident and intelligence reports — records of engagements, mishaps, intelligence on enemy activity and other events from the war in Afghanistan — that were made public on Sunday on the Internet. The New York Times, The Guardian newspaper in London, and the German magazine Der Spiegel were given access to the material several weeks ago. These reports are used by desk officers in the Pentagon and troops in the field when they make operational plans and prepare briefings on the situation in the war zone..."

Further, regarding the source of the material The New York Times article relates:

"The documents — some 92,000 individual reports in all — were made available to The Times and the European news organizations by WikiLeaks, an organization devoted to exposing secrets of all kinds, on the condition that the papers not report on the data until July 25, when WikiLeaks said it intended to post the material on the Internet. WikiLeaks did not reveal where it obtained the material."

While the information reported by The New York Times identifies approximately 92,000 reports being disclosed, about 15,000 reports were not published by either the website WikiLeaks or the mentioned news media organizations due to this material believed to contain information more sensitive than in the published material. The New York Times article suggests information even more sensitive than the published Classified U.S. Government materials were obtained from WikiLeaks as the article further relates:

"We have, for example, withheld any names of operatives in the field and informants cited in the reports. We have avoided anything that might compromise American or allied intelligence-gathering methods such as communications intercepts."

The WikiLeaks website in regard to the 15,000 unpublished Classified U.S.

Government documents published on its website:

"We have delayed the release of some 15,000 reports from the total archive as part of a harm minimization process demanded by our source. After further review, these reports will be released, with occasional redactions, and eventually in full, as the security situation in Afghanistan permits."

Personnel associated with the website WikiLeaks have publicly acknowledged having other Classified U.S. Government material (which are believed to have been unlawfully disclosed by MANNING) such as the Gharani, Afghanistan airstrike video and associated report; however, for reasons unknown WikiLeaks has not published this material to the public.

MANNING's Unit Redeploys From Iraq to Fort Drum

During the month of August 2010, MANNING's unit began the process of redeploying from Iraq to Fort Drum after having completed the unit's tour of duty in Iraq. As part of this redeployment process MANNING's unit packed a specific U.S. Government Shipping Container (commonly referred to as a "Connex") with many of the unit's assigned 'Sensitive Items'. According to the DA Form 5748-R, Shipment Unit Packing List and Load Diagram, completed on August 18, 2010, by personnel assigned to MANNING's unit – this Shipping Container was packed with numerous U.S. Government: computers, of various makes and models; cryptological communication equipment; communication equipment; computer networking and peripheral hardware components; high security safes; miscellaneous paper and office supplies; office equipment; over 225 computer hard disk drives packed in boxes or with other equipment; as well as various other miscellaneous U.S. Government Property assigned to HHC, 2nd BCT, 10th Mountain Division. On these shipping documents it was further

noted that several of these U.S. Government computer systems and/or equipment was identified as being Classified systems or components.

This Shipping Container, further referred to by unit personnel as the unit's "Sensitive Items Connex", was reportedly securely sealed in accordance with U.S. Army and/or Department of Defense regulations for shipping containers of this nature and was transported under U.S. Government control from Iraq to the United States by sea freight, arriving at the U.S. Port of Beaumont, Texas, on September 6, 2010. This Shipping Container was further transported under U.S. Government control by truck from Beaumont, Texas to Fort Drum, and arrived at Fort Drum, New York on or about September 9, 2010. Upon the arrival of this Shipping Container at Fort Drum and its customary processing by the Fort Drum Transportation Office, the HHC, 2nd BCT unit command arranged for this container to be positioned within the HHC, 2nd BCT unit area. The unit Command further arranged for unit personnel to be on hand to assist USACIDC Special Agents in opening, identifying, inventorying, and preparing the identified computers and/or hard disk drives for examination – to determine if each may have been used by MANNING and/or be of evidentiary value to this investigation.

On September 10, 2010, USACIDC Special Agents from CCIU, under the authority of a Military Magistrate issued Search Authorization by CPT (b)(6)(b)(7)(C) Military Magistrate, B Company, Division Special Troops Battalion, 1st Armor Division, Camp Liberty, Iraq, searched the aforementioned connexes for the items mentioned. In addition to the computers and/or hard disk drives from the connex, additional sensitive items, to include computers and/or computer hard disk drives (similar to and/or identical to ones transported in the aforementioned connex) which had been hand-carried by

HHC, 2nd BCT unit members redeploying from Iraq back to Fort Drum, were also examined. These items had been placed into a Secured Storage Space, referred to as the "Unit Vault", within the Unit Area. Further, a second Shipping Container, identified as the "S-2 Connex" was also found to contain similar and/or identical computer equipment and/or digital media, although reportedly these items have been identified for processing 'Unclassified' information. All of the aforementioned connex and non-connex items were included as items to be searched/examined in the above mentioned Military Magistrate Search Authorization. Upon completion of the examination/search, several identified computers and/or hard disk drives were collected as evidence.

Additional Computers and/or Hard Disk Drives Identified

Upon USACIDC Special Agents returning to Fort Belvoir with computers and/or hard disk drives identified and collected at Fort Drum, it was determined one of the major items that was collected – which was related to the Server and/or Network Storage Space identified that MANNING utilized – needed to be physically connected to computers/servers at Fort Drum which were not believed to be of evidentiary value and were not collected as evidence, in order to conduct an examination of the other related items collected at Fort Drum. Due to this technical problem, on September 28, 2010, USACIDC Special Agents returned to Fort Drum with the collected evidence (related to the Server and/or Network Storage Space MANNING used) in order to physically

connect this item of evidence with other computers which had been deployed in Iraq; to complete the examination of the collected evidence.

During the completion of this technical/investigative effort, HHC, 2nd BCT, 10th Mountain Division personnel identified additional computer hard disk drives that had not been previously identified to USACIDC Special Agents in their previous examinations/ searches of connex items and other Information Technology equipment returned from Iraq and/or possibly used by MANNING. These previously unidentified items (which consisted of more computer hard disk drives) were found in a connex which had been located within a motor pool assigned to HHC, 2nd BCT. The hard disk drives were stored in a plastic portable 'Pelican' brand shipping container which was removed from the connex by Staff Sergeant (b)(6)(b)(7)(C), on September 30, 2010. (b)(6)(b)(7)(C) secured the container and its contents (hard disk drives) in the 2nd BCT Headquarters, located at 10200 North Riva Ridge Loop, Fort Drum, New York. It was noted that during the previous search of connexes and other locations by USACIDC Special Agents at Fort Drum on or about September 10, 2010, that HHC, 2nd BCT unit personnel who would have been more knowledgeable about the recently identified additional computer hard disk drives, were on block leave due to their deployment and were physically unavailable to assist investigators at that time.

On September 30, 2010, a Military Magistrate Search Authorization was issued by CPT (b)(6)(b)(7)(C) Military Magistrate, Office of the Staff Judge Advocate, Fort Belvoir, Virginia, for conducting a search of the additional items identified to USACIDC Special Agents which originated in the aforementioned connex identified in the 2nd BCT motor pool and were moved by TAUA to the the 2nd BCT Headquarters Building.

After obtaining this Military Magistrate Search Authorization on September 30, 2010, personnel assigned to 2nd BCT, 10th Mountain Division, while unpacking additional items in the S-2 Connex – previously identified by unit personnel as not containing any additional hard disk drives beyond those already identified to USACIDC Special Agents which were searched/examined on or about September 10, 2010 – found approximately fifty (50) additional hard disk drives. These hard drives were further removed from the S-2 Connex by 2nd BCT, 10th Mountain Division personnel who placed these drives in a 2nd BCT, 10th Mountain Division SCIF, located at 10200 North Riva Ridge Loop, Fort Drum, New York. These hard disk drives had apparently been placed in a container which was mislabeled and/or otherwise did not identify the contents as items USACIDC Special Agents would have examined during the September 10, 2010, search of the S-2 Connex.

On October 1, 2010, USACIDC Special Agents had Master Sergeant (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Non-Commissioned Officer in Charge (NCOIC) S-2 Section, HHC, 2nd BCT, 10th Mountain Division, identify which hard disk drives, out of the approximate fifty (50) additional hard drives found within the S-2 Connex, that could have been accessed by MANNING while in Iraq. (b)(6)(b)(7)(C) who had been deployed with MANNING and was his supervisor while in Iraq, subsequently identified approximately thirty (30) of the hard disk drives as potentially having been used by MANNING while he was in Iraq. These thirty (30) hard disk drives are currently stored in the 2nd BCT SCIF.

**Method of Examination of U.S. Government Computers by USACIDC Personnel
While at Fort Drum**

In an attempt to identify what previously unidentified computers MANNING may have used which are in possession of the U.S. Government, USACIDC Special Agents plan on: identifying all computer hard disk drives found in the above described location; they will then connect the hard disk drives using methods and procedures to forensically preserve any potential evidence on those drives, to forensic computers installed with commercially available computer forensic software. The USACIDC Special Agents will further attempt to determine by the inspection of the electronic file system contained on each hard disk drive as to whether a Windows User Profile related to MANNING's SIPR and/or NIPR network account(s) are present on the drive(s). Should a drive be found containing a Windows User Profile for MANNING, this will provide a strong indication this drive was once contained in or associated with a computer used by MANNING's network user account. Consequently these hard disk drive(s) will be seized, collected as evidence, and further computer forensic examination will be conducted to determine the drive's evidentiary value to this investigation as further described in Attachment C.

I have learned in my professional experience in conducting forensic examinations that intentional or unintentional data and information stored on hard disk drives and other digital media is highly persistent and may remain on digital media, computers, and computer-related devices nearly indefinitely without concerted efforts to purge or "wipe" this data by personnel with specialized tools and/or knowledge beyond the average computer user. More specifically when data is "Deleted" by a computer user, although this data may be no longer accessible to the computer user by normal means of the Operating System - this data is not removed from the digital media it was contained on necessarily, but the space this data occupies may simply be marked as available for

future data to be stored in its place by the Operating System. However, until overwritten by future data it may remain fully or partially intact and can provide further evidence of criminal violations or in some cases exculpatory evidence. Consequently, although considerable time has passed since MANNING may have accessed any computers and/or hard disk drives contained in the mentioned Shipping Container, the likelihood evidence related to MANNING's activities is still present should MANNING have used that given computer or hard disk drive is relatively high.

Requirement for Military Magistrate Search Authorization

While the aforementioned physical items USACIDC Special Agents wish to evaluate for potential evidence have been: identified as U.S. Government property and that no personal property has been identified as having been co-mingled into the identified items to be examined/searched; that the unit responsible for the property identified have consented to USACIDC Special Agents inspecting the items for evidence and are cooperating in this process – the information contained on items of digital media (such as hard disk drives) may still contain personal information, documents, electronic communications between third-parties associated or not associated with MANNING, who in various circumstances may still have a limited expectation to privacy to this information stored on these hard disk drives and/or digital media owned by the U.S. Government. Further, although USACIDC Special Agents will attempt to quickly evaluate each item of digital media for signs of its previous use by MANNING as a practical matter to facilitate the expeditious evaluation of a large number of items – in some cases inadvertent or unavoidable viewing of personal data, third-party communications, digital photographs, and/or other electronic information

which individuals, to include MANNING, may have limited privacy expectations to this data, may still occur. Further, the evaluation process mentioned herein, while minimally invasive, could be considered in a certain sense, a "search" in of itself, as the hard disk drives and/or digital media to be evaluated are not merely 'open containers' easily viewable without specialized computer forensic hardware, forensic software tools and training.

Upon the identification of any hard disk drives or digital media located in the place to be searched, as described in Attachment B, which are believed to have been previously used by MANNING, USACIDC Special Agents will seize and further search these identified digital media items for additional evidence, fruits and instrumentalities of violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information), in accordance with the procedures specified in Attachment C.

Conclusion

Given the facts and circumstances of the incidents related to the unlawful disclosure of Classified U.S. Government material by MANNING; the identification of Classified U.S. Government materials on MANNING's personal computer; the identification MANNING may have used other computers belonging to his unit to conduct his unlawful activities; that a hard disk drive(s) from MANNING's identified SIPR computer may have been replaced with other hard disk drives due to computer mechanical failures, and that these hard disk drives may still be in the possession of MANNING's former unit; that MANNING's assigned SIPR computer may have been

replaced with another U.S. Government computer containing a hard disk drive which may now be present as one of the identified hard disk drive present in the 2nd BCT SCIF; and that data and/or evidence on all of these items could reasonably still exist - there is probable cause to believe that additional evidence, fruits and instrumentalities of the offenses believed to have committed by MANNING to include violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information) are contained on hard disk drives present within computers and/or as stand-alone items within the identified SCIF located at 10200 North Riva Ridge Loop, Fort Drum, New York – and described in more detail in Attachment C.

ATTACHMENT B

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The following locations are to be searched (as explained in Attachment A): the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team (BCT), 10th Mountain Division, located at 10200 North Riva Ridge Loop, Fort Drum, New York.

ATTACHMENT C

ITEMS TO BE SEIZED AND SEARCHED

Special Agents of USACIDC or other Army law enforcement personnel assisting USACIDC to search the Sensitive Compartmented Information Facility, located at 10200 North Riva Ridge Loop, Fort Drum, New York, as described in Attachment B, and therein to seize and subsequently search all computer hardware and digital media, specifically hard disk drives, having been identified as associated with or previously used by Private First Class (PFC) Bradley Edward MANNING, formerly assigned to Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division – specifically as it relates to information, documents, and data, both classified and unclassified, as mentioned in Attachment A, which is herein incorporated into Attachment C, in regard to violations of 18 U.S.C. § 793(d) (Unlawfully Transmitting National Defense Information) and 18 U.S.C. § 1030 (Unlawfully Obtaining National Security Information).

The Computer Hardware and Digital Media is further described as any and all computer equipment including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data processing hardware, such as internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical disc storage devices such as CDs or DVDs, USB drives, flash memory cards or similar solid-state storage media, and other

memory storage devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

FURTHER SEARCH OF SEIZED COMPUTERS AND DIGITAL MEDIA ITEMS

The items seized as part of this Search Authorization, which should consist of hard disk drives, will have forensically sound images (digital copies) produced of the seized items as appropriate, which will in turn be searched in lieu of the original seized items as part of a digital media/computer forensic examination. The search of digital copies of the items seized is done to ensure and preserve the forensic integrity of the seized items for additional and/or future examination(s) in accordance with criminal procedure and rules of evidence. These examination(s) of seized items will be conducted by personnel assigned to the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) who are certified by the Department of Defense and/or Department of the Army to conduct such types of examinations. These personnel will use computer forensic hardware and/or software, which have been approved for use in conducting such examinations. Due to the unknown nature and/or number of items which could be seized within the scope of this Search Authorization, it is not necessarily practical or feasible to make forensically sound images (digital copies) of seized evidence while at the search location. Subsequently, these digital copies will be produced within a reasonable amount of time, unless extended by authorization of the Military Magistrate, with the originally seized items being returned to the owner of the property in accordance with Army Regulation 195-5, "Evidence Procedures". Further, due to the unknown number of items seized, as well as the complexity of examining these items, it is also not feasible to conduct a search/forensic examination

of the items while at the search location to determine their complete evidentiary value. Consequently, this search/examination activity will be completed within facilities operated by the U.S. Army Criminal Investigation Command and/or Computer Crime Investigative Unit (CCIU) and completed as expeditiously as possible.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0950, 1 Oct 10, SA (b)(6)(b)(7)(C) received the results from Department of Defense Inspector General (DOD/IG) Subpoena 2010247-10458, served on The Massachusetts Institute of Technology (MIT) for subscriber information for the following MIT Email accounts: unlocked@mit.edu and kaba-mas@mit.edu. The subpoena also requested disclosure of any MIT Email accounts used by Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) who were previously identified as potential co-conspirators of PFC MANNING.

The following information was provided by Ms. (b)(6)(b)(7)(C) Office of General Counsel, Massachusetts Institute of Technology:

The account Unlocked@mit.edu was created 8 May 2005. The account holder was Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C). The account was used for file storage and Email services. MIT did not provide any information regarding last login dates/time or associated Internet Protocol (IP) addresses.

The account holder for account (b)(6)(b)(7)(C)@mit.edu was (b)(6)(b)(7)(C) (b)(6)(b)(7)(C). No creation date was provided. The account was used as a mailing list maintained by Mr (b)(6)(b)(7)(C). MIT did not provide any information regarding the last login dates/time or associated IP addresses.

According to the results from MIT, Mr (b)(6)(b)(7)(C) had an Email account, (b)(6)(b)(7)(C)@mit.edu. The account was created 8 May 2005 and was registered to (b)(6)(b)(7)(C) (b)(6)(b)(7)(C). MIT did not provide any information regarding last login dates/time or associated IP addresses.

MIT could find no record of an Email account for Mr. (b)(6)(b)(7)(C). See results from MIT for further information. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b)(7)(E)		ORGANIZATION Washington Metro Resident Agency Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE SA. (b)(6)(b)(7)(C)	DATE 1 October 2010	EXHIBIT 231

Exhibit 232

Page(s) 001559 thru 001565 referred to:

Department of Defense
Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1835, 4 Oct 10, SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) (formerly SPC (b)(6)(b)(7)(C) assigned to Headquarters and Headquarters Company (HHC), 3rd Brigade Combat Team (BCT), 82nd Airborne Division, Fort Bragg, NC 28307) as he was identified as having been assigned with PFC MANNING during Basic Training at Fort Leonard Wood, MO and was also one of the soldiers PFC MANNING's unit replaced in Iraq about October 2009. Mr. (b)(6)(b)(7)(C) related PFC MANNING was in his Basic Training company and that PFC MANNING had a rough time in training. Mr. (b)(6)(b)(7)(C) related that in his opinion PFC MANNING seemed "mentally disturbed" and that PFC MANNING was sent out of his Basic Training unit to another unit as he did not appear to be mentally able to do the job of a soldier. Mr. (b)(6)(b)(7)(C) said he did not remember discussing soldiers that would be replacing his unit in Iraq, but explained he was surprised that PFC MANNING was in Iraq, as he did not think PFC MANNING would have still been in the U.S. Army at that point. Mr. (b)(6)(b)(7)(C) said he did not remember the incident related to PFC MANNING allegedly attempting to stab someone with a pencil while in Basic Training; but he believed SPC (b)(6)(b)(7)(C) who was assigned in the same platoon as PFC MANNING during Basic Training, would be better able to answer any questions about this reported incident. Mr. (b)(6)(b)(7)(C) could not immediately provide any additional information in regard to any incidents involving PFC MANNING while in Basic Training and did not have any information to provide in relation to PFC MANNING's activities in Iraq and/or any unlawful disclosure offenses allegedly committed by PFC MANNING.

AGENT'S COMMENT: Mr. (b)(6)(b)(7)(C) was identified as having been interviewed in CID Case 0326-10-CID023 (Fort Bragg CID Office) after having been identified as a subject of wrongful use of a controlled substance Tetrahydrocannabinol (THC) which was discovered from unit urinalysis test results on or about 29 Jun 10.

//////////////////// LAST ENTRY //////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b) (7)(E)		ORGANIZATION Washington Metro RA, Computer Crime Investigative Unit Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 4 Oct 10	EXHIBIT 233	

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0028-10-CID221-10117
0483-10-CID014-

PAGE 1 OF 1 PAGES

DETAIL

Basis For Investigation: About 1330, 5 Oct 10, this office received a Request For Assistance (RFA) from SA (b)(6)(b)(7)(C) Acting Special Agent in Charge, Computer Crime Investigative Unit (CCIU), Washington Metro resident Agency, 9805 Lowen Road, Building 193, Fort Belvoir, VA 22060-5598 (FBVA), requesting this office locate, identify, and conduct a victim/witness interview of SPC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) 501st Combat Support Battalion (CSB), 1st Brigade Combat Team (BCT), 1st Armor Division (AD), Fort Bliss, TX 79916 (FBTX), to determine if he was involved in the stabbing/attempted stabbing incident as described by SPC (b)(6)(b)(7)(C) B Company (CO), 717th Military Intelligence Battalion (MIBN), 470th Military Intelligence Brigade (MI BDE), Lackland Air Force Base, San Antonio, TX 78543 (LAFBSATX).

About 1510, 5 Oct 10, SA (b)(6)(b)(7)(C) coordinated with CIC, this office, to ascertain additional information pertaining to SPC (b)(6)(b)(7)(C). CIC was able to identify that SPC (b)(6)(b)(7)(C) was stationed at FBTX, but is presently deployed to Iraq with an expected return date of 17 Nov 10.

About 1530, 5 Oct 10, SA (b)(6)(b)(7)(C) briefed CPT (b)(6)(b)(7)(C) Rear Detachment (RD) Commander, 501st BSB, 1st BCT, 1st AD, FBTX, who confirmed SPC (b)(6)(b)(7)(C) was deployed to Forward Operating Base (FOB) Warrior, Kirkuk, Iraq. The contact number obtained for the unit (FORWARD) is 94-318-444-4352/3087. ///LAST ITEM///

TYPE AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Fort Bliss CID Office, P.O. Box 6350
Fort Bliss, TX 79916-6350

SIGNATURE

(b)(6)(b)(7)(C)

DATE

5 Oct 10

EXHIBIT

234

Exhibit(s) 235

Page(s) 001568 and 01568a withheld:

5 U.S.C. § 552(b)(1)

Permits withholding information that
is classified for
National Security purposes

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 2001, 7 Oct 10, SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) National Geospatial-Intelligence Agency (NGA), Aerospace Data Facility Colorado, 18201 E. Devils Thumb Avenue, Buckley Air Force Base, CO 80011 (formerly U.S. Air Force Technical Sergeant), as he was identified as a member of Cryptological Support Team 5 (CST5) and was assigned with PFC MANNING's unit in Iraq. Mr. (b)(6)(b)(7)(C) related he was assigned in Iraq from about 20 Jul 09 to 5 Jan 10. Mr. (b)(6)(b)(7)(C) said initially he was assigned with the 3rd Brigade Combat Team (BCT), 82nd Airborne Division and was based at Forward Operating Base (FOB) Loyalty, Iraq, until his team was redeployed to FOB Hammer around October 2009. Mr. (b)(6)(b)(7)(C) explained PFC MANNING's unit, the 2nd BCT, 10th Mountain Division arrived in Iraq sometime in October and replaced the 3rd BCT, 82nd Airborne Division at FOB Hammer. Mr. (b)(6)(b)(7)(C) stated the other personnel assigned to CST5 with him were: Ms. (b)(6)(b)(7)(C) MSgt (b)(6)(b)(7)(C) SrA (b)(6)(b)(7)(C) and SrA (b)(6)(b)(7)(C). Mr. (b)(6)(b)(7)(C) explained Mr. (b)(6)(b)(7)(C) also from NGA, was the person who relieved him in Iraq in January 2010, when his Iraq assignment ended. Mr. (b)(6)(b)(7)(C) said he remembered PFC MANNING as someone who seemed like a nice guy when dealing with him one-on-one, but also as someone who was unstable. Mr. (b)(6)(b)(7)(C) explained due to his physical location within the SCIF, on several occasions he remembered hearing PFC MANNING screaming about something while in the SCIF. Mr. (b)(6)(b)(7)(C) related because he did not work in direct proximity to PFC MANNING, but was in a partitioned area away from PFC MANNING within the SCIF, he could not determine what would cause PFC MANNING's outbursts and/or whether PFC MANNING may have been provoked by another unit member. Mr. (b)(6)(b)(7)(C) said he did not remember any incidents where personnel had said any derogatory remarks either directly to PFC MANNING or said things about PFC MANNING behind his back. Mr. (b)(6)(b)(7)(C) explained he was in the SCIF at the time PFC MANNING had some form of physical altercation/incident; however, Mr. (b)(6)(b)(7)(C) related he only heard the initial commotion, but by the time he was able to see anything due to his physical location within the SCIF, PFC MANNING had already been restrained by other personnel from PFC MANNING's unit. Mr. (b)(6)(b)(7)(C) could not provide any further details relating to the incident and said he did not remember any other incidents of a similar nature involving PFC MANNING. Mr. (b)(6)(b)(7)(C) said PFC MANNING was placed on the night shift and didn't believe PFC MANNING was given that much work to do. Mr. (b)(6)(b)(7)(C) said he believed this move of PFC MANNING to the night shift spoke to the level of confidence PFC MANNING's unit had in him; however, Mr. (b)(6)(b)(7)(C) said he did not work with PFC MANNING enough to make a complete judgment on PFC MANNING's abilities or proficiencies as an Intelligence Analyst. Mr. (b)(6)(b)(7)(C) said he did not know whether PFC MANNING had any friends within PFC MANNING's own unit and when directly asked whether PFC MANNING may have been friendly to any of the CST5 personnel, Mr. (b)(6)(b)(7)(C) said if he had to guess he believed PFC MANNING may have spoken with SrA (b)(6)(b)(7)(C) and/or MSgt (b)(6)(b)(7)(C) more than any of the other CST5 personnel. When asked how PFC MANNING may have seen imagery products PFC MANNING mentioned in chat conversations with Mr. (b)(6)(b)(7)(C). Mr. (b)(6)(b)(7)(C) said PFC MANNING could have seen this type of data from the NGA website which is on the Secure Internet Protocol Router (SIPR) network. Mr. (b)(6)(b)(7)(C) went on to explain various NGA imagery products can be viewed there and that he did not believe it required any type of login or account to access this imagery information. Mr. (b)(6)(b)(7)(C) said he could not remember any instances in which PFC MANNING requested data which

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

7 Oct 10

EXHIBIT

236

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001569

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

was outside the scope of PFC MANNING's duties of conducting analysis of targets in Iraq. Mr. (b)(6)(b)(7)(C) further said that he himself did not access anything unrelated to Iraq in regard to imagery or intelligence information. Mr. (b)(6)(b)(7)(C) explained in regard to the general security practices and/or Operational Security (OPSEC) conditions while in Iraq, that procedures were more relaxed than what could be expected in a CONUS-based SCIF environment. Mr. (b)(6)(b)(7)(C) specifically mentioned personnel playing video games, watching movies, and/or listening to music on computers within the SCIF. Mr. (b)(6)(b)(7)(C) mentioned Ms. (b)(6)(b)(7)(C) took issue with this and made attempts to curb the use of computers in the SCIF for non-approved uses. Mr. (b)(6)(b)(7)(C) reiterated several times that one of the biggest issues he saw in relation to security procedures in the SCIF was the lack of accountability for removable media. Mr. (b)(6)(b)(7)(C) said it was a common practice for information to be passed from CST5 personnel to the other 'organic' intelligence analysts on optical media (Compact Discs and/or DVDs) and there was not accountability for all of this removable media. Mr. (b)(6)(b)(7)(C) remarked that someone could have easily exfiltrated data from the SCIF due to this practice. Mr. (b)(6)(b)(7)(C) explained this situation would not occur in a CONUS-based SCIF environment due to the operational/organizational structure that was set up in Iraq which had an emphasis on getting the mission accomplished. Mr. (b)(6)(b)(7)(C) related there were no JWICS terminals in the SCIF during the time he was assigned to FOB Hammer and that the only access to JWICS would have been through the National Security Agency Network (NSANET). Mr. (b)(6)(b)(7)(C) explained it was possible to connect to JWICS by a Virtual Private Network (VPN) type connection; but that to do this personnel would need to have both an NSANET account as well as would have had to request VPN access. Mr. (b)(6)(b)(7)(C) said only the CST5 personnel as well as the organic Signals Intelligence (SIGINT) personnel would have had NSANET accounts to his knowledge. Mr. (b)(6)(b)(7)(C) when asked about the '9/11 Pager Messages' mentioned by PFC MANNING in Internet chat conversations with Mr. (b)(6)(b)(7)(C) said he had no knowledge of this. Mr. (b)(6)(b)(7)(C) said he became aware of the allegations against PFC MANNING when he was contacted by SrA (b)(6)(b)(7)(C) on Facebook this past summer (Summer 2010) with a message related to PFC MANNING and/or media stories about this incident. Mr. (b)(6)(b)(7)(C) related he became aware of the website WikiLeaks when this website released the 2007 Iraq Apache video (April 2010). Mr. (b)(6)(b)(7)(C) could not immediately provide any additional information related to this investigation or PFC MANNING.

AGENT'S COMMENT: It was noted after the interview that Mr. (b)(6)(b)(7)(C) appeared to know about the incident involving PFC MANNING assaulting another soldier in his unit in which PFC MANNING was demoted from Specialist to Private First Class; and that Mr. (b)(6)(b)(7)(C) believed this was the incident he was present for in the SCIF. However, this known incident in which PFC MANNING assaulted SPC (b)(6)(b)(7)(C) occurred around May 2010, and Mr. (b)(6)(b)(7)(C) had already completed his assignment in Iraq in January 2010. Mr. (b)(6)(b)(7)(C) explained by the time he was able to visually see what was occurring during the incident he mentioned PFC MANNING being involved in, PFC MANNING was already restrained by a male soldier. It is believed the incident Mr. (b)(6)(b)(7)(C) was referring to was another altercation wherein PFC MANNING pushed over a table in the SCIF containing a computer and was restrained and ejected from the SCIF by other unit members.

//////////////////// **LAST ENTRY** //////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b) (7)(E)		ORGANIZATION Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)		DATE 7 Oct 10	EXHIBIT 236

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Between 1140 - 1510, 10 Oct 10, SA (b)(6)(b)(7)(C) recorded PFC MANNING's visitation period at the Marine Corps Brig - Quantico, Quantico, VA 22134. Upon completion of the visitation period, SA (b)(6)(b)(7)(C) was informed by brig personnel that PFC MANNING was visited by Mr. (b)(6)(b)(7)(C)

About 1143, 12 Oct 10, SA (b)(6)(b)(7)(C) collected as evidence one compact disc (CD) which captured the recording of PFC MANNING's 10 Oct 10 visitation period at the Marine Corps Brig - Quantico. The collection of evidence was documented on DA Form 4137, Evidence/Property Custody Document (EPCD), Document Number (DN) 148-10.

Between 1200 - 1610, 12 Oct 10, SA (b)(6)(b)(7)(C) reviewed the digitally recorded conversation between PFC MANNING and Mr. (b)(6)(b)(7)(C) which took place on 10 Oct 10. PFC MANNING requested Mr. (b)(6)(b)(7)(C) make contact with a Mr. (b)(6)(b)(7)(C) (NFI) on his behalf and solicit assistance in raising funds for his defense.

//////////////////////////////////////LAST ENTRY//////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

12 Oct 10

EXHIBIT

237

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001571

Approved

(b)(6)(b)(7)(C)

Exhibit(s) 238

Page(s) 001572 and 01572a withheld:

5 U.S.C. § 552(b)(1)

Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 239

Page(s) 001573 and 001574 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0750, 12 Oct 10, SA (b)(6)(b)(7)(C) received the results from Department of Defense Inspector General (DOD/IG) Subpoena 2010279-10510, served on the custodian of records at Yahoo, Inc, for subscriber information regarding the email account whoeverwhereever@yahoo.com .Yahoo provided the following results:

Internal reference number: 160327

The email account whoeverwhereever@yahoo.com was created on Wednesday, 6 Feb 2002 at 01:33:49 GMT.

Registered name: Mr. who ever

Address: (no street name given), (b)(6)(b)(7)(C)

Internet Protocol (IP) address at registration: 64.196.93.138

(This IP address was registered to PaeTec Communications, Inc. One PAETEC Plaza, 600 Willowbrook Office Park, Fairport, NY 14450).

No secondary email address was provided during registration.

Yahoo also provided a Microsoft Excel spreadsheet detailing the login dates, times and the recorded IP addresses of the user accessing the account from 1 Sep 09 though 14 Aug 10. SA (b)(6)(b)(7)(C) reviewed the provided data and found a total of 252 logins from IP addresses 199.208.239.140 and 199.208.239.141, registered to the US Department of Defense Information Network. Yahoo further stated that they could find no account registered under the name (b)(6)(b)(7)(C) See results from Yahoo for further information. ///LAST ENTRY///.

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION Washington Metro Resident Agency
Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGN

(b)(6)(b)(7)(C)

DATE

14 Oct 10

EXHIBIT

240

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001575
Approved

(b)(6)(b)(7)(C)

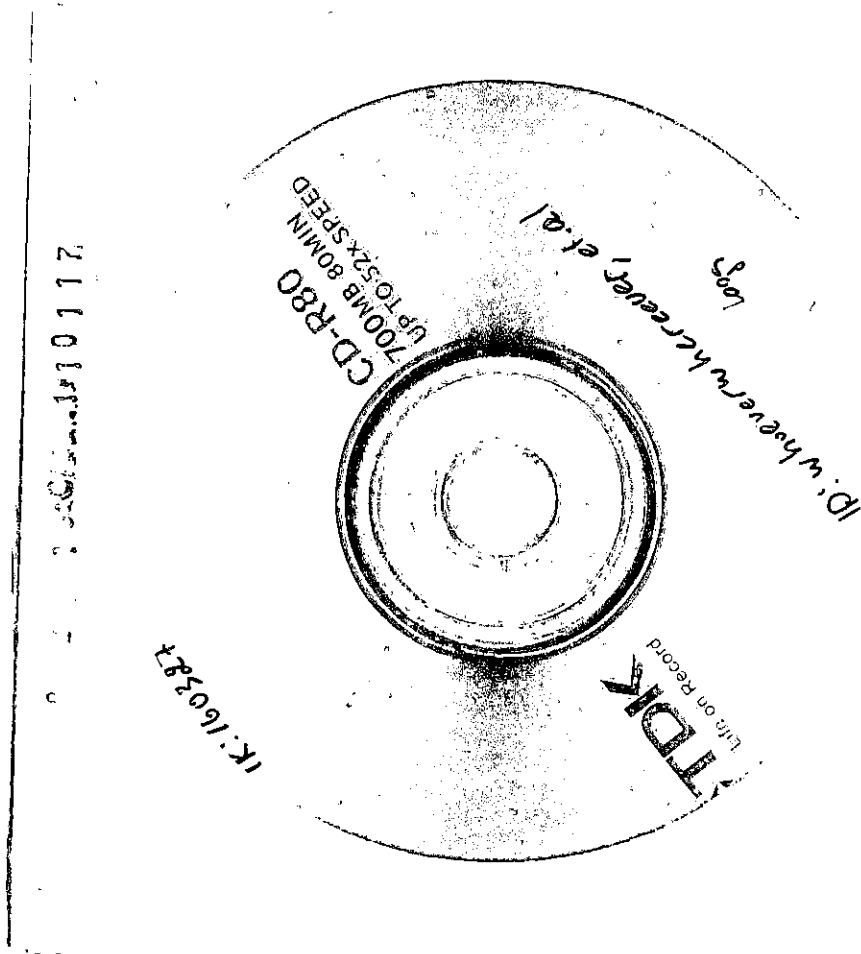
Exhibit 241

Page(s) 001576 thru 001595 referred to:

Department of Defense
Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

Subpoena Results

whoeverwhereever@yahoo.com



FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 242
001596

Search for whoeverwhereever

Date Range 21-Sep-2009 00:00:00 / 23-Aug-2010 23:59:59

Total Results 635

Yahoo ID IP Address Login Time

whoeverwl 71.191.26.1 Sun 10:56:41 (GMT) 22-Aug-2010
whoeverwl 71.191.26.1 Sat 14:50:14 (GMT) 21-Aug-2010
whoeverwl 71.191.26.1 Sat 14:40:41 (GMT) 21-Aug-2010
whoeverwl 71.191.26.1 Sat 13:29:37 (GMT) 21-Aug-2010
whoeverwl 71.191.26.1 Sat 11:15:40 (GMT) 21-Aug-2010
whoeverwl 71.178.108 Thu 09:37:52 (GMT) 19-Aug-2010
whoeverwl 199.208.23 Wed 17:16:28 (GMT) 18-Aug-2010
whoeverwl 199.208.23 Tue 12:28:41 (GMT) 17-Aug-2010
whoeverwl 71.191.22.1 Mon 21:02:07 (GMT) 16-Aug-2010
whoeverwl 71.191.22.1 Sun 17:03:38 (GMT) 15-Aug-2010
whoeverwl 71.191.22.1 Sun 16:04:03 (GMT) 15-Aug-2010
whoeverwl 71.191.22.1 Sat 12:07:14 (GMT) 14-Aug-2010
whoeverwl 71.191.22.1 Thu 21:17:32 (GMT) 12-Aug-2010
whoeverwl 71.191.22.1 Tue 00:46:40 (GMT) 10-Aug-2010
whoeverwl 71.191.22.1 Sun 17:41:32 (GMT) 08-Aug-2010
whoeverwl 71.191.22.1 Sat 13:19:13 (GMT) 07-Aug-2010
whoeverwl 199.208.23 Thu 18:45:27 (GMT) 05-Aug-2010
whoeverwl 71.191.22.1 Wed 16:50:16 (GMT) 04-Aug-2010
whoeverwl 71.163.233 Tue 21:33:54 (GMT) 03-Aug-2010
whoeverwl 199.208.23 Tue 13:09:54 (GMT) 03-Aug-2010
whoeverwl 96.231.81.1 Tue 03:56:19 (GMT) 03-Aug-2010
whoeverwl 96.231.81.1 Mon 05:05:31 (GMT) 02-Aug-2010
whoeverwl 12.192.13.1 Fri 16:25:30 (GMT) 30-Jul-2010
whoeverwl 12.192.13.1 Thu 20:55:35 (GMT) 29-Jul-2010
whoeverwl 12.192.13.1 Wed 19:59:19 (GMT) 28-Jul-2010
whoeverwl 71.191.25.1 Tue 14:30:14 (GMT) 27-Jul-2010
whoeverwl 71.163.232 Tue 11:13:18 (GMT) 27-Jul-2010
whoeverwl 71.191.24.1 Mon 18:01:58 (GMT) 26-Jul-2010
whoeverwl 71.191.24.1 Mon 17:22:37 (GMT) 26-Jul-2010
whoeverwl 71.191.30.1 Mon 13:38:16 (GMT) 26-Jul-2010
whoeverwl 71.178.116 Sun 16:10:07 (GMT) 25-Jul-2010
whoeverwl 71.178.116 Sun 16:02:35 (GMT) 25-Jul-2010
whoeverwl 71.178.116 Sun 15:07:07 (GMT) 25-Jul-2010
whoeverwl 71.178.116 Sun 13:15:11 (GMT) 25-Jul-2010
whoeverwl 98.247.169 Fri 06:31:51 (GMT) 23-Jul-2010
whoeverwl 98.247.169 Thu 20:50:48 (GMT) 22-Jul-2010
whoeverwl 98.247.169 Thu 19:11:31 (GMT) 22-Jul-2010
whoeverwl 98.247.169 Thu 07:04:46 (GMT) 22-Jul-2010
whoeverwl 71.217.32.1 Wed 04:57:57 (GMT) 21-Jul-2010
whoeverwl 199.208.23 Fri 15:58:34 (GMT) 16-Jul-2010
whoeverwl 199.208.23 Thu 12:22:53 (GMT) 15-Jul-2010

whoeverwl 71.191.31.: Tue 23:33:00 (GMT) 13-Jul-2010
whoeverwl 199.208.23 Tue 15:41:34 (GMT) 13-Jul-2010
whoeverwl 199.208.23 Tue 13:20:48 (GMT) 13-Jul-2010
whoeverwl 71.191.16.: Tue 09:42:28 (GMT) 13-Jul-2010
whoeverwl 71.178.107 Mon 23:02:21 (GMT) 12-Jul-2010
whoeverwl 199.208.23 Mon 17:49:02 (GMT) 12-Jul-2010
whoeverwl 71.163.226 Mon 02:02:56 (GMT) 12-Jul-2010
whoeverwl 71.163.226 Sun 15:09:57 (GMT) 11-Jul-2010
whoeverwl 71.163.226 Sat 20:05:45 (GMT) 10-Jul-2010
whoeverwl 199.208.23 Fri 14:55:22 (GMT) 09-Jul-2010
whoeverwl 96.231.76.: Thu 09:48:21 (GMT) 08-Jul-2010
whoeverwl 199.208.23 Wed 17:40:53 (GMT) 07-Jul-2010
whoeverwl 199.208.23 Tue 16:05:20 (GMT) 06-Jul-2010
whoeverwl 204.212.13 Sun 14:37:37 (GMT) 04-Jul-2010
whoeverwl 204.212.13 Sun 12:24:10 (GMT) 04-Jul-2010
whoeverwl 204.212.13 Sat 03:47:30 (GMT) 03-Jul-2010
whoeverwl 204.212.13 Sat 01:00:20 (GMT) 03-Jul-2010
whoeverwl 71.191.24.: Fri 13:44:11 (GMT) 02-Jul-2010
whoeverwl 71.191.24.: Fri 12:50:21 (GMT) 02-Jul-2010
whoeverwl 71.191.24.: Fri 11:53:16 (GMT) 02-Jul-2010
whoeverwl 199.208.23 Thu 16:07:49 (GMT) 01-Jul-2010
whoeverwl 199.208.23 Wed 15:11:34 (GMT) 30-Jun-2010
whoeverwl 199.208.23 Tue 14:39:01 (GMT) 29-Jun-2010
whoeverwl 199.208.23 Mon 12:09:46 (GMT) 28-Jun-2010
whoeverwl 71.178.113 Mon 03:36:42 (GMT) 28-Jun-2010
whoeverwl 71.178.113 Sun 16:01:22 (GMT) 27-Jun-2010
whoeverwl 96.231.79.: Sat 13:12:49 (GMT) 26-Jun-2010
whoeverwl 199.208.23 Fri 15:34:28 (GMT) 25-Jun-2010
whoeverwl 199.208.23 Thu 19:54:34 (GMT) 24-Jun-2010
whoeverwl 199.208.23 Thu 17:24:54 (GMT) 24-Jun-2010
whoeverwl 199.208.23 Thu 12:47:03 (GMT) 24-Jun-2010
whoeverwl 199.208.23 Tue 18:36:11 (GMT) 22-Jun-2010
whoeverwl 199.208.23 Tue 14:45:01 (GMT) 22-Jun-2010
whoeverwl 199.208.23 Mon 14:12:52 (GMT) 21-Jun-2010
whoeverwl 71.178.105 Mon 00:36:28 (GMT) 21-Jun-2010
whoeverwl 204.212.13 Sun 13:16:08 (GMT) 20-Jun-2010
whoeverwl 204.212.13 Fri 19:19:33 (GMT) 18-Jun-2010
whoeverwl 204.212.13 Fri 17:19:28 (GMT) 18-Jun-2010
whoeverwl 204.212.13 Thu 21:34:47 (GMT) 17-Jun-2010
whoeverwl 204.212.13 Thu 17:07:10 (GMT) 17-Jun-2010
whoeverwl 70.63.78.2 Wed 04:38:37 (GMT) 16-Jun-2010
whoeverwl 199.208.23 Tue 12:46:34 (GMT) 15-Jun-2010
whoeverwl 96.231.68.: Mon 09:16:18 (GMT) 14-Jun-2010
whoeverwl 96.231.68.: Sun 16:08:58 (GMT) 13-Jun-2010
whoeverwl 71.178.104 Sun 11:15:56 (GMT) 13-Jun-2010
whoeverwl 71.191.18.: Sat 14:25:05 (GMT) 12-Jun-2010
whoeverwl 71.191.18.: Sat 12:52:22 (GMT) 12-Jun-2010

whoeverwl 71.191.18.: Sat 11:51:57 (GMT) 12-Jun-2010
whoeverwl 71.191.18.: Sat 11:43:05 (GMT) 12-Jun-2010
whoeverwl 128.82.41.: Fri 11:32:42 (GMT) 11-Jun-2010
whoeverwl 68.115.176 Fri 01:03:24 (GMT) 11-Jun-2010
whoeverwl 68.115.176 Thu 22:15:29 (GMT) 10-Jun-2010
whoeverwl 68.115.176 Thu 19:28:28 (GMT) 10-Jun-2010
whoeverwl 68.115.176 Thu 10:10:29 (GMT) 10-Jun-2010
whoeverwl 68.115.176 Wed 20:05:22 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Wed 15:57:22 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Wed 13:22:49 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Wed 11:15:54 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Tue 22:21:53 (GMT) 08-Jun-2010
whoeverwl 68.115.176 Tue 10:04:30 (GMT) 08-Jun-2010
whoeverwl 71.178.110 Sun 15:45:44 (GMT) 06-Jun-2010
whoeverwl 71.178.110 Sun 14:16:08 (GMT) 06-Jun-2010
whoeverwl 71.178.110 Sun 13:38:29 (GMT) 06-Jun-2010
whoeverwl 71.178.110 Sun 13:23:52 (GMT) 06-Jun-2010
whoeverwl 71.191.28.: Sat 14:48:02 (GMT) 05-Jun-2010
whoeverwl 71.191.28.: Sat 11:54:35 (GMT) 05-Jun-2010
whoeverwl 199.208.23 Fri 15:42:29 (GMT) 04-Jun-2010
whoeverwl 199.208.23 Fri 13:01:00 (GMT) 04-Jun-2010
whoeverwl 71.163.236 Thu 21:58:15 (GMT) 03-Jun-2010
whoeverwl 71.163.236 Thu 21:13:52 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 19:48:37 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 19:04:18 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 16:05:21 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 11:39:47 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Wed 18:18:00 (GMT) 02-Jun-2010
whoeverwl 199.208.23 Wed 14:50:19 (GMT) 02-Jun-2010
whoeverwl 199.208.23 Wed 12:11:36 (GMT) 02-Jun-2010
whoeverwl 71.191.31.: Tue 21:14:36 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 16:16:50 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 14:57:46 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 14:21:19 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 13:27:35 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 12:03:37 (GMT) 01-Jun-2010
whoeverwl 204.212.13 Sun 18:00:29 (GMT) 30-May-2010
whoeverwl 204.212.13 Sun 13:44:18 (GMT) 30-May-2010
whoeverwl 204.212.13 Sat 13:52:59 (GMT) 29-May-2010
whoeverwl 204.212.13 Fri 22:58:05 (GMT) 28-May-2010
whoeverwl 71.191.31.: Fri 13:55:53 (GMT) 28-May-2010
whoeverwl 71.191.31.: Fri 12:01:45 (GMT) 28-May-2010
whoeverwl 71.191.20.: Fri 03:49:09 (GMT) 28-May-2010
whoeverwl 199.208.23 Thu 19:19:11 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 15:16:49 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 14:09:18 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 13:07:51 (GMT) 27-May-2010

whoeverwl 199.208.23 Thu 11:46:25 (GMT) 27-May-2010
whoeverwl 199.208.23 Wed 15:03:01 (GMT) 26-May-2010
whoeverwl 199.208.23 Wed 10:46:59 (GMT) 26-May-2010
whoeverwl 199.208.23 Tue 17:08:10 (GMT) 25-May-2010
whoeverwl 199.208.23 Tue 12:08:27 (GMT) 25-May-2010
whoeverwl 199.208.23 Mon 12:16:29 (GMT) 24-May-2010
whoeverwl 71.178.108 Sun 20:00:15 (GMT) 23-May-2010
whoeverwl 71.178.108 Sun 14:42:27 (GMT) 23-May-2010
whoeverwl 96.241.135 Sat 13:40:19 (GMT) 22-May-2010
whoeverwl 199.208.23 Fri 16:13:47 (GMT) 21-May-2010
whoeverwl 199.208.23 Fri 12:48:09 (GMT) 21-May-2010
whoeverwl 71.163.229 Thu 21:15:40 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 19:19:24 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 17:56:40 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 16:39:40 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 16:15:29 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 14:39:48 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 11:56:47 (GMT) 20-May-2010
whoeverwl 71.191.24.: Thu 00:18:45 (GMT) 20-May-2010
whoeverwl 71.191.24.: Wed 20:55:32 (GMT) 19-May-2010
whoeverwl 71.178.106 Wed 00:49:32 (GMT) 19-May-2010
whoeverwl 199.208.23 Tue 12:34:06 (GMT) 18-May-2010
whoeverwl 71.178.108 Tue 09:50:58 (GMT) 18-May-2010
whoeverwl 96.241.128 Tue 00:24:51 (GMT) 18-May-2010
whoeverwl 96.241.128 Tue 00:24:51 (GMT) 18-May-2010
whoeverwl 71.191.21.: Mon 21:59:56 (GMT) 17-May-2010
whoeverwl 199.208.23 Mon 18:53:20 (GMT) 17-May-2010
whoeverwl 199.208.23 Mon 11:55:55 (GMT) 17-May-2010
whoeverwl 71.191.21.: Mon 03:13:53 (GMT) 17-May-2010
whoeverwl 71.178.103 Sun 18:31:50 (GMT) 16-May-2010
whoeverwl 71.178.103 Sun 15:50:04 (GMT) 16-May-2010
whoeverwl 71.178.103 Sun 15:22:27 (GMT) 16-May-2010
whoeverwl 96.241.129 Sat 15:37:31 (GMT) 15-May-2010
whoeverwl 199.208.23 Fri 16:56:31 (GMT) 14-May-2010
whoeverwl 199.208.23 Fri 12:21:03 (GMT) 14-May-2010
whoeverwl 71.178.108 Thu 13:12:12 (GMT) 13-May-2010
whoeverwl 71.178.108 Thu 12:09:40 (GMT) 13-May-2010
whoeverwl 199.208.23 Wed 18:34:28 (GMT) 12-May-2010
whoeverwl 199.208.23 Wed 13:22:06 (GMT) 12-May-2010
whoeverwl 96.231.75.: Wed 10:57:37 (GMT) 12-May-2010
whoeverwl 199.208.23 Tue 18:42:49 (GMT) 11-May-2010
whoeverwl 199.208.23 Tue 12:48:11 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 09:47:17 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 02:16:30 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 00:30:33 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 00:13:30 (GMT) 11-May-2010
whoeverwl 96.231.75.: Mon 23:30:53 (GMT) 10-May-2010

whoeverwl 199.208.23 Mon 18:39:07 (GMT) 10-May-2010
whoeverwl 199.208.23 Mon 15:20:50 (GMT) 10-May-2010
whoeverwl 199.208.23 Mon 12:15:09 (GMT) 10-May-2010
whoeverwl 71.191.26.: Sun 19:33:37 (GMT) 09-May-2010
whoeverwl 71.191.26.: Sun 14:41:47 (GMT) 09-May-2010
whoeverwl 71.191.26.: Sun 12:18:19 (GMT) 09-May-2010
whoeverwl 71.191.26.: Sat 18:43:55 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 18:36:24 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 17:31:10 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 13:10:44 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 10:51:42 (GMT) 08-May-2010
whoeverwl 199.208.23 Fri 12:09:00 (GMT) 07-May-2010
whoeverwl 96.231.74.: Fri 01:55:52 (GMT) 07-May-2010
whoeverwl 199.208.23 Thu 17:22:30 (GMT) 06-May-2010
whoeverwl 199.208.23 Thu 11:58:43 (GMT) 06-May-2010
whoeverwl 71.178.104 Wed 21:30:50 (GMT) 05-May-2010
whoeverwl 199.208.23 Wed 12:53:56 (GMT) 05-May-2010
whoeverwl 71.163.234 Wed 09:47:29 (GMT) 05-May-2010
whoeverwl 96.231.68.: Tue 14:02:17 (GMT) 04-May-2010
whoeverwl 96.231.68.: Tue 12:05:04 (GMT) 04-May-2010
whoeverwl 199.208.23 Mon 14:42:45 (GMT) 03-May-2010
whoeverwl 199.208.23 Mon 12:28:47 (GMT) 03-May-2010
whoeverwl 96.231.79.: Sun 11:56:26 (GMT) 02-May-2010
whoeverwl 96.231.79.: Sun 09:59:28 (GMT) 02-May-2010
whoeverwl 71.178.112 Sat 13:42:12 (GMT) 01-May-2010
whoeverwl 71.178.112 Sat 10:30:44 (GMT) 01-May-2010
whoeverwl 199.208.23 Fri 18:16:03 (GMT) 30-Apr-2010
whoeverwl 71.178.115 Thu 21:59:18 (GMT) 29-Apr-2010
whoeverwl 199.208.23 Thu 11:52:48 (GMT) 29-Apr-2010
whoeverwl 71.191.29.: Thu 00:26:05 (GMT) 29-Apr-2010
whoeverwl 71.191.29.: Wed 21:51:29 (GMT) 28-Apr-2010
whoeverwl 199.208.23 Tue 12:06:46 (GMT) 27-Apr-2010
whoeverwl 199.208.23 Mon 12:03:47 (GMT) 26-Apr-2010
whoeverwl 71.191.16.: Sun 16:29:41 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 16:29:41 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 15:20:02 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 14:57:02 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 14:11:37 (GMT) 25-Apr-2010
whoeverwl 96.231.79.: Sat 13:29:47 (GMT) 24-Apr-2010
whoeverwl 199.208.23 Fri 12:04:43 (GMT) 23-Apr-2010
whoeverwl 199.208.23 Tue 14:10:12 (GMT) 20-Apr-2010
whoeverwl 71.178.115 Tue 00:53:25 (GMT) 20-Apr-2010
whoeverwl 71.178.115 Mon 20:38:13 (GMT) 19-Apr-2010
whoeverwl 199.208.23 Mon 12:48:30 (GMT) 19-Apr-2010
whoeverwl 71.178.115 Sun 13:14:28 (GMT) 18-Apr-2010
whoeverwl 71.178.115 Sun 12:29:55 (GMT) 18-Apr-2010
whoeverwl 71.178.115 Sat 13:27:00 (GMT) 17-Apr-2010

whoeverwl 71.178.115 Sat 11:15:32 (GMT) 17-Apr-2010
whoeverwl 199.208.23 Fri 12:32:05 (GMT) 16-Apr-2010
whoeverwl 71.178.115 Thu 16:05:26 (GMT) 15-Apr-2010
whoeverwl 199.208.23 Thu 12:13:58 (GMT) 15-Apr-2010
whoeverwl 199.208.23 Wed 18:33:53 (GMT) 14-Apr-2010
whoeverwl 199.208.23 Wed 14:34:25 (GMT) 14-Apr-2010
whoeverwl 71.178.115 Tue 23:15:05 (GMT) 13-Apr-2010
whoeverwl 71.178.115 Tue 22:57:42 (GMT) 13-Apr-2010
whoeverwl 199.208.23 Tue 18:01:20 (GMT) 13-Apr-2010
whoeverwl 199.208.23 Tue 15:01:15 (GMT) 13-Apr-2010
whoeverwl 71.178.115 Tue 09:22:20 (GMT) 13-Apr-2010
whoeverwl 71.178.115 Mon 23:59:51 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 19:34:43 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 17:58:03 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 15:21:54 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 12:57:40 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 11:51:14 (GMT) 12-Apr-2010
whoeverwl 71.178.115 Mon 08:49:01 (GMT) 12-Apr-2010
whoeverwl 71.178.115 Sun 15:56:10 (GMT) 11-Apr-2010
whoeverwl 71.178.115 Sat 11:01:08 (GMT) 10-Apr-2010
whoeverwl 96.241.132 Fri 15:38:42 (GMT) 09-Apr-2010
whoeverwl 199.208.23 Thu 12:29:00 (GMT) 08-Apr-2010
whoeverwl 199.208.23 Wed 12:26:59 (GMT) 07-Apr-2010
whoeverwl 12.53.175. Mon 21:18:09 (GMT) 05-Apr-2010
whoeverwl 71.178.113 Sun 20:57:53 (GMT) 04-Apr-2010
whoeverwl 71.178.113 Sun 14:36:24 (GMT) 04-Apr-2010
whoeverwl 71.178.113 Sat 14:30:04 (GMT) 03-Apr-2010
whoeverwl 199.208.23 Fri 15:29:33 (GMT) 02-Apr-2010
whoeverwl 199.208.23 Fri 13:17:48 (GMT) 02-Apr-2010
whoeverwl 199.208.23 Fri 13:12:40 (GMT) 02-Apr-2010
whoeverwl 199.208.23 Thu 16:48:29 (GMT) 01-Apr-2010
whoeverwl 199.208.23 Wed 13:01:27 (GMT) 31-Mar-2010
whoeverwl 199.208.23 Tue 20:16:14 (GMT) 30-Mar-2010
whoeverwl 199.208.23 Tue 12:11:55 (GMT) 30-Mar-2010
whoeverwl 199.208.23 Mon 12:09:26 (GMT) 29-Mar-2010
whoeverwl 71.178.113 Mon 09:55:15 (GMT) 29-Mar-2010
whoeverwl 71.178.112 Sun 18:03:57 (GMT) 28-Mar-2010
whoeverwl 71.178.112 Sun 15:06:05 (GMT) 28-Mar-2010
whoeverwl 71.178.112 Sat 16:19:35 (GMT) 27-Mar-2010
whoeverwl 71.178.112 Sat 14:55:50 (GMT) 27-Mar-2010
whoeverwl 199.208.23 Fri 18:40:05 (GMT) 26-Mar-2010
whoeverwl 199.208.23 Fri 12:15:57 (GMT) 26-Mar-2010
whoeverwl 96.231.68. Fri 01:53:21 (GMT) 26-Mar-2010
whoeverwl 96.241.136 Thu 20:47:17 (GMT) 25-Mar-2010
whoeverwl 71.178.105 Thu 18:44:00 (GMT) 25-Mar-2010
whoeverwl 199.208.23 Thu 17:23:47 (GMT) 25-Mar-2010
whoeverwl 199.208.23 Thu 13:21:55 (GMT) 25-Mar-2010

whoeverwl 71.163.235 Thu 00:35:59 (GMT) 25-Mar-2010
whoeverwl 71.178.114 Wed 11:56:32 (GMT) 24-Mar-2010
whoeverwl 96.231.76.: Tue 21:28:03 (GMT) 23-Mar-2010
whoeverwl 199.208.23 Tue 15:34:45 (GMT) 23-Mar-2010
whoeverwl 199.208.23 Tue 12:46:17 (GMT) 23-Mar-2010
whoeverwl 199.208.23 Mon 19:36:29 (GMT) 22-Mar-2010
whoeverwl 199.208.23 Mon 16:57:10 (GMT) 22-Mar-2010
whoeverwl 199.208.23 Mon 14:16:35 (GMT) 22-Mar-2010
whoeverwl 199.208.23 Mon 12:08:46 (GMT) 22-Mar-2010
whoeverwl 71.163.234 Sun 17:20:59 (GMT) 21-Mar-2010
whoeverwl 71.163.234 Sun 10:56:19 (GMT) 21-Mar-2010
whoeverwl 96.231.78.: Sat 12:17:06 (GMT) 20-Mar-2010
whoeverwl 199.208.23 Fri 14:42:07 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Fri 13:17:20 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Fri 13:02:38 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Fri 12:24:47 (GMT) 19-Mar-2010
whoeverwl 71.191.18.: Fri 09:59:42 (GMT) 19-Mar-2010
whoeverwl 71.191.18.: Fri 08:31:38 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Thu 19:38:34 (GMT) 18-Mar-2010
whoeverwl 71.178.108 Thu 08:15:35 (GMT) 18-Mar-2010
whoeverwl 71.178.108 Wed 21:17:12 (GMT) 17-Mar-2010
whoeverwl 199.208.23 Wed 18:26:30 (GMT) 17-Mar-2010
whoeverwl 199.208.23 Tue 16:21:37 (GMT) 16-Mar-2010
whoeverwl 199.208.23 Tue 13:59:03 (GMT) 16-Mar-2010
whoeverwl 199.208.23 Tue 12:10:56 (GMT) 16-Mar-2010
whoeverwl 199.208.23 Mon 19:24:51 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 16:39:01 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 14:57:36 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 14:08:45 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 13:01:41 (GMT) 15-Mar-2010
whoeverwl 71.163.233 Sat 18:31:06 (GMT) 13-Mar-2010
whoeverwl 199.208.23 Fri 14:46:06 (GMT) 12-Mar-2010
whoeverwl 199.208.23 Mon 16:36:29 (GMT) 08-Mar-2010
whoeverwl 138.88.16.: Sat 12:29:53 (GMT) 06-Mar-2010
whoeverwl 199.208.23 Fri 14:09:22 (GMT) 05-Mar-2010
whoeverwl 199.208.23 Thu 19:50:08 (GMT) 04-Mar-2010
whoeverwl 141.156.21 Thu 12:34:14 (GMT) 04-Mar-2010
whoeverwl 199.208.23 Wed 15:10:20 (GMT) 03-Mar-2010
whoeverwl 141.156.43 Wed 09:50:19 (GMT) 03-Mar-2010
whoeverwl 199.208.23 Tue 17:01:00 (GMT) 02-Mar-2010
whoeverwl 199.208.23 Tue 13:35:16 (GMT) 02-Mar-2010
whoeverwl 141.156.25 Tue 02:38:42 (GMT) 02-Mar-2010
whoeverwl 138.88.245 Sun 12:11:29 (GMT) 28-Feb-2010
whoeverwl 12.70.195.: Sat 00:54:52 (GMT) 27-Feb-2010
whoeverwl 12.70.195.: Fri 15:36:50 (GMT) 26-Feb-2010
whoeverwl 12.70.195.: Fri 14:12:35 (GMT) 26-Feb-2010
whoeverwl 12.70.195.: Thu 21:35:46 (GMT) 25-Feb-2010

whoeverwl 12.70.195.(Thu 17:32:20 (GMT) 25-Feb-2010
whoeverwl 12.70.195.(Thu 11:47:13 (GMT) 25-Feb-2010
whoeverwl 12.70.195.(Wed 10:40:20 (GMT) 24-Feb-2010
whoeverwl 12.70.195.(Tue 19:42:48 (GMT) 23-Feb-2010
whoeverwl 12.70.195.(Tue 12:15:40 (GMT) 23-Feb-2010
whoeverwl 12.70.195.(Mon 23:45:15 (GMT) 22-Feb-2010
whoeverwl 12.70.195.(Mon 04:26:19 (GMT) 22-Feb-2010
whoeverwl 70.155.177 Sat 22:52:42 (GMT) 20-Feb-2010
whoeverwl 206.113.11 Tue 22:35:04 (GMT) 16-Feb-2010
whoeverwl 206.113.11 Mon 22:08:58 (GMT) 15-Feb-2010
whoeverwl 206.113.11 Mon 22:08:14 (GMT) 15-Feb-2010
whoeverwl 71.166.227 Thu 13:46:54 (GMT) 11-Feb-2010
whoeverwl 71.166.227 Wed 19:11:43 (GMT) 10-Feb-2010
whoeverwl 71.166.227 Wed 11:33:44 (GMT) 10-Feb-2010
whoeverwl 71.166.227 Wed 10:31:27 (GMT) 10-Feb-2010
whoeverwl 138.88.241 Tue 12:03:52 (GMT) 09-Feb-2010
whoeverwl 138.88.200 Mon 18:24:11 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Mon 14:44:29 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Mon 13:57:19 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Mon 01:49:17 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Sun 20:09:54 (GMT) 07-Feb-2010
whoeverwl 138.88.218 Sun 14:50:13 (GMT) 07-Feb-2010
whoeverwl 138.88.218 Sat 15:21:18 (GMT) 06-Feb-2010
whoeverwl 138.88.255 Fri 22:48:08 (GMT) 05-Feb-2010
whoeverwl 138.88.255 Fri 21:12:19 (GMT) 05-Feb-2010
whoeverwl 141.156.19 Fri 17:51:26 (GMT) 05-Feb-2010
whoeverwl 138.88.221 Fri 00:18:32 (GMT) 05-Feb-2010
whoeverwl 138.88.221 Thu 22:37:32 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 20:03:30 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 19:11:07 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 17:35:25 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 16:29:08 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 15:21:11 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 12:58:18 (GMT) 04-Feb-2010
whoeverwl 141.156.25 Wed 21:15:20 (GMT) 03-Feb-2010
whoeverwl 141.156.43 Wed 12:09:17 (GMT) 03-Feb-2010
whoeverwl 141.156.43 Wed 10:45:55 (GMT) 03-Feb-2010
whoeverwl 199.208.23 Tue 20:22:10 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 20:08:10 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 18:26:09 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 17:40:26 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 15:55:39 (GMT) 02-Feb-2010
whoeverwl 141.156.43 Tue 10:50:59 (GMT) 02-Feb-2010
whoeverwl 141.156.43 Mon 22:52:35 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 20:21:18 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 19:36:27 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 17:53:54 (GMT) 01-Feb-2010

whoeverwl 199.208.23 Mon 16:23:58 (GMT) 01-Feb-2010
whoeverwl 141.156.37 Sun 22:48:16 (GMT) 31-Jan-2010
whoeverwl 141.156.37 Sun 14:31:35 (GMT) 31-Jan-2010
whoeverwl 141.156.37 Sat 14:42:43 (GMT) 30-Jan-2010
whoeverwl 199.208.23 Fri 14:23:33 (GMT) 29-Jan-2010
whoeverwl 138.88.230 Fri 01:24:37 (GMT) 29-Jan-2010
whoeverwl 199.208.23 Thu 20:50:08 (GMT) 28-Jan-2010
whoeverwl 199.208.23 Thu 12:53:28 (GMT) 28-Jan-2010
whoeverwl 138.88.211 Wed 21:27:15 (GMT) 27-Jan-2010
whoeverwl 199.208.23 Wed 13:25:43 (GMT) 27-Jan-2010
whoeverwl 199.208.23 Tue 13:20:42 (GMT) 26-Jan-2010
whoeverwl 199.208.23 Mon 13:19:45 (GMT) 25-Jan-2010
whoeverwl 138.88.253 Sun 12:50:47 (GMT) 24-Jan-2010
whoeverwl 199.208.23 Fri 13:12:28 (GMT) 22-Jan-2010
whoeverwl 138.88.16.: Fri 10:08:06 (GMT) 22-Jan-2010
whoeverwl 199.208.23 Thu 15:05:32 (GMT) 21-Jan-2010
whoeverwl 199.208.23 Wed 18:29:27 (GMT) 20-Jan-2010
whoeverwl 199.208.23 Tue 20:20:32 (GMT) 19-Jan-2010
whoeverwl 199.208.23 Tue 13:46:18 (GMT) 19-Jan-2010
whoeverwl 141.156.39 Mon 13:11:31 (GMT) 18-Jan-2010
whoeverwl 138.88.226 Sun 17:06:01 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 15:46:32 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 13:36:57 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 12:25:25 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 12:24:38 (GMT) 17-Jan-2010
whoeverwl 199.208.23 Fri 12:38:14 (GMT) 15-Jan-2010
whoeverwl 199.208.23 Thu 20:11:36 (GMT) 14-Jan-2010
whoeverwl 141.156.24 Thu 03:11:23 (GMT) 14-Jan-2010
whoeverwl 138.88.235 Wed 01:34:10 (GMT) 13-Jan-2010
whoeverwl 138.88.235 Tue 01:31:38 (GMT) 12-Jan-2010
whoeverwl 138.88.235 Tue 01:26:48 (GMT) 12-Jan-2010
whoeverwl 138.88.235 Tue 00:57:33 (GMT) 12-Jan-2010
whoeverwl 138.88.246 Sun 15:50:47 (GMT) 10-Jan-2010
whoeverwl 138.88.246 Sun 14:18:48 (GMT) 10-Jan-2010
whoeverwl 138.88.246 Sat 13:55:33 (GMT) 09-Jan-2010
whoeverwl 138.88.246 Sat 11:55:37 (GMT) 09-Jan-2010
whoeverwl 199.208.23 Thu 13:13:36 (GMT) 07-Jan-2010
whoeverwl 199.208.23 Wed 14:44:46 (GMT) 06-Jan-2010
whoeverwl 199.208.23 Mon 18:26:00 (GMT) 04-Jan-2010
whoeverwl 138.88.209 Mon 09:32:04 (GMT) 04-Jan-2010
whoeverwl 138.88.209 Mon 01:39:55 (GMT) 04-Jan-2010
whoeverwl 138.88.209 Sun 15:09:57 (GMT) 03-Jan-2010
whoeverwl 138.88.209 Sun 13:21:04 (GMT) 03-Jan-2010
whoeverwl 138.88.240 Sat 11:50:53 (GMT) 02-Jan-2010
whoeverwl 138.88.240 Sat 09:45:33 (GMT) 02-Jan-2010
whoeverwl 138.88.240 Sat 01:52:44 (GMT) 02-Jan-2010
whoeverwl 138.88.240 Thu 09:53:53 (GMT) 31-Dec-2009

whoeverwl 138.88.204 Wed 14:22:30 (GMT) 30-Dec-2009
whoeverwl 199.208.23 Tue 18:08:00 (GMT) 29-Dec-2009
whoeverwl 199.208.23 Tue 15:54:37 (GMT) 29-Dec-2009
whoeverwl 199.208.23 Tue 13:06:22 (GMT) 29-Dec-2009
whoeverwl 199.208.23 Mon 17:39:04 (GMT) 28-Dec-2009
whoeverwl 199.208.23 Mon 13:50:30 (GMT) 28-Dec-2009
whoeverwl 141.156.34 Sun 17:37:40 (GMT) 27-Dec-2009
whoeverwl 141.156.24 Sat 18:26:32 (GMT) 26-Dec-2009
whoeverwl 141.156.24 Sat 14:39:44 (GMT) 26-Dec-2009
whoeverwl 141.156.24 Sat 03:01:11 (GMT) 26-Dec-2009
whoeverwl 141.156.24 Thu 12:43:38 (GMT) 24-Dec-2009
whoeverwl 141.156.24 Wed 20:03:31 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 19:33:27 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 18:30:01 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 17:49:10 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 16:22:47 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 14:25:03 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 12:28:01 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Tue 21:23:34 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 18:17:10 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 17:57:21 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 17:43:11 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 17:16:35 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 13:43:27 (GMT) 22-Dec-2009
whoeverwl 141.156.24 Mon 11:19:43 (GMT) 21-Dec-2009
whoeverwl 141.156.24 Mon 09:40:47 (GMT) 21-Dec-2009
whoeverwl 138.88.229 Sun 15:58:10 (GMT) 20-Dec-2009
whoeverwl 138.88.229 Sun 11:13:19 (GMT) 20-Dec-2009
whoeverwl 138.88.222 Sat 11:58:28 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 11:58:01 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 11:47:55 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 10:33:44 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 09:33:44 (GMT) 19-Dec-2009
whoeverwl 199.208.23 Fri 18:20:30 (GMT) 18-Dec-2009
whoeverwl 199.208.23 Fri 13:32:08 (GMT) 18-Dec-2009
whoeverwl 199.208.23 Thu 12:36:06 (GMT) 17-Dec-2009
whoeverwl 138.88.218 Thu 09:20:11 (GMT) 17-Dec-2009
whoeverwl 138.88.218 Thu 02:06:14 (GMT) 17-Dec-2009
whoeverwl 138.88.218 Thu 01:13:49 (GMT) 17-Dec-2009
whoeverwl 199.208.23 Wed 19:33:13 (GMT) 16-Dec-2009
whoeverwl 138.88.218 Wed 10:11:47 (GMT) 16-Dec-2009
whoeverwl 138.88.218 Tue 17:06:52 (GMT) 15-Dec-2009
whoeverwl 199.208.23 Tue 12:53:42 (GMT) 15-Dec-2009
whoeverwl 138.88.218 Mon 22:25:52 (GMT) 14-Dec-2009
whoeverwl 199.208.23 Mon 13:42:46 (GMT) 14-Dec-2009
whoeverwl 138.88.218 Sun 19:40:28 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sun 16:28:10 (GMT) 13-Dec-2009

whoeverwl 138.88.218 Sun 15:16:59 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sun 12:24:12 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sat 18:23:22 (GMT) 12-Dec-2009
whoeverwl 138.88.218 Sat 12:06:31 (GMT) 12-Dec-2009
whoeverwl 199.208.23 Fri 13:20:13 (GMT) 11-Dec-2009
whoeverwl 141.156.22 Fri 10:18:11 (GMT) 11-Dec-2009
whoeverwl 138.88.195 Thu 01:50:04 (GMT) 10-Dec-2009
whoeverwl 138.88.195 Wed 23:39:47 (GMT) 09-Dec-2009
whoeverwl 199.208.23 Fri 18:31:00 (GMT) 04-Dec-2009
whoeverwl 199.208.23 Fri 12:51:53 (GMT) 04-Dec-2009
whoeverwl 199.208.23 Wed 16:20:35 (GMT) 02-Dec-2009
whoeverwl 199.208.23 Wed 13:22:03 (GMT) 02-Dec-2009
whoeverwl 199.208.23 Tue 14:51:35 (GMT) 01-Dec-2009
whoeverwl 138.88.224 Tue 01:33:49 (GMT) 01-Dec-2009
whoeverwl 199.208.23 Mon 13:21:01 (GMT) 30-Nov-2009
whoeverwl 138.88.224 Mon 03:38:58 (GMT) 30-Nov-2009
whoeverwl 138.88.224 Sat 16:30:43 (GMT) 28-Nov-2009
whoeverwl 138.88.224 Thu 14:01:49 (GMT) 26-Nov-2009
whoeverwl 138.88.224 Wed 01:04:47 (GMT) 25-Nov-2009
whoeverwl 138.88.224 Tue 01:56:02 (GMT) 24-Nov-2009
whoeverwl 199.208.23 Mon 14:37:06 (GMT) 23-Nov-2009
whoeverwl 138.88.224 Sun 11:35:19 (GMT) 22-Nov-2009
whoeverwl 138.88.224 Sat 13:07:35 (GMT) 21-Nov-2009
whoeverwl 138.88.224 Sat 11:57:12 (GMT) 21-Nov-2009
whoeverwl 195.145.13 Thu 23:49:46 (GMT) 19-Nov-2009
whoeverwl 195.145.13 Thu 08:17:23 (GMT) 19-Nov-2009
whoeverwl 195.145.13 Wed 12:02:00 (GMT) 18-Nov-2009
whoeverwl 195.145.13 Tue 21:28:48 (GMT) 17-Nov-2009
whoeverwl 195.145.13 Tue 20:22:50 (GMT) 17-Nov-2009
whoeverwl 195.145.13 Mon 17:02:59 (GMT) 16-Nov-2009
whoeverwl 195.145.13 Mon 11:51:09 (GMT) 16-Nov-2009
whoeverwl 195.145.13 Sun 16:51:21 (GMT) 15-Nov-2009
whoeverwl 138.88.51.: Sat 13:12:24 (GMT) 14-Nov-2009
whoeverwl 138.88.51.: Sat 04:53:40 (GMT) 14-Nov-2009
whoeverwl 199.208.23 Fri 13:51:43 (GMT) 13-Nov-2009
whoeverwl 138.88.51.: Thu 23:51:26 (GMT) 12-Nov-2009
whoeverwl 199.208.23 Thu 12:44:15 (GMT) 12-Nov-2009
whoeverwl 138.88.51.: Wed 12:26:06 (GMT) 11-Nov-2009
whoeverwl 138.88.51.: Wed 05:56:34 (GMT) 11-Nov-2009
whoeverwl 199.208.23 Tue 13:57:12 (GMT) 10-Nov-2009
whoeverwl 199.208.23 Mon 13:13:02 (GMT) 09-Nov-2009
whoeverwl 138.88.119 Sun 15:33:03 (GMT) 08-Nov-2009
whoeverwl 138.88.119 Sun 12:31:41 (GMT) 08-Nov-2009
whoeverwl 138.88.119 Sat 13:07:50 (GMT) 07-Nov-2009
whoeverwl 199.208.23 Fri 13:50:56 (GMT) 06-Nov-2009
whoeverwl 141.156.22 Fri 01:29:04 (GMT) 06-Nov-2009
whoeverwl 141.156.15 Thu 02:22:43 (GMT) 05-Nov-2009

whoeverwl 199.208.23 Wed 17:43:11 (GMT) 04-Nov-2009
whoeverwl 199.208.23 Tue 18:01:51 (GMT) 03-Nov-2009
whoeverwl 199.208.23 Tue 15:42:36 (GMT) 03-Nov-2009
whoeverwl 199.208.23 Tue 13:05:20 (GMT) 03-Nov-2009
whoeverwl 138.88.199 Tue 01:33:24 (GMT) 03-Nov-2009
whoeverwl 199.208.23 Mon 20:19:06 (GMT) 02-Nov-2009
whoeverwl 199.208.23 Mon 17:55:11 (GMT) 02-Nov-2009
whoeverwl 199.208.23 Mon 13:39:52 (GMT) 02-Nov-2009
whoeverwl 138.88.249 Sun 18:14:18 (GMT) 01-Nov-2009
whoeverwl 138.88.249 Sun 17:00:52 (GMT) 01-Nov-2009
whoeverwl 141.156.25 Sun 12:44:13 (GMT) 01-Nov-2009
whoeverwl 141.156.25 Sat 12:32:58 (GMT) 31-Oct-2009
whoeverwl 141.156.25 Sat 12:04:22 (GMT) 31-Oct-2009
whoeverwl 138.88.16.: Fri 11:37:04 (GMT) 30-Oct-2009
whoeverwl 199.208.23 Thu 18:06:05 (GMT) 29-Oct-2009
whoeverwl 199.208.23 Thu 12:34:23 (GMT) 29-Oct-2009
whoeverwl 199.208.23 Wed 17:38:42 (GMT) 28-Oct-2009
whoeverwl 199.208.23 Wed 12:25:53 (GMT) 28-Oct-2009
whoeverwl 141.156.22 Tue 21:56:58 (GMT) 27-Oct-2009
whoeverwl 141.156.23 Tue 20:46:38 (GMT) 27-Oct-2009
whoeverwl 138.88.228 Tue 11:44:20 (GMT) 27-Oct-2009
whoeverwl 138.88.228 Tue 02:47:57 (GMT) 27-Oct-2009
whoeverwl 199.208.23 Mon 19:30:16 (GMT) 26-Oct-2009
whoeverwl 199.208.23 Mon 15:28:46 (GMT) 26-Oct-2009
whoeverwl 199.208.23 Mon 12:06:01 (GMT) 26-Oct-2009
whoeverwl 138.88.245 Mon 02:41:03 (GMT) 26-Oct-2009
whoeverwl 138.88.245 Sat 14:20:35 (GMT) 24-Oct-2009
whoeverwl 138.88.245 Sat 12:51:19 (GMT) 24-Oct-2009
whoeverwl 199.208.23 Fri 18:16:32 (GMT) 23-Oct-2009
whoeverwl 199.208.23 Fri 11:39:07 (GMT) 23-Oct-2009
whoeverwl 138.88.105 Thu 19:26:22 (GMT) 22-Oct-2009
whoeverwl 199.208.23 Thu 12:26:38 (GMT) 22-Oct-2009
whoeverwl 199.208.23 Wed 19:15:47 (GMT) 21-Oct-2009
whoeverwl 199.208.23 Wed 12:34:33 (GMT) 21-Oct-2009
whoeverwl 141.156.25 Wed 01:22:45 (GMT) 21-Oct-2009
whoeverwl 199.208.23 Tue 12:47:36 (GMT) 20-Oct-2009
whoeverwl 138.88.224 Mon 20:25:36 (GMT) 19-Oct-2009
whoeverwl 199.208.23 Mon 12:53:41 (GMT) 19-Oct-2009
whoeverwl 138.88.251 Sun 16:50:59 (GMT) 18-Oct-2009
whoeverwl 138.88.251 Sun 14:58:53 (GMT) 18-Oct-2009
whoeverwl 138.88.251 Sun 13:26:38 (GMT) 18-Oct-2009
whoeverwl 138.88.212 Sun 00:23:28 (GMT) 18-Oct-2009
whoeverwl 138.88.212 Sat 17:07:15 (GMT) 17-Oct-2009
whoeverwl 138.88.212 Sat 06:52:34 (GMT) 17-Oct-2009
whoeverwl 138.88.198 Sat 00:00:18 (GMT) 17-Oct-2009
whoeverwl 138.88.198 Fri 21:23:49 (GMT) 16-Oct-2009
whoeverwl 199.208.23 Fri 12:43:02 (GMT) 16-Oct-2009

whoeverwl 138.88.89.: Thu 20:46:53 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Thu 10:15:17 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Thu 02:54:18 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Thu 00:22:22 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Wed 22:03:52 (GMT) 14-Oct-2009
whoeverwl 199.208.23 Wed 11:40:53 (GMT) 14-Oct-2009
whoeverwl 138.88.89.: Wed 00:48:27 (GMT) 14-Oct-2009
whoeverwl 138.88.89.: Wed 00:48:04 (GMT) 14-Oct-2009
whoeverwl 199.208.23 Tue 20:16:54 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 18:49:37 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 17:01:13 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 15:01:56 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 11:53:36 (GMT) 13-Oct-2009
whoeverwl 138.88.89.: Mon 23:28:03 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Mon 20:14:18 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Mon 13:09:43 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Mon 12:39:02 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Sun 13:59:54 (GMT) 11-Oct-2009
whoeverwl 138.88.89.: Sun 11:36:29 (GMT) 11-Oct-2009
whoeverwl 138.88.89.: Sat 10:55:45 (GMT) 10-Oct-2009
whoeverwl 138.88.89.: Fri 21:06:53 (GMT) 09-Oct-2009
whoeverwl 199.208.23 Fri 17:15:56 (GMT) 09-Oct-2009
whoeverwl 199.208.23 Fri 12:08:10 (GMT) 09-Oct-2009
whoeverwl 199.208.23 Thu 17:10:01 (GMT) 08-Oct-2009
whoeverwl 199.208.23 Thu 12:58:59 (GMT) 08-Oct-2009
whoeverwl 199.208.23 Wed 11:54:36 (GMT) 07-Oct-2009
whoeverwl 138.88.89.: Tue 21:34:29 (GMT) 06-Oct-2009
whoeverwl 199.208.23 Tue 12:13:24 (GMT) 06-Oct-2009
whoeverwl 138.88.238 Tue 00:43:01 (GMT) 06-Oct-2009
whoeverwl 138.88.238 Tue 00:18:00 (GMT) 06-Oct-2009
whoeverwl 199.208.23 Mon 12:47:05 (GMT) 05-Oct-2009
whoeverwl 138.88.214 Sun 19:54:01 (GMT) 04-Oct-2009
whoeverwl 138.88.214 Sun 14:38:36 (GMT) 04-Oct-2009
whoeverwl 138.88.48.: Sat 12:40:33 (GMT) 03-Oct-2009
whoeverwl 138.88.48.: Sat 12:22:23 (GMT) 03-Oct-2009
whoeverwl 199.208.23 Fri 18:53:08 (GMT) 02-Oct-2009
whoeverwl 199.208.23 Fri 13:47:37 (GMT) 02-Oct-2009
whoeverwl 138.88.122 Fri 03:06:38 (GMT) 02-Oct-2009
whoeverwl 199.208.23 Thu 18:55:59 (GMT) 01-Oct-2009
whoeverwl 199.208.23 Thu 16:30:02 (GMT) 01-Oct-2009
whoeverwl 199.208.23 Thu 12:46:46 (GMT) 01-Oct-2009
whoeverwl 199.208.23 Wed 18:22:59 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Wed 16:57:48 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Wed 15:23:43 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Wed 12:21:14 (GMT) 30-Sep-2009
whoeverwl 138.88.105 Wed 01:53:56 (GMT) 30-Sep-2009
whoeverwl 138.88.105 Wed 01:42:18 (GMT) 30-Sep-2009

whoeverwl 199.208.23 Tue 16:35:53 (GMT) 29-Sep-2009
whoeverwl 141.156.39 Tue 01:10:21 (GMT) 29-Sep-2009
whoeverwl 138.88.232 Mon 23:11:37 (GMT) 28-Sep-2009
whoeverwl 199.208.23 Mon 19:23:11 (GMT) 28-Sep-2009
whoeverwl 199.208.23 Mon 11:39:59 (GMT) 28-Sep-2009
whoeverwl 138.88.122 Sun 13:16:14 (GMT) 27-Sep-2009
whoeverwl 138.88.122 Sun 09:49:34 (GMT) 27-Sep-2009
whoeverwl 138.88.122 Sun 03:24:51 (GMT) 27-Sep-2009
whoeverwl 138.88.122 Sat 17:12:50 (GMT) 26-Sep-2009
whoeverwl 138.88.122 Sat 14:06:34 (GMT) 26-Sep-2009
whoeverwl 138.88.122 Sat 13:42:36 (GMT) 26-Sep-2009
whoeverwl 138.88.122 Sat 04:31:07 (GMT) 26-Sep-2009
whoeverwl 138.88.206 Fri 14:38:10 (GMT) 25-Sep-2009
whoeverwl 138.88.206 Fri 13:31:57 (GMT) 25-Sep-2009
whoeverwl 138.88.206 Fri 12:53:56 (GMT) 25-Sep-2009
whoeverwl 138.88.201 Thu 14:35:56 (GMT) 24-Sep-2009
whoeverwl 138.88.201 Thu 10:58:38 (GMT) 24-Sep-2009
whoeverwl 138.88.201 Thu 02:14:32 (GMT) 24-Sep-2009
whoeverwl 141.156.25 Wed 17:14:24 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 13:56:50 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 12:58:58 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 12:50:07 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 11:38:29 (GMT) 23-Sep-2009
whoeverwl 138.88.222 Tue 19:22:15 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 12:44:41 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 11:30:22 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 10:52:34 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 03:13:14 (GMT) 22-Sep-2009
whoeverwl 138.88.255 Mon 14:07:28 (GMT) 21-Sep-2009
whoeverwl 138.88.255 Mon 11:35:40 (GMT) 21-Sep-2009

Search for whoeverwhereever

Date Range 01-Sep-2009 00:00:00 / 14-Aug-2010 23:59:59

Total Results 674

Yahoo ID IP Address Login Time

whoeverwl 71.191.22.: Sat 12:07:14 (GMT) 14-Aug-2010
whoeverwl 71.191.22.: Thu 21:17:32 (GMT) 12-Aug-2010
whoeverwl 71.191.22.: Tue 00:46:40 (GMT) 10-Aug-2010
whoeverwl 71.191.22.: Sun 17:41:32 (GMT) 08-Aug-2010
whoeverwl 71.191.22.: Sat 13:19:13 (GMT) 07-Aug-2010
whoeverwl 199.208.23 Thu 18:45:27 (GMT) 05-Aug-2010
whoeverwl 71.191.22.: Wed 16:50:16 (GMT) 04-Aug-2010
whoeverwl 71.163.233 Tue 21:33:54 (GMT) 03-Aug-2010
whoeverwl 199.208.23 Tue 13:09:54 (GMT) 03-Aug-2010
whoeverwl 96.231.81.: Tue 03:56:19 (GMT) 03-Aug-2010
whoeverwl 96.231.81.: Mon 05:05:31 (GMT) 02-Aug-2010
whoeverwl 12.192.13.: Fri 16:25:30 (GMT) 30-Jul-2010
whoeverwl 12.192.13.: Thu 20:55:35 (GMT) 29-Jul-2010
whoeverwl 12.192.13.: Wed 19:59:19 (GMT) 28-Jul-2010
whoeverwl 71.191.25.: Tue 14:30:14 (GMT) 27-Jul-2010
whoeverwl 71.163.232 Tue 11:13:18 (GMT) 27-Jul-2010
whoeverwl 71.191.24.: Mon 18:01:58 (GMT) 26-Jul-2010
whoeverwl 71.191.24.: Mon 17:22:37 (GMT) 26-Jul-2010
whoeverwl 71.191.30.: Mon 13:38:16 (GMT) 26-Jul-2010
whoeverwl 71.178.116 Sun 16:10:07 (GMT) 25-Jul-2010
whoeverwl 71.178.116 Sun 16:02:35 (GMT) 25-Jul-2010
whoeverwl 71.178.116 Sun 15:07:07 (GMT) 25-Jul-2010
whoeverwl 71.178.116 Sun 13:15:11 (GMT) 25-Jul-2010
whoeverwl 98.247.169 Fri 06:31:51 (GMT) 23-Jul-2010
whoeverwl 98.247.169 Thu 20:50:48 (GMT) 22-Jul-2010
whoeverwl 98.247.169 Thu 19:11:31 (GMT) 22-Jul-2010
whoeverwl 98.247.169 Thu 07:04:46 (GMT) 22-Jul-2010
whoeverwl 71.217.32.: Wed 04:57:57 (GMT) 21-Jul-2010
whoeverwl 199.208.23 Fri 15:58:34 (GMT) 16-Jul-2010
whoeverwl 199.208.23 Thu 12:22:53 (GMT) 15-Jul-2010
whoeverwl 71.191.31.: Tue 23:33:00 (GMT) 13-Jul-2010
whoeverwl 199.208.23 Tue 15:41:34 (GMT) 13-Jul-2010
whoeverwl 199.208.23 Tue 13:20:48 (GMT) 13-Jul-2010
whoeverwl 71.191.16.: Tue 09:42:28 (GMT) 13-Jul-2010
whoeverwl 71.178.107 Mon 23:02:21 (GMT) 12-Jul-2010
whoeverwl 199.208.23 Mon 17:49:02 (GMT) 12-Jul-2010
whoeverwl 71.163.226 Mon 02:02:56 (GMT) 12-Jul-2010
whoeverwl 71.163.226 Sun 15:09:57 (GMT) 11-Jul-2010
whoeverwl 71.163.226 Sat 20:05:45 (GMT) 10-Jul-2010
whoeverwl 199.208.23 Fri 14:55:22 (GMT) 09-Jul-2010
whoeverwl 96.231.76.: Thu 09:48:21 (GMT) 08-Jul-2010

whoeverwl 199.208.23 Wed 17:40:53 (GMT) 07-Jul-2010
whoeverwl 199.208.23 Tue 16:05:20 (GMT) 06-Jul-2010
whoeverwl 204.212.13 Sun 14:37:37 (GMT) 04-Jul-2010
whoeverwl 204.212.13 Sun 12:24:10 (GMT) 04-Jul-2010
whoeverwl 204.212.13 Sat 03:47:30 (GMT) 03-Jul-2010
whoeverwl 204.212.13 Sat 01:00:20 (GMT) 03-Jul-2010
whoeverwl 71.191.24.: Fri 13:44:11 (GMT) 02-Jul-2010
whoeverwl 71.191.24.: Fri 12:50:21 (GMT) 02-Jul-2010
whoeverwl 71.191.24.: Fri 11:53:16 (GMT) 02-Jul-2010
whoeverwl 199.208.23 Thu 16:07:49 (GMT) 01-Jul-2010
whoeverwl 199.208.23 Wed 15:11:34 (GMT) 30-Jun-2010
whoeverwl 199.208.23 Tue 14:39:01 (GMT) 29-Jun-2010
whoeverwl 199.208.23 Mon 12:09:46 (GMT) 28-Jun-2010
whoeverwl 71.178.113 Mon 03:36:42 (GMT) 28-Jun-2010
whoeverwl 71.178.113 Sun 16:01:22 (GMT) 27-Jun-2010
whoeverwl 96.231.79.: Sat 13:12:49 (GMT) 26-Jun-2010
whoeverwl 199.208.23 Fri 15:34:28 (GMT) 25-Jun-2010
whoeverwl 199.208.23 Thu 19:54:34 (GMT) 24-Jun-2010
whoeverwl 199.208.23 Thu 17:24:54 (GMT) 24-Jun-2010
whoeverwl 199.208.23 Thu 12:47:03 (GMT) 24-Jun-2010
whoeverwl 199.208.23 Tue 18:36:11 (GMT) 22-Jun-2010
whoeverwl 199.208.23 Tue 14:45:01 (GMT) 22-Jun-2010
whoeverwl 199.208.23 Mon 14:12:52 (GMT) 21-Jun-2010
whoeverwl 71.178.105 Mon 00:36:28 (GMT) 21-Jun-2010
whoeverwl 204.212.13 Sun 13:16:08 (GMT) 20-Jun-2010
whoeverwl 204.212.13 Fri 19:19:33 (GMT) 18-Jun-2010
whoeverwl 204.212.13 Fri 17:19:28 (GMT) 18-Jun-2010
whoeverwl 204.212.13 Thu 21:34:47 (GMT) 17-Jun-2010
whoeverwl 204.212.13 Thu 17:07:10 (GMT) 17-Jun-2010
whoeverwl 70.63.78.2 Wed 04:38:37 (GMT) 16-Jun-2010
whoeverwl 199.208.23 Tue 12:46:34 (GMT) 15-Jun-2010
whoeverwl 96.231.68.: Mon 09:16:18 (GMT) 14-Jun-2010
whoeverwl 96.231.68.: Sun 16:08:58 (GMT) 13-Jun-2010
whoeverwl 71.178.104 Sun 11:15:56 (GMT) 13-Jun-2010
whoeverwl 71.191.18.: Sat 14:25:05 (GMT) 12-Jun-2010
whoeverwl 71.191.18.: Sat 12:52:22 (GMT) 12-Jun-2010
whoeverwl 71.191.18.: Sat 11:51:57 (GMT) 12-Jun-2010
whoeverwl 71.191.18.: Sat 11:43:05 (GMT) 12-Jun-2010
whoeverwl 128.82.41.: Fri 11:32:42 (GMT) 11-Jun-2010
whoeverwl 68.115.176 Fri 01:03:24 (GMT) 11-Jun-2010
whoeverwl 68.115.176 Thu 22:15:29 (GMT) 10-Jun-2010
whoeverwl 68.115.176 Thu 19:28:28 (GMT) 10-Jun-2010
whoeverwl 68.115.176 Thu 10:10:29 (GMT) 10-Jun-2010
whoeverwl 68.115.176 Wed 20:05:22 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Wed 15:57:22 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Wed 13:22:49 (GMT) 09-Jun-2010
whoeverwl 68.115.176 Wed 11:15:54 (GMT) 09-Jun-2010

whoeverwl 68.115.176 Tue 22:21:53 (GMT) 08-Jun-2010
whoeverwl 68.115.176 Tue 10:04:30 (GMT) 08-Jun-2010
whoeverwl 71.178.110 Sun 15:45:44 (GMT) 06-Jun-2010
whoeverwl 71.178.110 Sun 14:16:08 (GMT) 06-Jun-2010
whoeverwl 71.178.110 Sun 13:38:29 (GMT) 06-Jun-2010
whoeverwl 71.178.110 Sun 13:23:52 (GMT) 06-Jun-2010
whoeverwl 71.191.28.: Sat 14:48:02 (GMT) 05-Jun-2010
whoeverwl 71.191.28.: Sat 11:54:35 (GMT) 05-Jun-2010
whoeverwl 199.208.23 Fri 15:42:29 (GMT) 04-Jun-2010
whoeverwl 199.208.23 Fri 13:01:00 (GMT) 04-Jun-2010
whoeverwl 71.163.236 Thu 21:58:15 (GMT) 03-Jun-2010
whoeverwl 71.163.236 Thu 21:13:52 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 19:48:37 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 19:04:18 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 16:05:21 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Thu 11:39:47 (GMT) 03-Jun-2010
whoeverwl 199.208.23 Wed 18:18:00 (GMT) 02-Jun-2010
whoeverwl 199.208.23 Wed 14:50:19 (GMT) 02-Jun-2010
whoeverwl 199.208.23 Wed 12:11:36 (GMT) 02-Jun-2010
whoeverwl 71.191.31.: Tue 21:14:36 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 16:16:50 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 14:57:46 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 14:21:19 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 13:27:35 (GMT) 01-Jun-2010
whoeverwl 199.208.23 Tue 12:03:37 (GMT) 01-Jun-2010
whoeverwl 204.212.13 Sun 18:00:29 (GMT) 30-May-2010
whoeverwl 204.212.13 Sun 13:44:18 (GMT) 30-May-2010
whoeverwl 204.212.13 Sat 13:52:59 (GMT) 29-May-2010
whoeverwl 204.212.13 Fri 22:58:05 (GMT) 28-May-2010
whoeverwl 71.191.31.: Fri 13:55:53 (GMT) 28-May-2010
whoeverwl 71.191.31.: Fri 12:01:45 (GMT) 28-May-2010
whoeverwl 71.191.20.: Fri 03:49:09 (GMT) 28-May-2010
whoeverwl 199.208.23 Thu 19:19:11 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 15:16:49 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 14:09:18 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 13:07:51 (GMT) 27-May-2010
whoeverwl 199.208.23 Thu 11:46:25 (GMT) 27-May-2010
whoeverwl 199.208.23 Wed 15:03:01 (GMT) 26-May-2010
whoeverwl 199.208.23 Wed 10:46:59 (GMT) 26-May-2010
whoeverwl 199.208.23 Tue 17:08:10 (GMT) 25-May-2010
whoeverwl 199.208.23 Tue 12:08:27 (GMT) 25-May-2010
whoeverwl 199.208.23 Mon 12:16:29 (GMT) 24-May-2010
whoeverwl 71.178.108 Sun 20:00:15 (GMT) 23-May-2010
whoeverwl 71.178.108 Sun 14:42:27 (GMT) 23-May-2010
whoeverwl 96.241.135 Sat 13:40:19 (GMT) 22-May-2010
whoeverwl 199.208.23 Fri 16:13:47 (GMT) 21-May-2010
whoeverwl 199.208.23 Fri 12:48:09 (GMT) 21-May-2010

whoeverwl 71.163.229 Thu 21:15:40 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 19:19:24 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 17:56:40 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 16:39:40 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 16:15:29 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 14:39:48 (GMT) 20-May-2010
whoeverwl 199.208.23 Thu 11:56:47 (GMT) 20-May-2010
whoeverwl 71.191.24.: Thu 00:18:45 (GMT) 20-May-2010
whoeverwl 71.191.24.: Wed 20:55:32 (GMT) 19-May-2010
whoeverwl 71.178.106 Wed 00:49:32 (GMT) 19-May-2010
whoeverwl 199.208.23 Tue 12:34:06 (GMT) 18-May-2010
whoeverwl 71.178.108 Tue 09:50:58 (GMT) 18-May-2010
whoeverwl 96.241.128 Tue 00:24:51 (GMT) 18-May-2010
whoeverwl 96.241.128 Tue 00:24:51 (GMT) 18-May-2010
whoeverwl 71.191.21.: Mon 21:59:56 (GMT) 17-May-2010
whoeverwl 199.208.23 Mon 18:53:20 (GMT) 17-May-2010
whoeverwl 199.208.23 Mon 11:55:55 (GMT) 17-May-2010
whoeverwl 71.191.21.: Mon 03:13:53 (GMT) 17-May-2010
whoeverwl 71.178.103 Sun 18:31:50 (GMT) 16-May-2010
whoeverwl 71.178.103 Sun 15:50:04 (GMT) 16-May-2010
whoeverwl 71.178.103 Sun 15:22:27 (GMT) 16-May-2010
whoeverwl 96.241.129 Sat 15:37:31 (GMT) 15-May-2010
whoeverwl 199.208.23 Fri 16:56:31 (GMT) 14-May-2010
whoeverwl 199.208.23 Fri 12:21:03 (GMT) 14-May-2010
whoeverwl 71.178.108 Thu 13:12:12 (GMT) 13-May-2010
whoeverwl 71.178.108 Thu 12:09:40 (GMT) 13-May-2010
whoeverwl 199.208.23 Wed 18:34:28 (GMT) 12-May-2010
whoeverwl 199.208.23 Wed 13:22:06 (GMT) 12-May-2010
whoeverwl 96.231.75.: Wed 10:57:37 (GMT) 12-May-2010
whoeverwl 199.208.23 Tue 18:42:49 (GMT) 11-May-2010
whoeverwl 199.208.23 Tue 12:48:11 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 09:47:17 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 02:16:30 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 00:30:33 (GMT) 11-May-2010
whoeverwl 96.231.75.: Tue 00:13:30 (GMT) 11-May-2010
whoeverwl 96.231.75.: Mon 23:30:53 (GMT) 10-May-2010
whoeverwl 199.208.23 Mon 18:39:07 (GMT) 10-May-2010
whoeverwl 199.208.23 Mon 15:20:50 (GMT) 10-May-2010
whoeverwl 199.208.23 Mon 12:15:09 (GMT) 10-May-2010
whoeverwl 71.191.26.: Sun 19:33:37 (GMT) 09-May-2010
whoeverwl 71.191.26.: Sun 14:41:47 (GMT) 09-May-2010
whoeverwl 71.191.26.: Sun 12:18:19 (GMT) 09-May-2010
whoeverwl 71.191.26.: Sat 18:43:55 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 18:36:24 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 17:31:10 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 13:10:44 (GMT) 08-May-2010
whoeverwl 71.191.26.: Sat 10:51:42 (GMT) 08-May-2010

whoeverwl 199.208.23 Fri 12:09:00 (GMT) 07-May-2010
whoeverwl 96.231.74.: Fri 01:55:52 (GMT) 07-May-2010
whoeverwl 199.208.23 Thu 17:22:30 (GMT) 06-May-2010
whoeverwl 199.208.23 Thu 11:58:43 (GMT) 06-May-2010
whoeverwl 71.178.104 Wed 21:30:50 (GMT) 05-May-2010
whoeverwl 199.208.23 Wed 12:53:56 (GMT) 05-May-2010
whoeverwl 71.163.234 Wed 09:47:29 (GMT) 05-May-2010
whoeverwl 96.231.68.: Tue 14:02:17 (GMT) 04-May-2010
whoeverwl 96.231.68.: Tue 12:05:04 (GMT) 04-May-2010
whoeverwl 199.208.23 Mon 14:42:45 (GMT) 03-May-2010
whoeverwl 199.208.23 Mon 12:28:47 (GMT) 03-May-2010
whoeverwl 96.231.79.: Sun 11:56:26 (GMT) 02-May-2010
whoeverwl 96.231.79.: Sun 09:59:28 (GMT) 02-May-2010
whoeverwl 71.178.112 Sat 13:42:12 (GMT) 01-May-2010
whoeverwl 71.178.112 Sat 10:30:44 (GMT) 01-May-2010
whoeverwl 199.208.23 Fri 18:16:03 (GMT) 30-Apr-2010
whoeverwl 71.178.115 Thu 21:59:18 (GMT) 29-Apr-2010
whoeverwl 199.208.23 Thu 11:52:48 (GMT) 29-Apr-2010
whoeverwl 71.191.29.: Thu 00:26:05 (GMT) 29-Apr-2010
whoeverwl 71.191.29.: Wed 21:51:29 (GMT) 28-Apr-2010
whoeverwl 199.208.23 Tue 12:06:46 (GMT) 27-Apr-2010
whoeverwl 199.208.23 Mon 12:03:47 (GMT) 26-Apr-2010
whoeverwl 71.191.16.: Sun 16:29:41 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 16:29:41 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 15:20:02 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 14:57:02 (GMT) 25-Apr-2010
whoeverwl 71.191.16.: Sun 14:11:37 (GMT) 25-Apr-2010
whoeverwl 96.231.79.: Sat 13:29:47 (GMT) 24-Apr-2010
whoeverwl 199.208.23 Fri 12:04:43 (GMT) 23-Apr-2010
whoeverwl 199.208.23 Tue 14:10:12 (GMT) 20-Apr-2010
whoeverwl 71.178.115 Tue 00:53:25 (GMT) 20-Apr-2010
whoeverwl 71.178.115 Mon 20:38:13 (GMT) 19-Apr-2010
whoeverwl 199.208.23 Mon 12:48:30 (GMT) 19-Apr-2010
whoeverwl 71.178.115 Sun 13:14:28 (GMT) 18-Apr-2010
whoeverwl 71.178.115 Sun 12:29:55 (GMT) 18-Apr-2010
whoeverwl 71.178.115 Sat 13:27:00 (GMT) 17-Apr-2010
whoeverwl 71.178.115 Sat 11:15:32 (GMT) 17-Apr-2010
whoeverwl 199.208.23 Fri 12:32:05 (GMT) 16-Apr-2010
whoeverwl 71.178.115 Thu 16:05:26 (GMT) 15-Apr-2010
whoeverwl 199.208.23 Thu 12:13:58 (GMT) 15-Apr-2010
whoeverwl 199.208.23 Wed 18:33:53 (GMT) 14-Apr-2010
whoeverwl 199.208.23 Wed 14:34:25 (GMT) 14-Apr-2010
whoeverwl 71.178.115 Tue 23:15:05 (GMT) 13-Apr-2010
whoeverwl 71.178.115 Tue 22:57:42 (GMT) 13-Apr-2010
whoeverwl 199.208.23 Tue 18:01:20 (GMT) 13-Apr-2010
whoeverwl 199.208.23 Tue 15:01:15 (GMT) 13-Apr-2010
whoeverwl 71.178.115 Tue 09:22:20 (GMT) 13-Apr-2010

whoeverwl 71.178.115 Mon 23:59:51 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 19:34:43 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 17:58:03 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 15:21:54 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 12:57:40 (GMT) 12-Apr-2010
whoeverwl 199.208.23 Mon 11:51:14 (GMT) 12-Apr-2010
whoeverwl 71.178.115 Mon 08:49:01 (GMT) 12-Apr-2010
whoeverwl 71.178.115 Sun 15:56:10 (GMT) 11-Apr-2010
whoeverwl 71.178.115 Sat 11:01:08 (GMT) 10-Apr-2010
whoeverwl 96.241.132 Fri 15:38:42 (GMT) 09-Apr-2010
whoeverwl 199.208.23 Thu 12:29:00 (GMT) 08-Apr-2010
whoeverwl 199.208.23 Wed 12:26:59 (GMT) 07-Apr-2010
whoeverwl 12.53.175. Mon 21:18:09 (GMT) 05-Apr-2010
whoeverwl 71.178.113 Sun 20:57:53 (GMT) 04-Apr-2010
whoeverwl 71.178.113 Sun 14:36:24 (GMT) 04-Apr-2010
whoeverwl 71.178.113 Sat 14:30:04 (GMT) 03-Apr-2010
whoeverwl 199.208.23 Fri 15:29:33 (GMT) 02-Apr-2010
whoeverwl 199.208.23 Fri 13:17:48 (GMT) 02-Apr-2010
whoeverwl 199.208.23 Fri 13:12:40 (GMT) 02-Apr-2010
whoeverwl 199.208.23 Thu 16:48:29 (GMT) 01-Apr-2010
whoeverwl 199.208.23 Wed 13:01:27 (GMT) 31-Mar-2010
whoeverwl 199.208.23 Tue 20:16:14 (GMT) 30-Mar-2010
whoeverwl 199.208.23 Tue 12:11:55 (GMT) 30-Mar-2010
whoeverwl 199.208.23 Mon 12:09:26 (GMT) 29-Mar-2010
whoeverwl 71.178.113 Mon 09:55:15 (GMT) 29-Mar-2010
whoeverwl 71.178.112 Sun 18:03:57 (GMT) 28-Mar-2010
whoeverwl 71.178.112 Sun 15:06:05 (GMT) 28-Mar-2010
whoeverwl 71.178.112 Sat 16:19:35 (GMT) 27-Mar-2010
whoeverwl 71.178.112 Sat 14:55:50 (GMT) 27-Mar-2010
whoeverwl 199.208.23 Fri 18:40:05 (GMT) 26-Mar-2010
whoeverwl 199.208.23 Fri 12:15:57 (GMT) 26-Mar-2010
whoeverwl 96.231.68. Fri 01:53:21 (GMT) 26-Mar-2010
whoeverwl 96.241.136 Thu 20:47:17 (GMT) 25-Mar-2010
whoeverwl 71.178.105 Thu 18:44:00 (GMT) 25-Mar-2010
whoeverwl 199.208.23 Thu 17:23:47 (GMT) 25-Mar-2010
whoeverwl 199.208.23 Thu 13:21:55 (GMT) 25-Mar-2010
whoeverwl 71.163.235 Thu 00:35:59 (GMT) 25-Mar-2010
whoeverwl 71.178.114 Wed 11:56:32 (GMT) 24-Mar-2010
whoeverwl 96.231.76. Tue 21:28:03 (GMT) 23-Mar-2010
whoeverwl 199.208.23 Tue 15:34:45 (GMT) 23-Mar-2010
whoeverwl 199.208.23 Tue 12:46:17 (GMT) 23-Mar-2010
whoeverwl 199.208.23 Mon 19:36:29 (GMT) 22-Mar-2010
whoeverwl 199.208.23 Mon 16:57:10 (GMT) 22-Mar-2010
whoeverwl 199.208.23 Mon 14:16:35 (GMT) 22-Mar-2010
whoeverwl 199.208.23 Mon 12:08:46 (GMT) 22-Mar-2010
whoeverwl 71.163.234 Sun 17:20:59 (GMT) 21-Mar-2010
whoeverwl 71.163.234 Sun 10:56:19 (GMT) 21-Mar-2010

whoeverwl 96.231.78.: Sat 12:17:06 (GMT) 20-Mar-2010
whoeverwl 199.208.23 Fri 14:42:07 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Fri 13:17:20 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Fri 13:02:38 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Fri 12:24:47 (GMT) 19-Mar-2010
whoeverwl 71.191.18.: Fri 09:59:42 (GMT) 19-Mar-2010
whoeverwl 71.191.18.: Fri 08:31:38 (GMT) 19-Mar-2010
whoeverwl 199.208.23 Thu 19:38:34 (GMT) 18-Mar-2010
whoeverwl 71.178.108 Thu 08:15:35 (GMT) 18-Mar-2010
whoeverwl 71.178.108 Wed 21:17:12 (GMT) 17-Mar-2010
whoeverwl 199.208.23 Wed 18:26:30 (GMT) 17-Mar-2010
whoeverwl 199.208.23 Tue 16:21:37 (GMT) 16-Mar-2010
whoeverwl 199.208.23 Tue 13:59:03 (GMT) 16-Mar-2010
whoeverwl 199.208.23 Tue 12:10:56 (GMT) 16-Mar-2010
whoeverwl 199.208.23 Mon 19:24:51 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 16:39:01 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 14:57:36 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 14:08:45 (GMT) 15-Mar-2010
whoeverwl 199.208.23 Mon 13:01:41 (GMT) 15-Mar-2010
whoeverwl 71.163.233 Sat 18:31:06 (GMT) 13-Mar-2010
whoeverwl 199.208.23 Fri 14:46:06 (GMT) 12-Mar-2010
whoeverwl 199.208.23 Mon 16:36:29 (GMT) 08-Mar-2010
whoeverwl 138.88.16.: Sat 12:29:53 (GMT) 06-Mar-2010
whoeverwl 199.208.23 Fri 14:09:22 (GMT) 05-Mar-2010
whoeverwl 199.208.23 Thu 19:50:08 (GMT) 04-Mar-2010
whoeverwl 141.156.21 Thu 12:34:14 (GMT) 04-Mar-2010
whoeverwl 199.208.23 Wed 15:10:20 (GMT) 03-Mar-2010
whoeverwl 141.156.43 Wed 09:50:19 (GMT) 03-Mar-2010
whoeverwl 199.208.23 Tue 17:01:00 (GMT) 02-Mar-2010
whoeverwl 199.208.23 Tue 13:35:16 (GMT) 02-Mar-2010
whoeverwl 141.156.25 Tue 02:38:42 (GMT) 02-Mar-2010
whoeverwl 138.88.245 Sun 12:11:29 (GMT) 28-Feb-2010
whoeverwl 12.70.195.(Sat 00:54:52 (GMT) 27-Feb-2010
whoeverwl 12.70.195.(Fri 15:36:50 (GMT) 26-Feb-2010
whoeverwl 12.70.195.(Fri 14:12:35 (GMT) 26-Feb-2010
whoeverwl 12.70.195.(Thu 21:35:46 (GMT) 25-Feb-2010
whoeverwl 12.70.195.(Thu 17:32:20 (GMT) 25-Feb-2010
whoeverwl 12.70.195.(Thu 11:47:13 (GMT) 25-Feb-2010
whoeverwl 12.70.195.(Wed 10:40:20 (GMT) 24-Feb-2010
whoeverwl 12.70.195.(Tue 19:42:48 (GMT) 23-Feb-2010
whoeverwl 12.70.195.(Tue 12:15:40 (GMT) 23-Feb-2010
whoeverwl 12.70.195.(Mon 23:45:15 (GMT) 22-Feb-2010
whoeverwl 12.70.195.(Mon 04:26:19 (GMT) 22-Feb-2010
whoeverwl 70.155.177 Sat 22:52:42 (GMT) 20-Feb-2010
whoeverwl 206.113.11 Tue 22:35:04 (GMT) 16-Feb-2010
whoeverwl 206.113.11 Mon 22:08:58 (GMT) 15-Feb-2010
whoeverwl 206.113.11 Mon 22:08:14 (GMT) 15-Feb-2010

whoeverwl 71.166.227 Thu 13:46:54 (GMT) 11-Feb-2010
whoeverwl 71.166.227 Wed 19:11:43 (GMT) 10-Feb-2010
whoeverwl 71.166.227 Wed 11:33:44 (GMT) 10-Feb-2010
whoeverwl 71.166.227 Wed 10:31:27 (GMT) 10-Feb-2010
whoeverwl 138.88.241 Tue 12:03:52 (GMT) 09-Feb-2010
whoeverwl 138.88.200 Mon 18:24:11 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Mon 14:44:29 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Mon 13:57:19 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Mon 01:49:17 (GMT) 08-Feb-2010
whoeverwl 138.88.200 Sun 20:09:54 (GMT) 07-Feb-2010
whoeverwl 138.88.218 Sun 14:50:13 (GMT) 07-Feb-2010
whoeverwl 138.88.218 Sat 15:21:18 (GMT) 06-Feb-2010
whoeverwl 138.88.255 Fri 22:48:08 (GMT) 05-Feb-2010
whoeverwl 138.88.255 Fri 21:12:19 (GMT) 05-Feb-2010
whoeverwl 141.156.19 Fri 17:51:26 (GMT) 05-Feb-2010
whoeverwl 138.88.221 Fri 00:18:32 (GMT) 05-Feb-2010
whoeverwl 138.88.221 Thu 22:37:32 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 20:03:30 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 19:11:07 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 17:35:25 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 16:29:08 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 15:21:11 (GMT) 04-Feb-2010
whoeverwl 199.208.23 Thu 12:58:18 (GMT) 04-Feb-2010
whoeverwl 141.156.25 Wed 21:15:20 (GMT) 03-Feb-2010
whoeverwl 141.156.43 Wed 12:09:17 (GMT) 03-Feb-2010
whoeverwl 141.156.43 Wed 10:45:55 (GMT) 03-Feb-2010
whoeverwl 199.208.23 Tue 20:22:10 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 20:08:10 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 18:26:09 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 17:40:26 (GMT) 02-Feb-2010
whoeverwl 199.208.23 Tue 15:55:39 (GMT) 02-Feb-2010
whoeverwl 141.156.43 Tue 10:50:59 (GMT) 02-Feb-2010
whoeverwl 141.156.43 Mon 22:52:35 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 20:21:18 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 19:36:27 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 17:53:54 (GMT) 01-Feb-2010
whoeverwl 199.208.23 Mon 16:23:58 (GMT) 01-Feb-2010
whoeverwl 141.156.37 Sun 22:48:16 (GMT) 31-Jan-2010
whoeverwl 141.156.37 Sun 14:31:35 (GMT) 31-Jan-2010
whoeverwl 141.156.37 Sat 14:42:43 (GMT) 30-Jan-2010
whoeverwl 199.208.23 Fri 14:23:33 (GMT) 29-Jan-2010
whoeverwl 138.88.230 Fri 01:24:37 (GMT) 29-Jan-2010
whoeverwl 199.208.23 Thu 20:50:08 (GMT) 28-Jan-2010
whoeverwl 199.208.23 Thu 12:53:28 (GMT) 28-Jan-2010
whoeverwl 138.88.211 Wed 21:27:15 (GMT) 27-Jan-2010
whoeverwl 199.208.23 Wed 13:25:43 (GMT) 27-Jan-2010
whoeverwl 199.208.23 Tue 13:20:42 (GMT) 26-Jan-2010

whoeverwl 199.208.23 Mon 13:19:45 (GMT) 25-Jan-2010
whoeverwl 138.88.253 Sun 12:50:47 (GMT) 24-Jan-2010
whoeverwl 199.208.23 Fri 13:12:28 (GMT) 22-Jan-2010
whoeverwl 138.88.16. Fri 10:08:06 (GMT) 22-Jan-2010
whoeverwl 199.208.23 Thu 15:05:32 (GMT) 21-Jan-2010
whoeverwl 199.208.23 Wed 18:29:27 (GMT) 20-Jan-2010
whoeverwl 199.208.23 Tue 20:20:32 (GMT) 19-Jan-2010
whoeverwl 199.208.23 Tue 13:46:18 (GMT) 19-Jan-2010
whoeverwl 141.156.39 Mon 13:11:31 (GMT) 18-Jan-2010
whoeverwl 138.88.226 Sun 17:06:01 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 15:46:32 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 13:36:57 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 12:25:25 (GMT) 17-Jan-2010
whoeverwl 138.88.226 Sun 12:24:38 (GMT) 17-Jan-2010
whoeverwl 199.208.23 Fri 12:38:14 (GMT) 15-Jan-2010
whoeverwl 199.208.23 Thu 20:11:36 (GMT) 14-Jan-2010
whoeverwl 141.156.24 Thu 03:11:23 (GMT) 14-Jan-2010
whoeverwl 138.88.235 Wed 01:34:10 (GMT) 13-Jan-2010
whoeverwl 138.88.235 Tue 01:31:38 (GMT) 12-Jan-2010
whoeverwl 138.88.235 Tue 01:26:48 (GMT) 12-Jan-2010
whoeverwl 138.88.235 Tue 00:57:33 (GMT) 12-Jan-2010
whoeverwl 138.88.246 Sun 15:50:47 (GMT) 10-Jan-2010
whoeverwl 138.88.246 Sun 14:18:48 (GMT) 10-Jan-2010
whoeverwl 138.88.246 Sat 13:55:33 (GMT) 09-Jan-2010
whoeverwl 138.88.246 Sat 11:55:37 (GMT) 09-Jan-2010
whoeverwl 199.208.23 Thu 13:13:36 (GMT) 07-Jan-2010
whoeverwl 199.208.23 Wed 14:44:46 (GMT) 06-Jan-2010
whoeverwl 199.208.23 Mon 18:26:00 (GMT) 04-Jan-2010
whoeverwl 138.88.209 Mon 09:32:04 (GMT) 04-Jan-2010
whoeverwl 138.88.209 Mon 01:39:55 (GMT) 04-Jan-2010
whoeverwl 138.88.209 Sun 15:09:57 (GMT) 03-Jan-2010
whoeverwl 138.88.209 Sun 13:21:04 (GMT) 03-Jan-2010
whoeverwl 138.88.240 Sat 11:50:53 (GMT) 02-Jan-2010
whoeverwl 138.88.240 Sat 09:45:33 (GMT) 02-Jan-2010
whoeverwl 138.88.240 Sat 01:52:44 (GMT) 02-Jan-2010
whoeverwl 138.88.240 Thu 09:53:53 (GMT) 31-Dec-2009
whoeverwl 138.88.204 Wed 14:22:30 (GMT) 30-Dec-2009
whoeverwl 199.208.23 Tue 18:08:00 (GMT) 29-Dec-2009
whoeverwl 199.208.23 Tue 15:54:37 (GMT) 29-Dec-2009
whoeverwl 199.208.23 Tue 13:06:22 (GMT) 29-Dec-2009
whoeverwl 199.208.23 Mon 17:39:04 (GMT) 28-Dec-2009
whoeverwl 199.208.23 Mon 13:50:30 (GMT) 28-Dec-2009
whoeverwl 141.156.34 Sun 17:37:40 (GMT) 27-Dec-2009
whoeverwl 141.156.24 Sat 18:26:32 (GMT) 26-Dec-2009
whoeverwl 141.156.24 Sat 14:39:44 (GMT) 26-Dec-2009
whoeverwl 141.156.24 Sat 03:01:11 (GMT) 26-Dec-2009
whoeverwl 141.156.24 Thu 12:43:38 (GMT) 24-Dec-2009

whoeverwl 141.156.24 Wed 20:03:31 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 19:33:27 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 18:30:01 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 17:49:10 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 16:22:47 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 14:25:03 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Wed 12:28:01 (GMT) 23-Dec-2009
whoeverwl 141.156.24 Tue 21:23:34 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 18:17:10 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 17:57:21 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 17:43:11 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 17:16:35 (GMT) 22-Dec-2009
whoeverwl 199.208.23 Tue 13:43:27 (GMT) 22-Dec-2009
whoeverwl 141.156.24 Mon 11:19:43 (GMT) 21-Dec-2009
whoeverwl 141.156.24 Mon 09:40:47 (GMT) 21-Dec-2009
whoeverwl 138.88.229 Sun 15:58:10 (GMT) 20-Dec-2009
whoeverwl 138.88.229 Sun 11:13:19 (GMT) 20-Dec-2009
whoeverwl 138.88.222 Sat 11:58:28 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 11:58:01 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 11:47:55 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 10:33:44 (GMT) 19-Dec-2009
whoeverwl 138.88.222 Sat 09:33:44 (GMT) 19-Dec-2009
whoeverwl 199.208.23 Fri 18:20:30 (GMT) 18-Dec-2009
whoeverwl 199.208.23 Fri 13:32:08 (GMT) 18-Dec-2009
whoeverwl 199.208.23 Thu 12:36:06 (GMT) 17-Dec-2009
whoeverwl 138.88.218 Thu 09:20:11 (GMT) 17-Dec-2009
whoeverwl 138.88.218 Thu 02:06:14 (GMT) 17-Dec-2009
whoeverwl 138.88.218 Thu 01:13:49 (GMT) 17-Dec-2009
whoeverwl 199.208.23 Wed 19:33:13 (GMT) 16-Dec-2009
whoeverwl 138.88.218 Wed 10:11:47 (GMT) 16-Dec-2009
whoeverwl 138.88.218 Tue 17:06:52 (GMT) 15-Dec-2009
whoeverwl 199.208.23 Tue 12:53:42 (GMT) 15-Dec-2009
whoeverwl 138.88.218 Mon 22:25:52 (GMT) 14-Dec-2009
whoeverwl 199.208.23 Mon 13:42:46 (GMT) 14-Dec-2009
whoeverwl 138.88.218 Sun 19:40:28 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sun 16:28:10 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sun 15:16:59 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sun 12:24:12 (GMT) 13-Dec-2009
whoeverwl 138.88.218 Sat 18:23:22 (GMT) 12-Dec-2009
whoeverwl 138.88.218 Sat 12:06:31 (GMT) 12-Dec-2009
whoeverwl 199.208.23 Fri 13:20:13 (GMT) 11-Dec-2009
whoeverwl 141.156.22 Fri 10:18:11 (GMT) 11-Dec-2009
whoeverwl 138.88.195 Thu 01:50:04 (GMT) 10-Dec-2009
whoeverwl 138.88.195 Wed 23:39:47 (GMT) 09-Dec-2009
whoeverwl 199.208.23 Fri 18:31:00 (GMT) 04-Dec-2009
whoeverwl 199.208.23 Fri 12:51:53 (GMT) 04-Dec-2009
whoeverwl 199.208.23 Wed 16:20:35 (GMT) 02-Dec-2009

whoeverwl 199.208.23 Wed 13:22:03 (GMT) 02-Dec-2009
whoeverwl 199.208.23 Tue 14:51:35 (GMT) 01-Dec-2009
whoeverwl 138.88.224 Tue 01:33:49 (GMT) 01-Dec-2009
whoeverwl 199.208.23 Mon 13:21:01 (GMT) 30-Nov-2009
whoeverwl 138.88.224 Mon 03:38:58 (GMT) 30-Nov-2009
whoeverwl 138.88.224 Sat 16:30:43 (GMT) 28-Nov-2009
whoeverwl 138.88.224 Thu 14:01:49 (GMT) 26-Nov-2009
whoeverwl 138.88.224 Wed 01:04:47 (GMT) 25-Nov-2009
whoeverwl 138.88.224 Tue 01:56:02 (GMT) 24-Nov-2009
whoeverwl 199.208.23 Mon 14:37:06 (GMT) 23-Nov-2009
whoeverwl 138.88.224 Sun 11:35:19 (GMT) 22-Nov-2009
whoeverwl 138.88.224 Sat 13:07:35 (GMT) 21-Nov-2009
whoeverwl 138.88.224 Sat 11:57:12 (GMT) 21-Nov-2009
whoeverwl 195.145.13 Thu 23:49:46 (GMT) 19-Nov-2009
whoeverwl 195.145.13 Thu 08:17:23 (GMT) 19-Nov-2009
whoeverwl 195.145.13 Wed 12:02:00 (GMT) 18-Nov-2009
whoeverwl 195.145.13 Tue 21:28:48 (GMT) 17-Nov-2009
whoeverwl 195.145.13 Tue 20:22:50 (GMT) 17-Nov-2009
whoeverwl 195.145.13 Mon 17:02:59 (GMT) 16-Nov-2009
whoeverwl 195.145.13 Mon 11:51:09 (GMT) 16-Nov-2009
whoeverwl 195.145.13 Sun 16:51:21 (GMT) 15-Nov-2009
whoeverwl 138.88.51.: Sat 13:12:24 (GMT) 14-Nov-2009
whoeverwl 138.88.51.: Sat 04:53:40 (GMT) 14-Nov-2009
whoeverwl 199.208.23 Fri 13:51:43 (GMT) 13-Nov-2009
whoeverwl 138.88.51.: Thu 23:51:26 (GMT) 12-Nov-2009
whoeverwl 199.208.23 Thu 12:44:15 (GMT) 12-Nov-2009
whoeverwl 138.88.51.: Wed 12:26:06 (GMT) 11-Nov-2009
whoeverwl 138.88.51.: Wed 05:56:34 (GMT) 11-Nov-2009
whoeverwl 199.208.23 Tue 13:57:12 (GMT) 10-Nov-2009
whoeverwl 199.208.23 Mon 13:13:02 (GMT) 09-Nov-2009
whoeverwl 138.88.119 Sun 15:33:03 (GMT) 08-Nov-2009
whoeverwl 138.88.119 Sun 12:31:41 (GMT) 08-Nov-2009
whoeverwl 138.88.119 Sat 13:07:50 (GMT) 07-Nov-2009
whoeverwl 199.208.23 Fri 13:50:56 (GMT) 06-Nov-2009
whoeverwl 141.156.22 Fri 01:29:04 (GMT) 06-Nov-2009
whoeverwl 141.156.15 Thu 02:22:43 (GMT) 05-Nov-2009
whoeverwl 199.208.23 Wed 17:43:11 (GMT) 04-Nov-2009
whoeverwl 199.208.23 Tue 18:01:51 (GMT) 03-Nov-2009
whoeverwl 199.208.23 Tue 15:42:36 (GMT) 03-Nov-2009
whoeverwl 199.208.23 Tue 13:05:20 (GMT) 03-Nov-2009
whoeverwl 138.88.199 Tue 01:33:24 (GMT) 03-Nov-2009
whoeverwl 199.208.23 Mon 20:19:06 (GMT) 02-Nov-2009
whoeverwl 199.208.23 Mon 17:55:11 (GMT) 02-Nov-2009
whoeverwl 199.208.23 Mon 13:39:52 (GMT) 02-Nov-2009
whoeverwl 138.88.249 Sun 18:14:18 (GMT) 01-Nov-2009
whoeverwl 138.88.249 Sun 17:00:52 (GMT) 01-Nov-2009
whoeverwl 141.156.25 Sun 12:44:13 (GMT) 01-Nov-2009

whoeverwl 141.156.25 Sat 12:32:58 (GMT) 31-Oct-2009
whoeverwl 141.156.25 Sat 12:04:22 (GMT) 31-Oct-2009
whoeverwl 138.88.16.: Fri 11:37:04 (GMT) 30-Oct-2009
whoeverwl 199.208.23 Thu 18:06:05 (GMT) 29-Oct-2009
whoeverwl 199.208.23 Thu 12:34:23 (GMT) 29-Oct-2009
whoeverwl 199.208.23 Wed 17:38:42 (GMT) 28-Oct-2009
whoeverwl 199.208.23 Wed 12:25:53 (GMT) 28-Oct-2009
whoeverwl 141.156.22 Tue 21:56:58 (GMT) 27-Oct-2009
whoeverwl 141.156.23 Tue 20:46:38 (GMT) 27-Oct-2009
whoeverwl 138.88.228 Tue 11:44:20 (GMT) 27-Oct-2009
whoeverwl 138.88.228 Tue 02:47:57 (GMT) 27-Oct-2009
whoeverwl 199.208.23 Mon 19:30:16 (GMT) 26-Oct-2009
whoeverwl 199.208.23 Mon 15:28:46 (GMT) 26-Oct-2009
whoeverwl 199.208.23 Mon 12:06:01 (GMT) 26-Oct-2009
whoeverwl 138.88.245 Mon 02:41:03 (GMT) 26-Oct-2009
whoeverwl 138.88.245 Sat 14:20:35 (GMT) 24-Oct-2009
whoeverwl 138.88.245 Sat 12:51:19 (GMT) 24-Oct-2009
whoeverwl 199.208.23 Fri 18:16:32 (GMT) 23-Oct-2009
whoeverwl 199.208.23 Fri 11:39:07 (GMT) 23-Oct-2009
whoeverwl 138.88.105 Thu 19:26:22 (GMT) 22-Oct-2009
whoeverwl 199.208.23 Thu 12:26:38 (GMT) 22-Oct-2009
whoeverwl 199.208.23 Wed 19:15:47 (GMT) 21-Oct-2009
whoeverwl 199.208.23 Wed 12:34:33 (GMT) 21-Oct-2009
whoeverwl 141.156.25 Wed 01:22:45 (GMT) 21-Oct-2009
whoeverwl 199.208.23 Tue 12:47:36 (GMT) 20-Oct-2009
whoeverwl 138.88.224 Mon 20:25:36 (GMT) 19-Oct-2009
whoeverwl 199.208.23 Mon 12:53:41 (GMT) 19-Oct-2009
whoeverwl 138.88.251 Sun 16:50:59 (GMT) 18-Oct-2009
whoeverwl 138.88.251 Sun 14:58:53 (GMT) 18-Oct-2009
whoeverwl 138.88.251 Sun 13:26:38 (GMT) 18-Oct-2009
whoeverwl 138.88.212 Sun 00:23:28 (GMT) 18-Oct-2009
whoeverwl 138.88.212 Sat 17:07:15 (GMT) 17-Oct-2009
whoeverwl 138.88.212 Sat 06:52:34 (GMT) 17-Oct-2009
whoeverwl 138.88.198 Sat 00:00:18 (GMT) 17-Oct-2009
whoeverwl 138.88.198 Fri 21:23:49 (GMT) 16-Oct-2009
whoeverwl 199.208.23 Fri 12:43:02 (GMT) 16-Oct-2009
whoeverwl 138.88.89.: Thu 20:46:53 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Thu 10:15:17 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Thu 02:54:18 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Thu 00:22:22 (GMT) 15-Oct-2009
whoeverwl 138.88.89.: Wed 22:03:52 (GMT) 14-Oct-2009
whoeverwl 199.208.23 Wed 11:40:53 (GMT) 14-Oct-2009
whoeverwl 138.88.89.: Wed 00:48:27 (GMT) 14-Oct-2009
whoeverwl 138.88.89.: Wed 00:48:04 (GMT) 14-Oct-2009
whoeverwl 199.208.23 Tue 20:16:54 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 18:49:37 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 17:01:13 (GMT) 13-Oct-2009

whoeverwl 199.208.23 Tue 15:01:56 (GMT) 13-Oct-2009
whoeverwl 199.208.23 Tue 11:53:36 (GMT) 13-Oct-2009
whoeverwl 138.88.89.: Mon 23:28:03 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Mon 20:14:18 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Mon 13:09:43 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Mon 12:39:02 (GMT) 12-Oct-2009
whoeverwl 138.88.89.: Sun 13:59:54 (GMT) 11-Oct-2009
whoeverwl 138.88.89.: Sun 11:36:29 (GMT) 11-Oct-2009
whoeverwl 138.88.89.: Sat 10:55:45 (GMT) 10-Oct-2009
whoeverwl 138.88.89.: Fri 21:06:53 (GMT) 09-Oct-2009
whoeverwl 199.208.23 Fri 17:15:56 (GMT) 09-Oct-2009
whoeverwl 199.208.23 Fri 12:08:10 (GMT) 09-Oct-2009
whoeverwl 199.208.23 Thu 17:10:01 (GMT) 08-Oct-2009
whoeverwl 199.208.23 Thu 12:58:59 (GMT) 08-Oct-2009
whoeverwl 199.208.23 Wed 11:54:36 (GMT) 07-Oct-2009
whoeverwl 138.88.89.: Tue 21:34:29 (GMT) 06-Oct-2009
whoeverwl 199.208.23 Tue 12:13:24 (GMT) 06-Oct-2009
whoeverwl 138.88.238 Tue 00:43:01 (GMT) 06-Oct-2009
whoeverwl 138.88.238 Tue 00:18:00 (GMT) 06-Oct-2009
whoeverwl 199.208.23 Mon 12:47:05 (GMT) 05-Oct-2009
whoeverwl 138.88.214 Sun 19:54:01 (GMT) 04-Oct-2009
whoeverwl 138.88.214 Sun 14:38:36 (GMT) 04-Oct-2009
whoeverwl 138.88.48.: Sat 12:40:33 (GMT) 03-Oct-2009
whoeverwl 138.88.48.: Sat 12:22:23 (GMT) 03-Oct-2009
whoeverwl 199.208.23 Fri 18:53:08 (GMT) 02-Oct-2009
whoeverwl 199.208.23 Fri 13:47:37 (GMT) 02-Oct-2009
whoeverwl 138.88.122 Fri 03:06:38 (GMT) 02-Oct-2009
whoeverwl 199.208.23 Thu 18:55:59 (GMT) 01-Oct-2009
whoeverwl 199.208.23 Thu 16:30:02 (GMT) 01-Oct-2009
whoeverwl 199.208.23 Thu 12:46:46 (GMT) 01-Oct-2009
whoeverwl 199.208.23 Wed 18:22:59 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Wed 16:57:48 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Wed 15:23:43 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Wed 12:21:14 (GMT) 30-Sep-2009
whoeverwl 138.88.105 Wed 01:53:56 (GMT) 30-Sep-2009
whoeverwl 138.88.105 Wed 01:42:18 (GMT) 30-Sep-2009
whoeverwl 199.208.23 Tue 16:35:53 (GMT) 29-Sep-2009
whoeverwl 141.156.39 Tue 01:10:21 (GMT) 29-Sep-2009
whoeverwl 138.88.232 Mon 23:11:37 (GMT) 28-Sep-2009
whoeverwl 199.208.23 Mon 19:23:11 (GMT) 28-Sep-2009
whoeverwl 199.208.23 Mon 11:39:59 (GMT) 28-Sep-2009
whoeverwl 138.88.122 Sun 13:16:14 (GMT) 27-Sep-2009
whoeverwl 138.88.122 Sun 09:49:34 (GMT) 27-Sep-2009
whoeverwl 138.88.122 Sun 03:24:51 (GMT) 27-Sep-2009
whoeverwl 138.88.122 Sat 17:12:50 (GMT) 26-Sep-2009
whoeverwl 138.88.122 Sat 14:06:34 (GMT) 26-Sep-2009
whoeverwl 138.88.122 Sat 13:42:36 (GMT) 26-Sep-2009

whoeverwl 138.88.122 Sat 04:31:07 (GMT) 26-Sep-2009
whoeverwl 138.88.206 Fri 14:38:10 (GMT) 25-Sep-2009
whoeverwl 138.88.206 Fri 13:31:57 (GMT) 25-Sep-2009
whoeverwl 138.88.206 Fri 12:53:56 (GMT) 25-Sep-2009
whoeverwl 138.88.201 Thu 14:35:56 (GMT) 24-Sep-2009
whoeverwl 138.88.201 Thu 10:58:38 (GMT) 24-Sep-2009
whoeverwl 138.88.201 Thu 02:14:32 (GMT) 24-Sep-2009
whoeverwl 141.156.25 Wed 17:14:24 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 13:56:50 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 12:58:58 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 12:50:07 (GMT) 23-Sep-2009
whoeverwl 138.88.194 Wed 11:38:29 (GMT) 23-Sep-2009
whoeverwl 138.88.222 Tue 19:22:15 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 12:44:41 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 11:30:22 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 10:52:34 (GMT) 22-Sep-2009
whoeverwl 138.88.222 Tue 03:13:14 (GMT) 22-Sep-2009
whoeverwl 138.88.255 Mon 14:07:28 (GMT) 21-Sep-2009
whoeverwl 138.88.255 Mon 11:35:40 (GMT) 21-Sep-2009
whoeverwl 138.88.49.! Sun 15:19:11 (GMT) 20-Sep-2009
whoeverwl 138.88.49.! Sun 12:54:08 (GMT) 20-Sep-2009
whoeverwl 138.88.49.! Sun 12:21:30 (GMT) 20-Sep-2009
whoeverwl 138.88.49.! Sat 18:09:45 (GMT) 19-Sep-2009
whoeverwl 138.88.49.! Sat 16:50:16 (GMT) 19-Sep-2009
whoeverwl 138.88.49.! Sat 14:21:17 (GMT) 19-Sep-2009
whoeverwl 138.88.49.! Sat 12:16:09 (GMT) 19-Sep-2009
whoeverwl 199.208.23 Fri 18:10:08 (GMT) 18-Sep-2009
whoeverwl 199.208.23 Fri 16:48:56 (GMT) 18-Sep-2009
whoeverwl 199.208.23 Fri 14:30:12 (GMT) 18-Sep-2009
whoeverwl 199.208.23 Fri 12:09:01 (GMT) 18-Sep-2009
whoeverwl 138.88.110 Fri 00:15:27 (GMT) 18-Sep-2009
whoeverwl 141.156.38 Thu 21:34:11 (GMT) 17-Sep-2009
whoeverwl 141.156.38 Thu 20:22:47 (GMT) 17-Sep-2009
whoeverwl 199.208.23 Thu 12:39:03 (GMT) 17-Sep-2009
whoeverwl 138.88.236 Thu 04:14:04 (GMT) 17-Sep-2009
whoeverwl 138.88.220 Wed 21:37:46 (GMT) 16-Sep-2009
whoeverwl 199.208.23 Wed 14:22:29 (GMT) 16-Sep-2009
whoeverwl 138.88.225 Wed 08:30:12 (GMT) 16-Sep-2009
whoeverwl 138.88.225 Wed 02:45:33 (GMT) 16-Sep-2009
whoeverwl 138.88.229 Tue 21:15:35 (GMT) 15-Sep-2009
whoeverwl 199.208.23 Tue 16:42:22 (GMT) 15-Sep-2009
whoeverwl 199.208.23 Tue 15:15:25 (GMT) 15-Sep-2009
whoeverwl 199.208.23 Tue 13:55:08 (GMT) 15-Sep-2009
whoeverwl 199.208.23 Tue 12:18:38 (GMT) 15-Sep-2009
whoeverwl 141.156.25 Mon 23:24:16 (GMT) 14-Sep-2009
whoeverwl 138.88.87.. Mon 20:33:56 (GMT) 14-Sep-2009
whoeverwl 141.156.19 Sun 23:33:08 (GMT) 13-Sep-2009

whoeverwl 141.156.19 Sun 11:46:33 (GMT) 13-Sep-2009
whoeverwl 141.156.19 Sat 12:17:28 (GMT) 12-Sep-2009
whoeverwl 141.156.19 Fri 21:07:09 (GMT) 11-Sep-2009
whoeverwl 141.156.19 Fri 13:07:39 (GMT) 11-Sep-2009
whoeverwl 141.156.22 Thu 15:00:12 (GMT) 10-Sep-2009
whoeverwl 141.156.22 Thu 13:24:15 (GMT) 10-Sep-2009
whoeverwl 138.88.205 Wed 16:30:10 (GMT) 09-Sep-2009
whoeverwl 204.212.13 Tue 14:03:36 (GMT) 08-Sep-2009
whoeverwl 204.212.13 Mon 11:58:00 (GMT) 07-Sep-2009
whoeverwl 204.212.13 Sun 22:58:44 (GMT) 06-Sep-2009
whoeverwl 204.212.13 Sun 13:39:37 (GMT) 06-Sep-2009
whoeverwl 204.212.13 Sat 22:15:55 (GMT) 05-Sep-2009
whoeverwl 204.212.13 Sat 18:15:41 (GMT) 05-Sep-2009
whoeverwl 204.212.13 Sat 15:12:36 (GMT) 05-Sep-2009
whoeverwl 204.212.13 Sat 14:44:55 (GMT) 05-Sep-2009
whoeverwl 199.208.23 Fri 15:10:19 (GMT) 04-Sep-2009
whoeverwl 199.208.23 Thu 18:18:58 (GMT) 03-Sep-2009
whoeverwl 199.208.23 Wed 15:37:10 (GMT) 02-Sep-2009
whoeverwl 199.208.23 Wed 12:40:33 (GMT) 02-Sep-2009
whoeverwl 199.208.23 Tue 19:14:50 (GMT) 01-Sep-2009
whoeverwl 138.88.102 Tue 09:23:14 (GMT) 01-Sep-2009
whoeverwl 138.88.247 Tue 00:41:26 (GMT) 01-Sep-2009

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1450, 15 Oct 10, SA (b)(6)(b)(7)(C) collected as evidence one compact disc (CD) containing the U.S. Department of State firewall logs from SA (b)(6)(b)(7)(C) U.S. Department of State, Bureau of Diplomatic Security. The collection was documented on Evidence/Property Custody Document (EPCD), Document Number 151-10.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

SA (b)(6)(b)(7)(C)

DATE

15 Oct 10

EXHIBIT

243

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001626
Approved

(b)(6)(b)(7)(C)

Intentionally left blank
001627

Exhibit(s) 244

Page(s) 001628 withheld:

5 U.S.C. § 552(b)(1)

Permits withholding information that
is classified for
National Security purposes

CLASSIFIED

Exhibit(s) 245

Page(s) 001629 thru 01629b referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1605, 20 Oct 10, SA (b)(6)(b)(7)(C) interviewed U.S. Navy Petty Officer First Class (PO1) (b)(6)(b)(7)(C) Center for Information Dominance - Corry Station, 440 Roberts Avenue, Pensacola, FL 32511, as he was identified as having been assigned with PFC MANNING at Forward Operating Base (FOB) Hammer, Iraq. PO1 (b)(6)(b)(7)(C) related he was assigned in Iraq from Dec 09 through Aug 10, and was assigned at FOB Hammer between 4 Jan 10 through about the first or second week of Apr 10, whereafter PO1 (b)(6)(b)(7)(C) related he was reassigned to Contingency Operating Base (COB) Basrah, Iraq. PO1 (b)(6)(b)(7)(C) stated while he was at FOB Hammer he was not technically assigned to Cryptologic Support Team 5 (CST5), but worked with the National Security Agency (NSA) personnel assigned to this team in the SCIF at FOB Hammer as part of an element called the Joint Expeditionary SIGINT Tactical Recon (JESTER) Team. PO1 (b)(6)(b)(7)(C) related while at FOB Hammer he worked with WO1 (b)(6)(b)(7)(C) 2nd Brigade Combat Team (BCT), FOB Hammer, Iraq; SPC (b)(6)(b)(7)(C) SrA (b)(6)(b)(7)(C) SSgt (b)(6)(b)(7)(C) TSgt (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) all assigned to CST5 while deployed in Iraq. PO1 (b)(6)(b)(7)(C) said he remembered PFC MANNING and mentioned eating with him at the FOB Hammer dining facility approximately a handful of times during the midnight meal. PO1 (b)(6)(b)(7)(C) described PFC MANNING as being shy, quiet, and kept to himself. PO1 (b)(6)(b)(7)(C) felt PFC MANNING was good at answering questions related to his job, and if there was a question PFC MANNING couldn't answer he would refer it to someone else to find an answer. PO1 (b)(6)(b)(7)(C) related he did not believe PFC MANNING was the most squared away Intelligence Analyst, but was also not a bad one either. PO1 (b)(6)(b)(7)(C) said he was not present for or had any firsthand knowledge about any incidents involving PFC MANNING while assigned at FOB Hammer. PO1 (b)(6)(b)(7)(C) explained he had spoken numerous times with PFC MANNING, but PO1 (b)(6)(b)(7)(C) could not remember PFC MANNING mentioning any information in regard to his friends or any travel PFC MANNING may have done while on mid-tour leave. PO1 (b)(6)(b)(7)(C) said he believed PFC MANNING said he was snowed in for a couple of days while on leave and thought PFC MANNING may have traveled to the East Coast of the U.S. while on leave; however, he could not say for sure. PO1 (b)(6)(b)(7)(C) said he did not remember anyone saying anything derogatory to PFC MANNING or behind his back. PO1 (b)(6)(b)(7)(C) related he noticed two things about PFC MANNING he felt were odd, which was that he had somewhat feminine characteristics and had a habit of putting on lip balm unusually often. PO1 (b)(6)(b)(7)(C) said PFC MANNING appeared to be nervous when speaking in front of other personnel, such as at the daily shift-change briefings; however, PO1 (b)(6)(b)(7)(C) said he did not find PFC MANNING was any worse than other personnel who also had to brief at these meetings. PO1 (b)(6)(b)(7)(C) added he did not feel PFC MANNING was singled out during any of these meetings when making a mistake, such as mispronouncing an Arabic name, and that all of the personnel briefing who made similar mistakes would be treated equally. PO1 (b)(6)(b)(7)(C) felt PFC MANNING was not very motivated or what could be described as a 'self-starter' in regard to his work. PO1 (b)(6)(b)(7)(C) explained if PFC MANNING wasn't given things to do he didn't seem to produce a lot of work on his own. PO1 (b)(6)(b)(7)(C) did now that he looks back and he remembers seeing PFC MANNING sitting in the Sensitive Compartmented Information Facility (SCIF) and singing to himself with head phones on, PO1 (b)(6)(b)(7)(C) wishes he would have been paying more attention to what PFC MANNING had been doing on his computer. PO1 (b)(6)(b)(7)(C) related he first learned of the allegations related to this investigation from reading a news story on the Internet while he assigned at another location in Iraq. PO1 (b)(6)(b)(7)(C) explained he had no knowledge in regard to the alleged unlawful disclosure of U.S. Government Classified materials by PFC MANNING. PO1 (b)(6)(b)(7)(C) additionally related he

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

20 Oct 10

EXHIBIT

246

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

had no knowledge of the '9/11 Pager Messages' nor did he remember PFC MANNING ever mentioning anything in regard to the 2007 Apache air-strike video. PO1 (b)(6)(b)(7)(C) in regard to the Operational Security procedures at FOB Hammer, he believed some things were too relaxed and gave examples of the curtain which separated the main SCIF area from where the CST5 personnel were located; in that it should have been a solid door and that the SCIF should have been more sound-proof than it was. PO1 (b)(6)(b)(7)(C) marked the use of removable media within the SCIF would not normally have been used, but due to the lack of Information Technology infrastructure in the SCIF it was necessary to transfer data. PO1 (b)(6)(b)(7)(C) could not immediately provide any additional information related to this investigation.

AGENT'S COMMENT: PO1 (b)(6)(b)(7)(C) stated during the interview he had been a witness to an incident involving the accidental discharge of a small arms weapon (what he believed was an M-16) while in Iraq and was spoken to about this incident by law enforcement. SA (b)(6)(b)(7)(C) noted when entering PO1 (b)(6)(b)(7)(C) information into ACI2 that PO1 (b)(6)(b)(7)(C) was also listed in a 1999 CID Investigation from the Ansbach CID Office in relation to being a witness to an allegation of Indecent Acts during the Navy Ball at the Chiemsee Hotel. It was noted by SA (b)(6)(b)(7)(C) the allegations in this case, CID Case 0202-99-CID137, did not appear to have been founded. PO1 (b)(6)(b)(7)(C) was asked about the '9/11 Pager Messages' as this was something mentioned by PFC MANNING in Internet chat conversations. During those conversations PFC MANNING mentioned to the individual he was chatting with that he recognized data posted on the WikiLeaks website as data from an NSA database. Lastly SA (b)(6)(b)(7)(C) noted that PO1 (b)(6)(b)(7)(C) may also be referred to as CTR1 (b)(6)(b)(7)(C) "CTR1" being the abbreviation for the U.S. Navy rating for a Petty Officer First Class who is a Cryptologic Technician who works with collection activities.

//////////////////// **LAST ENTRY** //////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

20 Oct 10

EXHIBIT

246

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1903, 20 Oct 10, SA (b)(6)(b)(7)(C) interviewed U.S. Air Force Staff Sergeant (SSgt) (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) 301st Intelligence Squadron, Misawa Air Base, Japan, APO AP 96319, as he was identified as a member of Cryptological Support Team 5 (CST5) and was assigned at FOB Hammer with PFC MANNING. SSgt (b)(6)(b)(7)(C) related he was assigned in Iraq from December 2009 to June 2010, but that he was only assigned to FOB Hammer between March 2010 through late May 2010. SSgt (b)(6)(b)(7)(C) explained prior to being at FOB Hammer he was assigned to a base in Baghdad, Iraq. SSgt (b)(6)(b)(7)(C) explained he left Iraq in early June 2010 to return to his home station in Japan. SSgt (b)(6)(b)(7)(C) related he was the replacement for SrA (b)(6)(b)(7)(C) who was a CST5 member who had returned to the United States for medical reasons. SSgt (b)(6)(b)(7)(C) said while at FOB Hammer the personnel on CST5 that he worked with included: WO1 (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C), SPC (b)(6)(b)(7)(C) PO1 (b)(6)(b)(7)(C) and SSgt (b)(6)(b)(7)(C) SSgt (b)(6)(b)(7)(C) stated he remembered PFC MANNING from FOB Hammer as someone who was quiet and what he described as a smaller build male soldier. SSgt (b)(6)(b)(7)(C) made the statement that he thought the whole incident in which PFC MANNING assaulted SPC (b)(6)(b)(7)(C) was odd, because PFC MANNING was a physically smaller person. SSgt (b)(6)(b)(7)(C) further stated he and others had been at lunch when the incident with SPC (b)(6)(b)(7)(C) had occurred and had returned to the SCIF minutes after it was over. SSgt (b)(6)(b)(7)(C) related he did not have any professional interaction with PFC MANNING while at FOB Hammer with the exception of seeing him at shift-change briefings, and added he could not remember having any personal interactions with PFC MANNING while in Iraq. When told by SA (b)(6)(b)(7)(C) this interview was not in regard to the physical altercation incident PFC MANNING was involved in with SPC (b)(6)(b)(7)(C), but was in regard to the disclosure of U.S. Government Classified material; SSgt (b)(6)(b)(7)(C) stated he did not know PFC MANNING was involved in any incidents related to Classified information. SSgt (b)(6)(b)(7)(C) said he remembered someone he was assigned with in Baghdad sending him a story about an incident involving the unlawful disclosure of Classified information, and that it involved someone from the 10th Mountain Division; however, SSgt (b)(6)(b)(7)(C) related he did not know the person involved in this incident was PFC MANNING. SSgt (b)(6)(b)(7)(C) explained he did not know of any interactions PFC MANNING had with other members of CST5 nor did he know anyone on CST5 which would have been more friendly or had more frequent interactions with PFC MANNING than anyone else on the team. SSgt (b)(6)(b)(7)(C) related he had heard of the website WikiLeaks.org, but personnel in his unit were advised not to visit this website based on the type of information contained on the site. SSgt (b)(6)(b)(7)(C) said he did not know of anything referred to as the '9/11 Pager Messages', but did mention having seen the 2007 Apache air-strike video while in Iraq – SSgt (b)(6)(b)(7)(C) explained he remembered seeing it on television news broadcasts. SSgt (b)(6)(b)(7)(C) could not immediately provide any additional information in regard to this investigation.

AGENT'S COMMENT: SA (b)(6)(b)(7)(C) thought it was remarkable SSgt (b)(6)(b)(7)(C) worked in the field of Intelligence but he did not know more about this incident involving PFC MANNING and the unlawful disclosure of hundreds of thousands of U.S. Government Classified documents; especially given the amount of recent news media coverage. SSgt (b)(6)(b)(7)(C) was asked about the '9/11 Pager Messages' as this was something mentioned by PFC MANNING in chat conversations with Mr. (b)(6)(b)(7)(C).

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

20 Oct 10

EXHIBIT

247

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

During those conversations PFC MANNING mentioned to the individual he was chatting with that he recognized data posted on the WikiLeaks website as data from an NSA database. SSgt (b)(6)(b)(7)(C) could not provide any information as to what PFC MANNING may have been referring to in regard to the 9/11 Pager Messages. SA (b)(6)(b)(7)(C) noted SSgt (b)(6)(b)(7)(C) appeared genuinely unaware of the general nature of this investigation involving PFC MANNING during his interview.

////////////////////////////////// **LAST ENTRY** //////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

20 Oct 10

EXHIBIT

247

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

001633
Approved _____

Exhibit(s) 248

Page(s) 001634 thru 001636 referred to:

Federal Bureau of Investigation
Record Information/Dissemination Section
170 Marcel Drive
Winchester, Virginia 22602-4843

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0932, 28 Oct 10, SA (b)(6)(b)(7)(C) collected as evidence one Digital Versatile Disc (DVD), received via United States Postal Service Registered Mail # 121 632 875 US, which purportedly contained the recorded phone conversations of PFC MANNING while he was located at the Theater Correctional Facility (TCF), Kuwait. The collection of evidence was documented on DA Form 4137, Evidence/Property Custody Document (EPCD), Document Number (DN) 160-10.

////////////////////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

28 Oct 10

EXHIBIT

249

OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001637
Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0945, 28 Oct 10, SA (b)(6)(b)(7)(C) was sworn to the search warrant pertaining to evidence previously collected and documented on an Evidence/Property Custody Document (EPCD), Document Number (DN) 117-10, Items 3-4, by the Honorable (b)(6)(b)(7)(C) U.S. Magistrate Judge, Eastern District of Virginia, 401 Courthouse Square, Alexandria, VA. (See search warrant for details)

About 1230, 1 Nov 10, SA (b)(6)(b)(7)(C) searched the box previously collected from Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) and documented on an EPCD as Item 4, DN 117-10. The box, property of PFC MANNING, contained numerous items of military issued equipment. Nothing of evidentiary value was discovered during the search. The items found within the box were photographed. (See photo packet for details)

////////////////////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

1 Nov 10

EXHIBIT

250

1 FEB 77

OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001638
Approved

(b)(6)(b)(7)(C)

Exhibit(s) 251

Page(s) 001639 thru 001643

Documents

SEALED

by the

U.S. District Court
for the Eastern District of Virginia

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1858, 2 Nov 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) this office, met with Ms. (b)(6)(b)(7)(C) at her residence as she was identified as PFC MANNING's (b)(6)(b)(7)(C) and was believed to be in possession of property belonging to PFC MANNING that had been left at her residence by PFC MANNING. Ms. (b)(6)(b)(7)(C) was also believed to be in possession of mail and/or a sealed container sent to her address by personnel at the Kuwait Theater Confinement Facility (TCF), which contained personal property of PFC MANNING. SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) requested Ms. (b)(6)(b)(7)(C) consent to search for the aforementioned property as well as to collect any sealed packages or mail which had been received at her address on PFC MANNING's behalf. Ms. (b)(6)(b)(7)(C) executed a written Consent to Search form, allowing SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) to search her residence for the aforementioned items belonging to PFC MANNING. Ms. (b)(6)(b)(7)(C) further explained, since investigators had been to her home previously and searched areas containing PFC MANNING's personal property, she had since placed property she identified as belonging to PFC MANNING into several plastic storage containers and a dresser, which were located in a basement room of her residence. SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) searched the containers and areas Ms. (b)(6)(b)(7)(C) indicated as containing personal belongings of PFC MANNING. Before and during the search, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) each recorded digital photos of the basement room and items contained in various containers/locations. As a result of the search of several plastic storage containers, a dresser, and items which were contained on top of a bed, the following items were collected as evidence which Ms. (b)(6)(b)(7)(C) identified as PFC MANNING's property:

- (1) Hard Disk Drive, Maxtor Brand, Serial Number (SN): "T4J8XNLC";
- (1) SD Memory Card, SN: "BE0915514353G";
- (1) SD Memory Card, SN: "BE0730513278G";
- (1) SD Memory Card, SN: "BE0828613591D";
- (1) Compact Flash Memory Card, SN: "AA0407XFA";
- (1) Smart Media Memory Card, SN: "8R94 CL0201 64296V";
- (10) Compact Disc-Recordable (CD-R) Discs, Maxell brand, 80min/700MB;
- (3) Compact Disc-Recordable (CD-R) Disc, FujiFilm brand, 80min/700MB;
- (2) Compact Disc-Rewritable (CD-RW) Disc, Memorex Brand, 4x/700MB/80min;
- (1) Compact Disc (CD) Disc, Kodak brand;
- (1) Paper Disc Envelope, Kodak brand;
- (1) Memory Card, Free Software Foundation brand;
- (1) Paperback Book, "Jane Austen Pride and Prejudice";
- (1) Sealed Card Board Box, contents unknown.

All of the above items were retained on Evidence/Property Custody Document (EPCD), Document Number (DN) 0162-10.

AGENT'S COMMENT: The aforementioned search was conducted in order to identify any additional items of digital media which may not have been previously found during the initial search of PFC

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b)(7)(E)		ORGANIZATION Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 2 Nov 10	EXHIBIT 252	

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

MANNING's personal property which he had left in Ms. (b)(6)(b)(7)(C) custody; given that much more information related to the facts and circumstances of this investigation were now known to investigators since initial contact was made with Ms. (b)(6)(b)(7)(C) in June 2010. It was further noted that the personal property items of PFC MANNING, which had been collected from him by corrections personnel at the Kuwait TCF and were later shipped to PFC MANNING's home of record address (b)(6)(b)(7)(C) (b)(6)(b)(7)(C), were believed to be contained in the sealed cardboard box collected during this search. This cardboard box contained the U.S. Certified Mail label, Certified Mail Number 7008 1300 0000 2028 4546, which matched the copy of the Certified U.S. Mail Return Receipt received by the Kuwait TCF for this property they had sent to Ms. (b)(6)(b)(7)(C) address. Ms. (b)(6)(b)(7)(C) explained the U.S. Postal Service attempted to deliver the sealed cardboard box once, but PFC MANNING's (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) who is also her brother, had apparently refused to accept the package. Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) said because this box was unexpected and its contents were unknown, her brother declined to accept the package during its initial delivery. Ms. (b)(6)(b)(7)(C) related PFC MANNING's father as well as another brother had been visiting around the time the box first arrived due to their mother having recently died. Ms. (b)(6)(b)(7)(C) explained she had contacted PFC MANNING's attorney who advised where the box originated and that it was okay to accept this package. Ms. (b)(6)(b)(7)(C) related PFC MANNING's father later obtained the box; wherein it was placed in the basement room with all of PFC MANNING's other belongings. Ms. (b)(6)(b)(7)(C) stated the box had remained sealed and she did not know what the contents of the box were. SA (b)(6)(b)(7)(C) noted an initial examination of the cardboard box revealed this box did not appear to have been opened since being placed in the U.S. Mail system. It was further noted, prior to conducting the search of the basement room in the (b)(6)(b)(7)(C) residence, that Ms. (b)(6)(b)(7)(C) said she had collected all of PFC MANNING's property within her home and had packed these items into the containers/areas mentioned. SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) noted the basement room which investigators had previously searched was in a much more orderly state than it was in June 2010.

//////////////////// LAST ENTRY //////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNA

(b)(6)(b)(7)(C)

DATE

2 Nov 10

EXHIBIT

252

**FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE**

Date: 2 Nov 10		Consent To Search (USACIDC Supplement 1 to AR 190-22)		Time: 1911	
1. Name of person consenting to the search: Ms. (b)(6)(b)(7)(C)			2. Organization and location: (b)(6)(b)(7)(C)		
3. I have been informed by the undersigned USACIDC Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law: 18 U.S.C. 1030 - Fraud and related activity in connection with computers (Article 134, U.C.M.J.) 18 U.S.C. 793 - Gathering, transmitting or losing defense information (Article 134, U.C.M.J.) Article 92, U.C.M.J. - Failure to obey order or regulation					
4. I have been requested by the undersigned USACIDC Special Agent to give my consent to a search of my person, premises, or property as indicated below. I have been advised of my right to refuse a search of my person, premises, or property. (If you <u>do not</u> give your consent, do not sign this form.)					
5. I hereby authorize the undersigned USACIDC Special Agent and/or other Authorized Law Enforcement Officials assisting the undersigned USACIDC Special Agent to conduct a search of: <i>(Initial and sign applicable blocks)</i>					
a.	My Person	Initials	Signature		
b.	My Quarters	Initials	Signature	(b)(6)(b)(7)(C)	
Located At:		(b)(6)(b)(7)(C)			
c.	My Vehicle	Initials	Signature		
Located At:					
Described As:					
d.	Other	Initials	Signature		
Located At:					
Described As:					
I am authorizing the above search(s) for the following general types of property which may be removed by the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations: Any property belonging to Bradley E. MANNING which was left in my possession at (b)(6)(b)(7)(C) to include: clothing, books, papers, documents, digital media (computers and related electronic storage devices), military equipment, opened packages/postal mail, sealed containers to include postal mail and/or packages, and/or any other item which contain U.S. Government Classified Information.					
6. This written permission is given to the undersigned USACIDC Special Agent freely, voluntarily and without threats or promises of any kind:					
(b)(6)(b)(7)(C) Signature of USACIDC Special Agent		(b)(6)(b)(7)(C) Signature of Person Granting Consent			
		Signature of Witness (If Available)			

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1109, 9 Nov 10, SA (b)(6)(b)(7)(C) collected as evidence from Mr. (b)(6)(b)(7)(C) GG-14, Program Manager, Information Review Task Force (IRTF), Bldg 251, South 18th St, Arlington, VA 22202, two Compact Discs (CDs) containing classified information downloaded from the internet by the IRTF. The collection of evidence was documented on DA Form 4137, Evidence/Property Custody Document (EPCD), Document Number (DN) 164-10.

/////////////////////////////////LAST ENTRY/////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

9 Nov 10

EXHIBIT

254

CID F...ICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

1 FEB 11

001647

Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

About 1310, 22 Jul 10, SA (b)(6)(b)(7)(C) received (b)(7)(D)
(b)(7)(D)

(b)(7)(D)

(b)(7)(D)

About 1520, 6 Aug 10, SA (b)(6)(b)(7)(C) coordinated with Mr. (b)(6)(b)(7)(C) DOB: (b)(6)(b)(7)(C) SSN (b)(6)(b)(7)(C) via Email, who delivered a copy of the notes pertaining to his analysis of the Wikileaks site. (See 302)

About 2150, 6 Aug 10, SA (b)(6)(b)(7)(C) coordinated with Mr. (b)(6)(b)(7)(C) via Email, who related he had completed an analysis of the Uniform Resource Locator <http://web.archive.org/web/20071020051936/http://iq.org/>, which is believed to be the archived storage of data of web pages pertaining to Mr. ASSANGE, revealed the following Email accounts were possibly associated with Mr. ASSANGE, proff@iq.org, me@iq.org, proff@suburbia.apana.org.au, proff@gnu.ai.mit.edu, proff@suburbia.net, proff@four.net, and strobe@suburbia.net. Internet Archive: Wayback Machine (<http://www.archive.org>) is a web site that provides a searchable database containing over 150 billion web pages archived from 1996 to a few months ago. (See Email)

About 1100, 6 Sep 10, SA (b)(6)(b)(7)(C) received the cellular phone Toll Records pertaining to Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) via Fed Ex (Tracking Number 871482582010), from SA (b)(6)(b)(7)(C) (See Toll Records)

AGENT'S COMMENT: Grand Jury Material, 6E Letter required to review the records.

About 1300, 8 Sep 10, SA (b)(6)(b)(7)(C) U.S. Immigration and Customs Enforcement (ICE), Joint Terrorism Task Force (JTTF), 26 Federal Plaza, New York, NY 10278 and SSA (b)(6)(b)(7)(C) Homeland Security Investigations National Security Unit ICE liaison to the DHS/Joint Analysis Group Digital Media Analysis/Cyber Exploitation, Fairfax, VA, attended this office's synchronization meeting. Upon completion of the meeting, SA (b)(6)(b)(7)(C) provided SA (b)(6)(b)(7)(C) with copies of Mr. (b)(6)(b)(7)(C) items that were detained under ICE Border Search Authority on 29 Jul 10, and requested, this office, determine if anything is significant to the ongoing investigation regarding unauthorized access to

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro Resident Agency, CCIU
U.S. Army CID, Fort Belvoir, VA 22060

DATE

10 Nov 10

EXHIBIT

255

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

U.S. Government classified material that was posted by wikileaks.org. Additionally, SA (b)(6)(b)(7)(C) provided copies of the following reports: a forensic report pertaining to the 29 Jul 10, secondary inspection of Mr. APPLEBAUM and his property, two forensic reports pertaining to the examination of digital items obtained from Mr. APPLEBAUM during the secondary inspection of Mr. APPLEBAUM on 29 Jul 10, a report pertaining to the HOPE Conference, and two reports pertaining to the secondary inspection of Mr. (b)(6)(b)(7)(C) See Reports)

AGENT'S COMMENT: SA (b)(6)(b)(7)(C) subsequently provided an endorsed ICE Demand Letter, requesting the assistance specified above.

About 1300, 2 Nov 10, SA (b)(6)(b)(7)(C) collected as evidence one CD containing the centaur data pertaining to the following IP addresses known to have been used by PFC MANNING during acquisition of classified information, from the hands of Mr. (b)(6)(b)(7)(C) Targeting Analyst, G37, Targeting, ARCYBER, 8825 Beulah Street, Fort Belvoir, VA 22060, which was documented on EPCD, DN 161-10.

AGENT'S COMMENT: Mr. (b)(6)(b)(7)(C) also provided SA (b)(6)(b)(7)(C) with a report of his Centaur analysis, which disclosed numerous connections between IP addressed assigned to PFC MANNING and other .mil and .gov domains. (See E-mail and Report / SIPR safe)

About 1040, 10 Nov 10, SA (b)(6)(b)(7)(C) collected as evidence one hard drive, Western Digital brand, Passport model, serial number WX70C8958878, purportedly containing Iraq Combined Information Data Network Exchange (CIDNE) logs related to the time period when PFC MANNING was deployed and working in Iraq, via APO Registered Mail, registration number 852621483US, from Mr. (b)(6)(b)(7)(C) USF-I J3 Knowledge Management Officer, CIDNE, APO AE, 09342, which was documented on EPCD, DN 165-10.///LAST ITEM///

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b) (7)(E)

ORGANIZATION

Washington Metro Resident Agency, CCIU
U.S. Army CID, Fort Belvoir, VA 22060

DATE

10 Nov 10

EXHIBIT

255

Exhibit(s) 256

Page(s) 001650 thru 001657 withheld.

5 U.S.C. § 552(b)(6) & (b)(7)(C)
Third Party Information
Not Reasonably Segregable

From: (b)(6)(b)(7)(C)@abixx.com>
Subject: Re: Contact email
Date: August 6, 2010 3:19:46 PM EDT
To: (b)(6)(b)(7)(C)@gmail.com>
▶ 1 Attachment, 79.6 KB

I certainly will. Attached is a PDF of the printed file I gave you. The file also has the additional information I looked up for you while here.

Thank you

(b)(6)(b)(7)(C)

On Fri, 6 Aug 2010 14:37:44 -0400, (b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)@gmail.com> wrote:

| Let me know if you find out anything else about wiki



wikileaks MI...pdf (79.6 KB)

Printed by: (b)(6)(b)(7)(C) 05 August 2010
 (b)(6)(b)(7)(C)
 [M] 308.685.1310 [C] 308.367.8201

New journalistic search interface for Afghan War Diary <http://bit.ly/buPyez> about 21 hours ago via bitly

#####

<http://www.diarydig.org/>

#####

ping diarydig.org
 PING diarydig.org (18.85.28.35): 56 data bytes
 64 bytes from 18.85.28.35: icmp_seq=0 ttl=46 time=21.675 ms

#####

whois 18.85.28.35

 # Query terms are ambiguous. The query is assumed to be:
 # "n 18.85.28.35"
 #
 # Use "?" to get help.
 #

 # The following results may also be obtained via:
 # <http://whois.arin.net/rest/nets;q=18.85.28.35?showDetails=true&showARIN=false>
 #

NetRange: 18.0.0.0 - 18.255.255.255
 CIDR: 18.0.0.0/8
 OriginAS:
 NetName: MIT
 NetHandle: NET-18-0-0-1
 Parent:
 NetType: Direct Assignment
 NameServer: W2ONS.MIT.EDU
 NameServer: BITSY.MIT.EDU
 NameServer: STRAWB.MIT.EDU
 RegDate: 1994-01-01
 Updated: 2009-06-19
 Ref: <http://whois.arin.net/rest/net/NET-18-0-0-1>

OrgName: Massachusetts Institute of Technology
 OrgId: MIT-2
 Address: Room W92-190
 Address: 77 Massachusetts Avenue
 City: Cambridge
 StateProv: MA
 PostalCode: 02139-4307
 Country: US
 RegDate: 2003-12-12
 Updated: 2003-12-12
 Ref: <http://whois.arin.net/rest/org/MIT-2>

OrgTechHandle: JIS-ARIN
 OrgTechName: (b)(6)(b)(7)(C)
 OrgTechPhone: +1-707-276-0409
 OrgTechEmail: jis@mit.edu
 OrgTechRef: <http://whois.arin.net/rest/poc/JIS-ARIN>

RTechHandle: JIS-ARIN
 RTechName: (b)(6)(b)(7)(C)
 RTechPhone: +1-707-276-0409
 RTechEmail: jis@mit.edu
 RTechRef: <http://whois.arin.net/rest/poc/JIS-ARIN>

 # ARIN WHOIS data and services are subject to the Terms of Use
 # available at: https://www.arin.net/whois_tou.html
 #

#####

nmap -sV diarydig.org

Starting Nmap 5.21 (<http://nmap.org>) at 2010-08-05 13:29 EDT
 Nmap scan report for diarydig.org (18.85.28.35)
 Host is up (0.027s latency).
 rDNS record for 18.85.28.35: loco.media.mit.edu
 Not shown: 988 closed ports
 PORT STATE SERVICE VERSION
 22/tcp open ssh OpenSSH 5.3p1 Debian 3ubuntu4 (protocol 2.0)
 23/tcp filtered telnet
 25/tcp filtered smtp
 80/tcp open http Apache httpd 2.2.14 ((Ubuntu))
 135/tcp filtered msrpc
 139/tcp filtered netbios-ssn
 161/tcp filtered snmp
 443/tcp open http Apache httpd 2.2.14 ((Ubuntu))
 445/tcp filtered microsoft-ds
 554/tcp open tcpwrapped
 7070/tcp open tcpwrapped
 8000/tcp open http Apache httpd 2.2.14 ((Ubuntu))
 Service Info: OS: Linux

Service detection performed. Please report any incorrect results at <http://nmap.org/submit/>.
 Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds

Subject: Re: Contact email

From: (b)(6)(b)(7)(C)@abixx.com>

Date: Fri, 06 Aug 2010 13:19:46 -0600

To: (b)(6)(b)(7)(C)@gmail.com>

I certainly will. Attached is a PDF of the printed file I gave you. The file also has the additional information I looked up for you while here.

Thank you

(b)(6)(b)(7)(C)

On Fri, 6 Aug 2010 14:37:44 -0400, (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C)@gmail.com> wrote:

Let me know if you find out anything else about wiki

wikileaks_MIT_contacts_06Aug2010.pdf

Content-Type: application/pdf
Content-Encoding: base64

Prepared by: (b)(6)(b)(7)(C) 16 August 2010
 (b)(6)(b)(7)(C) @abixx.com || (b)(6)(b)(7)(C) @gmail.com
 [H] 508.883.1316 [C] 508.967.8201

This may or may not be helpful, the link below is to a (very) old (Oct 2001) email thread between Assange (proff@iq.org) and several others. Assange is looking for volunteers to help with his distributed network.

<--- Added by me to break apart messages

Link to the emails below:

<http://marc.info/?t=100320899400003&r=1&w=2>

[Below is the thread list from the above link.]

1. 2001-10-16 Re: mirror volunteers needed
2. 2001-10-16 Re: mirror volunteers needed
3. 2001-10-16 Re: mirror volunteers needed
4. 2001-10-16 Re: mirror volunteers needed
5. 2001-10-16 Re: mirror volunteers needed
6. 2001-10-16 mirror volunteers needed
7. 2001-10-16 Re: mirror volunteers needed
8. 2001-10-16 Re: mirror volunteers needed
9. 2001-10-16 mirror volunteers needed

cypherpun (b)(6)(b)(7)(C)
 cypherpun
 cypherpun Julian Assange
 cypherpun (b)(6)(b)(7)(C)
 cypherpun Julian Assange
 cypherpun (b)(6)(b)(7)(C)
 cypherpun (b)(6)(b)(7)(C)
 cypherpun (b)(6)(b)(7)(C)
 cypherpun Julian Assange

Copies of the messages are below:

#####

List: cypherpunks
 Subject: mirror volunteers needed
 From: Julian Assange <proff@iq.org>
 Date: 2001-10-16 5:03:46
 [Download message RAW]

If you are brave and have a unix account/machine with approximately 2Gig of disk free, we need you.

--
 Julian Assange |If you want to build a ship, don't drum up people
 |together to collect wood or assign them tasks and
 proff@iq.org |work, but rather teach them to long for the endless
 proff@gnu.ai.mit.edu |immensity of the sea. -- Antoine de Saint Exupery

#####

List: cypherpunks
 Subject: Re: mirror volunteers needed
 From: (b)(6)(b)(7)(C) acmenet ! net>
 Date: 2001-10-16 5:19:54
 [Download message RAW]

Julian Assange wrote:

> If you are brave and have a unix account/machine with approximately
 > 2Gig of disk free, we need you.

More details, please. Mainly the kind of material to be hosted. Holding 2GB of kiddie porn (horseman alert!) might be objectionable on moral

grounds as well as legal grounds.

What kind of traffic is expected, in terms of connections per hours and bytes per hour?

Why does it need to be a *NIX machine? Ease of remote access, security, active content, or the requirements of the mirroring software?

The mirror would presumably need a fixed IP address. Are there any other requirements?

--
(b)(6)(b)(7)(C) Computer Condottiere Have GNU, Will Travel
(b)(6)(b)(7)(C)

"Good people do not need laws to tell them to act responsibly while bad people will find a way around the laws." -- Plato

#####

List: cypherpunks
Subject: Re: mirror volunteers needed
From: (b)(6)(b)(7)(C) <zem () zip ! com ! au>
Date: 2001-10-16 5:20:00
[Download message RAW]

On 16 Oct 2001, Julian Assange wrote:

> If you are brave and have a unix account/machine with approximately
> 2Gig of disk free, we need you.

I have a machine with 2 gig (or thereabouts), located in Australia.
Bandwidth is low (64k ISDN) but the machine is available.

If high bandwidth is a necessity I know someone who might be able to help depending on the content.

--
mailto:zem@zip.com.au F289 2BDB 1DA0 F4C4 DC87 EC36 B2E3 4E75 C853 FD93
<http://zem.squidly.org/> "I'm invisible, I'm invisible, I'm invisible..."

#####

List: cypherpunks
Subject: mirror volunteers needed
From: (b)(6)(b)(7)(C) <nobody () dizum ! com>
Date: 2001-10-16 5:50:14
[Download message RAW]

To mirror what?

#####

List: cypherpunks
Subject: Re: mirror volunteers needed
From: proff () iq ! org (Julian Assange)
Date: 2001-10-16 9:56:20
[Download message RAW]

> Julian Assange wrote:

>

> > If you are brave and have a unix account/machine with approximately
> > 2Gig of disk free, we need you.

>

> More details, please. Mainly the kind of material to be hosted. Holding
> 2GB of kiddie porn (horseman alert!) might be objectionable on moral
> grounds as well as legal grounds.

Documents and images. No kiddie porn, but there are still three other horsemen to choose from. Absolutely legal for now, bar retrospective legislation, but that won't stop the horse trainers from pretending otherwise. Constitutionally protected in the US, but that doesn't mean you won't cop flak from ISP higher-up and other organisations regardless of where you live.

If you'd be happy to mirror cryptome.org, then you'd probably be happy to mirror this material.

> What kind of traffic is expected, in terms of connections per hours and
> bytes per hour?

Depends on interest. We can use dns tricks to shape traffic to reflect your resources.

> Why does it need to be a *NIX machine? Ease of remote access, security,
> active content, or the requirements of the mirroring software?

The anonymous push nature of the mirroring software. We can support non-unix pull mirrors too, provided there are enough push mirrors to feed from. The software could be ported to other operating systems without too much difficulty, but that's another project.

> The mirror would presumably need a fixed IP address. Are there any other
> requirements?

An ability to create mail-aliases, gpg, perl5, and a good sense of humour :)

Cheers,
Julian.

--

Julian Assange |If you want to build a ship, don't drum up people
|together to collect wood or assign them tasks and
proff@iq.org |work, but rather teach them to long for the endless
proff@gnu.ai.mit.edu |immensity of the sea. -- Antoine de Saint Exupery

#####

List: cypherpunks
Subject: Re: mirror volunteers needed
From: (b)(6)(b)(7)(C) () ils ! unc ! edu>
Date: 2001-10-16 13:50:37
[Download message RAW]

On Tue, Oct 16, 2001 at 07:56:20PM +1000, Julian Assange wrote:

>

> > Julian Assange wrote:

> >
 > > > If you are brave and have a unix account/machine with approximately
 > > > 2Gig of disk free, we need you.
 > >
 > > More details, please. Mainly the kind of material to be hosted. Holding
 > > 2GB of kiddie porn (horseman alert!) might be objectionable on moral
 > > grounds as well as legal grounds.
 >
 > Documents and images. No kiddie porn, but there are still three
 > other horsemen to choose from. Absolutely legal for now, bar
 > retrospective legislation, but that won't stop the horse trainers
 > from pretending otherwise. Constitutionally protected in the US,
 > but that doesn't mean you won't cop flak from ISP higher-up and
 > other organisations regardless of where you live.

Where's the site? I'm sure some of us might be interested
 if we can see whether we care about the content.

> If you'd be happy to mirror cryptome.org, then you'd probably be
 > happy to mirror this material.

Thanks for the legal advice. cryptome still has decss.zip (and I'm
 damned happy they do). Nearly every other site with it caved to MPAA
 pressure. (Publicly) mirroring cryptome isn't for the timid. Asking
 people to mirror content that might be dangerous to their status with
 their upstream provider requires some more details.

(b)(6)(b)(7)(C)

#####

List: cypherpunks
 Subject: Re: mirror volunteers needed
 From: proff () iq ! org (Julian Assange)
 Date: 2001-10-16 14:11:33
 [Download message RAW]

> pressure. (Publicly) mirroring cryptome isn't for the timid. Asking
 > people to mirror content that might be dangerous to their status with
 > their upstream provider requires some more details.

Content is not fully predictable due to the distribution system employed.
 If your upstream shoots before threatening, you probably don't want to
 mirror this material.

Cheers,
 Julian.

#####

List: cypherpunks
 Subject: Re: mirror volunteers needed
 From: (b)(6)(b)(7)(C) () well ! com>
 Date: 2001-10-16 18:20:06
 [Download message RAW]

At 07:56 PM 10/16/2001 +1000, Julian Assange wrote:
 > The anonymous push nature of the mirroring software. We can support
 > non-unix pull mirrors too, provided there are enough push mirrors
 > to feed from. The software could be ported to other operating

> systems without too much difficulty, but that's another project.

I get the impression this isn't exactly "mirroring" static content, but participating in a distributed publishing/retrieval system, a la Freenet and Mojo Nation or BitTorrent .. or maybe more like Gnutella or Kazaa .. or even Publius, which was nice but never seemed to catch on.

Is that correct?

> > The mirror would presumably need a fixed IP address. Are there any other
> > requirements?

> > An ability to create mail-aliases, gpg, perl5, and a good sense of humour :)

What software are you using? Is it well-known? Debugged? Is the source available? (well, it's Perl, I guess..)

I don't mind mirroring Cryptome, but I'm pretty wary of installing other people's newly-hacked-up code in a [quasi-]production environment .. your proposal creates two kinds of risk. The first, which is relatively familiar by now, is content risk, from people angry about the content .. the second is the risk of security problems in the code or its configuration/installation, and that sounds like a bigger issue to me.

Why not just use one of the existing distributed systems for this content? If you put content in the Gnutella or Kazaa systems, you can give us filenames or search strings and then we just make locally cached copies and leave machines running (even crappy little windows boxes) to create dispersed hard-to-clobber-them-all content. If you put it in the Mojo/Freenet/BitTorrent systems, and make the URLs of the content publically available, helpful people can make local copies of all or parts of your files pretty easily, too.

Or, alternately, make just content available as a .zip or .tgz, and let others serve it using FTP/HTTP servers they're already familiar with.

If you can find a way to separate the content risk from the untrusted software risk, this project (whatever it is) might have a better chance of success.

(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)@well.com

"We have found and closed the thing you watch us with." -- New Delhi street kids

#####

List: cypherpunks
Subject: Re: mirror volunteers needed
From: (b)(6)(b)(7)(C) tightrope ! demon ! co ! uk>
Date: 2001-10-16 21:56:00
[Download message RAW]

proff@iq.org (Julian Assange) writes:

> An ability to create mail-aliases, gpg, perl5, and a good sense of humour :)

What and where is the source?

--
1024/D9C69DF9(b)(6)(b)(7)(C)@tightrope.demon.co.uk

its ok the problem solved itself

#####

#####

<http://www.diarydig.org:8000/> - Between the Bars: Human stories from prison

#####

Google Search for "between the bars"

http://www.google.com/#hl=en&source=hp&q=betweenthebars+blog&aq=f&aql=g-sx1&aql=&oeq=&gs_rfai=CIBxwqPZaTP72j4GQzQT2JnPCgAAAKoE8U_QsRfR&pbx=1&fp=c4337c63ee7a44b

5th search result:

Between the Bars | MIT Center for Future Civic Media
 Between the Bars is a blogging platform for one out of every 142 Americans---prisoners---that makes it easy to blog on paper, using standard postal mail. ...
civic.mit.edu/projects/c4fcm/between-the-bars - Cached - Similar

#####

<http://civic.mit.edu/projects/c4fcm/between-the-bars>

Project team:

(b)(6)(b)(7)(C)

Project team:

(b)(6)(b)(7)(C)

#####

<http://civic.mit.edu/team/charlie-detar>

(b)(6)(b)(7)(C)

Master's Student in Media Arts and Sciences, MIT Media Lab

#####

<http://civic.mit.edu/team/benjamin-mako-hill>

(b)(6)(b)(7)(C)

... is a technology and intellectual property researcher, activist, and consultant.

personal website: <http://mako.cc/>personal blog: <http://civic.mit.edu/blog/mako>

#####

<http://mako.cc/>

About: I am a scholar, technologist, programmer and free software and free culture activist.
 I write software, books and articles and currently live in Somerville, Massachusetts.

<http://mako.cc/copyrighteous/>

blog indicates he's traveling to Croatia on or around 08 August 2010

#####

(b)(6)(b)(7)(C)

Public Key

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.2.1 (GNU/Linux)

mQGI8DltLVERBAC7egUzr/mMwYznp5AqIOJ8x4qgra6554Vu2UGI0i6ib0of+fg9
 bcVcu53Dck6EJtqIi5b2w74Lp7+I3DLTYqIYXGQJpDgZucab+Y4GSNH12T7
 UxUGuJlN4L/CbT1A0z9A9Z7B44//CvX+abAk9FgmF14d4/5vOqF8yQvCg9e+O
 nW1HwQdcr7YCCwhYVCFAPUEA+5XX1/jcwG119em/6XNzQVCV3/5JisOwPqkgaf
 ezYgUDWp5BxsljddfhbOVawRCBA1GRCa8V87e/SW3wPoxoavSe6V4r2r7C6xH4
 JTB9Mergx9f6mZcjhpsOJCXro2BiOnMogqrRrBazfDTCT71BbLUF2wzrcei5
 D8veA/9H0n6LY6CWP/MS8y4JRMpl+n06cldv8FgK+/s9nDlGw/q+4uqKOKMLSQCI
 CM55knfKqA3xYUvuvw5/42W2hqn++fnApt0ZU9/QuvzvcfCnzs/hvSux9W7fHj
 KYBN3QEMiy7CLOxRbDAdOeseOCn8OWks/bxkgL+TuS+CVTsHrQuQmVuamFtaW4g
 SGIstCAoTWfbykPG1ha29AYm9yay5oYV1wc2hpcmlUuZW1PohW88MRagAW8QI5
 b5Tx8AsKBAMDQFQCAwYCAQIAAKRCJZUshYHVZ5gkAJ9kTYpkKycfAQYyqh
 o53mRYMxMwCfW0tKetKIJT2MIF1PbyW5O8kx7XGIRgQQEQIA8gUCOW+dLgAKCRAS
 WFNMN+x6Auo3AJ0WQ6LewW3ypJLRD+UWwxOp8q0gwCgJVRpcxbFCofBusc9bcM0
 LEowwDmIRgQQEQIA8gUCOK+kZAAKCRD2fipdHPLWKqfAKCTfjQcD2AZJzFFO9X
 B1FqT3tqIACIT95M4ui7pxxTPIZlqkNOzr/94LGRgQQEQIA8gUCO0vscgAKCRC6
 X38NRHRWisdLAKCd3fxbjYK20Gw13oww8sJBXU99QwCgnn18kx48CWgNLATd4kQr
 Jg8xE9ulRgQQEQIA8gUCO0wY6QAKCRBD3+IKINwWetrQAKCsVQNd18/KSPAfoZat
 fNDycUxdoACeLfvOWJkQwD+kLNS1z5h4ciulKWiRgQQEQIA8gUCO156jWAKCRDn
 deMk20Gzh/EJA9xLZT5yE1O6bkaORTC295AtVvFACITze49hNWhfEgZQbOobD81
 qju+sVqIRgQQEQIA8gUCO139JQAKCRACkx/k9VivQU1AAJ9y4EgmoRHD7wOGvFw4
 U5HOgQIACISf38wM5x11WYVn5KWndcs+tUm3yIRgQQEQIA8gUCO4MUIAAKCRK/
 458lafimgdQAKCR0xdPwZn+GOFnH1L/LvOGG85+3QCggo5V3DEPxmrmu593L+uw
 n921XfSIRgQQEQIA8gUCO5a+QAKCRD1zmjrb/CR818sAJ9CRWCTuWexgcGNpm/U
 XxvAZz1PKACfCpZa7a5mE57WjW5oFgg6p4H/rqIRgQQEQIA8gUCFJWUwWAKCRDe
 Ig+0cu3HJ5JA9uv51ZbVusCZvBhC4E1+wwwDlwCdhb3W0jrgJEh8+avHS/Ok
 UXkrFT+IRgQQEQIA8gUCPjCgwAKCRG5qzbzKpD54hd/AKCHgzt4hbUQCuyDo7c6
 kTel+cm6IQCEPXRGSYau5iSepzNihQdvN3WJ7/SIRgQQEQIA8gUCPC6ZAAKCR80
 StdKdZ5FDwRAJ4DZTqJrDMV4no2yZyHsPzAgTrcwCf8h/kvLR4hr+CboU6Z7Q
 HXQvSOIRgQQEQIA8gUCPOAQIAQCRCBqarLdvSd/rnWAJ9VfKz95VU+FcRCDJ
 1i06b118ACfYq6CUK7MqWGRmoD2lp/P+Zd7+0SIRgQQEQIA8gUCPQTpCAAKCRCE
 NYTon6H5XTdIAKCHz881yY8Psv6lWwlsdCoJhsrvAgCg158gSEWTS9b1nRYKwW8
 7T+GabalRgQTEQIA8gUCPSKOWdAKCRAuLP27d5amC1RJA41h56DO1+pGxkR1R1R1
 l3adDcy+SwCdFsx7C6nlu5aFyGrclhOOhbJX5KIRgQQEQIA8gUCPSJ/JAAKCR2
 z7pEjFrhDYZAKCOW5+Aza8vL4RwB2wXOx85/ufyQCXGCKnO9f3BwqW4WJsYof
 xNDClG6IRgQTEQIA8gUCPSKPRgAKCR8JrkoCdA0h5YAKCwbl2UdTxSLTV5
 ETRKPEaqtgCISQumK7ajLx27/nHbs04Yr2Hx2AJUDBRA9J814q/8HtEbzi508
 AUAtA/9L2IV3FagTws5vMhNR5+x2Xk08fhwTOWYfJ8c0YmI0oU9IMV5/necnTE
 5K5IDoQrCb+ypmdk2lxgU8vE3jotAxFl1dyYtqNgldBD1aVy4Ec1R750ETIS+
 4V8DvypRgW9aATyF033CHH57be+q+jclriccC6VMr05JJP4kYhG8BARAgACBQ9
 J8l0AAQJEMZf5JsKCSknLgAolJtmnQaM3IFDu1UHQobiM5IODcAJ4vQRvOqP+b
 pOOkPWYFqXq9LtlY4hG8BMRAGACBQ9JyzyzAAQJENsEChQJ17m8ctcAmwVbWADD
 faAA9BIZCRIZCtE9AZ/AJ4rVRWR57MhYY0uDb09LrTxh+MW4hG8BMRAGACBQ9
 KkmeAAQJENraec14J9MS4EAnAq+RQIZghaC4A4wZKJJOYp6m8AKDOMUDDBLpD
 /GK+qObuWm213zsjhG8BMRAGACBQ9LcG+AAwQEA6nVfU5EP1tV0AoKJAtLp0

PwEXI2Eb9LQyHyXitO3MAj0X7DPfM1wrqlxpign+OallezxdgihG8B8RagAGBQI9
 LCPnAAQjEEhs1UnEBNIEHAB8AnRq6XasB0AFVg23k2kxH+Lo5RFJA9NU5uJFHQW
 JGCI3DUTUY7qIEJThihG8B8RagAGBQI9LQ1AAQJECaKVT/2ZskdTVMAhJUEI5TC
 GIVFV6N0gHjhcSuanGTJA9B7YsUB92dCw4U3pF9xRuPaYUohG8B8RagAGBQI9
 MGfSAaQjEOaY7NL8IXZ80AnRkxmpSmnlb25Eulcs9D79c5/vwHAJ0cWTPVUFY0
 6lch8IX8lnQICuAvhG8B8RagAGBQI9LDKAAQJEEKfrmdTVol7J30AnihLhZr
 fMS5FLjw85MlbnadkpaJ4sanpqhAFDlW2leVolIdN/D7KohG8B8RagAGBQI9
 LM25AAQjELndEjOT8GFVqKAQJpFYhoOgcsVtM6mFgoyathc9xAKCSH79EKATN
 mKuKM7vtTG61zXGwnhG8B8RagAGBQI9MLwAAQjEMlJfuu5125YhAnRNPsgoK
 PiGv2Zzt8VYroovPef89AJ450+eP3qS86AWoowjK9vATIST94hG8B8RagAGBQI9
 K6lnAAQjEPnKAcXlami80dz8An3hPFSLZV24IqV5p95qnfAydm2AKCPQ4YrSimL
 agZCadd9UXn8j65jYhG8B8RagAGBQI9MqYAAQJEKO4lpZlYV3+48AR81dgpN
 nNtYwVqJ2glt8nV79x4AJoc919fJb8OCyHex8zzxlatwnlGohG8B8RagAGBQI9
 S5TAQJEDVzMSRagnotz94An3CET9+heqJCI9JlWNfzJITZpAKC85thQ66AN
 OhUdTu1+lhpgp07qthG8B8RagAGBQI9SVLUAAQJEC5nwkFyzwGoxAYAN03k88Yx
 nmF98wQJdrZlHjwHXLUMAJ45FK+teWfk+WcQXtvLvdP7G6alohG8B8RagAGBQI9
 Zc84AAQjEjFohWlv/FXMA8AoMxtGIDQbJZXNEK65q8mJCK75psAJ9VtqE4Y0y8
 hQ83yHYZU9IE3ZEWYjCB8MBAQAGBQI9P9yJAQJEUkhOQCS7Z+H64FY/OyqSfB
 V05GvWx1y7DMRCepJLNS6OUwHg20211m8o+P9PI7DPVL6mx8IS2xa8MXUQcn8
 lqvQw/jAH/4Z52v3Z2Ytuc8pUyPehrD82k0w08eUsK9UvXsIn8GCSEJMFqHOLI
 hJ7TAlvGTJ87XfU5WJXvR4KddJn8GhshFbksYh8+3xJ21Kf5K802ohA12we
 LFXPwPctXpuxZap2eE8+wzWxG7PjQJew+nstPzdC1K1hL2Fib2AUQeAohG8B8R
 agAGBQI9P9yJAQJEO5X/LjdWj7FFyAJ13FikNQJl/eo+m7qz8LP2MDLnAJ9Q
 S0R9P0xbGrh8YhG5G70K0dCihG8B8RagAGBQI9J7PLAAQJENVOkymHChky8A
 nJwZJULN8ToUZAFK9RtkQd5JBAKCV/XCNDV/Aqm9w/jA4H9v9f+pgvYhG8B8R
 agAGBQI9I8RAAQJECmRDC5V0Rhu8eKAnOyNf+te0u3M12+dwe7AOIQmN9RkADI
 wPrcV5bVHF/AcM0tqzAHc0Cr4hG8B8RagAGBQI9aT8AAQJEAkii8QQRHddmR4A
 nA4ZzOMloq1KggLy847J8vXSPUDAKCTeFF6rlb/pVmDwaJ5VPVGuoH3W4hG8B8R
 agAGBQI9Zd8RAAQJELXgHF3meNChU0QAnjWbJkVJQglnTjrMxQIdTxc1F21AKCM
 bx3/Ofat3eT5K5eCy8KJ7t04hG8B8RagAGBQI9aTDHAAQJEMg9K9YRtk6wPZQA
 oLmclucCNygnNDUHGKJ/Cxvujug9AJ9K2k8Kw1dRklw/NzNMUQJWWSfAYhG8B8R
 agAGBQI98I9HAAQJEFDSaIX2z14eatAAnI76EM6Bvix9Z1K8B8UmwW7z67E1AJ9I
 fS0HL/rxRyN6ohsM2bW9+ZihG8B8RagAGBQI9+HalgAAQJENQC8RtjnGpV51cA
 n1J4208k055uEn9hsOI1+JXKyDPyAJ0Qdhhqy1HLU8mjh+M80N2RKSZZYhG8B8R
 agAGBQI9+H1CBAAQJECm+XSJO/V5fCg4AnI8V4eAAU38DjCDS8B8KIB+Yd9AJ46
 JKTfJ/BcKmmGqH6rOHC635yYhG8B8RagAGBQI9+H1J0AAQJEAOS2Pb0EpV0rUYA
 nRjw7JGWPRA4PDwpFSI+FOpFZf0AJ9UwysQkH8a6D1q5KwL515mfQm4hG8B8R
 agAGBQI9+H3fRAAQJELac8XhY5SinopAaC0gNg0Jp4u55opaf0a2EULQm4hG8B8R
 rlcnyZ1gRgM40gE2ZcyYrIm7YhG8B8RagAGBQI9+H9QJAAQJEOJNYQzCJ9nCLAA
 oKibxAKKfIZUB8QndAeK5gmAJ9NAQJAJ16Jjpoht+7z9Cn8ILK4hG8B8R
 agAGBQI9+H1mAAQJELwvKwVXfRf4AnioFttA4OmrfE5t1b3t+0AvwmgTSAJ9d
 WbC/75QJLukJ2DoOHZzOSCHY2thG8B8RagAGBQI9+IBXUAAQJEOV6KVizRz7g5MA
 n2xPzW7C8Fy3cltyxWjset8B8AJ9celVbnV5VQslwWxVULdqlhA8hG8B8R
 agAGBQI9+H+AAQJECGr8mOxrpBghUan22ZpOHCRUJq5Hm8TgyikRdWmU0AJ9S
 evHqGhg0Ne3wWqN/SYmfnfWYhG8B8RagAGBQI9+IFR+AAQJEB8SRCCX8pM+Z6EA
 n3g5kSTGa977Xs6M74K5DgagPCCAKDDOY1yr/x/it+co8sv+bdHHP97fblhG8B8R
 agAGBQI9+IeX5AAQJEN56r26UWxj/JTQAmwHQP99VfM8x5VLYW6EKCWZ3Y3AJ9y
 314wtlts3p3m5YlHw5sCcl8qXohG8B8RagAGBQI9+lu8yAAQJEDsymJ0A88/kGNEA
 n1Oyo6m00Jig30PwJ9f5vAgMGDSBAJ9In8n2wJRDs8MKQJm4+9dneHNg8YhG8B8R
 agAGBQI99LZAAQJEAFAxx3RAGCs/OAOCn0klfxDCJGH90EG3nEh55xN/uAKCV
 F5Kw58FdbXW02VhZ8XdgJ384hG8B8RagAGBQI9+IZ/UAAQJENR9PQYKbXv+voA
 njag73fZcuc74YyQ7x8SvYesqU8AJ40N5I5YV8d0e0qJz75H7CJ50lCB8B8
 AQAGBQI9+JESXAAQJEQZQRkdEqAW1ApoD+wZ/WOkeOBfya8Hm1k+EHX+IVjnJSU
 O/KFORZldfyk105K5vhG+h2gDnmMa4G43fxpM5h0QeZaPJ8YoxirMnn8wQ05/
 YMUacFwzCELd1YgQ7P7RSEAM0/7spm+Lg/aB/1IAU3HV9izVB+sdXFPn22e6fHNI
 DllU7V6y5y7TIEYEECAAYFAJ4KtV4ACgkQ8T8A8dzVzGKTscgCAEhWH+7Wmrl
 h69YU+44auPRFVoAn0y8N3I6lv33R0CpAeb5ehfDulIEYEECAAYFAJ4KtGIA
 CgkQ8Z8k25E2S80nmngCelrisb5ZG5ZwloXA2rXKUpprM5A0NANN0U2IqI5mOHX
 AJ9SdoC1UGGIEYEECAAYFAJ4IIMACGkQJegJo1TbM9OfXQCFcd5Spp/q25w
 9KQ2X92KQWJH9UAnRdmwHXQetkznMsnTo+Hg9730hAFIEYEECAAYFAJ4pdwIA
 CgkQCIp23DZGZmurlWcWgkLhP3xv5Ae9QmZ25dP8CgD3KAn3yUaBEFP0uKQo
 K7N3OyEBYQmIEYEECAAYFAJ4pKIAcGkQhQKdeHWCwipQKvCfVdmA+N4+rumu
 XIKpsd1Prd+7w8AnjwJUP0dcioEnRwMHQCSFzLURCIMEYEECAAYFAJ4y0a
 CgkQRLAlg5I5Jm0sgCnfmR8XQYVlq/EQYQm6Gy4AmuDSZowCdhPNF7aIh5f
 r8KQuh8eq5IEYEECAAYFAJ7N5fEACgkQYm6Gy4AmuDSZowCdhPNF7aIh5f
 oWGCvenUS8J2VowwAJC8h8f8xswuN058K2TYWY49XUPeIEYEECAAYFAJ7h2uIA
 CgkQVwAaxwfnjgP8wCJFCfnyp8F8+OpIOWYjwldN92NcV5An2D6KlhfQCEfmoQ
 3wqthL1FQYIEYEECAAYFAJ7pn1QACQkQlGfI0YXJ218gCeN1231Pzgx00
 6P+O/J4WhtF2rLIAn1EpzPLZ/125KLU7H2QCd1XmE1CZCZW5qYw1pblisAWXs
 ICHNYWtKSA8bWf8bXZwJpYw4ub3JnPhW8B8RagAWBQJ57Y2I8XsKAWQDFQMC
 ACYXCAQK8AAKRCJZushYHVZ5gszAJwMK8/Rx3s0mu1Z+/AJQCI8XpE5JACgypnD
 PEvhCZDbLaO89xyDf0+4DmRlgQEQEIA8gUCOK+kbWAKCRD2fipdHPLWksplAJ96
 ybu2L6LwfnQ9Nk1Mhn5qNqTfCbnuLdmxv4prlN1MwRoc2OA1g6IRgQEQEIA
 BgUCO0v5IAAKRC6X38NRhRwlrIAJDRCEzRRDeMXuFgZ2IISuAkd9ZQACeM8U
 I7x0On43qyPZL/pkeDqJ2IRgQEQEIA8gUCO0wY7AAKCR8D3+ikInWwesiCAJ9x
 dElbu13Yw5VXRMAu8F8AW5I3wCenV4th5HUKR5Agv02GYgoH8BilwIRgQEQEIA
 BgUCO135LAAKCRDndcMK20GzhwVJAKCDVYUWQAS5Rwv12580l5ywlUe09QCfAunc
 B6MoQ7VdUcU5KVmh2govMyRgQEQEIA8gUCO139KAAKCRKacK9VIVQWQAKCQ
 SV1H+8Teuf51RISxH1THRerHpgCgn5VR+UkVPTUx29zxf6FPNFW8c6IRgQEQEIA
 BgUCO4MUJAAKRCJ/458layfImnyAJ9idZ/9e+4hLCr80rQNYaZIm0PewCgrU6u
 i0CSU8KskRTGZq4YjPBXqmlRgQEQEIA8gUCO5a+FwAKCRD1ZmJb/Cr8mXNAJ99
 PU9RbnTG6vkrU34W/V7anIFACVJ55I+keZV6kpbBokwIPkDialRgQEQEIA
 BgUCPJaxCAAKRCW5VJUX2mZmAKCnXGKwx/5lwrFCJkx0R7J4Jg6Gcgwzcm
 foCee+ntg8XZL8zQmYX13+IRgQEQEIA8gUCPJaxWwWgAKCRDelg+0cu3JhCwAKCS
 Jd1erQoQokuTfPzq7u09E3NZCg9Xp1MCMXCBW3JmWe3JH1+IlnAlRgQEQEIA
 BgUCPJaxCAAKCRAS+PYr+7+gFKAAC/26bIEJRZod5UNfGihy8VllecK8vp
 pZ39PCPZpWpW774L428VulRgQEQEIA8gUCPJc0wAKCRCSqzbKp5J4EpAKC
 hBLz1V8CgrHz7H/198k8eHgcQcguN7ZleAJakXCI8mbSAK0JgNX6IRgQEQEIA
 BgUCPJc6agAKCR805tdbKZ5fK9CAKCAmQXZLAJ815SHaxFnuP7WkYgCepBVZ
 CBR3z/JwbQKcSAHIBRHuCI8gQEQEIA8gUCPOAQJAKCRbaarlDvds/mKSAJ0Z
 Eqs5rDl8IDliskph25mdTPBeACf8bnf+X8f8R-Rt0B6eQpIA7/WeOIRgQEQEIA
 BgUCPQTpCAKRCENYTonh5Xf9EAKCXc2RnkgTydcS8U8J2gxEK24PFCgCgZ7Ti
 Cp0K8M2Qg4a68gUS12Q7YlRgQEQEIA8gUCPSK0fAAKCRaUlpZ7d5amC33SAJ9J
 Y+Vt0RJ4h0J8OH6UxVhgnAcaCg9cChXTQYF8JQI6v3U2CkxTh13aGIRgQEQEIA
 BgUCPSJl/wAKCRA2z7PdeFhN49AJ9pZcKRGQJEUyq6FXRr1QH+pWQVwCdf91s
 HsG1JGEX52f7UhtCI1tMgCIRgQEQEIA8gUCPSKFTQAKCRJxRkoGdA0hugQAKCB
 e8rkpP/W258T9Iy8D5G3RPM+gCel8M9b/Uf0bDn4wEwQHM+S3JlqPWAJUBDRA9
 J8I6q/8HtebzIS08A9hBAC1RCURCW8mdkPvu1x8RbW42mHNU9J3fzfnJ2W54vG
 mX121emPM9M3pHlRkXHyaoatpmvrf4+RoJpJ8DKRpxN3U0j+VvXKJldpUQymK0
 Aq+zn1N4t80rdVleqyPtm01b5XqywwZLmHdtaF2CtkQwP35X72L9k6IBGQJ0fe21
 a4hG8B8RagAGBQI9J8I2AAQJEMZf5J5KCSknGYAANAtplQmAnVaDwaOIS5c1+f9
 c0orAJ900t6dpyfngSUnX36H8RgsEQ054hG8B8RagAGBQI9Jy4AAQJEN5EchOJ
 17m8IzoAoMzHl/I06qZGyV+R5lawaowsmPlarAKDCbkuUIEXQ3pduQJ587QCMg240
 w8hG8B8RagAGBQI9KkmFAAQJENraec14Ij9MAAYAcLYTzThv/vIZTQJ58rcalc

z4HNAJ4noSG1hDQF+7z24M1b+GkPzVzKtHGB8MRAGACBQI9LCHJAAQJEA6NvRUU
 SEP1dFsAn2Q7Uy09gQ/v3gA29MizvCTGPaJ4wab+7AGkwtFaB6+8K+ObX1x1
 U4hGB8IRAGACBQI9LCPpAAQJEEhS1UnEBNleobwAn1dIHNTpQFomZ/YFXAY5Hb
 unHUAkCI86ibcpH2WY0vZbCbKeQ9zqAYhGB8IRAGACBQI9LQ5AAQJEGAKV7/2
 Zskds9gAn0foGGFE7d32rUOCz8WVwscX8YIMAKCC6AaQln379Vul6NeHj1pSj2
 p4hGB8IRAGACBQI9MGFVAAQJEOaY7NL8uIXTu0AnZaCvcV52VPecg6ymWeKd4n
 /rEAKDWAUmdj+YtmwEVWw/BwvH8EeYhGB8IRAGACBQI9LQdAAQJEGKfrmdT
 volJhIAn1Rzbpkl/W56VQJczfAxKXKXQwIAJ9TK6HHACyWT+jgk83C43K+FJJG
 A4hGB8IRAGACBQI9LMA8AaQJELNDEJTBGfVFPQwAqJlYnXSHZmIxMNG63aUGOLA
 ZPCJAKCZ2KmFCarx5o4f3aL8d5z1MQfYhGB8IRAGACBQI9MLxYAAQJEMIOJfuu
 S125hBQAOJHmklx3hNy83sao+B3eXJ/EGhmXAKCClabTSNdskycl6z2uoxymzhdV
 DYhGB8IRAGACBQI9K6lqAAQJEPnKAdXiam8oDgYAOjs0fImn2iUx+IAu0dNwX
 lwiQAJ4/1wivgWzm1MjashArc5Gh0vQ1w4hGB8IRAGACBQI9MQY0AAQJEDK4p2l
 fV3KWQAn1OPLKIH8qJzCdp5Dz8a3sIGCMACc1h7vPvAODSY9w3q1mPwqNix
 rYkGB8IRAGACBQI9NHMIAAQJEA7IK7Cj1YpjaUD/A83LAKESZzUw9SXXAQC4UAm
 examNBUDJ9xZng5NL0nHLDQ3NMWw+LoW/WGReSjICLUB5aMQ/MZ/BryHR0L
 USz7NINUNgZky94QO+5z0MFVmMvMzhWVW3Vcx1+2fzowOpINnGGOhKGS1q/
 ARDU3Bbw0MIRIEB04+/5yIEEEXECAAyFAJ1KxPEACgKQXKMyFqCel2AMACfehbM
 W1L8ZaVUutVhCN8TOUj5DoAn3p6AqJdy64VCvpONfE1H4Mu1e3IEEYEECAAyF
 AJ1JhAgCgkQZXFAP/LPzAJZgCfQeFNgwP03aymS8kbpGz4kXPcAnr0PJULQ
 OY+JeO269+7KeQ6FQKteIEEYEECAAyFAJ1JzAgCgkQWfA0l/8Vc9ACVQug
 BqB+xE0IUTDrKv27qkxAcQJL0XpFC7FV5H3q54nObKwXkLZyZmWEEBAAYF
 AJQ/InIACgKQp5S5CnN6EXQAX+YrYwKz5JfD49/NDFT1TQo/wX+ckWrl9Ch
 VSAHLO4jy4cdxrs+LD7FyEc2Ne54JzyDdE4V51mT/1am5Y591LNCBx6vIZRI
 Rbkqa2b4LPx+QJ2QLWIGDj/11ugqutUrmC90PDZyFETfzykF1fRxiU2e7YB
 APneWepE0ADZ17fj2fWcSNJ8XJzR8Df51JyDv0aGakweYyY1T2w/IVdGYB0uFF
 OwjS1LYXgncxAS05vYhLzW7EWTZaZIEEYEECAAyFAJ0/KJoACgKQ7Hkv81YITV6
 IACdFmeVDA77312l/4IYFAN8Nl0wYgAn03VKGSZ4N4+hjQLadyQeLUdNevIEYE
 EEECAAyFAJ1WgHIAcGkQ7IXePzBd+MRZACFR+8bFBKcdgr1GtYhBntLrkA0A
 n1RWdIt/Kdgr5L94w51aQJ35i0iEYEECAAyFAJ2LS9MACgKQ1U6u58mYcLH6
 6QCdDLZjckUYHWR05w7DQ54WLC66eUAmwajvWk4M8eWTSVDCXb04Fggc+8IEYE
 EEECAAyFAJ2LyxAcGkQZaZemL/RGCG6sUACGmQW/JVape5Vdyh2X2fW3KdQ8A
 nRP2zCSK77KeYCPxKEUyepK5vviEYEECAAyFAJ1pMHAACgKQCSK0F8BED10S
 TACeladrLMAvKgdmtETUtd947T1HNUAnjSjUQtWk0wKwLkEAB3rCsrzFIEYE
 EEECAAyFAJ110G8ACgKQeAcXeZ4DaHLNwCg2qCv0FGXm52eUatVLLDUqtzoA
 oKRfb/f4KvUdHLM5UBhdYCN8M6BIEEYEECAAyFAJ1pMMAACgKQD2TJNGS3rCS
 oCQgvxRzSLhQWntfLzQmGn1IPWLnagA0J3nj2HfPn1pbrXXIEE8sbuPtiEYE
 EEECAAyFAJ3Wj2gACgKQUNJqfVbP6h94wCfUuewxMlgfUzAb1420Y3vQKX/HYA
 nRuJ15v0kS1Tm1kxj9wpleU/ZCIEEYEECAAyFAJ4d0IsACgKQ1ALXG20CY+8+
 HACEODVIdEJDFDSQbLZ37qmgZgK8AnjcdCmaQcNoFbGQBUOJUT56R5gIEYE
 EEECAAyFAJ4fUJ0nGACgKQK5h9j9Vj++QwCCGbuF8dEwv1y7p3s+dz7aQ4A
 n0zge4FMpQ4b0q723p0QKPMYhAIEYEECAAyFAJ4RWOQACgKQ465Y9vQ5KQA
 kwCBNOR8aATmTYT4LooEu3ED2ccT8A0LdKzHTgxbu08UlyRc5b0661QKIEYE
 EEECAAyFAJ4fVSOACgKQ0zKYNQDz+RQPCG1Ww0KNsoJ8U8Uy449vPskJ1sA
 nAtqP9aZn+d2hys4VxcPmnbNI7HwIEEYEECAAyFAJ4f4+YACgKQtpzwxIEJf8
 +gCdGna7sQIUlnVak7VxN2TAXAbhg0YA0PAW0B0c2ps4ARVC3U4KPKVodCUIEYE
 EEECAAyFAJ4f1CkACgKQ41VDNz+L2CLfwmC8b1MN4A6vM84+eCYRTDDWqkLWAA
 n1wAatW7B7+SwmJZeM1klvZzRHd0IEEYEECAAyFAJ4f+aaACgKQnC/GTAHVf9+H
 pQCdFdwZ5kivWp55Sg6UwdMzcdv+6EAmwSufFo9EDWys3x6MNEWFGZ2HJKEyIEYE
 EEECAAyFAJ4fGfWACgKQ5bopWLOdHPDCAcGkNNfUbsJ6lrMPCaZww4hMSCKMAA
 oINEXbntle+k42e/FFD7JrsAGMJIEEYEECAAyFAJ4fUKUACgKQ5VJpDIWVfInz
 PgCg+gNWmVcfAYCkwyVMOgwet/SnnEaONN68LW07LFCFRvksfotQodg91wIEYE
 EEECAAyFAJ4f44msACgKQ7soSMHY9r1BJTgCgPZWJ/G2pd50FjclPcwltblypiboA
 oJaaJUpj6dQpbWNBH55UuvdAPrMIIEEYEECAAyFAJ4f72cACgKQJasGY7GukGBF
 pwcFQ5SDFdrBrYJXg+n1ZqAR6+q+O8AnJXPTkz0TqE28d0XufatitsfAIEYE
 EEECAAyFAJ4fGfWACgKQIPW4crEwDjsejCggyQlI6nAc4acNkKopUluo/3hxcA
 oOe+ezeQF7yCbmYaswu0hskuc5mIEEYEECAAyFAJ4fGhNUACgKQHDk8B53yAbWg
 +ACeOEXDsxCL/+aEHvPYhN75aT8ICKAnJpHY4Aev/Eg1Kf6j08xG2BE2K3MIEYE
 EEECAAyFAJ4fGfWACgKQZ2IEUcKlye/ucCFVDRM484+od6h4USTV4GEQBmf7gA
 mglIKfJUMU4zFTMN+evN96Ez7OSBIEEYEECAAyFAJ4fGfTACgKQ8Astmz5aFmR
 QCGxWjJ/+IPdYEEH69Z83Q1z126ABQAOmUj39QK27B0Qn+TWkzCTGEEUIEYE
 EEECAAyFAJ4f45TEACgKQ3nqvbp7AnIh/n/wCeOUEd4B08+SRH8IKT3wgNyLwJoA
 nRvYcdB1KtuDV8BbU5YMDotZRP7IEEYEECAAyFAJ4fIHVACgKQNFChpqpFDJnw
 FgCgUJNAU0U0B0RfXqJZ5rO+2bspsvAn3CA70FLOgLEWQJ4dvd5KCI8fALQCY
 AWUQIPf6QZK8K5eAWIAQJH9wQAO41/QWAMRqE5MBf8/B0f0PjpeOCTNEZF
 5I95/VjiedopJmW071CLAE0UDRLVpJdFQcLeH+TzY2WnZpJp09mWOC
 kw74uzad0o7VfUkEXPyS1+qJlJg0B0Wk9R85Zyazavx/DEGmsXDS+m8WJgF5
 q2I2u1mIRgQQEQIABgUCPIFFmWACR8PwDx3NXMYpO0AACUCZUGqJ4Z11nCSkUv
 h6HEEGRa4wCeMcl9lwnhHKC9+6rZ20waYHu30+IRgQQEQIABgUCPIF542QAKCRAB
 QMcD0YABrwDXAKDxwzV6E5LSQ28uEmMjLQ17bIqCF50EifYkLJ48S7z5bElv
 YLOFF6SIRgQTEQIABgUCPIFGwAKCRDUFT0Cm858gKAJ4x8TK/btq9jsqj6Jf
 EIdNSAawgCgkLT0d085mJ8bE7J46hOzYcW0Pi+IRgQQEQIABgUCPIcmewAKCRB4
 zJdXlPmISYAJ9YJFTOYRV2Yw8FqNfCJoGP+Iz12ACVQMdnTSQHEPPkMOMTY
 4JhWVKIRgQTEQIABgUCPIRN+wAKCRDxGTbKnnzYrUAJ48A0UTTW+2Lcfs56zK
 b1NWGS9AACdE8ImVx3mro7HG43g+qJ0U1YKwKIRgQTEQIABgUCPIWwWwAKCRCU
 SD+JVNsz05m1AKCSQAUI/EaQscjoo0ApekNFuvUaQCGwNFUxT4j7kxKTOdn2/6Q
 utVZlxylRgQQEQIABgUCPII3CQAKCRABWnbFQZma6oRKAJ94R9LxLPNn5sE0rsQh
 ooY8mbDNACRwNDgOv123eR2y8x7Z7IZTcmreSylRgQTEQIABgUCPIJ8pAAKCRCH
 Rd14dYLCGndHAJ44ckitJFEVUeZWjWn818ch/5kgCdF6N+3zT0n7ggF24yXXCO
 kZgIDLOIRgQTEQIABgUCPJL/RAAKCRBEsCKDk+wywOCAJ9ZswWrdM6S29R10KST
 QJzXzLn5SgCgtITWwZJCEBwJw74s/6TxGrxFmIRgQTEQIABgUCPz2wUQAKCRBU
 zpJgCa4Pjv+AJOV0hVpNnH7L2XVWsoJlJc/6Lk88PgCgqL27W/TB6f6lQafC882T
 JLYL86IRgQQEQIABgUCPUFlQAKCRBWSDFAWKIOISmAJ0eU1vikGA+kCQyAKJa
 lvHqWd0vTwCFVQgC1AVqEv+MbSX01YK26OhCEaIRgQTEQIABgUCPUmFWAAKCRAI
 88WU7JclnV8VAKCMz1VjnmEIZPhCTOvCFHqJkUwCQIBAVndgC3J6ZP2LEC0
 17Eajpu5Ag0EOWDvRAIAOXHuc5JHME09Cdf0OIH/H66kkIEZv+ZNDVYXf8
 7GXD7k80NAAv54RQ4pzi9am5h8BE6GHAlem2Myw51+5NKpx5US+E1zCQ6ZGu
 Ju9KATR2K6xENpNRWmUkMSWkrmtT8LEnF1+OS/yexOJ7UykyKT2/m4K3/sbkJj
 pq+Yct+QzETP2UHRrkRfVr4YRjG6MRxSwWou986wxt+1Q0ataCYC+K0PER7Xv
 T4XURJczf2061J7aZLQOY7p/NUViz0wSnNoR/XZQ8mUQF8wQ2Nw/Wah/YkVo+
 myGdg+FYH5x6nf6khwk6KcKdrALPeS1vdxQbncAAwUJ/2+T1WY7dyPn2Eqp
 JdXtnfz5OXnePqol+6faV+/CJFwMV+ol1akeKW1x9J0V5bN1P8DczVCHSnC1wNl
 We3b8orEvzEmpn7fQz8FYQX/KWY6ukD5e/JiemX06azix0rkM8rgJ1Nj56c
 +Av6ISJ75brgRN6sgSMC20gIO5IZaKRSnMvInhYidCniMjTfP3J+n8TInbShVjeA
 H6f1GW98UqKEgcB/Cn0d3NGCPwB+LhjTEEPcn9HvSuspo+wDUlJlD6KXtlU4w4
 pJf9JQSNf/w8FBIGThz5IZlyU8PspGUYC/adZ5T8aGAJE8JA1ggc82uQL8r
 XLatSuelRgQTEQIABgUCOWvNCAKCRCKJzUshYHVZ5mdCAKDEvbqQ5wB+76ss4gG3
 BHEJxK1yNACDEOHJzAJC9bXmPrtKv0HW1q5QJG8=

```

(b)(6)(b)(7)(C) ping iq.org
PING iq.org (203.24.247.1): 56 data bytes
64 bytes from 203.24.247.1: icmp_seq=0 ttl=51 time=286.360 ms
64 bytes from 203.24.247.1: icmp_seq=1 ttl=51 time=286.146 ms
^C
--- iq.org ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 286.146/286.253/286.360/0.107 ms
comsec:~ (b)(6)(b)(7)(C)
comsec:~ (b)(6)(b)(7)(C)
comsec:~ (b)(6)(b)(7)(C)
comsec:~ (b)(6)(b)(7)(C) whois 203.24.247.1
#
# Query terms are ambiguous. The query is assumed to be:
# "n 203.24.247.1"
#
# Use "?" to get help.
#
#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=203.24.247.1?showDetails=true&showARIN=false
#

NetRange: 203.0.0.0 - 203.255.255.255
CIDR: 203.0.0.0/8
OriginAS:
NetName: APNIC-203
NetHandle: NET-203-0-0-0-1
Parent:
NetType: Allocated to APNIC
NameServer: TINNIE.ARIN.NET
NameServer: SEC1.AUTHDNS.RIPE.NET
NameServer: NS4.APNIC.NET
NameServer: NS3.APNIC.NET
NameServer: NS1.APNIC.NET
NameServer: DNS1.TELSTRA.NET
Comment: This IP address range is not registered in the ARIN database.
Comment: For details, refer to the APNIC Whois Database via
Comment: WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment: ** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment: for the Asia Pacific region. APNIC does not operate networks
Comment: using this IP address range and is not able to investigate
Comment: spam or abuse reports relating to these addresses. For more
Comment: help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
RegDate: 1994-04-05
Updated: 2010-08-02
Ref: http://whois.arin.net/rest/net/NET-203-0-0-0-1

OrgName: Asia Pacific Network Information Centre
OrgId: APNIC
Address: PO Box 2131
City: Milton
StateProv: QLD
PostalCode: 4064
Country: AU
RegDate:
Updated: 2004-03-01
Ref: http://whois.arin.net/rest/org/APNIC

ReferralServer: whois://whois.apnic.net

OrgTechHandle: AWC12-ARIN
OrgTechName: APNIC Whois Contact
OrgTechPhone: +61 7 3858 3188
OrgTechEmail: search-apnic-not-arin@apnic.net
OrgTechRef: http://whois.arin.net/rest/poc/AWC12-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#

% [whois.apnic.net node-1]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

inetnum: 203.24.247.0 - 203.24.247.255
netname: SUBPUBACCESS-AU
descr: Suburbia Public Access Network
descr: 3 Bray Street
descr: North Sydney
descr: NSW 2060
country: AU
admin-c: MD72-AP
tech-c: MD72-AP
remarks: ** Conversion note - reference 'MD11-AU' changed to 'MD72-AP'
remarks: Record imported from AUNIC as part of AUNIC->APNIC migration
remarks: Please see http://www.apnic.net/db/aunic/
mnt-by: APNIC-HM
status: ALLOCATED PORTABLE
changed: nobody@apnic.net 19960304
changed: aunic-transfer@apnic.net 20010525
changed: hm-changed@apnic.net 20041214
source: APNIC

person: (b)(6)(b)(7)(C)
address: Suburbia Public Access Network
address: (b)(6)(b)(7)(C)
address: (b)(6)(b)(7)(C)
address: (b)(6)(b)(7)(C)

```


phone: (b)(6)(b)(7)(C)
e-mail: (b)(6)(b)(7)(C)
nrc-hdl: (b)(6)(b)(7)(C)
remarks: This data originated from AUNIC, and was copied as part of
the AUNIC to APNIC migration. <http://www.apnic.net/db/aunic/>
remarks: Original nrc-hdl in AUNIC: MD11-AU
mnt-by: MAINT-AU-MD72-AP
changed: nobody@aunic.net 19981112
changed: nobody@aunic.net 19990922
changed: aunic-transfer@apnic.net 20010523
source: APNIC

#####

Subject: Assange Information

From: (b)(6)(b)(7)(C)@abixx.com>

Date: Fri, 06 Aug 2010 19:53:16 -0600

To: (b)(6)(b)(7)(C)@gmail.com>

I'm not sure if you are aware of these other email aliases, but I've found these on the web as ones that Assange has used in the past and might still be utilizing:

proff@iq.org

me@iq.org

proff@suburbia.apana.org.au

proff@gnu.ai.mit.edu

proff@suburbia.net

proff@four.net

strobe@suburbia.net

I've also attached a archive of a email thread I came across from back in 2001 of

Assange asking for volunteers to help with what I'm guessing eventually became WikiLeaks.

You may or may not already have seen that, but in my search, I came across it and wanted to pass it along.

Thank you

-(b)(6)(b)(7)(C)

On Fri, 6 Aug 2010 15:23:50 -0400, (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C)@gmail.com> wrote:

Thanks for your assistance, let me know if you find out anything else of value from the archived blog. Keep searching I am sure something will break for you in the employment or business game.

On Aug 6, 2010 3:19 PM, (b)(6)(b)(7)(C)@abixx.com> wrote:

I certainly will. Attached is a PDF of the printed file I gave you. The file also has the additional information I looked up for you while here.

Thank you

(b)(6)(b)(7)(C)

On Fri, 6 Aug 2010 14:37:44 -0400, (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C)@gmail.com> wrote:

Let...

Assange_eMail_asking_for_volunteers_emails.pdf

Content-Type: application/pdf
Content-Encoding: base64

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

RUI NUMBER

0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Between 1140 - 1505, 13 Nov 10, SA (b)(6)(b)(7)(C) recorded PFC MANNING's visitation period at the Marine Corps Brig - Quantico, Quantico, VA 22134. PFC MANNING was visited by Mrs. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)

About 1226, 15 Nov 10, SA (b)(6)(b)(7)(C) reviewed the digitally recorded conversation between PFC MANNING and Mrs. (b)(6)(b)(7)(C) which took place on 13 Nov 10. The conversation was limited to family matters and contained nothing relating to the investigation. The recording was transferred to compact disc (CD) and SA (b)(6)(b)(7)(C) collected the CD as evidence on a DA Form 4137, Evidence/Property Custody Document (EPCD), DN 167-10.

////////////////////////////////////LAST ENTRY////////////////////////////////////

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Washington Metro RA, Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

SIGNATURE

(b)(6)(b)(7)(C)

DATE

15 Nov 10

EXHIBIT

258

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

001673
Approved

(b)(6)(b)(7)(C)

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 28-10-CID221-10117
0483-10-CID014-

PAGE 1 OF 1 PAGE

DETAIL

About 0930, 17 Nov 10, SA (b)(6)(b)(7)(C) interviewed SPC (b)(6)(b)(7)(C) 501st CS BN, FBTX, who related he was not in Basic Training between Oct 07 -Dec 07, but was there during on Jan 08. SPC (b)(6)(b)(7)(C) related he had no knowledge of who PVT MANNING or PVT (b)(6)(b)(7)(C) were. SPC (b)(6)(b)(7)(C) further related he was never in an altercation with anyone wherein he was stabbed by a pencil or any other object.

AGENT'S COMMENT: SPC (b)(6)(b)(7)(C) did not match the description provided in SPC (b)(6)(b)(7)(C) statement.

About 0950, 17 Nov 10, SA (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) and briefed him on all aspects of this investigation. SA (b)(6)(b)(7)(C) related no further investigative activity was required.

STATUS: All requested investigative activity has been completed and no other investigative activity is anticipated. This case is being closed within the files of this office. ///LAST ITEM///

TYPE AGENT'S NAME AND SEQUENCE NUMBER

SA (b)(6)(b)(7)(C), (b)(7)(E)

ORGANIZATION

Fort Bliss CID
Fort Bliss, TX 79916-6350

SIG (b)(6)(b)(7)(C)

DATE

17 Nov 10

EXHIBIT

259