

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 1 OF 4 PAGES

DETAILS

About 1843, 29 May 13, SA (b)(6)(b)(7)(C) coordinated with MAJ (b)(6)(b)(7)(C) Trial Counsel, Military District of Washington, Office of the Staff Judge Advocate, 210 A Street, Suite 300, Fort McNair, DC 20319, who provided three (3) pages of Defense Reciprocal Discovery which were received from PFC MANNING's Defense Counsel. The three (3) pages of Defense Reciprocal Discovery were identified in two (2) PDF files, numbered 028711 through 028713, dated 29 May 13, which appeared to depict communications between PFC MANNING and an individual using the account name (b)(6)(b)(7)(C) (NFI), sent and received within the internal YouTube website messaging system. MAJ (b)(6)(b)(7)(C) requested this office examine these documents and provide additional information in relation to the YouTube account used by PFC MANNING, further identified as "bradmanning", which was previously unidentified during the course of this investigation.

AGENT'S COMMENT: The Defense Reciprocal Discovery items appeared to depict a screen capture of PFC MANNING's YouTube account showing selected 'Sent' and 'Inbox' messages; specifically, a message sent to (b)(6)(b)(7)(C) and a message received from (b)(6)(b)(7)(C) were shown. It was noted within the Defense Reciprocal Discovery document numbered 028711, the screen capture shows seven (7) "Inbox" messages, one (1) "Shared with You" items, and six (6) "Contact Notifications" within the PFC MANNING account. However, in the second Defense Reciprocal Discovery document numbered 028713, there are three (3) "Inbox" messages, no "Shared with You" items, and three (3) "Contact Notifications". There was no information provided to explain the discrepancy between the two documents in relation to the numbers of messages, contact notifications, and shared items within this account. At the time of this investigation, YouTube was identified as a video sharing website owned and maintained by Google, Inc.

About 1140, 13 Jun 13, SA (b)(6)(b)(7)(C), (b)(7)(E) this office, met with the Honorable (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) U.S. Magistrate Judge, Eastern District of Virginia, 401 Courthouse Square, Alexandria, VA 22314, and obtained a Federal Magistrate Search Warrant, from the U.S. District Court for the Eastern District of Virginia, Search Warrant Number 1:13-SW-446, for the YouTube account "bradmanning" maintained on the computer systems of Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043. The "bradmanning" YouTube account had been identified as an online video sharing account used by PFC MANNING and was believed to have information relevant to this investigation as selected messages had been provided by PFC MANNING's Defense Counsel as Defense Reciprocal Discovery.

AGENT'S COMMENT: It was noted PFC MANNING's Defense Counsel only provided selected sent and received messages, and it was unknown what other communications this account may contain between PFC MANNING and other individuals. During a review of the publically available information related to PFC MANNING's YouTube account it was noted some videos were marked 'Private' as well as videos previously uploaded by PFC MANNING that were deleted were not viewable. During the course of this investigation it was alleged PFC MANNING had previously created and uploaded videos to YouTube which reportedly contained classified and/or sensitive information about training facilities at Fort Huachuca, AZ, where PFC MANNING attended his Advanced Individual Training (AIT) course.

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, Quantico, VA 22134	
SIGN (b)(6)(b)(7)(C)	DATE 16 Sep 13	EXHIBIT 411	

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

002130

Approved

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

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 2 OF 4 PAGES

DETAILS

About 2147, 17 Jun 13, SA (b)(6)(b)(7)(C) executed the Search Warrant by faxing the Search Warrant to Google's Legal Department as well as emailed a copy of the Search Warrant to Google's Law Enforcement Response email address.

AGENT'S COMMENT: A previous attempt to execute this Search Warrant by fax on 13 Jun 13, was made; however, subsequent contact with Google, Inc., on 17 Jun 13, revealed this Search Warrant had not been received by Google, Inc.

About 1701, 19 Jun 13, Google, Inc., provided a response to the executed Search Warrant which consisted of a two page document which identified: the "bradmanning" account was associated with PFC MANNING's known email account of "bradley.e.manning@gmail.com"; the "bradmanning" YouTube account was an active account created on 27 Jul 06; and the account contained three (3) messages sent between 14 Feb 10 and 16 Feb 10, within the YouTube messaging system to/from the "bradmanning" account and another user identified as (b)(6)(b)(7)(C). Additionally, the provided Search Warrant results identified six (6) videos which had been associated with this account between 27 Dec 06 and 26 Apr 08, but had been deleted; and that the "bradmanning" account had been recently accessed on 23 May 13 and again on 29 May 13.

AGENT'S COMMENT: A review of the Search Warrant results identified the YouTube communications showed the "bradmanning" account had contacted (b)(6)(b)(7)(C) to comment on videos posted by that user; wherein the "bradmanning" further identified themselves as "Brad", mentioned they were a soldier assigned in Iraq, and discussed gender/sexual issues they (presumably PFC MANNING) were experiencing. It was noted four (4) of the deleted videos identified in the Search Warrant results, were uploaded and/or associated with this account on: 14 Apr 08, 25 Apr 08, and 26 Apr 08, while PFC MANNING was attending AIT at Fort Huachuca, AZ. While the recent access to PFC MANNING's YouTube account on 29 May 13, was likely made by PFC MANNING's Defense Counsel, it was unknown who had accessed this YouTube account on 23 May 13; although this was also presumed to be PFC MANNING's Defense Counsel.

About 1957, 25 Jun 13, Google, Inc., provided a supplemental response to Search Warrant 1:13-SW-446 which contained a listing of the 39 videos associated with the "bradmanning" account. These videos were listed by time and date the videos were associated with the "bradmanning" account, and a unique eleven (11) character identifier for each video was provided.

AGENT'S COMMENT: A review of the videos associated with the "bradmanning" YouTube account identified two videos of interest which were associated as 'Favorite Videos' with this account. The first was the video titled, "Collateral Murder - Wikileaks - Iraq" (YouTube unique identifier "5rXPrfnU3G0") which had been uploaded by the user "sunshinepress" and contained the content of the Apache Video believed to have been wrongfully disclosed by PFC MANNING. The second video was titled, "The Listening Post - Trading coverage for access?" (YouTube unique identifier "Oi9tf7m7sic"), uploaded by the user "AlJazeeraEnglish" and contained news media discussion of the disclosure of the Apache Video. It

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, Quantico, VA 22134	
SIGNAT (b)(6)(b)(7)(C)	DATE 16 Sep 13	EXHIBIT 411	

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

002131

Approved

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 3 OF 4 PAGES

DETAILS

should be noted based on the Search Warrant results provided by Google, Inc., these videos were associated with the "bradmanning" account on 16 Apr 10 and 19 Apr 10, respectively. It was also noted the YouTube account "sunshinepress" appeared to be associated with and/or under control of personnel associated with WikiLeaks.

About 1105, 5 Jul 13, SA (b)(6)(b)(7)(C) met with the Honorable (b)(6)(b)(7)(C) U.S. Magistrate Judge, Eastern District of Virginia, 401 Courthouse Square, Alexandria, VA 22314, and obtained a Federal Magistrate Search Warrant, from the U.S. District Court for the Eastern District of Virginia, Search Warrant Number 1:13-SW-492, for the YouTube account "bradmanning" maintained on the computer systems of Google, Inc. This second Search Warrant was issued in order to obtain copies of the six (6) videos identified as having been deleted from the "bradmanning" YouTube account and the one (1) video associated with the "bradmanning" YouTube account which had been marked 'Private' and was not available for viewing by the general public.

AGENT'S COMMENT: A second Search Warrant was obtained as Google, Inc., failed to provide certain information such as the content of the video associated with the "bradmanning" account which had been marked 'Private', details related to other messages sent/received by the "bradmanning" account within the YouTube message system, as well as detailed information on the videos identified as having been deleted. The failure to provide this information was due to a dispute by Google, Inc., in relation to the wording of the previously obtained Search Warrant obtained on 13 Jun 13.

About 1737, 5 Jul 13, SA (b)(6)(b)(7)(C) executed the Search Warrant by faxing the Search Warrant to two separate numbers associated with Google's Legal Department as well as emailed a copy of the Search Warrant to Google's Law Enforcement Response email address.

Between 1030 and 1151, 16 Jul 13, SA (b)(6)(b)(7)(C) manually downloaded thirty-eight (38) of the thirty-nine (39) video files associated with PFC MANNING's YouTube account using the Google, Inc., provided YouTube unique identifiers.

About 1526, 16 Jul 13, SA (b)(6)(b)(7)(C) collected one DVD disc containing two (2) PDF files, "final prod 331257 (19 Jun 13).pdf" and "final prod 331257 (25 Jun 13).pdf" which were the Google, Inc., provided Search Warrant results from Search Warrant 1:13-SW-446; and thirty-eight (38) of the identified video files associated with the "bradmanning" YouTube account. DVD was retained as Evidence/Property Custody Document (EPCD), Document Number (DN) 075-13.

About 1645, 16 Sep 13, SA (b)(6)(b)(7)(C) received the Search Warrant results from Search Warrant 1:13-SW-492, from Google, Inc., which contained additional details related to the "bradmanning" YouTube account. Specifically the provided documents gave additional detail in relation to other messages associated with PFC MANNING's YouTube account, associated YouTube Contacts, and dates/times that previously identified deleted videos had been deleted. The results also included a video file which had been associated

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, Quantico, VA 22134	
SIGN (b)(6)(b)(7)(C)	DATE 16 Sep 13	EXHIBIT 411	

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

0028-10-CID221-10117

PAGE 4 OF 4 PAGES

DETAILS

with PFC MANING's YouTube account which had been marked 'Private'. A review of this video revealed the video contained political content and was titled "Newsom for California" and appeared to be related to State of California Lieutenant Governor Gavin C. NEWSOM.

About 1710, 16 Sep 13, SA (b)(6)(b)(7)(C) collected one Compact Disc (CD) received from Google, Inc., which contained seven (7) PDF files related to videos associated with PFC MANNING's YouTube account that had been deleted, additional messages related to PFC MANNING's YouTube account, and one video file related to the video identified with the YouTube unique identifier as "BH0jnyuJ1Tg" and marked 'Private' within the "bradmanning" account. The CD was retained on EPCD DN 099-13.

////////////////////////////////// **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, Quantico, VA 22134

SIGNATURE

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

DATE

16 Sep 13

EXHIBIT

411

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

002133

Approved



Upload

bradmanning

Video Manager

Video Editor

Subscriptions

Analytics

Inbox

Settings

Inbox (7)

Personal Messages

Shared with You (1)

Comments

Contact Notifications (6)


Video Responses

Sent

Address Book »

Sent

1-2

<input type="checkbox"/> To	Subject	Date
<input type="checkbox"/> KimberATL	Re: Re: Thank you (and my story)	02/16/10
<input type="checkbox"/> 	Thank you (and my story)	02/14/10

KimberATL

Hi Kimber,

I don't normally message people on YouTube but I'm going to make a particular exception for you.

I just wanted to thank you for having the courage to post your videos, and tell your story. I've found it very educational and inspirational, as well as emotional. I mostly admire your honesty about the situations that you have encountered in over the last year or so.

Now for the stereotypical reflective story:

My name is Brad, I'm 22 years old, and I've had issues with my gender identity and sexual orientation throughout my life. I've always known I was "different", but could never pin down what it was. I was often made fun of at home and in school of for being "effeminate", "girly", "faggy", etc. just for having different interests and behaviors. But, as I grew up, I always wanted to fit in. So, throughout adolescence I tried very hard to fit in, and I was very successful in doing so: I joined sports and athletic teams, gained a "charged" and "aggressive" attitude. I avoided, and over time somehow self-denied my interests in more "feminine" things. I still very secretly and occasionally cross-dressed and maintained a few of my interests, but would somehow deny even to myself that I ever did. This all started to break away when I finished school and started my own life, however I still wasn't quite sure what it was that was bothering me so much. I had admitted and was living openly gay by this point (4 years ago), but still didn't quite feel right. I don't know how, or even why I did, but in a quick few weeks of confusion and denial, I enlisted in the Army for four years. It's been over two years since I did, and now over the last few months of being deployed in Iraq, I'm finally starting to come to terms with my own identity.

However, figuring out my identity under my current circumstances is not a very safe situation to be in. I'm surrounded by hyper-masculinity and aggression in a somewhat secured (compared to 2 years ago), but still dangerous combat zone in a foreign country. I'm trapped, and don't know what to do, or who to turn to... I have at least 5 months left in Iraq, and a year and a half in Army. Watching your videos with my... okayish broadband connection in my trailer out here, has been a massive relief, and an inspiration for me. I finally know what I want, and know that... at some point, it will be achievable and will work out.

In fact, while I was on my mid-tour leave, I finally gained the courage to buy a nice natural looking wig (I've got a military regulation hair cut), go into Macy's, buy a gorgeous casual business outfit... a subtle toned set of make up from Sephora, and a coat from Square One (because its so COLD in the States right now)... spend a few hours getting everything right, and I actually spent a solid day, in public, dressed a woman... and PASSED. I was both proud of myself, and relieved. Sadly, I cleaned up everything, put everything away, and waited a couple more days, and I gave it another go... and did it one more time after that... 3 out of 15 days were spent dressed as a young twenty-something woman. I knew it felt more "right" than before. I even think I've found a name for myself: "Breanna" (or maybe "Breanne", just a syllable difference)

Sadly, I had to head back... and now I'm back in the desert... alone, and with literally nowhere safe to go.

Anyway, thats just my little story. It's just so hard because all the defenses and walls I put up by denying it have placed me here, in the middle of nowhere, with no real friends, and no safe avenues of support. But, yet, somehow, I know it will probably work out, as long as I don't start denying it all over again.

And again,

Defense Reciprocal Discovery

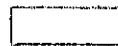
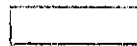
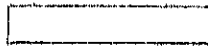
028711

Thank you,

Brad or maybe "Breanna"



YouTube



About Press & Blogs Copyright Creators & Partners Advertising Developers
Terms Privacy Policy & Safety Send feedback Try something new!



Upload

bradmanning

Video Manager

Video Editor

Subscriptions

Analytics

Inbox

Settings

Inbox

Inbox (3)

Personal Messages

Shared with You

Comments

Contact Notifications (3)

Video Responses

Sent

Address Book »

1-1

☐ From

Subject

Date

☐

KimberATL

Re: Thank you (and my story)

02/15/10

Omg thank you for that :)

that really meant alot to read and have someone sit down and write all that.

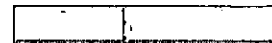
Everyone's story is different and unique. Not one person will live the same life as another. The choice you made to go to military was out of comfort, there was a future and still is a future in it for you. Though yes your time is on limit and and you still have more time to serve in the end you can say that you completed that part of your life. Dont get to held down, My drag mother (Another drag queen\ transgender) Sonique, was in the army to. She is on LOGO on Rupauls Drag Race 2. She went through the same things you are and she is finally starting to transition into a woman. she's 26.

Dont ever let this bring you down, it's not your fault. The fact that you can accept it is great, I remember in the beginning for me it was really hard just to accept the fact I was transgendered and I let it really get to me. But one day things just made since and I realized that this is me, and actually Im proud to be me, because Im in the next generation that is going to make a difference in this world. The transgender issue is slowly but surely getting more and more open and accepted but the unfortunate part though is there are people who really do not want to see us happy and will be the biggest obstacles.

And dont think your not making a difference on me either. Sonique's boyfriend Billy Vito just got back from iraq maybe a year ago? He was out there and found me and her on myspace. they started talking and he moved to atlanta just to be with her and got a job as a police officer.

I hope this letter finds you well
Keep your head up my dear, as long as you keep the finish line in your head then thats all that matters :)

xoxo- Kimber

[About](#) [Press & Blogs](#) [Copyright](#) [Creators & Partners](#) [Advertising](#) [Developers](#)[Terms](#) [Privacy](#) [Policy & Safety](#) [Send feedback](#) [Try something new!](#)

028713

Defense Reciprocal Discovery
FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 412
002136

Exhibit 413 and 414

Page(s): 002137 thru 002163

These documents, “Search and Seizure Warrants” are considered public documents.

The USACIDC does not have the authority to release; therefore, the documents can be retrieved at the clerks’ office where the documents were filed.



0028 10-CID221-10117

DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATION UNIT
DIGITAL FORENSICS AND RESEARCH BRANCH
9805 LOWEN RD
FORT BELVOIR, VA 22060-5536

REPLY TO
ATTENTION OF

CISA-CCI-DF

16 Jun 10

1. **Case Number:** CAF 0028-10-CID361/ROI 0028-10-CID221-10117
2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA
3. **Date of Report:** 16 Jun 10
4. **Examiner:** SAC (b)(6)(b)(7)(C), (b)(7)(E)
5. **Summary of Analysis:** The items in question were three Arabic language instruction compact discs and of no evidentiary value.

For Official Use Only
Law Enforcement Sensitive

EXHIBIT 415
002164



Forensic Report for DN 067-10, Item 6



Table of Contents

1.	CASE NUMBER.....	3
2.	INVESTIGATING OFFICE.....	3
3.	DATE OF REPORT	3
4.	EXAMINER	3
5.	ANALYSIS	3
5.1	EXAMINATION OF THE COMPACT DISCS.....	3
5.1.1	<i>Voucher information</i>	3
5.1.2	<i>Pertinent Information</i>	3
6.	SUMMARY OF EXAMINATION.....	3
7.	EVIDENCE DISPOSITION:.....	3



1. Case Number

CAF 0028-10-CID361/ROI 0028-10-CID221-10117

2. Investigating Office

Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA

3. Date of Report

16 Jun 10

4. Examiner

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

5. Analysis

5.1 Examination of the Compact Discs

5.1.1 Voucher information

Item 6, Evidence/Property Custody Document, Document Number 067-10, consisting of three Arabic language instructional compact discs.

5.1.2 Pertinent Information

The three CDs in question were production Arabic language instructional compact discs and were not of evidentiary value.

6. Summary of Examination

The items in question were three Arabic language instruction compact discs and of no evidentiary value. The other CD collected under this Item and Document number was of evidentiary value and was discussed in other forensic reports.

7. Evidence Disposition:

All evidence was placed into the evidence room of this office.



Forensic Report for DN 067-10, Item 6



Report Prepared/ Approved By:

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

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

Special Agent-in-Charge

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER CAF# 0028-10-CID361
ROI# 0028-10-CID221-10117

PAGE 1 OF 9 PAGES

DETAILS

Between 15 and 18 Jun 10, SA (b)(6)(b)(7)(C), (b)(7)(E) conducted a preliminary forensic examination of the forensic images of SSG (b)(6)(b)(7)(C) personal laptop computer, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 073-10, Item 1.

FINDINGS:

Operating System (OS) Information:

Product Name:	Windows Vista (TM) Home Premium
Current Version:	6.0
Registered Owner:	(b)(6)(b)(7)(C)
Registered Organization:	Hewlett-Packard
System Root:	C:\Windows
Current Build Number:	6002
Path Name:	C:\Windows
Product ID:	89583-OEM-7332157-00061
Last Service Pack:	Service Pack 2
Product Key:	
VersionNumber:	
Source Path:	
Install Date:	12/14/08 09:42:58
Last Shutdown Time:	05/28/10 11:14:56

Figure 1 – OS data showing the registered owner as (b)(6)(b)(7)(C)

Time Zone Information:

All dates and times shown in this report are Eastern Time (GMT -4:00) unless otherwise noted.

Keyword Searches:

Keyword searches for the terms in Figure 2 produced numerous hits that indicated a user utilized the examined computer to access data related to Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and other items related to this investigation; however, no evidence of the possession or transmittal of classified material was identified.

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	
SIG (b)(6)(b)(7)(C)	DATE 18 Jun 10	EXHIBIT 416	

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361

ROI# 0028-10-CID221-10117

PAGE 2 OF 9 PAGES

DETAILS

"Embassy	Hannesson
100427_203012	iceland-profile
12 JUL 07 CZ ENGAGEMENT ZONE	
30 GC Anyone.avi	icesave
12 JUL 07 CZ ENGAGEMENT ZONE	
30 GC Anyone.wmv	JONSSON
	LOOKING FOR ALTERNATIVES TO
	AN ICESAVE REFERENDUM
199.56.188.121	Mr. Company Computer Guy
199.56.188.122	ncd.state.sgov.gov
199.56.188.53	Net-Centric Diplomacy Version
199.56.188.71	NOFORN
199.56.188.73	NTNCDDOSWS1SB
199.56.188.75	NTNCDDOSWS2S
199.56.188.76	NTNCDDOSWS3SB
199.56.188.79	NTNCDDOSWS3SB
88.80.12.160	NTNCDDOSWS3SB
88.80.2.32	NTNCDDOSWS3SB
\\22.225.53.205\QDrive	NTNCDDOSWS3SB
\\22.225.53.205\TDrive	NTNCDDOSWS3SB
adrianlamo	NTNCDDOSWS3SB
assange	NTNCDDOSWS3SB
backup.xlsx	NTNCDDOSWS3SB
bradass87	NTNCDDOSWS3SB
breanna.jpg	NTNCDDOSWS3SB
collateral murder	NTNCDDOSWS3SB
dates.csv	NTNCDDOSWS3SB
dump2.csv	NTNCDDOSWS3SB
farah	NTNCDDOSWS3SB
files.zip	NTNCDDOSWS3SB
gmail.com	NTNCDDOSWS3SB
Gunnarsson	NTNCDDOSWS3SB

Figure 2 – Keywords used to search examined drive

References to (b)(6)(b)(7)(C) and (b)(6)(b)(7)(C) were found in numerous locations on the disk, such as in a text fragment found in physical sector (PS) 308287239:

TYPED AGENT'S NAME AND SEQUENCE NUMBER		ORGANIZATION	
SA (b)(6)(b)(7)(C), (b)(7)(E)		Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE	(b)(6)(b)(7)(C)	DATE	EXHIBIT
		18 Jun 10	416

CID F

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

002169

Approved

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

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361

ROI# 0028-10-CID221-10117

PAGE 6 OF 9 PAGES

DETAILS

```

Visited: [REDACTED]https://twitter.com/statuses/user_timeline/147937041.rss.....0...
b.m.a.n.n.i.n.g.f.m.'s'.T.w.e.e.t.s'.....i%~P%i%~PURL.....B^!_ûf..B^!_ûû.Ô<c.....
.....h...p.....L.....<hd.....i%~P%Visted:[REDACTED]https://twitt
er.com/favorites/147937041.rss?.....8...b.m.a.n.n.i.n.g.f.m.'s'.F.a.v.o.r.i.t.e.s
.....i%~P%i%~P:://mail.google.com/mail/?hl=en&shva=1-?.....8...https://mail
.google.com/mail/images/favicon.ico.....C.m.a.i.l.-.-C.o.n.f.i.r.m.y.o.u.r
.T.w.i.t.t.e.r.a.c.c.o.u.n.t.,.b.m.a.n.n.i.n.g.f.m.!...b.r.e.a.n.n.a.e.m.a.n.n.i.n
g.@g.m.a.i.l.c.o.m.....i%~P%i%~P%i%~P%i%~P%i%~P%i%~P%i%~P%i%~P%i%~P%i%~P%i%~P
i%~P%i%~P%i%~P%i%~P%i%~PURL.....@.Ó.^ûû.@.Ó.^ûû.Ô<c.....h...p
i.....<cd.....i%~P%Visted:[REDACTED]https://twitter.com/followers~P~P
....T...https://s3.amazonaws.com/twitter-production/a/1274739546/images/favicon.ico
...X...T.w.i.t.t.e.r./..P.e.o.p.l.e.w.h.o.f.o.l.l.o.w.b.m.a.n.n.i.n.g.f.m.....
i%~P%i%~P%i%~P%i%~P%i%~PURL.....è%~ûû.è%~ûû.Ô<c.....h...p.....

```

Figure 10 - Text referencing Gmail and Twitter accounts believed to belong to PFC MANNING as "Breanna"

References to both “bradley.e.manning” and “breanna.e.manning” were found in numerous locations on the disk, including indications that someone accessed and managed those email account from the examined system.

References to “wikileaks” were found in numerous locations on the disk, primarily in the Internet history for the “swamp rat” user. The “wikileaks” references in the active Internet history on the disk all appear in sites last accessed between 22 and 24 May 10. Many of the pertinent references to “wikileaks” appear to relate to searches for or the accessing of stories related to the (b)(6)(b)(7)(C) video release”, as well as searches for Wikileaks on Twitter and FriendFeed.com.

Examination of the C:\Users\██████████\AppData\Roaming\Google\Local Search History\google%2Eweb.w file revealed what appeared to be the content of the user's Google Web History file. Google Web History is an add-on function of a user's normal user account that allows the user to view and search across the full text of pages they have visited, including Google searches, web pages, images, and video and news stories. The contents of this google%2Eweb.w file appear to relate to PFC MANNING's interests.

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 18 Jun 10	EXHIBIT 416

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361
ROI# 0028-10-CID221-10117

PAGE 7 OF 9 PAGES

DETAILS

lady.izabella.
 plus size thongs for women.
 watertown new york florists.
 nonverbal communication examples.
 examples of nonverbal communication.
 meaning of hand gestures in different cultures.
 meaning of holding hands by men.
 meaning of holding hands by men in europe.
 meaning of hand holding between men in asia.
 meaning of hand holding between men in europe.
 meaning of smiling in europe.
 cultural meaning of smiling in europe.
 meaning of smiling in middle east.
 culture meaning of smiling in middle east.
 mypay.
 bass pro shop.
 boat trader.
 probass shop.
 honda motorcycles.
 honda motorcycles.
 probass shop.
 aafes.com.
 sports authority.
 new york bow hunter safety classes.
 watertown atv dealers.
 watertown new york atv dealers.
 example of a philanthropic business model.
 metric conversion.
 wikileaks.
 (b)(6)(b)(7)(C) f.s.f.
 (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)
 (b)(6)(b)(7)(C) wikileaks.
 (b)(6)(b)(7)(C) french classified.
 (b)(6)(b)(7)(C) france.
 wikileaks.
 gmail.pgp.
 vpn.
 m.h.y.s.
 syracuse therapist lgbt.
 skype download.

Figure 11 – Excerpt from google%2web.w file

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

18 Jun 10

EXHIBIT

416

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361

ROI# 0028-10-CID221-10117

PAGE 8 OF 9 PAGES

DETAILS

```

.z.u.m.a.
(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)
.s.y.r.a.c.u.s.e.
.i.n.t.e.l.l.i.g.e.n.c.e. a.n.a.l.y.s.t. p.o.s.i.t.i.o.n.s.
.f.o.r.m.e.r. i.n.t.e.l.l.i.g.e.n.c.e. a.n.a.l.y.s.t.
.m.h.y.s.
1.6. u.p.p.e.r. m.a.r.k.e.t. s.t.r.e.e.t. h.a.v.e.r.f.o.r.d.w.e.s.t. w.a.l.e.s.
.z.o.r.t.o. i.n.c. h.u.d.s.o.n.
.s.o.u.t.h. h.u.d.s.o.n. o.k.l.a.h.o.m.a. c.i.t.y.
.i.n.t.e.l.l.i.g.e.n.c.e. a.n.a.l.y.s.t. 3.5.f.
.g.p.g.
.u.n.l.o.c.k. m.i.t.
.u.n.l.o.c.k.e.d. m.i.t.
.u.n.l.o.c.k.e.d@m.i.t..e.d.u.
.g.n.u.
(b)(6)(b)(7)(C)
.m.h.y.s.
.d.r.e.a.m. i.n.t.e.r.p.r.e.t.a.t.i.o.n.
.d.r.e.a.m. i.n.t.e.r.p.r.e.t.a.t.i.o.n.
.i.n.t.e.r.s.t.a.t.e.
.i.n.t.e.r.s.t.a.t.e. m.a.c.
.i.n.t.e.r.s.t.a.t.e. m.a.c. f.o.n.t.
.g.e.n.e.v.a. f.o.n.t.
.g.e.n.e.v.a. f.o.n.t.
.t.y.p.e.f.a.c.e.
.r.e.a.l.i.s.t. s.a.n.s. s.e.r.i.f.
.i.n.t.e.r.s.t.a.t.e. s.a.n.s. s.e.r.i.f.
.b.u.t.t.e.r.f.l.y.f.x.
.b.u.t.t.e.r.f.l.y..f.m.
.d.c. f.r.e.e.l.a.n.c.e.
.f.m. d.o.m.a.i.n.

```

Figure 12 – Excerpt from google%2web.w file

```

.m.h.y.s.
.h.u.f.f.i.n.g.t.o.n. p.o.s.t.
.p.a.i.n.t. s.h.o.p. p.r.o. m.a.c.
.g.i.m.p. v.e.r.s.u.s. p.h.o.t.o.s.h.o.p.
.m.e.g.h.a.n. f.a.c.e.s.
.t.a.g. s.i.z.e.
.k.e.y.w.o.r.d. s.i.z.e.
.k.e.y.w.o.r.d. f.r.e.q.u.e.n.c.y.
b.o.s.t.o.n. r.o.o.m.m.a.t.e.s.
.t.i.n.g.t.i.n.g.s.
.m.h.y.s.
.c.o.n.n.e.c.t.i.v.i.t.y.
.c.o.n.n.e.c.t.i.v.i.t.y. w.i.r.e.l.e.s.s.
.c.o.n.n.e.c.t.i.f.y.
.c.o.n.n.e.c.t.i.f.y. f.o.r. v.i.s.t.a.
.d.o.w.n.l.o.a.d. c.o.n.n.e.c.t.i.f.y. f.o.r. v.i.s.t.a.
.t.u.r.n. v.o.u.r. l.a.p.t.o.p. i.n.t.o. a. w.i.r.e.l.e.s.s. r.o.u.t.e.r.
.g.e.n.d.e.r. i.d.e.n.t.i.t.y. d.i.s.o.r.d.e.r.

```

Figure 13 – Excerpt from google%2web.w file

The google%2web.w file also appeared to contain the "Work Experience" section from a résumé pertaining to an "Intelligence Analyst (35F)".

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 18 Jun 10	EXHIBIT 416	

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361
ROI# 0028-10-CID221-10117

PAGE 9 OF 9 PAGES

DETAILS

LEADS:

1. Interview SSG (b)(6)(b)(7)(C) to determine if he allowed PFC MANNING to utilize his personal computer during the 22-24 May 10 timeframe.
2. Interview SSG (b)(6)(b)(7)(C) to determine if he is responsible for accessing sites related to or has had interaction with Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) or Wikileaks.
3. Preserve content of "breanna.e.manning" and "bradley.e.manning" Gmail accounts, and the "bmanningfm" twitter account.
4. Determine significance of search items shown in Figure 11-13, including "unlocked@mit.edu" and the address in Wales.

-----///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

18 Jun 10

EXHIBIT

416

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361
ROI# 0028-10-CID221-10117

PAGE 1 OF 3 PAGES

DETAILS

Between 0955 and 1001, 18 Jun 10, SA (b)(6)(b)(7)(C), (b)(7)(E) this office, obtained a forensic image of the 2GB "Corner Office" thumb drive (unknown serial number), reported to be property of Mr. (b)(6)(b)(7)(C)

Thumb drive make/model/capacity: Corner Office, 2GB
Thumb drive serial number: Unknown

Method of imaging: FTK Imager v2.9
Type of Image: Encase (.E01)
Make and model of write block: Tableau Ultrabay II hardware USB write-blocker

The image was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of both message-digest (MD5) and SHA1 algorithm hash values with no errors.

MD5 Acquisition Hash: 861e9f766235fb17b3d15141970d78f0
MD5 Verification Hash: 861e9f766235fb17b3d15141970d78f0

SHA1 Acquisition Hash: a3ee6a82a19408b64a1de1ce2aa3e204498475d2
SHA1 Verification Hash: a3ee6a82a19408b64a1de1ce2aa3e204498475d2

Between 1006 and 1012, 18 Jun 10, SA (b)(6)(b)(7)(C) obtained a forensic image of the 2GB "DANE-ELEC" thumb drive (serial number 2VE029554), reported to be property of Mr. (b)(6)(b)(7)(C)

Thumb drive make/model/capacity: DANE-ELEC, 2GB
Thumb drive serial number: 2VE029554

Method of imaging: FTK Imager v2.9
Type of Image: Encase (.E01)
Make and model of write block: Tableau Ultrabay II hardware USB write-blocker

The image was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of both message-digest (MD5) and SHA1 algorithm hash values with no errors.

MD5 Acquisition Hash: e63624207afc10fc86be0431164848aa
MD5 Verification Hash: e63624207afc10fc86be0431164848aa

SHA1 Acquisition Hash: cdbdfb82874030f387cd46b3fffc3d77b2c3f91b
SHA1 Verification Hash: cdbdfb82874030f387cd46b3fffc3d77b2c3f91b

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

SIGN

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

DATE

18 Jun 10

EXHIBIT

417

1 FEB 77

ONLY - LAW ENFORCEMENT SENSITIVE

002177
Approved

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

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361

ROI# 0028-10-CID221-10117

PAGE 2 OF 3 PAGES

DETAILS

About 1125, 18 Jun 10, SA (b)(6)(b)(7)(C) transferred the EnCase images pertaining to Mr. (b)(6)(b)(7)(C) thumb drives to one Digital Versatile Disc (DVD).

About 1128, 18 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence one DVD containing the EnCase images pertaining to Mr. (b)(6)(b)(7)(C) thumb drives from the forensic computer, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 085-10.

Between 1145 and 1215, 18 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of each thumb drive to determine its contents. Both thumb drives were scanned using Symantec Endpoint Protection, v11.0.4000.2295r22, but no malicious files were identified.

The "Corner Office" thumb drive contained four (4) user files, all of which are listed below.

Name	File Created	Logical Size
bradass87.html	5/25/2010 18:40	90,314 bytes
LOG1.RTF	5/25/2010 21:55	14,656 bytes
LOG2.RTF	5/25/2010 21:56	37,159 bytes
otr_print	5/25/2010 18:43	36 bytes

The "DANE-ELEC" thumb drive contained four (8) user files, all of which are listed below.

Name	File Created	Logical Size
5-21LOG4.RTF	5/27/2010 18:54	1,082 bytes
5-22LOG3.RTF	5/27/2010 18:54	37,155 bytes
5-23LOG2.RTF	5/27/2010 18:53	37,159 bytes
5-24LOG1.RTF	5/27/2010 18:53	14,656 bytes
b-523logX.rtf	5/27/2010 19:14	14,656 bytes
Hackers Wanted.mp4.mp4	5/27/2010 19:43	729,574,543 bytes
manning_pgp_jan_2010	5/27/2010 21:53	1,768 bytes

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

18 Jun 10

EXHIBIT

417

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE

002178
Approved _____

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF# 0028-10-CID361

ROI# 0028-10-CID221-10117

PAGE 3 OF 3 PAGES

DETAILS

Screenshot-1.png

5/27/2010
19:34

116,127 bytes

The log files were provided to SA (b)(6)(b)(7)(C) this office, on classified media, per his request.

-----//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

18 Jun 10

EXHIBIT

417

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

002179
Approved _____

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

Examination and Contents:

On 24 Jun 10, SA (b)(6)(b)(7)(C), (b)(7)(E) Digital Forensics and Research Branch, Computer Crime Investigative Unit (CCIU), conducted a preliminary examination of Gmail account information (for the account bradley.e.manning@gmail.com) provided by Google and documented on Item 1, Evidence/Property Custody Document (EPCD), Document Number (DN) 089-10.

Findings:

The email files, bradley.e.manning@gmail.com.mbox and bradley.e.manning@gmail.com_preserved.mbox were converted to Internet Message Format (RFC-2822) using Emailchemy Forensic Edition. A review of the resulting message files using EnCase 6.16.2 and Mozilla Thunderbird v3.0.5 revealed 99 emails sent to bradley.e.manning@gmail.com from 23 May 10 through 21 Jun 10.

Examination of the messages from that time period revealed email from Mr. (b)(6)(b)(7)(C) to members of a mailing list named kaba-mas@mit.edu on 12 Jun 10 (excerpt shown below).


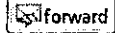
from (b)(6)(b)(7)(C) <unlocked@mit.edu> ☆	 
subject Apache video leaker arrested, WL has US gov't by the balls	6/12/2010 12:26 PM
to (b)(6)(b)(7)(C)@mit.edu ☆	other actions ▸
<p>This is big.</p> <p>The 'people's intelligence service' WikiLeaks just got promoted from 'thorn in the side' to 'major player' status. Notably, they've apparently done so while maintaining a very high degree of internal operational security.</p> <p>The Wikileaks Apache Helicopter leaker was a military intelligence officer (and occasional MIT visitor) named Bradley Manning, who may have leaked 250k internal State Dept cables to the site as well (with lots of nasty things about foreign leaders). Manning was caught when he told his story to (b)(6)(b)(7)(C) (you should know who this is), and (b)(6)(b)(7)(C) decided to turn him in. I'm not even going to try and selectively quote relevant bits, you'll just have to read the links.</p> <p>http://www.guardian.co.uk/media/2010/jun/11/wikileaks-founder-assange-pentagon-manning</p> <p>http://www.wired.com/threatlevel/2010/06/leak/</p> <p>http://www.thedailybeast.com/blogs-and-stories/2010-06-08/state-department-anxious-about-diplomatic-secrets-bradley-manning-allegedly-downloaded/?cid=hp:mainpromot1</p>	

Figure 1 – Excerpt of email message from Mr. (b)(6)(b)(7)(C) to (b)(6)(b)(7)(C)@mit.edu list

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b)(7)(E)	Digital Forensics and Research Branch Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
S (b)(6)(b)(7)(C)	DATE 24 Jun 10
	EXHIBIT 418

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

Further examination of the messages revealed a PGP encrypted email from Mr. (b)(6)(b)(7)(C) to bradley.e.manning@gmail.com on 3 Jun 10 (excerpt shown below).



from: (b)(6)(b)(7)(C) <unlocked@mit.edu> ☆	 
subject: the New Yorker on truth and philosophy	6/3/2010 1:12 AM
to: bradley.e.manning@gmail.com ☆	other actions ▾
<p>-----BEGIN PGP MESSAGE----- Charset: windows-1252 Version: GnuPG v1.4.8 (Darwin) hQEMA6+ie/zKNF87AQgAledQ09a4Q7JxMDj0Q0n9yTx6akY6rj/ZCO0gcHM/47UD o/CLzg23dPFatojFYB4tAuyeI543zNLGvXvdf7D6GnUe2cCvBy7B0Wvzcn23ryqB oiGU/lnLP1CIQm10k9PMq31DJ1srHiHJts1BDFFO/qDfaERmSv6r9rFP1815fdSL qM3Ag550dXNbUQzK5Ss5F816diH1VEq1iPN3WCtwlQ05h5doAWEp8eKEE70RCO/E uPZierc2D3P7EUJa9RtTCpBvhXF2/+Djngd/yzVhGeRajRc2oUKo8jLqtQCD44oP</p>	

Figure 2 – Excerpt of encrypted email from Mr. (b)(6)(b)(7)(C) to bradley.e.manning@gmail.com

No classified information was discovered.

Leads:

1. None.

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

TYPED AGENT'S NAME AND SEQUENCE NUMBER		ORGANIZATION
SA (b)(6)(b)(7)(C), (b)(7)(E)		Digital Forensics and Research Branch Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIC (b)(6)(b)(7)(C)	DATE	EXHIBIT
	24 Jun 10	418

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Approved
002181

Exhibit(s) 419

Page(s) 002182 thru 2182a 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

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Examination and Contents:

On 21 Jul 10, SA (b)(6)(b)(7)(C) Digital Forensics and Research Branch, CCIU, conducted a preliminary examination of the Evidence/Property Custody Document (EPCD), DA Form 4137, Document Number (DN) 101-10, Item 2 (consisting of two CD-RW discs) and Item 4 (consisting of eight DVD-RW discs) and it was determined they were all blank and of no evidentiary value.

Leads:

1. None.

//////////////////////////////////////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

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

DATE
21 Jul 10

EXHIBIT

420

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY

Law Enforcement Sensitive

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

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Imaging:

Between 0900 and 1000, 26 Jul 10, SSA (b)(6)(b)(7)(C) created an EnCase digital forensic image of the IBM ThinkCentre PC, which was recorded on the Department of Army Form 4137, Evidence/Property Custody Document (EPCD), as Document Number (DN) 103-10, item #1.

Computer Make	IBM
Computer Model	ThinkCentre PC
Computer Serial Number	KZK85T
Hard Drive Make	Western Digital
Hard Drive Model	WD1600SB
Hard Drive Serial Number	WCAN7K655403
Image Type	EnCase
Acquisition MD5	88a70abc780e54badce51ebab47ebbbb
Verification MD5	88a70abc780e54badce51ebab47ebbbb
Acquisition SHA1	122880094c37389cd3ca5ed5dd3144ca089c4e24
Verification SHA1	122880094c37389cd3ca5ed5dd3144ca089c4e24

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

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SSA (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

26 Jul 10

EXHIBIT

421

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

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY

Law Enforcement Sensitive

Approved 002184

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 0800, 3 Aug 10, SAC (b)(6)(b)(7)(C) seized as evidence one DVD-R containing the encrypted file "insurance.aes.256" downloaded from the website WikiLeaks.org recorded on the Department of Army Form 4137, Evidence/Property Custody Document (EPCD), as Document Number (DN) 109-10, item #1.//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SSA (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

3 Aug 10

EXHIBIT

422

CID FORM 94
1 FEB 77FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Approved 00

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



DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATIVE UNIT
DIGITAL FORENSICS AND RESEARCH BRANCH
27130 TELEGRAPH ROAD
QUANTICO, VIRGINIA 22134

REPLY TO
ATTENTION OF

CISA-CCI-DF

15 Sep 10

1. **Case Number:** CAF 0028-10-CID361/ROI 028-10-CID221-10117
2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134
3. **Date of Report:** 15 Sep 10
4. **Examiner:** SAC (b)(6)(b)(7)(C)
5. **Summary of Analysis:** Examination of the U.S. Government computer (UNCLASSIFIED) utilized by PFC Bradley MANNING (account name bradley.manning) at Forward Operating Base (FOB) Hammer, Iraq revealed the following:
 - A. Between 7 March and 3 May 10, the user profile bradley.manning searched on the Internet and visited various websites dealing with the term "wget.exe".
 - B. At 19:51:16, 3 May 10, the user profile bradley.manning downloaded wget.exe, which was unauthorized software and was the exact same file identified on the classified U.S. Army computer assigned the Internet Protocol (IP) address 22.225.41.22.
 - C. Between 25 March and 4 May 10, the user profile bradley.manning searched on the Internet and visited various websites dealing with the term "Wikileaks".
 - D. Between 7 and 12 April 10, the user profile bradley.manning searched on the Internet and visited various websites pertaining to Mr. Julian ASACNGE.
 - E. Between 27 March and 4 May 10, the user profile bradley.manning visited the website schwab.com and conducted various brokerage trading.

For Official Use Only
Law Enforcement Sensitive

EXHIBIT 423
002186



Table of Contents

1.	CASE NUMBER:	3
2.	INVESTIGATING OFFICE:	3
3.	DATE OF REPORT:	3
4.	EXAMINER:	3
5.	DEFINITIONS OF TECHNICAL TERMS:	3
5.1	BASE64:	3
5.2	GREP:	3
5.3	HOST NAME:	3
5.4	INDEX.DAT FILE:	3
5.5	INTERNET PROTOCOL (IP) ADDRESS:	4
5.6	MESSAGE DIGEST-5 (MD5):	4
5.7	SECURE HASH ALGORITHM-1 (SHA-1):	4
5.8	SECURITY IDENTIFIER (SID):	4
5.9	UNALLOCATED CLUSTER:	4
5.10	VIRTUAL COMPUTER:	4
5.11	WGET:	5
6.	ANALYSIS:	5
6.1	EXAMINATION OF THE HARD DRIVE, SERIAL NUMBER 5MH0TB78:	5
6.1.1	Imaging Information:	6
6.1.2	Voucher information:	6
6.1.3	Time zone information:	6
6.1.4	A review of the hard drive using Anti-Virus:	6
6.1.5	Event Logs Examination:	6
6.1.6	Unallocated Clusters Examination:	6
6.1.7	Bradley.manning Internet History Examination :	7
6.1.8	Examination of the C:\Documents and Settings\bradley.manning\My Documents\folder:	8
7.	NON-LEAD OBSERVATIONS:	9
8.	SUMMARY OF EXAMINATION:	10
9.	INVESTIGATIVE LEADS:	10
10.	EVIDENCE DISPOSITION:	10
11.	ATTACHMENT:	10



1. Case Number:

CAF 0028-10-CID361/ROI 028-10-CID221-10117

2. Investigating Office:

Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134

3. Date of Report:

15 Sep 10

4. Examiner:

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

5. Definitions of Technical Terms:

5.1 Base64:

Base64 is a method used to encode data to make it faster and easier to transmit. Base64 is most commonly used to encode attachments in email messages.

5.2 GREP:

Global Recursive Expression (GREP) is a program written for several different operating systems that will search a file/folder for a keyword or phrase.

5.3 Host Name:

A host name identifies a workstation or server on a network and (together with a domain name) can be used in place of an IP address. A host name is often used because it is easier to remember than an IP address.

5.4 Index.dat File:

Index.dat files are hidden system files that act as indices for a user's Internet and file activities. The files are used to record websites and local files accessed by a user to help speed up the loading of pages in Microsoft Internet Explorer and Windows Explorer. Each index.dat file contains a *list of locations* for cached files, not the actual cached files themselves. When a user clears Internet activity on a computer system (such as deleting the Temporary Internet Files cache), the associated index.dat file is not deleted. Each user of the computer is assigned a separate folder by the system, which contains user-specific index.dat files.



5.5 Internet Protocol (IP) Address:

An IP address is part of the Transmission Control Protocol/Internet Protocol (TCP/IP). A protocol is the standard language used to communicate over a network. TCP/IP is the most common "language" that computers use to communicate over the Internet. An IP address is the method of identifying a specific computer on a network--only one computer can be assigned a specific IP address at one time. Internet service providers (ISP) typically keep records showing the dates and times when an IP address was used by each customer account.

5.6 Message Digest-5 (MD5):

An MD5 hash value (as used in digital forensics) is a 128-bit (16-byte) number that uniquely describes the contents of a file. It is essentially the "digital fingerprint" of a file or an entire disk. The MD5 hash algorithm was developed by RSA Laboratories and is publicly available. For this reason, the 128-bit MD5 hash is a standard in digital forensics. The algorithm used to generate an MD5 hash is such that the odds of two different files having the same hash value are approximately 1 in 2^{128} .

5.7 Secure Hash Algorithm-1 (SHA-1):

A SHA-1 hash value is a 160-bit number that uniquely describes the contents of a data set. It is essentially a "digital fingerprint" of a file or set of data (e.g., an entire disk). The SHA-1 algorithm was developed by the National Security Agency (NSA), is publicly available, and (like the MD5 algorithm) is commonly used in the forensic community to calculate hash values. The algorithm used to generate a 160-bit SHA-1 hash value is such that the odds of two different files or data sets having the same hash value are approximately 1 in 2^{160} .

5.8 Security Identifier (SID):

The SID is a number most modern Windows operating systems use to identify specific user accounts. Information regarding the associations between a specific user and his assigned SID are found in the SAM registry hive.

5.9 Unallocated Cluster:

Unallocated Clusters represent a data area on a disk that does not currently contain active data. However, remnants of data previously stored in these locations can often still be found in and recovered from Unallocated Clusters, even after the active data has been deleted from the disk. This "left-over" data can be useful in an investigation because it may not be found anywhere else on an examined disk; however, because of the nature of the data in unallocated space, it can be difficult to attribute data ownership or times and dates to the information.

5.10 Virtual Computer:

A Virtual Computer or Virtual Machine (VM) refers to a concept where one computer will run another computer within the memory (RAM) of a host computer. There are several



Forensic Report for U.S. Army Computer, IP 144.107.17.139



different programs which can allow a VM to run, such as VMware or VirtualBox. In a VM the host computer will allocate some physical room on the hard drive and some memory (RAM). The VM will operate separately of the host computer and could be an entirely different Operating System. For example, the host computer could be running Microsoft Windows 7 and the VM would be running Windows XP.

5.11 Wget:

Wget is a freely available network utility used to retrieve files from a Web server using HTTP (Hyper Text Transfer Protocol) and FTP (File Transfer Protocol), two very widely used Internet protocols.

6. Analysis:

About 1100, 11 Jun 10, SAC (b)(6)(b)(7)(C) received a DA Form 2922, Forensic Laboratory Examination Request from SA (b)(6)(b)(7)(C) Central Baghdad CID Office, USF-I, Unit #42232, Camp Liberty, Iraq APO, AE 09342. SA (b)(6)(b)(7)(C) requested this office conduct a forensic examination of the digital media seized as Item 2, Evidence/Property Custody Document (EPCD), Document Number (DN) 0585-10.

EXAMINER'S NOTE: Upon receipt by this office, DN 0585-10 was assigned the local CCIU DN 073-10. These items were collected as evidence pertaining to PFC Bradley E. MANNING in connection with the following offenses:

- UCMJ Article 106a: Espionage.
- 18 USC 793: Gathering, transmitting or losing defense information
- 18 USC 798: Disclosure of Classified Information

6.1 Examination of the Hard Drive, Serial Number 5MH0TB78:

Examination of the Hard Drive revealed it had the Microsoft XP Professional operating system installed at 02:52:35, 17 Dec 08. It was assigned the computer name N2D10MTNBDE7139 and IP 144.107.17.139. The computer was UNCLASSIFIED.

	EnCase file name	2315-27May10
	Operating System Installed	17 Dec 08 02:52:35
	IP address	144.107.17.139
	Operating System	Windows XP (SP3)
	Computer Name	N2D10MTNBDE7139
	Time Zone	(GMT+03:00) Baghdad
	Domain	2BCT10MTN (Primary)
	Date bradley.manning first logged on	18 Feb 10 04:03:30
	Date bradley.manning last logged off	7 May 10 17:00:10



Forensic Report for U.S. Army Computer, IP 144.107.17.139



	Number of times bradley.manning logged on	Unknown	
--	---	---------	--

Figure 1 - System Information

6.1.1 Imaging Information:

Actual Date 30 May 10 22:30:50
 Target Date 30 May 10 22:30:50
 File Path J:\Source\Voucher072_073-10\2315-27May10\2315-27May10.E01
 Case Number 0160-10-CID899-14463
 Evidence Number 2315-27May10
 Examiner Name SA (b)(6)(b)(7)(C)
 Notes This is the HDD serial 5MH0TB78 from the Laptop serial 93H4QD1
 Model Disk
 Drive Type Fixed
 File Integrity Completely Verified, 0 Errors
 Acquisition MD5 ffdcbfc918d5cfc6b3fefaf12953c96f
 Verification MD5 ffdcbfc918d5cfc6b3fefaf12953c96f
 Acquisition SHA1 e2b49bd3ed0e2f5d798ab44febaac3b15d0070be
 Verification SHA1 e2b49bd3ed0e2f5d798ab44febaac3b15d0070be

Figure 2 - Imaging Information

6.1.2 Voucher information:

Item #1, DA Form 4137, Evidence Property Custody Document (EPCD),
Document Number (DN) 073-10.

6.1.3 Time zone information:

All times shown in this preliminary report are in relation to (GMT+03:00 UTC)
unless otherwise noted.

6.1.4 A review of the hard drive using Anti-Virus:

The examined hard disk was scanned using Symantec Endpoint Protection Version 11.0.4000.2295 with Definitions dated August 25, 2010 r40. No malicious files were located.

6.1.5 Event Logs Examination:

Examination of the N2D10MTNBDE7139 computer's event logs failed to identify any pertinent information.

6.1.6 Unallocated Clusters Examination:

Examination of the N2D10MTNBDE7139 Unallocated Clusters for any pertinent information identified sixteen (16) deleted photographic image files which appeared to be of PFC MANNING. See Appendix A for the complete files.



Forensic Report for U.S. Army Computer, IP 144.107.17.139



Figure 3 - Carved_4482_5753069157_5753462110.png

6.1.7 Bradley.manning Internet History Examination :

Examination revealed on 10 Apr 10, there were three (3) Google searches for base64 and Excel and two (2) web pages concerning base64 encoding. See Appendix B for the complete file.

C	D
Date	URL
2010/04/10 10:18:39 (GMT)	Visited: bradley.manning@http://www.google.com/search?hl=en&source=hp&q=base64+excel&aq=0&aql=g10&aql=&aq=8
2010/04/10 10:19:13 (GMT)	Visited: bradley.manning@http://www.google.com/search?hl=en&safe=active&q=base64+excel&start=10&sa=N
2010/04/10 10:20:06 (GMT)	Visited: bradley.manning@http://www.motobit.com/util/base64-decoder-encoder.asp
2010/04/10 10:21:27 (GMT)	Visited: bradley.manning@http://www.thecodecage.com/forumz/excel-vba-programming/168783-convert-image-base64-s
2010/04/10 10:21:44 (GMT)	Visited: bradley.manning@http://www.google.com/search?hl=en&safe=active&q=base64+excel&start=20&sa=N

Figure 4 - Keywords base64 and Excel

Examination of search term "wikileaks" revealed ninety-three (93) Google searches and various web sites concerning Wikileaks and or the released U.S. Army Apache video (Excerpt shown below).

2010/04/07 17:43:07 (GMT)	Visited: bradley.manning@http://www.theatlanticwire.com/opinions/view/opinion/The-Focus-Falls-on-Wikileaks-3130
2010/04/07 17:43:10 (GMT)	Visited: bradley.manning@http://theedge.blogs.nytimes.com/2010/04/06/wikileaks-defends-release-of-video-showing-kil
2010/04/07 17:49:28 (GMT)	Visited: bradley.manning@http://www.geekosystem.com/wikileaks-vldao-jokes
2010/04/07 17:49:50 (GMT)	Visited: bradley.manning@http://news.google.com/news/search?pz=1&cf=all&ned=us&hl=en&q=wikileaks&cf=all&start=1
2010/04/07 17:49:55 (GMT)	Visited: bradley.manning@http://www.theatlantic.com/international/archive/2010/04/two-reader-responses-on-the-wiki
2010/04/07 17:53:57 (GMT)	Visited: bradley.manning@http://www.nationalreview.com/the-feed/3598/wikileaks-defense-everyone-iraq-has-ak-47

Figure 5 - keyword wikileaks

Examination of search term "Assange" revealed four (4) Google news searches and various web sites concerning Mr. Julian ASSANGE.

2010/04/07 18:56:04 (GMT)	:2010040520100412: bradley.manning@http://www.fastcompany.com/1608468/crtb-sheet-julian-assange-of-wikileaks
2010/04/12 13:31:18 (GMT)	Visited: bradley.manning@http://news.google.com/news?pz=1&cf=all&ned=us&hl=en&q=julian+assange&cf=all&output=
2010/04/12 13:35:43 (GMT)	Visited: bradley.manning@http://news.google.com/news/search?aq=f&pz=1&cf=all&ned=us&hl=en&q=julian+assange
2010/04/12 16:31:18 (GMT)	:2010041220100419: bradley.manning@http://news.google.com/news/search?aq=f&pz=1&cf=all&ned=us&hl=en&q=julian+

Figure 6 - Keyword Assange



Forensic Report for U.S. Army Computer, IP 144.107.17.139



Examination of search term "wget" revealed fourteen (14) Google searches and various web sites concerning wget.exe.

2010/05/03 16:50:22 (GMT) Visited: bradley.manning@http://www.google.com/search?hl=en&source=hp&q=wget&aq=f&aql=
2010/05/03 16:51:09 (GMT) Visited: bradley.manning@http://users.ugent.be/~bpuype/wget
2010/05/03 16:51:10 (GMT) Visited: bradley.manning@http://users.ugent.be/~bpuype/cgi-bin/fetch.pl?dl=wget/wget.exe
2010/05/03 16:51:23 (GMT) Visited: bradley.manning@http://users.ugent.be/~bpuype/wget/wget.exe

Figure 7 - Keyword wget

Examination of search term "grep" revealed thirty-six (36) Google searches and various web sites concerning grep. NOTE: PFC MANNING owned a Macintosh computer and the user account bradley.manning viewed websites pertaining to Windows computers and grep. Further, grep is built into the Macintosh operating system while it is not built into the Windows operating system.

2010/05/03 18:53:24 (GMT) Visited: bradley.manning@http://www.google.com/search?hl=en&source=hp&q=grep+exe&aq=f&aql=&aql=&cc=&g
2010/05/03 18:53:46 (GMT) Visited: bradley.manning@http://www.wingrep.com/favicon.ico
2010/05/03 18:53:46 (GMT) Visited: bradley.manning@http://www.wingrep.com/resources/binaries/resources/binaries/WindowsGrep23.exe
2010/05/03 18:54:12 (GMT) Visited: bradley.manning@http://www.wingrep.com

Figure 8 - Keyword grep

Examination of search term "schwab" revealed ninety-nine (99) hits on schwab.com website. NOTE: The specific account information was identified, but will not be provided within this report.

C	D
Date	URL
2010/05/04 17:39:15 (GMT)	Visited: bradley.manning@https://client.schwab.com/Accounts/Brokers
2010/05/04 20:39:15 (GMT)	2010050420100505: bradley.manning@https://client.schwab.com/Account

Figure 9 - keyword brokerage

6.1.8 Examination of the C:\Documents and Settings\bradley.manning\My Documents\ folder:

Examination revealed the file wget.exe was created at 19:51:16, 3 May 10. See Appendix C for the complete file.

Name	File Created	Hash Value
wget.exe	03 May 10 19:51:16	bd126a7b59d5d1f97ba89a3e71425731

Figure 10 - wget.exe file properties

The wget.exe had the same hash value as the wget.exe located on PFC MANNING's primary SIRPNET computer between March and May 2010.



Forensic Report for U.S. Army Computer, IP 144.107.17.139



Evidence File	Name	File Created	Hash Value
2315-27May10	wget.exe	03 May 10 19:51:16	bd126a7b59d5d1f97ba89a3e71425731
2251-27May10	wget.exe	04 May 10 00:11:18	bd126a7b59d5d1f97ba89a3e71425731

Figure 11 - comparison between the two wget.exe files

Examination of the above (Figure 14) wget.exe file to determine where it was downloaded from disclosed the identified website
 "http://users.ugent.be/~bpuype/wget/wget.exe" as being the source.

C	D
Date	URL
2010/05/03 19:51:23 (GMT)	:2010050320100504: bradley.manning@http://users.ugent.be/~bpuype/wget/wget.exe

Figure 12 - location where wget.exe was downloaded

Examination of the file C:\Documents and Settings\bradley.manning\Local Settings\Temporary Internet Files\Content.IE5\WCZFP3HB\wget[1].htm revealed it was the source of the wget.exe which was located on this computer. NOTE: The web site has the same hash value listed as the one for the wget.exe located on this computer.

WGET for Windows (win32) - current version: 1.11.4

updated February 18 2010

Read below to download and for some [help with wget](#).

[license information and compiler details](#)

Downloads!

Latest version is 1.11.4, compiled with MS Visual C++ and linked with OpenSSL 0.9.8k. Page will be updated with new releases of wget. Wget tends to see a couple of incremental bugfix releases (i.e. 1.11.x). I am currently using wget 1.11.x on a daily basis.

>>

wget.exe (401408 bytes) << : win32 binary with OpenSSL support.

 MD5: b411da7b59d5d1f97ba89a3e71425731
 SHA1: 437b1cd905e407baef640c65e240e7c1b5da92759

- [license](#)
- [GNU wget](#)
- [OpenSSL](#)
- [downloads](#)
- [where is 1.12?](#)
- [previous versions](#)
- [usage](#)
- [basic options](#)
- [FTP](#)
- [proxy](#)
- [passwords](#)
- [SSL certificates](#)
- [wget in file](#)

Figure 13 - Website for wget.exe

7. Non-Lead Observations:

None.



Forensic Report for U.S. Army Computer, IP 144.107.17.139



8. Summary of Examination:

Examination of the N2D10MTNBDE7139 U.S. Government computer (UNCLASSIFIED) utilized by PFC Bradley MANNING (account name bradley.manning) at Forward Operating Base (FOB) Hammer, Iraq revealed the following:

- A. Between 7 March and 3 May 10, the user profile bradley.manning searched on the Internet and visited various websites dealing with the term "wget.exe".
- B. At 19:51:16, 3 May 10, the user profile bradley.manning downloaded wget.exe, which was unauthorized software and was the exact same file identified on the classified U.S. Army computer assigned the IP 22.225.41.22.
- C. Between 25 March and 4 May 10, the user profile bradley.manning searched on the Internet and visited various websites dealing with the term "Wikileaks".
- D. Between 7 and 12 April 10, the user profile bradley.manning searched on the Internet and visited various websites pertaining to Mr. Julian ASSANGE.
- E. Between 27 March and 4 May 10, the user profile bradley.manning visited the website schwab.com and conducted various brokerage trading.

9. Investigative Leads:

- A) None.

10. Evidence Disposition:

All evidence was placed into the evidence room of this office.

REPORT PREPARED \ APPROVED BY:

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

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

SPECIAL AGENT IN CHARGE

11. Attachment:

- Attachment A, Enclosure 1 (recovered photos from unallocated clusters)
 Attachment B, Enclosure 1 (internet history of the user profile bradley.manning)
 Attachment C, Enclosure 1 (wget.exe and the website it was downloaded from)

Exhibit(s) 424

Page(s) 002196 thru 002485 withheld.

5 U.S.C. § 552(b)(6), (b)(7)(C)
Third Party Information
Not Reasonably Segregable

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Imaging:

Between 1000 and 1100, 16 Sep 10, SSA (b)(6)(b)(7)(C) created an EnCase digital forensic image of the US Army computer assigned the Internet Protocol (IP) address of 147.198.178.143 and computer name DRUMNB22IB50014, recorded on the Department of Army Form 4137, Evidence/Property Custody Document (EPCD), as Document Number (DN) 132-10, item #1.

Hard Drive Make	Samsung
Hard Drive Model	HM121HJ
Hard Drive Serial Number	S1NSJD0Q800999
Image Type	EnCase
Acquisition MD5	26dd11e2758dc187a3fe9efbe3a47795
Verification MD5	26dd11e2758dc187a3fe9efbe3a47795
Acquisition SHA1	f59cbee2417e4d811939ba18587e7d7b16c80be6
Verification SHA1	f59cbee2417e4d811939ba18587e7d7b16c80be6

Examination Date and Contents:

Between 16 and 17 Sep 10, SSA (b)(6)(b)(7)(C) conducted a preliminary investigation of the computer assigned the IP 147.198.178.143, belonging to U.S. Army, Fort Drum Department Of Information Management (DOIM). All times shown in this preliminary report are in relation to Eastern Daylight Time (EDT -500 UTC) unless otherwise noted.

A review of the Hard Drive using Anti-Virus:

The examined hard disk was scanned using Symantec Endpoint Protection, Version 11.0.4000.2295, Definitions 25 Aug 10, r40. No malicious files were identified.

Pertinent Information:

Examination of the computer assigned the IP 147.198.178.143 disclosed it was an UNCLASSIFIED U.S. Army computer utilized by the assigned user bradley.manning between 08:47:15, 04 Jun 09 and 14:20:00, 24 Sep 09. An exhaustive search failed to identify any pertinent information to this investigation.

Leads/ Non-Lead Observations:

None

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

TYPED AGENT'S NAME AND SEQUENCE NUMBER

SSA (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

17 September 2010

EXHIBIT

425

CID FORM 94
1 FEB 77FOR OFFICIAL USE ONLY
Law Enforcement SensitiveApproved (b)(6)(b)(7)(C)
002486



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATIVE UNIT
DIGITAL FORENSICS AND RESEARCH BRANCH
27130 TELEGRAPH ROAD
QUANTICO, VIRGINIA 22134

CISA-CCI-DF

20 Sep 10

1. **Case Number:** CAF# 0028-10-CID361 / ROI# 0028-10-CID221-10117
2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134
3. **Date of Report:** 20 Sep 10
4. **Examiner:** SAC (b)(6)(b)(7)(C), (b)(7)(E)
5. **Summary of Analysis:** Examination of the DRUMNB22IB50014 U.S. Army computer assigned the IP Address 147.198.178.143 disclosed it was an unclassified computer utilized by the bradley.manning profile between 08:47:15, 4 Jun 09 and about 14:20:00, 24 Sep 09.

For Official Use Only
Law Enforcement Sensitive

EXHIBIT 426
002487



Table of Contents

TABLE OF CONTENTS	2
1. CASE NUMBER:.....	3
2. INVESTIGATING OFFICE:	3
3. DATE OF REPORT:	3
4. EXAMINER:.....	3
5. DEFINITIONS OF TECHNICAL TERMS:	3
5.1 HOST NAME:	3
5.2 INDEX.DAT FILE:	3
5.3 INTERNET PROTOCOL (IP) ADDRESS:	3
5.4 MESSAGE DIGEST-5 (MD5):	4
5.5 SECURE HASH ALGORITHM-A (SHA-1):.....	4
6. ANALYSIS:	4
6.1 EXAMINATION OF THE U.S. ARMY COMPUTER, ASSIGNED THE IP 147.198.178.143:	4
6.1.1 Voucher information:	5
6.1.2 Verification of imaging:.....	5
6.1.3 Time zone information:.....	5
6.1.4 Anti-Virus Scan Examination:.....	5
6.1.5 Event Log Examination:	5
6.1.6 Bradley.manning profile Examination:	5
6.1.7 Bradley.manning Internet History Examination:.....	6
7. NON-LEAD OBSERVATIONS:	6
8. SUMMARY OF EXAMINATION:	6
9. INVESTIGATIVE LEADS:	6
10. EVIDENCE DISPOSITION:	6
11. ATTACHMENT:	6

**1. Case Number:**

CAF# 0028-10-CID361 / ROI# 0028-10-CID221-10117

2. Investigating Office:

Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134

3. Date of Report:

20 Sep 10

4. Examiner:

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

5. Definitions of Technical Terms:**5.1 Host Name:**

A host name identifies a workstation or server on a network and (together with a domain name) can be used in place of an IP address. A host name is often used because it is easier to remember than an IP address.

5.2 Index.dat File:

Index.dat files are hidden system files that act as indices for a user's Internet and file activities. The files are used to record websites and local files accessed by a user to help speed up the loading of pages in Microsoft Internet Explorer and Windows Explorer. Each index.dat file contains a *list of locations* for cached files, not the actual cached files themselves. When a user clears Internet activity on a computer system (such as deleting the Temporary Internet Files cache), the associated index.dat file is not deleted. Each user of the computer is assigned a separate folder by the system, which contains user-specific index.dat files.

5.3 Internet Protocol (IP) Address:

An IP address is part of the Transmission Control Protocol/Internet Protocol (TCP/IP). A protocol is the standard language used to communicate over a network. TCP/IP is the most common "language" that computers use to communicate over the Internet. An IP address is the method of identifying a specific computer on a network--only one computer can be assigned a specific IP address at one time. Internet service providers (ISP) typically keep records showing the dates and times when an IP address was used by each customer account.



Forensic Report for the U.S. Army Computer, IP 147.198.178.143



5.4

Message Digest-5 (MD5):

An MD5 hash value (as used in digital forensics) is a 128-bit (16-byte) number that uniquely describes the contents of a file. It is essentially the "digital fingerprint" of a file or an entire disk. The MD5 hash algorithm was developed by RSA Laboratories and is publicly available. For this reason, the 128-bit MD5 hash is a standard in digital forensics. The algorithm used to generate an MD5 hash is such that the odds of two different files having the same hash value are approximately 1 in 2^{128} .

5.5 Secure Hash Algorithm-a (SHA-1):

A SHA-1 hash value is a 160-bit number that uniquely describes the contents of a data set. It is essentially a "digital fingerprint" of a file or set of data (e.g., an entire disk). The SHA-1 algorithm was developed by the National Security Agency (NSA), is publicly available, and (like the MD5 algorithm) is commonly used in the forensic community to calculate hash values. The algorithm used to generate a 160-bit SHA-1 hash value is such that the odds of two different files or data sets having the same hash value are approximately 1 in 2^{160} .

6. Analysis:

(U) About 0900, 16 Sep 10, SAC (b)(6)(b)(7)(C) received a verbal request from SA (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Washington Metro Resident Agency, Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, to search the digital media seized Item 1, Evidence/Property Custody Document (EPCD), Document Number (DN) 132-10.

SA (b)(6)(b)(7)(C) requested this office conduct a forensic examination of items collected as evidence pertaining to PFC Bradley E. MANNING in connection with the following offenses:

- UCMJ Article 106a: Espionage.
- 18 USC 793: Gathering, transmitting or losing defense information
- 18 USC 798: Disclosure of Classified Information

6.1 Examination of the U.S. Army computer, assigned the IP 147.198.178.143:

Examination disclosed it was UNCLASSIFIED, part of the North American East (NAE) domain and utilized the Windows Vista Operating System.

	EnCase file name	147.198.178.143
	Operating System Installed	25 Nov 08 22:58:52
	IP address	147.198.178.143
	Operating System	Windows Vista
	Computer Name	DRUMNB22IB50014
	Time Zone	(GMT -05:00) Eastern Time
	Domain	NAE
	Date bradley.manning first logged on	08:47:15, 4 Jun 09



Forensic Report for the U.S. Army Computer, IP 147.198.178.143



	Date bradley.manning last logged off	14:20:00, 24 Sep 09	
	Number of times bradley.manning logged on	Unknown	

Figure 1 - System Information

6.1.1 Voucher information:

Item 1, EPCD, DN 132-10.

6.1.2 Verification of imaging:

Evidence Number	147.198.178.143
Examiner Name	SA (b)(6)(b)(7)(C) 5437, CCIU
Notes	Samsung HDD, MD: HM121HJ, SN: S1NSJD0Q800999
Label	eSATA-2
Model	eSATA-2 HM121HJ
Serial Number	S1NSJD0Q800999
Drive Type	Fixed
File Integrity	Completely Verified, 0 Errors
Acquisition MD5	26dd11e2758dc187a3fe9efbe3a47795
Verification MD5	26dd11e2758dc187a3fe9efbe3a47795
Acquisition SHA1	f59cbee2417e4d811939ba18587e7d7b16c80be6
Verification SHA1	f59cbee2417e4d811939ba18587e7d7b16c80be6

Figure 2 - Image verification

6.1.3 Time zone information:

All times shown in this report are in relation to Eastern Daylight Time (EDT -4:00 UTC) unless otherwise noted.

6.1.4 Anti-Virus Scan Examination:

The DRUMNB22IB50014 hard disk was scanned using Symantec Endpoint Protection Version 11.0.4000.2295 with Definitions dated 25 Aug 10, r40. No malicious files were located.

6.1.5 Event Log Examination:

Examination of computer DRUMNB22IB50014's event log files did not identify any pertinent information.

6.1.6 Bradley.manning profile Examination:

Examination revealed it was created at 08:47:15, 4 Jun 09 and the last activity was on or about 14:20:00, 24 Sep 09.

	Name	File Created
	bradley.manning	04 Jun 09 08:47:15

Figure 3 - creation date for the bradley.manning profile



Forensic Report for the U.S. Army Computer, IP 147.198.178.143



6.1.7 Bradley.manning Internet History Examination:

Examination disclosed the Internet history of the bradley.manning user account from 4 Jun 09 to 24 Sep 09 time frame revealed the numerous websites which were visited by this account (excerpt shown below in Figure 4). See Appendix A, Enclosure 1 for the complete file.

C	D
Date	URL
2009/06/11 20:26:13 (GMT)	Cookie:bradley.manning@earthlink.net/
2009/06/11 20:26:14 (GMT)	Cookie:bradley.manning@webmail.earthlink.net/wam/
2009/09/11 15:06:34 (GMT)	http://www.wmdtrainingaids.com/images/claymore_ied.jpg
2009/09/14 09:20:25 (GMT)	:2009091420090921: bradley.manning@http://www.facebook.com
2009/09/14 09:20:25 (GMT)	:2009091420090921: bradley.manning@:Host: www.facebook.com
2009/09/14 09:20:38 (GMT)	:2009091420090921: bradley.manning@http://www.facebook.com/home.php?

Figure 4 - file and internet history

7. Non-Lead Observations:

None.

8. Summary of Examination:

Examination of the DRUMNB22IB50014 U.S. Army computer assigned the IP Address 147.198.178.143 disclosed it was an unclassified computer utilized by the bradley.manning profile between 08:47:15, 4 Jun 09 and about 14:20:00, 24 Sep 09.

9. Investigative Leads:

None.

10. Evidence Disposition:

All evidence was placed into the evidence room of this office.

REPORT PREPARED \ APPROVED BY:

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

SPECIAL AGENT IN CHARGE



Forensic Report for the U.S. Army Computer, IP 147.198.178.143

**11. Attachment:**

Attachment A, Enclosure 1 (File and Internet History for the bradley.manning profile from the U.S. Army computer assigned the IP 147.198.178.143)

Exhibit(s) 427

Page(s) 002494 thru 002715 withheld.

5 U.S.C. § 552(b)(6), (b)(7)(C)
Third Party Information
Not Reasonably Segregable



DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATION UNIT
DIGITAL FORENSICS AND RESEARCH BRANCH
27130 TELEGRAPH ROAD
QUANTICO, VIRGINIA 22134

REPLY TO
ATTENTION OF

CISA-CCI-DF

28 Sep 10

1. **Case Number:** CAF 0028-10-CID361/ROI 0028-10-CID221-10117
2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134
3. **Date of Report:** 28 Sep 10
4. **Examiner:** SA (b)(6)(b)(7)(C), (b)(7)(E)
5. **Summary of Analysis:** Examination of the U.S. Government Supply Annex NIPRNET Computer (UNCLASSIFIED), utilized by PFC Bradley MANNING revealed the following:
 - A. PFC MANNING communicated with Mr. (b)(6)(b)(7)(C) via a PGP-encrypted email.
 - B. A scanned .PDF file pertaining to the Article 15 of PFC MANNING was located within the Recycler folder of the (b)(6)(b)(7)(C) user account (primarily used by SSG (b)(6)(b)(7)(C)).
 - C. A user of the user account bradley.manning searched for the keyword "wikileaks".
 - D. A user of the user account (b)(6)(b)(7)(C) searched for the keywords "wikileaks" and "Julian Assange".
 - E. A user of the user account (b)(6)(b)(7)(C) logged into PFC MANNING's AKO account, Gmail email account and Amazon account.
 - F. There were text files containing extracts from a Defense Global Address List in the Recycler folder and the My Documents folder of the user account (b)(6)(b)(7)(C).



Table of Contents

1.	CASE NUMBER:.....	4
2.	INVESTIGATING OFFICE:	4
3.	DATE OF REPORT:.....	4
4.	EXAMINER:	4
5.	DEFINITIONS OF TECHNICAL TERMS:.....	4
5.1	COOKIE:.....	4
5.2	HOST NAME:.....	4
5.3	INDEX.DAT FILE:.....	4
5.4	INTERNET PROTOCOL (IP) ADDRESS:.....	4
5.5	MESSAGE DIGEST-5 (MD5):.....	5
5.6	NON-CLASSIFIED INTERNET PROTOCOL ROUTING NETWORK (NIPRNET):	5
5.7	SECURE HASH ALGORITHM-1 (SHA-1):	5
5.8	SECURITY IDENTIFIER (SID):	5
5.9	UNALLOCATED CLUSTERS (UC):	5
5.10	WINDOWS REGISTRY:	5
6.	ANALYSIS:	6
6.1	EXAMINATION OF THE HARD DISK DRIVE (HDD), SERIAL NUMBER 070817DP0C10DSG2J1DP:	6
6.1.1	<i>Voucher information:</i>	6
6.1.2	<i>Verification of imaging:</i>	6
6.1.3	<i>Time zone information:</i>	7
6.1.4	<i>A Review of the HDD using Anti-Virus:</i>	7
6.1.5	<i>Examination of the bradley.manning user account:</i>	7
6.1.6	<i>Examination of the Supply Annex NIPRNET computer's logon policies:</i>	8
6.1.7	<i>Examination of the Supply Annex NIPRNET computer's policies for removable media:</i> 9	
6.1.8	<i>Examination of the Microsoft Outlook Nickname file:</i>	10
6.1.9	<i>Examination of the folder C:\Documents and Settings: \bradley.manning\Recent..</i> 10	
6.1.10	<i>Examination of the bradley.manning Recycle Bin:</i>	10
6.1.11	<i>Examination of files containing Global Address List (GAL) information:</i>	11
6.1.12	<i>Examination of the file C:\RECYCLER\S-1-5-21-2175376772-4088186718- 847205759-4624\tmp.pdf:</i>	17
6.1.13	<i>Examination of the Internet History files for the user account bradley.manning:</i>	19
6.1.14	<i>Examination of the Internet History files for the user account (b)(6)(b)(7)(C)</i>	20
7.	SUMMARY OF EXAMINATION:.....	33



Forensic Report for Supply Annex NIPRNET computer



8.	INVESTIGATIVE LEADS:.....	34
9.	EVIDENCE DISPOSITION:.....	34
10.	ATTACHMENTS:.....	35



1. Case Number:

CAF 0028-10-CID361/ROI 0028-10-CID221-10117

2. Investigating Office:

Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134

3. Date of Report:

28 Sep 10

4. Examiner:

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

5. Definitions of Technical Terms:

5.1 Cookie:

A cookie is a small text file placed on a user's hard drive by a Web server, commonly used to record site preferences and usage. A cookie can include usernames, session id, user preferences and previously viewed web pages.

5.2 Host Name:

A host name identifies a workstation or server on a network and (together with a domain name) can be used in place of an IP address. A host name is often used because it is easier to remember than an IP address.

5.3 Index.dat File:

Index.dat files are hidden system files that act as indices for a user's Internet and file activities. The files are used to record websites and local files accessed by a user to help speed up the loading of pages in Microsoft Internet Explorer and Windows Explorer. Each index.dat file contains a *list of locations* for cached files, not the actual cached files themselves. When a user clears Internet activity on a computer system (such as deleting the Temporary Internet Files cache), the associated index.dat file is not deleted. Each user of the computer is assigned a separate folder by the system, which contains user-specific index.dat files.

5.4 Internet Protocol (IP) Address:

An IP address is part of the Transmission Control Protocol/Internet Protocol (TCP/IP). A protocol is the standard language used to communicate over a network. TCP/IP is the most common "language" that computers use to communicate over the Internet. An IP address is the method of identifying a specific computer on a network--only one computer can be assigned a



Forensic Report for Supply Annex NIPRNET computer



specific IP address at one time. Internet service providers (ISP) typically keep records showing the dates and times when an IP address was used by each customer account.

5.5 Message Digest-5 (MD5):

An MD5 hash value (as used in digital forensics) is a 128-bit (16-byte) number that uniquely describes the contents of a file. It is essentially the "digital fingerprint" of a file or an entire disk. The MD5 hash algorithm was developed by RSA Laboratories and is publicly available. For this reason, the 128-bit MD5 hash is a standard in digital forensics. The algorithm used to generate an MD5 hash is such that the odds of two different files having the same hash value are approximately 1 in 2^{128} .

5.6 Non-Classified Internet Protocol Routing Network (NIPRNET):

Information network operated by the U.S. Department of Defense based on the use of IP addresses for non-classified communications.

5.7 Secure Hash Algorithm-1 (SHA-1):

A SHA-1 hash value is a 160-bit number that uniquely describes the contents of a data set. It is essentially a "digital fingerprint" of a file or set of data (e.g., an entire disk). The SHA-1 algorithm was developed by the National Security Agency (NSA), is publicly available, and (like the MD5 algorithm) is commonly used in the forensic community to calculate hash values. The algorithm used to generate a 160-bit SHA-1 hash value is such that the odds of two different files or data sets having the same hash value are approximately 1 in 2^{160} .

5.8 Security Identifier (SID):

The SID is a number most modern Windows operating systems use to identify specific user accounts. Information regarding the associations between a specific user and his assigned SID are found in the SAM registry hive.

5.9 Unallocated Clusters (UC):

Unallocated Clusters represent a data area on a disk that does not currently contain active data. However, remnants of data previously stored in these locations can often still be found in and recovered from Unallocated Clusters, even after the active data has been deleted from the disk. This "left-over" data can be useful in an investigation because it may not be found anywhere else on an examined disk; however, because of the nature of the data in unallocated space, it can be difficult to attribute data ownership or times and dates to the information.

5.10 Windows Registry:

The Windows Registry contains data and setting/configuration information used by a Windows operating system (OS) to operate the computer, interact with users, and provide a cohesive computing environment. Information contained in the Registry can include user information, program data, OS installation data, and passwords. The Windows Registry is subdivided into smaller parts called keys (e.g., HKEY_LOCAL_MACHINE, or HKLM) and



Forensic Report for Supply Annex NIPRNET computer



subkeys (e.g., HKLM\SYSTEM\CurrentControlSet\Control\usbstor). By following the paths of these keys and subkeys, users (and investigators) can find specific data stored within the registry.

6. Analysis:

About 1100, 11 Jun 10, SA (b)(6)(b)(7)(C) received a DA Form 2922, Forensic Laboratory Examination Request from SA (b)(6)(b)(7)(C) Central Baghdad CID Office, USF-I, Unit #42232, Camp Liberty, Iraq APO, AE 09342. SA (b)(6)(b)(7)(C) requested this office conduct a forensic examination of the digital media seized as Item 2, Evidence/Property Custody Document (EPCD), Document Number (DN) 0585-10.

EXAMINER'S NOTE: Upon receipt by this office, DN 0585-10 was assigned the local CCIU DN 073-10. These items were collected as evidence pertaining to PFC Bradley E. MANNING in connection with the following offenses:

- UCMJ Article 106a: Espionage.
- 18 USC 793: Gathering, transmitting or losing defense information
- 18 USC 798: Disclosure of Classified Information

6.1 Examination of the hard disk drive (HDD), Serial Number 070817DP0C10DSG2J1DP:

Examination of the HDD revealed it contained the Windows XP operating system. The HDD was identified on EPCD DN 073-10 as obtained from the U.S. Government computer (Supply Annex NIPRNET; Computer Name N2D10MTNBDE7019; UNCLASSIFIED), assigned Internet Protocol (IP) Address 144.107.17.19, property of the Headquarters & Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division (10th Mtn Div).

6.1.1 Voucher information:

Item 1, EPCD DN 073-10

6.1.2 Verification of imaging:

Name	1140-28May10-Item2
Actual Date	05/31/10 02:52:04PM
Target Date	05/31/10 02:52:04PM
File Path	C:\Users\Administrator\Desktop\068-10\1140-28May10-Item2.E01
Case Number	0160-10-CID899-14463
Evidence Number	1140-28May10-Item2
Examiner Name	SA (b)(6)(b)(7)(C)
Notes	This is the HDD serial 070817DP0C10DSG2J1DP
Model	Disk
Drive Type	Fixed



Forensic Report for Supply Annex NIPRNET computer



File Integrity Completely Verified, 0 Errors
 Acquisition MD5 b0b530ea63552253e0dc814db4b618f2
 Verification MD5 b0b530ea63552253e0dc814db4b618f2
 Acquisition SHA1 309df99f068fba2e81aae03d1a93d471cde90bf0
 Verification SHA1 309df99f068fba2e81aae03d1a93d471cde90bf0
 GUID f5b7f4cb2a3bef408d08ed84e5f4cd23
 EnCase Version 6.14
 System Version Windows Vista
 Is Physical •
 Raid Stripe Size 0
 Error Granularity 64
 Process ID 0
 Index File C:\Program Files\EnCase6.16.2\Index\1140-28May10-Item2-f5b7f4cb2a3bef408d08ed84e5f4cd23.Index
 Read Errors 0
 Missing Sectors 0
 CRC Errors 0
 Compression None
 Total Size 120,034,123,776 Bytes (111.8GB)
 Total Sectors 234,441,648
 Disk Signature 1DFB1DFB
 Partitions Valid

Partitions

Name	Id	Type	Start Sector	Total Sectors	Size
	07	NTFS	0	234,436,545	111.8GB

Figure 1 – Imaging and verification report for the HDD extracted from the Supply Annex NIPRNET computer

6.1.3 Time zone information:

All times shown in this preliminary report are in relation to Baghdad Time (+3:00 UTC) unless otherwise noted.

EXAMINER'S NOTE: The time format used for figures/graphic depictions is MM/DD/YY.

6.1.4 A Review of the HDD using Anti-Virus:

The examined HDD was scanned using Symantec Endpoint Protection Version 11.0.5002.333 with Definitions dated September 19, 2010 r3. No malicious files were located.

6.1.5 Examination of the bradley.manning user account:

Examination of the bradley.manning user account revealed it was assigned the SID S-1-5-21-2175376772-4088186718-847205759-4641. The user account was created on the computer on 21 May 10 and last accessed on 28 May 10.



Forensic Report for Supply Annex NIPRNET computer



User name: bradley.manning
 Full Name:
 Type of User: Domain User
 Account Description:
 Primary Group Number: 0
 Security Identifier: S-1-5-21-2175376772-4088186718-847205759-4641
 Logon Script:
 Profile Path: %SystemDrive%\Documents and Settings\bradley.manning
 Last Logon:
 Last Password Change:
 Last Incorrect Password Logon:

Figure 2 - The SID of the user account bradley.manning

EnCase Law Enforcement				
File Edit View Tools Help				
New Open Save Print Add Device Search Refresh				
Cases Keywords X Table Report Gallery Timeline Disk Code				
<div> <div>Home Entries Bookmarks</div> <div>Search Hits Records Devices</div> <div>Secure Storage Keywords</div> <div>Home File Extents Permissions</div> <div>References Hash Properties</div> <div> <div>\$Extend</div> <div>ddffd95a880daa66a7b786c4</div> <div>dell</div> <div>Documents and Settings</div> <div>3BDES6ADMIN</div> <div>4-10bct_belodask</div> </div> </div>				
	Name	File Created	Last Written	Last Accessed
10	admin.sharp	01/01/09 11:56:50AM	08/11/09 05:02:10PM	05/27/10 01:21:32AM
11	Administrator	03/22/08 07:16:27PM	03/22/08 07:23:28PM	05/27/10 11:58:34PM
12	ADMIN~1~POW	01/11/10 12:13:37PM	01/11/10 12:13:37PM	05/24/10 09:16:15PM
13	(b)(6)(b)(7)(C)	04/21/09 10:56:06AM	04/21/09 10:56:10AM	05/27/10 01:21:35AM
14	All Users	01/30/08 02:52:27AM	05/27/10 11:13:44PM	05/27/10 11:13:44PM
15	(b)(6)(b)(7)(C)	01/18/09 03:34:21PM	01/31/09 11:51:34AM	05/27/10 01:21:36AM
16		01/30/08 10:58:16AM	01/30/08 10:58:20AM	05/27/10 01:21:39AM
17		12/11/09 02:47:37PM	12/11/09 02:47:39PM	05/27/10 11:58:34PM
18	bradley.manning	05/21/10 12:28:45PM	05/21/10 12:28:49PM	05/28/10 12:00:00AM
19	(b)(6)(b)(7)(C)	11/26/09 11:12:44AM	11/26/09 11:12:47AM	05/27/10 11:58:34PM

Figure 3 - Creation and access dates for bradley.manning account

6.1.6 Examination of the Supply Annex NIPRNET computer's logon policies:

Examination of the Supply Annex NIPRNET computer's logon policies determined the policy was not configured for Common Access Card (CAC) login, as the scforceoption value was not present. The HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ policies\system subkey was set to display a Department of Defense (DoD) warning banner and DoD legal notice upon login.



Forensic Report for Supply Annex NIPRNET computer

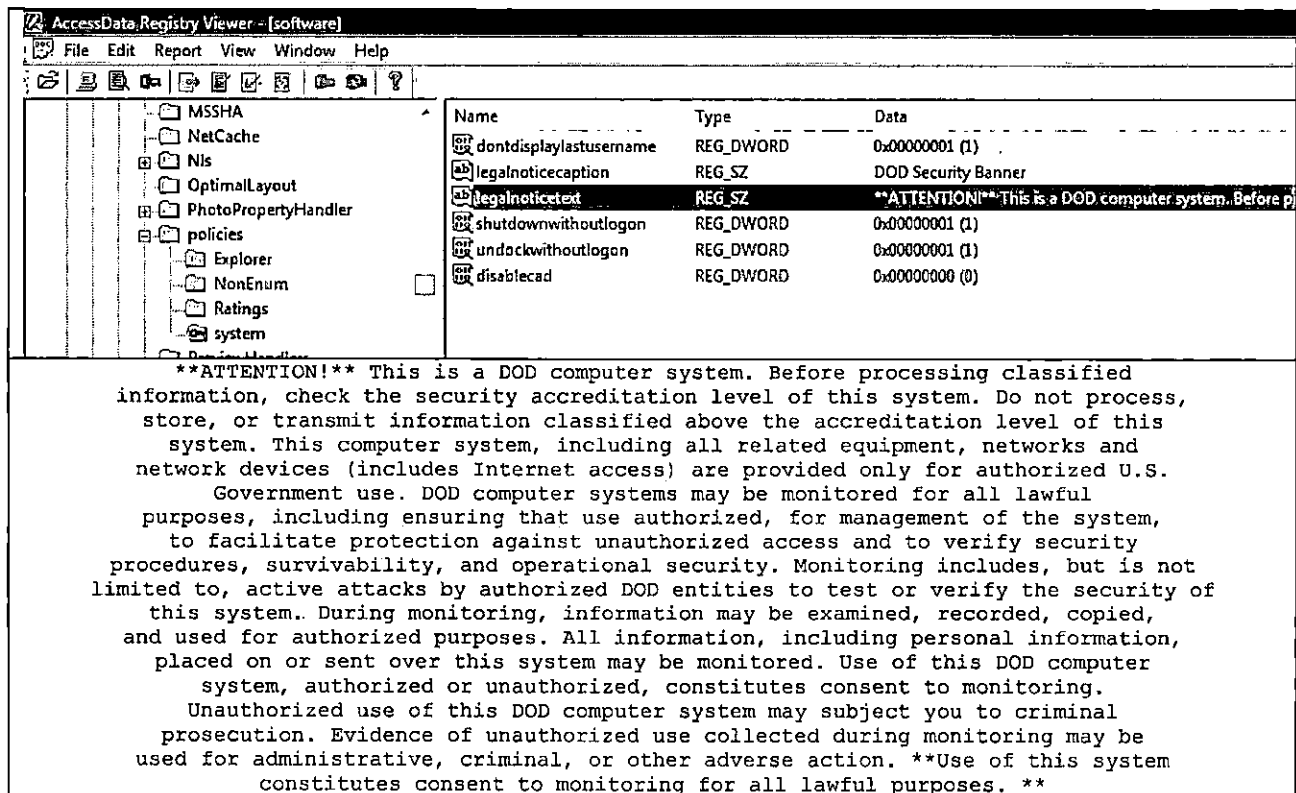


Figure 4 - Logon policy in the Software registry hive and DoD warning banner

6.1.7 Examination of the Supply Annex NIPRNET computer's policies for removable media:

Examination of the Supply Annex NIPRNET computer's policies for removable media determined the policy was set to disallow the use of USB external media. The HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR\Start subkey was set to prohibit the installation of USB drives on the system.

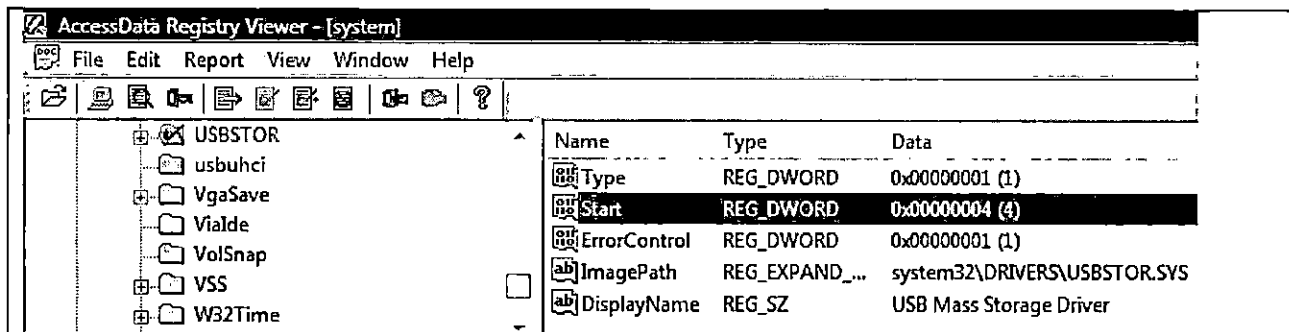


Figure 5 - Registry key preventing USB device access



6.1.8 Examination of the Microsoft Outlook Nickname file:

Examination of the file C:\Documents and Settings

\bradley.manning\Application Data\Microsoft\Outlook\Outlook.NK2 revealed two email addresses (b)(6)(b)(7)(C), both associated with Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)

EXAMINER'S NOTE: Microsoft Outlook maintains a nickname list that is used by both the automatic name checking and automatic completion features. The nickname list (.NK2 file) is automatically generated when a user sends email with Outlook.

(b)(6)(b)(7)(C) net SMTP (b)(6)(b)(7)(C) net
(b)(6)(b)(7)(C) SMTP (b)(6)(b)(7)(C) org

Figure 6 - Saved email addresses in the Outlook Nickname file

6.1.9 Examination of the folder C:\Documents and Settings:

\bradley.manning\Recent

The file C:\Documents and Settings\bradley.manning\Recent\Second Attempt.lnk was created on the computer at 12:45:24, 21 May 10. This file was a link to the file C:\Documents and Settings\bradley.manning\My Documents\Second Attempt.txt (detailed in paragraph 6.1.10 below).

Name	File Created	Symbolic Link
Desktop.ini	05/21/10 12:29:02PM	
Second Attempt.lnk	05/21/10 12:45:24PM	C:\Documents and Settings\bradley.manning\My Documents\Second Attempt.txt

Figure 7 - File attributes of Second Attempt.lnk

6.1.10 Examination of the bradley.manning Recycle Bin:

Examination of the folder C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4641 revealed the text file C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4641\Second Attempt.txt. The text file held the contents of a PGP-encrypted email communication from PFC MANNING to Mr.

(b)(6)(b)(7)(C) See Attachment A on Enclosure 1 to this report for the complete file.



Forensic Report for Supply Annex NIPRNET computer



Name		File Created	File Deleted
<input type="checkbox"/> 1	INFO2	05/21/10 07:15:02PM	
<input type="checkbox"/> 2	Second Attempt.txt	05/21/10 12:45:21PM	05/21/10 07:15:03PM
<input type="checkbox"/> 3	desktop.ini	05/21/10 07:15:02PM	

Figure 8 - File attributes for the deleted file Second Attempt.txt

From: Manning, Bradley SPC 2BCT 10MTN S2
 Sent: Friday, May 21, 2010 12:33 PM
 To: (b)(6)(b)(7)(C)
 Subject: Second Attempt

FCC:
 imap://bradley.e.manning%40gmail.com@imap.googlemail.com/[Gmail]/Sent Mail
 X-Identity-Key: id1
 Message-ID: <4BF64BF8.8030901@gmail.com>
 Date: Fri, 21 May 2010 12:02:50 +0300
 From: Bradley Manning <bradley.e.manning@gmail.com>
 Reply-To: bradley.e.manning@gmail.com
 X-Mozilla-Draft-Info: internal/draft; vcard=0; receipt=0; DSN=0; uuencode=0
 User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.1.9) Gecko/20100317 Thunderbird/3.0.4
 MIME-Version: 1.0
 To: (b)(6)(b)(7)(C).org>
 Subject: Second Attempt
 X-Enigmail-Version: 1.0.1
 Content-Type: multipart/encrypted;
 protocol="application/pgp-encrypted";
 boundary="-----enigBD91D3513DB65FD5D2053069"

This is an OpenPGP/MIME encrypted message (RFC 2440 and 3156)
 -----enigBD91D3513DB65FD5D2053069
 Content-Type: application/pgp-encrypted
 Content-Description: PGP/MIME version identification

U) Figure 9 - Excerpt of the PGP encrypted email content in Second Attempt.txt

6.1.11 Examination of files containing Global Address List (GAL) information:

Previous forensic examination of PFC MANNING's personal computer by Mr. (b)(6)(b)(7)(C) revealed a text fragment detailing the acquisition and exfiltration of a GAL from the United States Forces - Iraq SharePoint Exchange server. Further examination by Mr. (b)(6)(b)(7)(C) revealed what appeared to be an extract of an Exchange GAL. (See the forensic examination report for PFC MANNING's personal computer for details.)

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) My Documents\blah.txt on the Supply Annex NIPRNET computer revealed a large text file that appeared to be an extract of an Exchange GAL, located in the peter.bigelow user account (excerpt shown in Figure 10 below). See Attachment B on Enclosure 1 to this report for the complete file.



Forensic Report for Supply Annex NIPRNET computer



```

/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative
Group/cn=Recipients/cn=raymond.t.odierno.hood.iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil

```

Figure 10 - GAL extract contained in blah.txt

EXAMINER'S NOTE: Previous forensic examinations of PFC MANNING's personal computer and primary SIPRNET computer revealed that "Blah" appeared to be a naming convention for files commonly used by PFC MANNING.

Full Path C:\Documents and Settings\ (b)(6)(b)(7)(C) \My Documents\blah.txt

File Created 05/22/10 07:31:38PM

Logical Size 6,903,830

Hash Value a8e97b3e99d5f0e0f618f11c0d04fd3a

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 11 - File attributes for blah.txt

EXAMINER'S NOTE: As noted previously, the Supply Annex SIPRNET computer was not configured to require CAC logon. As such, it is unknown if SSG (b)(6)(b)(7)(C) was the actual creator of the files related to the GAL or if PFC MANNING used SSG (b)(6)(b)(7)(C) account.

User name:	(b)(6)(b)(7)(C)
Full Name:	
Type of User:	Domain User
Account Description:	
Primary Group Number:	0
Security Identifier:	S-1-5-21-2175376772-4088186718-847205759-4624
Logon Script:	
Profile Path:	%SystemDrive%\Documents and Settings\peter.bigelow
Last Logon:	



Forensic Report for Supply Annex NIPRNET computer



Last Password Change:

Last Incorrect Password Logon:

Figure 12 - The SID of the user (b)(6)(b)(7)(C)

Examination of the Recycle Bin for the (b)(6)(b)(7)(C) user account (C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624) revealed five (5) files related to the GAL, including two (2) text files named *blah.txt*, two (2) .ZIP archives named *blah.zip*, and a text file named *tmp.txt*. The .ZIP archives each contained a text file named *blah.txt*. Examination of the text files revealed what appeared to be extracts of an Exchange GAL similar to the extracts located in the file C:\Documents and Settings\My Documents\blah.txt and on PFC MANNING's personal computer. Although the extracts contained in the text files were similar, all the files were of different sizes and MD5 hash values, indicating that they were not identical.

Name	File Created	File Deleted	Hash Value	Logical Size
blah.txt	05/13/10 08:21:58PM	05/13/10 08:26:09PM	2231a1f4abbfcc02ca656a1625804bd7	3,051,535
blah.txt			2dd61d43dcd1200a289b95c78a43ff86	3,051,520
blah.txt	05/13/10 08:06:12PM	05/13/10 08:15:02PM	316cd22b96ca20d4ae898f65280b0e2a	6,906,165
blah.txt	05/22/10 07:31:38PM		a8e97b3e99d5f0e0f618f11c0d04fd3a	6,903,830
blah.txt			ab738fef80f667e0f4a265a37dfbf967	6,905,856
tmp.txt	05/13/10 07:08:54PM	05/13/10 08:18:14PM	bf60b84d3be180d16a059cf1bc395e5c	5,998

Figure 13 - File attributes for the six (6) files related to the GAL on the Supply Annex SIPRNET computer

Full Path C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.txt
 Description File, Recycled, Archive
 File Created 05/13/10 08:21:58PM
 Logical Size 3,051,535
 Hash Value 2231a1f4abbfcc02ca656a1625804bd7

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	



Forensic Report for Supply Annex NIPRNET computer



Figure 14 - File attributes for blah.txt (MD5:
2231alf4abbfcc02ca656a1625804bd7)

EXAMINER'S NOTE: Figure 15 below shows only an excerpt from the file
C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.txt
(MD5: 2231alf4abbfcc02ca656a1625804bd7). See Attachment C on Enclosure 1 to this
report for the complete file.

```
(Bragg)(b)(6)(b)(7)(C) LTG MNC-I CG
(Hood)(b)(6)(b)(7)(C) LTG MNC-I CMD GRP Commanding General
***Delete Duplicate account***(b)(6)(b)(7)(C) SSG 129 CSSB SPO Plans
1 AD STB S3 MAC
10 SBTB S-1 Customer Service
10 SBTB S3 TOC
100BSB BTL CPT
100BSB Helpdesk
101 ENG BN S6
101st FMD Travel Processing
101st HR CO,
1034 CSSB Battle Captain
```

Figure 15 - Excerpt of blah.txt (MD5: 2231alf4abbfcc02ca656a1625804bd7)

Full Path C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.txt
Description File, Recycled, Archive
File Created 05/13/10 08:06:12PM
Logical Size 6,906,165
Hash Value 316cd22b96ca20d4ae898f65280b0e2a

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 16 - File attributes for blah.txt (MD5:
316cd22b96ca20d4ae898f65280b0e2a)

EXAMINER'S NOTE: Figure 17 below shows only an excerpt from the file
C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.txt
(MD5: 316cd22b96ca20d4ae898f65280b0e2a). See Attachment D on Enclosure 1 to this report for
the complete file.

```
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C).iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative
```




Forensic Report for Supply Annex NIPRNET computer



```

/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=10sbtbslcustomerserv.iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=10sbtbs3toc.iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=100bsbtlcpt.iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=100bsbhelpdesk.iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=101engbns6.mnd-b.army.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=travel.processing.1bct3id.army.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=101hrco.iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=10341tffbattlecpt.iraq.centcom.mil

```

Figure 20 - Excerpt of blah.txt (MD5: ab738fef80f667e0f4a265a37dfbf967)

Full PathC:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.zip

DescriptionFolder, Recycled, Archive

File Created05/13/10 08:14:31PM

Logical Size1,114,687

Hash Value30f1b75288516fd1ab988a203fc2dc75

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 21 - File attributes for blah.zip (MD5: 30f1b75288516fd1ab988a203fc2dc75)

Full Path	C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.zip\blah.txt		
File Category	Document		
Description	File		
Logical Size	3,051,520		
Hash Value	2dd61d43dcd1200a289b95c78a43ff86		

Figure 22 - File attributes for blah.txt contained in blah.zip (MD5: 30f1b75288516fd1ab988a203fc2dc75)

EXAMINER'S NOTE: Figure 21 below shows only an excerpt from the file C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\blah.zip\blah.txt (MD5: 2dd61d43dcd1200a289b95c78a43ff86). See Attachment F on Enclosure 1 to this report for the complete file.

(b)(6)(b)(7)(C) MSG 330th Trans BN Sr Movements NCO
 (b)(6)(b)(7)(C) Military Assistance Support Team (MAST) MITT 0800
 (b)(6)(b)(7)(C) SSG 2-25 1-14 IN BN HHC THT
 (b)(6)(b)(7)(C) SSG HHB 3-133 FA Battle NCO
 (b)(6)(b)(7)(C) CPT 3-4 HHT XO
 (b)(6)(b)(7)(C) SGT MNC-I 749 EOD
 (b)(6)(b)(7)(C) SG MNSTC-I Force Protection



Forensic Report for Supply Annex NIPRNET computer



(b)(6)(b)(7)(C) SSG 2-25 1-27 BN PSG
 (b)(6)(b)(7)(C) CPT MNC-I 54th EN BN 535th ESC
 (b)(6)(b)(7)(C) CPT USA TF449 HHC PAO OIC
 (b)(6)(b)(7)(C) CIV ITT TAC-SWACAA RNOSC Theater VOIP
 (b)(6)(b)(7)(C) CPT 1-27 Redeployment Officer

Figure 23 - Excerpt of blah.txt (MD5: 2dd61d43dcd1200a289b95c78a43ff86)

Full Path C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\tmp.txt

Description File, Recycled, Archive

File Created 05/13/10 07:08:54PM

Logical Size 5,998

Hash Value bf60b84d3be180d16a059cf1bc395e5c

Permissions

Name	Id	Property	Permissions
(b)(6)(b)(7)(C)	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
(b)(6)(b)(7)(C)	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 24 - File attributes for tmp.txt

EXAMINER'S NOTE: Figure 25 below shows only an excerpt from the file

C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\tmp.txt.

See Attachment G on Enclosure 1 to this report for the complete file.

```
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) bucca.iraq.army.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) lbct3id.army.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) iraq.centcom.mil
/o=2BCT10MTN/ou=First Administrative Group/cn=Recipients/cn=(b)(6)(b)(7)(C) mnd-b.army.mil
```

Figure 25 - Excerpt of tmp.txt

6.1.12 Examination of the file C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\tmp.pdf:

Examination of the Recycle Bin for the user account (b)(6)(b)(7)(C) revealed the file C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\tmp.pdf, which contained military documents related to PFC MANNING. The file



Forensic Report for Supply Annex NIPRNET computer



contained 18 pages of scanned documents, including the following: DA 2627 (record of UCMJ action for striking SPC (b)(6)(b)(7)(C) Article 15 Rights; Maximum Punishments and Filing form; DA 4856 (counseling for assault of SPC (b)(6)(b)(7)(C) five (5) DA 2823 forms (Sworn Statements in reference to the SPC (b)(6)(b)(7)(C) assault); DA 3881 (Rights Warning/Waiver Certificate for PFC MANNING); DA 5248-R (Report of Unfavorable Information for Security Determination documenting the SPC (b)(6)(b)(7)(C) assault); and PFC MANNING's Enlisted Record Brief.

EXAMINER'S NOTE: As noted previously, the Supply Annex SIPRNET computer was not configured to require CAC logon. As such, it is unknown if SSG (b)(6)(b)(7)(C) was the actual creator of the *tmp.pdf* file or if PFC MANNING used SSG (b)(6)(b)(7)(C) account.

Full PathC:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\tmp.pdf

DescriptionFile, Recycled, Archive

File Created05/21/10 10:17:08AM

Logical Size1,148,809

Hash Value63e6a3463bb3a96cce17fb3fea7b258f

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]

Figure 26 - File attributes for tmp.pdf

EXAMINER'S NOTE: Figure 27 below shows only an excerpt from the file C:\RECYCLER\S-1-5-21-2175376772-4088186718-847205759-4624\tmp.pdf. See Attachment H on Enclosure 1 to this report for the complete file.

DEVELOPMENTAL COUNSELING FORM			
For use of this form see FM 22-100. The proponent agency is TRADOC			
DATA REQUIRED BY THE PRIVACY ACT OF 1974			
AUTHORITY:	5 USC 301 Departmental Regulations; 10 USC 3013, Secretary of the Army and E.O. 9397 (SSN)		
PRINCIPAL PURPOSE:	To assist leaders in conducting and recording counseling data pertaining to subordinates		
ROUTINE USES:	For subordinate leader development (AW FM 22-100) Leaders should use this form as necessary.		
DISCLOSURE:	Disclosure is voluntary.		
PART I - ADMINISTRATIVE DATA			
Name (Last, First, MI)	Rank/Grade	Social Security No.	Date of Counseling
Manning, Bradley	SPC	(b)(6)(b)(7)(C)	17 MAY 10
Organization	Name and Title of Counselor		
HHC 2BCT, 10th MTN DIV (LI)	SGT (b)(6)(b)(7)(C) PSG		
PART II - BACKGROUND INFORMATION			
Purpose of Counseling: (Leader states the reason for the counseling, e.g., performance/professional growth or event-oriented counseling and includes the leader's facts and observations prior to the counseling)			
Event-Oriented (Assault and Battery)			



Figure 27 - Excerpt of tmp.pdf displaying PFC MANNING's DA Form 4856

**6.1.13 Examination of the Internet History files for the user account
bradley.manning:**

Examination of the file *C:\Documents and Settings\bradley.manning\Local Settings\History\History.IE5\index.dat* (numerous excerpts shown in the figures below) revealed it was a list of local files viewed and web pages visited by a user of the user account bradley.manning. This file would have only captured activity if either Microsoft Internet Explorer or Windows Explorer were used for viewing the file or URL. See Attachment I on Enclosure 1 to this report for the complete file.

Further analysis of the *C:\Documents and Settings\bradley.manning\Local Settings\History\History.IE5\index.dat* file revealed the following:

A user of the user account bradley.manning viewed *Second Attempt.txt* while it was located in the account's *My Documents* folder.

Name	Url Name	Last Accessed
<input checked="" type="checkbox"/> index.dat	file:///C:/Documents and Settings/bradley.manning/My Documents/Second Attempt.txt	05/21/10 07:14:38PM

Figure 28 - Index.dat entry for Second Attempt.txt

A user of the user account bradley.manning visited the website *http://news.google.com* and searched for "wikileaks".

Name	Url Name	Last Accessed
<input checked="" type="checkbox"/> index.dat	http://news.google.com/news/search?aq=f&pz=1&cf=all&ned=us&hl=en&q=wikileaks	05/21/10 02:23:17PM
<input checked="" type="checkbox"/> index.dat	http://news.google.com/news/search?pz=1&cf=all&ned=us&hl=en&q=wikileaks&cf=all&as_qdr=d&as_drrb=q	05/21/10 02:23:48PM
<input checked="" type="checkbox"/> index.dat	http://news.google.com/news?pz=1&cf=all&ned=us&hl=en&q=wikileaks&as_qdr=d&as_drrb=q&cf=all&output=rss	05/21/10 02:23:25PM
<input checked="" type="checkbox"/> index.dat	http://news.google.com/news?pz=1&cf=all&ned=us&hl=en&q=wikileaks&cf=all&output=rss	05/21/10 02:23:16PM

Figure 29 - Index.dat entries for *http://news.google.com* related to "wikileaks"

A user of the user account bradley.manning visited the website *http://usmilitary.about.com* for information regarding Non-Judicial Punishment (Article 15).

Name	Url Name	Last Accessed
<input checked="" type="checkbox"/> index.dat	http://usmilitary.about.com/od/justicelawlegislation/a/article152.htm	05/21/10 01:00:43PM
<input checked="" type="checkbox"/> index.dat	http://usmilitary.about.com/od/justicelawlegislation/a/article152_2.htm	05/21/10 01:02:57PM

Figure 30 - Index.dat entries for *http://usmilitary.about.com* related to Article 15



Forensic Report for Supply Annex NIPRNET computer



A user of the user account bradley.manning visited the website <http://www.google.com> using the search terms "closed open article 15 hearing".

Name	Url Name	Last Accessed
index.dat	http://www.google.com/search?hl=en&source=hp&q=closed+open+article+15+hearing&aq=o&aqi=...	05/21/10 01:00:35PM

Figure 31 - Google search for "closed open article 15 hearing"

A user of the user account bradley.manning visited the websites <http://www.google.com>, <https://www.google.com>, and <https://mail.google.com> for Gmail email account access.

Name	Url Name	Last Accessed
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.1e.1.0&view=tl&start=...	05/21/10 12:50:43PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:dad.1e.2.0&view=tl&start=...	05/21/10 12:50:49PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.1e.3.0&view=tl&start=...	05/21/10 12:51:03PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.1e.4.0&view=tl&start=...	05/21/10 12:55:58PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.22.1.0&view=tl&start=...	05/21/10 02:09:29PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.23.1.0&view=tl&start=...	05/21/10 02:42:30PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.23.2.0&view=tl&start=...	05/21/10 02:46:06PM
index.dat	http://mail.google.com/mail/?hl=en&tab=wm	05/22/10 06:33:53PM
index.dat	https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&...	05/22/10 06:33:59PM
index.dat	https://www.google.com/accounts/ServiceLoginAuth?service=mail	05/22/10 06:34:02PM
index.dat	https://mail.google.com/mail/feed/atom	05/22/10 06:34:09PM
index.dat	https://mail.google.com/mail/feed/atom	05/22/10 06:34:15PM
index.dat	https://mail.google.com/mail/?hl=en&safe=on&shva=1	05/22/10 06:34:15PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:ex.29.2.1&view=cv&th=1...	05/22/10 06:34:28PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:ex.29.3.0&view=cv&th=1...	05/22/10 06:34:36PM
index.dat	https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:ex.29.3.0&view=cv&th=1...	05/22/10 06:34:37PM

Figure 32 - Index.dat entries for Gmail account access

6.1.14 Examination of the Internet History files for the user account

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

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) Local Settings\History\History.IE5\ index.dat (numerous excerpts shown in the figures below) revealed it was a list of local files viewed and web pages visited by the user account (b)(6)(b)(7)(C). This file would have only captured activity if either Microsoft Internet Explorer or Windows Explorer were used for viewing the file or URL. See Attachment J on Enclosure 1 to this report for the complete file.



Forensic Report for Supply Annex NIPRNET computer



Further analysis of the *C:\Documents and Settings*

(b)(6)(b)(7)(C) *Local Settings\History\History.IE5\index.dat* file revealed the following:

A user of the user account (b)(6)(b)(7)(C) viewed the files *blah.txt* and *tmp.pdf* while they were located in the account's *My Documents* folder.

Name	Url Name	Last Accessed
index.dat	file:///C:/Documents and Settings/peter.bigelow/My Documents/blah.txt	05/22/10 07:32:00PM
index.dat	file:///C:/Documents and Settings/peter.bigelow/My Documents/tmp.pdf	05/21/10 10:41:18AM

Figure 33 - Excerpt of the index.dat file for user peter.bigelow

EXAMINER'S NOTE: Examination of the Internet History for the user (b)(6)(b)(7)(C) suggested that PFC MANNING had access to the (b)(6)(b)(7)(C) user account. The Internet History contained web pages displaying the logged-in user as PFC MANNING. The file *index.dat* contained logins to PFC MANNING's Army Knowledge Online (AKO) and Gmail accounts, as well as visits to the Google Search page using search terms such as "wikileaks" and "julian assange". See Attachment K on Enclosure 1 to this report for examples.

Examination of the file *C:\Documents and Settings*

(b)(6)(b)(7)(C) *Local Settings\Temporary Internet Files\Content.IE5\R1S3NL93\ref=ox_signinddec9057[1].htm* revealed an Amazon.com checkout page. The page displayed "Bradley Manning, 1492 Selworthy Road, Potomac, Maryland 20854" in the "Shipping to" section. The second half of the page showed the same information in the "Billing" section.



Forensic Report for Supply Annex NIPRNET computer



our Order - Amazon.com Chec...

Place Your Order - Amazon.com Checkout

Please review and submit your order
By placing your order, you agree to Amazon.com's privacy notice and conditions of use.

Review the information below, then click "Place your order"

Shipping Details

Shipping to:

Bradley Manning
(b)(6)(b)(7)(C)

Shipping Options: [Learn more](#)

☐ FREE Two-Day Shipping on this Order: Bradley Manning, you can save \$2 with a free trial of Amazon Prime below.
» [Sign up for free trial](#)

Choose a shipping speed:

☐ FREE Super Saver Shipping (5-9 business days)

☐ FREE Two-Day Shipping with a free trial of --get it Tuesday, May 18! ([Learn more](#))

☐ Standard Shipping (3-5 business days)

☐ Two-Day Shipping --get it Tuesday, May 18!

☐ One-Day Shipping --get it Monday, May 17!

Need to ☐ [Change quantity](#) ?

Estimated delivery date for this item: May 20, 2010

Facial Feminization Surgery: A Guide for the Transgendered Woman - Douglas K. Ouster
\$49.95 - Quantity: 1 - In Stock - Eligible for Amazon Prime shipping rates: [join now](#)
Condition: New
Sold by: Amazon.com, LLC
Edit Gift Info Gift options None ☐ [Edit](#)



Forensic Report for Supply Annex NIPRNET computer



order.™ **Place your order**

Order Summary

Items: \$49.95
Shipping & Handling: \$3.99
Total Before Tax: \$53.94
Estimated Tax: \$0.00
Order Total: \$53.94

Save on shipping! Select FREE Super Saver Shipping as your shipping speed, and we'll remove the shipping fees on the eligible items in your order.

Have any gift cards, gift certificates or promotional claim codes? ([Learn more](#)) Enter them here (one at a time):

Payment Methods:
☐ Chk
Visa : ***-7216
Exp: 05/2013
Billing Address: ☐ Chk
Bradley Manning
(b)(6)(b)(7)(C)

ive \$3.99 on this order by selecting "FREE Two-Day Shipping"

!! ([Learn more](#))

Justerhout MD

order.™ **Place your order**

Figure 34 - Excerpt of the file ref=ox_signindec9057[1].htm (Amazon order page)

Full Path C:\Documents and Settings\ (b)(6)(b)(7)(C) \Local Settings\Temporary Internet Files\Content.IE5\R1S3NL93\ref=ox_signindec9057[1].htm
File Created 05/15/10 01:52:08PM
Last Accessed 05/15/10 01:52:12PM
Hash Value c075275fce3b4cbbcdf4e79b4b008dbf

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]



Forensic Report for Supply Annex NIPRNET computer



Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 35 - File attributes for ref=ox_signindec9057[1].htm

EXAMINER'S NOTE: Figure 34 above and Figures 36, 38, 45, 47, 49, 51 and 53 below show only excerpts of each file. See Attachment L on Enclosure 1 to this report for the complete files.

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\A7G1ULY9\ref=kinww_ddp[1].htm revealed an Amazon.com web page displaying a logged-in user of "Bradley Manning".

Figure 36 - Excerpt of the file ref=kinww_ddp[1].htm

Full Path	C:\Documents and Settings\peter.bigelow\Local Settings\Temporary Internet Files\Content.IE5\A7G1ULY9\ref=kinww_ddp[1].htm
-----------	---



Forensic Report for Supply Annex NIPRNET computer



File Created 05/20/10 08:49:54PM
 Last Accessed 05/20/10 08:57:27PM
 Hash Value 70941022a81b4241ebdf4a7b59557743

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 37 - File attributes for ref=kinww_ddp[1].htm

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\RJJUEUUU\search[3].htm revealed a Google search web page where the logged-in user was displayed as "bradley.e.manning@gmail.com".

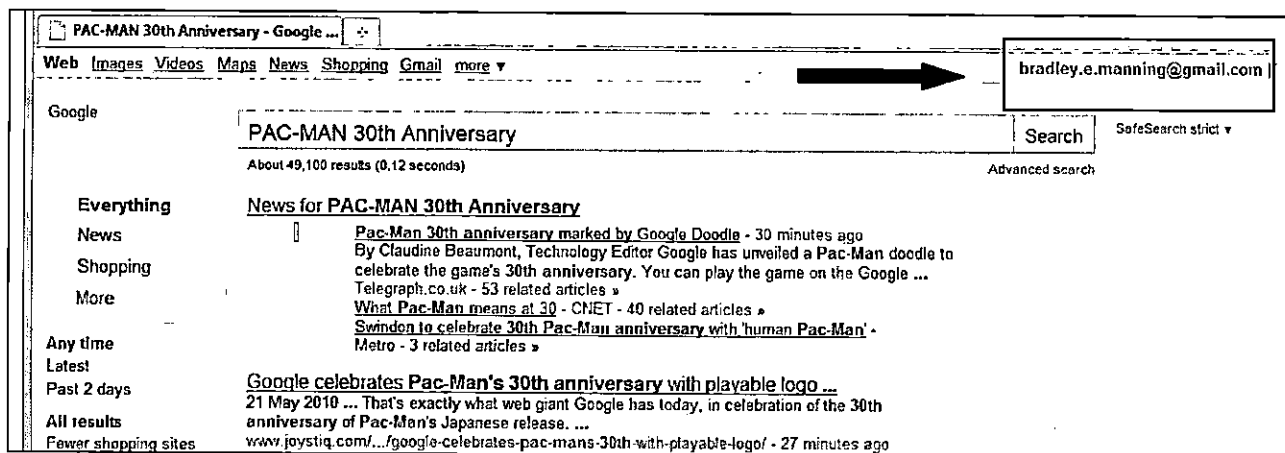


Figure 38 - Excerpt of the file search[3].htm

Full Path	C:\Documents and Settings\ (b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\RJJUEUUU\search[3].htm		
File Created	05/21/10 07:04:31PM		
Last Accessed	05/21/10 07:04:31PM		
Hash Value	769d1a985b9f26ced0492d511accadba		
Permissions			
Name	Id	Property	Permissions



Forensic Report for Supply Annex NIPRNET computer



Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 39 - File attributes for search[3].htm

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) Local Settings\History\History.IE5 \index.dat revealed a user of the (b)(6)(b)(7)(C) user profile visited the AKO website <https://www.us.army.mil> logged-in as "Bradley.Manning".

Uniform Resource Locator (URL)	Date Visited
(b)(6)(b)(7)(C)@https://www.us.army.mil/suite/portal/index.jsp;jsessionid=2870312C297E74A557551BDF0CA030BD.appd06 1-P.....8...https://www.us.army.mil/suite/login/favicon.ico.....X...Army Knowledge Online - bradley.manning	05/19/10 16:38:58

Figure 40 - Excerpt of the index.dat file for user profile peter.bigelow

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) Local Settings\History\History.IE5 \index.dat revealed a user of the (b)(6)(b)(7)(C) user profile visited the Gmail website <https://mail.google.com> logged-in as "bradley.e.manning@gmail.com".

Uniform Resource Locator (URL)	Date Visited
(b)(6)(b)(7)(C)@https://mail.google.com/mail/?shva=1.....8...https://mail.google.com/mail/images/favicon.ico.....h...Gmail - In-box (3) - bradley.e.manning@gmail.com	05/21/10 10:44:45

Figure 41 - Excerpt of the index.dat file for user profile (b)(6)(b)(7)(C)

Examination of the Unallocated Clusters revealed a remnant of an index.dat

Internet History file where a user of the (b)(6)(b)(7)(C) user profile visited the Gmail website <https://mail.google.com> logged-in as "bradley.e.manning@gmail.com".

Full Path C:\Unallocated Clusters File Offset 25131711345	Date Visited
(b)(6)(b)(7)(C)@https://mail.google.com/mail/?shva=1.....8...https://	05/13/10



Forensic Report for Supply Annex NIPRNET computer



mail.google.com/mail/images/favicon.ico.....h...Gmail...Inbox... (2) .. - bradley.e.manning@gmail.com	20:17:24
--	----------

Figure 42 - Excerpt of the index.dat file remnant for user profile

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

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) Cookies\ (b)(6)(b)(7)(C) @mail.google[2].txt revealed a cookie for Gmail listing the email account as "bradley.e.manning@gmail.com".

gmailchat bradley.e.manning@gmail.com/493521 mail.google.com/mail

Figure 43 - Excerpt of the file (b)(6)(b)(7)(C) mail.google[2].txt

Full PathC:\Documents and Settings\peter.bigelow\Cookies\peter.bigelow@mail.google[2].txt

DescriptionFile, Deleted, Archive, Not Indexed

File Created05/21/10 07:01:47PM

Logical Size112

Hash Value0c937a620ae442252a7cac1a97ccfd13

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 44 - File attributes for the file (b)(6)(b)(7)(C) @mail.google[2].txt

Examination of the file C:\Documents and Settings

(b)(6)(b)(7)(C) \Local Settings\Temporary Internet Files
\Content.IE5\NGI46ZO8\search[11].htm revealed a Google News search page with results for searching "wikileaks".



Forensic Report for Supply Annex NIPRNET computer



Maps News Shopping Gmail more ▾

wikileaks Search [Advanced news search](#)
[Preferences](#)

WikiLeaks works to expose government secrets, but Web site's sources are a mystery
Washington Post - [Joby Warrick](#) - 10 hours ago
BERLIN -- For an organization dedicated to exposing secrets, WikiLeaks keeps a close hold on its own affairs. Its Web site doesn't list a ...

Wikileaks Founder Thinks Everyone's Out to Get Him: Don't Buy It
Gawker - 9 hours ago
Wikileaks founder Julian Assange claims that Australian officials confiscated his passport. He added, ominously, that Australian police questioned him about ...

5 pioneering Web sites that could totally change the news
New York Daily News - [Paulina Reso](#) - 3 hours ago
WikiLeaks accepts submissions of confidential political documents, reviews them to determine accuracy and relevance, then publishes them for mass ...

WikiLeaks founder has his passport confiscated
Salon - [Glenn Greenwald](#) - May 19, 2010
The Australian founder of the whistleblower website Wikileaks had his passport confiscated by police when he arrived in Melbourne last ...

Figure 45 - Excerpt of the file search[11].htm

Full PathC:\Documents and Settings\ (b)(6)(b)(7)(C) \Local Settings\Temporary Internet Files\Content.IE5\NGI46ZO8\search[11].htm

File Created05/20/10 02:36:23PM

Last Accessed05/20/10 02:36:28PM

Hash Valueb1056fb1af8c0f00b48ac927a1ed29df

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 46 - File attributes for search[11].htm

Examination of the file C:\Documents and Settings
(b)(6)(b)(7)(C) \Local Settings\Temporary Internet Files
\Content.IE5\EN6P6BCB\search[3].htm revealed a Google search page with results
for searching "julian assange".



Forensic Report for Supply Annex NIPRNET computer



Julian assange - Google Search

Web Images Videos Maps News Shopping Gmail more ▾

Google

Search

About 637,000 results (0.34 seconds) Advanced search

Everything

Julian Assange - Wikipedia, the free encyclopedia
 Julian Assange (English pronunciation: /əˈsɑːnʒ/; born in the 1970s) is an Australian journalist, programmer and Internet activist, best known for his ...
en.wikipedia.org/wiki/Julian_Assange - 13 hours ago - Cached - Similar

News

Wikileaks - Wikipedia, the free encyclopedia
 Wikileaks editor Julian Assange said that some details in the Army report Presentation by Wikileaks representatives Julian Assange and Daniel Schmitt ...
en.wikipedia.org/wiki/Wikileaks - Cached - Similar

More

Any time

Past month

More search tools

Profile: Julian Assange, the man behind Wikileaks - Times Online
 11 Apr 2010 ... Julian Assange dreamt that one day the internet would streamline the leaking of state secrets.
technology.timesonline.co.uk/tel/news/tech_and_/article7094231.ece

Julian Assange | April 12, 2010 - Julian Assange | ColbertNation.com
 12 Apr 2010 ... ColbertNation.com video - Julian Assange entitled the Apache helicopter video 'Collateral Murder' in order to get maximum political impact.
www.colbertnation.com/the-colbert-report_/april.../julian-assange - Cached

Exclusives - Julian Assange Unedited Interview | April 12, 2010 ...
 12 Apr 2010 ... ColbertNation.com video - In this complete, unedited interview, Julian Assange defends the decision to expose the Apache helicopter attack ...
www.colbertnation.com/exclusives-julian-assange-unedited-interview - Cached

Julian Assange -- New Media Days
 JULIAN ASSANGE is a journalist, programmer and activist. He sits on the Advisory Board of WikiLeaks and acts as their spokesperson. ...
newmediadays.dk/julian-assange - Cached - Similar

Figure 47 - Excerpt of the file search[3].htm

Full PathC:\Documents and Settings\ (b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\EN6P6BCB\search[3].htm

File Created05/14/10 01:06:39PM

Last Accessed05/14/10 01:06:40PM

Hash Value8ba2c875381a2db64e27351e2815ed21

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 48 - File attributes for search[3].htm

Examination of the file C:\Documents and Settings\ (b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\EN6P6BCB\search[1].htm revealed a Google search page with results for searching "global address list microsoft excel macro".



Forensic Report for Supply Annex NIPRNET computer



EXAMINER'S NOTE: As noted previously, files were contained on the Supply Annex NIPRNET computer that appeared to contain extracts of a GAL from the United States Forces – Iraq SharePoint Exchange e-mail system. The search phrase results (shown in Figure 49 below) appeared to lead to instructions for exporting a GAL to a searchable format.

global address list microsoft excel macro

Web Images Videos Maps News Shopping Gmail more ▼

Google

global address list microsoft excel macro Search SafeSearch strict ▼

About 153,000 results (0.28 seconds) Advanced search

Everything More

Show search tools

Looking Up Names In A Global Address Book - Excel Help & Excel ...
 14 May 2008 ... GIVE YOURSELF OR YOUR COMPANY FREE 24/7 MICROSOFT EXCEL SUPPORT & QUESTIONS FOR LIFE ... AddressLists("Global Address List") Set M = oApp.

www.ozgrid.com ... HELP FORUMS ... Excel and/or Email Help - Cached

Global Address List Lookup From Within Workbook - Microsoft Excel ... - 8 Sep 2007
Outlook Global Address List in Listbox - Excel Help & Excel Macro Help - 20 Apr 2006
Open Outlook & Global Address Book - Microsoft Excel® Training ... - 1 Sep 2005
Address Book in a List/Combobox - Microsoft Excel® Training, Excel ... - 3 Aug 2004

More results from ozgrid.com >

VBA Express: Excel - Extract Email Data From Outlook Global ...
 Dumping the GAL to Excel provides an list in a form that can be easily searched or ... While in the VBE, choose Tools - References and put a check in Microsoft CDO ... Run the macro by going to Tools-Macro-Macros and double-click GetGAL ...
 www.vbaexpress.com/kb/getarticle.php?kb_id=222 - Cached - Similar

Free excel macro pull global address book Download - excel macro ...
 Related searches: download global address book excel macro ping ip address ...
 ExcelReport is a report generator for Microsoft excel that uses Microsoft ...
 software.informer.com/getfree-excel-macro-pull-global-address-book/ - Cached

How to record a macro using relative cell references in Excel
 In Macro Name list, click the name of the macro that you recorded, ... For more information about recording macros, click Microsoft Excel Help on the Help ...
 support.microsoft.com/kb/213740 - Cached - Similar

Converting Addresses
 cc:Mail distribution lists, Microsoft Exchange Server GAL, Excel Macro for Migration of cc:Mail Distribution Lists, cc:Mail directory and address lists ...
 www.clickick.com/clickick-excel-macro-pull-global-address-book/ - Cached - Similar

Figure 49 – Excerpt of the file search[1].htm

Full PathC:\Documents and Settings\(b)(6)(b)(7)(C)\Local Settings\Temporary Internet Files\Content.IE5\EN6P6BCB\search[1].htm

File Created05/11/10 03:28:35PM

Last Accessed05/11/10 03:28:36PM

Hash Value5988cf92bf5120b4caa55c839bcea81a

Permissions

Name	Id	Property	Permissions
(b)(6)(b)(7)(C)	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
(b)(6)(b)(7)(C)	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	



Forensic Report for Supply Annex NIPRNET computer



Figure 50 - File attributes for search[1].htm

Examination of the file *C:\Documents and Settings (b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\A7G1ULY9\search[2].htm* revealed a Google search page with results for searching "global address list macro outlook".

The screenshot shows a Google search results page. The search bar contains the text "global address list macro outlook". Below the search bar, it says "About 174,000 results (0.32 seconds)". The results are listed under the heading "Everything". The first result is "VBA Express : Excel - Extract Email Data From Outlook Global ...". The second result is "[SOLVED] Read details from Global Address Book in Outlook into ...". The third result is "Outlook Macro to get Exchange Info from Mail, help, FAQ, forums ...". The fourth result is "Outlook - New Message with Completed From Field | Amset.info". The fifth result is "outlook global address list in listbox - Excel Help & Excel Macro Help".

Figure 51 - Excerpt of the file search[2].htm

Full PathC:\Documents and Settings\ (b)(6)(b)(7)(C) Local Settings\Temporary Internet Files\Content.IE5\A7G1ULY9\search[2].htm

File Created05/11/10 03:33:19PM

Last Accessed05/11/10 03:33:46PM

Hash Valuecb6c9250e419851873a3585b1aa5b92b

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]



Forensic Report for Supply Annex NIPRNET computer



Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 52 - File attributes for search[2].htm

Examination of the file *C:\Documents and Settings*
(b)(6)(b)(7)(C) *Local Settings\Temporary Internet*
Files\Content.IE5\A7G1ULY9\search[1].htm revealed a Google search page with
 results for searching "vba outlook write text file".

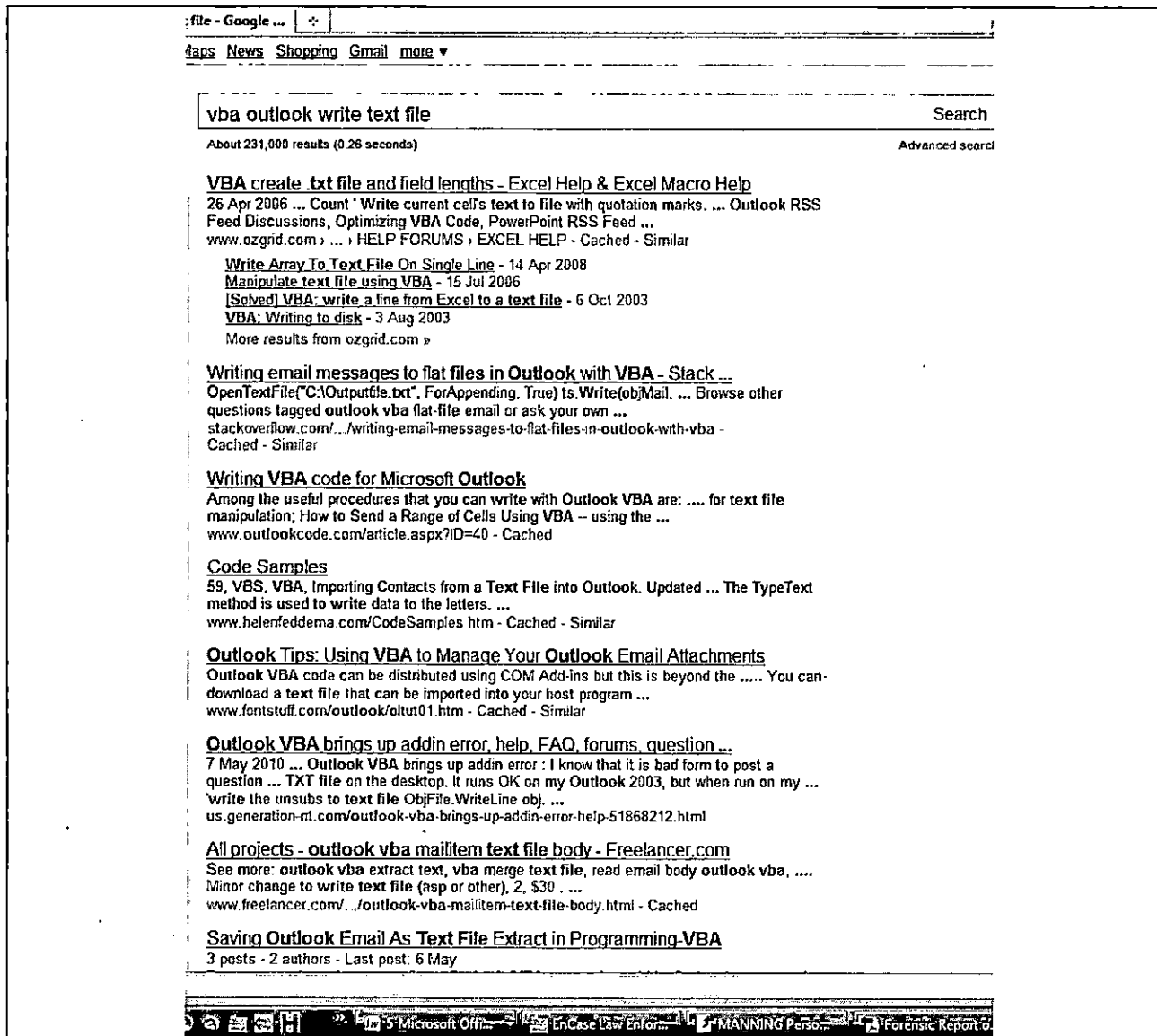


Figure 53 - Excerpt of the file search[1].htm



Forensic Report for Supply Annex NIPRNET computer



Full PathC:\Documents and Settings\ (b)(6)(b)(7)(C) \local Settings\Temporary Internet Files\Content.IE5\A7G1ULY9\search[1].htm

File Created05/13/10 07:05:38PM

Last Accessed05/13/10 07:09:46PM

Hash Valuee9bee42fd3552448c07e19701b10ef49

Permissions

Name	Id	Property	Permissions
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Allow	[FC] [M] [R&X] [R] [W] [Sync]
System	S-1-5-18	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] [W] [Sync]
Peter.Bigelow	S-1-5-21-2175376772-4088186718-847205759-4624	Owner	
Domain Users	S-1-5-21-2175376772-4088186718-847205759-513	Group	

Figure 54 - File attributes for search[1].htm

7. Summary of Examination:

Examination of the U.S. Government Supply Annex NIPRNET Computer (UNCLASSIFIED), utilized by PFC Bradley MANNING revealed the following:

- A. PFC MANNING communicated with Mr. (b)(6)(b)(7)(C) via a PGP-encrypted email.
- B. A scanned .PDF file pertaining to the Article 15 of PFC MANNING was located within the Recycler folder of the (b)(6)(b)(7)(C) user account (primarily used by SSG (b)(6)(b)(7)(C)).
- C. A user of the user account bradley.manning searched for the keyword "wikileaks".
- D. A user of the user account (b)(6)(b)(7)(C) searched for the keywords "wikileaks" and "Julian Assange".
- E. A user of the user account (b)(6)(b)(7)(C) logged into PFC MANNING's AKO account, Gmail email account and Amazon account.
- F. There were text files containing extracts from a Defense Global Address List in the Recycler folder and the My Documents folder of the user account (b)(6)(b)(7)(C).



Forensic Report for Supply Annex NIPRNET computer

**8. Investigative Leads:**

A) Contact Mr. (b)(6)(b)(7)(C) to obtain any private keys from his PGP key ring to attempt to decrypt the PGP encrypted email.

B) Interview SSG (b)(6)(b)(7)(C) to determine if he created the files tmp.pdf, tmp.txt, blah.txt and blah.zip. Determine if SSG (b)(6)(b)(7)(C) allowed PFC MANNING access to his user account and if SSG (b)(6)(b)(7)(C) had access to PFC MANNING's AKO, Gmail and Amazon accounts.

9. Evidence Disposition:

All evidence was placed into the evidence room of this office.

Report Prepared By:

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

Forensic Examiner

Report Approved By:

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

Special Agent-in-Charge



Forensic Report for Supply Annex NIPRNET computer



10. Attachments:

Attachment A, Enclosure 1 (PGP encrypted email - *Second Attempt.txt*)

Attachment B, Enclosure 1 (*blah.txt* - GAL extract from (b)(6)(b)(7)(C) My Documents folder)

Attachment C, Enclosure 1 (*blah.txt* - GAL extract, MD5-2231a1f4abbfcc02ca656a1625804bd7)

Attachment D, Enclosure 1 (*blah.txt* - GAL extract, MD5-316cd22b96ca20d4ae898f65280b0e2a)

Attachment E, Enclosure 1 (*blah.txt* - GAL extract, MD5-ab738fef80f667e0f4a265a37dfbf967 and *blah.zip*, MD5-f47456b90f199b0eeef59d4ebd1a76fe)

Attachment F, Enclosure 1 (*blah.txt* - GAL extract, MD5-2dd61d43dcd1200a289b95c78a43ff86 and *blah.zip*, MD5-30f1b75288516fd1ab988a203fc2dc75)

Attachment G, Enclosure 1 (*tmp.txt* - GAL Extract)

Attachment H, Enclosure 1 (*tmp.pdf* - Scanned documents related to PFC MANNING's Article 15)

Attachment I, Enclosure 1 (Internet history for the *bradley.manning* user account)

Attachment J, Enclosure 1 (Internet history for the (b)(6)(b)(7)(C) user account)

Attachment K, Enclosure 1 (Web pages from the *bradley.manning* user account)

Attachment L, Enclosure 1 (Web pages from the (b)(6)(b)(7)(C) user account)

Attachment M, Enclosure 1 (Timeline of events for the Supply Annex Computer, MM/DD/YYYY format)

Exhibit(s) 429

Page(s) 002751 thru 009944 withheld.

5 U.S.C. § 552(b)(6), (b)(7)(C)
Third Party Information
Not Reasonably Segregable

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 2 PAGES

DETAILS

Imaging:

Between 1000 and 1100, 4 Oct 10, SAC (b)(6)(b)(7)(C) created an EnCase digital forensic image of the US Army computer assigned the Internet Protocol (IP) address of 148.17.172.115 and computer name S2D10MTNBDE8133, recorded on Item #3, Evidence/Property Custody Document (EPCD), Document Number (DN) 147-10.

Hard Drive Make	Hitachi
Hard Drive Model	HTS721010G9SA00
Hard Drive Serial Number	MPC2N7Y0J9JMRL
Image Type	EnCase
Acquisition MD5	cfb89bafd9ca87c0cc6254ab30ef91f2
Verification MD5	cfb89bafd9ca87c0cc6254ab30ef91f2
Acquisition SHA1	f1fe31c34c30edb60879891982db422fea808a
Verification SHA1	f1fe31c34c30edb60879891982db422fea808a

Between 1100 and 1200, 4 Oct 10, SAC (b)(6)(b)(7)(C) created an EnCase digital forensic image of the US Army computer assigned the Internet Protocol (IP) address of 22.225.28.54 and computer name CPOFBDE66DC, recorded on the Item #2, EPCD, DN 147-10.

Hard Drive Make	Hitachi
Hard Drive Model	Unknown
Hard Drive Serial Number	070714DP1D00DGG08K6G
Image Type	EnCase
Acquisition MD5	3f0b0535507dfd2d539800118934b9a1
Verification MD5	3f0b0535507dfd2d539800118934b9a1
Acquisition SHA1	881270a483f96396c0537e34f2aaab281e66240e
Verification SHA1	881270a483f96396c0537e34f2aaab281e66240e

Between 1200 and 1230, 4 Oct 10, SAC (b)(6)(b)(7)(C) attempted to create an EnCase digital forensic image of the hard drive, recorded on the Item #1, EPCD, DN 147-10. However due to a hardware failure on the hard drive, no image was taken.

Hard Drive Make	Hitachi
Hard Drive Model	Unknown
Hard Drive Serial Number	K3HBYJDH
Image Type	EnCase
Acquisition MD5	N/A

TYPED AGENT'S NAME AND SEQUENCE NUMBER

ORGANIZATION

Digital Forensics and Research Branch
Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

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

DATE
4 Oct 10

EXHIBIT

430

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

CID FORM 94
1 FEB 77

FOR OFFICIAL USE ONLY
Law Enforcement Sensitive

Approve

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

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 2 OF 2 PAGES

DETAILS

Hard Drive Make	Hitachi
Verification MD5	N/A
Acquisition SHA1	N/A
Verification SHA1	N/A

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

TYPED AGENT'S NAME AND SEQUENCE NUMBER		ORGANIZATION
SAC (b)(6)(b)(7)(C), (b)(7)(E)		Digital Forensics and Research Branch Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C)	DATE 4 Oct 10	EXHIBIT 430

CID FORM 94
1 FEB 77FOR OFFICIAL USE ONLY
Law Enforcement SensitiveApproved (b)(6)(b)(7)(C)
0

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361

ROI: 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

Imaging:

Between 0822 and 0824, 27 Oct 10, SAC (b)(6)(b)(7)(C) created an EnCase digital forensic image of the Compact Disc (CD), recorded on Item #1, Evidence/Property Custody Document (EPCD), Document Number (DN) 153-10.

Item Description	CD
Image Type	EnCase
Acquisition MD5	31132753dd762dca2a8dd186243a398d
Verification MD5	31132753dd762dca2a8dd186243a398d

Between 0825 and 0830, 27 Oct 10, SAC (b)(6)(b)(7)(C) created an EnCase digital forensic image of the Digital Video Disc (DVD), recorded on Item #1, Evidence/Property Custody Document (EPCD), Document Number (DN) 154-10.

Item Description	DVD
Image Type	EnCase
Acquisition MD5	bee4b292a10ed457212f611a2c74cca0
Verification MD5	bee4b292a10ed457212f611a2c74cca0

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

TYPED AGENT'S NAME AND SEQUENCE NUMBER

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

ORGANIZATION

Digital Forensics and Research Branch
Computer Crime Investigative Unit
U.S. Army CID, Fort Belvoir, VA 22060

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

DATE

27 Oct 10

EXHIBIT

431

CID FORM 94

1 FEB 77

FOR OFFICIAL USE ONLY

Law Enforcement Sensitive

(b)(6)(b)(7)(C)
Approved: _____



DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATION UNIT
DIGITAL FORENSICS AND RESEARCH BRANCH
9805 LOWEN RD
FORT BELVOIR, VA 22060-5536

REPLY TO
ATTENTION OF

CISA-CCI-DF

30 Oct 2010

1. **Case Number:** CAF # 0028-10-CID361 / ROI # 0028-10-CID221-10117
2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA
3. **Date of Report:** 30 Oct 2010
4. **Examiner:** Mr. (b)(6)(b)(7)(C)
5. **Summary of Analysis:** The three NetApp arrays and domain controllers were reassembled into a working network by members of the 10th Mountain Division (10th Mtn Div) S-6 staff and inspected by the examiner for the presence of shadow copies or any other pertinent information. The items examined provided no evidentiary value.

For Official Use Only
Law Enforcement Sensitive

EXHIBIT 432
009948

Table of Contents

1.	CASE NUMBER.....	3
2.	INVESTIGATING OFFICE.....	3
3.	DATE OF REPORT	3
4.	EXAMINER	3
5.	ANALYSIS	3
5.1	EXAMINATION OF THE NETAPP DRIVE ARRAYS.....	3
5.1.1	<i>Voucher information</i>	3
5.1.2	<i>Pertinent Information</i>	3
6.	SUMMARY OF EXAMINATION.....	4
7.	EVIDENCE DISPOSITION:.....	4

1. Case Number

CAF # 0028-10-CID361 / ROI # 0028-10-CID221-10117

2. Investigating Office

Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA

3. Date of Report

30 Oct 2010

4. Examiner

Mr. (b)(6)(b)(7)(C)

5. Analysis

5.1 Examination of the NetApp drive arrays and Domain Controllers*5.1.1 Voucher information*

NetApp Disk Chassis:

Item 1, Evidence/Property Custody Document (EPCD), Document Numbers (DN)
131-10

Item 1, EPCD DN 133-10

Item 1, EPCD DN 145-10

Two Sun and one Dell servers hard drives:

Items 2 – 4, EPCD DN 145-10

5.1.2 Pertinent Information

The three NetApp arrays were reassembled by members of the 10th Mtn Div S-6 staff and inspected by the examiner for the presence of shadow copies which were not found. The items in examined provided no evidentiary value.

6. Summary of Examination

The three NetApp arrays and domain controllers were reassembled into a working network by members of the 10th Mtn Div S-6 staff and inspected by the examiner for the presence of shadow copies or any other pertinent information. The items examined provided no evidentiary value.

7. Evidence Disposition:

All evidence was placed into the evidence room of this office.

Report Prepared By:

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

Forensic Examiner

Approved By:

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

Special Agent in Charge

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER

CAF: 0028-10-CID361
ROI: 0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS**Examination Date and Contents:**

On 8 Nov 10, Mr. (b)(6)(b)(7)(C) forensic examiner, this office, conducted a preliminary investigation of forensic image of one hard disk drive (HDD), belonging to PFC Bradley MANNING and recorded on DA Form 4137, Voucher Number 086-10. All times shown in this preliminary report are in relation to Universal Time (UT) unless otherwise noted.

Pertinent Information:

Review of the hard disk drive identified the computer was likely installed on 2 Feb 10 and used IP address 192.168.1.25, a non-routable address. The computer had files modified only between 2 Feb 10 and 10 Feb 10 indicating the use only during this period. Connections were identified via Secure Shell (SSH) from another computer connected to the same local area network (LAN) using IP address 192.168.1.3. The Rivest, Shamir, Adleman (RSA) key used by the SSH services matches the SSH key identified on PFC MANNING's MacBookPro laptop.

Only minimal log information was available during the timeframe noted. No other information of interest was identified

Non-Lead Observations:

Internet Protocol (IP) address 192.168.1.3 was likely used by PFC MANNING's MacBook Pro.

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

TYPED AGENT'S NAME AND SEQUENCE NUMBER Mr. (b)(6)(b)(7)(C)		ORGANIZATION Digital Forensics and Research Branch Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C)	DATE 8 Nov 10	EXHIBIT 433



DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
COMPUTER CRIME INVESTIGATION UNIT
DIGITAL FORENSICS AND RESEARCH BRANCH
9805 LOWEN RD
FORT BELVOIR, VA 22060-5536

REPLY TO
ATTENTION OF

CISA-CCI-DF

12 Nov 10

1. **Case Number:** CAF 0028-10-CID361/ROI 0028-10-CID221-10117
2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA
3. **Date of Report:** 12 Nov 10
4. **Examiner:** SAC (b)(6)(b)(7)(C), (b) (7)(E)
5. **Summary of Analysis:** Item 1, Evidence/Property Custody Document (EPCD), Document Number (DN) 165-10, consisting of various log files from various Combined Information Data Network Exchange (CIDNE) database servers from Iraq was of no evidentiary value.

For Official Use Only
Law Enforcement Sensitive

EXHIBIT 434
009953



Forensic Report for DN 165-10, Item 1

Table of Contents



1.	(U) CASE NUMBER.....	3
2.	(U) INVESTIGATING OFFICE	3
3.	(U) DATE OF REPORT.....	3
4.	(U) EXAMINER.....	3
5.	(U) ANALYSIS.....	3
5.1	(U) EXAMINATION OF THE COMPACT DISCS	3
5.1.1	(U) Voucher information.....	3
5.1.2	(U) Pertinent Information.....	3
6.	(U) SUMMARY OF EXAMINATION	3
7.	(U) EVIDENCE DISPOSITION:	3

**1. Case Number**

CAF 0028-10-CID361/ROI 0028-10-CID221-10117

2. Investigating Office

Washington Metro Resident Agency, Computer Crime Investigative Unit, Fort Belvoir, VA

3. Date of Report

12 Nov 10

4. Examiner

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

5. Analysis**5.1 Examination of the Compact Discs****5.1.1 Voucher information**

Item 1, EPCD, DN 165-10, consisting of various log files from various CIDNE database servers in Iraq.

5.1.2 Pertinent Information

The item in question was not of evidentiary value.

6. Summary of Examination

The item in question was of no evidentiary value.

7. Evidence Disposition:

All evidence was placed into the evidence room of this office.

Report Prepared/ Approved By:

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

Special Agent-in-Charge