COMMANDER'S REPORT OF DISCIPLINARY OR ADMINISTRATIVE ACTION

For use of this form, see AR 190-45; the proponent agency is the Office of the Provost Marshal General.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10 USC Section 301; Title 5 USC Section 2951; E.O. 9397 dated November 22, 1943.

PRINCIPAL PURPOSE: To provide commanders and law enforcement officials with means by which information may be accurately identified.

ROUTINE USES: Your Social Security Number is used as an additional/alternate means of identification to facilitate filing and retrieval.

DISCLOSURE: Disclosure of your Social Security Number is voluntary.

1. CONTROL INFORMATION

Thru:	USACRC Number: 0160-2010-CID899-14463-5Y2P2
To: CDR, US Army Military District of Washington Ft Lesley J. McNair Washington, D.C. 20319	MP Report Number: N/A
	Sub-Installation: AE09342DC
Referred By: SAC, CID Office: HQUSACIDC (b)(6)(b)(7)(C)	Referral Date *(YYYYMMDD)* : 20100623 / Suspense Date *(YYYYMMDD)* : 20100807

The first Lieutenant Colonel in the chain of command is responsible and accountable for completing DA Form 4833 with support documentation (copies of Article 15s, court-martial orders, reprimands, etc) for all USACIDC investigations. The unit and brigade commander or their equivalent will also receive a copy of the DA Form 4833 for all USACIDC investigations.

Company, troop, and battery level commanders are responsible and accountable for completing DA Form 4833 with supporting documentation in all cases investigated by MPI, civilian detectives employed by the Department of the Army, and the PMO. Accurate and complete DA 4833 disposition reports are required to meet installation, command, HQDA, DOD, and federal statutory reporting requirements. The data is used to identify crime trends, establish command programs in law enforcement and other activities, and to ensure that resources are made available to support commanders who must address issues of soldier and family member indiscipline.

In court-martial cases, a conviction of an offense at court-martial may be for a different, or lesser included offense. List the offense for which the individual was convicted at court-martial in the remarks section. Provost Marshals must enter the "MP Report Number" (Block-1) for all cases referred to commanders. "Sub-Installation" (Block-1) is used to enter report number from a civilian law enforcement agency police report. Other information on the civilian law enforcement agency (e.g. civilian law enforcement agency address) may be anterad in the remarks section.

2. OFFENDER INFORMATION

Last Name: Manning	Cadency:	
First Name: Bradley	Grade: E-3 U.S. Army (PFC)	
Middle Name: Edward	SSN: (b)(6)(b)(7)(C)	Date of Birth: *(YYYYMMDD)* : (b)(6)(b)(7)(C)

3. REFERRAL INFORMATION

Commander Decision Date: 6/23/2010

No.	Offense	Basis	Date	Sexual Harassment	Action Taken	Reason
1	Espionage [5Y2P2]	UCMJ Article 106	20090830	☐ Yes ☑ No	☑ Yes ☐ No	Accepted
2	Disclosure of Classified Information [8P1]	Non-UCMJ Article 134	20090830	☐ Yes ☑ No	☑ Yes ☐ No	Accepted
3	Gathering, Transmitting or Losing Defense Information [8P3]	Non-UCMJ Article 134	20090830	☐ Yes ☑ No	☑ Yes ☐ No	Accepted
				☐ Yes ☐ No	☐ Yes ☐ No	

3. REFERRAL INFORMATION *(Continued)*						
No.	Offense	Basis	Date	Sexual Harassment	Action Taken	Reason
				☐ Yes ☐ No	☐ Yes ☐ No	
				☐ Yes ☐ No	☐ Yes ☐ No	
				☐ Yes ☐ No	☐ Yes ☐ No	
				☐ Yes ☐ No	☐ Yes ☐ No	
				☐ Yes ☐ No	☐ Yes ☐ No	
				☐ Yes ☐ No	☐ Yes ☐ No	

NOTE: For each offense marked NO for action taken, you must supply a reason.

If you selected "Yes" for any offense, continue to "Action Taken" (Block-4). If you selected "No" for ALL offenses, go directly to "Commander's Remarks" (Block-10), sign, date, and return the form to the agent specified in "Referred By" (Block-1).

4. ACTION TAKEN

☐ **Administrative**
Non-Adverse Referrals
Adverse Personnel Actions

☐ **Non-Judicial (Article 15)**
(see details below)

☑ **Judicial**
Court Martial or Civilian Criminal

Non-Judicial Punishment Authority *(select one)* **:**

☐ Summarized
☐ Company Grade
☐ Field Grade
☐ Principal Assistant
☐ GCMCA Imposed
☐ General Officer Imposed

Judicial Punishment Authority *(select one)* **:**

☐ Summary Court Martial
☐ Special Court Martial
☐ Civilian Criminal/Magistrate
☑ General Court Martial

5. NJP/Court-Martial/Civilian Criminal Court Proceeding Outcome

No.	Charged Offense	Plea	Finding Offense	Trial Finding
1	Espionage [5Y2P2]	N	Espionage [5Y2P2]	G
2	Disclosure of Classified Information [8P1] [8P1]	N	Disclosure of Classified Information [8P1] [8P1]	G
3	Gathering, Transmitting or Losing Defense Information [8P3] [8P3]	N	Gathering, Transmitting or Losing Defense Information [8P3] [8P3]	G

PLEA: G=Guilty, C=No Contest, N=Not Guilty, D=Pre-Trial Diversion, TRIAL FINDING: DCV=Dismissed (Civil), DCR=Dismissed (Criminal), P=Finding for Plaintiff, F=Finding for Respondent, G=Guilty, C=No Contest, N=Not Guilty, S=Settlement

5. NJP/Court-Martial/Civilian Criminal Court Proceeding Outcome *(Continued)*				
No.	Charged Offense	Plea	Finding Offense	Trial Finding

PLEA: G=Guilty, C=No Contest, N=Not Guilty, D=Pre-Trial Diversion, **TRIAL FINDING:** DCV=Dismissed (Civil), DCR=Dismissed (Criminal), P=Finding for Plaintiff, F=Finding for Respondent, G=Guilty, C=No Contest, N=Not Guilty, S=Settlement

6. ADMINISTRATIVE ACTIONS

Non-Adverse:

Agency	Date Referred *(YYYYMMDD)*	Date Responded *(YYYYMMDD)*	Date Imposed *(YYYYMMDD)*	Type of Action	Oral	Written	
						Local	OMPF
Family Advocacy				Counseling/Concern	☐	☐	☐
Drug/Alcohol Abuse				Reprimand	☐	☐	☐
Special Referral				Censure	☐	☐	☐
Equal Opportunity				Admonition	☐	☐	☐
Legal Office							
Mental Health							
Relief Agency							

Adverse:

Date Imposed *(YYYYMMDD)*	Description		
	Withholding of Privileges		
	Adverse Performance Evaluation (OER/NCOER/Academic Report)		
	Relief for Cause (OER/NCOER)		
	Mandatory Reassignment		
	Transfer (such as rehabilitative)		
	Adverse Record Entry - Flag		
	Denial of Reenlistment or Continued Service		
	Withholding of Promotion		
	Delay of Promotion		
	Promotion Revocation		
	Clearance Revocation		
	Control Roster (downgrade of clearance, PRP reclassification)		
	Resignation		
	Retirement		
	Retirement at Lower Grade	From:	
		To:	
	Transfer to Inactive Reserve		
	Military Occupational Specialty Reclassification		
	Debarment	Duration: ☐ Days ☐ Months ☐ Years	

6.	ADMINISTRATIVE ACTIONS *(Continued)*							
Adverse: *(Continued)*								
Date Imposed *(YYYYMMDD)*	**Description**							
	Job Termination							
	Job Suspension	Duration:	☐ Days	☐ Months	☐ Years			
	Leave Without Pay	Duration:	☐ Days	☐ Months	☐ Years			
	Loss of Warrant							
	Voluntary Disclosure							
	Restitution (to US Government)	Amount:						
	Restitution (to third party Non-US Government)	Amount:						
	Civil-Civil Action Initiation							
	Other (return to states, etc.)							
	Contract Suspension	Duration:	☐ Days	☐ Months	☐ Years			
	Contract Termination							
	Cost Adjustment	Amount:						
	Bid Rejection							
	Recoupment	Amount:						
	Denial of Continuation							
	Other Contract Action							

7.	DETAILS OF ADMINISTRATIVE SEPARATION	
Date Imposed *(YYYYMMDD)* :	Regulation:	Chapter:
Characterization:		Effective Date *(YYYYMMDD)*:

NOTE: Proceed to Commander's Remarks (Block-10) if you chose Administrative Action.

8.	NON-JUDICIAL/JUDICIAL SANCTIONS								
Date Adjudged *(YYYYMMDD)*	**Sanction**								
	Fine	Amount:							
	Forfeiture	Amount:	Duration:	☐ Days	☐ Months				
	Extra Duty	Days:							
	Restriction	Days:							
	Correctional Custody	Days:							
20130821	Confinement	Duration: 35	☐ Days	☐ Months	☑ Years	☐ Life			
	Bad Conduct Discharge	Effective Date:							
8/21/2013	Dishonorable Discharge	Effective Date:	8/21/2013						
20130821	Reduction in Grade	From:	Private First Class (PFC)						
		To:	Private (E1) (PVT)						
	Probation	Duration:	☐ Days	☐ Months	☐ Years				
	Special Assignment	Duration:	☐ Days	☐ Months	☐ Years				
20130821	Total Forfeiture (all pay/allowance)	Duration: 35	☐ Days	☐ Months	☑ Years	☐ Life			
	Death								
	Civil Recovery	Amount:							
	Civil Award	Amount:							

9.	SUSPENDED SANCTIONS	
Were Any Sanctions Suspended? ☐ Yes ☑ No		
NOTE: If no sanctions were suspended, proceed to "Commander's Remarks" (Block-10).		
Suspended Sanction	**Suspended Sanction Information**	
Fine	Date Suspended:	Suspension Duration:
	Suspended Portion US$:	
	Suspension Conditions:	
Forfeiture	Date Suspended:	Suspension Duration:
	Suspended Portion US$:	Suspended Portion Time:
	Suspension Conditions:	
Extra Duty	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Restriction	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Correctional Custody	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Confinement	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Reduction in Grade	Date Suspended:	Suspension Duration:
	Suspension Conditions:	
Probation	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Special Assignment	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Total Forfeiture	Date Suspended:	Suspension Duration:
	Suspended Portion Time:	
	Suspension Conditions:	
Civil Recovery	Date Suspended:	Suspension Duration:
	Suspended Portion US$:	
	Suspension Conditions:	
Civil Award	Date Suspended:	Suspension Duration:
	Suspended Portion US$:	
	Suspension Conditions:	

10.	Commander's Remarks

Data entered by HOUSACIDC on 30 Aug 13, based on DD Form 2707-1 (Department of Defense Report of Result of Trial), dated 21 Aug 13 and signed by MAJ (b)(6)(b)(7)(C) Trial Counsel.

Note that subject has 1181 days of pre-trial credit and another 112 days of credit as ordered by the trial judge, for a total of 1293 credit to his sentence.

USASCRC Number: 0160-2010-CID899-14463-5Y2P2	Sanction: AI 2013/08/21

11.	COMMANDING OFFICER

Was a DNA sample collected from the offender? ☑ Yes ☐ No

Name: LTG (b)(6)(b)(7)(C)	Grade: LTG
AKO e-Mail Address:	
Signature:	Signature Date *(YYYYMMDD)* : 20130821

DEPARTMENT OF THE ARMY
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
CCIU - Washington Metro Office
27130 Telegraph Road, Quantico, VA 22134-2253

26 Jun 2014

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: CID REPORT OF INVESTIGATION - FINAL/SSI/JOINT - 0028-2010-CID221-10117 - 5Y2P2 / 5Y2P4 / 7F1A1 / 8P2 / 5Y2B5 / 9G2F

DATES/TIMES/LOCATIONS OF OCCURRENCES:
1. 01 NOV 2009, 0001 - 27 MAY 2010, 2146; VARIOUS LOCATIONS, FORWARD OPERATING BASE (FOB) HAMMER, IRAQ, AE 09308

2. 23 JAN 2010, 0001 - 11 FEB 2010, 0000; VARIOUS LOCATIONS IN OR NEAR, ROCKVILLE, MD

DATE/TIME REPORTED: 10 JUN 2010, 1247

INVESTIGATED BY:
SA (b)(6)(b)(7)(C), (b) (7)(E)
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA
SA

SUBJECT:

1. MANNING, BRADLEY EDWARD; PFC; (b)(6)(b)(7)(C) (DOB); (POB); MALE; WHITE; HEADQUARTERS AND HEADQUARTERS COMPANY (HHC), 2ND BRIGADE COMBAT TEAM (BCT), 10TH MOUNTAIN DIVISION (MTN DIV), FOB HAMMER, IRAQ, ARMED FORCES AFRICA, CANADA, EUROPE & MIDDLE EAST 09308; CT ; [GATHERING, TRANSMITTING OR LOSING DEFENSE INFORMATION (18 USC § 793(E))], [THEFT OF PUBLIC MONEY, PROPERTY OR RECORDS (18 USC § 641)], [AIDING THE ENEMY (ARTICLE 104, UCMJ)], [EXCEEDING AUTHORIZED ACCESS TO A U.S. GOVERNMENT COMPUTER (18 USC § 1030(A)(1))], [FAILURE TO OBEY ORDER OR REGULATION (ARTICLE 92, UCMJ)]

VICTIM:

1. U.S. GOVERNMENT; [GATHERING, TRANSMITTING OR LOSING DEFENSE INFORMATION (18 USC § 793(E))], [THEFT OF PUBLIC MONEY, PROPERTY OR RECORDS (18 USC § 641)], [AIDING THE ENEMY (ARTICLE 104, UCMJ)], [EXCEEDING AUTHORIZED ACCESS TO A U.S. GOVERNMENT COMPUTER (18 USC § 1030(A)(1))], [FAILURE TO OBEY ORDER OR REGULATION (ARTICLE 92, UCMJ)]

INVESTIGATIVE SUMMARY:

This investigation was initiated upon receipt of information by this office on 25 May 10, that a Soldier stationed in Iraq claimed via online chat sessions that he had disclosed classified U.S. Government information to the operator(s) of the website "WikiLeaks" (http://www.wikileaks.org), which the operator(s) subsequently posted on the publicly available WikiLeaks website. The Soldier was subsequently identified as PFC MANNING, who served as an Intelligence Analyst and held a Top Secret security clearance at the time of the incident.

A joint investigation with Federal Bureau of Investigation (FBI) and the U.S. Department of State Diplomatic Security Service (DSS) determined probable cause to believe that between 1 Nov 09 and 27 May 10, PFC MANNING, while assigned to FOB Hammer, Iraq, and while on leave from Iraq in the United States, committed the offenses of Aiding the Enemy; Failure to Obey Order or Regulation; Gathering, Transmitting or Losing Defense Information; Theft of Public Money, Property or Records; and Exceeding Authorized Access to a U.S. Government Computer, when he exceeded his authorized access to various classified databases and network file systems, the property of various U.S. Government departments and agencies; knowingly gathered documents, communications, videos, and other records PFC MANNING knew or believed to be classified information at the Secret and Confidential level; and then without authorization, wrongfully disclosed this classified information to the operator(s) of "WikiLeaks" - knowing this classified information would be released to the public and accessible to enemies with which the U.S. Government was engaged in armed conflict.

The specific classified systems and information PFC MANNING accessed included the: Net-Centric Diplomacy (NCD) database, property of the U.S. State Department, wherein PFC MANNING gathered and wrongfully disclosed approximately 251,287 U.S. State Department Diplomatic Cables, many of these cables classified Secret and Confidential; the Combined Information Data Network Exchange (CIDNE) database, property of the Department of Defense, wherein PFC MANNING gathered and wrongfully disclosed approximately 391,883 documents related to combat operations in Iraq, and approximately 91,911 documents related to combat operations in Afghanistan, many of these documents classified Secret and Confidential; a video depicting a July 2007 combat operation in Baghdad, Iraq, and an encrypted video depicting a May 2009 combat operation in Gharani, Afghanistan, property of the U.S. Central Command; approximately 779 records pertaining to detainees housed at the U.S. Naval Station Guantanamo Bay, Cuba, classified at the Secret level, property of U.S. Southern Command (SOUTHCOM); a classified document from the U.S. Army Intelligence and Security Command (INSCOM), classified at the Secret level, property of the U.S. Army; as well as other miscellaneous documents which were classified and property of a U.S. Intelligence Agency. There was further probable cause to believe PFC MANNING attempted to exceed his authorized access to U.S. Central Command email systems in order to gather the Global Address List (GAL), containing the names and other personal information of U.S. service members, contractors, and civilians assigned in Iraq, with the intent of disclosing this information to the operator(s) of the WikiLeaks website.

On 1 Mar 11, 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, (b) (5)
(b) (5) PFC MANNING
(b) (5)

STATUTES:

Article 92, UCMJ: Failure to Obey Order or Regulation
Article 104, UCMJ: Aiding the Enemy
18 USC § 641: Theft of Public Money, Property or Records
18 USC § 793(e): Gathering, Transmitting or Losing Defense Information
18 USC § 1030(a)(1): Exceeding Authorized Access to a U.S. Government Computer

EXHIBITS:

ATTACHED:

1. Agent's Investigation Report (AIR) of SA (b)(6)(b)(7)(C) 2 Jun 10, detailing the receipt of the initial complaint, and coordination with CPT (b)(6)(b)(7)(C)

2. AIR of SA (b)(6)(b)(7)(C) 5 Jun 10, detailing the initial complaint; coordination with Military Magistrate, Office of the Staff Judge Advocate, FOB Hammer Post Office, and Netgate Internet Services; canvass interviews; Rights Advisal of PFC MANNING; interviews of SSG (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) PFC (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) and PFC (b)(6)(b)(7)(C) crime scene examinations; collection of evidence; Search and Seizure Authorizations; and Commander's Authorization to Search.

3. Department of the Army (DA) Form 3745, Search and Seizure Authorization, dated 27 May 10, with supporting affidavit.

4. Canvass Interview Worksheet, dated 27 May 10.

5. Non-Waiver Certificate of PFC MANNING, dated 27 May 10.

6. Article 15 Packet, pertaining to PFC MANNING, dated 24 May 10.

7. CID Form 98-R, Commander's Authorization to Search, dated 27 May 10.

8. Canvass Interview Worksheet, dated 28 May 10.

9. CID Form 87-R-E, Consent to Search from SSG (b)(6)(b)(7)(C) dated 28 May 10.

10. Consent to Search Computer/Electronic Equipment from SSG (b)(6)(b)(7)(C) dated 28 May 10.

11. Consent to Search Computer/Electronic Equipment from CPT (b)(6)(b)(7)(C) dated 28 May 10.

12. DA Form 3745, Search and Seizure Authorization, dated 28 May 10, with supporting affidavit.

13. Sworn Statement of SPC (b)(6)(b)(7)(C), dated 28 May 10.

14. Sworn Statement of SPC (b)(6)(b)(7)(C) dated 28 May 10.

15. Sworn Statement of SSG (b)(6)(b)(7)(C), dated 28 May 10.

16. CID Form 98-R, Commander's Authorization to Search, dated 28 May 10.

17. Sworn Statement of PFC (b)(6)(b)(7)(C), dated 28 May 10.

18. Affidavit supporting Pre-Trial Confinement of PFC MANNING, dated 29 May 10.

19. DA Form 3745-E, Search and Seizure Authorization, dated 31 May 10.

20. CID Form 98-R, Commander's Authorization to Search, dated 31 May 10, with DA Form 3744, Affidavit Supporting Request For Authorization To Search And Seize Or Apprehend, dated 28 May 10.

21. DA Form 3745-E, Search and Seizure Authorization, dated 5 Jun 10, with supporting affidavit.

22. AIR of SA (b)(6)(b)(7)(C) 27 May 10, detailing the crime scene examination of the Sensitive Compartmented Information Facility (SCIF).

23. Crime Scene Sketch, 27 May 10, prepared by SA (b)(6)(b)(7)(C)

24. Photographic packet depicting the Sensitive Compartmented Information Facility (SCIF).

25. AIR of SA (b)(6)(b)(7)(C) 28 May 10, detailing the crime scene examination of PFC MANNING's living area.

26. Crime Scene Sketch, 28 May 10, prepared by SA (b)(6)(b)(7)(C)

27. Photographic packet depicting PFC MANNING's living area.

28. Compact Disc (CD) containing all photographic images of crime scenes. (USACRC and File Copy Only)

29. U.S. Army Military Intelligence (Army MI) Memorandum, LCCN: BMB-10-036 (Classified ~~SECRET//NOFORN~~), documenting the receipt of initial reported allegation of wrongful disclosure of classified information, interviews of Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) initial notification of CID, records checks of PFC MANNING, receipt of chat logs from Mr. (b)(6)(b)(7)(C) and receipt of information from Mr. (b)(6)(b)(7)(C) dated 30 May 10.

30. DA Form 2823, Sworn Statement of SA (b)(6)(b)(7)(C) dated 7 Jun 10.

31. DA Form 2823, Sworn Statement of SA (b)(6)(b)(7)(C) dated 8 Jun 10.

32. DA Form 2823, Sworn Statement of SA (b)(6)(b)(7)(C) dated 8 Jun 10.

33. DA Form 2823, Sworn Statement of Mr. (b)(6)(b)(7)(C) dated 8 Jun 10.

34. AIR of SA (b)(6)(b)(7)(C) 5 Jun 10, detailing the forensic imaging of numerous items of

digital media, the property of PFC MANNING, SSG (b)(6)(b)(7)(C) and the U.S. Army; coordination with CPT (b)(6)(b)(7)(C) MAJ (b)(6)(b)(7)(C) and CPT (b)(6)(b)(7)(C) and the collection forensic images as evidence.

35. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR-PI-ACICA-10-009-001 (Classified ~~SECRET//NOFORN~~), documenting the interview of SPC (b)(6)(b)(7)(C) dated 14 Jun 10.

36. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR-PI-ACICA-10-009-002 (Classified ~~SECRET//NOFORN~~), documenting the interview of MSG (b)(6)(b)(7)(C) dated 14 Jun 10.

37. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR-PI-ACICA-10-009-003 (Classified ~~SECRET//NOFORN~~), documenting the interview of 1LT (b)(6)(b)(7)(C) dated 14 Jun 10.

38. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR-PI-ACICA-10-009-004 (Classified ~~CONFIDENTIAL//NOFORN~~), documenting the review of PFC MANNING's counseling records, dated 14 Jun 10.

39. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-005 (Classified ~~CONFIDENTIAL//NOFORN~~), documenting the review of PFC MANNING's personnel records, dated 14 Jun 10.

40. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-006 (Classified ~~SECRET//NOFORN~~), documenting the review of PFC MANNING's Army Leave and Earning Statement (LES), dated 14 Jun 10.

41. Intelligence Information Report, IIR 5 332 0069 10 (Classified ~~SECRET//NOFORN~~), reporting activities of WikiLeaks members and associates, dated 22 Apr 10.

42. Memorandum from Cyber CounterIntelligence Activity, 10-1303-PI-ACICA-10-009 (Classified ~~SECRET//NOFORN~~), documenting classification review of Chat-Log4 seized from a Macintosh Laptop Computer, the property of PFC MANNING, dated 15 Jun 10.

43. AIR of SA (b)(6)(b)(7)(C) 16 Jun 10, detailing USACRC name check results related to PFC MANNING and Mr. (b)(6)(b)(7)(C) consent to search documents executed by Mr. (b)(6)(b)(7)(C) collection of evidence from Mr. (b)(6)(b)(7)(C) interviews of Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) research related to the WikiLeaks website; National Crime Information Center (NCIC) name check results related to Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and PFC MANNING; and coordination with the U.S. Treasury Department, U.S. Department of State, CPT

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

44. CID Form 87-R-E, Consent to Search from Mr. (b)(6)(b)(7)(C) 12 Jun 10, authorizing a search of his Fujitsu hard disk drive taken from Mr. (b)(6)(b)(7)(C) Lenovo laptop computer.

45. CID Form 87-R-E, Consent to Search from Mr. (b)(6)(b)(7)(C) 12 Jun 10, authorizing a search of emails sent to USACIDC Investigators by Mr. (b)(6)(b)(7)(C)

46. CID Form 87-R-E, Consent to Search from Mr. (b)(6)(b)(7)(C) 12 Jun 10, authorizing a search of Mr. (b)(6)(b)(7)(C) HP laptop computer.

47. DA Form 2823, Sworn Statement of Mr. (b)(6)(b)(7)(C) dated 13 Jun 10.

48. EagleCash Transaction Records of PFC MANNING, dated 12 Oct 09 to 29 May 10.

49. Memorandum from Cyber CounterIntelligence Activity, 10-1303-PI-ACICA-10-009 (Classified ~~SECRET//NOFORN~~), documenting classification reviews of Chat-Log1, 3 pages beginning with a timestamp 7:18:03 AM, between Mr. (b)(6)(b)(7)(C) and PFC MANNING, 17 May 10 to 22 May 10, and associated documentation, dated 16 Jun 10.

50. Memorandum from Cyber CounterIntelligence Activity, 10-1303-PI-ACICA-10-009 (Classified ~~SECRET//NOFORN~~), documenting classification reviews of Chat-Log2, 6 pages beginning with a timestamp 10:13:20 AM, between Mr. (b)(6)(b)(7)(C) and PFC MANNING, 17 May 10 to 22 May 10, and associated documentation, dated 16 Jun 10.

51. Memorandum from Cyber CounterIntelligence Activity, 10-1303-PI-ACICA-10-009 (Classified ~~SECRET//NOFORN~~), documenting classification reviews of Chat-Log3, 10 pages beginning with a timestamp 12:24:04 PM, between Mr. (b)(6)(b)(7)(C) and PFC MANNING, 17 May 10 to 22 May 10, and associated documentation, dated 16 Jun 10.

52. AIR of SA (b)(6)(b)(7)(C) 17 Jun 10, documenting collection of evidence.

53. AIR of SA (b)(6)(b)(7)(C) 17 Jun 10, detailing Search and Seizure Authorization, and coordination with CPT (b)(6)(b)(7)(C) and the Camp Liberty Post Office.

54. DA Form 3745-E, Search and Seizure Authorization, dated 14 Jun 10.

55. DA Form 3745, Search and Seizure Authorization, with DA Form 3744, Affidavit Supporting Request For Authorization To Search And Seize or Apprehend, dated 14 Jun 10.

56. AIR of SA (b)(6)(b)(7)(C) 19 Jun 10, detailing the coordination with the Office of the Director for National Intelligence; collection of evidence; interviews of Mr. (b)(6)(b)(7)(C), Mrs. (b)(6)(b)(7)(C)

Ms. (b)(6)(b)(7)(C), Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and Mrs. (b)(6)(b)(7)(C)

57. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-008 (Classified ~~SECRET//NOFORN~~), documenting the interview of SPC (b)(6)(b)(7)(C) dated 19 Jun 10.

58. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-009 (Classified ~~SECRET//NOFORN~~), documenting (b)(6)(b)(7)(C), (b) (7)(D) dated 19 Jun 10.

59. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-012 (Classified ~~SECRET//NOFORN~~), documenting the interview of SPC (b)(6)(b)(7)(C) dated 20 Jun 10.

60. AIR of SA (b)(6)(b)(7)(C) 21 Jun 10, detailing the coordination with PFC MANNING's rear detachment and Fort Drum Exchange Administrator; canvass interviews; and interview of SSG (b)(6)(b)(7)(C)

61. Canvass Interview Worksheet, dated 21 Jun 10.

62. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-010 (Classified ~~SECRET//NOFORN~~), documenting the interview of SPC (b)(6)(b)(7)(C) dated 22 Jun 10.

63. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-011 (Classified ~~SECRET//NOFORN~~), documenting the interview of SGT (b)(6)(b)(7)(C) dated 22 Jun 10.

64. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-013 (Classified ~~SECRET//NOFORN~~), documenting the review of PFC MANNING's 2nd BCT personnel packet, dated 25 Jun 10.

65. Intelligence Information Report, IIR 5 332 0083 10 (Classified ~~SECRET//NOFORN~~), reporting activities of WikiLeaks members and associates, dated 14 Jun 10.

66. AIR of SA (b)(6)(b)(7)(C) 14 Jun 10, detailing the forensic analysis and evidence collection of PFC MANNING's cellular telephone.

67. AIR of SA (b)(6)(b)(7)(C) 16 Jun 10, detailing the forensic examination of PFC MANNING's camera.

68. AIR of SA (b)(6)(b)(7)(C) 16 Jun 10, detailing the forensic examination of the computer of the computer assigned IP address 144.107.17.19.

69. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the forensic imaging of Mr. (b)(6)(b)(7)(C) computers.

70. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the forensic examination of SSG (b)(6)(b)(7)(C) computer.

71. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the forensic imaging of Mr. (b)(6)(b)(7)(C) thumb drives and subsequent forensic analysis.

72. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the forensic imaging of the wikileaks.org website.

73. AIR of SSA (b)(6)(b)(7)(C) 18 Jun 10, detailing the forensic imaging of a Fujitsu hard disk drive and a hard disk drive contained in an Hewlett Packard laptop computer, the property of Mr. (b)(6)(b)(7)(C)

74. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the interview of Mr. (b)(6)(b)(7)(C)

75. DODIG Subpoena, 2010233-10428, pertaining to the Facebook account "bradley.e.emanning@facebook.com".

76. AIR of SA (b)(6)(b)(7)(C) 23 Jun 10, detailing the request for Office of Personnel Management (OPM) records pertaining to the Security Clearance Background Investigation of PFC MANNING, and the receipt of these records.

77. OPM Provided Security Clearance Background Investigation documents related to PFC MANNING, dated 18 Jun 10.

78. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-018 (Classified ~~CONFIDENTIAL//NOFORN~~), documenting the interview of PFC (b)(6)(b)(7)(C) dated 27 Jun 10.

79. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-017 (Classified ~~CONFIDENTIAL//NOFORN~~), documenting the review of PFC MANNING's Army Enlistment Documents, dated 28 Jun 10.

80. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-019 (Classified ~~CONFIDENTIAL//NOFORN~~), documenting the interview of Mr. (b)(6)(b)(7)(C) dated 28 Jun 10.

81. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-024 (Classified ~~CONFIDENTIAL//NOFORN),~~ documenting the interview of MSG (b)(6)(b)(7)(C) dated 3 Jul 10.

82. Army Regulation (AR) 380-5 Preliminary Inquiry of the Compromise of Classified Information Report related to PFC MANNING, dated 4 Jul 10.

83. AIR of SA (b)(6)(b)(7)(C), 12 Jul 10, detailing the interview of Ms. (b)(6)(b)(7)(C)

84. AIR of SA (b)(6)(b)(7)(C) 13 Jul 10, detailing the interview of Mr. (b)(6)(b)(7)(C), Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) coordination with U.S. State Department; Search Warrant for PFC MANNING's Gmail account; collection of evidence; and Department of Defense Inspector General (DoDIG) subpoena results.

85. Federal Magistrate Search Warrant, 10-330-M-01 (UNDER SEAL), dated 21 Jun 10, and Search Warrant results. (USACRC and File Copy Only)

86. DoDIG Subpoena, 2010233-10427, dated 18 Jun 10, pertaining to the AOL Instant Messenger (AIM) account (b)(6)(b)(7)(C) and the subpoena results from AOL.

87. DoDIG Subpoena, 2010233-10431, dated 18 Jun 10, pertaining to the Hotmail account (b)(6)(b)(7)(C)@hotmail.co.uk, and the subpoena results from Microsoft Corporation.

88. DoDIG Subpoena, 2010233-10430, dated 18 Jun 10, pertaining to the Hotmail account (b)(6)(b)(7)(C)@hotmail.com, and the subpoena results from Microsoft Corporation.

89. DoDIG Subpoena, 2010233-10432, dated 18 Jun 10, pertaining to the Hotmail account (b)(6)(b)(7)(C) @hotmail.com, and the subpoena results from Microsoft Corporation.

90. DoDIG Subpoena, 2010233-10424, dated 18 Jun 10, pertaining to the AOL AIM account (b)(6)(b)(7)(C), and the subpoena results from AOL.

91. DoDIG Subpoena, 2010233-10425, dated 18 Jun 10, pertaining to the AOL AIM account (b)(6)(b)(7)(C), and the subpoena results from AOL.

92. DoDIG Subpoena, 2010233-10426, dated 18 Jun 10, pertaining to the AOL AIM account (b)(6)(b)(7)(C), and the subpoena results from AOL.

93. DoDIG Subpoena, 2010247-10457, dated 6 Jul 10, pertaining to the Skype accounts "bradley.manning", (b)(6)(b)(7)(C), and "bradley.e.manning", and the subpoena results from Skype Communications (b)(6)(b)(7)(C)

94. U.S. Army Military Intelligence Investigative Memorandum For Record, IMFR PI-ACICA-10-009-025 (Classified ~~CONFIDENTIAL//NOFORN~~), documenting the (b)(6)(b)(7)(C), (b) (7)(D) dated 14 Jul 10.

95. AIR of SA (b)(6)(b)(7)(C) 14 Jul 10, detailing subpoena results from IC Group pertaining to the email account (b)(6)(b)(7)(C)@pobox.com.

96. DoDIG Subpoena, 2010251-10468, dated 12 Jul 10, pertaining to the email account (b)(6)(b)(7)(C)@pobox.com and the subpoena results from IC Group.

97. AIR of SA (b)(6)(b)(7)(C), 16 Jul 10, detailing subpoena results from T-Mobile pertaining to cellular telephone number (b)(6)(b)(7)(C)

98. DoDIG Subpoena, 2010246-10456, dated 29 Jun 10, pertaining to cellular telephone number (b)(6)(b)(7)(C) and the subpoena results from T-Mobile.

99. AIR of SA (b)(6)(b)(7)(C) 19 Jul 10, detailing subpoena results from Facebook pertaining to the Breanna MANNING Facebook accounts.

100. DoDIG Subpoena, 2010247-10461, dated 6 Jul 10, pertaining to (b)(6)(b)(7)(C) Facebook accounts and the subpoena results from Facebook.

101. AIR of SA (b)(6)(b)(7)(C) 20 Jul 10, detailing subpoena results from Google, Inc., pertaining to the email account (b)(6)(b)(7)(C)@gmail.com.

102. DoDIG Subpoena, 2010233-10429, dated 18 Jun 10, pertaining to the email address (b)(6)(b)(7)(C)@gmail.com.

103. AIR of SA (b)(6)(b)(7)(C) 21 Jul 10, detailing subpoena results from Google pertaining to the email address (b)(6)(b)(7)(C) @gmail.com.

104. DoDIG Subpoena, 2010247-10460, dated 6 Jul 10, pertaining to the email address (b)(6)(b)(7)(C) @gmail.com and the subpoena results from Google.

105. AIR of SA (b)(6)(b)(7)(C) 23 Jul 10, detailing Federal Magistrate Search Warrant 1:10-SW-396, pertaining to the search of a computer, the property of PFC MANNING, and execution of the search warrant.

106. Federal Magistrate Search Warrant 1:10-SW-396 (UNDER SEAL), dated 23 Jul 10. (USACRC and File Copy Only)

107. Informal AR 15-6 Investigation conducted by U.S. Forces-Iraq (USF-I) Findings and

Recommendations report, dated 26 Jul 10.

108. U.S. Army Military Intelligence Investigative Memorandum For Record, PI-ACICA-10-009-IMFR-001 (Classified ~~CONFIDENTIAL//NOFORN),~~ documenting the interview of Mr. (b)(6)(b)(7)(C) dated 29 Jul 10.

109. AIR of SA (b)(6)(b)(7)(C) 29 Jul 10, detailing the coordination with U.S. Immigration and Customs Enforcement, interview of Mr. (b)(6)(b)(7)(C) and cell phone data extraction.

110. AIR of SA (b)(6)(b)(7)(C) 30 Jul 10, detailing collection of evidence and subpoena results pertaining to IP address 71.190.140.39.

111. DoDIG Subpoena, 2010265-10489, dated 29 Jul 10, pertaining to IP address 71.190.140.39 and the subpoena results from Verizon.

112. AIR of SA (b)(6)(b)(7)(C) 2 Aug 10, detailing the coordination with CPT (b)(6)(b)(7)(C)

113. AIR of SA (b)(6)(b)(7)(C) 2 Aug 10, detailing the rights advisal and non-waiver of LTC (b)(6)(b)(7)(C)

114. DA Form 3881, Rights Warning Procedure/Non-Waiver Certificate of LTC (b)(6)(b)(7)(C) dated 2 Aug 10.

115. AIR of SA (b)(6)(b)(7)(C) 3 Aug 10, detailing the coordination with IC Group regarding the email account (b)(6)(b)(7)(C) @pobox.com.

116. FBI Form 302, documenting the interview of FBI Protected Identity Witness, dated 5 Aug 10.

117. Consent to Search, pertaining to a custom computer with four hard disk drives, executed by FBI Protected Identity Witness, dated 4 Aug 10.

118. Consent to Search, pertaining to a custom computer with four hard disk drives, executed by FBI Protected Identity Witness, dated 4 Aug 10.

119. Consent to Search, pertaining to an LG brand cellular phone, executed by FBI Protected Identity Witness, dated 4 Aug 10.

120. AIR of SA (b)(6)(b)(7)(C) 5 Aug 10, detailing the interview of SMSgt (b)(6)(b)(7)(C)

121. AIR of SA (b)(6)(b)(7)(C) 5 Aug 10, detailing collection of Hand Receipt and Daily Staff Journal or Duty Officer's Log from the 2nd BCT, 10th MTN DIV.

122. DA Form 2062, Hand Receipt/Annex Number, pertaining to two sealed boxes containing the personal property of PFC MANNING, undated.

123. DA Form 1594, Daily Staff Journal or Duty Officer's Log, containing the name of Mr. (b)(6)(b)(7)(C) undated.

124. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 9 Aug 10.

125. Metropolitan Moving and Storage Company (MMSC) records related to Mr. (b)(6)(b)(7)(C) undated.

126. AIR of SA (b)(6)(b)(7)(C) 9 Aug 10, detailing subpoena results from Twitter pertaining to the accounts (b)(6)(b)(7)(C) and (b)(6)(b)(7)(C) @gmail.com".

127. DoDIG Subpoena, 2010247-10459, dated 6 Jul 10, pertaining to Twitter the accounts (b)(6)(b)(7)(C) and (b)(6)(b)(7)(C) @gmail.com", and the subpoena results from Twitter.

128. AIR of SA (b)(6)(b)(7)(C) 9 Aug 10, detailing receipt of documents pertaining to FBI Protected Identity Witness and WikiLeaks, cell phone data extraction attempt, review of documents pertaining to FBI Protected Identity Witness and WikiLeaks, and collection of evidence.

129. Documents provided by FBI Protected Identity Witness related to WikiLeaks, dated 15 Jun 10.

130. AIR of SA (b)(6)(b)(7)(C) 9 Aug 10, detailing the interview of SrA (b)(6)(b)(7)(C)

131. AIR of SA (b)(6)(b)(7)(C) 11 Aug 10, detailing the coordination with 1LT (b)(6)(b)(7)(C)

132. Canvass Interview Worksheets of SGT (b)(6)(b)(7)(C) SGT (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) 1LT (b)(6)(b)(7)(C) SGT (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) SGT (b)(6)(b)(7)(C) SSGT (b)(6)(b)(7)(C) SSGT (b)(6)(b)(7)(C) PFC (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C), and SPC (b)(6)(b)(7)(C) dated 11 Aug 10.

133. AIR of SA (b)(6)(b)(7)(C) 11 Aug 10, detailing the re-interview of SPC (b)(6)(b)(7)(C)

134. AIR of SA (b)(6)(b)(7)(C) 11 Aug 10, detailing the re-interview of SPC (b)(6)(b)(7)(C)

135. AIR of SA (b)(6)(b)(7)(C) 11 Aug 10, detailing the interview of MSG (b)(6)(b)(7)(C)

136. AIR of SA (b)(6)(b)(7)(C) 12 Aug 10, detailing the interview of CPL (b)(6)(b)(7)(C)

137. Canvass Interview Worksheet of CPL (b)(6)(b)(7)(C) dated 12 Aug 10.

138. AIR of SA (b)(6)(b)(7)(C) 12 Aug 10, detailing the coordination with CWO4 (b)(6)(b)(7)(C)

139. AIR of SA (b)(6)(b)(7)(C) 12 Aug 10, detailing the interview of SPC (b)(6)(b)(7)(C)

140. AIR of SA (b)(6)(b)(7)(C) 12 Aug 10, detailing the interview of 1LT (b)(6)(b)(7)(C)

141. AIR of SA (b)(6)(b)(7)(C) 13 Aug 10, detailing the review of information pertaining to the email account (b)(6)(b)(7)(C) @gmail.com produced in response to search warrant.

142. Information pertaining to the email account (b)(6)(b)(7)(C) @gmail.com provided by Google in response to search warrant.

143. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 14 Aug 10.

144. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 14 Aug 10.

145. FBI Form 302, documenting the interviews of Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) dated 14 Aug 10.

146. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 16 Aug 10.

147. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 16 Aug 10.

148. AIR of SA (b)(6)(b)(7)(C) 16 Aug 10, detailing the interview of Mr (b)(6)(b)(7)(C) consent to search, and collection of evidence.

149. Consent to Search Computer/Electronic Equipment, executed by Mr. (b)(6)(b)(7)(C) dated 10 Aug 10.

150. AIR of SA (b)(6)(b)(7)(C) 16 Aug 10, detailing the interview of SSG (b)(6)(b)(7)(C)

151. AIR of SA (b)(6)(b)(7)(C) 16 Aug 10, detailing the interview of SPC (b)(6)(b)(7)(C)

152. AIR of SA (b)(6)(b)(7)(C) 16 Aug 10, detailing the interview of LTC (b)(6)(b)(7)(C)

153. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 17 Aug 10.

154. AIR of SA (b)(6)(b)(7)(C) 17 Aug 10, detailing the interview of SPC (b)(6)(b)(7)(C)

155. AIR of SA (b)(6)(b)(7)(C) 18 Aug 10, detailing the interview of CPL (b)(6)(b)(7)(C)

156. AIR of SA (b)(6)(b)(7)(C) 18 Aug 10, detailing the coordination with Mr. (b)(6)(b)(7)(C) receipt of information pertaining to LTC (b)(6)(b)(7)(C) AKO account, and collection of evidence.

157. Army Knowledge Online (AKO) header information pertaining to the AKO email account of LTC (b)(6)(b)(7)(C) undated.

158. AIR of SA (b)(6)(b)(7)(C) 18 Aug 10, detailing the interviews of MSG (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) and SPC (b)(6)(b)(7)(C)

159. AIR of SA (b)(6)(b)(7)(C) 23 Aug 10, detailing the receipt of Classified Nondisclosure documents signed by PFC MANNING.

160. DD Form 1847-1, Sensitive Compartmented Information Nondisclosure Agreement, signed by PFC MANNING, dated 22 Jan 09.

161. Standard Form 312, Classified Information Nondisclosure Agreement, signed by PFC MANNING, dated 17 Sep 08.

162. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 23 Aug 10.

163. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 23 Aug 10.

164. AIR of SA (b)(6)(b)(7)(C) 23 Aug 10, detailing the coordination with CENTCOM and collection of evidence.

165. AIR of SA (b)(6)(b)(7)(C) 24 Aug 10, detailing the interview of SFC (b)(6)(b)(7)(C)

166. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 25 Aug 10.

167. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 25 Aug 10.

168. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 25 Aug 10.

169. AIR of SA (b)(6)(b)(7)(C) 25 Aug 10, detailing the interview of 1SG (b)(6)(b)(7)(C)

170. DA Form 2823, Sworn Statement of 1SG (b)(6)(b)(7)(C) dated 25 Aug 10.

171. AIR of SA (b)(6)(b)(7)(C) 25 Aug 10, detailing the interview of SSgt (b)(6)(b)(7)(C)

172. AIR of SA (b)(6)(b)(7)(C) 25 Aug 10, detailing the interview of SSG (b)(6)(b)(7)(C)

173. DA Form 2823, Sworn Statement of CPT (b)(6)(b)(7)(C), dated 25 Aug 10.

174. AIR of SA (b)(6)(b)(7)(C) 25 Aug 10, detailing the interview of 1LT (b)(6)(b)(7)(C) coordination with CSM (b)(6)(b)(7)(C) and coordination with SFC (b)(6)(b)(7)(C).

175. DA Form 2823, Sworn Statement of 1LT (b)(6)(b)(7)(C) dated 25 Aug 10.

176. AIR of SA (b)(6)(b)(7)(C) 25 Aug 10, detailing the interview of SFC (b)(6)(b)(7)(C) and interview of SFC (b)(6)(b)(7)(C)

177. DA Form 2823, Sworn Statement of SFC (b)(6)(b)(7)(C) dated 25 Aug 10.

178. DA Form 2823, Sworn Statement of SFC (b)(6)(b)(7)(C) dated 25 Aug 10.

179. AIR of SA (b)(6)(b)(7)(C) 25 Aug 10, detailing the coordination with Ms. (b)(6)(b)(7)(C) regarding PFC MANNING's annual Information Assurance training.

180. AIR of SA (b)(6)(b)(7)(C) 26 Aug 10, detailing the interview of WO1 (b)(6)(b)(7)(C)

181. AIR of SA (b)(6)(b)(7)(C) 26 Aug 10, detailing the interview of CPT (b)(6)(b)(7)(C)

182. AIR of SA (b)(6)(b)(7)(C) 26 Aug 10, detailing the interview of Mrs. (b)(6)(b)(7)(C) coordination with Mrs. (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) re-interview of SSG (b)(6)(b)(7)(C) request for medical information and receipt of behavioral health records pertaining to PFC MANNING; and collection of Non-Disclosure Agreements signed by PFC MANNING.

183. DA Form 2823, Sworn Statement of Mrs. (b)(6)(b)(7)(C) dated 7 Jul 10.

184. AIR of SA (b)(6)(b)(7)(C) 27 Aug 10, detailing the interview of CW2 (b)(6)(b)(7)(C)

185. AIR of SA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 30 Aug 10, detailing the collection of evidence.

186. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 30 Aug 10.

187. AIR of SA (b)(6)(b)(7)(C) 31 Aug 10, detailing checks of the Centralized Operations Police Suite (COPS) system pertaining to PFC MANNING; the coordination with 1SG (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) and SGT (b)(6)(b)(7)(C) and interview of MAJ (b)(6)(b)(7)(C)

188. AIR of SA (b)(6)(b)(7)(C) 31 Aug 10, detailing the interview of MSG (b)(6)(b)(7)(C)

189. AIR of SA (b)(6)(b)(7)(C), 10 Sep 10, detailing the interview of SPC (b)(6)(b)(7)(C)

190. DA Form 2823, Sworn Statement of SPC (b)(6)(b)(7)(C), dated 9 Sep 10.

191. AIR of SA (b)(6)(b)(7)(C) 10 Sep 10, detailing the interviews of SFC (b)(6)(b)(7)(C), WO1 (b)(6)(b)(7)(C), SFC (b)(6)(b)(7)(C), SFC (b)(6)(b)(7)(C) and 1LT (b)(6)(b)(7)(C)

192. AIR of SA (b)(6)(b)(7)(C) 10 Sep 10, detailing the coordination with Mr. (b)(6)(b)(7)(C), obtaining a consent to search, and collection of evidence.

193. CID Form 87-R-E, Consent to Search, 9 Sep 10, executed by Mr. (b)(6)(b)(7)(C)

194. AIR of SA (b)(6)(b)(7)(C) 10 Sep 10, detailing the evidence recovery scene examination.

195. Recovery Scene Rough Sketch prepared by SA (b)(6)(b)(7)(C) dated 10 Sep 10.

196. CD containing photographs of the evidence recovery scene. (USACRC and File Copy Only)

197. AIR of SA (b)(6)(b)(7)(C) 10 Sep 10, detailing the collection Secure Compartmentalized Information (SCI) indoctrination documents, signed by PFC MANNING, as evidence.

198. SCI Indoctrination and Nondisclosure documents signed by PFC MANNING, dated 17 Sep 08 to 29 Jan 09.

199. Indoctrination for Sensitive Series COMINT (Classified ~~CONFIDENTIAL//~~COMINT//X1), signed by PFC MANNING, dated 29 Jan 09.

200. AIR of SA (b)(6)(b)(7)(C) 12 Sep 10, detailing the receipt of Search and Seizure Authorization, coordination with SFC (b)(6)(b)(7)(C) forensic preview of hard disk drives, and collection of evidence.

201. DA Form 3745, Search and Seizure Authorization, with supporting affidavit, dated 10 Sep 10.

202. AIR of SA (b)(6)(b)(7)(C), 12 Sep 10, detailing the interview of 1LT (b)(6)(b)(7)(C)

203. AIR of SA (b)(6)(b)(7)(C) (Classified ~~SECRET//~~REL TO USA, (b)(6)(b)(7)(C), 14 Sep 10, detailing the interview of SrA (b)(6)(b)(7)(C)

204. AIR of SA (b)(6)(b)(7)(C), 16 Sep 10, detailing the coordination with CDR (b)(6)(b)(7)(C) YN1 (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) MAC (b)(6)(b)(7)(C) MAJ (b)(6)(b)(7)(C) MAJ (b)(6)(b)(7)(C)

PO (b)(6)(b)(7)(C) and CPT (b)(6)(b)(7)(C) and request for medical and mental health records pertaining to PFC MANNING.

205. Reports received from the Kuwait Confinement Facility pertaining to PFC MANNING.

206. AIR of SA (b)(6)(b)(7)(C) 20 Sep 10, detailing the recording of PFC MANNING's visitation period at the Brig, Marine Corps Base (MCB) Quantico, and collection of evidence.

207. AIR of SA (b)(6)(b)(7)(C) 21 Sep 10, detailing the coordination with CPT (b)(6)(b)(7)(C) receipt of search authorization, and search of PFC MANNING's personal belongings obtained from his Containerized Housing Unit (CHU) in Iraq.

208. DA Form 3745, Search and Seizure Authorization 16 Sep 10, with supporting affidavit.

209. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 23 Sep 10.

210. FBI Form 302, documenting the interview of Ms. (b)(6)(b)(7)(C) dated 27 Sep 10.

211. Internet Chat Logs between (b)(6)(b)(7)(C) labeled (b)(6)(b)(7)(C) - 29 JUNE.pdf".

212. Internet Chat Logs between (b)(6)(b)(7)(C) labeled (b)(6)(b)(7)(C) - 30 JUNE.pdf".

213. Internet Chat Logs between (b)(6)(b)(7)(C) labeled (b)(6)(b)(7)(C) - File: 12 JULY.pdf".

214. Internet Chat Logs between (b)(6)(b)(7)(C) labeled (b)(6)(b)(7)(C) 19 JULY.pdf".

215. Internet Chat Logs between (b)(6)(b)(7)(C) (b)(6)(b)(7)(C), and (b)(6)(b)(7)(C), labeled (b)(6)(b)(7)(C) - 20 JULY.pdf".

216. Internet Chat Logs between (b)(6)(b)(7)(C), labeled (b)(6)(b)(7)(C) - 22 JULY.pdf".

217. Internet Chat Logs between (b)(6)(b)(7)(C), labeled (b)(6)(b)(7)(C) 25 JULY.pdf".

218. Internet Chat Logs between (b)(6)(b)(7)(C) and (b)(6)(b)(7)(C), labeled (b)(6)(b)(7)(C) - 25 JULY.pdf".

219. Internet Chat Logs between (b)(6)(b)(7)(C) labeled (b)(6)(b)(7)(C) 26 JULY.pdf".

220. Internet Chat Logs between (b)(6)(b)(7)(C) labeled (b)(6)(b)(7)(C) 6 AUG.pdf".

221. Resume of Ms. (b)(6)(b)(7)(C) dated 3 Sep 10, and Written Letter of Concern pertaining to Ms. (b)(6)(b)(7)(C) dated 19 Nov 07.

222. FBI Form 302, documenting the receipt and service of a Federal Magistrate Search Warrant upon Brookhaven National Laboratory, dated 27 Sep 10.

223. Federal Magistrate Search Warrant 10-M-1108 (UNDER SEAL), dated 22 Sep 10. (USACRC and File Copy Only)

224. AIR of SA (b)(6)(b)(7)(C) 27 Sep 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico and collection of evidence.

225. AIR of SA (b)(6)(b)(7)(C) 29 Sep 10, detailing subpoena results from Yahoo! Inc., pertaining to the email account bradass87@yahoo.com.

226. DoDIG Subpoena, 2010233-10433, dated 18 Jun 10, pertaining to the Yahoo! email address (b)(6)(b)(7)(C)@yahoo.com and the subpoena results from Yahoo! Inc.

227. AIR of SA (b)(6)(b)(7)(C) 1 Oct 10, detailing the coordination with CPT (b)(6)(b)(7)(C) and MSG (b)(6)(b)(7)(C) forensic previewing of hard disk drives; interview of CW2 (b)(6)(b)(7)(C) receipt of Military Magistrate Search Authorizations; and collection of evidence.

228. DA Form 3745, Search and Seizure Authorization, dated 30 Sep 10, with supporting affidavit.

229. DA Form 2823, Sworn Statement of CW2 (b)(6)(b)(7)(C) dated 1 Oct 10.

230. DA Form 3745, Search and Seizure Authorization, dated 1 Oct 10, with supporting affidavit.

231. AIR of SA (b)(6)(b)(7)(C) 1 Oct 10, detailing subpoena results from the Massachusetts Institute of Technology (MIT) pertaining to email accounts (b)(6)(b)(7)(C)@mit.edu and (b)(6)(b)(7)(C)@mit.edu.

232. DoDIG Subpoena, 2010247-10458, pertaining to MIT email accounts (b)(6)(b)(7)(C)@mit.edu and (b)(6)(b)(7)(C)@mit.edu, and the subpoena results from MIT.

233. AIR of SA (b)(6)(b)(7)(C) 4 Oct 10, detailing the interview of Mr. (b)(6)(b)(7)(C).

234. AIR of SA (b)(6)(b)(7)(C) 5 Oct 10, detailing attempts to locate SPC (b)(6)(b)(7)(C) and coordination with CPT (b)(6)(b)(7)(C)

235. AIR of SA (b)(6)(b)(7)(C) (Classified ~~CONFIDENTIAL~~//REL TO USA, (b)(6)(b)(7)(C) 5 Oct 10, detailing the interview of Mr. (b)(6)(b)(7)(C)

236. AIR of SA (b)(6)(b)(7)(C) 7 Oct 10, detailing the interview of Mr. (b)(6)(b)(7)(C)

237. AIR of SA (b)(6)(b)(7)(C) 12 Oct 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, collection of evidence, and review of the recording.

238. AIR of SA (b)(6)(b)(7)(C) Classified ~~SECRET//REL~~ TO USA, (b)(6)(b)(7)(C) 13 Oct 10, detailing the interview of Mr. (b)(6)(b)(7)(C)

239. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 14 Oct 10.

240. AIR of SA (b)(6)(b)(7)(C) 14 Oct 10, detailing subpoena results from Yahoo! Inc., pertaining to the email account (b)(6)(b)(7)(C) @yahoo.com.

241. DoDIG Subpoena, 2010279-10510, dated 18 Aug 10, pertaining to Yahoo! account (b)(6)(b)(7)(C) @yahoo.com, and the subpoena results from Yahoo! Inc.

242. CD containing logs pertaining to the Yahoo! email account (b)(6)(b)(7)(C) @yahoo.com. (USACRC and File Copy Only)

243. AIR of SA (b)(6)(b)(7)(C) 15 Oct 10, detailing the collection of Department of State firewall log files as evidence.

244. AIR of SA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 19 Oct 10, detailing the collection of Central Intelligence Agency (CIA) documents as evidence; collection of National Security Agency (NSA) log files as evidence; and collection of files pertaining to PFC MANNING's Intelink account as evidence.

245. FBI Washington Field CART Report of Examination (Classified ~~SECRET//NOFORN~~), documenting the forensic imaging of two hard disk drives; initial forensic examination; and forensic duplication of hard disk drives, unsigned, dated 19 Oct 10.

246. AIR of SA (b)(6)(b)(7)(C) 20 Oct 10, detailing the interview of PO1 (b)(6)(b)(7)(C)

247. AIR of SA (b)(6)(b)(7)(C) 20 Oct 10, detailing the interview of SSgt (b)(6)(b)(7)(C)

248. FBI Form 302, documenting the interview of Mr. (b)(6)(b)(7)(C) dated 22 Oct 10.

249. AIR of SA (b)(6)(b)(7)(C) 28 Oct 10, detailing the collection of recorded phone conversations from the Kuwait Confinement Facility as evidence.

250. AIR of SA (b)(6)(b)(7)(C) 1 Nov 10, detailing the receipt of Federal Magistrate Search Warrant and execution of Search Warrant.

251. Federal Magistrate Search Warrant 1:10-SW-576 (UNDER SEAL), dated 28 Oct 10. (USACRC and File Copy Only)

252. AIR of SA (b)(6)(b)(7)(C) 2 Nov 10, detailing the coordination with Ms. (b)(6)(b)(7)(C) consent to search, search, and collection of evidence.

253. CID Form 87-R-E, Consent to Search, executed by Ms. (b)(6)(b)(7)(C) dated 2 Nov 10.

254. AIR of SA (b)(6)(b)(7)(C) 9 Nov 10, detailing the collection of classified information downloaded from the internet by the IRTF as evidence.

255. AIR of SA (b)(6)(b)(7)(C) 10 Nov 10, (b)(6)(b)(7)(C), (b) (7)(D) (b)(6)(b)(7)(C), (b) (7)(D) collection of chat logs as evidence; coordination with and receipt of emails from Mr. (b)(6)(b)(7)(C) receipt of Mr. (b)(6)(b)(7)(C) property from U.S. Immigration and Customs Enforcement and collection of evidence.

256. Email containing Internet Chat logs between (b)(6)(b)(7)(C) org" and (b)(6)(b)(7)(C) dated 22 Jul 10.

257. Information regarding WikiLeaks provided by Mr. (b)(6)(b)(7)(C)

258. AIR of SA (b)(6)(b)(7)(C) 5 Nov 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

259. AIR of SA (b)(6)(b)(7)(C) 17 Nov 10, detailing the interview of SPC (b)(6)(b)(7)(C)

260. AIR of SA (b)(6)(b)(7)(C) 7 Dec 10, detailing the collection of Combined Information Data Network Exchange (CIDNE) log files as evidence.

261. AIR of SA (b)(6)(b)(7)(C) 9 Dec 10, detailing the receipt of a Federal Magistrate Search Warrant, execution of the warrant, and collection of evidence.

262. Federal Magistrate Search Warrant 1:10-SW-652 (UNDER SEAL), dated 9 Dec 10. (USACRC and File Copy Only)

263. AIR of SA (b)(6)(b)(7)(C) 13 Dec 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, and collection of evidence.

264. AIR of SA (b)(6)(b)(7)(C) 15 Dec 10, detailing the collection of CIA files as evidence.

265. Letter from the CIA, Office of the General Counsel (Classified ~~SECRET//ORCON/~~

~~NOFORN)~~ addressed to CPT (b)(6)(b)(7)(C) dated 15 Dec 10. (USACRC and File Copy Only)

266. Nine pages of printed documents (Classified ~~SECRET//ORCON/NOFORN)~~, containing access log entries related to CIA files access by PFC MANNING, dated 15 Dec 10. (USACRC and File Copy Only)

267. AIR of SA (b)(6)(b)(7)(C) 17 Dec 10, detailing the interview of CW2 (b)(6)(b)(7)(C)

268. AIR of SA (b)(6)(b)(7)(C) 17 Dec 10, detailing the interview of WO1 (b)(6)(b)(7)(C)

269. AIR of SA (b)(6)(b)(7)(C) 20 Dec 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

270. AIR of SA (b)(6)(b)(7)(C) 0 Dec 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, collection of evidence, and review of the recording.

271. AIR of SSA (b)(6)(b)(7)(C) 27 Dec 10, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, and collection of evidence.

272. AIR of SA (b)(6)(b)(7)(C) 30 Dec 10, detailing the interview of CPT (b)(6)(b)(7)(C)

273. AIR of SA (b)(6)(b)(7)(C) 3 Jan 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, and collection of evidence.

274. AIR of SA (b)(6)(b)(7)(C) 3 Jan 11, detailing the coordination with Ms. (b)(6)(b)(7)(C) consent to search, collection of evidence.

275. CID Form 87-R-E, Consent to Search from Ms. (b)(6)(b)(7)(C) 3 Jan 11.

276. AIR of SA (b)(6)(b)(7)(C) 5 Jan 11, detailing the interview of MSG (b)(6)(b)(7)(C)

277. AIR of SA (b)(6)(b)(7)(C) 5 Jan 11, detailing the interview of CW2 (b)(6)(b)(7)(C)

278. AIR of SA (b)(6)(b)(7)(C) 5 Jan 11, detailing the interview of 1LT (b)(6)(b)(7)(C)

279. AIR of SA (b)(6)(b)(7)(C), 5 Jan 11, detailing the interview of CPT (b)(6)(b)(7)(C)

280. AIR of SA (b)(6)(b)(7)(C) 5 Jan 11, detailing the interview of CPT (b)(6)(b)(7)(C)

281. AIR of SA (b)(6)(b)(7)(C) 6 Jan 11, detailing the interview of CPT (b)(6)(b)(7)(C)

282. AIR of SA (b)(6)(b)(7)(C) 6 Jan 11, detailing the interview of SPC (b)(6)(b)(7)(C)

283. AIR of SA (b)(6)(b)(7)(C) 6 Jan 11, detailing the interview of CPT (b)(6)(b)(7)(C)

284. AIR of SA (b)(6)(b)(7)(C) 6 Jan 11, detailing the interview of SGT (b)(6)(b)(7)(C)

285. AIR of SA (b)(6)(b)(7)(C) 6 Jan 11, detailing the interview of SPC (b)(6)(b)(7)(C)

286. AIR of SA (b)(6)(b)(7)(C) 7 Jan 11, detailing the interview of SSG (b)(6)(b)(7)(C)

287. AIR of SA (b)(6)(b)(7)(C) 13 Jan 11, detailing the coordination with Mr. (b)(6)(b)(7)(C) regarding Query Tree and Mr. (b)(6)(b)(7)(C) regarding PFC MANNING's acceptable use policies.

288. AIR of SA (b)(6)(b)(7)(C) 14 Jan 11, detailing the interview of MSG (b)(6)(b)(7)(C)

289. AIR of SA (b)(6)(b)(7)(C) 14 Jan 11, detailing the interview of SPC (b)(6)(b)(7)(C)

290. AIR of SA (b)(6)(b)(7)(C) 14 Jan 11, detailing the interview of MAJ (b)(6)(b)(7)(C)

291. AIR of SA (b)(6)(b)(7)(C) 14 Jan 11, detailing the interview of SPC (b)(6)(b)(7)(C)

292. AIR of SA (b)(6)(b)(7)(C) 14 Jan 11, detailing the interview of MAJ (b)(6)(b)(7)(C)

293. AIR of SA (b)(6)(b)(7)(C), 14 Jan 11, detailing the collection of Intelink log files as evidence.

294. AIR of SA (b)(6)(b)(7)(C) 21 Jan 11, detailing the interview of CPT (b)(6)(b)(7)(C)

295. AIR of SA (b)(6)(b)(7)(C) 21 Jan 11, detailing the interview of SGT (b)(6)(b)(7)(C)

296. AIR of SA (b)(6)(b)(7)(C) 21 Jan 11, detailing the coordination with Mr. (b)(6)(b)(7)(C) regarding PFC MANNING's IA training.

297. AIR of SA (b)(6)(b)(7)(C) 24 Jan 11, detailing the collection of the Gharani airstrike video as evidence and collection of Open Source Center audit logs as evidence.

298. Open Source Center (OSC) Account Information Document (Classified ~~SECRET//ORCON/NOFORN~~), pertaining the OSC Account of PFC MANNING, dated 6 Nov 09. (USACRC and File Copy Only)

299. AIR of SA (b)(6)(b)(7)(C) 25 Jan 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

300. AIR of SA (b)(6)(b)(7)(C) 25 Jan 11, detailing the review of the recording of PFC MANNING's visitation period at the Brig, MCB Quantico.

301. AIR of SA (b)(6)(b)(7)(C), 25 Jan 11, detailing the review of the recording of PFC MANNING's visitation period at the Brig, MCB Quantico.

302. AIR of SA (b)(6)(b)(7)(C) 31 Jan 11, detailing subpoena results from Zipcar, Inc., pertaining to PFC MANNING's Zipcar account.

303. DoDIG Subpoena, 2011073-10771, pertaining to Zipcar account number 501376 and the subpoena results from Zipcar, Inc.

304. AIR of SA (b)(6)(b)(7)(C) 1 Feb 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, collection of evidence, and review of the recording.

305. AIR of SA (b)(6)(b)(7)(C), 7 Feb 11, detailing the collection of the recording of PFC MANNING's visitation period at the Brig, MCB Quantico as evidence and review of the recording.

306. AIR of SA (b)(6)(b)(7)(C) 7 Feb 11, detailing the re-interview of SFC(Ret) (b)(6)(b)(7)(C)

307. AIR of SA (b)(6)(b)(7)(C) 12 Feb 11, detailing the review of multiple recordings of PFC MANNING's visitation period at the Brig, MCB Quantico.

308. AIR of SA (b)(6)(b)(7)(C), 14 Feb 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

309. AIR of SA (b)(6)(b)(7)(C), 14 Feb 11, detailing the receipt and execution of two Federal Magistrate Search Warrants.

310. Federal Magistrate Search Warrant 1:11SW-47 (UNDER SEAL), 11 Feb 11. (USACRC and File Copy Only)

311. Federal Magistrate Search Warrant 1:11SW-89 (UNDER SEAL), 11 Feb 11. (USACRC and File Copy Only)

312. AIR of SA (b)(6)(b)(7)(C), 17 Feb 11, detailing the collection of electronic files related to WikiLeaks as evidence.

313. AIR of SA (b)(6)(b)(7)(C), 24 Feb 11, detailing the interview of Mr. (b)(6)(b)(7)(C)

314. AIR of SA (b)(6)(b)(7)(C), 24 Feb 11, detailing the interview of SFC (b)(6)(b)(7)(C)

315. AIR of SA (b)(6)(b)(7)(C) 28 Feb 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

316. AIR of SA (b)(6)(b)(7)(C) 1 Mar 11, detailing subpoena results from Washington Metropolitan Area Transit Authority (WMATA) pertaining to PFC MANNING's SmarTrip card account and review of multiple recordings of PFC MANNING's visitation period at the Brig, MCB Quantico.

317. DoDIG Subpoena, 2011073-10772, pertaining to SmarTrip card of PFC MANNING and the subpoena results from WMATA.

318. AIR of SA (b)(6)(b)(7)(C) 2 Mar 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, collection of evidence, and review of the recording.

319. AIR of SA (b)(6)(b)(7)(C) 8 Mar 11, detailing the coordination with Mr. (b)(6)(b)(7)(C) regarding PFC MANNING's Information Assurance training.

320. AIR of SA (b)(6)(b)(7)(C) 13 Mar 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

321. AIR of SA (b)(6)(b)(7)(C) 28 Mar 11, detailing the interviews of CW4 (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C)

322. AIR of SA (b)(6)(b)(7)(C) 8 Apr 11, detailing the coordination with Mr (b)(6)(b)(7)(C) regarding mandatory annual IA examinations PFC MANNING would have completed.

323. Screen captures of IA examination questions provided by Mr. (b)(6)(b)(7)(C) undated.

324. AIR of SA (b)(6)(b)(7)(C) 11 Apr 11, detailing the recording of PFC MANNING's visitation period at the Brig, MCB Quantico, review of the recording, and collection of evidence.

325. AIR of SA (b)(6)(b)(7)(C) 11 Apr 11, detailing the coordination with Ms. (b)(6)(b)(7)(C) and collection of web server log files from the Joint Improvised Explosive Device Defeat Organization (JIEDDO) as evidence.

326. AIR of SA (b)(6)(b)(7)(C) 15 Apr 11, (Classified ~~SECRET//REL~~ TO USA, (b)(6)(b)(7)(C) detailing the interview of Mr (b)(6)(b)(7)(C)

327. AIR of SA (b)(6)(b)(7)(C) 15 Apr 11, (Classified ~~SECRET//REL~~ TO USA, (b)(6)(b)(7)(C) detailing the interview of CPT (b)(6)(b)(7)(C)

328. AIR of SA (b)(6)(b)(7)(C) 22 Apr 11, detailing the collection of access log files from the Army

Counter Intelligence Center (ACIC) as evidence.

329. AIR of SA (b)(6)(b)(7)(C), 3 May 11, detailing the interview of SPC (b)(6)(b)(7)(C)

330. AIR of SSA (b)(6)(b)(7)(C) 5 May 11, detailing the forensic testing of the computer program WGET.EXE, used by PFC MANNING, to download 766 PDF files related to Guantanamo Bay detainees from a SIPR Intelink website; the collection of the downloaded 766 PDF files as evidence; and the downloading and collection of 768 PDF files related to Guantanamo Bay from the WikiLeaks.ch website as evidence.

331. AIR of SA (b)(6)(b)(7)(C) 6 May 11, detailing the forensic downloading of the file "cablegate201105050833.7z" from the WikiLeaks.ch website, and the collection of this file as evidence.

332. AIR of SA (b)(6)(b)(7)(C) 19 May 11, detailing the receipt and collection as evidence of log files from ACIC, and the receipt and collection of evidence of Centaur log files as evidence.

333. AIR of SA (b)(6)(b)(7)(C) 26 May 11, detailing the interview of Mr. (b)(6)(b)(7)(C)

334. Intelligence Information Report, IIR 6 089 0563 11 (Classified ~~SECRET//REL~~ TO USA, (b)(6)(b)(7)(C) reporting documents contained on digital media collected during the capture of a high-value member of Hezb-e-Islami Gulbuddin (HIG) in Afghanistan contained classified data related to unlawful disclosures by PFC MANNING, dated 20 Jun 11.

335. AIR of SA (b)(6)(b)(7)(C) 21 Jun 11, detailing the interview of Inmate (b)(6)(b)(7)(C)

336. AIR of SA (b)(6)(b)(7)(C) 22 Jun 11, detailing coordination for an escort of PFC MANNING's attorney to meet with PFC MANNING.

337. AIR of SA (b)(6)(b)(7)(C) 28 Jun 11, detailing the collection of two DVDs as evidence containing recording(s) of visitations with PFC MANNING on 21 May 11; and the collection of one DVD as evidence containing recording(s) of visitations with PFC MANNING on 25 Jun 11.

338. AIR of SA (b)(6)(b)(7)(C) 14 Jul 11, detailing the receipt and collection of one DVD containing log files provided by the 902nd Military Intelligence Group as evidence; and initial forensic examination of the files contained on the DVD.

339. AIR of SA (b)(6)(b)(7)(C) 18 Jul 11, detailing the interview of Inmate (b)(6)(b)(7)(C)

340. AIR of SA (b)(6)(b)(7)(C) 18 Jul 11, detailing the interview of Inmate (b)(6)(b)(7)(C)

341. Canvass Interview worksheet of Inmate (b)(6)(b)(7)(C) undated.

342. AIR of SA (b)(6)(b)(7)(C) 19 Jul 11, detailing the interview of Mr. (b)(6)(b)(7)(C)

343. AIR of SA (b)(6)(b)(7)(C) 31 Aug 11, detailing the forensic downloading and collection of the file "cablegate-201108290338.7z" from the WikiLeaks.org website as evidence.

344. AIR of SA (b)(6)(b)(7)(C) 1 Sep 11, detailing the receipt and collection of 14 Intelink log files from Office of the Director of National Intelligence (ODNI) as evidence.

345. AIR of SA (b)(6)(b)(7)(C) 1 Sep 11, detailing the Internet search for the file "cables.csv"; discovery of various files on the Internet; and the collection of various associated files identified as evidence.

346. AIR of SA (b)(6)(b)(7)(C) 6 Sep 11, detailing the interviews of Inmate (b)(6)(b)(7)(C) coordination with SGT (b)(6)(b)(7)(C) and coordination with SA (b)(6)(b)(7)(C).

347. Hand written notes of Inmate (b)(6)(b)(7)(C) dated 19 Aug 11 to 25 Aug 11.

348. AIR of SA (b)(6)(b)(7)(C) 6 Sep 11, detailing the receipt and collection of one CD containing log files from the Central Intelligence Agency (CIA); and initial forensic examination of the contents of the CD.

349. Intelligence Information Report, IIR 6 089 0793 11 (Classified ~~SECRET//REL~~ TO USA, (b)(6)(b)(7)(C), reporting digital media collected during the capture of a high-value member of Hezb-e-Islami Gulbuddin in Afghanistan contained files and software code for harvesting data from the WikiLeaks website and conducting analysis of data related to unlawful disclosures by PFC MANNING, dated 14 Sep 11.

350. AIR of SA (b)(6)(b)(7)(C) 20 Sep 11, detailing the receipt and review of records related to DoDIG Subpoena 2011352-11200.

351. DoDIG Subpoena, 2011352-11200, dated 26 Aug 11, pertaining to records and transcripts of PFC MANNING from Montgomery College, and subpoena results.

352. AIR of SA (b)(6)(b)(7)(C) 27 Sep 11, detailing the coordination with Mr. (b)(6)(b)(7)(C) and receipt of user information related to the Open Source Center (OSC) accounts of PFC MANNING.

353. AIR of SA (b)(6)(b)(7)(C) 29 Sep 11, detailing the interview of SPC (b)(6)(b)(7)(C)

354. AIR of SA (b)(6)(b)(7)(C) 4 Oct 11, detailing the coordination with Mr. (b)(6)(b)(7)(C) receipt and review of Army Knowledge Online (AKO) Lightweight Directory Access Protocol

(LDAP) logs.

355. AIR of SA (b)(6)(b)(7)(C) 25 Oct 11, detailing the interview of Mr. (b)(6)(b)(7)(C)

356. AIR of SA (b)(6)(b)(7)(C) 3 Nov 11, detailing the coordination with Assistant U.S. Attorney regarding Search Warrant 1:11SW509; and receipt and collection of one CD containing the Search Warrant results as evidence.

357. Federal Magistrate Search Warrant 1:11SW509 (UNDER SEAL), 15 Sep 11. (USACRC and File Copy Only)

358. AIR of SA (b)(6)(b)(7)(C) 4 Nov 11, detailing the coordination with Ms. (b)(6)(b)(7)(C) and the collection of eight DVDs containing Intelink log files as evidence.

359. AIR of SA (b)(6)(b)(7)(C) Dec 11, detailing the coordination with the FBI, and collection of a hard disk drive containing a forensic image of the U.S. Government computer assigned to Mr. (b)(6)(b)(7)(C) at Brookhaven National Laboratory as evidence.

360. AIR of SSA (b)(6)(b)(7)(C) 9 Dec 11, detailing the preliminary forensic examination of the forensic image of the U.S. Government computer assigned to Mr. (b)(6)(b)(7)(C) at Brookhaven National Laboratory.

361. AIR of SA (b)(6)(b)(7)(C) 6 Dec 11, detailing the collection of two DVDs containing the Al-Shabaab produced videos, "Thou Art Held Responsible Only for Thyself" Part 1 and Part 2, as evidence.

362. AIR of SA (b)(6)(b)(7)(C) 20 Dec 11, detailing the interview of Mr. (b)(6)(b)(7)(C)

363. Sworn Statement of Mr (b)(6)(b)(7)(C) dated 20 Dec 11.

364. AIR of SA (b)(6)(b)(7)(C) 11 Jan 12, detailing the collection of one CD containing the file "manning1.ods" related to the email headers of PFC MANNING's AKO-S account as evidence.

365. AIR of SA (b)(6)(b)(7)(C) 23 Jan 12, detailing the coordination with Mr. (b)(6)(b)(7)(C) and LTC (b)(6)(b)(7)(C) regarding the authorized use of the computer program "wget".

366. Certificate of Networthiness, Cert#: 200906160, Distributed Common Ground System-Army (DCGS-A) 3.1 with WSS 3.1 and BAL 3.1, signed by Mr. (b)(6)(b)(7)(C) dated 20 Aug 09.

367. Certificate of Networthiness, Cert#: 200904700, Cygwin, Version 2.5, signed by Mr. (b)(6)(b)(7)(C) dated 27 Aug 09.

368. Certificate of Networthiness, Cert#: 200905573, Red Hat Enterprise Linux 5.X, Kernel 2.6, signed by Mr. (b)(6)(b)(7)(C) dated 5 Nov 09.

369. AIR of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET~~), 25 Jan 12, detailing coordination with CPT (b)(6)(b)(7)(C) in regard to digital media collected by U.S. Forces in Afghanistan during the capture of a high value detainee; coordination with personnel from the National Media Exploitation Center (NMEC), collection of one hard disk drive from NMEC personnel.

370. AIR of SA (b)(6)(b)(7)(C) 30 Jan 12, detailing the collection of one CD and one DVD as evidence containing recording(s) of visitations with PFC MANNING on 24 Sep 11.

371. AIR of SA (b)(6)(b)(7)(C) 3 Feb 12, detailing the interviews of CW2 (b)(6)(b)(7)(C) SFC (b)(6)(b)(7)(C) SGT (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) CW2 (b)(6)(b)(7)(C) SSG (b)(6)(b)(7)(C) receipt of the 2nd Brigade Combat Team (BCT) Acceptable User Policy (AUP) form; receipt of the Fort Drum NIPR AUP form; and coordination with SSG (b)(6)(b)(7)(C)

372. 2BCT Automated Information System (AIS) Security Policy Briefing (SIPR) form, undated.

373. Fort Drum Classified/Unclassified Installation Campus Area Network (ICAN) Acceptable Use Policy (AUP) form, dated February 2010.

374. AIR of SA (b)(6)(b)(7)(C) 10 Feb 12, detailing the coordination with Mr. (b)(6)(b)(7)(C) and receipt of a copy of the Version Description Document (VDD) for the Basic Analyst Laptop (BAL), dated 1 Oct 09.

375. VDD for BAL, DCGS-A Software Version 3.1 Patch 3, dated 1 Oct 09.

376. AIR of SA (b)(6)(b)(7)(C) 13 Feb 12, detailing the coordination with CW3 (b)(6)(b)(7)(C) and receipt of the 35F10 Student Evaluation Plan, a memorandum listing the names of PFC MANNING's Advanced Individual Training (AIT) instructors, a roster of students who attended AIT with PFC MANNING, and a DVD containing two files pertaining to the Plan Of Instruction (POI) and Lesson Plans for the Military Occupational Specialty 35F10 AIT class attended by PFC MANNING.

377. Memorandum For Record, containing the names of AIT instructors for class 243-35F10-027, signed by CW3 (b)(6)(b)(7)(C), dated 3 Feb 12.

378. Army Training Requirements and Resources System (ATRRS) R2 Data Report, Course 243-35F10-027, containing student names, dated 18 Jan 12.

379. AIR or SA (b)(6)(b)(7)(C) 15 Feb 12, detailing the coordination with SPC (b)(6)(b)(7)(C) and SGT (b)(6)(b)(7)(C) and receipt of the Joint Asset Movement Management System (JAMMS) detailing

PFC MANNING's movements between Iraq and Kuwait between 12 Oct 09 and 30 May 10.

380. JAMMS Movement Report by Person, detailing travel movements by PFC MANNING, dated 15 Feb 12.

381. AIR of SA [redacted] 27 Feb 12, detailing the interviews of Mr. [redacted] Mrs. [redacted] SGT [redacted] SSG [redacted] 1LT [redacted] SPC [redacted] and CW4 [redacted]

382. Student Evaluation Plan, Course 243-35F1O (V10), dated December 2007.

383. AIR of SA [redacted] 28 Feb 12, detailing the canvass interviews of Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmat [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted], Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted], Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] and Inmate [redacted] and interview of CPT [redacted]

384. Canvass Interview Worksheets of Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted], Inmate [redacted], Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted] Inmate [redacted], and CPT [redacted] undated.

385. AIR of SA [redacted] 28 Mar 12, detailing the coordination with CPT [redacted] and collection of 13 hard disk drives as evidence.

386. AIR of SSA [redacted] 18 Apr 12, detailing the forensic imaging of eight hard disk drives, and attempted forensic recovery of data from five hard disk drives.

387. AIR of SA [redacted] 31 Jul 12, (Classified ~~SECRET//ORCON/NOFORN)~~ detailing the coordination with MAJ [redacted] personnel from the National Media Exploitation Center (NMEC), and personnel from the FBI, in relation to specific items of digital media collected by the U.S. Government on 2 May 11; and the receipt of one DVD containing four files related to this investigation. (USACRC and File Copy Only)

388. AIR of Mr. [redacted] 2 Aug 12, detailing the forensic comparison of the files "afghan-war-diary.html[1814].7z" obtained from the FBI and "afg-war-diary.html.7z" obtained from the Information Review Task Force (IRTF).

389. AIR of SA [redacted] 31 Aug 12, (Classified ~~SECRET//ORCON/NOFORN)~~ detailing the examination of two electronic documents contained on a DVD provided by the FBI; and

coordination with CDR (b)(6)(b)(7)(C) to authenticate the two classified foreign language documents. (USACRC and File Copy Only)

390. Printed 16 page foreign language document (Classified ~~SECRET//ORCON/NOFORN~~) containing the initials of CDR (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) undated. (USACRC and File Copy Only)

391. Printed six page foreign language document (Classified ~~SECRET//ORCON/NOFORN~~) containing the initials of CDR (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) undated. (USACRC and File Copy Only)

392. AIR of SA (b)(6)(b)(7)(C) 13 Sep 12, detailing the coordination with MA1 (b)(6)(b)(7)(C) LCDR (b)(6)(b)(7)(C) MCPO (b)(6)(b)(7)(C) and CDR (b)(6)(b)(7)(C) pertaining to documentation of incidents related to PFC MANNING's confinement and items found at the Theater Field Confinement Facility, Camp Arifjan, Kuwait.

393. Sworn Statement of MA1 (b)(6)(b)(7)(C), dated 6 Sep 12.

394. Unsworn Statement of LCDR (b)(6)(b)(7)(C), dated 6 Sep 12.

395. Sworn Statement of MCPO (b)(6)(b)(7)(C) ated 6 Sep 12.

396. Sworn Statement of CDR (b)(6)(b)(7)(C) ated 6 Sep 12.

397. DD Form 2711, Initial Custody Classification pertaining to PFC MANNING, signed by CDR (b)(6)(b)(7)(C) dated 1 Jun 10.

398. DD Form 2713, Inmate Observation Report pertaining to PFC MANNING, prepared by LCDR (b)(6)(b)(7)(C) dated 2 Jun 10.

399. DD Form 2713, Inmate Observation Report pertaining to PFC MANNING, prepared by CPO (b)(6)(b)(7)(C) ated 2 Jun 10.

400. DD Form 2713, Inmate Observation Report pertaining to PFC MANNING, prepared by MCPO (b)(6)(b)(7)(C) dated 11 Jun 10.

401. DD Form 2711-1, Custody Reclassification pertaining to PFC MANNING, signed by CDR (b)(6)(b)(7)(C) dated 30 Jun 10.

402. Memorandum For Record, detailing Use of Force incident involving PFC MANNING, signed by CPO (b)(6)(b)(7)(C) dated 30 Jun 10.

403. DD Form 2713, Inmate Observation Report pertaining to PFC MANNING, prepared by LCDR (b)(6)(b)(7)(C) dated 28 Jul 10.

404. Memorandum For Record, detailing PFC MANNING's abnormal behavior while in custody, discovery of an improvised noose found in PFC MANNING's holding cell, and mental health evaluations provided by personnel from the Emergency Medical Facility Kuwait during PFC MANNING's confinement, signed by LCDR (b)(6)(b)(7)(C) dated 29 Jul 10.

405. Evidence Photograph of bed sheet tied in an apparent noose, undated.

406. Evidence Photograph of black nylon string, undated.

407. AIR of SA (b)(6)(b)(7)(C) 6 Nov 12, detailing the interviews of LCDR (b)(6)(b)(7)(C) PO1(Ret) (b)(6)(b)(7)(C) PO2 (b)(6)(b)(7)(C) CPO (b)(6)(b)(7)(C) CPO (b)(6)(b)(7)(C), and PO1 (b)(6)(b)(7)(C)

408. AIR of Mrs. (b)(6)(b)(7)(C) 15 Jan 13, detailing the collection of one green mattress, one blue mattress, one pillow, one suicide smock, and one blanket as evidence.

409. Statement in Support of Providence Inquiry -- U.S. v. Private First Class Bradley E. MANNING, dated 29 Jan 13.

410. Post Trial Confinement Packet of PFC MANNING, dated 21 Aug 13.

411. AIR of SA (b)(6)(b)(7)(C) 16 Sep 13, detailing receipt of Defense Reciprocal Discovery Documents, obtaining two Federal Magistrate Search Warrants related to the YouTube account of "bradmanning", execution of Search Warrants on Google, Inc., Search Warrant results, and collection of evidence.

412. Defense Reciprocal Discovery Documents, numbered 028711 through 028713, dated 29 May 13.

413. Federal Magistrate Search Warrant 1:13-SW-446 and Search Warrant results from Google, Inc.

414. Federal Magistrate Search Warrant 1:13-SW-492 and Search Warrant results from Google, Inc.

ATTACHED FORENSIC REPORTS:

415. Forensic Examination Report of SSA (b)(6)(b)(7)(C), 16 Jun 10, detailing the forensic examination of the forensic images of three Arabic language instruction CD's, property of PFC MANNING.

416. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the preliminary forensic examination of forensic image of a personal laptop computer, the property of SSG (b)(6)(b)(7)(C)

417. AIR of SA (b)(6)(b)(7)(C) 18 Jun 10, detailing the imaging of Mr (b)(6)(b)(7)(C) thumb drive, collection of evidence, and preliminary examination of the thumb drive.

418. AIR of SA (b)(6)(b)(7)(C) 24 Jun 10, detailing the preliminary forensic examination of the email account bradley.e.manning@gmail.com, used by PFC MANNING.

419. AIR of Mr. (b)(6)(b)(7)(C) (Classified ~~SECRET), 2~~ Jul 10, detailing the preliminary forensic examination of a Seagate hard disk drive, the property of PFC MANNING.

420. AIR of SSA (b)(6)(b)(7)(C) 21 Jul 10, detailing the preliminary forensic examination of two CD-R's and eight DVD-RW's, property of PFC MANNING.

421. AIR of SSA (b)(6)(b)(7)(C) 26 Jul 10, detailing the imaging of an IBM ThinkCentre desktop computer, the property of PFC MANNING.

422. AIR of SSA (b)(6)(b)(7)(C) Aug 10, detailing the collection of the file "insurance.aes.256" downloaded from the WikiLeaks.org website as evidence.

423. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 15 Sep 10, detailing the forensic examination of a NIPR computer used by PFC MANNING assigned IP address 144.107.17.139, the property of 2nd BCT, 10th MTN DIV.

424. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) dated 15 Sep 10. (USACRC and File Copy Only)

425. AIR of SSA (b)(6)(b)(7)(C) 17 Sep 10, detailing the imaging of a NIPR computer assigned IP address 147.198.178.143, the property of the Fort Drum Department of Information Management (DOIM).

426. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 20 Sep 10, detailing the forensic examination of a NIPR computer assigned IP address 147.198.178.143, the property of 2nd BCT, 10th MTN DIV.

427. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) dated 20 Sep 10. (USACRC and File Copy Only)

428. Forensic Examination Report of SA (b)(6)(b)(7)(C) 28 Sep 10, detailing the forensic examination of a US Government computer, formerly located in the Supply Annex, 2nd BCT,

10th MTN DIV.

429. DVD Containing Attachments to the Forensic Examination Report of SA (b)(6)(b)(7)(C) dated 28 Sep 10. (USACRC and File Copy Only)

430. AIR of SSA (b)(6)(b)(7)(C) 4 Oct 10, detailing the forensic imaging of a US Army computer assigned IP address 148.17.172.115, and US Army computer assigned IP address 22.225.28.54, both the property of 2nd BCT, 10th MTN DIV.

431. AIR of SSA (b)(6)(b)(7)(C) 27 Oct 10, detailing the imaging of one CD and one DVD containing Intelink data.

432. Forensic Examination Report of Mr. (b)(6)(b)(7)(C) 30 Oct 10, detailing the forensic examination of three NetApp arrays and domain controllers, the property of 2nd BCT, 10th MTN DIV.

433. AIR of Mr (b)(6)(b)(7)(C) 8 Nov 10, detailing the preliminary examination of an IBM ThinkCentre computer, the property of PFC MANNING.

434. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 12 Nov 10, detailing the forensic examination of the CIDNE-Iraq log files.

435. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 12 Nov 10, detailing the forensic examination of the CIDNE-Afghanistan log files.

436. AIR of SA (b)(6)(b)(7)(C) 30 Nov 10, detailing the website capture of a WikiLeaks website.

437. Defense Computer Forensics Laboratory Report of Mr. (b)(6)(b)(7)(C) 2 Dec 10, detailing efforts to decrypt the file "strongbox.dmg" created by PFC MANNING.

438. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 13 Dec 10, detailing the forensic examination of multiple digital media items collected from the (b)(6)(b)(7)(C) residence.

439. AIR of SSA (b)(6)(b)(7)(C) 3 Dec 10, detailing the forensic imaging of three SD memory cards, one Compact Flash memory card, one Smart Media memory card, nine CDs, and one USB memory card, the property of PFC MANNING.

440. AIR of Ms. (b)(6)(b)(7)(C) 11 Jan 11, detailing the forensic imaging of 36 Fujitsu hard disk drives, six SeaGate hard disk drives, and two unknown brand hard disk drives, the property of 2nd BCT, 10th MTN DIV.

441. AIR of SA (b)(6)(b)(7)(C) 12 Jan 11, detailing the forensic imaging of a Maxtor hard drive collected from the residence of Ms. (b)(6)(b)(7)(C) the property of PFC MANNING.

442. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 13 Jan 11, detailing the forensic examination of 44 hard drives, the property of 2nd BCT, 10th MTN DIV.

443. Forensic Examination Report of SA (b)(6)(b)(7)(C) 7 Feb 11, detailing the forensic examination of a CD-RW, the property of Mr. (b)(6)(b)(7)(C)

444. Forensic Examination Report of SA (b)(6)(b)(7)(C) 4 Mar 11, detailing the forensic examination of a hard disk drive collected from the residence of Ms. (b)(6)(b)(7)(C)

445. Forensic Examination Report of Mr. (b)(6)(b)(7)(C) 9 Mar 11, detailing the forensic examination of forensic images of hard disk drives, the property of FBI Protected Identity Witness.

446. DVD Containing Attachments to the Forensic Examination Report of Mr. (b)(6)(b)(7)(C) dated 9 Mar 11. (USACRC and File Copy Only)

447. Forensic Examination Report of SA (b)(6)(b)(7)(C) 10 Mar 11, detailing the forensic examination of a Subscriber Identity Module (SIM) card, the property of FBI Protected Identity Witness.

448. Forensic Examination Report of SA (b)(6)(b)(7)(C) 5 Apr 11, detailing the forensic examination of a computer, the property of Mr (b)(6)(b)(7)(C)

449. DVD Containing Attachments to the Forensic Examination Report of SA (b)(6)(b)(7)(C) dated 5 Apr 11. (USACRC and File Copy Only)

450. DVD Containing Attachments to the Forensic Examination Report of SA (b)(6)(b)(7)(C) dated 5 Apr 11. (USACRC and File Copy Only)

451. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 22 Apr 11, detailing the forensic examination of the JIEDDO server log files.

452. Forensic Examination Report of SA (b)(6)(b)(7)(C) 27 Jul 11, detailing the forensic examination of the Supply Section NIPR computer used by PFC MANNING assigned IP address 144.107.17.19, the property of 2nd BCT, 10th MTN DIV.

453. DVD Containing Attachments to the Forensic Examination Report of SA (b)(6)(b)(7)(C) dated 27 Jul 11. (USACRC and File Copy Only)

454. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 3 Aug 11, detailing the forensic examination of NIPR and SIPR log files collected from various network servers at FOB Hammer.

455. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 10 Aug 11, detailing the forensic examination of various network log files.

456. Forensic Examination Report of Mr. (b)(6)(b)(7)(C) (Classified ~~SECRET//REL~~ TO ACGU), 22 Sep 11, detailing the forensic examination of PFC MANNING's personally owned MacBook Pro laptop computer.

457. DVD Containing Attachments to the Forensic Examination Report of Mr. (b)(6)(b)(7)(C) (Classified ~~SECRET//REL~~ TO ACGU), dated 22 Sep 11. (USACRC and File Copy Only)

458. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of the primary SIPR computer used by PFC MANNING assigned IP address 22.225.41.22.

459. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

460. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of the secondary SIPR computer used by PFC MANNING assigned IP address 22.225.41.40.

461. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

462. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of an additional SIPR computer used by PFC MANNING assigned IP address 22.225.29.185.

463. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

464. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of a Secure Digital (SD) memory card collected at the residence of Ms. (b)(6)(b)(7)(C) the property of PFC MANNING.

465. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

466. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET~~), 22 Sep 11, detailing

the forensic examination of the (b)(6)(b)(7)(C) network folder on a U.S. Central Commander SIPR computer.

467. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET),~~ dated 22 Sep 11. (USACRC and File Copy Only)

468. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN),~~ 22 Sep 11, detailing the forensic examination of two hard disk drives previously contained in SIPR computers used by PFC MANNING assigned IP addresses 148.17.172.115 and 22.225.28.54.

469. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN),~~ dated 22 Sep 11. (USACRC and File Copy Only)

470. Forensic Examination Report of Mr. (b)(6)(b)(7)(C) (Classified ~~SECRET),~~ 22 Sep 11, detailing the forensic examination of the personally owned hard disk drive of PFC MANNING.

471. DVD Containing Attachments to the Forensic Examination Report of Mr. (b)(6)(b)(7)(C) (Classified ~~SECRET),~~ dated 22 Sep 11. (USACRC and File Copy Only)

472. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 22 Sep 11, detailing the forensic examination of a SIPR computer used by SPC (b)(6)(b)(7)(C) assigned IP address 22.225.28.216, the property of 2nd BCT, 10th MTN DIV.

473. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) dated 22 Sep 11. (USACRC and File Copy Only)

474. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN),~~ 22 Sep 11, detailing the forensic examination of the SIPR network share folder assigned to PFC MANNING, and the SIPR network share folder assigned to the 2nd BCT, 10th MTN DIV Office of the Staff Judge Advocate.

475. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN),~~ dated 22 Sep 11. (USACRC and File Copy Only)

476. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN),~~ 22 Sep 11, detailing the forensic examinations conducted in relation to an Army Counter Intelligence Center (ACIC) report, dated 28 Feb 08, titled, "(U) WikiLeaks.org An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?".

477. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN),~~ dated 22 Sep 11. (USACRC and File Copy Only)

478. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET~~), 22 Sep 11, detailing the forensic examinations of Centaur logs containing network traffic for U.S. Army SIPR computers used by PFC MANNING assigned IP addresses 22.225.41.22, 22.225.41.40, and 22.225.29.185.

479. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET~~), dated 22 Sep 11. (USACRC and File Copy Only)

480. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examinations conducted of U.S. Department of State documents, computer logs, and network logs in relation to two SIPR computers used by PFC MANNING assigned IP addresses 22.225.41.22 and 22.225.41.40.

481. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

482. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of documents collected from WikiLeaks.ch pertaining to Guantanamo Bay detainees.

483. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

484. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of SIPR Intelink log files pertaining to SIPR computers used by PFC MANNING assigned IP addresses 22.225.41.22 and 22.225.41.40.

485. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

486. Forensic Examination Report of SSA (b)(6)(b)(7)(C) Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of two hard disk drives, the property of Mr. (b)(6)(b)(7)(C) containing online chat conversations between PFC MANNING and Mr. (b)(6)(b)(7)(C)

487. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

488. Forensic Examination Report of SSA (b)(6)(b)(7)(C) Classified ~~SECRET//NOFORN~~), 22 Sep 11, detailing the forensic examination of CIDNE reports collected from the WikiLeaks.org website.

489. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C)

(Classified ~~SECRET//NOFORN~~), dated 22 Sep 11. (USACRC and File Copy Only)

490. Forensic Examination Report of SSA (b)(6)(b)(7)(C), 22 Sep 11, detailing the forensic examination of a rewritable Compact Disc (CD-RW) marked ~~"SECRET"~~ and recovered from the personal living quarters of PFC MANNING on FOB Hammer, Iraq.

491. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C), dated 22 Sep 11. (USACRC and File Copy Only)

492. Forensic Examination Report of SSA (b)(6)(b)(7)(C), 20 Oct 11 (Classified ~~SECRET//ORCON/NOFORN~~), detailing the forensic examinations conducted in relation to access to systems and information of a U.S. Intelligence Agency. (USACRC and File Copy Only)

493. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//ORCON/NOFORN~~), dated 20 Oct 11. (USACRC and File Copy Only)

494. AIR of SSA (b)(6)(b)(7)(C), 9 Dec 11, detailing the forensic examination of the file "b.zip" identified on a Brookhaven National Laboratory computer previously assigned to Mr (b)(6)(b)(7)(C) and the file "BE22 PAX.zip" identified on a SIPR computer previously used by PFC MANNING.

495. Forensic Examination Report of SSA (b)(6)(b)(7)(C) 4 Jan 12, detailing the forensic examination of the NIPR and SIPR PST (email archive) files of the account "bradley.manning".

496. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), 2 Feb 12, detailing the forensic examination of digital media collected from a member of the organization Hezb-e Islami Gulbuddin (HIG), in Parwan Province, Afghanistan, in relation to classified documents released by the WikiLeaks.org website.

497. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET//NOFORN~~), dated 2 Feb 12. (USACRC and File Only)

498. AIR of SSA (b)(6)(b)(7)(C) 18 Apr 12, detailing the forensic imaging of eight hard disk drives and attempts to obtain forensic images from five hard disk drives collected from 2nd BCT, 10th MTN DIV at Fort Drum, NY.

499. AIR of Mr. (b)(6)(b)(7)(C) 18 Apr 12, detailing forensic assistance in relation to a Military Court Order to search hard disk drives collected from the Temporary-SCIF (T-SCIF) and Tactical Operations Center (TOC) for certain Defense Counsel requested software applications and computer files.

500. AIR of SSA (b)(6)(b)(7)(C) 20 Jun 12, detailing the forensic imaging of a CD containing network log files provided by the Defense Information Systems Agency (DISA).

501. Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET~~), 22 Jun 12, detailing the forensic examination of Centaur logs containing network traffic from the U.S. Army computers used by PFC MANNING assigned the IP addresses 22.225.41.22, 22.225.41.40, and 22.225.29.185.

502. DVD Containing Attachments to the Forensic Examination Report of SSA (b)(6)(b)(7)(C) (Classified ~~SECRET~~), dated 22 Jun 12. (USACRC and File Copy Only)

503. (503-1 through 503-119) DA Form 4137, Evidence/Property Custody Document (EPCD), Document Number (DN) 066-10 (0577-10), 067-10 (0579-10), 068-10 (0580-10), 069-10 (0581-10), 070-10 (0582-10), 071-10 (0583-10), 072-10 (0584-10), 073-10 (0585-10), 075-10, 076-10, 077-10, 078-10, 079-10, 082-10, 083-10, 084-10, 085-10, 086-10, 087-10, 089-10, 091-10, 092-10, 095-10, 098-10 (0594-10), 099-10 (0592-10), 100-10 (0593-10), 101-10 (579-10), 102-10 (0578-10), 103-10, 106-10, 108-10, 109-10, 110-10 (0735-10), 111-10 (0734-10), 113-10, 114-10, 117-10, 118-10, 119-10, 120-10, 122-10, 123-10, 124-10, 131-10, 132-10, 133-10, 134-10, 135-10, 136-10 (139-10), 139-10, 144-10, 145-10, 146-10, 147-10, 148-10, 151-10, 153-10, 154-10, 160-10, 161-10, 162-10, 164-10, 165-10, 166-10, 167-10, 169-10, 170-10, 172-10, 175-10, 177-10, 184-10, 187-10, 188-10, 190-10, 192-10, 193-10, 001-11, 002-11, 004-11, 005-11, 008-11, 009-11, 010-11, 013-11, 019-11, 020-11, 021-11, 023-11, 030-11, 044-11, 045-11, 051-11, 053-11, 060-11, 062-11, 070-11, 088-11, 095-11, 099-11, 132-11, 134-11, 135-11, 137-11, 149-11, 163-11, 167-11, 179-11, 183-11, 185-11, 002-12, 011-12, 013-12, 036-12, 061-12, 068-12, 115-12, 063-13, 075-13, and 099-13.

504. DA Form 4137, EPCD, DN 152-10 (Classified: ~~SECRET//NOFORN~~). (USACRC and File Copy Only)

505. DVD Containing a copy of the FOIA released Record of Trial.

NOT ATTACHED:

None.

The originals of Exhibits 1 through 5, 7 through 28, 30 through 32, 34, 42 through 48, 51 through 56, 60, 61, 66 through 76, 83, 84, 86 through 93, 95 through 105, 109 through 115, 120, 121, 125 through 128, 130 through 142, 148 through 152, 154 through 161, 164, 165, 169 through 185, 187 through 197, 200 through 208, 224 through 238, 240 through 244, 246, 247, 249, 250, 252 through 261, 263, 264, 266 through 309, 312 through 333, 335 through 348, 350 through 356, 358 through 381, 383 through 408, 411, and 415 through 502 are maintained in the files of Headquarters, CCIU, Quantico, VA. The originals of Exhibits 6, 122 and 123, are retained in the files of the 2nd Brigade Combat Team, 10th Mountain Division, Fort Drum, NY. The originals of Exhibits 29, 33, 35 through 40, 49, 50, 57 through 59, 62 through 64, 78 through 81, 94, and 108

are retained in the files of the U.S. Army Intelligence and Security Command (INSCOM), Fort Belvoir, VA. The originals of Exhibits 41, 65, 334 and 349 are retained in the files of the Defense Intelligence Agency (DIA), Joint Base Anacostia-Bolling, Washington, DC. The originals of Exhibit 77 is retained in the files of the Office of Personnel Management (OPM), Boyers, PA. The originals of Exhibit 82 is retained in the files of Headquarters, 1st Armored Division, Fort Bliss, TX. The originals of Exhibit 85 is retained in the files of the Clerk of the Court, United States District Court for the District of Columbia, Washington, DC. The originals of Exhibits 106, 251, 262, 310, 311, 357, 413, and 414 are retained in the files of the Clerk of the Court, United States District Court for the Eastern District of Virginia, Alexandria, VA. The original of Exhibit 107 is retained in the files of U.S. Forces-Iraq. The originals of Exhibits 116 through 119, 124, 129, 143 through 147, 153, 162, 163, 166 through 168, 186, 209 through 222, 239, 245, and 248 are retained in the files of the Federal Bureau of Investigation, Washington Field Office, Washington, DC. The original of Exhibit 223 is retained in the files of the Clerk of the Court, United States District Court for the Eastern District of New York, Brooklyn, NY. The original of Exhibit 265 is retained in the files of the Staff Judge Advocate for the Military District of Washington, Fort McNair, DC. The original of Exhibit 382 is retained in the files of the U.S. Army Intelligence Center, Fort Huachuca, AZ. The originals of Exhibits 409, 410, 412, and 505 are retained in the files of The Clerk of Court, U.S. Army Court of Criminal Appeals, Fort Belvoir, VA. The originals of Exhibits 198 and 199 are retained in the Evidence Depository, Headquarters, CCIU, Quantico, VA. The originals of Exhibits 503 and 504 are retained in the files of the Evidence Depository, Headquarters, CCIU, Quantico, VA.

STATUS: This is a Final Report. On 30 Jul 13, pursuant to General Court-Martial proceedings, a Military Court found PFC MANNING: not guilty of the offense of Article 104, Aiding the Enemy; guilty of committing multiple offenses of Article 134 (18 USC § 641, 18 USC § 793(e), and 18 USC § 1030(a)(1)); not guilty of one offense of Article 134 (18 USC § 793(e)); and accepted PFC MANNING's plea of guilty for lesser included offenses of Article 134. On 21 Aug 13, PFC MANNING was sentenced to 35 years confinement, reduction to the grade of E-1, forfeiture of all pay and allowances, and a Dishonorable Discharge from the U.S. Army. On 10 Apr 14, the General Court Martial Convening Authority approved the sentence.

CID Reports of Investigation may be subject to a Quality Assurance review by CID higher headquarters.

REPORT PREPARED BY:

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

Special Agent

REPORT APPROVED BY:

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

Operations Officer

DISTRIBUTION:
Director, U.S. Army Crime Records Center, Quantico, VA 22134 (Original)
Commander, USACIDC, ATTN: CIOP-CO, Quantico, VA 22134 (E-mail)
Commander, USACIDC, ATTN: CIOP-IN-FW, Quantico, VA 22134 (E-mail)
Commander, 701st MP Group, U.S. Army CID, Quantico, VA 22134 (E-mail)
Director, Computer Crime Investigative Unit, Quantico, VA 22134 (E-mail)
Commander, U.S. Army Military District of Washington, Fort McNair, DC 20319 (E-mail)
Office of the Staff Judge Advocate, Fort McNair, DC 20319 (E-mail)
U.S. Attorney's Office, Eastern District of Virginia, Alexandria, VA 22314 (E-mail)
Special Agent in Charge, FBI, Washington Field Office, Washington, DC 20535 (E-mail)
Special Agent in Charge, DSS, Arlington, VA 22209 (E-mail)
Inspector General, Department of Defense, Arlington, VA 22202 (E-mail)
File

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

On 25 May 10, this office received an email sent by a Non-Governmental Organization named Project Vigilant. The email advised a member of the Project Vigilant organization had come across information of national security importance and attached a document which provided additional details. In the attached document the unidentified Project Vigilant member stated he had come into contact with an enlisted U.S. Army Intelligence Analyst, later identified as PFC MANNING, who was stationed in Baghdad, Iraq; and that this individual reportedly released sensitive data, and was planning to release additional sensitive data, all of which may have been derived from classified material. The document related the information was leaked to an unnamed Australian National, later identified as Mr. Julian P. ASSANGE, founder and Director of WikiLeaks, Townsville, Queensland, AU, who reportedly worked for the website WikiLeaks.org.

About 0900, 2 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Europe Branch Office, Computer Crime Investigative Unit (CCIU), Manheim, GE, coordinated with CPT (b)(6)(b)(7)(C) Brigade Automation Officer, S6, Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq, APO AE 09308, who related the FOB Hammer network contained a large Secure Internet Protocol Router (SIPR) Storage Area Network (SAN), over 10 TB, which was essentially handed down from one deployed BCT to another. CPT (b)(6)(b)(7)(C) related the current security settings for the Brigade Legal Team's data share located on FOB Hammer SIPR SAN were set to restricted; however, this setting had been changed sometime between 27 Apr 10 and 20 May 10. CPT (b)(6)(b)(7)(C) related prior to this time frame the aforementioned data share had unrestricted settings. CPT (b)(6)(b)(7)(C) related the classified SECRET video in question could be found in three locations on the FOB Hammer SIPR SAN: the Brigade Legal Team's data share; the 431st Infantry LNO's data share; and the 382nd Archived Training Material data share.

//LAST ENTRY//

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 2 Jun 10	EXHIBIT 1

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

DETAILS

BASIS FOR INVESTIGATION: About 1100, 27 May 10, this office was notified by the 11th MP BN (CID) (FWD), Victory Base Complex, Iraq, APO AE 09342 (VBC), of unauthorized sensitive information obtained and released by PFC MANNING.

Agent's Comment: (b) (7)(D) PFC MANNING (b) (7)(D) (b) (7)(D) (b) (7)(D) PFC MANNING (b) (7)(D) (b) (7)(D) (b) (7)(D) PFC MANNING also claimed he was a source for Mr Julian ASSANGE, director of WikiLeaks.com (NFI); an organization that publishes anonymous submissions and leaks of sensitive documents from governments and other organization and is dedicated to exposing government secrets. (b) (7)(D) (b) (7)(D) (b) (7)(D)

About 1400, 27 May 10, SA (b)(6)(b)(7)(C) briefed CPT (b)(6)(b)(7)(C), Military Magistrate, Office of the Staff Judge Advocate (OSJA), United States Division-Central (USD-C), Camp Liberty, APO AE 09342, on the current facts and circumstances of the investigation. CPT (b)(6)(b)(7)(C) provided Search and Seizure Authorization for this office to seize all personal computers and media storage devices belonging to PFC MANNING, any papers annotating passwords, and the assigned work terminals of PFC MANNING.

About 2000, 27 May 10, SA (b)(6)(b)(7)(C), SA (b)(6)(b)(7)(C), SA (b)(6)(b)(7)(C), both of this office, and SA (b)(6)(b)(7)(C) Counter Intelligence, 202nd Military Intelligence Battalion, VBC; briefed LTC (b)(6)(b)(7)(C) Brigade (BG) Executive Officer, MAJ (b)(6)(b)(7)(C) BG OSJA, CPT (b)(6)(b)(7)(C) OSJA, and CPT (b)(6)(b)(7)(C) S2 Section OIC, all of 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, APO AE 09308 (2/10th MTN), on certain facts and circumstances regarding this investigation. The unit members were provided an investigative plan on what activities this office currently needed to conduct and possible additional activities.

Between 2100-2300, 27 May 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) conducted canvass interviews of the Soldiers assigned to the Secret Compartmentalized Information Facility (SCIF), 2/10th MTN (PFC MANNING's assigned section prior to 8 May 10). The following questions were asked:

- Do you know MANNING?

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 2

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0160-10-CID899-14463

DETAILS

- Do you work with MANNING?
- What does he do on work & off work?
- Do you socialize with MANNING outside of work?
- Who does MANNING socialized with outside of work?
- Do you know what MANNING searched on the computer at work?
- Which work station MANNING worked at?
- Do you know if MANNING had any accidental disclosures?
- Do you if MANNING attempted to work by himself in the SCIF?

A majority of the Soldiers knew PFC MANNING; however, did not know much about him. PFC MANNING was considered a quiet person who did not socialize. He was an Intelligence Analyst and it was unknown if he had any accidental disclosures. The following individuals were identified as needing to be interviewed; CPT (b)(6)(b)(7)(C) and CPT (b)(6)(b)(7)(C) S2, 2/10th MTN.

About 2146, 27 May 10, SA (b)(6)(b)(7)(C) advised PFC MANNING of his legal rights, which he invoked requesting a lawyer.

About 2215, 27 May 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C) Supply NCOIC, HHC, 2/10th MTN DIV, who stated PFC MANNING was transferred to the Supply Office working directly his supervision about two-three weeks ago (beginning of May 10 sometime). SSG (b)(6)(b)(7)(C) stated this occurred because PFC MANNING received an Article 15 after he assaulted (punched in the face) SPC (b)(6)(b)(7)(C) S2, HHC, 2/10th MTN DIV, over a work issue. SSG (b)(6)(b)(7)(C) stated for the last couple weeks, since PFC MANNING has been assigned to the supply office, PFC MANNING has only used the two computers in the supply office. SSG (b)(6)(b)(7)(C) further related CPT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) CDR, HHC, 2/10th MTN DIV, was PFC MANNING's commander and was the property book holder for all the computers assigned to the BG TOC and Supply Annex (which includes the S2 and to the supply room).

About 2230, 27 May 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) who provided a copy of PFC MANNING's Company Grade Article 15, completed on 17 May 10. The Article 15 detailed on 8 May 10 PFC MANNING assaulted his female team leader, while in the SCIF. SPC MANNING invoked his legal rights requesting a lawyer and to remain silent. Results of Article 15: reduction in rank to E3, forfeiture of $446. PFC MANNING was also referred to mental health for an evaluation, his Top Secret clearance was temporarily revoked and he was re-assigned to the Supply Office.

About 2240, 27 May 10, SA (b)(6)(b)(7)(C) briefed CPT (b)(6)(b)(7)(C) on the outcome of the interview of PFC MANNING and notified CPT (b)(6)(b)(7)(C) there were reasons to believe PFC MANNING was suicidal in nature. SA (b)(6)(b)(7)(C) also briefed CPT (b)(6)(b)(7)(C) on certain facts and circumstances regarding the investigation and requested he provide Commander's Authorization to Search and Seizure of all computers PFC

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 2

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

DETAILS

MANNING was known to work on, which were not actually assigned to him, and to conduct a forensic examination of those computers collected. CPT (b)(6)(b)(7)(C) provided his Commander's Search Authorization and signed the computers release. The computers identified were the NIPR communal laptop in the S2 Section and the two computers in the supply office.

Between 2245 and 2330, 27 May 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) conducted a Crime Scene Examination of the SCIF, Room 14B, Brigade Headquarters Building, 2/10th MTN DIV.

About 0001, 28 May 10, SA (b)(6)(b)(7)(C) interviewed SPC (b)(6)(b)(7)(C) MP, HHC, 2/10th MTN DIV, who identified himself as PFC MANNING's roommate. SPC (b)(6)(b)(7)(C) provided SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) with a walk-through of his and PFC MANNING's living area to determine what property was his and what was PFC MANNING's. SPC (b)(6)(b)(7)(C) stated he had been PFC MANNING's roommate since the beginning of the deployment. He related he and PFC MANNING rarely spoke, but were often in the room at the same time, as they work similar hours. SPC (b)(6)(b)(7)(C) stated PFC MANNING spent his off time on his computer, which was always facing away from SPC (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) stated sometimes he would wake up in the middle of the night and PFC MANNING would still be on his computer; mostly typing. He related in Jan 10, PFC MANNING went on block leave and took several items home with him; however, SPC (b)(6)(b)(7)(C) could not remember what exactly, possibly his IPod. SPC (b)(6)(b)(7)(C) further stated PFC MANNING rarely mailed boxes, however, at the end of Apr 10, he mailed three boxes. SPC (b)(6)(b)(7)(C) did not know where or to whom.

Between 0030 and 0150, 28 May 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) conducted a Crime Scene Examination of PFC MANNINGS Containerized Housing Unit (CHU), (b)(6)(b)(7)(C) LSA Dragon.

About 0053, 28 May 10, SA (b)(6)(b)(7)(C) released PFC MANNING to 1SG (b)(6)(b)(7)(C) HHC, 2/10th MTN DIV.

About 1010, 28 May 10, SA (b)(6)(b)(7)(C) interviewed CPT (b)(6)(b)(7)(C) OIC, S6 Section, HHC, 2/10th MTN DIV, who related the only way to identify each computer accessed by PFC MANNING would be to log into each and attempt to pull up his profile. Further, SA (b)(6)(b)(7)(C) telephonically spoke with SA (b)(6)(b)(7)(C) Computer Crime Investigative Unit (CCIU), Manheim, Germany, who requested CPT (b)(6)(b)(7)(C) obtain Network Logs for all of PFC MANNING's assigned computers or ones identified which he accessed.

Between 1100-1300, 28 May 10, SA (b)(6)(b)(7)(C) conducted additional canvass interviews of the unit personal. The following individuals were identified as needing to be interviewed PFC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) 2/10th MTN.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 2

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

DETAILS

About 1140, 28 May 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C) who related he dropped off the two laptop computers maintained with the supply office to S6 to have the original hard drives removed. SA (b)(6)(b)(7)(C) collected the two original hard drives, which were removed from the two laptop computers in the supply office, as evidence from SSG (b)(6)(b)(7)(C) on EPCD, DN 0580-10.

About 1200, 28 May 10, SSG (b)(6)(b)(7)(C) further stated he had let PFC MANNING use his personal laptop on occasion within the last three weeks. SSG (b)(6)(b)(7)(C) provided Consent to Search for this office to collect his personal laptop as evidence and to conduct a forensic examination.

About 1202, 28 May 10, SSG (b)(6)(b)(7)(C) provided this office with Consent to Search Computer Electronic Equipment for the forensic examination of his laptop.

About 1210, 28 May 10, SA (b)(6)(b)(7)(C) collected two CD's containing the Application, Security and System Network logs for all of 2/10th MTN DIV servers from PFC (b)(6)(b)(7)(C) Help Desk Technician, S6, 2/10th MNT DIV, as evidence on EPCD, DN 0578-10.

About 1220, 28 May 10, SA (b)(6)(b)(7)(C) collected SSG (b)(6)(b)(7)(C) HP personal laptop computer as evidence on a DA Form 4137, Evidence Property Custody Document (EPCD), Document Number (DN) 0592-10.

About 1505, 28 May 10, SA (b)(6)(b)(7)(C) interviewed CPT (b)(6)(b)(7)(C) who stated when she returned from block leave, Apr 10, time frame she had heard of the Apache Video being released to WikiLeaks.com. CPT (b)(6)(b)(7)(C) stated on 25 Apr 10, PFC MANNING came to her, at work, and asked her if she had seen it and told her he believed it looked like the actual video. CPT (b)(6)(b)(7)(C) related to PFC MANNING she didn't believe it was the real video, so PFC MANNING forwarded her the actual video from the SIPR share drive at 1922, 25 Apr 10, for her to compare. CPT (b)(6)(b)(7)(C) stated PFC MANNING did not appear to be overly excited about the video or act smug in anyway.

About 1518, 28 May 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) who provided Consent to Search Computer/Electronic Equipment for the forensic examination of the computers and hard drive collected from his property book.

About 1550, 28 May 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C) NCOIC, FOB Hammer Post Office, who related this office required a search authorization in order to view any personal postal documents. SSG (b)(6)(b)(7)(C) further stated this office should request to view the PS Form 297-A, Customs Declaration and Dispatch notes, which identified the individual mailing the package, the packages' contents, and the recipients address. SSG (b)(6)(b)(7)(C) stated the certified mail subs would also be attached if the package was mailed insured, registered, or certified. SSG (b)(6)(b)(7)(C) explained how all packages were inspected

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 2

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0160-10-CID899-14463

DETAILS

and search for HAZMAT and other items not shippable by USPS standards. He stated the mail clerks would inspect each package; however, only looked for items prohibited for mail.

About 1600, 28 May 10, SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) Manager, Netgate Internet Services, FOB Hammer, who related there was no way to track how much data a customer has uploaded or downloaded. Mr. (b)(6)(b)(7)(C) stated that customers pay monthly and are not restricted to their amount of internet usage.

About 1610, 28 May 10, SA (b)(6)(b)(7)(C) briefed CPT (b)(6)(b)(7)(C) Magistrate, on the current facts and circumstances regarding this office's desire to search the Post Office's Customs Forms. CPT (b)(6)(b)(7)(C) provided Search Authorization for the search of all PS Form 297-A's within the last 60 days.

About 1625, 28 May 10, SA (b)(6)(b)(7)(C) submitted the Search and Seizure Authorization to SSG (b)(6)(b)(7)(C)

Between 1630-1750, 28 May 10, SA (b)(6)(b)(7)(C), SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) executed the Search Authorization to search the PS Form 297-A's forms maintained at FOB Hammer Post Office, which met with negative results. The custom forms search only extended from 30 Apr-28 May 10 and all forms were carbon copies, which were difficult to read and many were completely illegible. SSG (b)(6)(b)(7)(C) stated they had just burned a few stacks yesterday and were only required to keep the forms for 30 days.

About 2112, 28 May 10, SA (b)(6)(b)(7)(C) interviewed SPC (b)(6)(b)(7)(C) who provided a sworn statement detailing his living experience with PFC MANNING as his roommate and PFC MANNING's day to day living patterns.

About 2141, 28 May 10, SA (b)(6)(b)(7)(C) interviewed and obtained a statement from SPC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Paralegal, 2/10th MTN DIV, who related PFC MANNING had previously used her SIPR scanner to scan unknown documents and send them to her computer. PFC MANNING then requested SPC (b)(6)(b)(7)(C) print the documents and erase the scans. SPC (b)(6)(b)(7)(C) further stated PFC MANNING had related he was instructed to scan the documents by SSG (b)(6)(b)(7)(C)

About 2230, 28 May 10, SA (b)(6)(b)(7)(C) interviewed and obtained a statement from SSG (b)(6)(b)(7)(C) wherein he related he never instructed PFC MANNING to use the SIPR scanner. Further, SSG (b)(6)(b)(7)(C) stated while PFC MANNING was assigned to the Supply Section he did not conduct any activity in which he would require use of the SIPR scanner.

About 2235, 28 May 10, SA (b)(6)(b)(7)(C) obtained a Commander's Authorization to Search from CPT (b)(6)(b)(7)(C) to collect SPC (b)(6)(b)(7)(C) hard drive.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 2

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0160-10-CID899-14463

DETAILS

About 2258, 28 May 10, SA (b)(6)(b)(7)(C) interviewed PFC (b)(6)(b)(7)(C) who provided a sworn statement, wherein he stated he once had a conversation with PFC MANNING pertaining to passwords and hash marks, but there was no discussion about hacking during any of their conversations.

About 2310, 28 May 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C) who arranged with the S6 to have the original hard drive from SPC (b)(6)(b)(7)(C) SIPR computer extracted. SA (b)(6)(b)(7)(C) collected the hard drive from SSG (b)(6)(b)(7)(C) as evidence on an EPCD, DN 0582-10.

About 1054, 29 May 10, SA (b)(6)(b)(7)(C) drafted an affidavit in support of the unit decision to request pre-trail confinement for SPC MANNING.

About 1700, 29 May 10, SA (b)(6)(b)(7)(C) was contacted by CPT (b)(6)(b)(7)(C) who related the night prior PFC MANNING allegedly used SPC (b)(6)(b)(7)(C) computer to check his emails.

About 1750, 29 May 10, SA (b)(6)(b)(7)(C) interviewed SPC (b)(6)(b)(7)(C) Public Affairs Office, HHC, 2/10th MTN DIV, who stated during the day before PFC MANNING requested her to stop by his room at 2130 that evening. When she did she saw PFC MANNING was being guarded by two Soldiers from the unit's Commander's Security Team (CST): PFC (b)(6)(b)(7)(C) and PFC (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SPC (b)(6)(b)(7)(C) related she assumed PFC MANNING was been guarded because of his previous Article 15. SPC (b)(6)(b)(7)(C) stated she entered the room wherein PFC MANNING provided her with a small piece of paper containing his Gmail email account user names and passwords and yahoo stocks information in order for her to check his Gmail inbox and the current price of his stocks. SPC (b)(6)(b)(7)(C) stated she then returned to her room where she used her personal computer to check his email and stocks. SPC (b)(6)(b)(7)(C) related she wrote down the current price of his stocks and the fact he had five new messages: three from an (b)(6)(b)(7)(C) (NFI) and two others which she was not able to remember. SPC (b)(6)(b)(7)(C) stated she then returned to PFC MANNING's room and provided him with the paper. SPC (b)(6)(b)(7)(C) tated at no time did she send any emails for PFC MANNING, delete any emails from his account, nor did he use her computer.

About 1830, 29 May 10, SA (b)(6)(b)(7)(C) interviewed PFC (b)(6)(b)(7)(C) who stated he and SPC (b)(6)(b)(7)(C) where assigned to guard PFC MANNING the evening of 28 May 10. PFC (b)(6)(b)(7)(C) stated approximately 2130, SPC (b)(6)(b)(7)(C) entered the room wherein PFC MANNING passed her a piece of paper the size of an index card containing his email username and password. PFC (b)(6)(b)(7)(C) tated a few minutes later SPC (b)(6)(b)(7)(C) eturned to the room and passed the piece of paper back to PFC MANNING with a few more sentences written on it. PFC (b)(6)(b)(7)(C) stated PFC MANNING was never allowed to access a computer; although, he never actually saw what was written on the paper.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 2

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER: 0160-10-CID899-14463

DETAILS

About 1330, 30 May 10, SA (b)(6)(b)(7)(C) briefed CPT (b)(6)(b)(7)(C) CPT (b)(6)(b)(7)(C) Trial counsel, USD-C, OSJA, and CPT (b)(6)(b)(7)(C) Chief of Justice, USD-C, OSJA, on the investigation. CPT (b)(6)(b)(7)(C) related PFC MANNING had been approved and placed into pre-trial confinement. The OSJA team planned to prefer charges against PFC MANNING within two weeks if possible, all dependent on the status of the forensic examination. OSJA team was also briefed by SA (b)(6)(b)(7)(C) CCIU, on the process and procedures of the CCIU examinations.

Between 1755, 30 May 10 - 0300, 1 Jun 10, SA (b)(6)(b)(7)(C) extracted the hard drives from the two SIPR and one NIPR computers collected from the SCIF, the personal laptop of SSG (b)(6)(b)(7)(C) and the personal external hard drive of PFC MANNING. The reason for the extraction was documented with a Memorandum for Record and the removed hard drives were collected as evidence on EPCD, DN: 0577-10, 0584-10, 0583-10, and 0581-10.

About 1040, 31 May 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) who provided the Search and Seizure Authorization for the forensic examination of the items seized during the execution of his original Search Authorization dated 27 May 10.

About 2330, 31 May 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) CDR, HHC, 2/10th MTN DIV, and provided him with the written affidavit for the previously granted Commander's Authorization to Search from 27&28 May 10, for the collection and forensic examination of several HHC computer and hard drives. CPT (b)(6)(b)(7)(C) provided Commander's Search and Seizure Authorization specifically for the forensic examination of those seized computers and hard drives.

About 1300, 5 Jun 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C) who provided the Search and Seizure Authorization for the forensic examination of the all items seized by this office 27-28 May 10, during the course of the investigation.

///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
(b)(6)(b)(7)(C)	DATE: 5 Jun 10	EXHIBIT: 2

SEARCH AND SEIZURE AUTHORIZATION

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

TO: *(Name and Organization of the person to whom authorization is given)*
Special Agent (b)(6)(b)(7)(C), (b) (7)(E) Central Baghdad CID Office, 25th MP Det (CID), 11th MP BN (CID), Camp Liberty, APO AE 09342

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

Central Baghdad CID Office, 25th MP Det (CID), Camp Liberty, APO AE 09342
(Organization or Address of Affiant)

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

PFC MANNING, his current residence, any personal storage locations, and past/current assigned work areas on FOB Hammer

for the property described as All personal computers, electronic media storage devices (to include, but not limited to: CD's, DVD's VHS tapes, flash/thumb drives, hard drives, removable disk drives, itouchs, iphones, playstation and xbox systems, etc...), papers annotating passwords to access restricted files, and documents with classified marking, and all assigned NIPR/SIPR computers.

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

Evidence Custodian, 11th MP BN (CID), Camp Arifjan, APO AE 09342
(Name and Organization of Authorized Custodian)

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

Dated this 27 day of May , 2010 .

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL	DUTY POSITION OF AUTHORIZING OFFICIAL
CPT (b)(6)(b)(7)(C) JA	Military Magistrate
ORGANIZATION OF AUTHORIZING OFFICIAL Office of the Staff Judge Advocate Camp Liberty, APO AE 09342	SIGNATURE OF AUTHORIZING OFFICIAL (b)(6)(b)(7)(C)

DA FORM 3745, SEP 2002 DA FORM 3745-R, MA APD PE v1.02ES

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

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

I, Special Agent, (b)(6)(b)(7)(C) of the 25th Military Police Detachment (CID), Central Baghdad CID Office, Camp Liberty, Iraq, been first duly sworn, hereby depose and state as follows:

1. Introduction and Background:

a. I make this affidavit in support of an application for authorization to search and seize the personal and U.S. Government owned computers and storage devices owned and used by PVT Bradley E. Manning, and to search the hard drives and other assorted media owned and used by PVT Manning. As set forth, herein, there is probable cause to believe that inside the aforementioned digital media there exists communications that will establish PVT Manning committed the offense of Espionage.

b. I am a Special Agent with the 25th Military Police Detachment (CID) of the U.S. Army Criminal Investigation Command, located on Camp Liberty, Iraq, and have been employed as a Special Agent for approximately 5 years. In addition to my training as a criminal investigator, I have attended various seminars, schools, and training on criminal investigation techniques and procedure.

c. I have attended seminars and training programs on computer and telecommunications investigations instructed by the Military Police School, Fort Leonard Wood, MO. In addition to the training I have received, I have participated in numerous investigations involving the use of computers in criminal activity. As a Special Agent of the U.S. Army Criminal Investigation Command, I am authorized to investigate crimes involving violations of the Uniform Code of Military Justice and other applicable federal and state laws where there is an Army interest.

2. Search Procedure - Methods To Be Used To Search Computers

a. Based upon my training and experience, I am familiar with the means by which individuals use computers and information networks such as the Internet to commit various criminal offenses. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to search the hard drives and storable devices. In addition, the information contained in this affidavit is based upon conversations with other law enforcement officers, my review of various documents and records, and my personal observation and knowledge. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part only.

b. Based on my training, my experience, and through conversations with other law enforcement agents, I know that searching for computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately conduct the search by retrieving the system's data in a laboratory or other controlled environment. This is true for the following reasons:

(1) The volume of evidence. Computer storage devices can store the equivalent of thousands of pages of information. In addition, a user may seek to conceal evidence of criminal activity by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This sorting process can take weeks or months, depending upon the volume of data stored, and it would be impractical to attempt this kind of data analysis "on-site."

(2) Technical requirements. Analyzing computer systems—to include those found within pagers, wireless phones, electronic organizers, data watches and desktop computers—for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources or from destructive codes embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

c. Searching the computer system for the evidence described in the conclusion may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in conclusion.

d. If, after inspecting the system software, and pertinent computer related documentation, it becomes apparent that these items are no longer necessary to retrieve and preserve the evidence, such materials and/or equipment will be returned within a reasonable time.

3. Background Regarding Computers

a. The term "computer" as used herein is defined as set forth in 18 U.S.C. § 1030(e)(1), and includes any electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

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

(1) The Internet is a worldwide network of computer systems operated by governmental entities, corporations, other commercial entities and universities. To access the Internet, an individual computer user must subscribe to an Internet Service Provider, or ISP, which operates a host computer system with direct access to the Internet. In the work environment, many governmental entities, corporations and universities provided employees and students with access to the Internet.

(2) A device known as a modem allows any computer to communicate with another computer through the use of telephone lines or cable. The modem may be internal or external to the computer.

(3) By connection to the Internet, either through a commercial ISP or through access provided by a private service provider such as the government, an individual with a computer can make electronic contact with millions of computers around the world.

c. Based on training and through my personal use of computers, I have knowledge of the method by which e-mail and other files are transmitted over telephone lines or cable between computers. Based on my training and knowledge I know the following:

(1) With the modem, a computer user can transport a computer file to his own computer, so that the computer file is stored in his computer. The process of transporting a file to one's own computer from another is called "downloading."

(2) The user can then view the file on his/her computer screen (monitor), and can "save" or retain the file on his/her computer for an indefinite time period.

(3) In addition to permanently storing the file on the computer, the user may print the file.

(4) The original file that was downloaded is also maintained in the originating computer.

(5) With the modem, a computer user can send a file from the computer to another individual on the Internet. This process of sending a file is called "uploading."

(6) The process of "uploading" is similar to the "downloading" process except the user is sending the computer file to others instead of retrieving the information from another computer. As with the process of "downloading," the original file is maintained on the originating computer.

(7) A user can also use an e-mail program to send files to another individual on the Internet. Most e-mail programs allow the user to attach files to the e-mail. The attached files may be documents or images. Again, the original file is maintained on the originating computer.

(8) Users commonly configure the e-mail program to save a copy of all "sent" e-mail. These copies will remain on the computer until they are deleted. If the e-mail program operates from a server on which the user's files are stored and retrieved as needed, the files are likely to be archived by the system administrator on a regular basis.

4. Probable Cause:

a. On 27 May 10, my office was notified by CW4 (b)(6)(b)(7)(C) Operations Officer, 11th Military Police Battalion (CID), that PVT Manning is believed to have unlawfully obtained and released

sensitive data including, but not limited to, TS-SCI and CABLE clearance documents onto the internet. PVT Manning is an Army Intelligence Analyst and was assigned to the S2 Section of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Baghdad, Iraq.

b. The following information was received from a non-government agency. Due to security concerns, the name of the agency will be withheld. The withholding of the name should in no way effect the reliability of the information they provided. This agency studies attack attribution, cause and effect relationships, and are involved in the development of tools, methodologies, and solutions to the intelligence problems of today and tomorrow. This agency provides OSINT and HUMINT from various projects both in the United States and abroad. In the past they have briefed the Office of the Secretary of Defense on issues related to Iran and provided the DoD operational manuals on the infrastructure of Iran. The information obtained from this agency is considered reliable.

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

(b) (7)(D) [redacted] Later in the chat log, PVT Manning explained that the "crazy white haired dude = Julian Assage." Assage is known to be the director of the website WikiLeaks, a Swedish based organization that publishes anonymous submissions and leaks of sensitive documents from governments and other organizations and is dedicated to exposing government secrets.

f. Further into the chat logs, PVT Manning states (in regards to his relationship with Assange) "im a source, not quite a volunteer" "i mean, im a high profile source... and i've developed a relationship with assange... but i don't know much more than what he tells me, which is very little" "it took me four months to confirm that the person i was communicating with was in fact assange". PVT Manning went on to state (regarding a video Assange had in his possession) "they also caught wind that he had a video... of the Gharani airstrike in Afghanistan, which he has, but hasn't decrypted yet... the production team was actually working on the baghdad strike though, which was never really encrypted" "he's got the whole 15-6 for that incident... so it wont just be video with no context" "but its not nearly as damning... it was an awful incident, but nothing like the baghdad one" "the investigating officers left the material unprotected, sitting in a directory on a centcom.smil.mil" "server" but they did zip up the files, aes-256, with an excellent password... so afaik it hasn't been broken yet" "14+ chars..." "i can't believe what im telling you =L"

g. Based on the aforementioned chat logs, it can be surmised that PVT Manning illegally obtained a copy of the 15-6 report pertaining to the incident in Afghanistan and provided that for submission on WikiLeaks as well.

h. On 27 May 10, the Stars and Stripes newspaper printed an article written by Joby Warrick of The Washington Post. The article, titled "*A wiki for a world of secrets*", was written about the WikiLeaks website. The article stated "Some of the harshest criticism came after last month's Iraq video, which portrayed a U.S. Apache helicopter's assault on a group of Iraqis in Baghdad that killed several civilians, including two employees of the Reuters news service. An edited 17-minute version of the video – donated by an anonymous source and decrypted with the help of volunteers – was posted on the WikiLeaks site April 5 under the heading "collateral murder." Edited and unedited versions of the video have been viewed nearly 8 million times."

i. A review of all the information obtained to date established probable cause that PVT Manning was responsible, at a minimum, for the classified video of the aforementioned Baghdad helicopter attack being posted to the internet. It is further reasonable to believe,
(b) (7)(D) [redacted]

5. Conclusion

a. Based on the information above, I have probable cause to believe, and do believe, that electronic information exists on the hard drives and storage devices belonging to, and used by, PVT Manning. By this affidavit and application, I request that the magistrate issue a Search Authorization allowing agents to seize all computers and storage devices belonging to, and used by, PVT Manning whether they are personally owned or property of the U.S. Government assigned for PVT Manning's use during his duties. Further, I request that the magistrate issue a Search Authorization allowing agents to seize any electronic information pertaining to PVT Manning illegally collecting and disseminating classified information.

(1) As used herein, the term information, records, documents, and materials includes information, records, documents, and materials created, modified or stored in electronic or magnetic form and any data, image or information that is capable of being read or interpreted by a computer.

(2) Information related to the unlawful obtaining and dissemination classified information. As used herein, information includes information in whatever form and by whatever means the information may have been created or may currently be stored, including any written or printed form and any electrical, electronic, or magnetic form (such as compact disc, floppy diskette, hard disk, backup tape, CD-ROM, optical disc, Bernoulli drive, ZIP discs, and SuperDisks).

(3) Computers; central processing units; external and internal drives; external and internal storage equipment or media; terminals or video display units; optical scanners; computer software; computerized data storage devices, including data stored on hard disks or floppy disks, computer printouts or computer programs; computer or data processing software or data, including: hard disks, floppy disks, cassette tapes, video cassette tapes, and magnetic tapes, together with peripheral equipment such as keyboards, printers, modems or acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, fax machines (and data included therein), telephone blue boxes, and magnetic tapes which could contain or be used to transmit or store any of the foregoing information, records, documents, and materials.

b. Based on the foregoing, there is probable cause to believe that the information and items set forth above - all of which constitute evidence of the commission of violations of federal laws, wherefore, I respectfully request that search authorization be issued allowing law enforcement personnel to search the storage devices and therein to seize and subsequently search, as described above: All information, in whatever form found, to include records, documents, programs, applications, and materials including pictures, graphics, text, magazines, software, or data; computerized logs; account names; passwords; encryption codes, algorithms and formulae; personal notes or diaries concerning computer or data processing literature, central processing units; external and internal drives; external and internal storage equipment or media; terminals or video display units; optical scanners; computer software; computerized data storage devices, including data stored on hard disks or floppy disks, computer programs; computer or data processing software or data, including: hard disks, floppy disks, and magnetic tapes, together with peripheral equipment such as keyboards, printers, modems or acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, magnetic tapes which could contain or be used to transmit or store any of the foregoing information, records, documents, and materials; information, records, documents, and materials which refer, relate to, or are for use in. As used herein, the term information, records, documents, and materials includes information, records, documents, and materials created, modified or stored in electronic or magnetic form and any data, image or information that is capable of being read or interpreted by a computer; and other information or items in whatever form containing or reflecting evidence of violations.

TYPED NAME AND ORGANIZATION OF AFFIANT:

SA (b)(6)(b)(7)(C)
25th Military Police Detachment (CID)
Camp Liberty, Iraq

SIGNATURE OF AFFIANT:

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

SWORN TO AND SUBSCRIBED BEFORE ME THIS 27 DAY OF MAY 10, AT 1400 HRS

NAME, ORGANIZATION AND OFFICIAL

CPT (b)(6)(b)(7)(C)
Office of the Staff Judge Advocate
Camp Liberty, Iraq

CAPACITY OF AUTHORITY ADMINISTERING THE OATH:

Military Magistrate

SIGNATURE OF AUTHORITY:

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

CANVASS INTERVIEW WORKSHEET

NAME	RANK	SSN
(b)(6)(b)(7)(C)	PFC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
2 BSTB (b)(6)(b)(7)(C) BCT mos (35N)		674-7946
REMARKS		
Very little to any interaction with PVT manning. No socializing outside of work. ~~know~~ NO known Accidental disclosures. Does not agree with PVT manning's life style.		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	CW2	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC 2 BSTB (b)(6)(b)(7)(C) BCT mos (350F)		674-7946
REMARKS		
Highly knowledgable, computer work excelled. supervisor. / volatile personality. easily excited. --No known disclosures. -no known Attempts to stay late. - computer w/ Take Abuse. - NO social Interaction		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC 2 BCT mos (35F)		674-7946
REMARKS		
closed of person. not seen hanging out with people. Pressure cooker. no social interaction Possible friends with SPC (b)(6)(b)(7)(C) -- try to stay late - Product writing / never saw searches in the computer. would talk about politics and Global politics. - no Accidental disclosure - no security. Did leave camera once to - SCIF - (not allowed)		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	WO1	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
704th MI mos (25DN)		674-7946
REMARKS		
-no socializing - says hi in passing. - excitable personality. - no actual knowledge of work.		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SSG	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
B Co 2BSTB, 10th Mountain (mos 35P)		674-7946
REMARKS		
-Does not work with, no socialization. PVT manning Fusion Analyst. - no accidental disclosures, no staying late to work. - no known Associates		

CANVASS INTERVIEW WORKSHEET

NAME	RANK	SSN
(b)(6)(b)(7)(C)	1LT	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHD, 10th Mountain BDE (mos 35D)		674-0792

REMARKS
- only been here since MAY. Very little interaction w/ PVT Manning. No known Associates.
- No known Accidental

NAME	RANK	SSN
(b)(6)(b)(7)(C)	1LT	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC, 2BCT (mos 35D)		674-0792

REMARKS
- known for about year and A half; No known Associates;
- Article on nipper would spark. no extream conversations. Borrowed two books - anti religious in nature.
- NIPR - Politics/stockmarkets/
- SIPR - Nothing - only work related.

NAME	RANK	SSN
(b)(6)(b)(7)(C)	1LT	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC, 2BCT (mos 35D)		674-0792

REMARKS
- SPC Manning has spillage; wikileak; very little work related interaction; tried to help at the Gym, Didn't keep up.
- No search knowledge. on nipper All the time. no known accidental disclosures;

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC 2BCT (mos 35M)		674-7946

REMARKS
+ PVT Manning loner. No known associates - next door neighbor. several casual conversations.
- no known accidental disclosure
- had camera in scif.
- computer genious. - very Boastful. Does not see work on computer. Posting secrets on internet.

NAME	RANK	SSN
(b)(6)(b)(7)(C)	CPT	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC 2 BCT (mos 35D)		674-7946

REMARKS
- PVT Manning. hard worker, ethically intelligent, Good product from work. easily side tracked
- obvious mental issues. Behavioral health multiple times. Feminin in nature.
- No known Accidental disclosures; worked nights First half of mission. lots of Freedom to search computers. no observation of secret outside need of work.

CANVASS INTERVIEW WORKSHEET

NAME	RANK	SSN
* (b)(6)(b)(7)(C)	CPT	(b)(6)(b)(7)(C)
UNIT/ADDRESS HHC, 2nd BCT (mos 35D)		**PHONE** 674-7944
REMARKS - Believed to have psychological issues/hyper individuals - great work. excelled with computer work. - no hang out w/ anyone at work. spec (b)(6)(b)(7)(C) possible associate - no known accidental disclosures - no search outside scope of work - mentioned video as the same on the share drive.		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SGT	(b)(6)(b)(7)(C)
UNIT/ADDRESS HHC, 2nd BCT (mos 35F)		**PHONE** 674-7946
REMARKS -		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	CONTRACTOR	(b)(6)(b)(7)(C)
UNIT/ADDRESS L3 Communication (IT)		**PHONE** 674-7946
REMARKS - meek and mild on minute/ballistic. no known associates. - no known knowledge of work - Intelligent -		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	MSG	(b)(6)(b)(7)(C)
UNIT/ADDRESS HHC 2BCT (mos 35X)		**PHONE** 674-7946
REMARKS - reasonably good analyst. Instability issues. started counseling before deployment. - no known Accidental Disc. - no late work or Attn hours work. shared computer w/ opsit shift. - showed a lot of interest in niper computer. concerned about shocks. - no signs of secreting information.		

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SSG	(b)(6)(b)(7)(C)
UNIT/ADDRESS HHC, 2BCT (mos 35N)		**PHONE** 674-7946
REMARKS + very little work related / no socializing / no known Associates. + new to unit. + no Accidental disclosure		

CANVASS INTERVIEW WORKSHEET

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC 2BCT (mos 35F)		674-7946

REMARKS
- easily classed out. no known associates

NAME	RANK	SSN
(b)(6)(b)(7)(C)	PFC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC, 2BCT (mos 35F)		674-7946

REMARKS
- Not personally known. worked night shift. -> sat at computer. on the sipper. learning about FRAGO.
- PVT (b)(6)(b)(7)(C)
- no accidental disclosures
- no late work.

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC, 2BCT (mos 35F)		674

REMARKS
- talked to prior to deployment. stopped just before deploying due to husband disapproval. good computer skills. no known accidental disclosures. no knowledge of what was being worked on, on the SIPR/NIPR.
- might have been trying to get info after being removed from the section, but did not ask for anything.

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SGT	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
BCO, 2SBT BSTB (mos 35F)		674-7946

REMARKS
- no socializing. no known associates
- no work late
- no disclosures

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	(b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
BCO, 2 BSTB (mos 35N)		674-7946

REMARKS
+ Alot of personal stress, no social interaction. Personality don't click, no known associates. Good worker. no issues.
+ NO accidental disclosures.
+ no knowledge of search history.

CANVASS INTERVIEW WORKSHEET

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	(b)(6)(b)(7)(C)
UNIT/ADDRESS HHC, 2 BCT (MOS 356)		**PHONE**
REMARKS - Does not handle stress well. / Tries to socialize but distrd work / SPC (b)(6)(b)(7)(C) / (b)(6)(b)(7)(C) - would TOY rather than mental health - no known accidental disclosures - 2 person integrity		
NAME	**RANK**	**SSN**
UNIT/ADDRESS		**PHONE**
REMARKS		
NAME	**RANK**	**SSN**
UNIT/ADDRESS		**PHONE**
REMARKS		
NAME	**RANK**	**SSN**
UNIT/ADDRESS		**PHONE**
REMARKS		
NAME	**RANK**	**SSN**
UNIT/ADDRESS		**PHONE**
REMARKS		

RIGHTS WARNING PROCEDURE/WAIVER CERTIFICATE

For use of this form, see AR 190-30; the proponent agency is ODCSOPS

DATA REQUIRED BY THE PRIVACY ACT

AUTHORITY:	Title 10, United States Code, Section 3012(g)
PRINCIPAL PURPOSE:	To provide commanders and law enforcement officials with means by which information may be accurately identified.
ROUTINE USES:	Your Social Security Number is used as an additional/alternate means of identification to facilitate filing and retrieval.
DISCLOSURE:	Disclosure of your Social Security Number is voluntary.

1. LOCATION	2. DATE (b)(6)(b)(7)(C)	3. TIME	4. FILE NO.
	27 MAY 10	2146 (b)(6)(b)(7)(C)	

5. NAME *(Last, First, MI)*	8. ORGANIZATION OR ADDRESS
MANNING, BRADLEY EDWARD	HHC BRIGADE 2nd Combat Team 10th Mount. DIVISION
6. SSN (b)(6)(b)(7)(C)	7. GRADE/STATUS PFC / Active

PART 1 - RIGHTS WAIVER/NON-WAIVER CERTIFICATE

Section A. Rights

The investigator whose name appears below told me that he/she is with the United States Army Criminal Investigation Command as a Special Agent and wanted to question me about the following offense(s) of which I am suspected/~~accused~~: Espionage, Gathering, Transmitting and disclosing classified information (b)(6)(b)(7)(C)

Before ~~he/she~~ asked me any questions about the offense(s), however, ~~he/she~~ made it clear to me that I have the following rights:

(b)(6)(b)(7)(C) do not have to answer any questions or say anything.

Anything I say or do can be used as evidence against me in a criminal trial.

(For personnel subject to the UCMJ) I have the right to talk privately to a lawyer before, during, and after questioning and to have a lawyer present with me during questioning. This lawyer can be a civilian lawyer I arrange for at no expense to the Government or a military lawyer detailed for me at no expense to me, or both.

- or -

(For civilians not subject to the UCMJ) I have the right to talk privately to a lawyer before, during, and after questioning and to have a lawyer present with me during questioning. I understand that this lawyer can be one that I arrange for at my own expense, or if I cannot afford a lawyer and want one, a lawyer will be appointed for me before any questioning begins.

(b)(6)(b)(7)(C) I am now willing to discuss the offense(s) under investigation, with or without a lawyer present, I have a right to stop answering questions at any time, or privately with a lawyer before answering further, even if I sign the waiver below.

5. COMMENTS (Continue on reverse side)

Q: Have you been advised of your legal rights and requested a lawyer in the last 30 days? A: YES (b)(6)(b)(7)(C) FOR ASSAULT

Section B. Waiver

I understand my rights as stated above. I am now willing to discuss the offense(s) under investigation and make a statement without talking to a lawyer first and without having a lawyer present with me.

WITNESSES *(If available)*	3. SIGNATURE OF INTERVIEWEE
1a. NAME *(Type or Print)*	
b. ORGANIZATION OR ADDRESS AND PHONE	4. SIGNATURE OF INVESTIGATOR (b)(6)(b)(7)(C)
2a. NAME *(Type or Print)*	5. TYPED NAME OF INVESTIGATOR SA (b)(6)(b)(7)(C)
b. ORGANIZATION OR ADDRESS AND PHONE	6. ORGANIZ Central Bagdad CID Office, IRAQ

Section C. Non-Waiver

1. I do not want to give up my rights:

☒ I want a lawyer. (b)(6)(b)(7)(C) ☐ I do not want to be questioned or say anything.

2. SIGNATURE OF INTERVIEWEE (b)(6)(b)(7)(C)

ATTA SWORN STATEMENT *(DA form 2823)* SUBSEQUENTLY EXECUTED BY THE SUSPECT/ACCUSED.

DA FORM 3881, NOV 89 EDITION OF NOV 84 IS OBSOLETE

PART II - RIGHTS WARNING PROCEDURE

THE WARNING

1. WARNING - Inform the suspect/accused of:
   a. Your official position
   b. Nature of offense(s).
   c. The fact that he/she is a suspect/accused.
2. RIGHTS - Advise the suspect/accused of his/her rights as follows:
   "Before I ask you any questions, you must understand your rights."
   a. "You do not have to answer my questions or say anything."
   b. "Anything you say or do can be used as evidence against you in a criminal trial."
   c. (For personnel subject to the UCMJ) "You have the right to talk privately to a lawyer before, during, and after questioning and to have a lawyer present with you during questioning. This lawyer can be a civilian you arrange for at no expense to the Government or a military lawyer detailed for you at no expense to you, or both."

   - or -

   (*For civilians not subject to the UCMJ*) You have the right to talk privately to a lawyer before, during, and after questioning and to have a lawyer present with you during questioning. This lawyer can be one you arrange for at you own expense, or if you cannot afford a lawyer and want one, a lawyer will be appointed for you before any questioning begins."
   d. "If you are now willing to discuss the offense(s) under investigation, with or without a lawyer present, you have a right to stop answering questions at any time, or speak privately with a lawyer before answering further, even if you sign a waiver certificate."

Make certain the suspect/accused fully understands his/her rights.

THE WAIVER

"Do you understand your rights?"
(If the suspect/accused says "no," determine what is not understood, and if necessary repeat the appropriate rights advisement. If the suspect/accused says "yes," ask the following question.)

"Have you ever requested a lawyer after being read your rights?"
(If the suspect/accused says "yes," find out when and where. If the request was recent (i.e. fewer than 30 days ago), obtain legal advise on whether to continue the interrogation. If the suspect/accused says "no," or if the prior request was not recent, ask him/her the following question.)

"Do you want a lawyer at this time?"
(If the suspect/accused says "yes," stop the questioning until he/she has a lawyer. If the suspect/accused says "no," ask him/her the following question.)

"At this time, are you willing to discuss the offense(s) under investigation and make a statement without talking to a lawyer and without having a lawyer present with you?" (*If the suspect/accused says "no," stop the interview and have him/her read and sign the non-waiver section of the waiver certificate on the other side of this form. If the suspect/accused says "yes," have him/her read and sign the waiver section of the waiver certificate on the other side of this form.*)

SPECIAL INSTRUCTIONS

WHEN THE SUSPECT/ACCUSED REFUSES TO SIGN THE WAIVER CERTIFICATE: If the suspect/accused orally waives his/her rights but refuses to sign the waiver certificate, you may proceed with the questioning. Make notations on the waiver certificate to the effect that he/she has stated that he/she understands his/her rights, does not want a lawyer, wants to discuss the offense(s) under investigation, and refuses to sign the waiver certificate.

IF WAIVER CERTIFICATE CANNOT BE COMPLETED IMMEDIATELY:
In all cases the waiver certificate must be completed as soon as possible. Every effort should be made to complete the waiver certificate before any questioning begins. If the waiver certificate cannot be completed at once, as in the case of street interrogations, completion may be temporarily postponed. Notes should be kept on the circumstances.

PRIOR INCRIMINATING STATEMENTS:

1. If the suspect/accused has made spontaneous incriminating statements before being properly advised of his/her rights he/she should be told that such statements do not obligate him/her to answer further questions.
2. If the suspect/accused was questioned as such either without being advised of his/her rights or some question exists as to the propriety of the first statement, the accused must be so advised. The office of the serving Staff Judge Advocate should be contacted for assistance in drafting the proper rights advisal.

NOTE: If 1 or 2 applies, the fact that the suspect/accused was advised accordingly should be noted in the comment section on the waiver certificate and initialed by the suspect/accused.

WHEN SUSPECT/ACCUSED DISPLAYS INDECISION ON EXERCISING HIS OR HER RIGHTS DURING THE INTERROGATION PROCESS: If during the interrogation, the suspect displays indecision about requesting counsel (for example, "Maybe I should get a lawyer."), further questioning must cease immediately. At that point, you may question the suspect/accused only concerning whether he or she desires to waive counsel. The questioning may not be utilized to discourage a suspect/accused from exercising his/her rights. (For example, do not make such comments as "If you didn't do anything wrong, you shouldn't need an attorney.)"

COMMENTS (*Continued*)

DA FORM 3881, NOV 89 EDITION OF NOV 84 IS OBSOLETE

Exhibit 6

Page(s) 000066 thru 000086 referred to:

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

COMMANDER'S AUTHORIZATION TO SEARCH
For the use of this form see USACIDC Supplement 1 to AR 190-22

TO: CPT (b)(6)(b)(7)(C) Commander, HHC, 2/10th MTN BDG, FOB Hammer APO AE 09308
(Name and Organization of the person to whom authorization is given)

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

Central Baghdad CID Office, USACIDC, Camp Liberty APO AE 09342
(Organization or Address of Affiant)

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

NIPR Computers PFC Bradley MANNING had access to

for the property described as one NIPR Computer located within S-2, BGE TOC; two NIPR computers located within Supply Office Room 3, Supply Annex, BGE.

bring this authorization to the attention of the *(person searched) (person in possession, if any person be found at the place or on the premises searched)*. The search will be made in the *(daytime) (nighttime)*, and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to a USACIDC evidence custodian and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 27 day of MAY, 2010.

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

(b)(6)(b)(7)(C)
HHC, 2BCT

(Signature, typed name, and organization of Commander)

CID FORM 98-R
1 SEP 98

CANVASS INTERVIEW WORKSHEET

NAME	RANK	SSN
PFC (b)(6)(b)(7)(C)	E3/PFC	— (b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
S-2, 2/10th, SIGNT AN		

REMARKS
- Manning asked for help on a hash table project. personal profitable project
- Manning always reads the news - always knew what was going on everywhere
- He would always read the opened/closed source info - He liked the opened sources best. - Manning tryed to hard - Other people would put their names on his reports

NAME	RANK	SSN
S-2 2/10th HUMINT	CW2	
UNIT/ADDRESS		**PHONE**
(b)(6)(b)(7)(C)		— (b)(6)(b)(7)(C)

REMARKS
- Didn't see anything suspicious @ work, no rumors.
- Didn't see Manning hang out w/ anyone

NAME	RANK	SSN
(b)(6)(b)(7)(C)	CPT	— (b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
S-2 2/10th		

REMARKS
- After she returned from block leave Apr 10 timeframe. She heared about the Apache Story on Wiki leaks. Manning told her it looked like the same video. She didn't believe him so he forwared her (SIPR) the website from the SIPR ShareDrive (25Apr10-1922). He made no other comments.

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SPC	— (b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC BG, Supply		

REMARKS
Manning worked in supply room after his Art 15. About (b) (6), (b) (7)(C) he got on the supply room computers from time to time. (b)(6)(b)(7)(C) has been watching Manning since CID arrived. Manning does 2404 stuff mostly.

NAME	RANK	SSN
(b)(6)(b)(7)(C)	SGT	— (b)(6)(b)(7)(C)
UNIT/ADDRESS		**PHONE**
HHC BG Supply		

REMARKS
Works with Manning in Supply room. Last night Manning ~~opened~~ got on a computer. the Google page pulled up. - She got SSG (b)(6)(b)(7)(C) who (he put in username + password that it) then told Manning to get off the computer.

USACIDC Supplement 1 to AR 190-22

Date: 28 May 10	**Consent To Search** (USACIDC Supplement 1 to AR 190-22)	Time: 1200

1. Name of person consenting to the search: SSG (b)(6)(b)(7)(C)

2. Organization and location: HHC, 2/10th MTN BDE, FOB HAMMER (LT BRUM) APO AE 09308

3. I have been informed by the undersigned USACIDC Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law:

Espionage; Disclosure of classified info; gathering, transmitting, or losing defense info

4. I have been requested by the undersigned USACIDC Special Agent to give my consent to a search of my person, premises, or property as indicated below. I have been advised of my right to refuse a search of my person, premises, or property. (If you do not give your consent, do not sign this form.)

5. I hereby authorize the undersigned USACIDC Special Agent and/or other Authorized Law Enforcement Officials assisting the undersigned USACIDC Special Agent to conduct a search of: ***(Initial and sign applicable blocks)***

		Initials	*Signature*
a.	My Person		
b.	My Quarters		

Located At:

		Initials	*Signature*
c.	My Vehicle		

Located At:

Described As:

		Initials	*Signature*
d.	Other	(b)(6)(b)(7)(C)	(b)(6)(b)(7)(C)

Located At: Supply Annex, 2/10th MTN BDE, Supply Office Room 3

Described As: HP laptop, touch smart TS2, serial # CNF8492K3S

I am authorizing the above search(s) for the following general types of property which may be removed by the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations:

laptop computer listed above.

6. This written permission is given to the undersigned USACIDC Special Agent freely, voluntarily and without threats or promises of any kind:

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

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

Signature of Witness (If Available)

CID Form 87-R-E
1 Jan 00

PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE

DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
CENTRAL BAGHDAD CID OFFICE
25TH MILITARY POLICE DETACHMENT (CID)
11TH MILITARY POLICE BATTALION (CID)
CAMP LIBERTY, APO AE 09342

CONSENT TO SEARCH COMPUTER/ELECTRONIC EQUIPMENT

I, (b)(6)(b)(7)(C), have been asked to give my consent to the search of my computer/electronic equipment. I have also been informed of my right to refuse to consent to such a search.

I hereby authorized any Special Agent of USACIDC to conduct at any time a complete search of all computer/electronic equipment located at HP Smart touch T52, SN: CNF8492K3S. These agents/officers are authorized by me to take from the aforementioned location, any computer(s), including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/electronic hardware or personal digital assistants, cellular telephones and electronic pagers. I hereby consent to the search of those items for any data or material, which is contraband, or evidence of any crime. I understand that this contraband or evidence may be used against me in a court of law.

I give this written permission voluntarily. I have not been threatened, placed under duress or promised anything in exchange for my consent. I have read this form, it has been read to me and I understand it. I understand the English language and have been able to communicate with the agents/officers.

I understand that I may withdraw my consent at any time for any reason. I may also ask for a receipt for all things taken.

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

Date and Time: 28 May 2010 28 May 10/ 1202

DEPARTMENT OF THE ARMY
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
CENTRAL BAGHDAD CID OFFICE
25TH MILITARY POLICE DETACHMENT (CID)
11TH MILITARY POLICE BATTALION (CID)
CAMP LIBERTY, APO AE 09342

CONSENT TO SEARCH COMPUTER/ELECTRONIC EQUIPMENT

I, (b)(6)(b)(7)(C) _____, have been asked to give my consent to the search of my computer/electronic equipment. I have also been informed of my right to refuse to consent to such a search.

I hereby authorized any Special Agent of USACIDC to conduct at any time a complete search of all computer/electronic equipment located at HHC, 2/10th MTN BDE. These agents/officers are authorized by me to take from the aforementioned location, any computer(s), including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/electronic hardware or personal digital assistants, cellular telephones and electronic pagers. I hereby consent to the search of those items for any data or material, which is contraband, or evidence of any crime. I understand that this contraband or evidence may be used against me in a court of law.

I give this written permission voluntarily. I have not been threatened, placed under duress or promised anything in exchange for my consent. I have read this form, it has been read to me and I understand it. I understand the English language and have been able to communicate with the agents/officers.

I understand that I may withdraw my consent at any time for any reason. I may also ask for a receipt for all things taken.

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

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

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

Date and Time: 28 MAY 10, 15:18

FOR OFFICIAL USE ONLY
-Law Enforcement Sensitive-

EXHIBIT_____

SEARCH AND SEIZURE AUTHORIZATION

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

TO: *(Name and Organization of the person to whom authorization is given)*
Special Agent (b)(6)(b)(7)(C), (b) (7)(E) Central Baghdad CID Office, Camp Liberty, APO AE 09342

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

Central Baghdad CID Office, Camp Liberty, APO AE 09342
(Organization or Address of Affiant)

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

FOB Hammer Post Office, Building D37, FOB Hammer APO AE 09308

for the property described as Any PS Form 297-A, Customs Declaration and Dispatch Note, relating to any packages shipped by PFC Bradley E. MANNING within the last 60 days.

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

Evidence Custodian, 11th MP BN (CID), Camp Arifjan, APO AE 09366
(Name and Organization of Authorized Custodian)

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

Dated this 28 day of May, 2010.

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL	DUTY POSITION OF AUTHORIZING OFFICIAL
CPT (b)(6)(b)(7)(C)	Military Magistrate
ORGANIZATION OF AUTHORIZING OFFICIAL	**SIGNATURE OF AUTHORIZING OFFICIAL**
USD-C, Office of the Staff Judge Advocate Camp Liberty, APO AE 09342	(b)(6)(b)(7)(C)

DA FORM 3745, SEP 2002 DA FORM 3745-R, APD PE v1.02ES

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

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

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

I, SA (b)(6)(b)(7)(C), (b) (7)(E) (Name), Central Baghdad CID Office, 11th MP BN (CID), (Organization or Address)

Camp Liberty, APO AE 09342

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

On 27 May 10, this office was notified that PFC MANNING was believed to have unlawfully obtained and released sensitive data including, but not limited to, TS-SCI and CABLE clearance documents onto the internet. PFC MANNING is an Army Intelligence Analyst and was assigned to the S2 Section of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This information was obtained through a non-government agency, which chooses to remain unnamed; however, the withholding of this organization should have no effect of the information provided. This agency studies the attack attribution, cause and effect relationships, and are involved in the development of tools, methodologies, and the solutions to the intelligence problems of today and tomorrow; and provides OSINT and HUMINT from various projects to the United States and abroad. (b) (7)(D)
(b) (7)(D)

2. The affiant further states that:

(b) (7)(D)

On 27 May 10, the affiant using the above mentioned information obtained a Search and Seizure Authorization for the search of PFC Manning's work terminals, and a search of his designated living area for any and all electronic media storage devices and classified materials. While executing the Search Authorization within PFC Manning's living area, a DVD bearing "Secret" marking and labeled "12 Jul 07 CZ Engagement Zone 30 GC" was discovered within a USPS box, which appeared to be packaged for shipment.

An interview of PFC Manning's roommate, SPC (b)(6)(b)(7)(C) MP, revealed although PFC Manning rarely mailed out boxes; he had mailed three packages last month, late Apr '10 time frame. SPC [redacted] related there was only one mailing service at FOB Hammer, which was the FOB Hammer Post Office.

It it a known fact that all mail being shipped out of country must be accompanied by a custom form, which is tracked and maintained by the Post Office for a certain time period.

3. In view of the foregoing, the affiant requests that an authorization be issued for a search of FOB Hammer Post Office *(the person) (and)*

(the quarters or billets) (and)

(the automobile) ( ) and (seizure) (apprehension) of Any PS Form 297-A, Customs Declaration *(items/persons searched for)*

and Dispatch Notes, relating to any shipped from PFC Manning within the last 60 days.

TYPED NAME AND ORGANIZATION OF AFFIANT	SIGNATURE OF AFFIANT
SA (b)(6)(b)(7)(C) Central Baghdad CID Office, USACIDC, Camp Liberty, APO AE 09342	(b)(6)(b)(7)(C)

SWORN TO AND SUBSCRIBED BEFORE ME THIS 28 DAY OF May 2010 AT 1550hrs

TYPED NAME, ORGANIZATION AND OFFICIAL CAPACITY OF AUTHORITY ADMINISTERING THE OATH	SIGNATURE OF AUTHORITY ADMINISTERING THE OATH
CPT (b)(6)(b)(7)(C) Military Magistrate, Office of the Staff Judge Advocate, USD-C, Camp Liberty, APO AE 09342	(b)(6)(b)(7)(C)

INSTRUCTIONS FOR

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it has been committed. Use additional page if necessary.

2. In paragraph 2, set forth facts establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraphs 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she has plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary

3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under certain circumstances for evidentiary matters.

SWORN STATEMENT

For use of this form, see AR 190-45; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.

1. LOCATION	2. DATE (YYYYMMDD)	3. TIME	4. FILE NUMBER
FOB Hammer	20100528 (b)(6)(b)(7)(C)	2112 (b)(6)(b)(7)(C)	

5. LAST NAME, FIRST NAME, MIDDLE NAME	6. SSN	7. GRADE/STATUS
(b)(6)(b)(7)(C)	(b)(6)(b)(7)(C)	E4 / AD

8. ORGANIZATION OR ADDRESS
HHC, BSG, 2/10th MTN DIV

9. I, (b)(6)(b)(7)(C), WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH: That I am Bradley Mannings (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) I don't make it a point to have a conversation with him. Anytime we do speak, it's for small things like, "Turn off the light or turn your alarm off." I've noticed that he goes (b)(6)(b)(7)(C) to the room to get on his computer multiple times during the day. He also will be pretty upset anytime the internet is down. Another thing I have observed while being (b)(6)(b)(7)(C) is that a few times during the week, he either stays up late on the computer or either wakes up in the middle of the night to get on his computer. I never see what he is doing on his computer because it is turned away from me. I did notice that he had a hard drive, microphone, and some other kind of computer equipment that did not return with him when he came back from R&R.

Q- (b)(6)(b)(7)(C)

A- (b)(6)(b)(7)(C) (wrote the above narrative)

Q- When did Manning go on R&R?

A- I think it was about the 15th to the 20th of January.

10. EXHIBIT	11. INITIALS OF PERSON MAKING STATEMENT	PAGE 1 OF 3 PAGES
	(b)(6)(b)(7)(C)	

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF ____ TAKEN AT ____ DATED ____"

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE INDICATED.

STATEMENT OF | TAKEN AT | DATED | FILE NUMBER: | CONTINUED

Q- Does he ever talk to you about secret material?
A- No
Q- Have you ever noticed him bring home (back to the CHU) secret material?
A- No
Q- Does [redacted] have what type of electronic equipment does he keep in the room?
A- A computer, an external hard drive, his iPod, and a microphone. After he came back from his block leave in January, all I have seen was his computer.
Q- Has MANNING ever asked you to hold or hide something for him?
A- No
Q- Have you seen MANNING bring home (to the chu) CD's, DVD's etc?
A- I've see CD's laying around on his nightstand but I couldn't tell if they were blank or not. I've never viewed the discs to test them.
Q- How often does MANNING mail and recieve packages?
A- I only seen him take one group of packages to mail out [redacted] the end of April. He recieves packages very often. At least once a week he'll get a package.
Q- Do you know who sends [redacted] him the packages and what's in them?
A- I haven't looked at his packages to see the sender's name. His packages are mostly food items and he'll open them and leave them on the floor. Occasionally he'll get a package that he will leave closed and not open until [redacted] is at work or away from the room. I've never seen [redacted] the contents of packages like those.
Q- Do you know what was in the package he mailed out in April 10, and/or do you know who he mailed the package to?
A- I don't know what was in the packages he mailed out. He had three boxes, and when I questioned him if they were sent to him, [redacted] he told me he had some stuff to send home and locked them in his wall locker. I did not see who they were addressed to.
Q- Who is Manning friends with?
A- I don't think he has any friends out here. The only person I have seen him with, was other S-2 personnel when they are going to chow.
Q- Does he have any work friends?

INITIALS OF PERSON MAKING STATEMENT [redacted] PAGE 2 OF PAGES

STATEMENT OF | TAKEN AT | File Number: | DATED | CONTINUED:

STATEMENT *(Continued)*

A- The only person that i've seen him talk to is Spc (b)(6)(b)(7)(C) from S-2.
Q- Do you know the names of any of his on-line friends?
A- I've never looked on his computer and he doesn't speak of any.
Q- Where does MANNING hang out when he's not a work?
A- When he's not at work, he stays in the room on his computer. The only other times he leaves is for smoking, the bathroom, and to go to the PX.
Q- Describe SPC (b)(6)(b)(7)(C)
A- Her name is (b)(6)(b)(7)(C). She looks hispanic. She has black hair, wears glasses, and is about a medium build. The only time i've seen them talking was walking to and from chow. She works in S-2, but I don't know what her actual MOS is.
Q- Is there anything else you would like to add to your statement?
A- No /// End of Statement ///

AFFIDAVIT

I, (b)(6)(b)(7)(C), HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 3. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(b)(6)(b)(7)(C)
(Signature of Person Making Statement)

WITNESSES:

ORGANIZATION OR ADDRESS

ORGANIZATION OR ADDRESS

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 28 day of MAY, 20 10
at FOB HAMMER APO AE

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

SA (b)(6)(b)(7)(C)
(Typed Name of Person Administering Oath)

10 USC 936
(Authority To Administer Oaths)

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

PAGE 3 OF 3 PAGES

SWORN STATEMENT

For use of this form, see AR 190-45; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY:	Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).
PRINCIPAL PURPOSE:	To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.
ROUTINE USES:	Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.
DISCLOSURE:	Disclosure of your SSN and other information is voluntary.

1. LOCATION	2. DATE (YYYYMMDD)	3. TIME	4. FILE NUMBER
2nd BRIGADE ANNEX, FOB HAMMER	20100528	2141 28 MAY 10	0160-10-CID899

5. LAST NAME, FIRST NAME, MIDDLE NAME	6. SSN	7. GRADE/STATUS
(b)(6)(b)(7)(C)	(b)(6)(b)(7)(C)	SPC/Active

8. ORGANIZATION OR ADDRESS

HHC 2nd BG, 10th MT, FOB HAMMER, IRAQ

(b)(6)(b)(7)(C) (b)(6)(b)(7)(C), WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

About one to two weeks ago, then SPC Manning came into the Paralegal office and said that he needed to use our Sipr Scanner. We told him to go ahead, we assumed - I believe but do not recall exactly who was in the Paralegal office with me, but I believe SFC (b)(6)(b)(7)(C) I remember telling SPC Manning to just hit SH and my name will pop up and I will either forward the email to whomever it needs to go to. SPC Manning stated for me just to print out the pages and he will take it to SFC (b)(6)(b)(7)(C) I said "OK". SPC (PFC) Manning came and stood over my desk I opened the email and attachment - hit print and SPC Manning took the pages off the printer. He the asked me to delete the email. SPC Manning stood over me as I deleted the email from my inbox and my deleted folder. - SPC Manning then left my office. About 30 minutes later (b)(6)(b)(7)(C)

10. EXHIBIT	11. INITIALING STATEMENT (b)(6)(b)(7)(C)	PAGE 1 OF 3 PAGES

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF ____ TAKEN AT ____ DATED ____"

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE INDICATED.

STATEMENT OF (b)(6)(b)(7)(C) TAKEN AT 2141 DATED 28 MAY 10 CONTINUED

SPC Manning came back into the Paralegal office, and had me do the exact same thing again. He again grabbed the pages off the printer and also watched as I deleted the emails again. (b)(6)(b)(7)(C)

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

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

Q. Why did you allow SPC Manning to use your SIPR scanner?
A. Because everyone uses our scanner. Everyone else has a NIPR scanner. I believe we are the only office with a SIPR Scanner.
Q. Who is SPC (b)(6)(b)(7)(C)
A. SPC (b)(6)(b)(7)(C) is the Paralegals NCOIC - She was not really paying attention. She was preoccupied at her desk. I do not recall if she did say anything.
Q. Who did you forward the e-mail to?
A. Absolutely No one, SPC Manning asked me to go ahead and just print it out.
Q. Why would SPC MANNING scan something through the SIPR scanner just to be printed out and not e-mailed?
A. I have no idea. I thought it was strange - for when most people use our Sipr printer, the want it emailed to someone. I thought maybe the black ink cartridges were low or people or offices were out of black toner again. I did remember thinking "Wow that was strange!"
Q. How many pages did SPC manning SCAN and print?
A. I believe just one page each time.
Q. Did you see the page?
A. Glanced at the pages, saw lines on the pages and typed information, but not enough glancing to make out what it said.
Q. Did you ~~did~~ delete the e-mail from your inbox and deleted items box?
A. YES.
Q. What was SPC MANNINGS DEMEANOR? DID HE SEEM NERVOUS?

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

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

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

STATEMENT OF (b)(6)(b)(7)(C) TAKEN AT 2141 File Number: DATED 28 MAY 10 CONTINUED:

STATEMENT (Continued)

A. High strung & hyper - but he always seems that way.
Q. DOES EVERYONE ENSURE YOU DELETE THEIR SCAN?
A. No
Q. DID HIS REQUEST SEEM STRANGE TO YOU?
A. A little
Q. DID SPC MANNING TELL YOU WHAT THE SCAN WAS?
A. Did not tell me exactly what it was for, only for the investigation So I assumed it was for the sensitive missing items from the supply shop.
Q. HAVE you ever allowed SPC MANNING TO ACCESS your computer?
A. No
Q. IS there anything else you want to add to this statement?
A. Not at this time - NO! ///END STATEMENT/// (b)(6)(b)(7)(C)

AFFIDAVIT

I, (b)(6)(b)(7)(C), HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1 AND ENDS ON PAGE 3. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(b)(6)(b)(7)(C)
(Signature of Person Making Statement)

WITNESSES:

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 28 day of May, 20 10 at 2nd Brigade Annex, Fort Hammer.

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

ORGANIZATION OR ADDRESS

SA (b)(6)(b)(7)(C)
(Typed Name of Person Administering Oath)

ORGANIZATION OR ADDRESS

10 USC 936
(Authority To Administer Oaths)

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

PAGE 3 OF 3 PAGES

SWORN STATEMENT

For use of this form, see AR 190-45; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.

1. LOCATION	2. DATE (YYYYMMDD)	3. TIME	FILE NUMBER
2nd BRIGADE ANNEX, FOB HAMMER	20100528	2230	0160-10-CID899

5. LAST NAME, FIRST NAME, MIDDLE NAME	6. SSN	7. GRADE/STATUS
(b)(6)(b)(7)(C)	(b)(6)(b)(7)(C)	SSG / ACTIVE

8. ORGANIZATION OR ADDRESS

HHC 2nd BRIGADE COMBAT TEAM, 10TH MT, FOB HAMMER, APO AE 09308

(b)(6)(b)(7)(C) (b)(6)(b)(7)(C), WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

Q. (b)(6)(b)(7)(C)

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

Q. Have you ever directed SPC MANNING, TO USE THE SIPR SCANNER IN THE PARALEGAL OFFICE?

A. NO

Q. Have you ever directed SPC manning to use any SIPR Scanner?

A. NO

Q. WAS SPC MANNING involved in the sensitive items investigation in your section?

A. NO

Q Did you ask SPC manning to scan, copy or distribute any documents pertaining to the investigation?

A. NO

Q. Is there any reason why SPC MANNING would use the SIPR Scanner?

A. NO

Q. Did SPC MANNING ever bring you documents he claimed to have scanned through the SIPR scanner?

A. NO

Q. Is there anything else you would like to add to this state-

10. EXHIBIT	11. INITIALS OF PERSON MAKING STATEMENT	PAGE 1 OF 2 PAGES
	(b)(6)(b)(7)(C)	

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF _____ TAKEN AT _____ DATED _____"

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE INDICATED.

STATEMENT OF (b)(6)(b)(7)(C) TAKEN AT 2230 (b)(6)(b)(7)(C) DATED 28 May 10

9. STATEMENT *(Continued)*

ment?
A. with all paperwork that goes thourgh my office it is done by email or by Viper Scanner and Nothing else. As the agencies that I deal with all use Viper.
Q. Is there anything else you would like to add to this statement?
A. NO!!!END STATEMENT!!! (b)(6)(b)(7)(C)

AFFIDAVIT

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

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

WITNESSES:

ORGANIZATION OR ADDRESS

ORGANIZATION OR ADDRESS

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 28 day of MAY 2010 at 2BCT Annex Bldg FOB Hammer

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

SFC (b)(6)(b)(7)(C)
(Typed Name of Person Administering Oath)

10 USC 936
(Authority To Administer Oaths)

INITIALS OF PERSON M (b)(6)(b)(7)(C) PAGE 2 OF 2 PAGES

DA FORM 2823, NOV 2006 APD PE v1.01ES

COMMANDER'S AUTHORIZATION TO SEARCH
For the use of this form see USACIDC Supplement 1 to AR 190-22

TO: CPT (b)(6)(b)(7)(C) CMDR, HHC, 2/10TH MTN BDE, FOB HAMMER, 09308
(Name and Organization of the person to whom authorization is given)

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

Central Baghdad CID Office, USACIDC, Camp Liberty, IRAQ, APO AE 09342
(Organization or Address of Affiant)

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

SPC (b)(6)(b)(7)(C) SIPR computer

for the property described as One SIPR computer located within the Paralegal office, BDE Annex building.

bring this authorization to the attention of the *(person searched) (person in possession, if any person be found at the place or on the premises searched)*. The search will be made in the *(daytime) (nighttime)*, and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to a USACIDC evidence custodian and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 28TH day of May, 2010.

(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)
HHC, 2BCT 10MTN DIV (LI)

(Signature, typed name, and organization of Commander)

CID FORM 98-R
1 SEP 98

SWORN STATEMENT

FILE NUMBER : 0160-10-CID899
LOCATION : FOB Hammer, Iraq, APO AE 09308
DATE : 28 May 10 (b)(6)(b)(7)(C) TIME: 2030/2258 (b)(6)(b)(7)(C)
NAME : (b)(6)(b)(7)(C)
SSN : XXX-XX-(b)(6)(b)(7)(C) GRADE/STATUS: PFC / RA
ORG/ADDRESS : B Co, 2nd BSTB, 10th Mountain Division, FOB Hammer, Iraq

I, (b)(6)(b)(7)(C) want to make the following statement under oath:
I briefly talked to SPC Manning last year. He seemed to be very interested in news relating to his job, he said he would brief current events at work. I believe SPC Manning to be a kind person, he does not drink but he does smoke cigarettes. He did not have a vehicle in Garrison, nor did I see him leave often. I have never been in his room nor have I spent time outside of work hours with him other then random occurrences in the hallway or parking lot. (b)(6)(b)(7)(C)
Q: SA (b)(6)(b)(7)(C)
A: PFC (b)(6)(b)(7)(C)
Q: Did you type the above narrative?
A: Yes. (b)(6)(b)(7)(C)
Q: How long did you talk to SPC MANNING last year?
A: It was more of random occurrences as he was at brigade level and I was company level. I talked to him at briefly at JRTC and on occasions. Our conversations were brief in nature. (b)(6)(b)(7)(C)
Q: What did those conversations consist of?
A: The one at JRTC was a group of S2 people joking around at 0300 in the morning. We were just trying to keep awake due to the hours. There was no meaningful content. I can't think of another time we talked for any particular length of time. At some point I found out he was from England, but I don't remember when I found this out. PFC MANNING use to be very happy, very hyper individual, but his leadership wore him down. He was upset that no one cared about the mission. The unit made it very difficult on PFC MANNING as it seemed to outcast him as though they were trying to get him out of the Army. (b)(6)(b)(7)(C)
Q: Did you see any examples of the unit trying to get rid of PFC MANNING?
A: I saw very little as I did not work in the same room as him. I have heard other people talking about how the unit was treating PFC MANNING. An example of what the unit did was placed another Soldier of equal rank in a leadership position in the shop when she was not qualified over PFC MANNING. (b)(6)(b)(7)(C)
Q: Did you have any direct conversations with PFC MANNING about these situations?
A: No. I might have talked to him at the DFAC about it, but I don't remember.
Q: Did you have a conversation with PFC MANNING pertaining to computer programming? (b)(6)(b)(7)(C)
A: He asked about setting up hash table software and making a security auditing business out of it. I told him that it was already publicly available enough to not be viable. (b)(6)(b)(7)(C)
Q: What does hash table software do?
A: When you make a password, it is run through a one-way hash algorithm to obfuscate your password so that no one can reuse it. A hash table is a table of passwords and their associated hashes. (b)(6)(b)(7)(C)
INITIALS OF PERSON MAKING STATEMENT: (b)(6)(b)(7)(C)

"Statement of (b)(6)(b)(7)(C) taken on, 28 May 10, at FOB Hammer Continued:"
Q: What would be the benefit of developing this type of software?
A: The software is already publically available. It allows you to type in a password and it will provide the appropriate hash. If you have the person's hash you can use the software, put the hash into the program, and if it's a hash in the table the program will come up with a password that matches the hash. (b)(6)(b)(7)(C)
Q: Other than trying to market the program did PFC MANNING state what he was planning to use the program for?
A: No. (b)(6)(b)(7)(C)
Q: Have you ever heard PFC MANNING talking about computer hacking?
A: No. (b)(6)(b)(7)(C)
Q: Other than the above conversation did PFC MANNING discuss any other computer endeavors or desires?
A: No. (b)(6)(b)(7)(C)
Q: Did PFC MANNING ever discuss the Apache shooting incident with you?
A: No. (b)(6)(b)(7)(C)
Q: Did he bring it to your attention when the news broke the WikiLeak story about the Apache shooting?
A: No. (b)(6)(b)(7)(C)
Q: Did PFC MANNING act any different either before or after the WikiLeak story broke on the news?
A: I do not have the information to answer the question. I have not talked to PFC MANNING in several months. (b)(6)(b)(7)(C)
Q: When was the last time you talked to PFC MANNING?
A: I don't remember I know it's been several months though. (b)(6)(b)(7)(C)
Q: Do you know if PFC MANNING has ever had an accidental disclosure?
A: No. (b)(6)(b)(7)(C)
Q: Have you ever seen PFC MANNING attempting to work in the SCIF by himself or before and after normal work hours?
A: No. There has to be two people in the room at all times. (b)(6)(b)(7)(C)
Q: Have you ever seen PFC MANNING placing a classified disk into the unclassified computer?
A: No. (b)(6)(b)(7)(C)
Q: Have you ever seen PFC MANNING with classified material outside the SCIF?
A: Yes, He was on trash and burn detail for the SCIF, where he was involved in the destruction of classified material. (b)(6)(b)(7)(C)
Q: Was PFC MANNING properly supervised during this detail?
A: I believe there were other people present and he was never left alone as far as I remember. (b)(6)(b)(7)(C)
Q: How difficult would it be for PFC MANNING to remove classified information from the SCIF?
A: As easy as removing classified material from any other SCIF. (b)(6)(b)(7)(C)
Q: Is there any additional information pertaining to this investigation that has not been discussed that needs to be addressed in this statement?
A: No. (b)(6)(b)(7)(C)

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

"Statement of (b)(6)(b)(7)(C) taken on, 28 May 10, at FOB Hammer Continued:"

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

A: The network computer security in the housing units are very lax as anyone can get on the system by guessing the simple password. You can also access other peoples computers as individuals leave there sharing on. All users network passwords are readable by LN personnel and it would be easy to recover someone else's password by looking at the screen when inputting your own password. (b)(6)(b)(7)(C)

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

A: No (b)(6)(b)(7)(C)

Q: Is this statement an accurate depiction of our conversation?

A: Yes.///END OF STATEMENT/// (b)(6)(b)(7)(C)

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

"Statement of (b)(6)(b)(7)(C) taken on, 28 May 10, at FOB Hammer Continued:"

AFFIDAVIT

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

(b)(6)(b)(7)(C)
(Signature of Person Making Statement)

WITNESSES:

Subscribed and sworn to before me, a person authorized by law to administer oaths, on this 28th day of May, 2010, at FOB Hammer, Iraq, APO AE 09308

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

ORGANIZATION AND ADDRESS

SA (b)(6)(b)(7)(C), (b) (7)(E)
(Typed Name of Person Administering Oath)

10 USC 936
(Authority to Administer Oath)

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

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

AFFIDAVIT SUPPORTING REASONABLE BELIEF PFC MANNING HAS CLASSIFIED INFORMATION, HAS SENT CLASSIFIED INFORMATION, AND WILL ATTEMPT TO SEND MORE CLASSIFIED INFORMATION

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

I, Special Agent, (b)(6)(b)(7)(C) of the 25th Military Police Detachment (CID), Central Baghdad CID Office, Camp Liberty, Iraq, been first duly sworn, hereby depose and state as follows:

On 27 May 10, my office was notified by CW4 (b)(6)(b)(7)(C) Operations Officer, 11th Military Police Battalion (CID), that PFC Manning is believed to have unlawfully obtained and released sensitive data including, but not limited to, TS-SCI and CABLE clearance documents onto the internet. PFC Manning is an Army Intelligence Analyst and was assigned to the S2 Section of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Baghdad, Iraq.

The following information was received from a non-government agency. Due to security concerns, the name of the agency will be withheld. The withholding of the name should in no way effect the reliability of the information they provided. This agency studies attack attribution, cause and effect relationships, and are involved in the development of tools, methodologies, and solutions to the intelligence problems of today and tomorrow. This agency provides OSINT and HUMINT from various projects both in the United States and abroad. In the past they have briefed the Office of the Secretary of Defense on issues related to Iran and provided the DoD operational manuals on the infrastructure of Iran. The information obtained from this agency is considered reliable.

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

On 27 May 10, the Stars and Stripes newspaper printed an article written by Joby Warrick of The Washington Post. The article, titled "*A wiki for a world of secrets*", was written about the WikiLeaks website. The article stated "Some of the harshest criticism came after last month's Iraq video, which portrayed a U.S. Apache helicopter's assault on a group of Iraqis in Baghdad that killed several civilians, including two employees of the Reuters news service. An edited 17-minute version of the video – donated by an anonymous source and decrypted with the help of volunteers – was posted on the WikiLeaks site April 5 under the heading "collateral murder." Edited and unedited versions of the video have been viewed nearly 8 million times."

On 27 May 10, the affiant using the above mentioned information obtained a Search and Seizure Authorization for the search of PFC Manning's work terminals and a search of his designated living area for any and all electronic media storage equipment/devices. While executing the Search Authorization within PFC Manning's living area, a DVD bearing "Secret" markings and labeled "12 Jul 07 Chopper Reuters" was discovered within a USPS box, which appeared to be packaged for shipment.

An interview of PFC Manning's roommate, SPC (b)(6)(b)(7)(C) MP, revealed although PFC Manning rarely mailed out boxes; he had mailed three packages last month, late Apr 10 time frame.

Between 27-28 May 10, the affiant and a team of CID Special Agents conducted various canvass interviews, which revealed approximately three weeks ago (early May 10) PFC Manning received an Article 15 for assaulting a co-worker, wherein he was transferred from the S2 Section to the Unit Supply. While performing his duties with the supply section, PFC Manning would have no reason or means to access classified information. Although, approximately one week ago PFC Manning entered the office of SPC (b)(6)(b)(7)(C) Brigade Paralegal, and asked if he could scan Secret documents to her computer to be printed off, twice. PFC Manning informed SPC (b)(6)(b)(7)(C) this was a request from the Supply NCOIC. After scanning the documents to SPC (b)(6)(b)(7)(C) which she printed, PFC Manning requested she delete the emails from the computer files completely. When this office coordinated with the Supply NCOIC he related he never informed PFC Manning to scan Secret documents, and that no one in the supply section, including PFC Manning, would have any reason to review secret documents.

(b) (7)(D)

Based on the aforementioned 12 Jul 07 Chopper leak, it can be surmised that PFC Manning illegally obtained a copy of the 15-6 investigation pertaining to the incident in Afghanistan and provided that for submission on WikiLeaks as well.

A review of all the information obtained to date established probable cause that PFC Manning was responsible, at a minimum, for the classified video of the aforementioned Baghdad helicopter attack being posted to the internet. It is further reasonable to believe, based on the information PFC Manning had access to that he may submit additional classified information in the future if this incident is not immediately investigated and computer evidence seized and examined.

TYPED NAME AND ORGANIZATION OF AFFIANT:

SA (b)(6)(b)(7)(C)
25th Military Police Detachment (CID)
Camp Liberty, Iraq

SIGNATURE OF AFFIANT:

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

SWORN TO AND SUBSCRIBED BEFORE ME THIS 29 DAY OF MAY 10, AT 1054 HRS, AT COS HAMMER, IRAQ.

NAME, ORGANIZATION AND OFFICIAL

CPT (b)(6)(b)(7)(C)
Office of the Staff Judge Advocate
COS Hammer, Iraq

SIGNATURE OF AUTHORITY:

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

CAPACITY OF AUTHORITY ADMINISTERING THE OATH:

Judge Advocate
10 U.S.C. 1044(a)

SEARCH AND SEIZURE AUTHORIZATION

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

TO: Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), US Army Criminal Investigations Command (USACIDC), Camp Liberty, APO AE 09342, USA **AND/OR** any CID Special Agent, **AND/OR** other Law Enforcement Official deemed needed.

An affidavit having been made before me by:

Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), Camp Liberty, APO AE 09342,

(which affidavit is attached hereto and made part of this authorization), and as I am satisfied that there is probable cause to believe the matters mentioned in the affidavit are true and correct, that the offenses of:

UCMJ Art 106a: Espionage
18 USC § 793: Gathering, Transmitting, or Losing Defense Information
18 USC § 798: Disclosure of Classified Information

set forth therein has been committed, and the evidence to be seized is located in:

Two US Government owned laptop computers: Alienware laptop, serial number NKD900TA6D00661 and Dell laptop, serial number HLVJQF1; and the following property seized from Bradley E. Manning's current residence: one Apple laptop, serial number W8939AZ066E; two Memorex CD's, serial numbers 1308120503204625 and 1308120503204624; one Imation CD, serial number LD623 MJ04184038 B16; one Samsung cellular telephone, serial number RPRS303202D, containing SIM card, serial number 525033, 8901260520008043773; eight Memorex DVD's, serial numbers 2009052100920487, 2009052100920485, 2009052100920483, 2009052100920481, 2009052100920471, 1909052107834102, 1909052107834101, and 2009052104924365; one Seagate external hard drive, serial number 2GEWJKLJ; and one Kodak camera, serial number KCXKS9 containing a Scandisk, bearing serial number BE0828613591D.

For the property described as:

Digital evidence of the commission of the above cited offenses or any device or media capable of storing digital data (thus digital evidence), including tapes, cassettes, cartridges, optical disks, floppy disks, flash media, thumb drives, micro drives and hard disk drives.

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

Evidence Custodian, USACIDC, USA.

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

Dated this 31st Day of May, 2010.

NAME AND GRADE OF AUTHORIZING OFFICIAL:	DUTY POSITION OF AUTHORIZING OFFICIAL:
CPT (b)(6)(b)(7)(C)	Military Magistrate
ORGANIZATION OF AUTHORIZING OFFICIAL:	**SIGNATURE OF AUTHORIZING**
Office of the Staff Judge Advocate, USD-C, Camp Liberty, APO AE 09342	(b)(6)(b)(7)(C) [redacted]

DA FORM 3745-E, Mar 85 (gen)

COMMANDER's SEARCH AND SEIZURE AUTHORIZATION

For use of this form see USACIDC Supplement 1 to AR 190-22

TO: Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), US Army Criminal Investigations Command (USACIDC), Camp Liberty, APO AE 09342, USA **AND/OR** any CID Special Agent, **AND/OR** other Law Enforcement Official deemed needed.

An affidavit having been made before me by:

Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), Camp Liberty, APO AE 09342.

(which affidavit is attached hereto and made part of this authorization), and as I am satisfied that there is probable cause to believe the matters mentioned in the affidavit are true and correct, that the offenses of:

UCMJ Art 106a, Espionage
18 USC § 793; Gathering, Transmitting, or Losing Defense Information
18 USC § 798; Disclosure of Classified Information

set forth therein has been committed, and that the property to be seized is located (on the person)(at the place) to be searched, you are hereby ordered to search the (person)(place) known as:

Dell laptop, serial number 93114QD1, Toshiba hard drive, serial number Z5FX1422S 6P2 EC A; Seagate hard drive, serial number CN-0MN922-21232-793-002L; and Hitachi hard drive, serial number 070817DP0C10DSG2J1DP

For the property described as:

Digital evidence of the commission of the above cited offenses or any device or media capable of storing digital data (thus digital evidence), including tapes, cassettes, cartridges, optical disks, floppy disks, flash media, thumb drives, micro drives and hard disk drives.

bring this authorization to the attention of the (person searched)(person in possession, if any person be found at the place or on the premises searched). The search will be made in the (daytime) (nighttime), and if the property is found there, you shall seize it, issue a receipt therefor to the person from whom the property is taken or in whose possession the property is found, deliver the property to a USACIDC evidence custodian and prepare a written inventory of the property. If there is no person at the searched place to whom the receipt may be delivered, the receipt will be left in a conspicuous location at the place or on the premises where the property is found.

Dated this 31st Day of May, 2010.

NAME AND GRADE OF AUTHORIZING OFFICIAL:	DUTY POSITION OF AUTHORIZING OFFICIAL:
CPT (b)(6)(b)(7)(C)	Company Commander and Property Book Holder
ORGANIZATION OF AUTHORIZING OFFICIAL: Headquarters and Headquarter Company, 2nd Brigade Combat Team, 10th Mountain Div USD-C, FOB Hammer, APO AE 09308	**SIGNATURE OF AUTHORIZING** (b)(6)(b)(7)(C)

CID FORM 98-R
1 Sep 98

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

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

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

I. I, SA (b)(6)(b)(7)(C), (b) (7)(E) (Name), Central Baghdad CID Office, 11th MP BN (CID), (Organization or Address)

Camp Liberty, APO AE 09342

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

On 27 May 10, this office was notified that PFC MANNING was believed to have unlawfully obtained and released sensitive data including, but not limited to, TS-SCI and CABLE clearance documents onto the internet. PFC MANNING is an Army Intelligence Analyst and was assigned to the S2 Section of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This information was obtained through a non-government agency, which chooses to remain unnamed; however, the withholding of this organization should have no effect of the information provided. This agency studies the attack attribution, cause and effect relationships, and are involved in the development of tools, methodologies, and the solutions to the intelligence problems of today and tomorrow; and provides OSINT and HUMINT from various projects to the United States and abroad. (b) (7)(D)
(b) (7)(D)

2. The affiant further states that:

(b) (7)(D)

On 27 May 10, the affiant using the above mentioned information obtained a Search and Seizure Authorization for the search of PFC Manning's work terminals, and a search of his designated living area for any and all electronic media storage devices and classified materials. While executing the Search Authorization within PFC Manning's living area, a DVD bearing "Secret" marking and labeled "12 Jul 07 CZ Engagement Zone 30 GC" was discovered within a USPS box, which appeared to be packaged for shipment.

An interview of PFC Manning's roommate, SPC (b)(6)(b)(7)(C) MP, revealed although PFC Manning rarely mailed out boxes; he had mailed three packages last month, late Apr '10 time frame. SPC (b)(6)(b)(7)(C) related there was only one mailing service at FOB Hammer, which was the FOB Hammer Post Office.

Further between 27-28 May 10, the affiant and a team of CID Special Agents conducted various canvass interviews of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer; which revealed approximately three weeks ago (early May '10) PFC Manning received an Article 15 for assaulting a co-worker. As a result, PFC Manning was transferred from the S2 Section to the Unit Supply Office. While performing his duties with the supply section PFC Manning would have no reason or means to access classified information. Although, approximately one week ago PFC Manning entered the office of SPC (b)(6)(b)(7)(C) Paralegal, on two separate occasions requesting if he could scan Secret documents to her computer to be printed off. PFC Manning informed SPC (b)(6)(b)(7)(C) this was at the request of the Supply NCOIC. After scanning the documents to SPC (b)(6)(b)(7)(C) computer, which she printed, PFC Manning requested her to completely delete the emails from her computer. When this office coordinated with the Supply NCOIC he related he never informed PFC Manning to scan Secret documents, and that no one in the supply section, including PFC Manning, would have any reason to view classified materials.

Based on the aforementioned 12 Jul 07, Apache leak, and the coincidental situation involving PFC Manning claiming he leaked it and the discovery of the Secret DVD in his designated living area, it can be surmised that PFC Manning illegally obtained a copy of the AR 15-6 Investigation pertaining to the incident in Afghanistan and provided that for submission to WikiLeaks as well. PFC Manning has been deployed to Iraq since Oct 09 it is reasonable to assume he has obtained an unknown quantity of classified materials. PFC Manning as also demonstrated that even after being removed from the S2 Section he has still obtained resources to classified documents and systems. It is further reasonable to believe, based on this information that PFC Manning has had access to, that he may have submitted or is currently storing additional classified information for future dissemination. For this investigation it is imperative for USACIDC to identify, seize, and examine all computers and digital storage media device PFC Manning has had access to.

SEARCH AND SEIZURE AUTHORIZATION 0160-10-CID899-14463

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

TO: Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), US Army Criminal Investigations Command (USACIDC), Camp Liberty, APO AE 09342, USA AND/OR any CID Special Agent, AND/OR other Law Enforcement Official deemed needed.

An affidavit having been made before me by Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), Camp Liberty, APO AE 09342, which affidavit is attached hereto and made part of this authorization, and as I am satisfied that there is probable cause to believe the matters mentioned in the affidavit are true and correct, that the offenses of:

UCMJ Art 106a: Espionage
18 USC § 793: Gathering, Transmitting, or Losing Defense Information
18 USC § 798: Disclosure of Classified Information
18 USC § 1030: Fraud and related activity in connection with computers

set forth therein has been committed, and the property described as:

From the S2 Section, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Seagate Hard Drive, model number ST980825A, serial number 3MH036M1; extracted from Alienware laptop computer, serial number: NKD900TA6D00661 "Secret"
b. Unknown make and model Hard Drive, serial number 5MH0HWKN; extracted from Dell laptop computer, serial number HLVJQFI "Secret"
c. Unknown make and model Hard Drive, serial number 5MH0TB78; extracted from Dell laptop computer, serial number 93H4QD1 "Unclassified"

From the Supply Office, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Seagate Hard Drive, serial number CN-0MN922-21232-793-002L "Secret"
b. Hitachi Hard Drive, serial number 070817DP0C10DSG2J1DP "Unclassified"

From the Paralegal Office, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Toshiba Hard Drive, serial number Z5FX1422S 6P2 EC A "Secret"

From the digital Network Logs maintained by the S6 Section, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. (2) Imation CDs, serial numbers LD621 MK06232788 A20 and LD621 MK06232576 B10

From Room 4C93, designated living area of PFC Manning, LSA Dragon, FOB Hammer, Iraq:

a. Apple laptop computer, serial number W8939AZ066E
b. (2) Samsung CDs, serial numbers 1308120503204625 and 1308120503204624
c. Samsung Cellular Telephone, serial number RPRS303202D containing SIM card, serial number 525033 8901260520008043773

d. (8) Memorex DVD-RW, serial numbers 2009052100920487, 2009052100920485, 2009052100920483, 2009052100920481, 2009052100920471, 1909052107834102, 1909052107834101, and 2009052104924365
e. Seagate hard drive, serial number 9VS1S2TZ; extracted from Seagate External Hard Drive serial number 2GEWJKLJ
f. Imation CD, serial number LD623 MJ04184038 B16 "Secret"
g. Kodak Camera, serial number KCXKS9 containing Scandisk Memory Card, serial number BE0828613591D

From SSG (b)(6)(b)(7)(C) Supply NCOIC, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. SAMSUNG Hard Drive, serial number S1AKJDNQ816517; extracted from HP laptop computer, serial number CNF8492K3S

previously seized under proper legal authority (see Commander's Search and Seizure Authorization, dated 27 and 28 May 10, authorized by CPT (b)(6)(b)(7)(C) Commander, Headquarters and Headquarters Company, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq, APO AE 09308; and Search and Seizure Authorization, 27 May 10, authorized by CPT (b)(6)(b)(7)(C) Military Magistrate, USF-I, Camp Liberty, Iraq, APO AE 09342), which is presently located within the Evidence Depository, 11th MP BN (CID), USACIDC, Camp Arifjan, Kuwait, APO AE 09366.

Dated this 5th Day of June, 2010.

NAME AND GRADE OF AUTHORIZING OFFICIAL:	DUTY POSITION OF AUTHORIZING OFFICIAL:
CPT (b)(6)(b)(7)(C)	Military Magistrate
ORGANIZATION OF AUTHORIZING OFFICIAL:	SIGNATURE OF AUTHORIZING
Office of the Staff Judge Advocate, USD-C, Camp Liberty, Iraq APO AE 09342	(b)(6)(b)(7)(C) [redacted]

DA FORM 3745-E, Mar 85 (gen)

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

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

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 4

1. I, Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), US Army Criminal Investigations Command, Camp Liberty, APO AE 09342 having been duly sworn, on oath depose and state that:

On 27 May 10, this office was notified that PFC Manning was believed to have unlawfully obtained and released sensitive data including, but not limited to, TS-SCI and CABLE clearance documents onto the internet. PFC Manning is an Army Intelligence Analyst and was assigned to the S2 Section of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This information was obtained through a non-government agency, which chooses to remain unnamed; however, the withholding of this organization should have no effect on the information provided. This agency studies the attack attribution, cause and effect relationships, and are involved in the development of tools, methodologies, and the solutions to the intelligence problems of today and tomorrow; and provides OSINT and HUMINT from various projects to the United States and abroad.

(b) (7)(D) [redacted]

(b) (7)(D) [redacted]

On 27 May 10, the affiant using the above mentioned information obtained a Search and Seizure Authorization for the search of PFC Manning's work terminals, and a search of his designated living area for any and all electronic media storage devices and classified materials. While executing the Search Authorization within PFC Manning's living area, a DVD bearing "Secret" marking and labeled "12 Jul 07 CZ Engagement Zone 30 GC" was discovered within a USPS box, which appeared to be packaged for shipment.

An interview of PFC Manning's roommate, SPC (b)(6)(b)(7)(C) MP, revealed although PFC Manning rarely mailed out boxes; he had mailed three packages last month, late Apr '10 time frame. SPC (b)(6)(b)(7)(C) related there was only one mailing service at FOB Hammer, which was the FOB Hammer Post Office.

Further between 27-28 May 10, the affiant and a team of CID Special Agents conducted various canvass interviews of the 2nd Brigade Combat Team, 10th Mountain Division, FOB

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND (CONTINUED)

Hammer; which revealed approximately three weeks ago (early May '10) PFC Manning received an Article 15 for assaulting a co-worker. As a result, PFC Manning was transferred from the S2 Section to the Unit Supply Office. While performing his duties with the supply section, PFC Manning would have no reason or means to access classified information. Although, approximately one week ago PFC Manning entered the office of SPC (b)(6)(b)(7)(C) Paralegal, on two separate occasions requesting if he could scan Secret documents to her computer to be printed off. PFC Manning informed SPC (b)(6)(b)(7)(C) his was at the request of the Supply NCOIC. After scanning the documents to SPC (b)(6)(b)(7)(C) computer, which she printed, PFC Manning requested her to completely delete the emails from her computer. When this office coordinated with the Supply NCOIC he related he never informed PFC Manning to scan Secret documents, and that no one in the supply section, including PFC Manning, would have any reason to view classified materials.

2. The affiant further states that: Based on the aforementioned 12 Jul 07, Apache leak, and the coincidental situation involving PFC Manning claiming he leaked the video, and the discovery of the Secret DVD in his designated living area, it can be surmised that PFC Manning illegally obtained a copy of the AR 15-6 Investigation pertaining to the incident in Afghanistan and provided that for submission to WikiLeaks as well. PFC Manning has been deployed to Iraq since Oct 09, it is reasonable to assume he has obtained an unknown quantity of classified materials. PFC Manning as also demonstrated that even after being removed from the S2 Section he has still obtained resources to classified documents and systems. It is further reasonable to believe, based on this information that PFC Manning has had access to, that he may have submitted or is currently storing additional classified information for future dissemination. For this investigation it is imperative for USACIDC to conduct a forensic examination of all items seized during the course of the preliminary investigation.

3. In view of the foregoing, the affiant request that an authorization be issued for the digital forensic search of the following items seized as evidence in relation to the offenses of: UCMJ Art 106a: Espionage; 18 USC § 793: Gathering, Transmitting, or Losing Defense Information; 18 USC § 798: Disclosure of Classified Information; and 18 USC § 1030: Fraud and related activity in connection with computers:

From the S2 Section, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Seagate Hard Drive, model number ST980825A, serial number 3MH036M1; extracted from Alienware laptop computer, serial number: NKD900TA6D00661 "Secret"
b. Unknown make and model Hard Drive, serial number 5MH0HWKN; extracted from Dell laptop computer, serial number HLVJQF1 "Secret"
c. Unknown make and model Hard Drive, serial number 5MH0TB78; extracted from Dell laptop computer, serial number 93H4QD1 "Unclassified"

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND (CONTINUED)

From the Supply Office, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Seagate Hard Drive, serial number CN-0MN922-21232-793-002L "Secret"
b. Hitachi Hard Drive, serial number 070817DP0C10DSG2J1DP "Unclassified"

From the Paralegal Office, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Toshiba Hard Drive, serial number Z5FX1422S 6P2 EC A "Secret"

From the digital Network Logs maintained by the S6 Section, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. (2) Imation CDs, serial numbers LD621 MK06232788 A20 and LD621 MK06232576 B10

From Room 4C93, designated living area of PFC Manning, LSA Dragon, FOB Hammer, Iraq:

a. Apple laptop computer, serial number W8939AZ066E
b. (2) Samsung CDs, serial numbers 1308120503204625 and 1308120503204624
c. Samsung Cellular Telephone, serial number RPRS303202D containing SIM card, serial number 525033 8901260520008043773
d. (8) Memorex DVD-RW, serial numbers 2009052100920487, 2009052100920485, 2009052100920483, 2009052100920481, 2009052100920471, 1909052107834102, 1909052107834101, and 2009052104924365
e. Seagate hard drive, serial number 9VS1S2TZ; extracted from Seagate External Hard Drive serial number 2GEWJKLJ
f. Imation CD, serial number LD623 MJ04184038 B16
g. Kodak Camera, serial number KCXKS9 containing Scandisk Memory Card, serial number BE0828613591D

From SSG (b)(6)(b)(7)(C) Supply NCOIC, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. SAMSUNG Hard Drive, serial number S1AKJDNQ816517; extracted from HP laptop computer, serial number CNF8492K3S

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND (CONTINUED)

Sworn to and subscribed before me this 5th day of June, 2010, at 1300hrs, at Camp Liberty, Iraq APO AE 09342.

NAME AND ORGANIZATION OF AFFIANT:

SA (b)(6)(b)(7)(C)
Central Baghdad CID Office, 11th MP BN (CID),
Camp Liberty, APO AE 09342

SIGNATURE OF AFFIANT:

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

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

CPT (b)(6)(b)(7)(C)
Military Magistrate, USD-C,
Camp Liberty, APO AE 09342

SIGNATURE OF AUTHORITY:

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

INSTRUCTIONS FOR
AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it had been committed. Use additional page if necessary.

2. In paragraph 2, set forth fact establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraph 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she had plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary.

3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under circumstances for evidentiary matters.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

PAGE 1 OF 1 PAGES

DETAILS

Crime Scene Examination of PFC MANNING's work station: Between 2245 and 2330, 27 May 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) conducted a Crime Scene Examination of the SCIF, Room 14B, Brigade Headquarters Building, FOB Hammer, Iraq.

Characteristics of the Scene: Room 14B was a SCIF designed for the processing, utilization, and storage of classified information. Room 14B was internal to the Brigade Headquarters Building, FOB Hammer, Iraq. The Brigade Headquarters Building was a brown in color, wood and metal type construction building designed to support 24 hour brigade activities. The room consisted of plywood walls and ceiling, and a concrete floor. The Entry/Exit (E/E) was on the south wall near the southeast corner of the room, and opened inward. There were three work stations along the east wall, six work stations along the north wall, four work stations along the south wall, and three work stations on a table in the middle of the room. There was an adjoining storage room in the southwest corner of the room.

Conditions of the Scene: Room 14B was cluttered and dirty. There were multiple maps and documents attached to the walls both unclassified and classified in nature. The floor was dirty and had not been swept or maintained. There were various papers and disposable products strewn across the surface of the work stations. PFC MANNING's SIPR workstation was identified as being either the Dell laptop located on the north wall, second from the northwest corner of the room or the Alien ware computer located on the north wall, third form the northwest corner of the room. A communal NIPR computer which PFC MANNING also used during duty hours was located on the east wall, closest to the southeast corner of the room

Factors Pertinent to Entry/Exit: Room 14B had only one E/E located in the south corner near the southeast corner opening outward. The door was a push button cipher lock. The room was void of windows or a second E/E.

Crime Scene Documentation: SA (b)(6)(b)(7)(C) exposed photographs of Room 14B using a Nikon D80 digital camera with integrated flash and prepared a crime scene sketch.

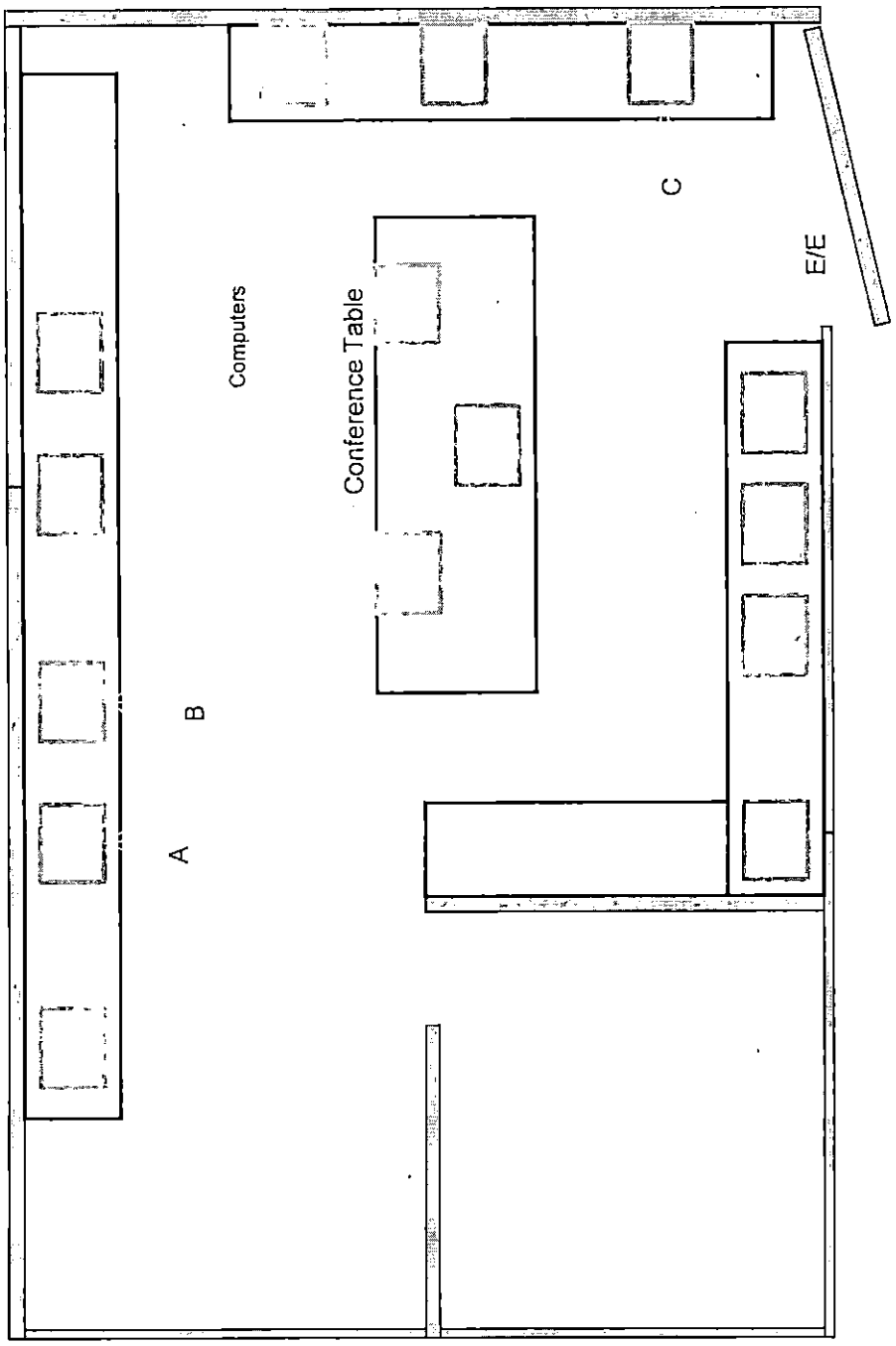
Collection of Evidence: Between 2251-2315, 27 May 10, SA (b)(6)(b)(7)(C) collected two SIPR computers and one NIPR computer from the work area on a DA Form 4137, Evidence Property Custody Document, Document Numbers 0593-10 and 0594-10.

///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C) [redacted]	DATE 27 May 10	EXHIBIT 22

CID FORM 94
1 FEB 77

Rough Sketch Depicting Crime Scene



TITLE BLOCK
CASE NUMBER: 0160-10-CID899-14463
OFFENSE: Disclosure of Classified Information
SCENE PORTRAYED: Room 14B, Brigade Headquarters
LOCATION: FOB Hammer, Iraq
VICTIM: US Government
SUBJECT: PFC MANNING
TIME/DATE BEGAN: 2330/27 May 10
SKETCHED BY: SA [redacted]
VERIFIED BY: SA [redacted]

N

NOT TO SCALE

LEGEND

A: Location of SIPR Computer

B. Location of SIPR Computer

C. Location of NIPR Computer

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 27

Photographic Packet, Crime Scene (SCIF)

0028-10-CID221-10117
0160-10-CID899-14463

1

4

2

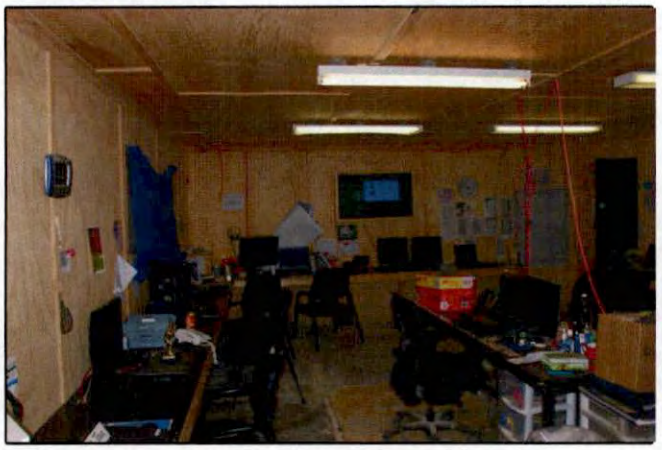
5

3

6

1. Entrance to SCIF, Room 14B, Brigade Headquarters Building, FOB Hammer, Iraq.
2. 360 degree view of SCIF, from E/E to back right corner
3. 360 degree view of SCIF, from E/E to front right corner
4. 360 degree view of SCIF, from back right corner to E/E
5. 360 degree view of SCIF, from front right corner to back left corner
6. 360 degree view of SCIF, from front right corner to back right corner

EXHIBIT 24

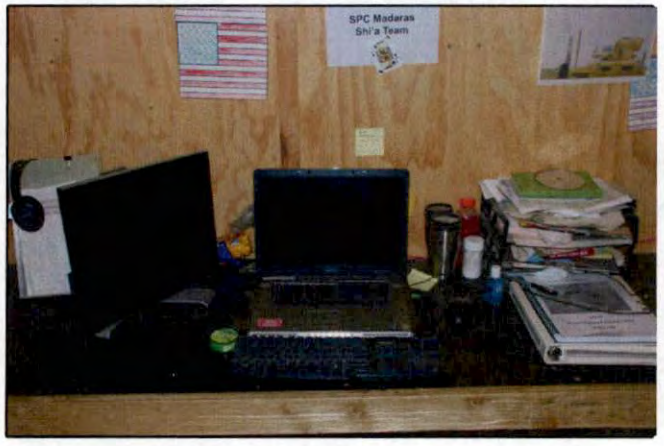


7

10

8

11



9

12

7. View from PFC MANNING's SCIF work stations toward E/E.
8. View of PFC MANNING's SCIF work stations from E/E.
9. PFC MANNING's work station, SIPR Terminal (1).
10. PFC MANNING's work station, SIPR Terminal (2).
11. Communal NIPR terminal to the left of the E/E.
12. View of Communal NIPR Terminal.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

DETAILS

CRIME SCENE EXAMINATION: Between 0030 and 0150, 28 May 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) conducted a Crime Scene Examination of PFC MANNINGS Containerized Housing Unit (CHU), Room C, Building 4C98, LSA Dragon, FOB Hammer, Iraq.

Characteristics of the Scene: CHU Room C was a two-person room located on the west end of building 4C98, LSA Dragon, FOB Hammer, Iraq. The CHU is white and clear of color, metal, glass, and particle board construction designed to house Soldiers while in a deployed environment. The Entry/Exit (E/E) was on the north wall near the northwest corner of the CHU, and opened outward. A bed was located in the northeast corner of the room with a night stand adjacent on the east wall; a second nightstand was against the east wall adjacent to the bed in the southeast corner. There was a wall locker in the southwest corner of the room with the back against the west wall; a second wall locker was located adjacent to it with its back against the west wall.

Conditions of the Scene: Room C was cluttered and dirty. There were clothing and TA-50 items located throughout the room. There were two large plastic containers against the west wall of the room belonging to PFC MANNING's roommate. There was a portable computer stand holding a Macintosh laptop computer adjacent to the side railing of PFC MANNING's bed. There was a tuff box, and two cardboard boxes stacked on top of each other, the one on top containing a CD with a SECRET sticker at the foot of PFC MANNING's bed. There was a pile of TA-50 to include an ACU patterned assault pack at the foot of the bed between the tuff box and the wall locker, pushed against the south wall. There were two CD's located on the top of the nightstand adjacent to PFC MANNING's bed, a cellular telephone in the drawer, and several writable CDs located in the cubby hole of the nightstand. There was TA-50 stored on top of PFC MANNING's wall locker.

Factors Pertinent to Entry/Exit: Room C had only one entrance/exit located in the north wall near the northwest corner opening outward. There was a single window in the middle of the north wall. The door was opened and the window was locked and secured upon our arrival.

Crime Scene Documentation: SA (b)(6)(b)(7)(C) exposed photographs of Room C using a Nikon D80 digital camera with integrated flash while SA (b)(6)(b)(7)(C) prepared a crime scene sketch.

Collection of Evidence: Between 0043-0130, 28 May 10, SA (b)(6)(b)(7)(C) collected a computer from the portable computer stand, CDs from the nightstand, an external hard drive from an ACU patterned assault pack, a pack of eight CDs, a classified CD from a box, and a camera from on top of the tuff box as evidence on a DA Form, Evidence Property Custody Document, Document Number 0579-10.

2nd Search of the Scene: A second search of the scene and the immediate area around the CHU failed to locate anything of evidentiary value.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNATURE (b)(6)(b)(7)(C)	DATE 28 May 10	EXHIBIT 25

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

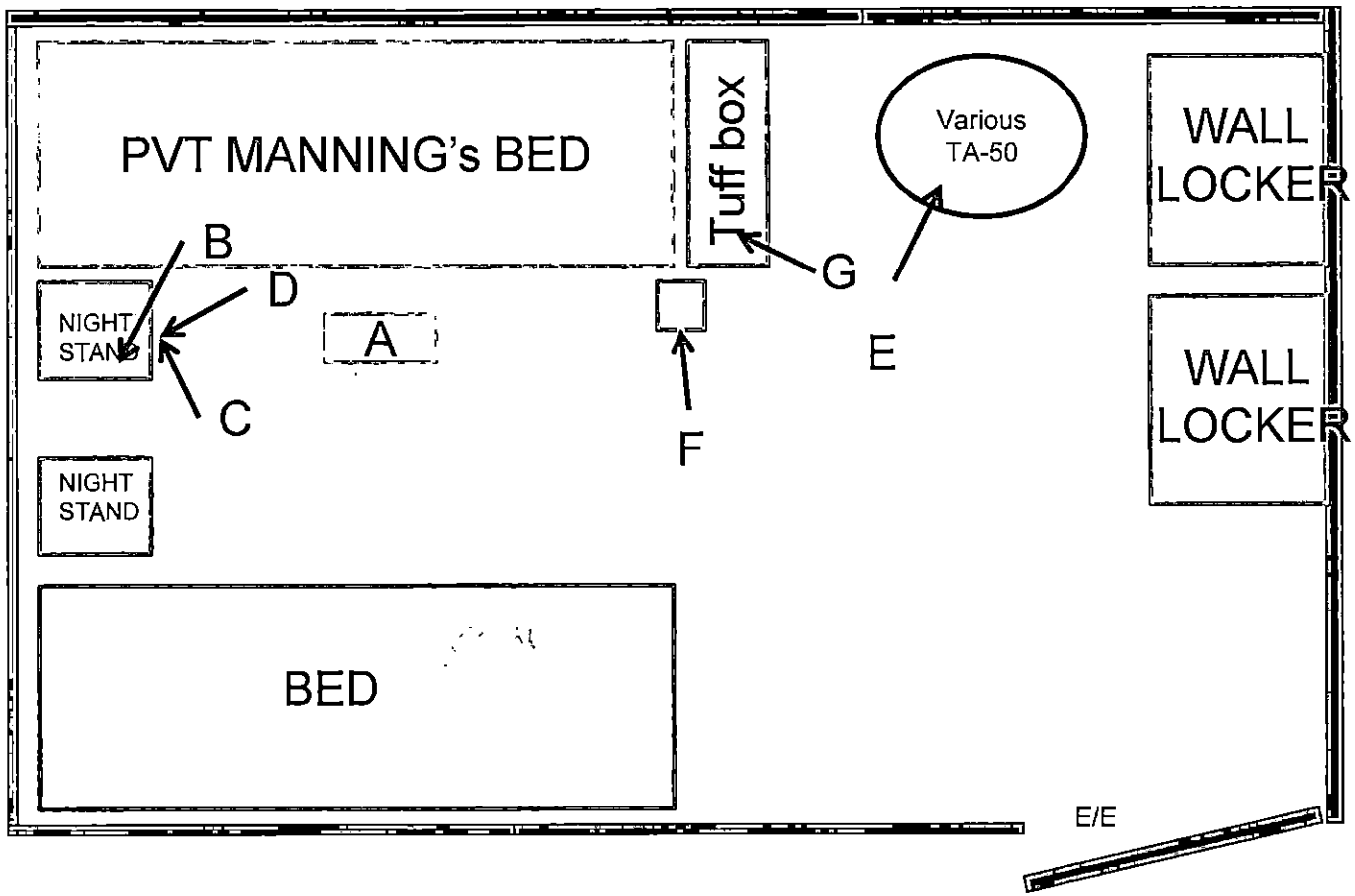
ROI NUMBER
0160-10-CID899-14463

DETAILS

3rd Search of the Scene: A third scarch, conducted during daylight hours, of the immediate area around the CHU failed to identify anything of evidentiary value. ///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIG (b)(6)(b)(7)(C) [redacted]	DATE 28 May 10	EXHIBIT 25

Rough Sketch Depicting PFC MANNING's ROOM



LEGEND

A: Apple laptop computer on computer stand
B. Two writable CDs found on nightstand
C. Cellular Telephone in nightstand drawer
D. Eight DVDs found in nightstand cubby
E. External Hard drive in assault pack
F. CD in box
G. Camera on tuff box

N

NOT TO SCALE

TITLE BLOCK
CASE NUMBER: 0160-10-CID899-14463
OFFENSE: Disclosure of Classified Information
SCENE PORTRAYED: Room 14B, Brigade Headquarters
LOCATION: FOB Hammer, Iraq
VICTIM: US Government
SUBJECT: PFC MANNING
TIME/DATE BEGAN: 0030/28 May 10
SKETCHED BY: SA (b)(6)(b)(7)(C)
VERIFIED BY: SA (b)(6)(b)(7)(C)

0028-10-CID221-10117
0160-10-CID899-14463

Exhibit 26

[redacted]

Photographic Packet, Crime Scene (CHU)

[redacted]0-CID221-10117
0160-10-CID899-14463

1

4

2

5

3

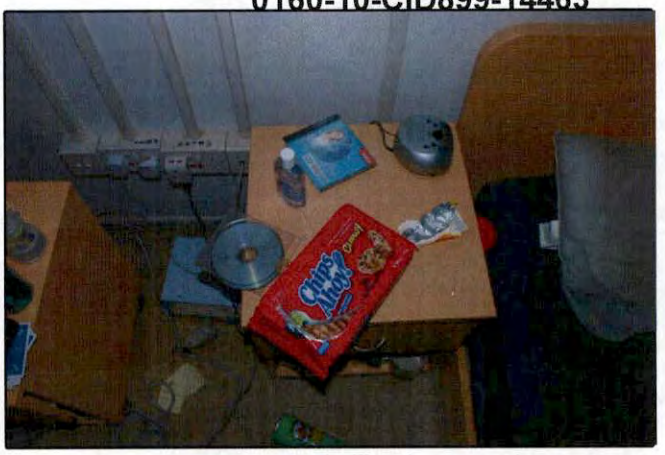
6

1. Entrance to room PFC MANNING's room 4C93-C, FOB Hammer, Iraq.
2. Right side of the room assigned to PFC MANNING.
3. Right side of the room assigned to PFC MANNING.
4. Close view of items at bottom of bed.
5. Right wall locker assigned to PFC MANNING.
6. View of top of wall locker.

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 27

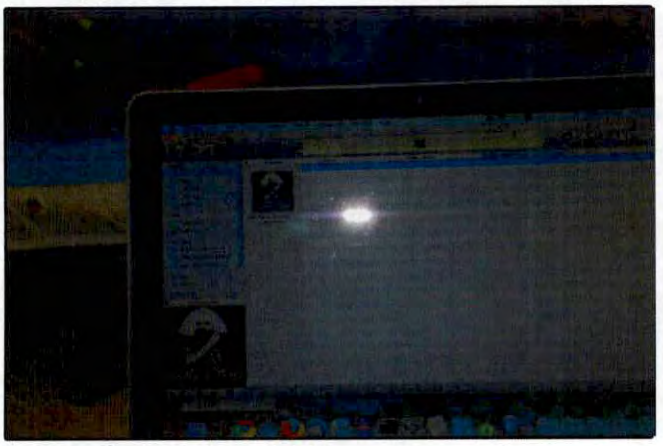
7



10

8

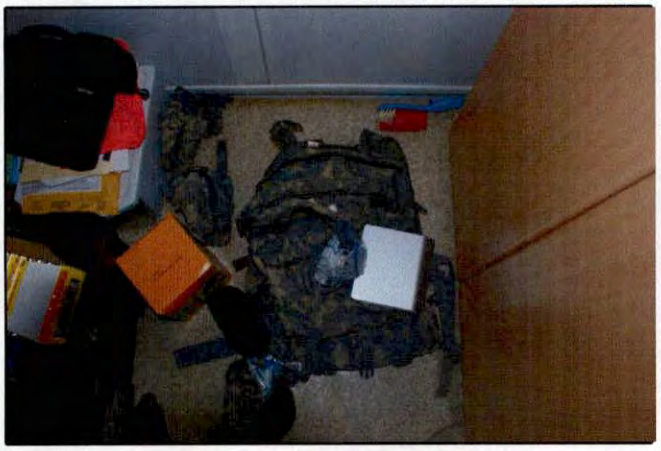
11



9

12

7. View of PFC MANNING's bed, also depicting location of laptop computer.
8. View of PFC MANNING's laptop computer from above.
9. View depicting what was on the computer at time of search.
10. View of PFC MANNING's nightstand and stack of CDs.
11. Inner view of top drawer of night stand.
12. Close-up view of contents of top drawer depicting an cellular phone.



13

16

14

17

15

18

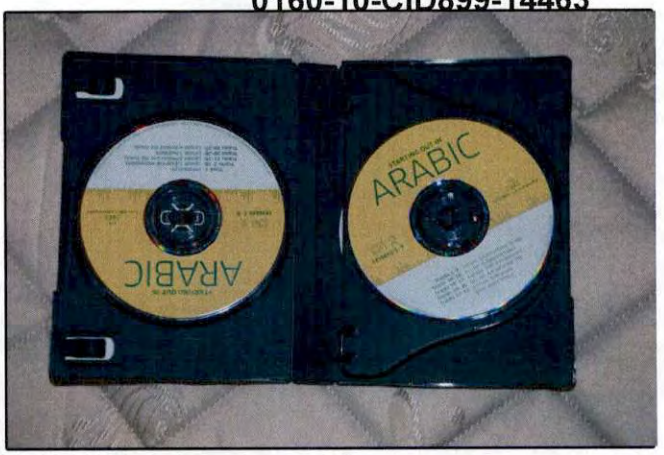
13. View depicting the bag the external hard drive was discovered in.
14. Close-up view of portable hard drive.
15. View of the external hard drive serial number.
16. View of bottom of tuff box depicting location of digital camera.
17. Close-up view of back side of camera.
18. Close-up view of front side of camera.

[redacted] [redacted]

Photographic Packet, Crime Scene (CHU)

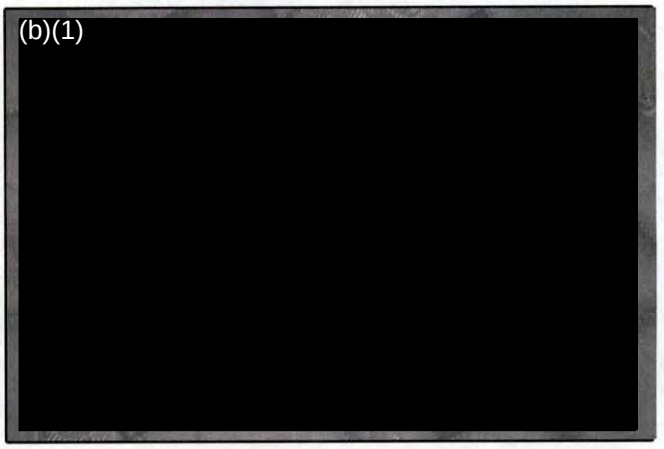
0028-10-CID221-10117
0160-10-CID899-14463

19

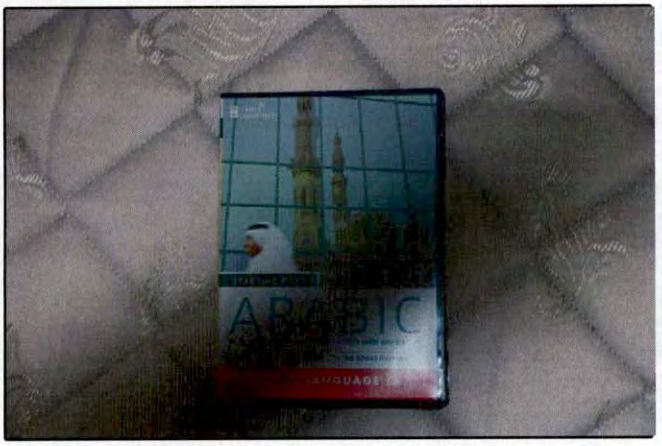


22

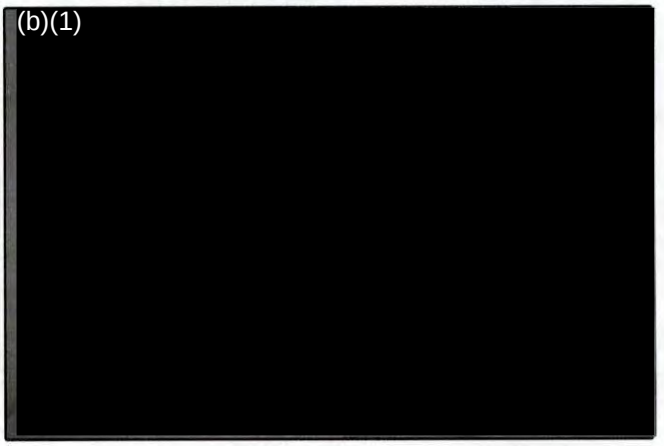
20



23



21



24

19. View of Priority Mail box (Top).
20. View of Priority Mail box (Side).
21. View of CD case found within Priority Mail Box.
22. First two CD sleeves within the CD case.
23. Second two CD sleeves within the CD case.
24. Close-up view of last CD found within the case.

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

EXHIBIT 27

0028-10-CID221-10117

Compact Disc Containing:

- Images from CID ROI 0160-10-CID899-14463

(100028.221)

USACRC Copy

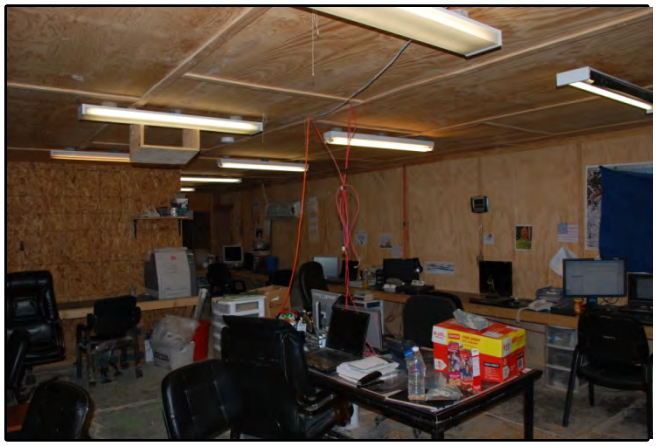
FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE

Exhibit 28

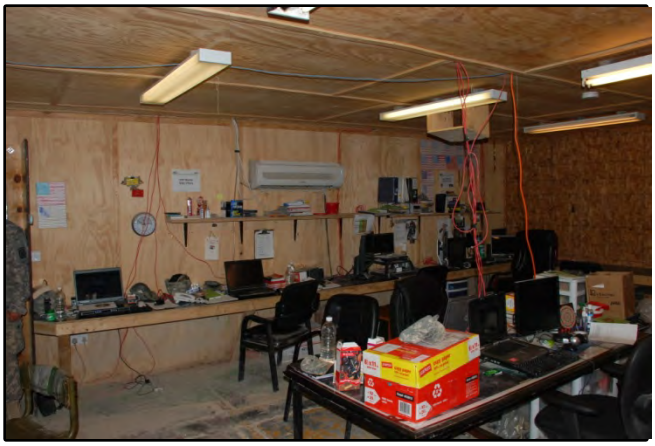
[redacted]

1

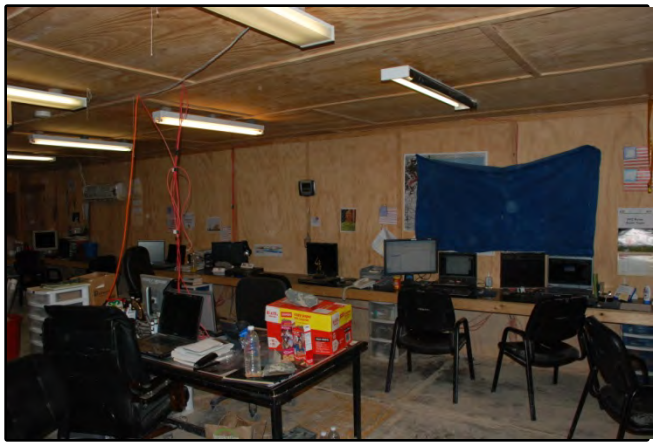
4



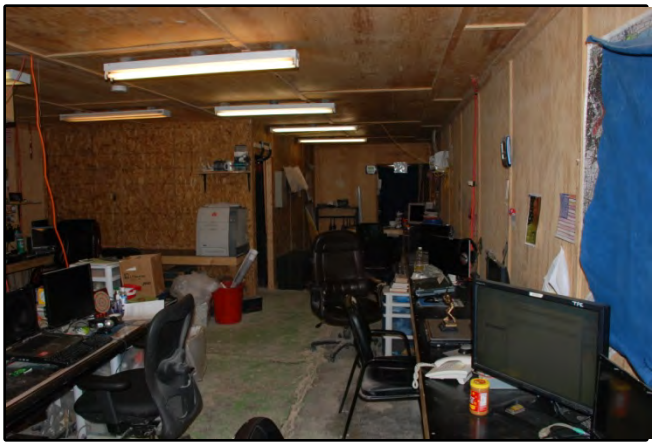
2



5

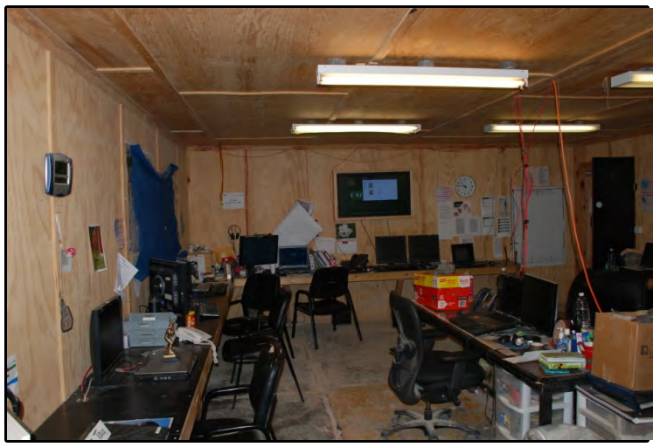


3



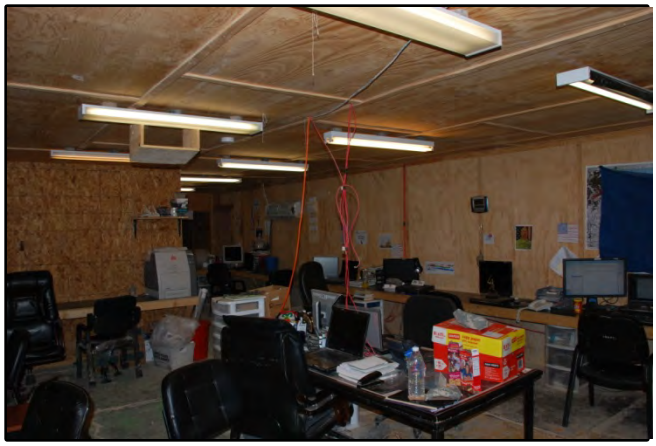
6

1. Entrance to SCIF, Room 14B, Brigade Headquarters Building, FOB Hammer, Iraq.
2. 360 degree view of SCIF, from E/E to back right corner
3. 360 degree view of SCIF, from E/E to front right corner
4. 360 degree view of SCIF, from back right corner to E/E
5. 360 degree view of SCIF, from front right corner to back left corner
6. 360 degree view of SCIF, from front right corner to back right corner



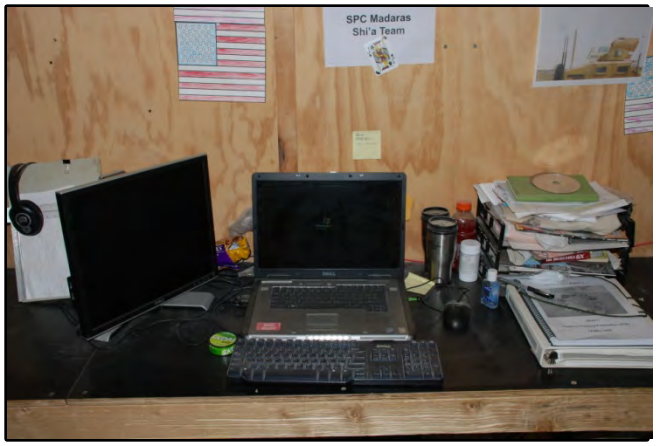
7

10



8

11



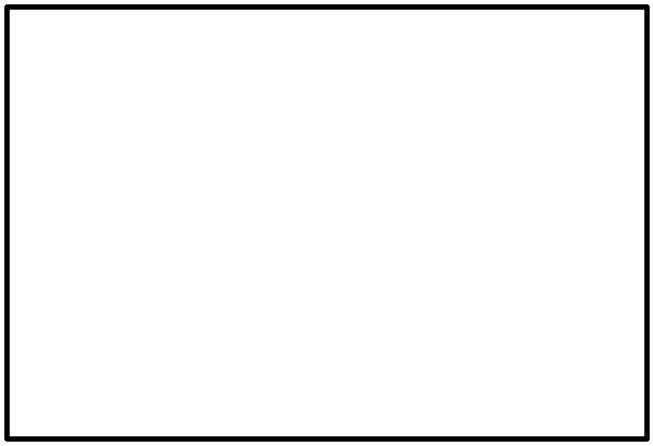
9

12

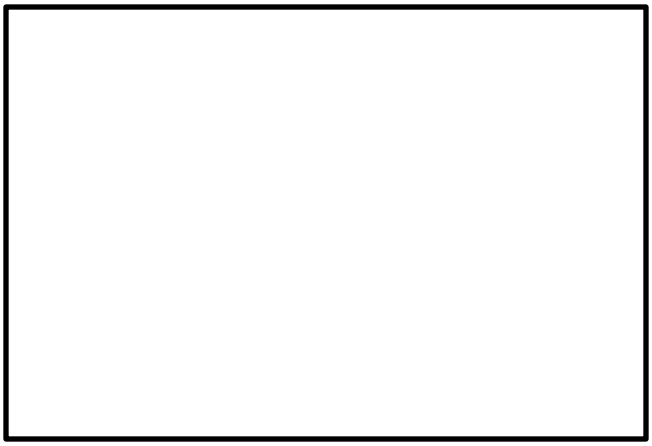
7. View from PFC MANNING's SCIF work stations toward E/E.
8. View of PFC MANNING's SCIF work stations from E/E.
9. PFC MANNING's work station, SIPR Terminal (1).
10. PFC MANNING's work station, SIPR Terminal (2).
11. Communal NIPR terminal to the left of the E/E.
12. View of Communal NIPR Terminal.

13

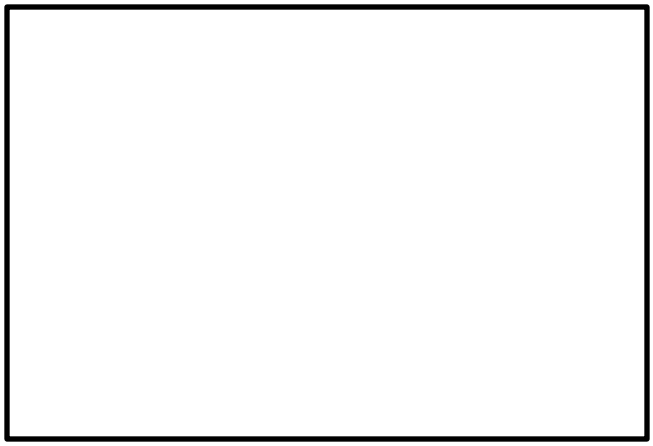
16



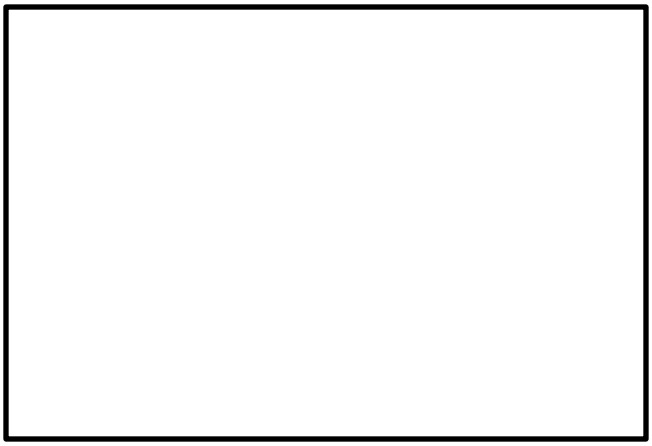
14



17



15

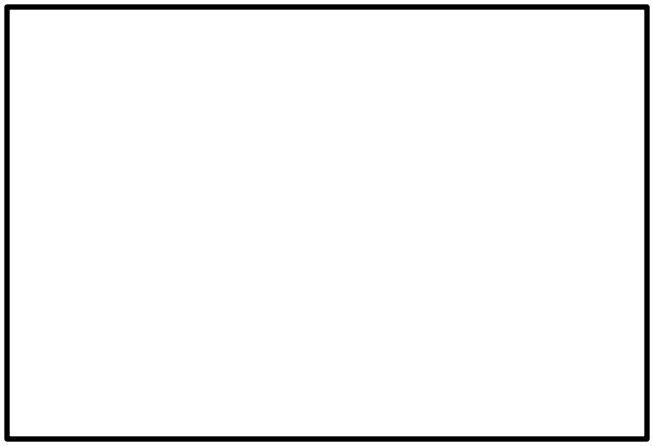


18

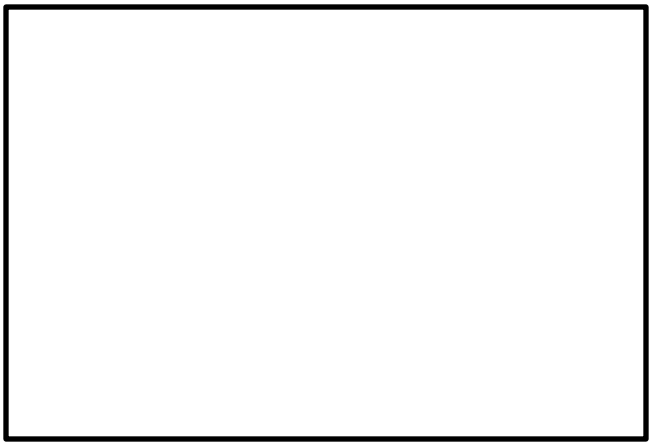
13. Door to 047A, SGT [redacted]' office location.
14. Hall view from door into the Building.
15. Entrance to SGT [redacted]' office area.
16. View into SGT [redacted] office area.
17. SGT [redacted]' desk.
18. SGT [redacted]' desk.

19

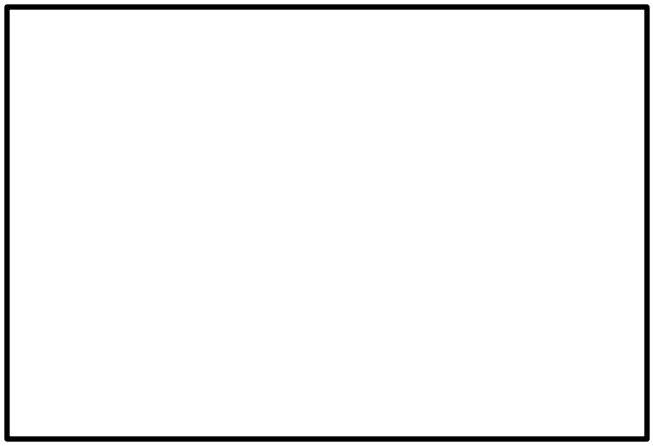
22



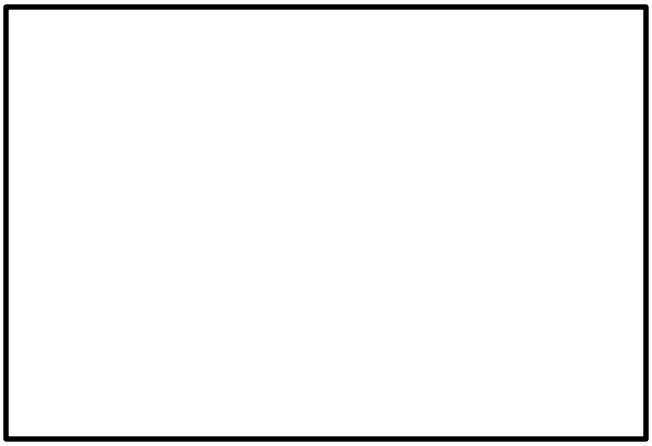
20



23



21



24

19. Closer view of writing in notebook .
20. Envelope addressed to SGT (b)(6)(b)(7)(C)
21. Closer view of sender
22. Closer view of recipient
23. View of official Postal Service stamp
24. View of official Postal Service stamp

25

28

26

29

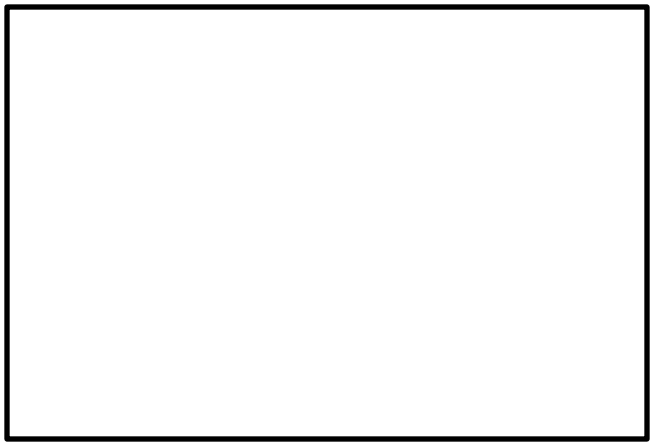
27

30

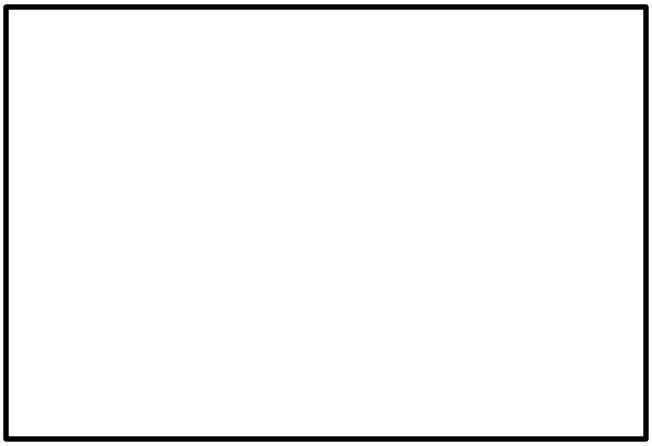
25. View of SGT [redacted]' IPhone
26. Back view of IPhone
27. Front view of IPhone
28. Hard drive remove from SGT [redacted]' office computer
29. Serial number from hard drive remove from SGT [redacted]' office computer
30.

31

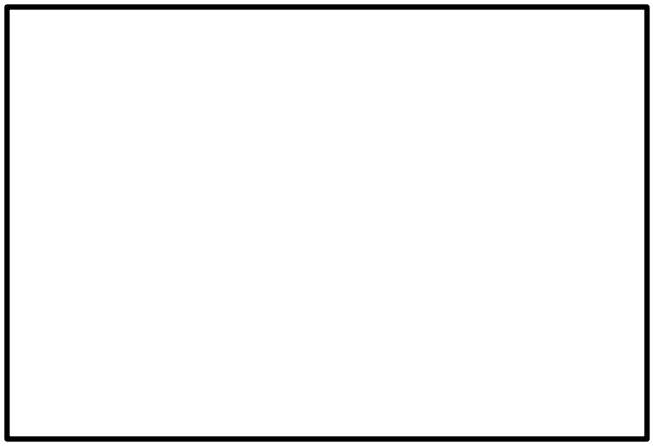
34



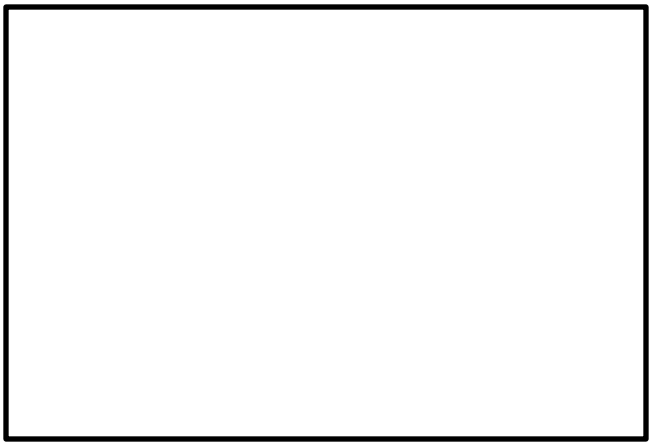
32



35



33

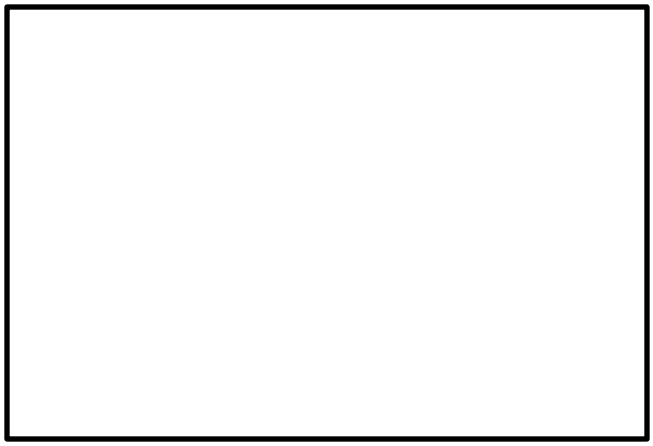


36

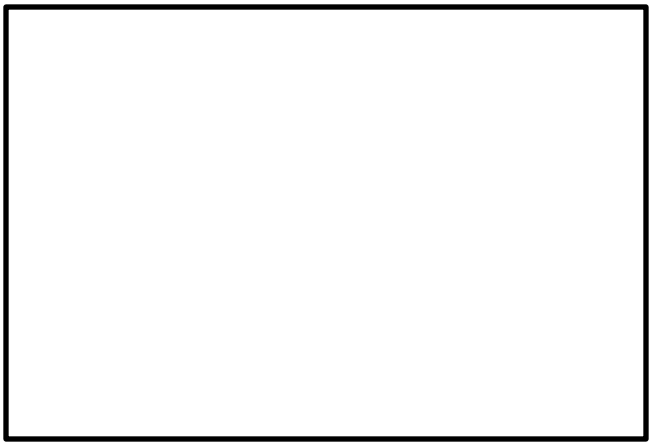
31.
32.
33.
34.
35.
36.

37

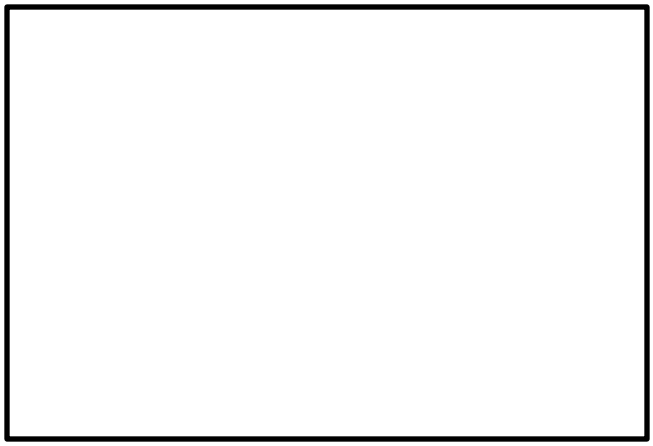
40



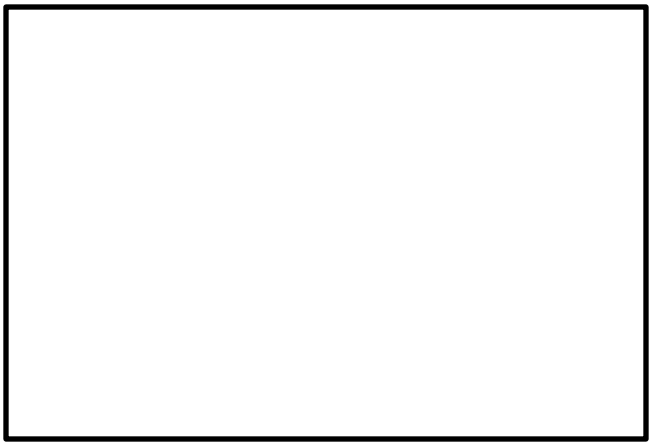
38



41



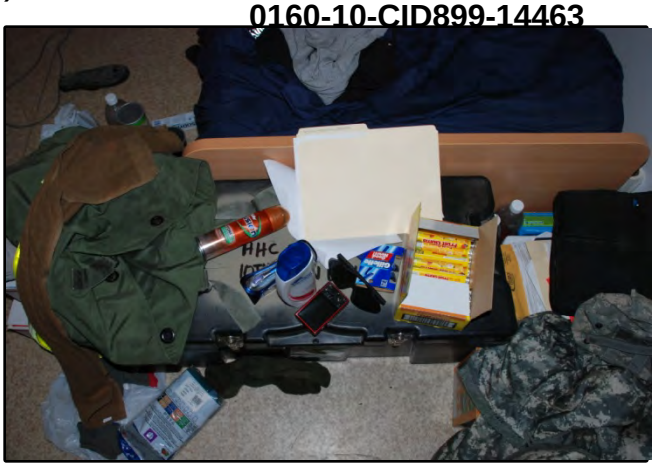
39



42

37.
38.
39
40.
41.
42.

1



4

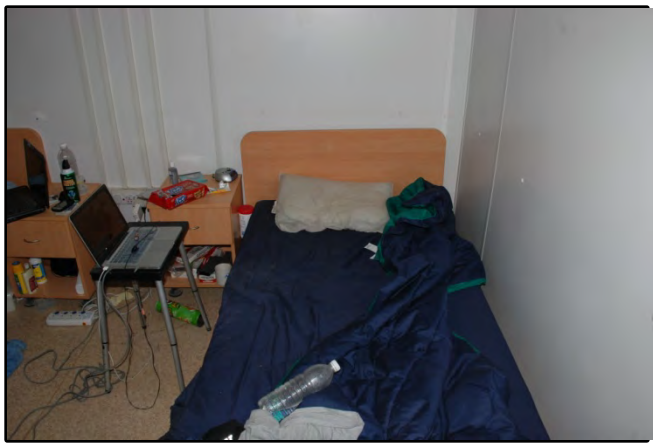
2

5

3

6

1. Entrance to room PFC MANNING's room 4C93-C, FOB Hammer, Iraq.
2. Right side of the room assigned to PFC MANNING.
3. Right side of the room assigned to PFC MANNING.
4. Close view of items at bottom of bed.
5. Right wall locker assigned to PFC MANNING.
6. View of top of wall locker.

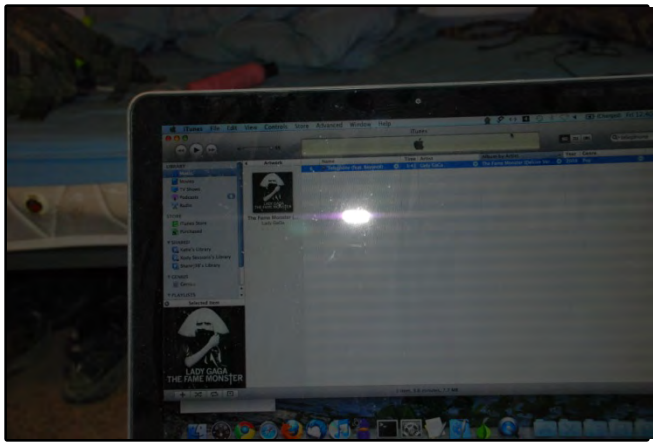


7

10

8

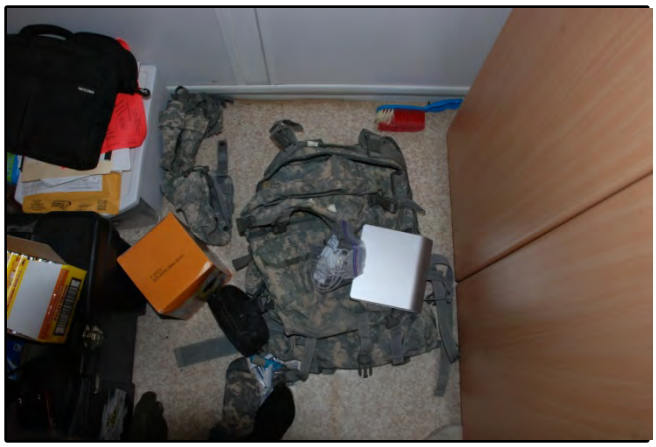
11



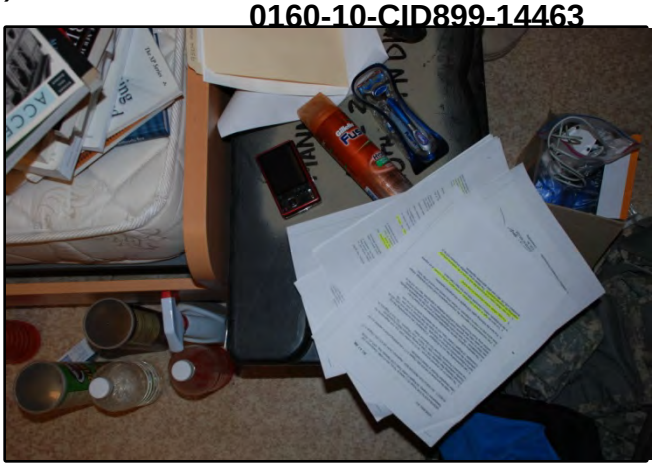
9

12

7. View of PFC MANNING's bed, also depicting location of laptop computer.
8. View of PFC MANNING's laptop computer from above.
9. View depicting what was on the computer at time of search.
10. View of PFC MANNING's nightstand and stack of CDs.
11. Inner view of top drawer of night stand.
12. Close-up view of contents of top drawer depicting an cellular phone.



13



16

14

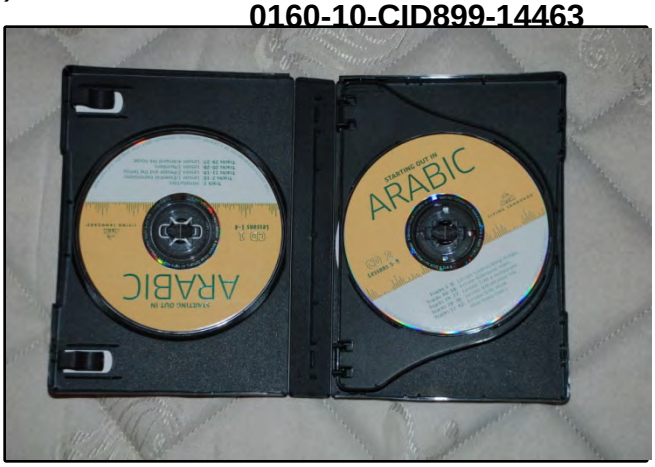
17

15

18

13. View depicting the bag the external hard drive was discovered in.
14. Close-up view of portable hard drive.
15. View of the external hard drive serial number.
16. View of bottom of tuff box depicting location of digital camera.
17. Close-up view of back side of camera.
18. Close-up view of front side of camera.

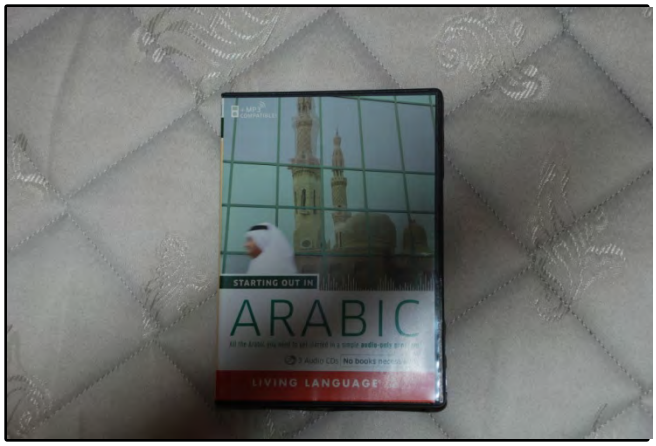
19



22

20

23



21

24

19. View of Priority Mail box (Top).
20. View of Priority Mail box (Side).
21. View of CD case found within Priority Mail Box.
22. First two CD sleeves within the CD case.
23. Second two CD sleeves within the CD case.
24. Close-up view of last CD found within the case.

25

28

26

29

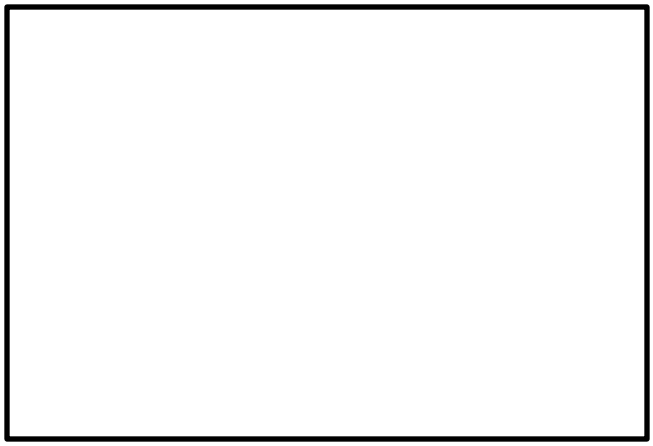
27

30

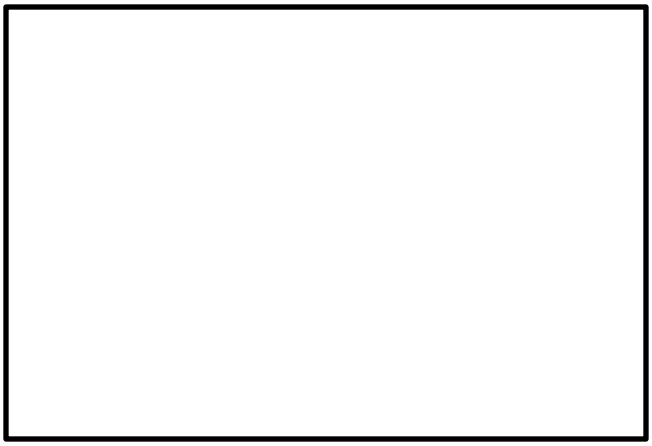
25. View of SGT [redacted]' IPhone
26. Back view of IPhone
27. Front view of IPhone
28. Hard drive remove from SGT [redacted]' office computer
29. Serial number from hard drive remove from SGT [redacted]' office computer
30.

31

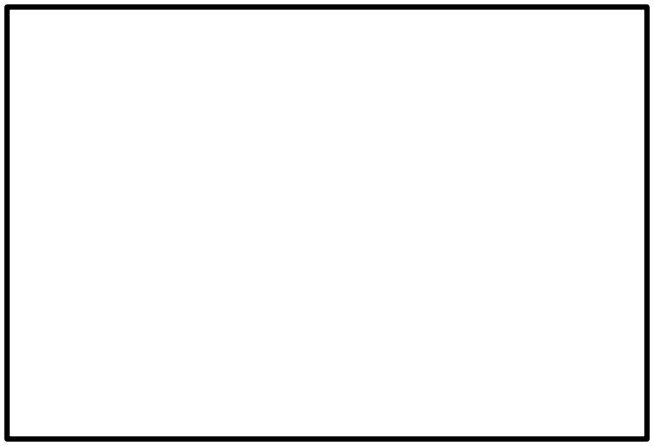
34



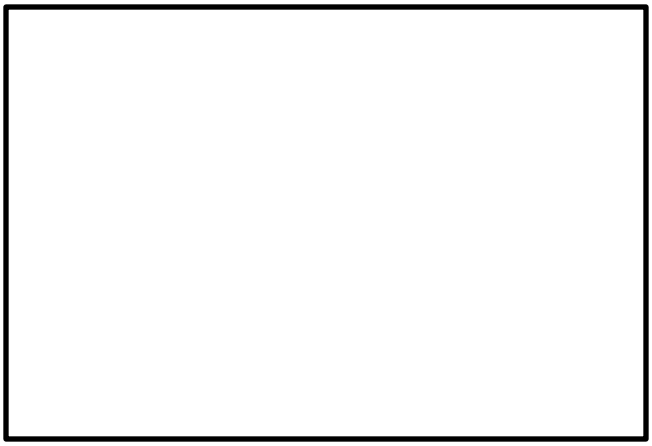
32



35



33

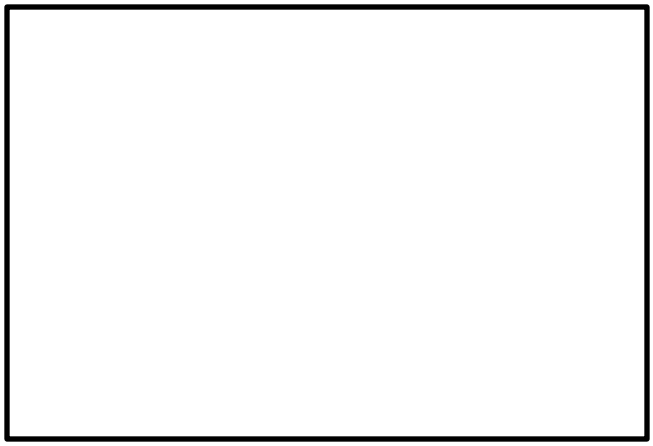


36

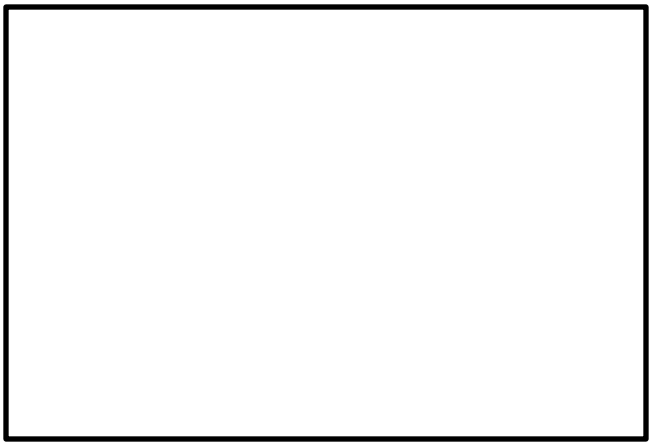
31.
32.
33.
34.
35.
36.

37

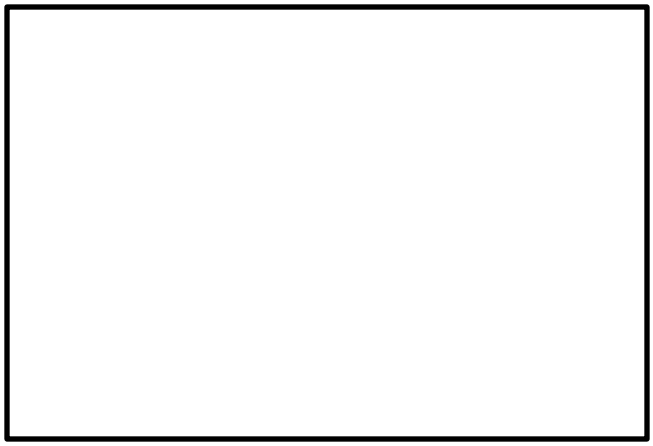
40



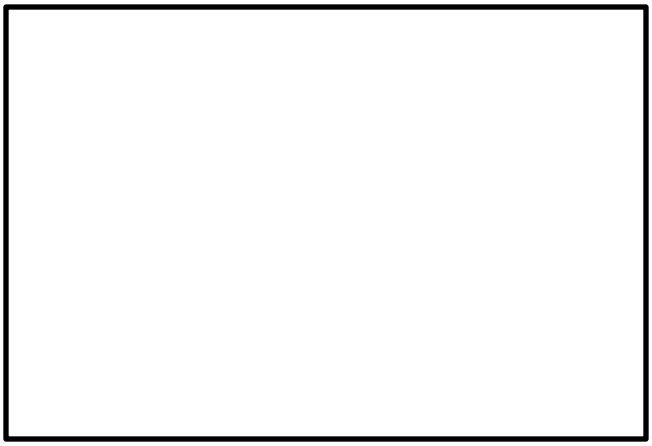
38



41



39



42

37.
38.
39
40.
41.
42.

4C93
B. 10


4C93
B-10
C
YORK
000147

MOUNTAIN
2BCT HHC
B10
SPC
(b)(6)(b)(7)(C)
SPC MANNING
CLIMB TO GLORY

MOUNTAIN
2BCT HHC
B10
SPC (b)(6)(b)(7)(C)
SPC MANNING
CLIMB TO GLORY


4C93
000150

000151

000152

000153


000154

000155

000156

000157

000160

000161

000162

000163

000164


000165

HHC

Gillette
Fruit Gums

Gillette
Fruit Gums

000169

000170

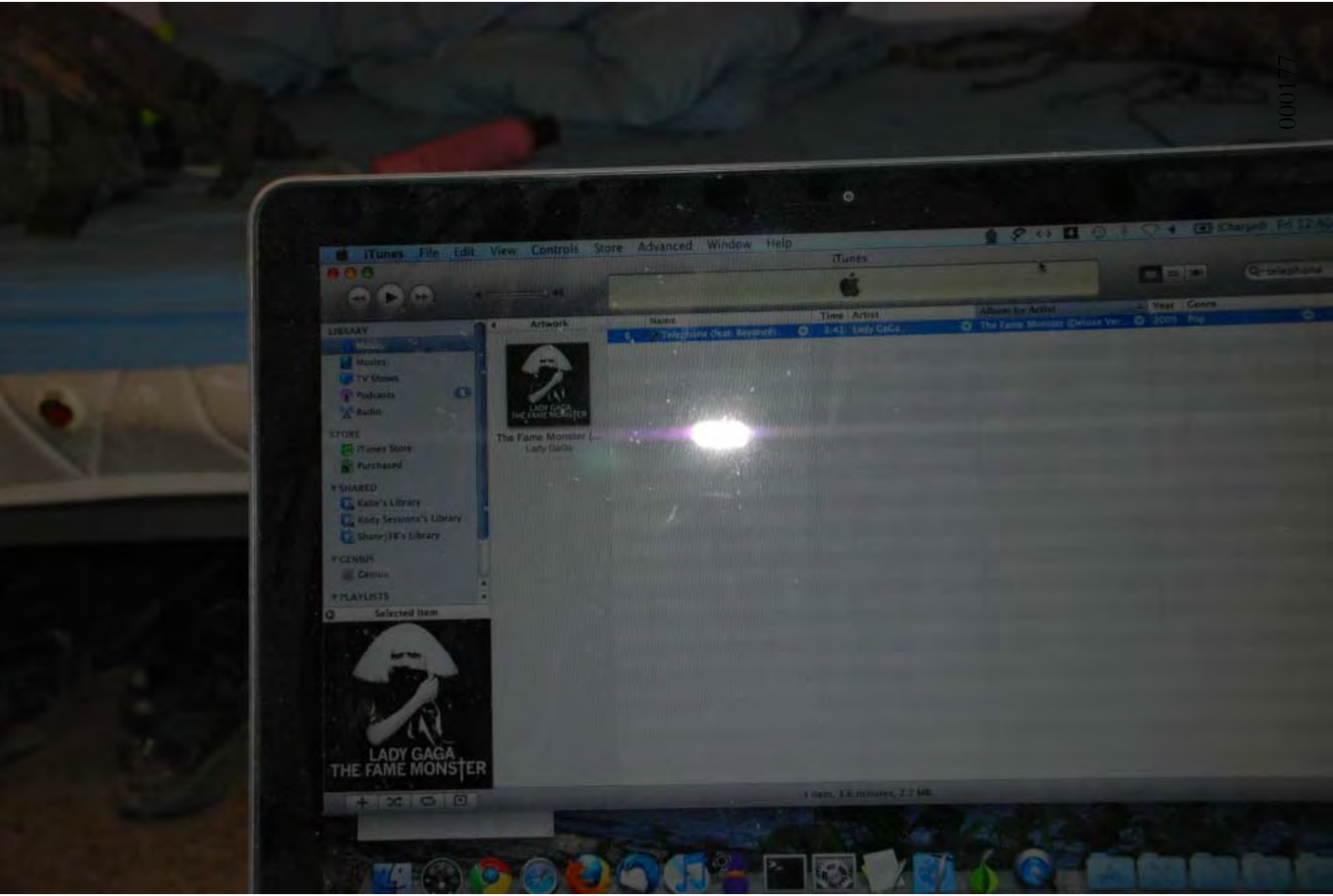
000171


Chips Ahoy!


000173

000174


MacBook Pro
000176


iTunes File Edit View Controls Store Advanced Window Help
iTunes
LIBRARY
Movies
TV Shows
Podcasts
Radio
STORE
iTunes Store
Purchased
SHARED
GENIUS
PLAYLISTS
Selected Item
Artwork
Name
Time
Artist
Telephone (feat. Beyoncé)
3:41
Lady GaGa
The Fame Monster (Deluxe Ver...
2009
Pop
The Fame Monster (...
Lady GaGa
LADY GAGA
THE FAME MONSTER

000178


CD-RW
memorex
Chips Ahoy!
Same Amount of
Less Packa

000180

000181

000182


Wet Ones
CD-RW

OPEN
Drug Facts
A Unilever BRAND
0 79400 38492 8
WRIGLEY'S
SUGARFREE GUM

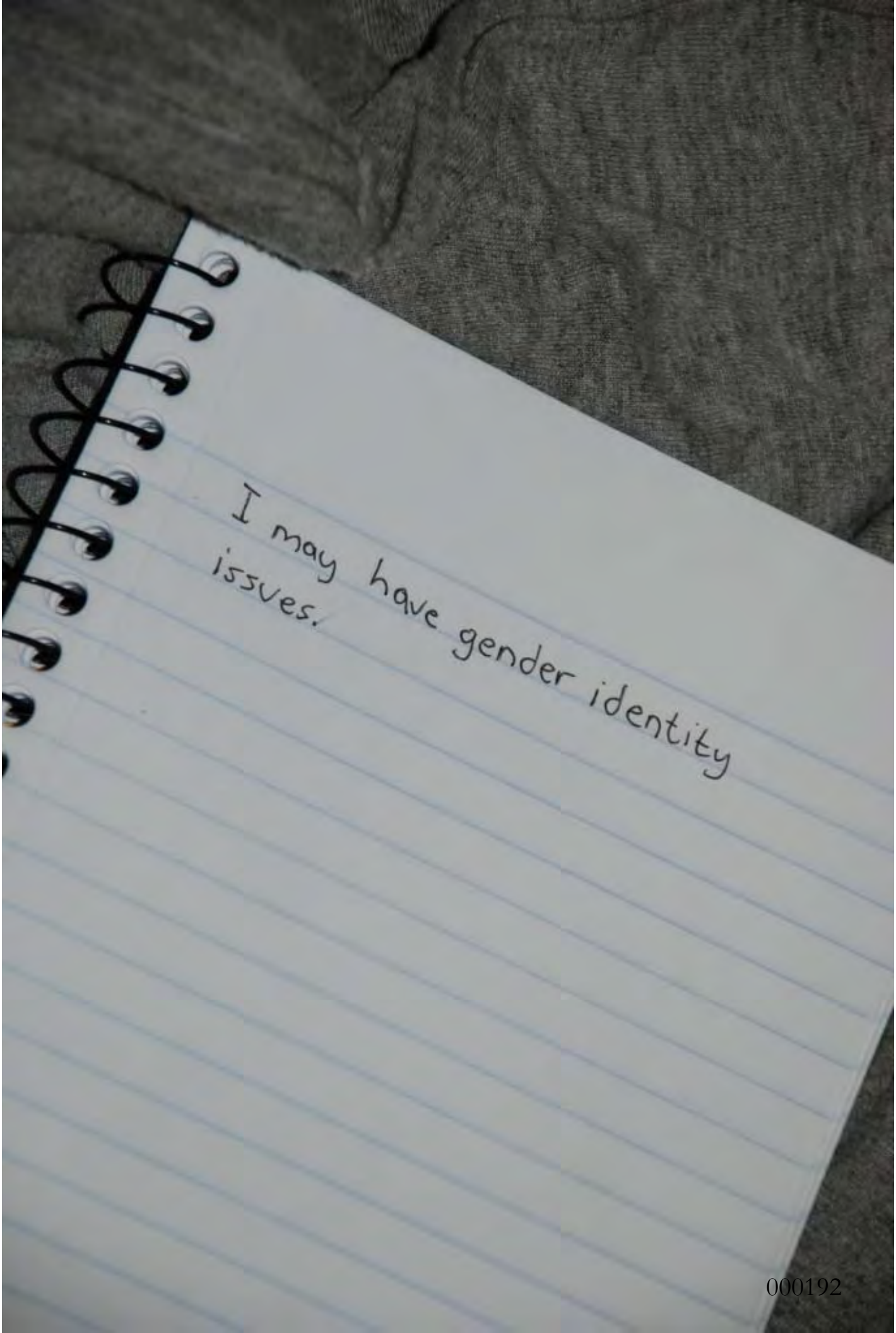
000185

000186

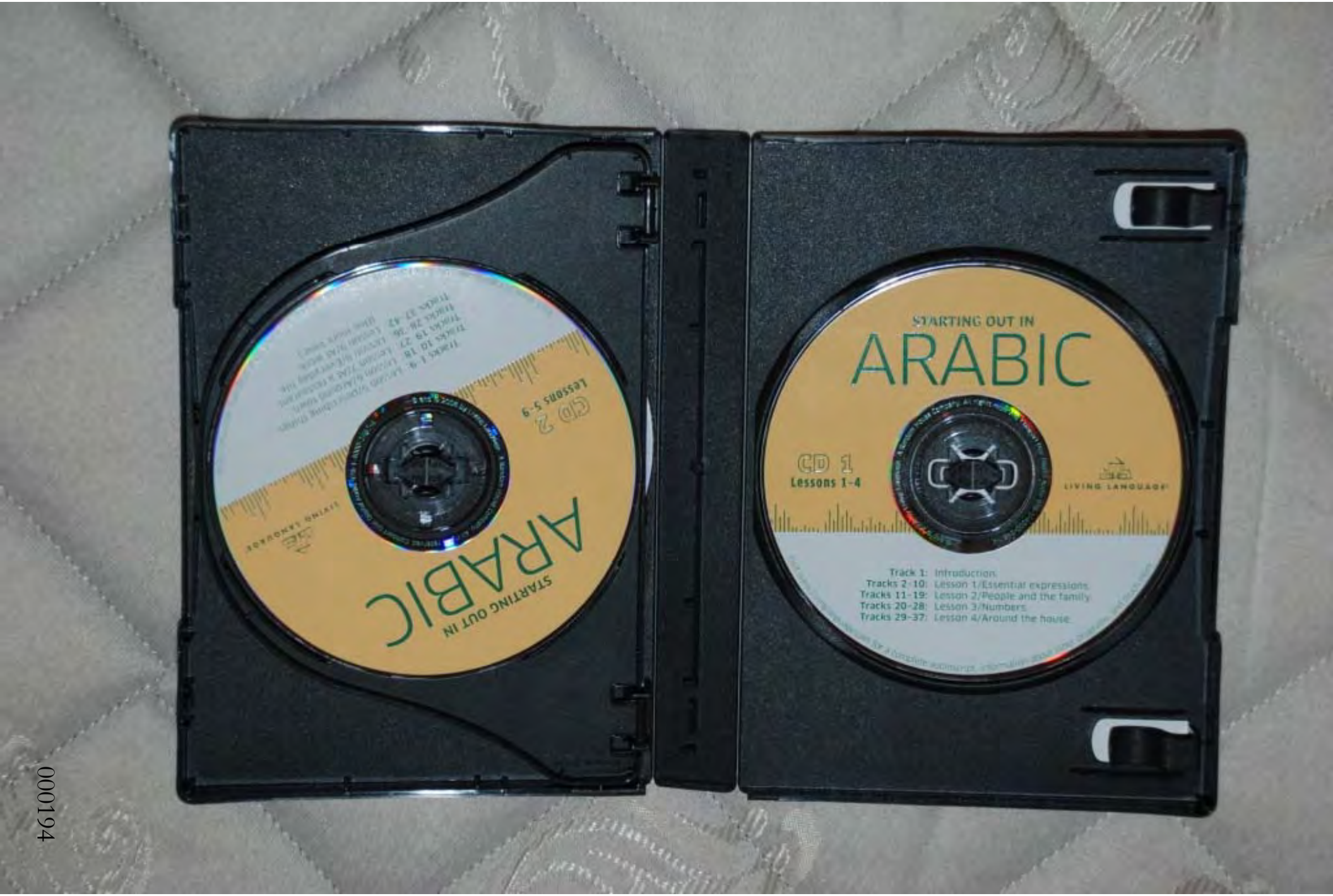

Seagate
FreeAgent™Desk
1500GB P/N:9ZC2A8-501
S/N:2GEWJKLJ
Product of Thailand (HDD) Assembled in China
Other items marked thereon
NOM
CE FC


memorex
DVD+RW
memorex
DVD+RW
000189

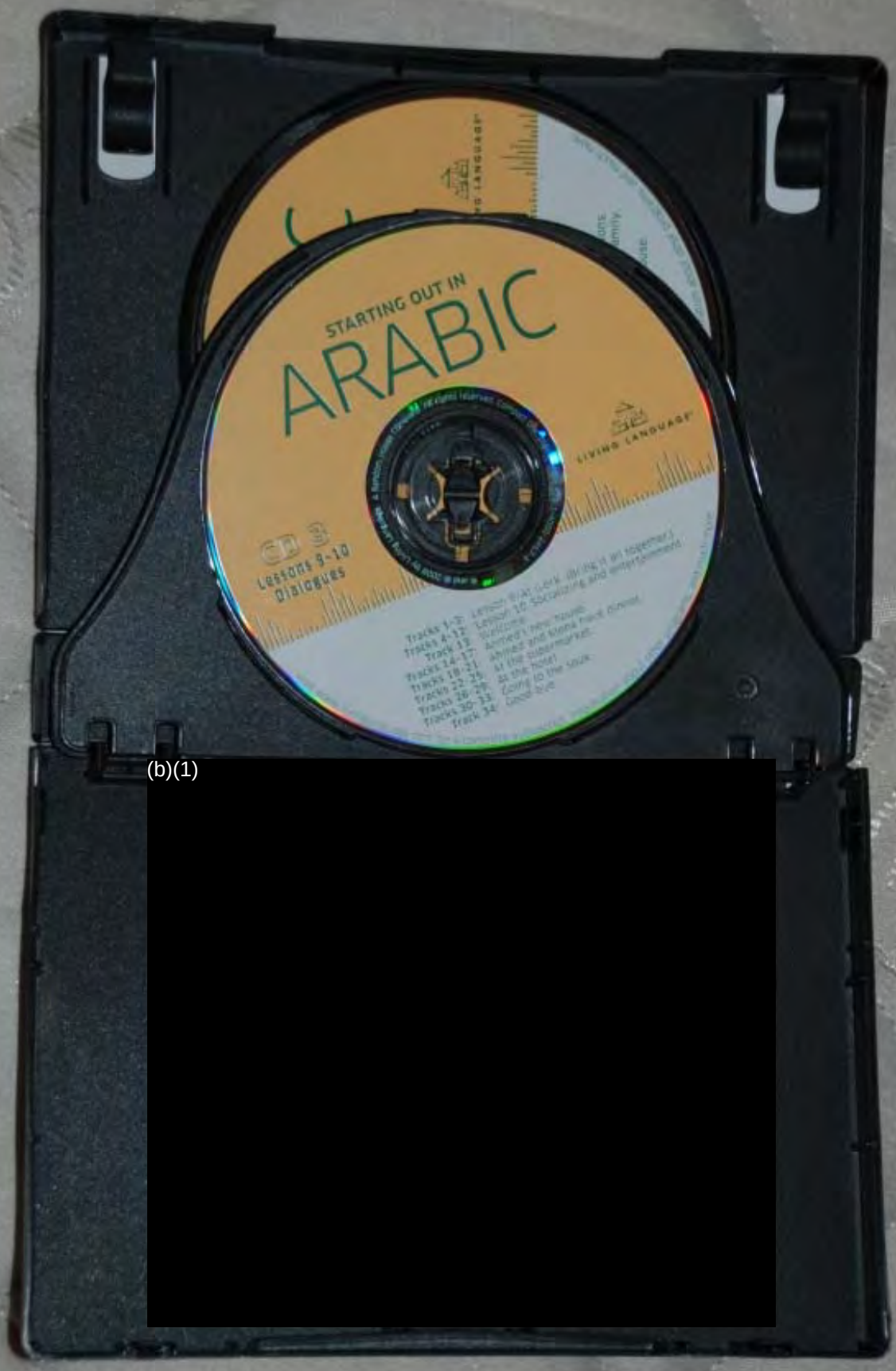

5PK
memorex
10PK
DVD+RW
4X
4.7GB
120min
memorex
10PK
DVD+RW
4X
4.7GB
120min

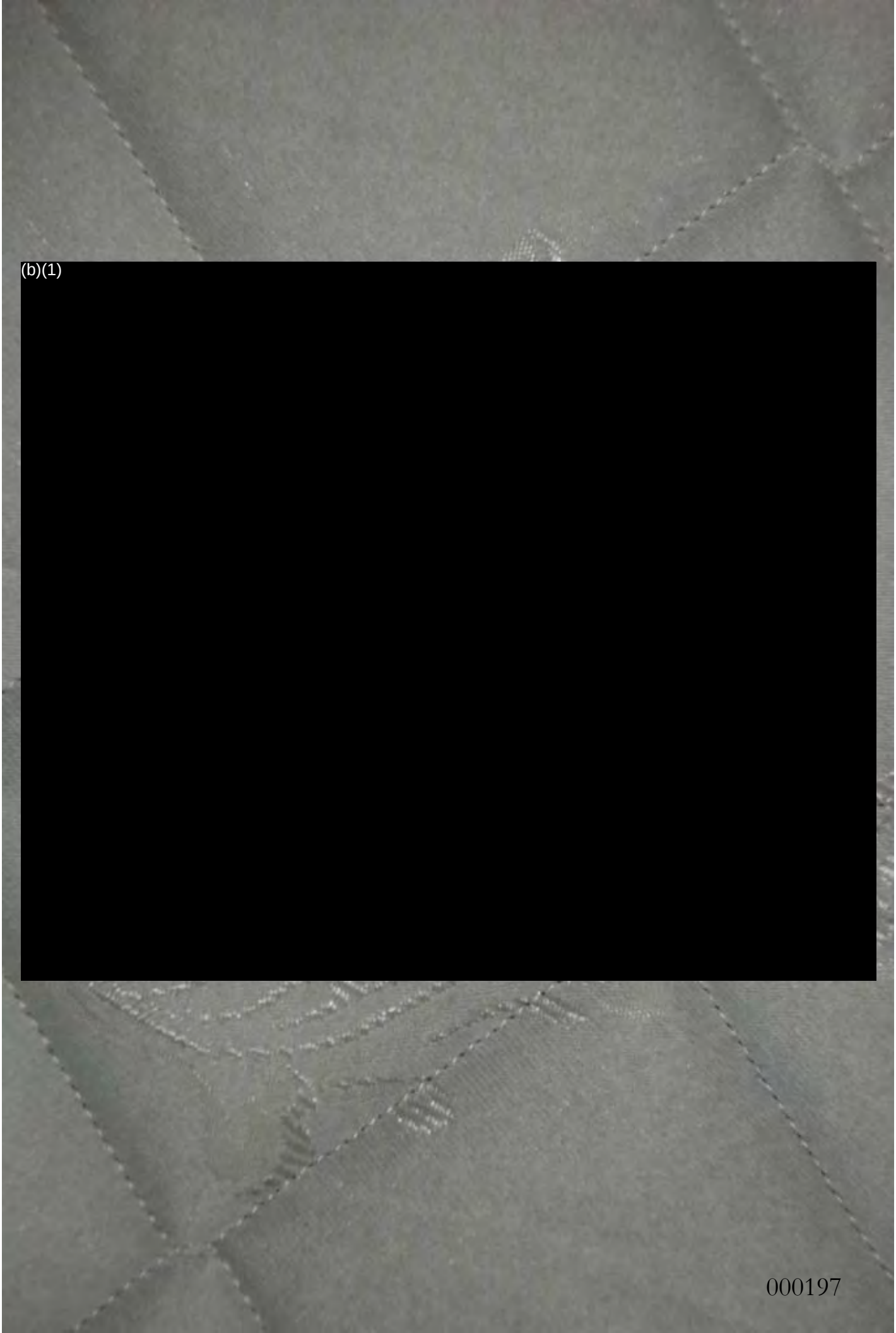

I may have gender identity
issues.

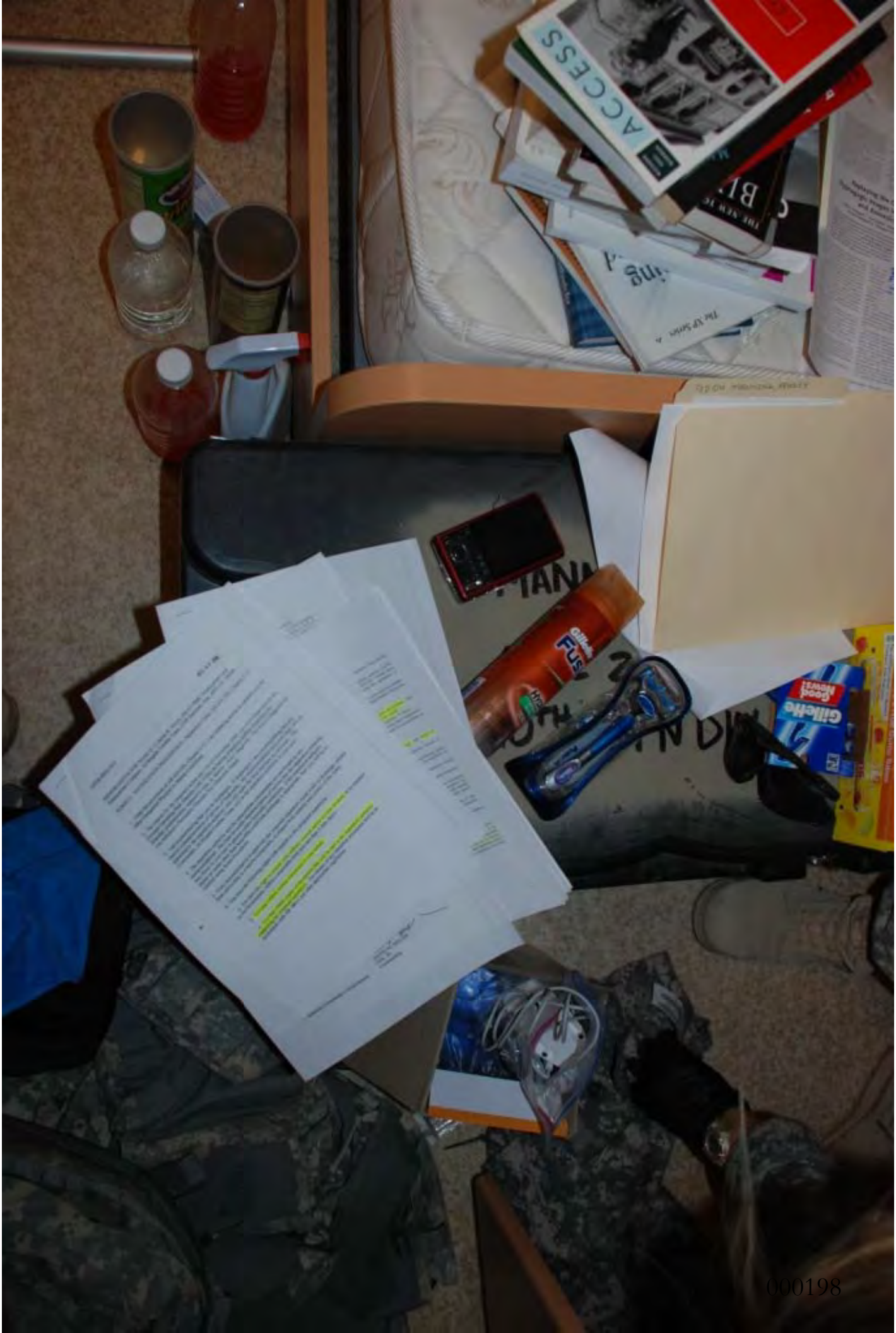
000193

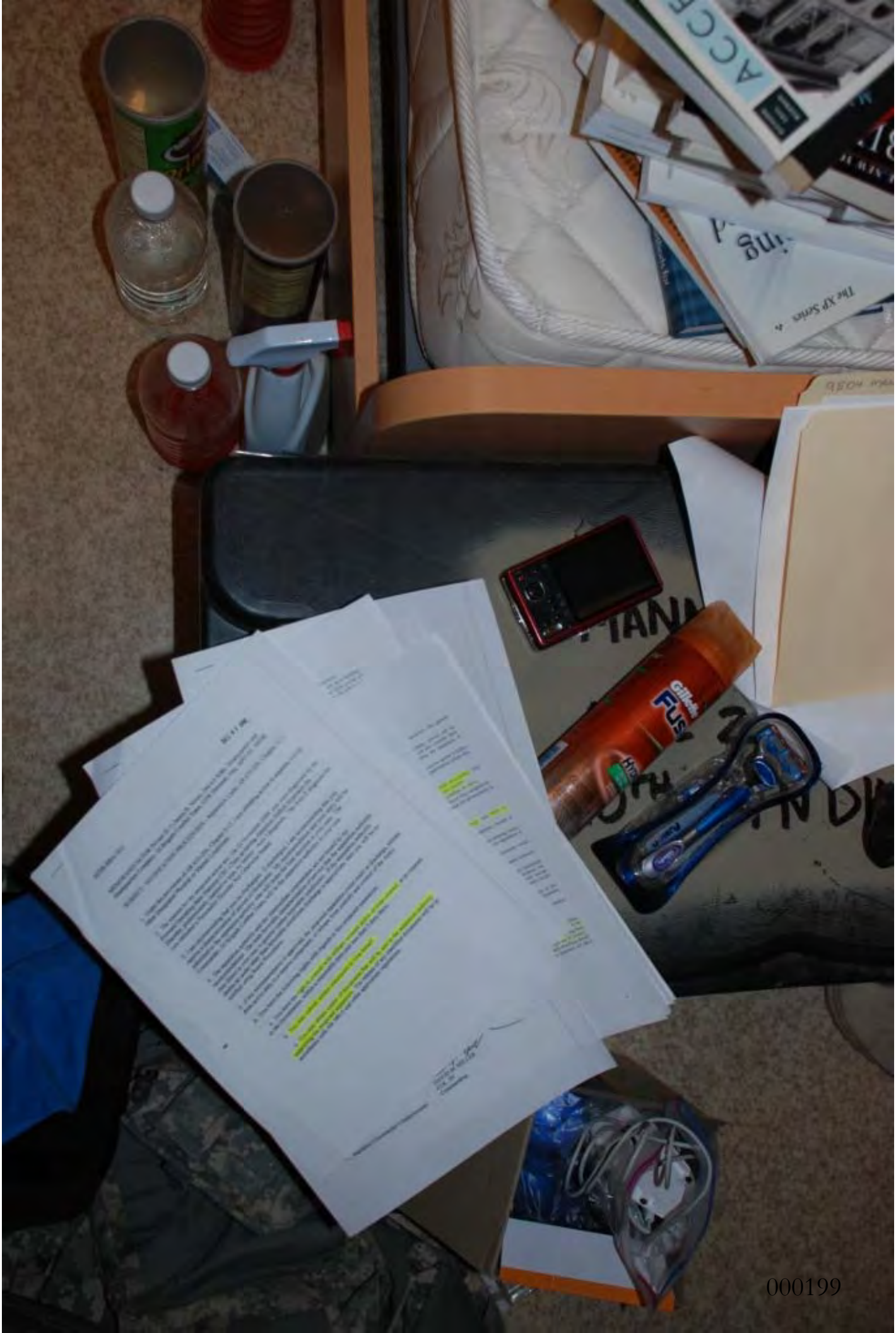

STARTING OUT IN
ARABIC
CD 1
Lessons 1-4
LIVING LANGUAGE
Track 1: Introduction.
Tracks 2-10: Lesson 1/Essential expressions.
Tracks 11-19: Lesson 2/People and the family.
Tracks 20-28: Lesson 3/Numbers.
Tracks 29-37: Lesson 4/Around the house.
CD 2
Lessons 5-9
ARABIC
STARTING OUT IN

000195


STARTING OUT IN
ARABIC
LIVING LANGUAGE
Lessons 9-10
Dialogues
(b)(1)


(b)(1)
000197


ACCESS
Gillette
Good Morning


ACCE
The XP Series
Gillette
Fusion

therefore, this general
ulitary service will be
will also consider these
sding the separation, if
action against a soldier
habilitation efforts does
ation proceedings. Also
and morale
continuic or recur.
future duty assignments
ential for advancement or
ings, and letters of
ishment, records of
cial training, duties,
on separations or
formation would
Gillette
Fusion
HYDR
Fusion


000201

000202


PRIORITY®
MAIL
UNITED STATES POSTAL SERVICE
By air mail
Par avion
Priority
Prioritaire
INTERNATIONAL
EXPRESS
PRIORITY
TM
PRIORITY MAIL
POSTAGE REQUIRED
000203


PRIORITY
MAIL
UNITED STATES POSTAL SERVICE
By air mail
Par avion
Priority
Prioritaire
INTERNATIONAL
EXPRESS
PRIORITY
TM
000204


P
10

7557686
3/1/10

.005
.010
.015

.005
.010
.015


PRIORITY®
MAIL
UNITED STATES POSTAL SERVICE
Large Flat Rate Box
For Domestic and International Use
Large Flat Rate Box
usps.com

000207

PRIORITY
MAIL
UNITED STATES POSTAL SERVICE
Flat Rate Box
Visit us at usps.com

Large Flat Rate Box
For Domestic and International Use
PRIORITY MAIL
Visit us at usps.com
INTERNATIONAL RESTRICTIONS APPLY:
20-POUND WEIGHT LIMIT
ON INTERNATIONAL APPLIES
Customs forms are required.
Consult the International Mail Manual (IMM)
at pe.usps.gov or ask a retail associate
for details.
From: Expéditeur:
UNITED STATES POSTAL SERVICE
Visit us at usps.com
Label 10EA, May 2008
PRIORITY MAIL

PRIORITY®
MAIL

UNITED STATES POSTAL SERVICE

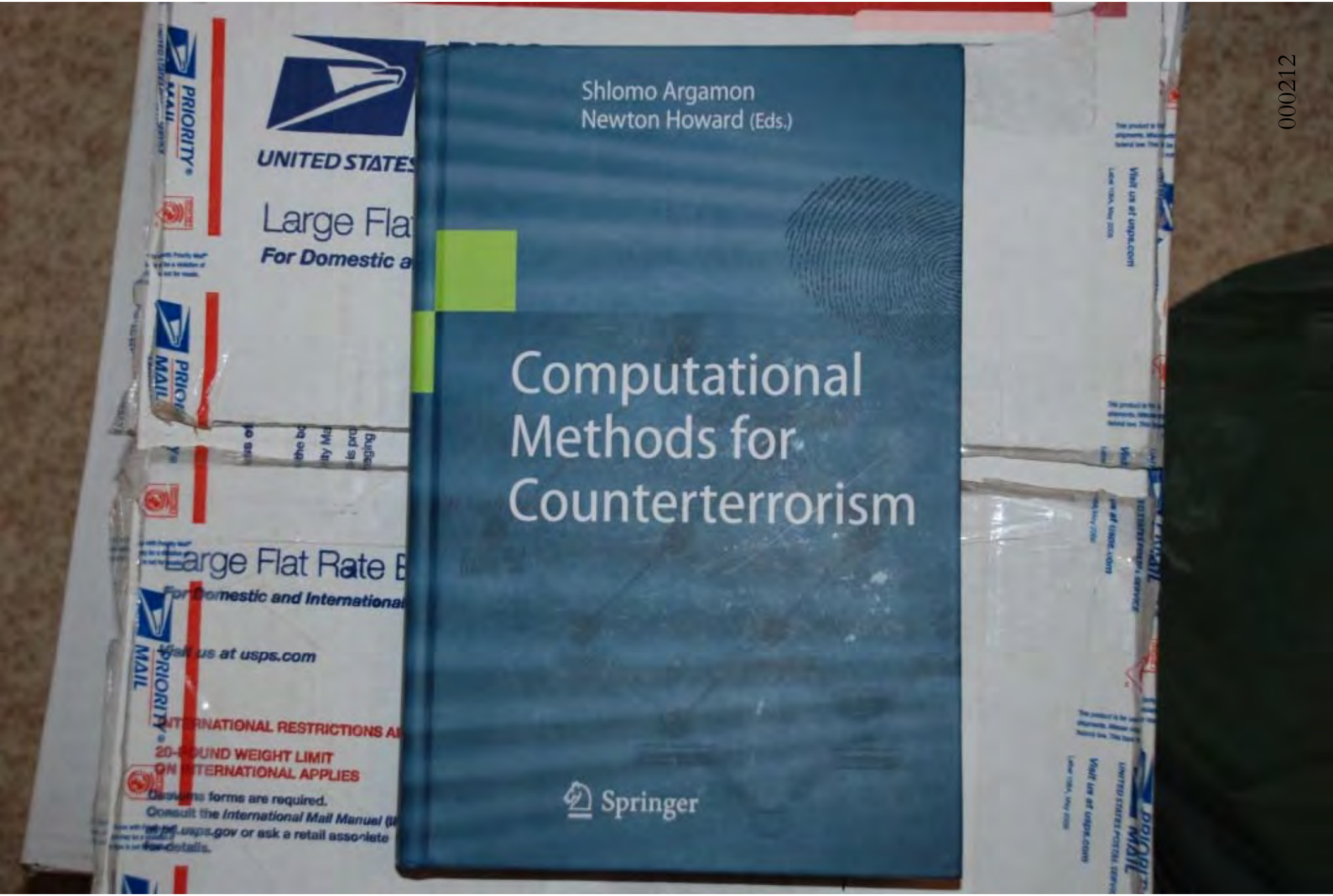
Large Flat Rate Box

For Domestic and International Use

Visit us at usps.com

000210

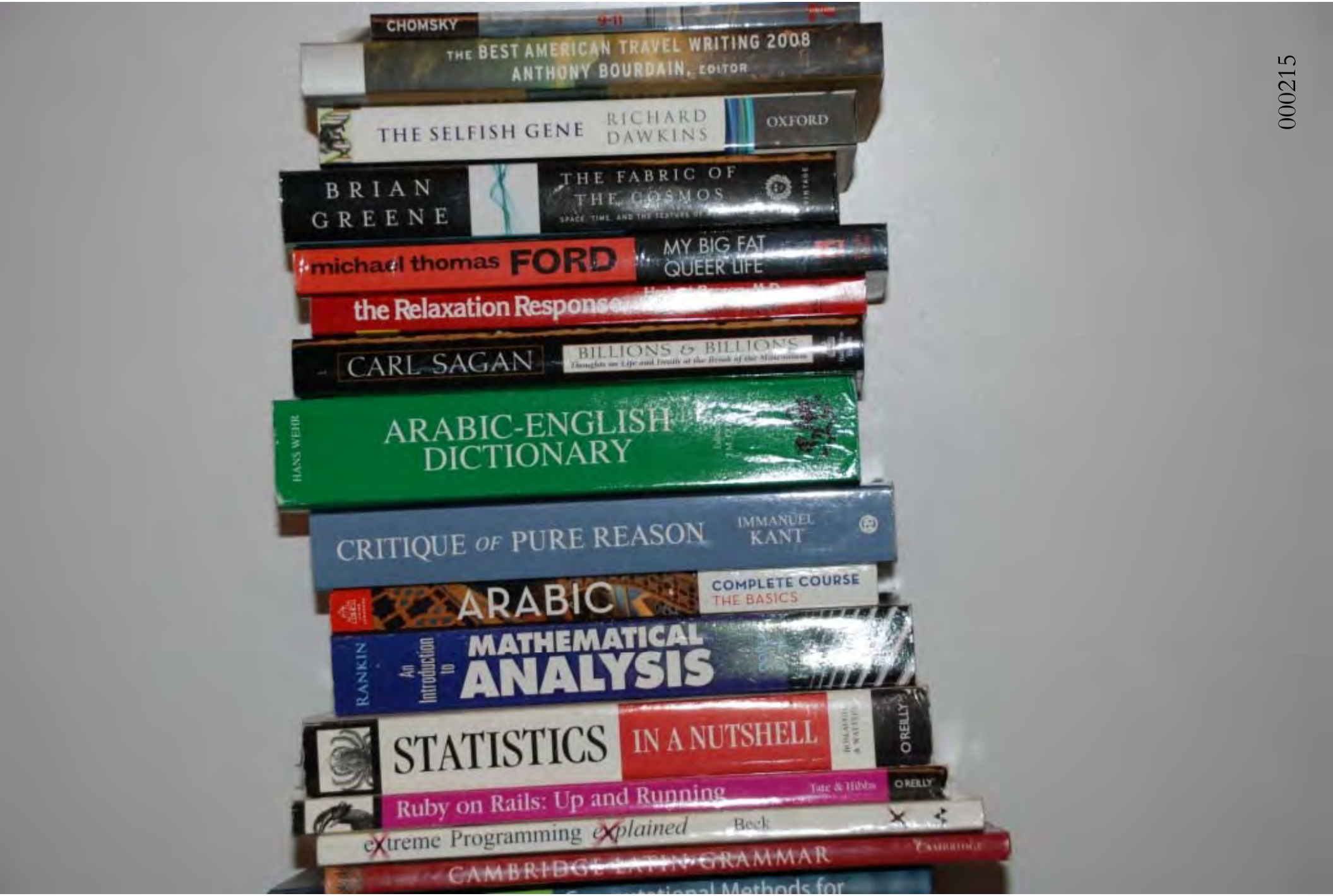
000211


Shlomo Argamon
Newton Howard (Eds.)
Computational Methods for Counterterrorism
Springer
UNITED STATES
Large Flat
For Domestic a
Large Flat Rate B
Visit us at usps.com
PRIORITY MAIL
INTERNATIONAL RESTRICTIONS A
20-POUND WEIGHT LIMIT
ON INTERNATIONAL APPLIES
forms are required.
Consult the International Mail Manual
or ask a retail associate
for details.
000212

The Complete Reference
C
Fourth Edition
Schildt
SOUND
WHEELOCK'S LATIN
RICHARD DAWKINS
THE GREATEST SHOW ON EARTH
UNFRIENDLY FIRE
ONLY A THEORY
Ruby on Rails: Up and Running
CAMBRIDGE LATIN COURSE
STATISTICS
IN A NUTSHELL
ARABIC
MATHEMATICAL ANALYSIS
CRITIQUE OF PURE REASON
ARABIC-ENGLISH DICTIONARY
CARL SAGAN
michael thomas FORD
the Relaxation Response
MY BIG FAT QUEER LIFE
BRIAN GREENE
THE FABRIC OF THE COSMOS
THE SELFISH GENE

Covers C99, the New ANSI/ISO Standard for C
BONUS!
The Complete Reference
C
Fourth Edition
Schildt
OSBORNE
212124-6
Rossing
Moore
Wheeler
THE SCIENCE OF SOUND
THIRD EDITION
Addison Wesley
WHEELOCK'S LATIN
6TH EDITION, REVISED
Frederic M. Wheelock
Revised by Richard A. LaFleur
Collins
RICHARD DAWKINS
THE GREATEST SHOW ON EARTH
fP
UNFRIENDLY FIRE
HOW THE GAY BAN UNDERMINES THE MILITARY AND WEAKENS AMERICA
NATHANIEL FRANK
ONLY A THEORY
KENNETH R. MILLER
VIKING
Argamon
Howard (Eds.)
Computational Methods for Counterterrorism
CAMBRIDGE LATIN GRAMMAR
eXtreme Programming eXplained
Beck
Ruby on Rails: Up and Running
O'REILLY
STATISTICS IN A NUTSHELL
O'REIL

000214


CHOMSKY
9-11
THE BEST AMERICAN TRAVEL WRITING 2008
ANTHONY BOURDAIN, EDITOR
THE SELFISH GENE
RICHARD DAWKINS
OXFORD
BRIAN GREENE
THE FABRIC OF THE COSMOS
michael thomas FORD
MY BIG FAT QUEER LIFE
the Relaxation Respons
CARL SAGAN
BILLIONS & BILLIONS
ARABIC-ENGLISH DICTIONARY
HANS WEHR
CRITIQUE OF PURE REASON
IMMANUEL KANT
ARABIC
COMPLETE COURSE
THE BASICS
RANKIN
An Introduction to
MATHEMATICAL ANALYSIS
STATISTICS
IN A NUTSHELL
O'RELLY
Ruby on Rails: Up and Running
Tate & Hibbs
O'REILLY
eXtreme Programming eXplained
Beck
CAMBRIDGE LATIN GRAMMAR

000215

Bradley Edward MANNING

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

DOB: (b)(6)(b)(7)(C)

35F intelligence Analyst

HHC, 2nd Brigade Combat team, 10th Mountain Division

000217

000218

000219


14B
SCIF
ATTENTION
2145 Meeting Nightly
ATTENTION
WARNING: SECURE FACILITY
• USE OF DEADLY FORCE HAS BEEN AUTHORIZED
• THIS SECURE FACILITY IS PATROLLED BY ARMED GUARDS
• USE OF FORCE OR SUBVERSION TO ENTER THIS FACILITY WILL RESULT IN THE ALERT OF DEFENSE FORCES AND YOUR DETENTION BY SECURITY PERSONNEL
• PLEASE KNOCK AND WAIT FOR AN ESCORT
• YOU MUST HAVE AN APPROVED AND VALID USF-I APPROVED BADGE AND PROPER SECURITY CLEARANCE TO ENTER
STOP
STOP


14B
ATTENTION
2145 Meeting Nightly
ATTENTION
WARNING: SECURE FACILITY
• USE OF DEADLY FORCE HAS BEEN AUTHORIZED
• THIS SECURE FACILITY IS PATROLLED BY ARMED GUARDS
• USE OF FORCE OR SUBVERSION TO ENTER THIS FACILITY WILL RESULT IN THE ALERT OF DEFENSE FORCES AND YOUR DETENTION BY SECURITY PERSONNEL
• PLEASE KNOCK AND WAIT FOR AN ESCORT
• YOU MUST HAVE AN APPROVED AND VALID USF-I APPROVED BADGE AND PROPER SECURITY CLEARANCE TO ENTER
STOP
STOP

000222

000223

000224

000225

000226

000227

000228

CD-R

000230

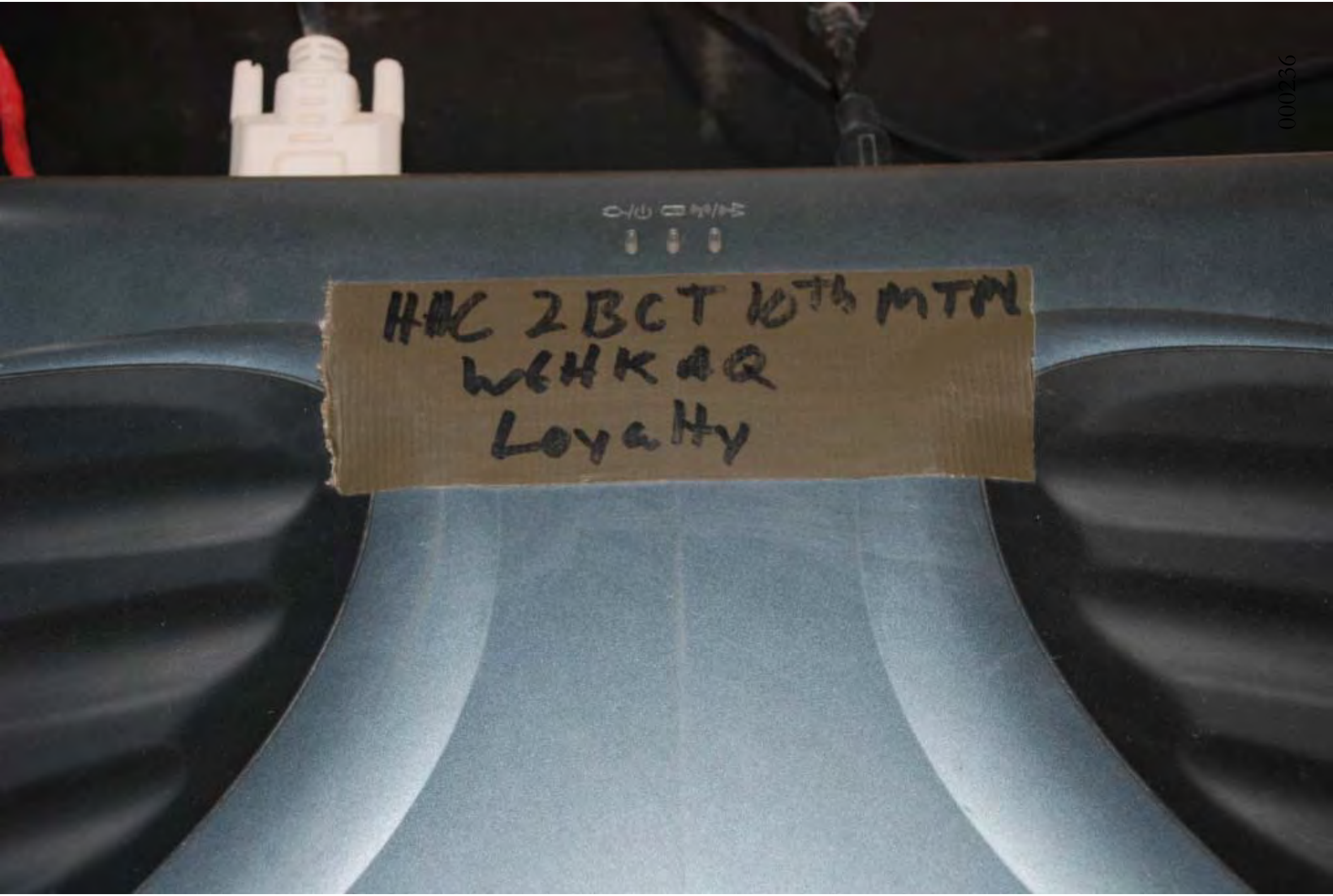
000231

000232

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

(b)(6)(b)(7)(C)
ALIENWARE
D354-2119

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


HHC 2BCT 10TH MTN
WEHKAQ
LOYALTY

000237

CAUTION
87-D9TA5-4D6A
NOTEBOOK COMPUTER


PRODUCT CODE/ 產品代碼 : D900T
FC
Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE
R31132
VCI
Support
CLEVO
藍天電
Apparatus Claims of U.S. Patent Nos. 4,631,603, 4,577,216, 4,819, 098, and4,907,093licensed for li- mited viewing uses only.
This device complies with Part 15 of the FCC Rules. Operation is subject to the foll
two conditions: (1) this device may not cause harmful interference,and (2) this
must accept any interference received, including interference that may cause und
operation.
This Class B digital apparatus meets all requirements of the Canadian Interfe
Causing Equipment Regulation.
Cet appareil mumérique de la classe B respecte toutes les exigences du Règl
Sur le matériel brouilleur du Canada.
Serial No./ 序號 :
NKD900TA6D00661
MADE IN CH
中國製

000240

SPC
Shi'a Team
(b)(6)(b)(7)(C)


(b)(6)(b)(7)(C)
SECRET
DELL

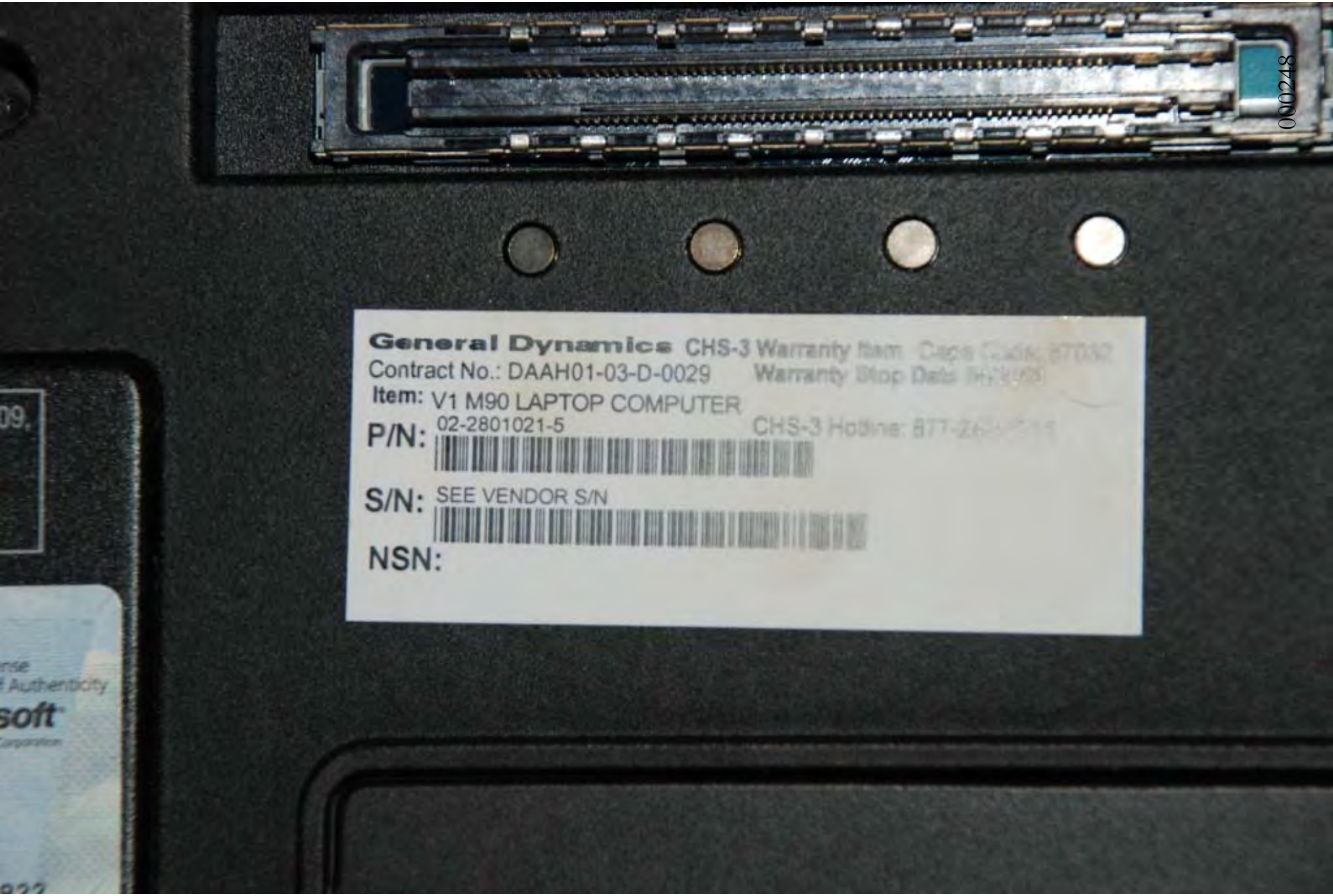
MAC: 001C232BF580


MAC: 001C232BF580
SECRET
U.S. Government Property


DELL PRECISION
MAC: 001C232BF580
000245


DELL PRECISION
MAC: 001C232B
000246

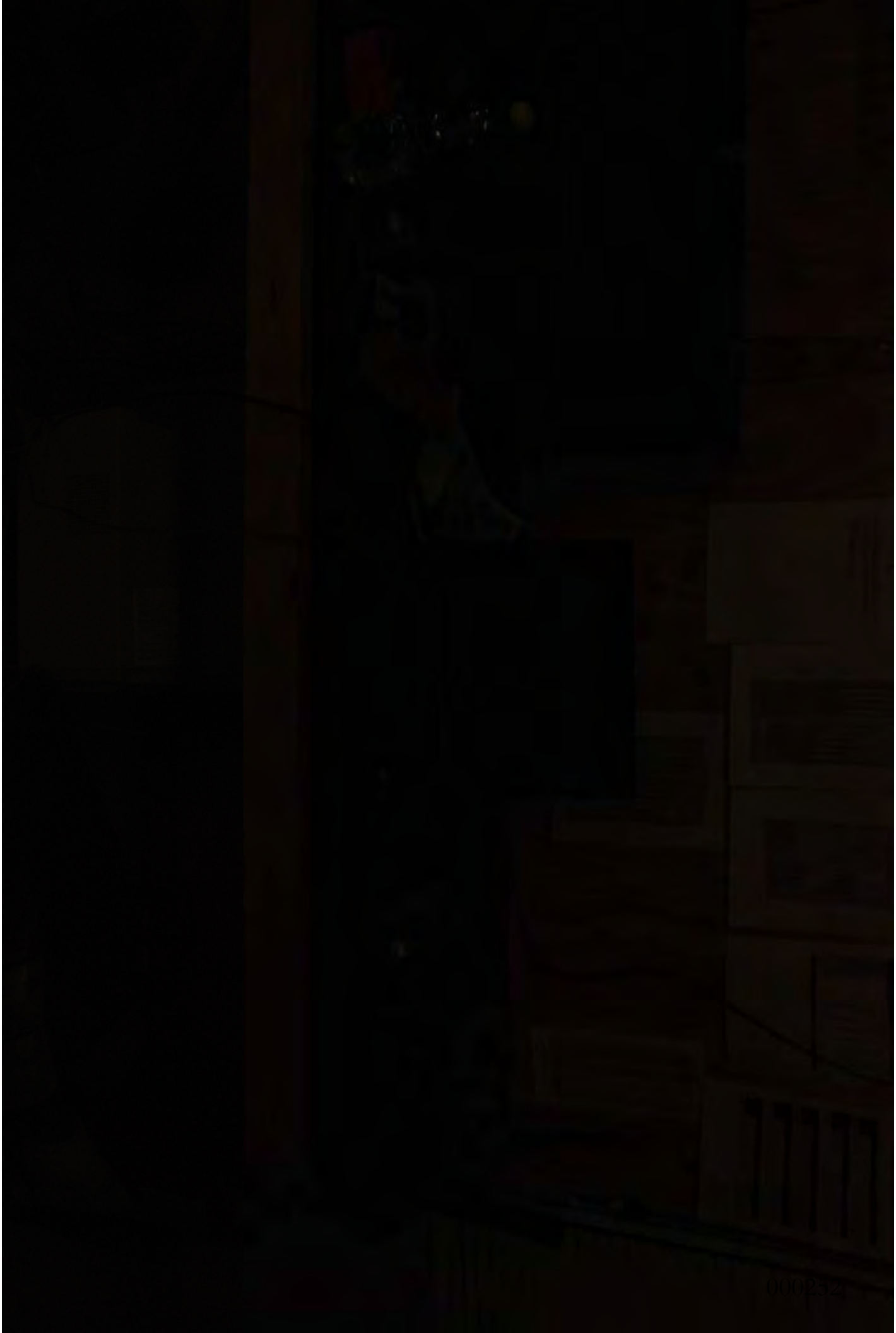

WIRELESS CARD
HAS BEEN REMOVED
AN/TYQ-93B(V) 4
NSN: 7010-01-548-0844
SN: AL90
HARDWARE SUPPORT:
General Dynamics Hotline
1-877-247-7711
CHS2-WARRANTY@GDC4S.COM


General Dynamics CHS-3 Warranty Item
Contract No.: DAAH01-03-D-0029
Item: V1 M90 LAPTOP COMPUTER
P/N: 02-2801021-5
S/N: SEE VENDOR S/N
NSN:
000218


General Dynamics CHS-3
Contract No.: DAAH01-03-D-0029
Item: V1 M90 LAPTOP COMPUTER
P/N: 02-2801021-5
S/N: SEE VENDOR S/N
NSN:

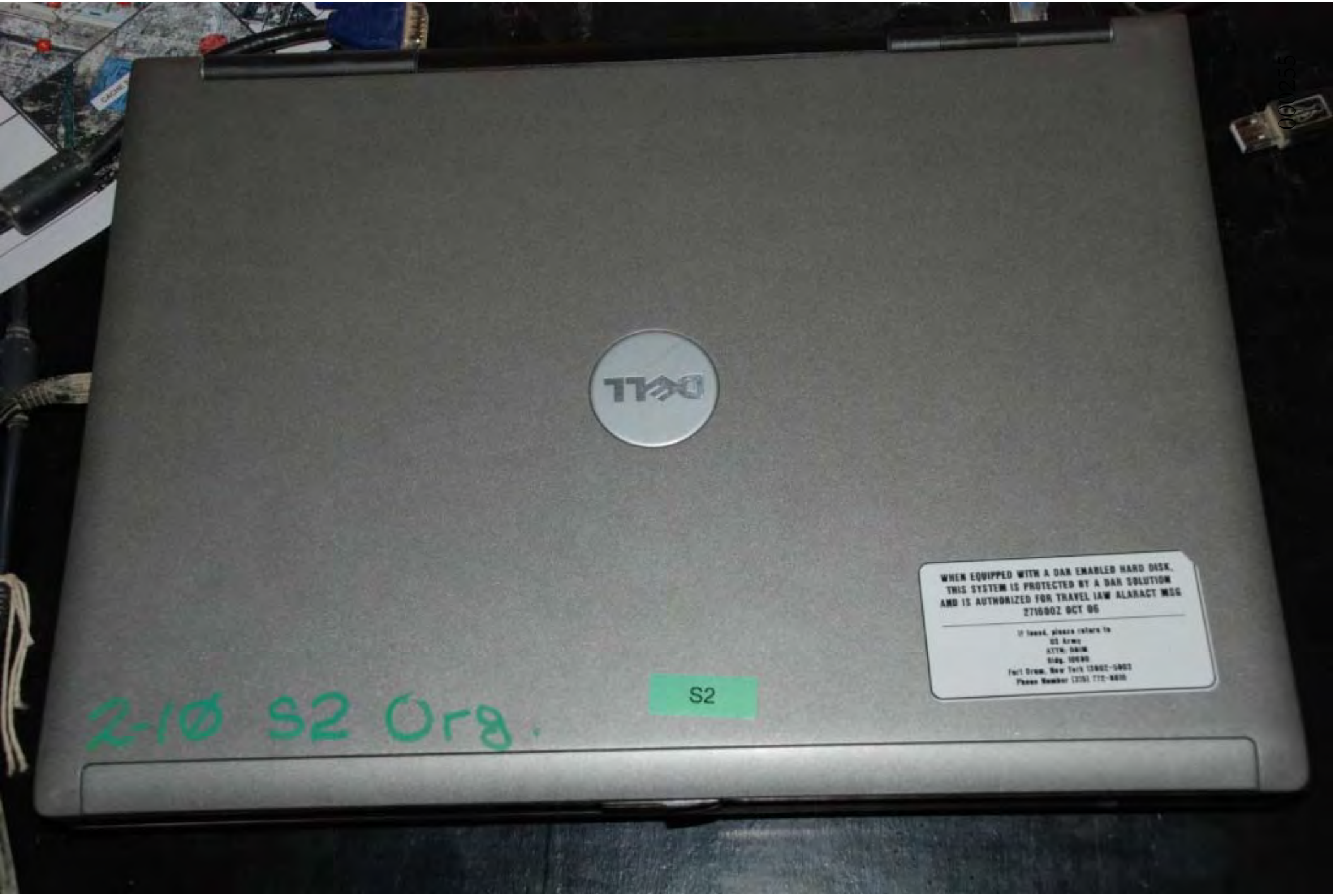
000250

000251



000253

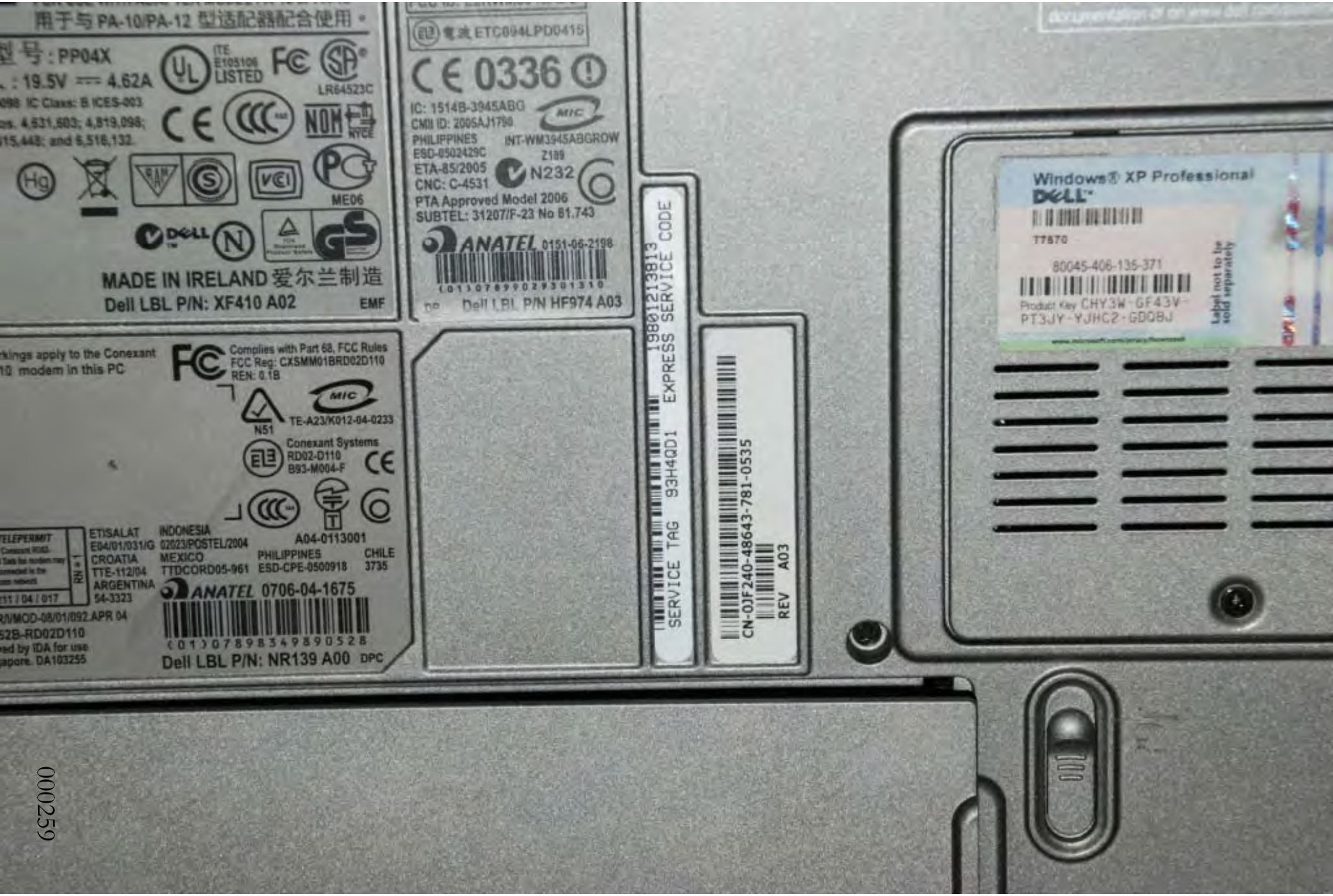
000254


WHEN EQUIPPED WITH A DAR ENABLED HARD DISK,
THIS SYSTEM IS PROTECTED BY A DAR SOLUTION
AND IS AUTHORIZED FOR TRAVEL IAW ALARACT MSG
271600Z OCT 06
S2
2-10 S2 Org.

000256


LEGEND
DELL
2-10 S2 Org.


DELL
MADE IN IRELAND


用于与 PA-10/PA-12 型适配器配合使用。
型号 : PP04X
. : 19.5V ⎓ 4.62A
LISTED
LR64523C
ME06
MADE IN IRELAND 爱尔兰制造
Dell LBL P/N: XF410 A02
EMF
ETC094LPD0415
0336
IC: 1514B-3945ABG
CMII ID: 2005AJ1799
PHILIPPINES
INT-WM3945ABGROW
ESD-0502429C
Z189
ETA-85/2005
N232
CNC: C-4531
PTA Approved Model 2006
SUBTEL: 31207/F-23 No 81.743
ANATEL 0151-06-2198
(01)07899029301310
Dell LBL P/N HF974 A03
Windows® XP Professional
DELL
T7570
80045-406-135-371
Product Key CHY3W-GF43V-
PT3JY-YJHC2-GDQBJ
Label not to be sold separately
Complies with Part 68, FCC Rules
FCC Reg: CXSMM01BRD02D110
REN: 0.1B
N51
TE-A23/K012-04-0233
Conexant Systems
RD02-D110
B93-M004-F
A04-0113001
ETISALAT
E04/01/031/G
CROATIA
TTE-112/04
ARGENTINA
54-3323
INDONESIA
02023/POSTEL/2004
MEXICO
TTDCORD05-961
PHILIPPINES
ESD-CPE-0500918
CHILE
3735
ANATEL 0706-04-1675
(01)07898349890528
Dell LBL P/N: NR139 A00
DPC
SERVICE TAG 93H4QD1 EXPRESS SERVICE CODE
19801213813
CN-0JF240-48643-781-0535
REV A03

000259

CLASSIFIED

Exhibit(s) 29

Page(s) 000260 thru 000260k referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

Exhibit(s) 30 thru 33

Page(s) 000261 thru 000268 referred to:

Commander
INSCOM
ATTN: IAMG-C-FOI
4552 Pike Road
Fort Meade, MD 20755-5995

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

AGENT's COMMENT: All times in this report are in Greenwich Mean Time (GMT) +1, with Daylight Savings Time (DST) in effect equaling GMT +2, the time zone for Mannheim, Germany. All Evidence / Property Custody Document (EPCD), Document Numbers (DN), referenced in this report were issued by the 11th Military Police (MP) Battalion (CID) consolidated evidence room located at the deployed battalion headquarters building, Camp Arifjan, Kuwait. Prior to the initiaion of all the below listed forensic imaging and preliminary forensic analysis, a detailed legal document review was conducted with the assistance of the Computer Crime Investigative Unit (CCIU) Legal Team, ensuring CCIU possessed the adequate consent to search and/or search authorization.

About 1655, 30 May 10, SA (b)(6)(b)(7)(C) unsealed a Hewlett Packard (HP) brand, laptop computer, serial number CNF8492K3S, property of SSG (b)(6)(b)(7)(C) Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, forward deployed to Forward Operating Base (FOB) Hammer, Iraq, collected as evidence on EPCD, DN 0592-10, and verified the item with no documentary errors noted. SSG (b)(6)(b)(7)(C) previously informed CID special agents that he allowed PFC Bradley E. MANNING, HHC, 2nd BCT, to borrow this laptop on several occasions during May 2010. The laptop was checked for any data bearing devices or media, but none were found. It was noted that the Basic Input Output System (BIOS) reflected the correct time and date (GMT -5), with DST in effect equaling GMT -4. The hard disk drive (HDD), Samsung brand, serial number S1AKJDNQ816517, 320 gigabyte (GB) in size, was removed from the HP laptop for forensic imaging.

About 1755, 30 May 10, SA (b)(6)(b)(7)(C) collected the aforementioned Samsung HDD as evidence on EPCD, DN 0583-10.

Between approximately 1805, 30 May 10, and 0330, 31 May 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned Samsung HDD. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of Secure Hash Algorithm 1 (SHA1) values with no errors:

Acquisition Hash SHA1: 676162e5305d9a8688a44ebd89a7fdef3567db36
Verification Hash SHA1: 676162e5305d9a8688a44ebd89a7fdef3567db36

About 2135, 30 May 10, SA (b)(6)(b)(7)(C) unsealed a Macintosh brand, laptop computer, serial number MV9371AJ9935A, property of PFC MANNING, collected as evidence on EPCD, DN 0579-10, and verified the item with no documentary errors noted. The laptop was checked for any data bearing devices or media, but none were found. The HDD, Fujitsu brand, serial number K94DT9829WPY, 250 GB in size, was removed from the laptop for forensic imaging and subsequently reinstalled.

About 2150, 30 May 10, SA (b)(6)(b)(7)(C) attempted to boot the aforementioned Macintosh laptop with a Helix 3 Pro Live Disc, which was unsuccessful and resulted in the laptop booting from the internal Fujitsu brand HDD. This inadvertent HDD boot determined at least one user

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
(b)(6)(b)(7)(C) [redacted]	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT
CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

account on the laptop was not password protected. The Macintosh laptop was then gracefully shut down.

AGENT's COMMENT: An initial attempt was made to obtain a forensic image of the aforementioned Macintosh brand laptop computer via Helix 3 Pro Live Disc, due to the often difficult/delicate task of removing HDDs from Macintosh products.

Between approximately 1240 and 2100, 31 May 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned Macintosh HDD. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: 3cf107db8b3865a5e3ebfce400bae1da9691fb49
Verification Hash SHA1: 3cf107db8b3865a5e3ebfce400bae1da9691fb49

Between 1420 and 1620, 1 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of this forensic image, and determined it was formatted with the Hierarchical File System (HFS), had Mac OS installed, and had a user account resembling PFC MANNING's name. A review of device logs contained on the HDD determined some form of optical disc activity occurred (e.g., wiping or burning) on or around 27 Apr 10. A review of the `User` files associated with the user account suspected to pertain to PFC MANNING located several files containing text that was specifically referenced in the chat logs received by U.S. Army CID (USACIDC) during the initial phases of this investigation. A review of installed programs, determined a chat client was installed. A review of other partitions on the HDD revealed a separate partition named "images," which contained file named `strongbox.dmg`, which was approximately 6 GB in size, password protected, and possibly encrypted.

About 0410, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a Dell brand, laptop computer, serial number 93H4QD1, property of HHC, 2nd BCT, collected as evidence on EPCD, DN 0593-10, and verified the item with no documentary errors noted. This was determined to be the Non-classified Internet Protocol Router Network (NIPRNET) laptop computer, which had been located near the work area of PFC MANNING. The laptop was checked for any data bearing devices or media, but none were found. It was noted that the BIOS reflected the correct time and date (GMT +3). The HDD, unknown brand, serial number 5MH0TB78, 100 GB in size, was removed from the Dell laptop for forensic imaging.

About 0510, 31 May 10, SA (b)(6)(b)(7)(C) collected the aforementioned unknown brand HDD as evidence on EPCD, DN 0584-10.

Between approximately 0515 and 0840, 31 May 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned unknown brand HDD. The resulting forensic image

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: e2b49bd3ed0e2f5d798ab44 febaac3b15d0070be
Verification Hash SHA1: e2b49bd3ed0e2f5d798ab44 febaac3b15d0070be

About 0600, 31 May 10, SA (b)(6)(b)(7)(C) unsealed the Memorex brand, Compact Disc – Rewritable (CD-RW) discs, serial numbers 1308120503204624 and 1308120503204625, property of PFC MANNING, collected as evidence on EPCD, DN 0579-10, and verified the item with no documentary errors noted.

Between 0605 and 0615, 31 May 10, SA (b)(6)(b)(7)(C) utilizing a Gateway brand, model E-475 MG, laptop computer, running a Helix 3 Pro Live Disc, determined no data was written or likely had been written to the CD-RW discs. This observation was supported by inspection of the underside of the aforementioned CD-RW discs.

About 0630, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a package containing eight Memorex brand, Digital Versatile Disc – Rewritable (DVD-RW) discs, serial numbers 1909052107834101, 1909052107834102, 2009052100920471, 2009052100920481, 2009052100920483, 2009052100920485, 2009052100920487 and 2009052104924365, property of PFC MANNING, collected as evidence on EPCD, DN 0579-10, and verified the item with no documentary errors noted.

Between 0640 and 0700, 31 May 10, SA (b)(6)(b)(7)(C) used Helix 3 Pro Live Disc to determine no data was written or likely had been written to the DVD-RW discs. This observation was supported by visual inspection of the underside of the aforementioned DVD-RW discs.

About 0930, 31 May 10, SA (b)(6)(b)(7)(C) unsealed an Alienware brand, laptop computer, serial number NKD900TA6D00661, property of HHC, 2nd BCT, collected as evidence on EPCD, DN 0594-10, and verified the item with no documentary errors noted. This was determined to be the first of two Secret Internet Protocol Router Network (SIPRNET) laptop computers assigned to PFC MANNING. The laptop was checked for any data bearing devices or media, but none were found. The device was then checked for any data bearing devices or media, but none were found. It was noted that the BIOS reflected the correct time and date (GMT +3). The HDD, Seagate brand, serial number 3MH036M1, 80 GB in size, was removed from this device for forensic imaging.

About 1030, 31 May 10, SA (b)(6)(b)(7)(C) collected the aforementioned Seagate HDD as evidence on EPCD, DN 0577-10.

Between approximately 2310, 31 May 10, and 0240, 1 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned HDD. The resulting forensic image was

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT
CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: c7400fbed0b4db68a582a585eeaa34ab1a62cd64
Verification Hash SHA1: c7400fbed0b4db68a582a585eeaa34ab1a62cd64

Between 1800, 1 Jun 10, and 1000, 2 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of this forensic image, which revealed PFC MANNING had a user account on this laptop. Analysis also determined b(1) was located on this machine, as well as what appeared to be a similar production video released by the WikiLeaks Team. A review of PFC MANING's stored email revealed he notified someone in his chain of command that the aforementioned classified SECRET video was on the Internet and of his (PFC MANNING's) belief that it was the same video from the FOB Hammer SIPRNET data server. Further analysis revealed multiple artifacts indicating browsing from PFC MANNING's user account to the Brigade Legal Team's share on the FOB Hammer data server, as well as the possible downloading of legal documents unrelated to the PFC MANNING. A review of PFC MANNING's `My Documents` folders revealed a file that appeared to be instructions to a web download program used to reach out to a SIPRNET site and download large amounts of specific documents of a sensitive and classified nature. This `My Documents` folder review further revealed an archive file that contained approximately 11,000 sensitive and classified documents, downloaded in Hyper Text Markup Language (HTML) format, likely from a SIPRNET site. This archive file further contained a file that appeared also to be instructions or log results for a web download program.

About 1120, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a Hitachi brand, laptop computer, serial number 070817DP0C10DSG2 J1DP, property of HHC, 2nd BCT, collected as evidence on EPCD, DN 0580-10, and verified the item with no documentary errors noted. This was determined to be the NIPRNET computer that was located in PFC MANNING's unit Supply Office, where the he worked temporarily during May 2010.

Between approximately 2050, 31 May 10, and 0030, 1 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the HDD contained with the aforementioned Hitachi laptop computer. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: 309df99f068fba2e81aae03d1a93d471cde90bf0
Verification Hash SHA1: 309df99f068fba2e81aae03d1a93d471cde90bf0

About 2030, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a Samsung brand, mobile phone, serial number RPRS303202D, property of PFC MANNING, collected as evidence on EPCD, DN 0579-10, and verified

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

the item with no documentary errors noted. SA (b)(6)(b)(7)(C) only verified the mobile phone manufacturer, as it was impossible to verify further information without removing the mobile phone's battery, which had the potential to damage data contained thereon.

About 2035, 31 May 10, SA (b)(6)(b)(7)(C) determined the equipment necessary to forensically process the aforementioned mobile phone was not available.

About 2040, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a Kodak brand, digital camera, partial serial number KCXKS9, property of PFC MANNING, collected as evidence on EPCD, DN 0579-10, and verified the item with no documentary errors noted. The Mini-Secure Digital (SD) card, Scandisk brand, serial number BE0828613591D, 2 GB in capacity, was removed from this device for forensic imaging.

Between 2050 and 2055, 31 May 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned Mini-SD card. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of Message Digest 5 (MD5) hash algorithm values with no errors:

Acquisition Hash MD5: b6fe0f698c3d648a49f3432bdaaac828
Verification Hash MD5: b6fe0f698c3d648a49f3432bdaaac828

About 2100, 31 May 10, SA (b)(6)(b)(7)(C) reviewed this device's specifications, available on the Kodak manufacturer's website, which revealed it contained approximately 32 Megabytes (Mb) of internal memory. A review of the device determined the necessary cables were not available to process the aforementioned internal memory cache.

Between 1130 and 1300, 2 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of the forensic image for the SD card, which revealed it contained two folders of digital photographic images. These photographs were of unclassified documents (e.g., what appeared to be an Article 15 involving PFC MANNING, of a promotion ceremony, of PFC MANNING himself, of an unidentified Caucasian male, and of several unidentified locations).

About 2110, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a multi-disc case containing three Arabic language Compact Discs (CD)s, property of PFC MANNING, and one CD-RW, serial number LD623 MJ04184038 B16, recovered from the quarters of PFC MANNING, all collected as evidence on EPCD, DN 0579-10, and verified the item with no documentary errors noted.

About 2120, 31 May 10, SA (b)(6)(b)(7)(C) used Helix 3 Pro Live Disc to determine the three language discs contained only audio files, consistent with the manufacturer's markings.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

Between 2125 and 2135, 31 May 10, SA (b)(6)(b)(7)(C) obtained a forensic image of the aforementioned CD-RW. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of MD5 hash algorithm values with no errors:

Acquisition Hash MD5: 5c993ee621b036482bae1353f844322f
Verification Hash MD5: 5c993ee621b036482bae1353f844322f

Between 1400 and 1430, 2 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of this image, revealing it contained two files with identical names, one of which contained no data and the other contained b(1) [redacted] The video appeared to have been burned to the disc on 27 Apr 10 and appeared to have been burned by utilizing Macintosh disc creation software.

About 2230, 31 May 10, SA (b)(6)(b)(7)(C) unsealed a Dell brand, laptop computer, serial number JP-0F5126-42016-76D-0517, property of HHC, 2nd BCT, collected as evidence on EPCD, DN 0594-10, and verified the item with no documentary errors noted. This was determined to be the second of the two SIPRNET laptop computers assigned to PFC MANNING. The Dell laptop was checked for any data bearing devices or media, but none were found. It was noted that the BIOS reflected the correct time and date (GMT +1), with DST in effect equaling GMT +2. The HDD, unknown brand, serial number 5MH0HWKN, was removed from this device for forensic imaging.

About 2330, 31 May 10, SA (b)(6)(b)(7)(C) collected the aforementioned unknown brand HDD, unknown brand, serial number 5MH0HWKN, as evidence on EPCD, DN 0577-10.

Between approximately 0530 and 1130, 1 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned unknown brand HDD. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: c3473c3df1d131e0022f0c56bfc46087e9d5150f
Verification Hash SHA1: c3473c3df1d131e0022f0c56bfc46087e9d5150f

Between 1500 and 1530, 2 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of this forensic image, which revealed PFC MANNING had a user account on the laptop.

About 0200, 1 Jun 10, SA (b)(6)(b)(7)(C) unsealed a Seagate brand, external HDD, serial number 2GEWJKLJ, property of PFC MANNING, collected as evidence on EPCD, DN 0579-10, and verified the item with no documentary errors noted. SA (b)(6)(b)(7)(C) determined the necessary power adapter was not available to reliably and safely power the Seagate brand external HDD. For this reason, the HDD,

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

CID FO[redacted]
1 FEB 77

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

Seagate brand, serial number 9VS1S2TZ, 1.5 Terabyte (Tb) in size, was removed for forensic imaging, using a fine tool set causing minimal cosmetic damage to the external casing and no damage to the HDD.

About 0300, 1 Jun 10, SA (b)(6)(b)(7)(C) collected the aforementioned Seagate HDD as evidence on EPCD, DN 0581-10.

Between approximately 1345, 1 Jun 10, and 0800, 2 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned HDD. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: 151183463c5b5841a8115627bf51e8d9e74abb48
Verification Hash SHA1: 151183463c5b5841a8115627bf51e8d9e74abb48

Between 1600 and 1700, 2 Jun 10, SA (b)(6)(b)(7)(C) conducted a preliminary forensic examination of this image and determined it was formatted with HFS. A review of its contents revealed a file containing the contact information of a member of the WikiLeaks Team. This contact information appeared to have been produced and released by the WikiLeaks Team and did not appear to be of a personal nature.

About 0940, 1 Jun 10, SA (b)(6)(b)(7)(C) unsealed a Toshiba brand, laptop computer, serial number Z5FX1 [redacted] 6P2 EC A, property of HHC, 2nd BCT, collected as evidence on EPCD, DN 0582-10, and verified the item with no documentary errors noted. This was determined to be the SIPRNET computer of SPC (b)(6)(b)(7)(C) HHC, 2nd BCT, who reported that she was asked by PFC MANNING on more than one occasion in May 2010 to receive digitally scanned documents via email and print them on his behalf. PFC MANNING then allegedly asked SPC (b)(6)(b)(7)(C) to delete the emails from her MS Outlook Inbox.

Between approximately 0320 and 0520, 1 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the HDD within the aforementioned Toshiba laptop. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: 6a9b4e366790fb9f02b88a9ba29c3f3fbe610300
Verification Hash SHA1: 6a9b4e366790fb9f02b88a9ba29c3f3fbe610300

About 0845, 1 Jun 10, SA (b)(6)(b)(7)(C) unsealed a Seagate brand, HDD, serial number CN-0MN922-21232-793-002L, property of HHC, 2nd BCT, collected as evidence on EPCD, DN 0580-10, and verified the item with no documentary errors noted. This was determined to be from the SIPRNET computer located in PFC MANNING's unit Supply Office, where he worked temporarily during May of 2010.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

Between approximately 1000 and 1300, 1 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase forensic image (.E01) of the aforementioned Seagate HDD. The resulting forensic image was verified to be an exact, bit-for-bit copy of the HDD through a comparison of SHA1 values with no errors:

Acquisition Hash SHA1: cf6d703f0023773e b9e30eeb318660ac0d18f404
Verification Hash SHA1: cf6d703f0023773e b9e30eeb318660ac0d18f404

About 0900, 2 Jun 10, SA (b)(6)(b)(7)(C) coordinated this investigation with CPT (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Brigade Automation Officer, 2nd BCT, who was asked to describe the storage area network (SAN) on the SIPR local area network (LAN) at FOB Hammer. CPT (b)(6)(b)(7)(C) related the SAN was large, over 10 terabytes (TB) in size, and was essentially handed down from one deployed BCT to another. CPT (b)(6)(b)(7)(C) was asked to describe the current security settings for the Brigade Legal Team's data share at FOB Hammer. CPT (b)(6)(b)(7)(C) advised they were currently set to restricted; however, this setting had only been changed between 27 Apr 10 and 20 May 10. Prior to this time frame, the aforementioned data share had unrestricted settings. When asked about b(1) b(1) CPT (b)(6)(b)(7)(C) related that the video could be found in three locations on the FOB Hammer SIPR SAN. Copies were located on the aforementioned Brigade Legal Team's data share, the 431st Infantry LNO's data share, the 382nd Archived Training Material data share. CPT (b)(6)(b)(7)(C) related none of these copies of the video in question appeared to be related to an investigation or the response to a Freedom of Information Act (FOIA) request.

About 1130, 4 Jun 10, SA (b)(6)(b)(7)(C) coordinated this investigation with MAJ (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Commander, Brigade Legal Team, 2nd BCT, 10th Mountain, who was briefed on the status of this investigation as it pertained to this office's desire to preserve and collect a copy of his unit's data share at FOB Hammer. MAJ (b)(6)(b)(7)(C) confirmed that no Trial Defense Service (TDS) unit was using or had used the aforementioned data share. SA (b)(6)(b)(7)(C) subsequently forwarded MAJ (b)(6)(b)(7)(C) the Preservation Request Notification titled "Request to Preserve SJA Shared Directory," drafted by Ms. (b)(6)(b)(7)(C) Chief Legal Counsel, CCIU, and dated 4 Jun 10.

About 1200, 4 Jun 10, SA (b)(6)(b)(7)(C) coordinated this investigation with CPT (b)(6)(b)(7)(C) S-2, 2nd BCT, and CPT (b)(6)(b)(7)(C) Commander, HHC, 2nd BCT, who were briefed on the status of this investigation as it pertained to this office's desire to preserve and collect a copy of PFC MANNING's data share at FOB Hammer. SA (b)(6)(b)(7)(C) subsequently forwarded both individuals the Preservation Request Notification titled "Request to Preserve Individual Shared Directory of Bradley E. Manning," drafted by Ms. (b)(6)(b)(7)(C) and dated 4 Jun 10.

About 1600, 5 Jun 10, SA (b)(6)(b)(7)(C), collected as evidence one Seagate brand, HDD, serial number 9VS25G5M, containing the unclassified forensic images of the following devices which had been previously transferred to the HDD for consolidation and evidence retention, on EPCD, DN 0585-10:

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C)	DATE 5 Jun 10	EXHIBIT 34

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

- One HDD, unknown brand, serial number 5MH0TB78, collected as evidence on EPCD, DN 0584-10, previously contained in the Dell brand, laptop computer, serial number 93H4QD1, collected as evidence on EPCD, DN 593-10 (SHA1 Hash - e2b49bd3ed0e2f5d798ab44 febaac3b15d0070be)
- One HDD, Fujitsu brand, serial number K94DT9829WPY, collected as evidence on EPCD, DN 0579-10, previously contained in the Mac brand, laptop computer, serial number MV9371AJ9935A, collected as evidence on EPCD, DN 0579-10 (SHA1 Hash - 3cf107db8b3865a5e3ebfce400bae1da9691fb49)
- One HDD, Seagate brand, serial number 9VS1S2TZ, collected as evidence on EPCD, DN 0581-10, previously contained in the Seagate brand, external HDD, serial number 2GEWJKLJ, collected as evidence on EPCD, DN 0579-10 (SHA1 Hash - 151183463c5b5841a8115627bf51e8d9e74abb48)
- One Mini-SD card, Scandisk brand, serial number BE0828613591D, collected as evidence on EPCD, DN 0579-1, previously contained in the Kodak brand, digital camera, partial serial number KCXKS9, collected as evidence on EPCD, DN 0579-10 (MD5 Hash - b6fe0f698c3d648a49f3432bdaaac828)
- One HDD, Hitachi brand, serial number 070817DP0C10DSG2J1DP, collected as evidence on EPCD, DN 0580-10 (SHA1 Hash - 309df99f068fba2e81aae03d1a93d471cde90bf0)
- One HDD, Samsung brand, serial number S1AKJDNQ816517, collected as evidence on EPCD, DN 0583-10, previously contained in the HP brand, laptop computer, serial number CNF8 492K3S, collected as evidence on EPCD, DN 0592-10 (SHA1 Hash - 676162e5305d9a8688a44ebd89a7fdef 3567db36)

SA (b)(6)(b)(7)(C) also collected as evidence one Seagate brand, HDD, serial number 5VG1826C,

b(1) [redacted]

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E) [redacted]	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C) [redacted]	DATE 5 Jun 10	EXHIBIT 34

CID F[redacted]
1 FEB 77

Approved: 000277

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0004-10-CID187

DETAILS

b(1) [redacted]

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit-Europe U.S. Army CID, Mannheim, Germany	
SIGNATURE (b)(6)(b)(7)(C) [redacted]	DATE 5 Jun 10	EXHIBIT 34

CID [redacted]
1 FEB 77

CLASSIFIED

Exhibit(s) 35

Page(s) 000279 thru 000279b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 36

Page(s) 000280 thru 000280b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 37

Page(s) 000281 thru 000281b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 38

Page(s) 000282 thru 000282f referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 39

Page(s) 000283 thru 000283c referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 40

Page(s) 000284 thru 000284b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 41

Page(s) 000285 thru 00285c referred to:

Defense Intelligence Agency
ATTN: DAN-1A (FOIA)
200 MacDill Blvd
Washington, DC 20340-5100

CLASSIFIED

Exhibit(s) 42

Page(s) 000286 thru 00286e referred to:

Defense Intelligence Agency
ATTN: DAN-1A (FOIA)
200 MacDill Blvd
Washington, DC 20340-5100

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 0025, 12 Jun 10, this office received the name check results on PFC MANNING from the U.S. Army Crime Records Center (USACRC), Fort Belvoir, VA 22060, which revealed no derogatory information.

About 0037, 12 Jun 10, SA (b)(6)(b)(7)(C) 7169, Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, obtained Consent to Search from Mr. (b)(6)(b)(7)(C) authorizing a search of his hard disk drive (HDD), collected on Evidence/Property Custody Document (EPCD), Document Number (DN) 076-10. (See Consent to Search)

About 0048, 12 Jun 10, SA (b)(6)(b)(7)(C) obtained Consent to Search from Mr. (b)(6)(b)(7)(C) authorizing a search of eight email messages forwarded to SA (b)(6)(b)(7)(C) Gmail account (b)(6)(b)(7)(C) @gmail.com) from Mr. (b)(6)(b)(7)(C) account (b)(6)(b)(7)(C) org), which purportedly originated form PFC MANNING. (See Consent to Search)

About 0100, 12 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence a HDD removed from the Lenovo laptop computer of Mr. (b)(6)(b)(7)(C) purportedly containing four of Mr. (b)(6)(b)(7)(C) chat logs pertaining to his chats with PFC MANNING, which was documented on EPCD, DN 076-10.

About 0203, 12 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence an HP Mini laptop computer from Mr. (b)(6)(b)(7)(C) purportedly containing one of Mr. (b)(6)(b)(7)(C) chat logs pertaining to his chats with PFC MANNING, which was documented on EPCD, DN 077-10.

About 0204, 12 Jun 10, SA (b)(6)(b)(7)(C) obtained Consent to Search from Mr. (b)(6)(b)(7)(C) authorizing a search of his HP Mini laptop computer collected on EPCD, DN 077-10. (See Consent to Search)

About 1200, 12 Jun 10, SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) former Military Intelligence (MI) SA, (b)(6)(b)(7)(C) , who related he met and initiated a relationship with Mr. (b)(6)(b)(7)(C) during their employment with AOL, approximately 2001-2002, which ended when Mr. (b)(6)(b)(7)(C) enlisted in the U.S. Army in 2002; however, periodic communication as friends was continual. Mr. (b)(6)(b)(7)(C) related in late May 10, or early Jun 10, Mr. (b)(6)(b)(7)(C) approached Mr. (b)(6)(b)(7)(C) via telephone, to discuss his communication pertaining to PFC MANNING, who admitted to Mr. (b)(6)(b)(7)(C) that he had distributed classified information to WikiLeaks and Mr. Julian P. ASSANGE, founder and Director of WikiLeaks, Townsville, Queensland, AU. Mr. (b)(6)(b)(7)(C) related he told Mr. (b)(6)(b)(7)(C) to contact the appropriate authorities and Mr. (b)(6)(b)(7)(C) reported the information to the Federal Bureau of Investigation (FBI) and U.S. Army MI.

About 1853, 12 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence two thumb drives, purportedly containing Mr. (b)(6)(b)(7)(C) chat logs with PFC MANNING, which was initially seized through transfer on the U.S. Army MI EPCD, DN 001-10 and the FBI Evidence Chain of Custody (ECC) Form E4270311 and then collected and documented upon return to this office, on EPCD, DN 079-10.

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
(b)(6)(b)(7)(C)	DATE: 16 Jun 10 / EXHIBIT: 437

DETAILS

About 1830, 13 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, conducted online research at wikileaks.org and identified the submission Uniform Resource Locator (URL) as https://secure.wikileaks.org, which resolved to the following Internet Protocol (IP) addresses 88.80.2.32 and 88.80.13.160.

About 2220 (PST), 13 Jun 10, SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) in a non-custodial setting, who rendered a Sworn Statement, wherein he described the chats and emails he exchanged with PFC MANNING. (See Sworn Statement)

About 0913, 14 Jun 10, this office received the name check results on Mr. (b)(6)(b)(7)(C) from the USACRC, Fort Belvoir, VA 22060, which revealed no derogatory information.

About 0939, 14 Jun 10, this office received the name check results on Mr. (b)(6)(b)(7)(C) from the USACRC, Fort Belvoir, VA 22060, which revealed no derogatory information.

About 0900, 15 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, received an email from Mr. (b)(6)(b)(7)(C) Manager, Stored Value Card Programs, U.S. Treasury Department, 401 14th Street, SW, Washington, DC 20227, containing the transaction records for PFC MANNING's EagleCash stored value card account and PFC MANNING's application for a DoD stored value card dated, 12 Oct 09. The record contained all of PFC MANNING's EagleCash transactions between 12 Oct 09 and 29 May 10. The record showed PFC MANNING's EagleCash card was used on 21 Apr 10, at the Forward Operating Base (FOB) Hammer Post Office for $13.50. (See EagleCash Transaction Records)

About 1110, 15 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both WMRA, CCIU, Fort Belvoir, VA 22060, coordinated with Mr. (b)(6)(b)(7)(C) Special Projects, Mr. (b)(6)(b)(7)(C) Program Manager, and Mr. (b)(6)(b)(7)(C) Division Chief, all with the U.S. Department of State (DoS), Springfield, VA 22052, to obtain the logs for the DoS server, which hosted the Netcentric Diplomacy Database (NDD) that contained the State Department cables. SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) travelled to the Harry S. Truman Building (State Department), 2201 C Street NW, Washington DC 22052, to access the server hostname: NTNCDSQL5S, IP address 199.56.188.73, located in Room 3684A, which was storing the data to be retrieved. Mr. (b)(6)(b)(7)(C) advised the host computer was in a "DMZ" located between two firewalls on the DoS side and two firewalls on the Secure Internet Protocol Router (SIPR) side. SA (b)(6)(b)(7)(C) was given access to Old War Rack C-2 and the server in question, into which SA (b)(6)(b)(7)(C) placed a USB storage device ("thumbdrive") to collect the data. SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) collected the files "logs.zip" and "newlogs.zip" which contained the server logs for the periods Jan-Jun 09, and Apr 30 to present, respectively. System time on server was set to GMT (+4:00). Additionally, Mr. (b)(6)(b)(7)(C) advised he had verified that PFC MANNING had an INTELINK account, and PFC MANNING had logged into it numerous times beginning 21 Feb 10 and continuing through part of Mar 10.

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 16 Jun 10	EXHIBIT 43

DETAILS

Between 1510 and 1530, 15 Jun 10, SA (b)(6)(b)(7)(C) obtained an EnCase Logical Evidence File of the zip files collected from the U.S. DoS Server and supporting hash values. The Logical Evidence File was named "DoS_Server_Logs.L01", and placed on a DVD. The computed hash value of the Logical Evidence File was: ac4ccbea1f96257576604a47335b72fa.

About 1535, 15 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence one DVD, containing the EnCase Logical Evidence File pertaining to the logs of the computer assigned IP address 199.56.188.73 from the forensic computer, which was documented on EPCD, DN 078-10.

About 0930, 16 Jun 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, coordinated with Mr. (b)(6)(b)(7)(C) Investigative Technician, Directorate of Emergency Services (DES), Fort Belvoir, VA 22060, who conducted a National Crime Information Center (NCIC), Interstate Identification Index (III), name checks on the following individuals, which revealed no derogatory information:

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

(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)
(b)(6)(b)(7)(C)
Bradley E. MANNING

About 1130, 16 Jun 10, SA (b)(6)(b)(7)(C) coordinated with CPT (b)(6)(b)(7)(C), Brigade Automation Officer, S6, and CPT (b)(6)(b)(7)(C) S2, both with Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq, APO AE 09308. CPT (b)(6)(b)(7)(C) related the unit did not maintain any Joint Worldwide Intelligence Communication System (JWICS) equipment. CPT (b)(6)(b)(7)(C) related the S-2 section did have NSANet computers; however, PFC MANNING did not have an account and was not authorized to use them. CPT (b)(6)(b)(7)(C) clarified that the NSANet belonged to the Signals Intelligence section, and was outside the scope of PFC MANNING's duties. CPT (b)(6)(b)(7)(C) stated there was a two person rule, which would have had to have been violated in order for PFC MANNING to have had access. CPT (b)(6)(b)(7)(C) further stated when she returned from leave, on or about 22 Apr 10, she asked the personnel in her section if they had seen the Apache video played on the news. PFC MANNING told her he believed it was the same video they had on the shared drive and later proved it to her by sending her a link to it. CPT (b)(6)(b)(7)(C) stated the video was in four places on the shared drive that included a training folder pertaining to "Positive Identification," which contained the Apache video and another [unspecified] video. CPT (b)(6)(b)(7)(C) related any Soldier was permitted access to the training folder, though it was unlikely PFC MANNING would have known to look there. According to CPT (b)(6)(b)(7)(C) PFC MANNING should not have been accessing the SJA folder.

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 16 Jun 10	EXHIBIT 43

DETAILS

About 1315, 16 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E), WMRA, CCIU, Fort Belvoir, VA 22060, collected as evidence the email and attached file from Mr. (b)(6)(b)(7)(C) Army Knowledge Online (AKO), Fort Belvoir, VA 22060, containing the To/From, Dates and Times for PFC MANNING's AKO account, which was collected on an EPCD, DN 082-10.////////////////////////////////////LAST ENTRY////////////////////////////////

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 16 Jun 10	EXHIBIT 43

USACIDC Supplement 1 to AR 190-22

Date: 12 Jun 10 (b)(6)(b)(7)(C)	**Consent To Search** (USACIDC Supplement 1 to AR 190-22)	Time: 0037 (b)(6)(b)(7)(C)

1. Name of person consenting to the search: Mr. (b)(6)(b)(7)(C)

2. Organization and location: (b)(6)(b)(7)(C)

3. I have been informed by the undersigned USACIDC Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law:
Title 18 U.S.C., Section 1030: Fraud and related activity in connection with computers,
Title 18 U.S.C., Section 793: Gathering, transmitting or losing defense information (b)(6)(b)(7)(C)
Title 18 U.S.C., Section 798: Disclosure of classified information; and,
U.C.M.J., Article 106a: Espionage

4. I have been requested by the undersigned USACIDC Special Agent to give my consent to a search of my person, premises, or property as indicated below. I have been advised of my right to refuse a search of my person, premises, or property. (If you do not give your consent, do not sign this form)

5. I hereby authorize the undersigned USACIDC Special Agent and/or other Authorized Law Enforcement Officials assisting the undersigned USACIDC Special Agent to conduct a search of: ***(Initial and sign applicable blocks)*** Additionally, I further give my expressed consent to allow the items I am consenting to have searched, be searched by non-law enforcement and/or technical subject matter expert personnel under the supervision of USACIDC.

		Initials	Signature
a.	My Person		
b.	My Quarters		

Located At:

		Initials	Signature
c.	My Vehicle		

Located At:

Described As:

		Initials	Signature
d.	Other	(b)(6)(b)(7)(C)	

Located At: (b)(6)(b)(7)(C) (to be collected as evidence and (b)(6)(b)(7)(C) examined at USACIDC facilities or other locations under the supervision of USACIDC personnel)

Described As: A Hard Disk Drive (HDD), Fujitsu brand, Model MH[redacted]4D [redacted] from Lenovo Laptop Computer, SN: LU-A0384 07/10); the property of Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C)

I am authorizing the above search(s) for the following general types of property which [redacted] the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations:

All information in any form, pertaining to communications which may be in the form: of emails, instant messaging chats, documents, data, computer code, log files, drawings, photographs, or any other data; in encrypted, plain text, or any other format; relating to PFC Bradley [redacted] and/or the disclosure of classified information or information which is the property of the U.S. Government. (b)(6)(b)(7)(C)

6. This written permission is given to the undersigned [redacted] without threats or promises of any kind:

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

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

SA

Signature of Witness (If Available)

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

CID Form 87-R-E
1 Jan 00

PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE

For Official Use Only
Law Enforcement
Sensitive

Exhibit 44
000291

USACIDC Supplement 1 to AR 190-22

Date: 12 Jun 10 (b)(6)(b)(7)(C)

Consent To Search

(USACIDC Supplement 1 to AR 190-22)

Time: 0048 (b)(6)(b)(7)(C)

1. Name of person consenting to the search: Mr. (b)(6)(b)(7)(C)

2. Organization and location: (b)(6)(b)(7)(C)

3. I have been informed by the undersigned USACIDC Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law:
Title 18 U.S.C., Section 1030: Fraud and related activity in connection with computer (b)(6)(b)(7)(C)
Title 18 U.S.C., Section 793: Gathering, transmitting or losing defense information;
Title 18 U.S.C., Section 798: Disclosure of classified information; and,
U.C.M.J., Article 106a: Espionage

4. I have been requested by the undersigned USACIDC Special Agent to give my consent to a search of my person, premises, or property as indicated below. I have been advised of my right to refuse a search of my person, premises, or property. (If you **do not** give your consent, do not sign this form)

5. I hereby authorize the undersigned USACIDC Special Agent and/or other Authorized Law Enforcement Officials assisting the undersigned USACIDC Special Agent to conduct a search of: ***(Initial and sign applicable blocks)*** Additionally, I further give my expressed consent to allow the items I am consenting to have searched, be searched by non-law enforcement and/or technical subject matter expert personnel under the supervision of USACIDC.

		Initials	Signature
a.	My Person		
b.	My Quarters		

Located At:

		Initials	Signature
c.	My Vehicle		

Located At:

Described As:

		Initials	Signature
d.	Other	(b)(6)(b)(7)(C)	

Located At: (b)(6)(b)(7)(C) (to be collected as evidence and searched/examined at USACIDC facilities or other locations under the supervision of USACIDC personnel) (b)(6)(b)(7)(C)

Described As: Email messages sent from the email accounts (b)(6)(b)(7)(C) com" and/or (b)(6)(b)(7)(C) org", the property of Mr. (b)(6)(b)(7)(C) sent to the email address(es) of USACIDC investigators (b)(6)(b)(7)(C)

I am authorizing the above search(s) for the following general types of property which may be removed by the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations:

All information in any form, pertaining to communications which may be in the form: of emails, instant messaging chats, documents, data, computer code, log files, drawings, photographs, or any other data; in encrypted, plain text, or any other format; relating to PFC Bradley E. MANNING and/or the disclosure of classified information or information which is the property of the U.S. Government. (b)(6)(b)(7)(C)

6. This written permission is given to the undersig (b)(6)(b)(7)(C) or promises of any kind:

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

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

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

Signature of USACIDC Special Agent

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

Signature of Witness (If Available)

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

CID Form 87-R-E
1 Jan 00

PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE

For Official Use Only
Law Enforcement
Sensitive

Exhibit 45

USACIDC Supplement 1 to AR 190-22

Date: 12 Jun 10 (b)(6)(b)(7)(C) redacted	**Consent To Search** (USACIDC Supplement 1 to AR 190-22)	Time: 0204 (b)(6)(b)(7)(C) redacted

1. Name of person consenting to the search: Mr. (b)(6)(b)(7)(C) redacted

2. Organization and location: (b)(6)(b)(7)(C) redacted

3. I have been informed by the undersigned USACIDC Special Agent that an inquiry is being conducted in connection with the following possible violation(s) of law:
Title 18 U.S.C., Section 1030: Fraud and related activity in connection with computer; (b)(6)(b)(7)(C) redacted
Title 18 U.S.C., Section 793: Gathering, transmitting or losing defense information;
Title 18 U.S.C., Section 798: Disclosure of classified information; and,
U.C.M.J., Article 106a: Espionage

4. I have been requested by the undersigned USACIDC Special Agent to give my consent to a search of my person, premises, or property as indicated below. I have been advised of my right to refuse a search of my person, premises, or property. (If you **do not** give your consent, do not sign this form)

5. I hereby authorize the undersigned USACIDC Special Agent and/or other Authorized Law Enforcement Officials assisting the undersigned USACIDC Special Agent to conduct a search of: ***(initial and sign applicable blocks)*** Additionally, I further give my expressed consent to allow the items I am consenting to have searched, be searched by non-law enforcement and/or technical subject matter expert personnel under the supervision of USACIDC.

		Initials	Signature
a.	My Person		
b.	My Quarters		
Located At:			
c.	My Vehicle		
Located At:			
Described As:			
d.	Other (b)(6)(b)(7)(C) redacted		

Located At: (b)(6)(b)(7)(C) redacted (to be collected as evidence and searched/examined at USACIDC facilities or other locations under the supervision of USACIDC personnel) (b)(6)(b)(7)(C) redacted

Described As: An HP2133 Laptop Computer, HPMini Brand, SN: CN490513UT; with AC Power Adapter, SN: F1-08122282330C; both the property of Mr. (b)(6)(b)(7)(C) redacted

I am authorizing the above search(s) for the following general types of property which may be removed by the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations:

All information in any form, pertaining to communications which may be in the form: of emails, instant messaging chats, documents, data, computer code, log files, drawings, photographs, or any other data; in encrypted, plain text, or any other format; relating to PFC Bradley E. MANNING and/or the disclosure of classified information or information which is the property of the U.S. Government. (b)(6)(b)(7)(C) redacted

6. This written permission is given to the undersigned USACIDC Special Agent freely, voluntarily and without threats or promises of any kind:

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

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

Signature of USACIDC Special Agent

SA (b)(6)(b)(7)(C) redacted

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

Signature of Witness (If Available)

SA (b)(6)(b)(7)(C) redacted

CID Form 87-R-E
1 Jun 00

PREVIOUS EDITIONS OF THIS FORM ARE OBSOLETE

Exhibit 46

FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE
SWORN STATEMENT

FILE NUMBER : 0028-10-CID221-10117
LOCATION : Fort Belvoir, VA 22060
DATE : 13 Jun 2010 TIME: 2120
NAME : Mr (b)(6)(b)(7)(C)
SSAN : (b)(6)(b)(7)(C) Grade/Status: Civilian
ORG/ADDRESS : (b)(6)(b)(7)(C)

(b)(6)(b)(7)(C) WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

About 2031 (UTC), 20 May 10, Bradley E. Manning, contacted me via e-mail from the account bradley.e.manning@gmail.com, sending an encrypted e-mail to my account, (b)(6)(b)(7)(C) I was not able to read Mr. Manning's e-mail because I was no longer utilizing the public PGP key that he utilized to encrypt the e-mail. I believed he recovered my public PGP encryption key from the key server at pgp.mit.edu (searchable as (b)(6)(b)(7)(C) I responded to Mr. Manning relating that I was no longer utilizing the PGP key he used, and requesting that we initiate communication via AOL Instant Messenger (AIM), at my account, user name, (b)(6)(b)(7)(C) and via Facebook, through my account, user name, (b)(6)(b)(7)(C) which is linked to my account (b)(6)(b)(7)(C) Between 20 May 10 and 21 May 10, Mr. Manning and I subsequently exchanged about eight e-mails, seven of which were encrypted; however, one e-mail was unencrypted, and originated form the account bradley.e.manning@gmail.com, which simply related an affirmative reply of acknowledgment to my aforementioned request for AIM or Facebook communication. Additionally, one e-mail, although encrypted, originated form bradley.manning@2bct10mtn.army.mil.

Subsequently, Mr. Manning utilized AIM (Chat ID (b)(6)(b)(7)(C) to contact me, and he utilized Off the Record (OTR), an automated encryption service, to encrypt all of his AIM communications to me. We subsequently chatted utilizing AIM on or about the following dates: 20 May 10, 21 May 10, 22 May 10, 23 May 10, 24 May 10, 25 May 10, and 26 May 10. During Mr. Manning's chats, he identified himself as the person who contacted me via email and related he worked with the U.S. Army at 2bct 10mtn at FOB Hammer as a 35F intelligence analyst. Additionally, Mr. Manning provided me with his Army Knowledge Online username and password. Mr. Manning subsequently utilized Facebook to send me a Facebook friend request from his account utilizing the account bradley.e.manning@gmail.com. I accepted Mr. Manning's friend request and we associated our Facebook accounts, an association which continues to present day.

During AIM chats Mr. Manning revealed he utilized his ongoing U.S. Army access to classified information to obtain and disclose U.S. Army and other U.S. government classified information to Wikileaks. Mr. Manning also related he had a close and ongoing relationship with Mr. Julian Assange, the organizer of Wikileaks, who had offered him a position with Wikileaks that he had turned down, but nevertheless continued to obtain and disclose classified information to Wikileaks. Additionally, Mr. Manning related he had disclosed the following classified information to Mr. Assange and Wikileaks: "collateral murder video", a classified 2007 video of an U.S. Army Apache helicopter attack in Iraq; the classified U.S. State Department Icelandic

[redacted]e; a classified video of a U.S. Army attack in Afghanistan; and roughly 260,000 classified State Department cables.

[redacted]

Q. [redacted]

A. Mr. [redacted]

Q. You stated you are a reporter, were you acting as a reporter when you spoke with Mr. Manning?

A. I was not acting as a reporter because after I offered him the option of reporting the information as a source or as a penitent to a minister, which I am recognized as in the Universal Life Church; he declined both offers. Additionally, his communication is not the typical communication expected to be revealed to a reporter or a minister.

Q. What type of information was provided to you that allowed you to establish that you were speaking with Mr. Bradley Manning?

A. Mr. Manning provided access to his Facebook account, which revealed a user name of Bradley Manning, his photograph, and detailed information pertaining to his life, including his association to the U.S. Army as a 35F intelligence analyst. Additionally, the e-mail headers revealed during correspondence on one occasion exposed that the e-mail originated from an Army.mil domain and revealed the name Bradley Manning. Mr. Manning also provided me with his AKO user name and password.

Q. Why do you think he contacted you?

A. I am well known within the hacker and Information Disclosure community, as is Mr. Assange, and I recently requested that donations be made to Wikileaks, which lead Mr. Manning to believe that I was Wikileaks friendly.

Q. Why did you expose Mr. Manning's disclosure of classified information?

A. I believe that his actions, disclosing classified information, are national security violations that are analogous to playing "Russian Roulette" with the lives of those serving their country and the lives of Americans abroad. Additionally, I believed if his revelations to me were discovered, I could be penalized in some way for failing to reveal his actions, and I feared for his life.

Q. Where were you when you communicated with Mr. Manning?

A. I was in my parent's home at [redacted] where I use Comcast as an ISP, or at the Starbucks located near my home at Safeway, 4040 Manzinata, Carmichael, CA 95608, where there is free wireless.

Q. Were you alone?

A. Yes, but I did approach my father, Mr. [redacted] when I became aware of Mr. Manning's actions for advice, and he advised that I make contact the appropriate authorities.

Q. Did you tell anyone else?

A. Yes, I also spoke with Mr. [redacted] a former U.S. Army Counterintelligence agent, explaining the entire situation pertaining to Mr. Manning's classified disclosures. In the past, I was involved in an intimate relationship with Mr. [redacted] however, I was not involved with him when I approached him about Mr. Manning's actions. I contacted Mr. [redacted] via telephone. Additionally, I contacted Mr. [redacted] a prior employer.

Q. What is your relationship with Mr. [redacted]

EXHIBIT 47

"Statement of: [redacted] Taken At: LA Quinta Inn Sacramento CA Dated: 13 Jun 2018 Continued:"

[redacted]: He has been an employer. I worked for him in the areas of computer security and adversary characterization, which is determining the capabilities and the identity of information security adversaries. I was not working with or for Mr. [redacted] when Mr. Manning revealed his actions to me.

Q. What did you use to communicate with Mr. Manning?

A. I used my laptop computers, a Lenovo Thinkpad and an HP Mini. I did not use any other computers or devices. Thinkpad user name: [redacted] Password: [redacted] HP mini user name: Administrator, no password.

Q. What accounts did you use to communicate with Mr. Manning?

A. [redacted] org (account hosted at Tucows.com and AIM chat address), Facebook (account: [redacted] org), AIM (account: [redacted] .org), and AIM (account: [redacted] @aol.com), and [redacted] account hosted at 2600 Magazine).

Q. What accounts did Mr. Manning use to communicate with you?

A. bradely.e.manning@gmail.com, bradley.manning@2bct10mtn.army.mil, Facebook (Account shows name as Bradley Manning), and AIM (Chat ID [redacted]

Q. Do you use any other encryption on your computers?

A. Yes, PGP, and my key [redacted] which is potentially the same passphrase I used to encrypt with before reinstalling PGP.

Q. Were you intentionally logging to monitor your computer when you communicated with Mr. Manning?

A. No, chats were set to log from installation of AIM.

Q. Do you use any external data storage?

A. Besides 2600 Magazine, where there is e-mail on a mail server, I do not use any other external data storage devices, to include any remote server locations. I did not store any information or data I received from Mr. Manning in any external or remote storage devices or servers that remain in my possession. I have turned over all the information related to communication with Mr. Manning to the appropriate authorities and I no longer have any such information in my possession, nor will I transmit any potentially classified information disclosed to me by Mr. Manning to any other entities.

Q. Did you wipe your devices and computers? When? How frequently?

A. No, I did not wipe either computer I used to communicate with Mr. Manning.

Q. Who is bradass87?

A. bradass87 is the online identity of the person I know as Mr. Bradley Manning. I do not know of any other monikers or online identities used by Mr. Bradley Manning.

Q. Did Mr. Manning express an interest in harming the U.S.A?

A. Yes, Mr. Manning expressed an interest in harming the U.S.A when he stated he wanted to damage this countries ability to conduct foreign policy abroad.

Q. When was the last time you communicated with Mr. Manning?

A. About 26 May 10, immediately before his apprehension by authorities.

Q. When did the topic of Mr. Assange, come into your communication with Mr. Manning?

A. By at least the third day of chat conversations, Mr. Manning brought up Mr. Assange and Wikileaks. I believe he thought I recognized Mr. Assange's name and would be impressed by [redacted]

INITIALS OF PERSON MAKING STATEMENT: [redacted]

is involvement with both Mr. Assange and Wikileaks, resulting in Mr. Manning being more memorable to me.

Q. What exactly did Mr. Manning relate to you that he sent to Mr. Assange and/or Wikileaks?

A. The "Icelandic cable", roughly 260,000 U.S. State Department cables, and two U.S. Army videos, which he related were all classified.

Q. Did Mr. Manning relate any further information pertaining to the exact U.S. State Department cables he released?

A. No, he did not state the exact cables released, or give any further detail pertaining to the cables, with the exception of the Icelandic cable. Additionally, I am not aware whether Mr. Manning described or gave any further details pertaining to U.S. State Department cables to any one else.

Q. Did Mr. Manning relate that he sent any information pertaining to data sent to Wikileaks to anyone else?

A. No, he did not indicate that he sent the information to anyone else.

Q. Did Mr. Manning indicate that anyone else was involved in obtaining and disclosing classified information?

A. No, but he did indicate that a coworker had successfully intruded into other U.S. Army and U.S. government classified (.smil and .sgov) computers. I am not aware of the identity of this person.

Q. Did Mr. Manning relate any information pertaining to his family or relatives?

A. No

Q. Do you know how Mr. Manning transmitted information to Wikileaks? Where, Domain, URL, IPs?

A. No, Mr. Manning only indicated that it was a blind network where he did not know the identity of the servers. Mr. Manning did indicate he had a special arrangement with Mr. Assange so that Mr. Assange would expedite review of the classified information sent by Mr. Manning. Additionally, Mr. Manning indicated that he utilized a CD convincingly disguised as a Lady GAGA CD to exfiltrate the classified data. Mr. Manning did relate that he asked an NSA representative if the representative was aware of any suspicious traffic being routed across the network and the representative responded that he did notice not any information pertaining to illegitimate traffic.

Q. Have you ever sent any information to Mr. Assange and/or Wikileaks?

A. Yes, I sent an excerpt of a log in which Mr. Manning confesses to leaking classified information to Wikileaks. I used the Wikileaks web interface to send the aforementioned information on or about 7 Jun 10, but it has not been posted on Wikileaks.

Q. What server did the CM videos come from? What Domain? Uploaded February? (Open SSL aes-256, sftp prearranged drop IP, used TOR, wl.org submission system)

A. I do not know.

Q. Do you know Mr. Assange?

A. No, but I am aware of Wikileaks.

Q. What do you know about Assange's offer of work to Mr. Manning? (b)(6)(b)(7)(C)

 EXHIBIT 47

A. Mr. Manning related an offer was made, but he declined; however, I believe that Mr. Manning continued to provide Mr. Assange with information because he characterized his relationship with Wikileaks as ongoing.

Q. Do you know anything about (b)(6)(b)(7)(C) and Mr. Manning's twitter and YouTube account?

A. No, I do not know anything about (b)(6)(b)(7)(C) or Mr. Manning's Twitter or YouTube account.

Q. Do you know anything about Mr. (b)(6)(b)(7)(C)

A. No

Q. What do you know about Ms. (b)(6)(b)(7)(C)

A. No, but Mr. Manning did relate that Ms. (b)(6)(b)(7)(C) was a related to him.

Q. What do you know about the SIGINT (b)(6)(b)(7)(C) analyst mentioned by Mr. Manning?

A. I do not know anything about (b)(6)(b)(7)(C) except for that which was related to me by Mr. Manning in the chats.

Q. Did Mr. Manning give you his private and/or public OTR or PGP key?

A. OTR handshakes are automatic, if he provided his PGP key it would have been imported to my client or it is contained in another PGP message. I do not recall utilizing Mr. Manning's public PGP key to communicate.

Q. What do you know about ccc.de jabber service? (www.jabber.org)?

A. I know of their service and that Mr. Manning related that it was a service frequented by Mr. Assange.

Q. What do you know about Mr. Manning's satellite Internet use?

A. I recall he related that he used a satellite Internet connection from his location at FOB Hammer from his personal laptop.

Q. Were you were offered a job a JTF-CNO?

A. Yes, approximately December 2001.

Q. Who is Mr. (b)(6)(b)(7)(C)

A. PFC Manning related that Mr. (b)(6)(b)(7)(C) was his ex-boyfriend, which I believe means that they were involved in a homosexual relationship.

Q. What did you do with Mr. Manning's AKO username and password?

A. I received and ignored the information. I never used it nor do I intend to ever use it.

Q. Where did Mr. Manning store the classified files he gathered?

A. I believe he stored the classified files on his government system because he related the information could not be found in the event that he was caught, because the drives were reclaimed and zeroed.

Q. Did Mr. Manning use online storage/backup services?

A. He did not relate any information pertaining to his use of online storage or backup.

Q. How did Mr. Manning get the files he gathered?

A. Mr. Manning utilized his preexisting access to classified US Army systems to gather classified information.

Q. What is OTR?

A. Off the Record, an encryption service.

Q. What information did you send to Wired.com or any other news or media outlet? (b)(6)(b)(7)(C)

 EXHIBIT 47

"Statement of: (b)(6)(b)(7)(C) Taken At: Lu Quinta INN Sacramento, CA Dated: 13 Jan 2011 Continued:"

(b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) of Wired.com has full excerpts of all of the Mr. Manning chat logs, which I delivered to him via thumb drive at a meeting in the New Rice Bowl Express restaurant, 7416 Fair Oaks Blvd, Carmichael, CA 95608. Additionally, I delivered excerpts of the Mr. Manning chat logs to Ms. (b)(6)(b)(7)(C) of the Washington Post, via e-mail, utilizing the e-mail account (b)(6)(b)(7)(C) org.

Q. Do you have anything further you wish to add to this statement?

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

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE **EXHIBIT 47**

(b)(6)(b)(7)(C) (b)(6)(b)(7)(C) File Number: (28-10-CID221-10117

Statement of: (b)(6)(b)(7)(C) Taken At: LA QUINTA INN SACRAMENTO CA Dated: 15 Jun 2010 Continued:"

AFFIDAVIT

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

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

WITNESSES:

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

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

902nd MI Group - Monterey Field Office
360 Patton Ave
Presidio of Monterey, CA 93944
ORGANIZATION AND ADDRESS

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 13 day of June, 2010
at La Quinta Inn

(b)(6)(b)(7)(C)
(Signature of Person Administering Oath)

SA (b)(6)(b)(7)(C)
(Typed Name of Person Administering Oath)

ART 136 UCMJ or 5 USC 303
(Authority to Administer Oath)

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

FOR OFFICIAL USE ONLY
LAW ENFORCEMENT SENSITIVE **EXHIBIT** 47

Exhibit(s) 48

Page(s) 000301 thru 000303 withheld.

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

CLASSIFIED

Exhibit(s) 49

Page(s) 000304 referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 50

Page(s) 000305 thru 000305a referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 51

Page(s) 000306 thru 000306a referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1700, 17 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence one DVD containing emails purported to have been exchanged between PFC MANNING and RS221-0005 and a copy of PFC MANNING's Facebook account pages, from the forensic computer, which was documented on EPCD, DN 083-10.///Last Entry///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro Resident Agency, CCIU U.S, Army, Quantico, VA 22134	
(b)(6)(b)(7)(C)	DATE 17 Jun 10	EXHIBIT 52

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

DETAILS

About 1100, 14 Jun 10, SA (b)(6)(b)(7)(C) coordinated with CPT [redacted] who provided the Search and Seizure Authorization for the forensic examination of the all items seized by this office 27-28 May 10, during the course of the investigation; using specific verbiage to clarify the search of all items for information in whatever form it was found i.e. written, electrical, electronic, optical or magnetic. CPT [redacted] also provided the Search and Seizure Authorization for the Unit's share drive network logs assigned to PFC MANNING and the OSJA Directory.

About 1930, 16 Jun 10, SA (b)(6)(b)(7)(C) coordinated with CPT [redacted] who stated 2/10th MTN DIV, FOB Hammer, never had any Joint Worldwide Intelligence Communications System (JWICS) terminals in their SCIF. He related the unit never set up the Trojan Spirit; therefore, they never had JWICS access during the entire deployment. CPT [redacted] stated the unit did have access to the National Security Agency (NSA) network. The NSA terminal was owned by the Cryptological Support Group (CSG) from NSA. CPT [redacted] further related there were a few CSG members attached to the unit; only those CSG and a few Signals Intelligence (SIGINT) Soldiers had user names and passwords. CPT [redacted] stated the NSA net was extremely secure. The area was always manned by at least two people at all times. CPT [redacted] ensured at no point did PFC MANNING ever have access to the NSA net; in fact, no one was authorized to look at those screens except the CSG and SIGINT operators. CPT [redacted] also related the unit did not run an organic Prophet Spiral System either. They used the TPE Prophet Hammer system which was maintained in a different accredited SCIF on FOB Hammer, which PFC MANNING did not have access to. CPT [redacted] stated it was manned by the SIGINT operators assigned to the Military Intelligence Company. They were not actually assigned to HHC, 2/10th MTN DIV, but were attached as operational Control (OPCON) under his section (S2) for the deployment; they were actually assigned to B Company, 2nd Brigade Special Troops Battalion. CPT [redacted] further related PFC MANNING never had access to Top Secret material.

CPT [redacted] identified the Soldiers who operated the TPE Prophet System and the NSA Network:
B/2d BSTB MI Co, All active duty Soldiers-home station Fort Drum, NY:
1LT (b)(6)(b)(7)(C) (platoon leader)
SFC (b)(6)(b)(7)(C) (platoon sergeant)
SSG (b)(6)(b)(7)(C)
SSG (b)(6)(b)(7)(C)
SSG (b)(6)(b)(7)(C)
SSG (b)(6)(b)(7)(C)
SGT (b)(6)(b)(7)(C)
SGT (b)(6)(b)(7)(C)
SPC (b)(6)(b)(7)(C)
SPC (b)(6)(b)(7)(C)
SPC (b)(6)(b)(7)(C)

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGNA (b)(6)(b)(7)(C) [redacted]	DATE 17 Jun 10	EXHIBIT 53

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0160-10-CID899-14463

DETAILS

Cryptological Support Team, NSA; All active duty Soldiers-home station: B Co. 741 MI BN, Fort Meade:
WO1 (b)(6)(b)(7)(C)
SPC (b)(6)(b)(7)(C)

About 1045, 17 Jun 10, SA (b)(6)(b)(7)(C) coordinated with SGT (b)(6)(b)(7)(C) NCOIC, Camp Liberty Post Office, 387th Human Resources Command, Camp Liberty, Iraq APO AE 09342, who related all APO Post Offices are only required to hold all forms for 30 days (minus registered mail); most of the offices keep the forms for years, and others i.e. FOB Hammer Post Office only retained the forms for the required amount of time. SGT (b)(6)(b)(7)(C) related SSG (b)(6)(b)(7)(C) NCOIC, Post Office, FOB Hammer, took over the Post Office in the beginning of May 10, because of problems with the previous unit. SGT (b)(6)(b)(7)(C) related all insured, certified, and delivery confirmation slips would be attached to the customs forms: the originals would be maintained with the package, a copy would be maintained at the post office (for the required 30 days), and a copy goes to the customer. SGT (b)(6)(b)(7)(C) stated once the packages left the mailroom to begin their journal through the postal system to their final destination the bar codes would not be scanned again until they hit a stateside hub; most likely NY. At that time the tracking system would pick up again; however, there would be no way for the local post office to track the package, unless they still had the copies of the forms that included the barcodes.

///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Central Baghdad CID Office, Camp Liberty, Iraq, APO AE 09342	
SIGN (b)(6)(b)(7)(C)	DATE 17 Jun 10	EXHIBIT 53

CID FORM 94
1 FEB 77

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

TO: Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), US Army Criminal Investigations Command (USACIDC), Camp Liberty, APO AE 09342, USA AND/OR any CID Special Agent, AND/OR Forensic Examiner assigned to the USACIDC.

An affidavit having been made before me by Special Agent (b)(6)(b)(7)(C) Central Baghdad CID Office, 11th MP BN (CID), Camp Liberty, APO AE 09342, which affidavit is attached hereto and made part of this authorization, and as I am satisfied that there is probable cause to believe the matters mentioned in the affidavit are true and correct, that the offenses of:

UCMJ Art 106a: Espionage
18 USC § 793: Gathering, Transmitting, or Losing Defense Information
18 USC § 798: Disclosure of Classified Information
18 USC § 1030: Fraud and related activity in connection with computers

set forth therein has been committed, and the property described as:

From the S2 Section, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Seagate Hard Drive, model number ST980825A, serial number 3MH036M1; extracted from Alienware laptop computer, serial number: NKD900TA6D00661 "Secret"
b. Unknown make and model Hard Drive, serial number 5MH0HWKN; extracted from Dell laptop computer, serial number HLVJQF1 "Secret"
c. Unknown make and model Hard Drive, serial number 5MH0TB78; extracted from Dell laptop computer, serial number 93H4QD1 "Unclassified"

From the Supply Office, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Seagate Hard Drive, serial number CN-0MN922-21232-793-002L "Secret"
b. Hitachi Hard Drive, serial number 070817DP0C10DSG2J1DP "Unclassified"

From the Paralegal Office, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. Toshiba Hard Drive, serial number Z5FX1422S 6P2 EC A "Secret"

From the digital Network Logs maintained by the S6 Section, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. (2) Imation CDs, serial numbers LD621 MK06232788 A20 and LD621 MK06232576 B10

From Room 4C93, designated living area of PFC Manning, LSA Dragon, FOB Hammer, Iraq:

a. Apple laptop computer, serial number W8939AZ066E
b. (2) Samsung CDs, serial numbers 1308120503204625 and 1308120503204624
c. Samsung Cellular Telephone, serial number RPRS303202D containing SIM card, serial number 525033 8901260520008043773
d. (8) Memorex DVD-RW, serial numbers 2009052100920487, 2009052100920485, 2009052100920483, 2009052100920481, 2009052100920471, 1909052107834102, 1909052107834101, and 2009052104924365

e. Seagate hard drive, serial number 9VS1S2TZ; extracted from Seagate External Hard Drive serial number 2GEWJKLJ

f. Imation CD, serial number LD623 MJ04184038 B16 "Secret"

g. Kodak Camera, serial number KCXKS9 containing Scandisk Memory Card, serial number BE0828613591D

From SSG (b)(6)(b)(7)(C) Supply NCOIC, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq:

a. SAMSUNG Hard Drive, serial number S1AKJDNQ816517; extracted from HP laptop computer, serial number CNF8492K3S

Was previously seized under proper legal authority (see Commander's Search and Seizure Authorization, dated 27 and 28 May 10, authorized by CPT (b)(6)(b)(7)(C) Commander, Headquarters and Headquarters Company, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq, APO AE 09308; and Search and Seizure Authorization, 27 May 10, authorized by CPT (b)(6)(b)(7)(C) Military Magistrate, USF-I, Camp Liberty, Iraq, APO AE 09342), which is presently located within the Evidence Depository, 11th MP BN (CID), USACIDC, Camp Arifjan, Kuwait, APO AE 09366.

The persons described above are authorized to search the listed items for all information, in whatever form it may be found, to include written, electrical, electronic, optical or magnetic, which relates to the cited offenses.

Dated this 14th Day of June, 2010.

NAME AND GRADE OF AUTHORIZING OFFICIAL:	DUTY POSITION OF AUTHORIZING OFFICIAL:
CPT (b)(6)(b)(7)(C)	Military Magistrate
ORGANIZATION OF AUTHORIZING OFFICIAL:	SIGNATURE OF AUTHORIZING
Office of the Staff Judge Advocate, USD-C, Camp Liberty, Iraq APO AE 09342	(b)(6)(b)(7)(C) [redacted]

DA FORM 3745-E, Mar 85 (gen)

SEARCH AND SEIZURE AUTHORIZATION

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

TO: *(Name and Organization of the person to whom authorization is given)*
Special Agent (b)(6)(b)(7)(C) AND/OR any CID Special Agent authorized Special Agent and/or Forensic Examiner assigned to the US Army Criminal Investigation Command (USACIDC)

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

Central Bagdad CID Office, 11th MP BN (CID), USACIDC, Camp Liberty APO AE 09342
(Organization or Address of Affiant)

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

FOB HAMMER system administrator area

for the property described as preserved shared directories assigned to PFC Bradley E. Manning and to the OSJA and to subsequently search the directories for information related to the offenses of Article 106a, Espionage; 18 USC 703, Gathering or transmitting defense information; 18 USC 798, Disclosure of classified information; and 18 USC 1030 Fraudulent activity related to computers.

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

the Evidence Custodian, CCIU, 9805 Lowen Road, Fort Belvoir, VA 22060
(Name and Organization of Authorized Custodian)

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

Dated this 14 day of June, 2010.

TYPED NAME AND GRADE OF AUTHORIZING OFFICIAL	DUTY POSITION OF AUTHORIZING OFFICIAL
CPT (b)(6)(b)(7)(C)	Military Magistrate
ORGANIZATION OF AUTHORIZING OFFICIAL Office of the Staff Judge Advocate USD-C Camp Liberty APO AE 09342	SIGNATURE OF AUTHORIZING OFFICIAL (b)(6)(b)(7)(C) [redacted]

DA FORM 3745, SEP 2002 DA FORM 3745-R, MAR 80, IS OBSOLETE APD PE v1.02ES

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

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

BEFORE COMPLETING THIS FORM, SEE INSTRUCTIONS ON PAGE 2

1. I, Special Agen (b)(6)(b)(7)(C) (*Name*), 11th Military Police Battalion (CID), Central (*Organization or Address*)

Bagdad CID Office, Camp Liberty APO AE 09342

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

I hereby incorporate the information in the sworn Affidavits related to PFC Bradley E. Manning, 2nd Brigate Combat Team, 10th Mountain Division, FOB HAMMER, Iraq, provided to CPT (b)(6)(b)(7)(C) Military Magistrate, Office of the Staff Judge Advocate Office, Bagdad, Iraq at 1400 hours on 27 May 2010, 1550 hours on 28 May 2010 and 1300 hours on 5 Jun 2010.

I have been informed by SA (b)(6)(b)(7)(C) Special Agent in Charge (SAC), CCIU-Europe that SA (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) forensic examination of PFC Manning's two assigned SIPRNet computers and his personal Apple computer disclosed that Manning created "links of interest" using his primary SIPRNet computer to a file called "dump2.csv.zip" which was stored in Manning's shared directory on the FOB HAMMER SIPRNet LAN ("tdrive"). He also viewed the "dump2.csv.zip" file using his secondary SIPRNet computer and the "dump2.csv.zip" file was found on his personal Apple computer. The contents of the "dump2.csv.zip" file have not been found on any of these three computers but may still be available in Manning's shared directory, which was preserved by CPT (b)(6)(b)(7)(C) the system administrator for the FOB HAMMER SIPRNet LAN at CCIU's request. SA (b)(6)(b)(7)(C) is the SAC, Digital Forensics and Research Branch, CCIU.

2. The affiant further states that:

The forensic examinations also disclosed that PFC Manning viewed numerous files on the OSJA shared drive on the FOB HAMMER SIPRNet LAN, including information related to Article 15 actions taken against other soldiers. The OSJA shared drive was also preserved by CPT (b)(6)(b)(7)(C) after notice was provided to the SJA. Examination of these files will help define the extent of PFC Manning's unauthorized access.

I therefore request authority to seize and subsequently search the shared directories assigned to PFC Manning and the OSJA for information related to the offenses set out in my Affidavit of 5 Jun 10: Article 106a, Espionage; 18 USC 703, Gathering, transmitting or losing defense information; 18 USC 798, Disclosure of classified information; and 18 USC 1030, Fraud and related activity in connection with computers.

3. In view of the foregoing, the affiant requests that an authorization be issued for a search of FOB HAMMER system
(the person) (and)

administrator area for FOB shared directories assigned to PFC Manning and the OSJA which have been preserved
(the quarters or billets) (and)

(the automobile) ( ) and (seizure) (apprehension) of to subsequently search for information
(items/persons searched for)

related to the offenses listed in the referenced Affidavits as incorporated herein

TYPED NAME AND ORGANIZATION OF AFFIANT
SA (b)(6)(b)(7)(C) Central Bagdad CID Office, 11th MP BN (CID)
Camp Liberty APO AE 09342

(b)(6)(b)(7)(C) [redacted]

SWORN TO AND SUBSCRIBED BEFORE ME THIS 14 DAY OF June 2010 AT 1100

TYPED NAME, ORGANIZATION AND OFFICIAL CAPACITY OF AUTHORITY ADMINISTERING THE OATH
CPT (b)(6)(b)(7)(C)
Military Magistrate, USD-C
Camp Liberty APO AE 09342

SIGNATURE OF AUTHORITY ADMINISTERING THE OATH
(b)(6)(b)(7)(C) [redacted]

INSTRUCTIONS FOR

AFFIDAVIT SUPPORTING REQUEST FOR AUTHORIZATION TO SEARCH AND SEIZE OR APPREHEND

1. In paragraph 1, set forth a concise, factual statement of the offense that has been committed or the probable cause to believe that it has been committed. Use additional page if necessary.

2. In paragraph 2, set forth facts establishing probable cause for believing that the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended are connected with the offense mentioned in paragraph 1, plus facts establishing probable cause to believe that the property to be seized or the person(s) to be apprehended are presently located on the person, premises, or place to be searched. Before a person may conclude that probable cause to search exists, he or she must first have a reasonable belief that the person, property or evidence sought is located in the place or on the person to be searched. The facts stated in paragraphs 1 and 2 must be based on either the personal knowledge of the person signing the affidavit or on hearsay information which he/she has plus the underlying circumstances from which he/she has concluded that the hearsay information is trustworthy. If the information is based on personal knowledge, the affidavit should so indicate. If the information is based on hearsay information, paragraph 2 must set forth some of the underlying circumstances from which the person signing the affidavit has concluded that the informant (whose identity need not be disclosed) or his/her information was trustworthy. Use additional pages if necessary.

3. In paragraph 3, the person, premises, or place to be searched and the property to be seized or the person(s) to be apprehended should be described with particularity and in detail. Authorization for a search may issue with respect to a search for fruits or products of an offense, the instrumentality or means of committing the offense, contraband or other property the possession of which is an offense, the person who committed the offense, and under certain circumstances for evidentiary matters.

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1227, 17 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, coordinated with Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Office of the Director for National Intelligence (ODNI), Washington, DC 20511, who stated PFC MANNING held two accounts with INTELINK, one account for unclassified information and one for secret information. Mr. (b)(6)(b)(7)(C) stated PFC MANNING logged in a few times to his unclassified account but then never renewed his password and the account became inactive. Mr. (b)(6)(b)(7)(C) stated a user does not have to log into the unclassified INTELINK to read posted information. Mr. (b)(6)(b)(7)(C) stated PFC MANNING may have accessed the unclassified INTELINK site to read posted information but never posted any information to that site. Mr. (b)(6)(b)(7)(C) related that anyone can read information that has already been posted but only users logged into INTELINK can post information. Mr. (b)(6)(b)(7)(C) related the secret INTELINK drive crashed and to date no logs have been recovered.

About 1700, 17 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, collected as evidence one Digital Versatile Disc (DVD), which contained emails allegedly from PFC MANNING to Mr. (b)(6)(b)(7)(C) and a copy of PFC MANNING's Facebook Friend accessible pages, from the forensic computer, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 083-10.

About 1728, 18 Jun 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, SA (b)(6)(b)(7)(C) Diplomatic Security Service (DSS), U.S. Department of State (DoS), Boston, MA 02222, and SA (b)(6)(b)(7)(C) 902 Military Intelligence (MI) Group, U.S. Army Intelligence and Security Command, Fort Devens, MA 01434, interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) who related he first met PFC MANNING around Jan 10, during a visit to the Techniques Office at the Massachusetts Institute of Technology (MIT), in which he believed PFC MANNING was on leave from the U.S. Army. Mr. (b)(6)(b)(7)(C) related he spoke with PFC MANNING for approximately 40 minutes, during which time PFC MANNING divulged he was an intelligence officer and discussed the history of American Intelligence. Additionally, Mr. (b)(6)(b)(7)(C) related he discussed security containers and physical security with PFC MANNING and subsequently received an email from emax@csail.mit.edu, NFI, pertaining to the security of storage facilities in which himself and PFC MANNING were Carbon Copied (CC), and in which he elaborated on the use of a "Robo Dialer". Mr. (b)(6)(b)(7)(C) related he did subsequently exchange email with PFC MANNING, but he refused to comment to agents on the content of some of the email; however, Mr. (b)(6)(b)(7)(C) related he would discuss the email that he believed to be relevant to this investigation, and he would subsequently forward relevant email to SA (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related some time after speaking with PFC MANNING he traveled to the Dominican Republic where he became aware of PFC MANNING's apprehension by U.S. Army authorities through an email received from the news web sites "slashdot.org" and the "Washington Post", which revealed PFC MANNING released documents obtained from the "Iraq Database" that included "airstrike videos" and State Department documents. Mr. (b)(6)(b)(7)(C) related he conducted research and found the "Wired.com" articles pertaining to Mr. (b)(6)(b)(7)(C) disclosure of his chats logs with PFC MANNING. Mr.

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	
(b)(6)(b)(7)(C)	DATE 19 Jun 10	EXHIBIT 56

DETAILS

(b)(6)(b)(7)(C) related he would not comment about any of his acquaintances or anyone associated with PFC MANNING. Mr. (b)(6)(b)(7)(C) related he would not comment on whether he knew Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related he knew of Mr. Julian P. ASSANGE, founder and Director of WikiLeaks, Townsville, Queensland, AU, but was not personally acquainted with Mr. ASSANGE, however, when in Amsterdam, Mr. (b)(6)(b)(7)(C) stays at the townhouse of Mr. (b)(6)(b)(7)(C) NFI (known associate of Mr. ASSANGE). Mr. (b)(6)(b)(7)(C) related he hoped Mr. (b)(6)(b)(7)(C) would distance himself from Mr. ASSANGE and WikiLeaks, which he indicated had better security then the American Intelligences apparatus, because of the attention drawn to WikiLeaks after the revelation of PFC MANNING's disclosure of 260,000 State Department documents, which he characterized as an irresponsible action on the part of PFC MANNING. SA (b)(6)(b)(7)(C) informed Mr. (b)(6)(b)(7)(C) that PFC MANNING did release classified information and if any of the information released by PFC MANNING is in his possession he should not store, transfer, or discuss the information with anyone, and should immediately turn over the information to SA (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related PFC MANNING did not reveal anything classified to him, but he would provide SA (b)(6)(b)(7)(C) with any information he deemed to be relevant to the investigation.

About 1730, 18 Jun 2010, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both assigned to CCIU, WMRA, Fort Belvoir, VA 22060, and SA (b)(6)(b)(7)(C) DSS, DoS, Dallas, TX 75242, interviewed Mrs. (b)(6)(b)(7)(C) of PFC MANNING. Mrs. (b)(6)(b)(7)(C) related she is aware of (b)(6)(b)(7)(C) current situation and had read articles on "wired.com" and other internet media sites, and the information she knew came only from these sources. Mrs. (b)(6)(b)(7)(C) related she has not spoken with PFC MANNING since sometime in Oct 09; and hasn't seen him since Apr or May 07, in Potomac, MD. Mrs. (b)(6)(b)(7)(C) related she was only able to keep up with PFC MANNING through the social website, "Facebook", where she was a friend of his. Mrs. (b)(6)(b)(7)(C) related she and (b)(6)(b)(7)(C) were not very close after PFC MANNING told her she would not be a very good mother. Mrs. (b)(6)(b)(7)(C) took great offense to his comments and distanced herself from him. Mrs. (b)(6)(b)(7)(C) related PFC MANNING was extremely intelligent, especially with computers, knew C++ around the age of 7, and was very good at manipulating the software in computer games. Mrs. (b)(6)(b)(7)(C) related PFC MANNING was always very good academically, but was kind of awkward socially. Mrs. (b)(6)(b)(7)(C) related her parents got divorced sometime in 1999, and this had a big effect on (b)(6)(b)(7)(C) Mrs. (b)(6)(b)(7)(C) related PFC MANNING went to live with his mother in the United Kingdom, and lived there until he finished high school. Mrs. (b)(6)(b)(7)(C) related PFC MANNING returned to Oklahoma after high school, and lived with his father for a short time. Mrs. (b)(6)(b)(7)(C) related PFC MANNING always seemed to be a patriot, and she was very surprised at the allegations against him. Mrs. (b)(6)(b)(7)(C) stated "I believe he may have been indoctrinated in England, just looking at the United States the way the English do." Mrs. (b)(6)(b)(7)(C) related PFC MANNING had friends in the UK but does not know any of their names. Mrs. (b)(6)(b)(7)(C) related she had not received any items or mail from PFC MANNING.

About 1810, 18 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both assigned to WMRA, CCIU, Fort Belvoir, VA 22060; SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) both assigned to

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 19 Jun 10	EXHIBIT 56

DETAILS

DSS, DoS, Arlington, VA 22209; and SA (b)(6)(b)(7)(C) National Capital Regional Military Intelligence Detachment (NCR MID), 902nd MI Group, Fort Belvoir, VA 22060, interviewed Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) PFC MANNING and the person who PFC MANNING lived with prior to joining the U.S. Army in Oct 07. Ms. (b)(6)(b)(7)(C) stated the last time she saw PFC MANNING was in Jan 10, when PFC MANNING returned from Iraq while on his mid-tour leave. Ms. (b)(6)(b)(7)(C) explained PFC MANNING stayed a few days at her residence in (b)(6)(b)(7)(C) and then told her he was going to Boston, MA. Ms. (b)(6)(b)(7)(C) related PFC MANNING returned from Boston and stayed a few more days before returning to Iraq. Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) related PFC MANNING called her from Iraq several weeks prior to his apprehension by the U.S. Army Criminal Investigation Command (USACIDC) and asked her if she had seen the Apache helicopter video and asked her to search for it. Ms. (b)(6)(b)(7)(C) stated PFC MANNING told her it would be big news. Ms. (b)(6)(b)(7)(C) said she did not know PFC MANNING had anything to do with the release of the video until she read about his apprehension in the news media. Ms. (b)(6)(b)(7)(C) stated after PFC MANNING was apprehended by CID, PFC MANNING contacted her by telephone on or about 5 Jun 10, and asked her to post a message to his Facebook account. Ms. (b)(6)(b)(7)(C) stated PFC MANNING has called her about four times since being in confinement as well as she had also received a phone call from PFC MANNING's attorney, advising her PFC MANNING was okay. Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) said she bought PFC MANNING an iPod as a Christmas gift two years ago but indicated she had not seen it while PFC MANNING was living in her home and did not believe it was currently at her residence. Ms. (b)(6)(b)(7)(C) stated PFC MANNING purchased a computer in Feb 10, while he was home on leave from Iraq. Ms. (b)(6)(b)(7)(C) showed SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) the computer, which was an IBM Desktop Computer that had been placed under a desk in the bedroom she shares with her (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) noted the computer was connected to the home internet service within Ms. (b)(6)(b)(7)(C) home and was connected to a power source; however, the computer was not powered on. Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) related although she could physically access this computer, neither she nor anyone else in her household had electronic access to log into, and/or to access the computer to know what was on the machine and/or what its purpose was. Ms. (b)(6)(b)(7)(C) related she received a box from PFC MANNING, which she recalled had been marked 'U.S. Priority Mail' approximately six-weeks ago. Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) said the box contained two soft-cover computer books, two Maryland T-shirts, and one FOB Hammer Iraq T-shirt. Ms. (b)(6)(b)(7)(C) said there was no note or explanation as to why PFC MANNING sent the items, and she explained she had previously sent the Maryland T-shirts to PFC MANNING for Christmas a few months prior upon PFC MANNING's request. Ms. (b)(6)(b)(7)(C) related she took the items sent by PFC MANNING from Iraq out of the box they came in and placed these items with PFC MANNING's other belongings. Ms. (b)(6)(b)(7)(C) further explained the original box these items had been sent in had since been thrown away and she had not found any items of digital media within this box. Ms. (b)(6)(b)(7)(C) when asked about whom PFC MANNING may have sent additional packages to from Iraq, related it would have likely been Mr. (b)(6)(b)(7)(C) or Mr. (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) stated during the time PFC MANNING lived at her home she only met one friend of PFC MANNING's approximately two years ago, Mr. (b)(6)(b)(7)(C) who reportedly lived in Boston, MA. Ms. (b)(6)(b)(7)(C)

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
S (b)(6)(b)(7)(C)	DATE: 19 Jun 10 / EXHIBIT: 56

DETAILS

(b)(6)(b)(7)(C) related she was contacted by Mr. (b)(6)(b)(7)(C) via Facebook about 1 Jun 10, asking if PFC MANNING was okay as PFC MANNING had stopped posting messages on his Facebook page. Ms. (b)(6)(b)(7)(C) stated she replied to Mr. (b)(6)(b)(7)(C) that PFC MANNING was okay as far as she knew, as she had not heard anything to the contrary. Ms. (b)(6)(b)(7)(C) explained she had contacted PFC MANNING over the years using several email addresses, to include: (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) further identified the email addresses she knew PFC MANNING had used as: (b)(6)(b)(7)(C)

About 1700, 18 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Arizona Branch Office, CCIU, Fort Huachuca, AZ 85613, SA (b)(6)(b)(7)(C) 902d MI, Fort Sill, OK, and SA (b)(6)(b)(7)(C) DSS, DoS, Dallas, TX, interviewed Mr. (b)(6)(b)(7)(C) PFC MANNING. Mr. (b)(6)(b)(7)(C) related he had not been in contact with (b)(6)(b)(7)(C) since he left for Iraq. Mr. (b)(6)(b)(7)(C) related he sent PFC MANNING a DVD player for Christmas while deployed and the gift was not even acknowledged. Mr. (b)(6)(b)(7)(C) related PFC MANNING resided in England with his ex-wife until the age of 18 when he returned to the U.S. Mr. (b)(6)(b)(7)(C) related after returning to the U.S., PFC MANNING got a job doing web design for a company called Zoto.com. Mr. (b)(6)(b)(7)(C) related his son did well at the job for a while but then had issues at work which he did not expound upon which resulted in PFC MANNING being fired. Mr. (b)(6)(b)(7)(C) related he helped (b)(6)(b)(7)(C) move to Tulsa, OK, where PFC MANNING was employed at Credible Pizza until he also lost that job. Mr. (b)(6)(b)(7)(C) indicated that during his time in Tulsa that PFC MANNING had become close to members of an unidentified music band. PFC MANNING apparently provided mixing of musical tracks for the band and followed them to Chicago, IL at an undisclosed time. Mr. (b)(6)(b)(7)(C) related he had not heard from (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) until he turned up in Maryland at his Aunts residence. Mr. (b)(6)(b)(7)(C) related he had spoken with his son about military service and was pleased when PFC MANNING decided to join the Army. Mr. (b)(6)(b)(7)(C) related he traveled to Fort Huachuca, AZ, for PFC MANNING's Advanced Individual Training (AIT) graduation and felt that based upon his attitude and outward expression PFC MANNING had changed his life around for the better. Mr. (b)(6)(b)(7)(C) related he had no mail box in front of his house and he had all of his mail forwarded to a P.O. Box. Mr. (b)(6)(b)(7)(C) related the P.O. Box was in his current wife's control and he did not even have a key to the box. Mr. (b)(6)(b)(7)(C) related they had received no packages or other correspondence from PFC MANNING and he did not think PFC MANNING was even aware of the P.O. Box address. Mr. (b)(6)(b)(7)(C) related he had no contact with PFC MANNING via the internet e-mail or chat session.

About 1925, 18 Jun 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) related he generally tried to avoid PFC MANNING during the time PFC MANNING lived in his home due to PFC MANNING's personality, which Mr. (b)(6)(b)(7)(C) described as irritating. Mr. (b)(6)(b)(7)(C) related the computer identified as belonging to PFC MANNING was located in his bedroom under a desk and had been powered on for quite a long period of time while PFC MANNING was in Iraq. Mr. (b)(6)(b)(7)(C) said although he had physical access to the computer due to

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
SI (b)(6)(b)(7)(C)	DATE: 19 Jun 10 / EXHIBIT: 56

DETAILS

its location, he did not know what information was on this computer nor did he have the ability to log into the computer. Mr. (b)(6)(b)(7)(C) stated although the computer had been powered on for a period of time he could not specifically identify a reason the computer was powered off at the time of this interview, but thought it may have been due to a power outage and that no one had powered the computer back on.

Between 1937 and 1945, 18 Jun 10, SA (b)(6)(b)(7)(C) collected: one IBM Brand, ThinkCentre 36U Model Computer, Serial Number (SN): KCZK85T; one Book, titled "Free Software Free Society: Select Essays of Richard M. Stallman", ISBN: 1-882114-98-1, which further contains the hand written note "Brad – Fight for freedom any way you can! – (b)(6)(b)(7)(C)"; and one Postcard, bearing the hand written note "Hi Brad! Just a quick post card to test the mail – (b)(6)(b)(7)(C) Sent Sat Nov 7th 2009", from Ms. (b)(6)(b)(7)(C) which was documented on an EPCD, DN 086-10.

Between 2258, 18 Jun 10, and 1233, 19 Jun 10, SA (b)(6)(b)(7)(C) obtained a forensic image of the Western Digital,WD1600SB, 160GB hard disk drive, SN: WCANMK655403, which was extracted from the IBM ThinkCentre Computer, SN: KCZK85T, the property of PFC MANNING.

Method of imaging: EnCase Version 6.15.0.82
Type of Image: EnCase
Make and model of write block: WiebeTech Forensic UltraDock V4, SN: 31305-2409-0091

The image was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the hash values with no errors.

Acquisition Hash:
MD5 - 88A70ABC780E54BADCE51EBAB47EBBBB
SHA1 - 122880094C37389CD3CA5ED5DD3144CA089C4E24

Verification Hash:
MD5 - 88A70ABC780E54BADCE51EBAB47EBBBB
SHA1 - 122880094C37389CD3CA5ED5DD3144CA089C4E24

About 1050, 19 Jun 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) and Mrs. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) stated he knew PFC MANNING, but was unaware of any investigation pertaining to him. Mrs. (b)(6)(b)(7)(C) related her son, Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) was a childhood friend of PFC MANNING, and PFC MANNING would spend a lot of time at their residence. Mrs. (b)(6)(b)(7)(C) related PFC MANNING and Mr. (b)(6)(b)(7)(C) were very intelligent boys that were very good with computers and programming. Mrs. (b)(6)(b)(7)(C) related PFC MANNING and Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) were very good friends with Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Mrs. (b)(6)(b)(7)(C) related she believed Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) have been

DETAILS

in contact over Facebook, but did not think PFC MANNING had been back to Oklahoma in several years. Mrs. (b)(6)(b)(7)(C) described PFC MANNING as a "Lost Soul", and very impulsive. The (b)(6)(b)(7)(C) related they had not received any packages or mail from PFC MANNING.

About 1324, 19 Jun 10, SA (b)(6)(b)(7)(C) collected one DVD, containing the forensic image files of the Western Digital,WD1600SB, 160GB hard disk drive, SN: WCANMK655403, which was extracted from the IBM ThinkCentre Computer, SN: KCZK85T, the property of PFC MANNING, from the forensic computer, which was document on an EPCD, DN 087-10.

//LAST ENTRY//

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
SIGN (b)(6)(b)(7)(C) [redacted]	DATE: 19 Jun 10 / EXHIBIT: 56

CLASSIFIED

Exhibit(s) 57

Page(s) 000321 thru 000321b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 58

Page(s) 000322 thru 000322b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 59

Page(s) 000323 thru 000323g referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0172-10-CID452

DETAILS

BASIS FOR INVESTIGATION: About 1600, 17 Jun 10, this office received a Category 1 Request for Assistance (RFA) from the Washington Metro Resident Agency, Computer Crimes Investigative Unit (CCIU), Fort Belvoir, VA, requesting canvass interviews of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), Fort Drum, NY 13602 (FDNY), rear-detachment personnel who had contact with PFC Bradley E. MANNING, (b)(6)(b)(7)(C) HHC, 2nd BCT, Forward, prior to his deployment. Additionally, CCIU requested this office determine if PFC MANNING had a Joint Worldwide Intelligence Computer System (JWICS) account at FDNY, coordinate with the Directorate of Information Management (DOIM) to preserve any local e-mail accounts, and obtain a printout of the "To/From" e-mail addresses, and obtain a copy of PFC MANNING's local personnel file.

About 1700, 17 Jun 10, SA (b)(6)(b)(7)(C) coordinated with SSG (b)(6)(b)(7)(C), Rear-Detachment S-2 NCOIC, HHC, 2nd BCT, FDNY, who stated he was not aware of any personnel assigned to HHC having a JWICS account while stationed at FDNY. Additionally, SSG (b)(6)(b)(7)(C) provided a copy of PFC MANNING's personnel file maintained at the brigade S-1, which contained a DA Form 31, DD Form 4/1 and 4/2, SGLI, DD Form 93, and orders assigning him to FDNY. SSG (b)(6)(b)(7)(C) stated PFC MANNING was a strange guy, but did not have any additional information about him.

About 0830, 18 Jun 10, SA (b)(6)(b)(7)(C) coordinated with Mrs. (b)(6)(b)(7)(C) Exchange Administrator, Net Communication Enterprise (NEC), FDNY, who verified PFC MANNING had an inactive Microsoft Outlook account at FDNY. Mrs. (b)(6)(b)(7)(C) reviewed the "To/From" e-mail addresses and stated the majority of them are the post wide e-mails or the System Administrator ones. She identified several e-mail addresses she was not familiar with.

About 0900, 21 Jun 10, SA (b)(6)(b)(7)(C) received the e-mail address list pertaining PFC MANNING's Fort Drum Outlook account, (b)(6)(b)(7)(C) There was one e-mail address identified in the "Sent" folder and 23 addresses identified in the "In" box.

About 1030, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) this office, interviewed SSG (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) S-2, HCC, 2nd BCT, FDNY, who stated he was deployed with PFC MANNING; however, he re-deployed prior to the incident. SSG (b)(6)(b)(7)(C) stated PFC MANNING was a basic analyst who focused on Shia threat groups while deployed. PFC MANNING was a self proclaimed computer guru whose interests were primarily in computer code and programming. SSG (b)(6)(b)(7)(C) did not have much interaction with PFC MANNING as they worked different shifts. Further, SSG (b)(6)(b)(7)(C) stated PFC MANNING was mentally unstable, and would pull a "Jekel and Hyde" act if someone said the wrong thing to him. SSG (b)(6)(b)(7)(C) was aware of two occasions when PFC MANNING had done this: the first was when he was being counseled he flipped over a table and tried to fight a NCO; the second was when he was trying to talk with a female Soldier, and when she told him to leave her alone, he struck her several times. PFC MANNING was being treated for

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	62nd MP Det (CID), Fort Drum, NY	
SIGN (b)(6)(b)(7)(C)	DATE 21 Jun 10	EXHIBIT 60

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0172-10-CID452

DETAILS

anger management issues. SSG (b)(6)(b)(7)(C) was unaware of any friends or associations of PFC MANNING and stated he was a loner.

About 1058, 21 Jun 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) coordinated with Ms. (b)(6)(b)(7)(C) Special Compartmentalized Information (SCI) Program Manager, G-2, 10th Mountain Division, FDNY, who stated PFC MANNING was never issued a JWICS account at FDNY.///LAST ENTRY///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	62nd MP Det (CID), Fort Drum, NY	
SIG (b)(6)(b)(7)(C)	DATE 21 Jun 10	EXHIBIT 60

CID FOR OFFICIAL USE ONLY/ LAW ENFORCEMENT SENSITIVE

1 FEB 77

FO[illegible]ICIAL USE ONLY/LAW ENFORCEME[illegible]SITIVE

0028-10-CID221-10117

Case Number 0172-10-CID452
Agent/Investigator: SA (b)(6)(b)(7)(C)
Time/Date: 1034/21 June 2010

CANVASS INTERVIEW WORKSHEET

NAME/GRADE SSG/E-4 (b)(6)(b)(7)(C)	SSN (b)(6)(b)(7)(C)	NOTES:
UNIT/ADDRESS HHC, 2nd BCT	WK PH: HM PH: (b)(6)(b)(7)(C)	
NAME/GRADE 2Lt (b)(6)(b)(7)(C)	SSN (b)(6)(b)(7)(C)	NOTES: S-2 shop arrived 22 Mar 10
UNIT/ADDRESS HHC, 2 BCT	WK PH: 314-774-2041 HM PH: (b)(6)(b)(7)(C)	
NAME/GRADE	SSN	NOTES:
UNIT/ADDRESS	WK PH: HM PH:	
NAME/GRADE	SSN	NOTES:
UNIT/ADDRESS	WK PH: HM PH:	
NAME/GRADE	SSN	NOTES:
UNIT/ADDRESS	WK PH: HM PH:	
NAME/GRADE	SSN	NOTES:
UNIT/ADDRESS	WK PH: HM PH:	
NAME/GRADE	SSN	NOTES:
UNIT/ADDRESS	WK PH: HM PH:	
NAME/GRADE	SSN	NOTES:
UNIT/ADDRESS	WK PH: HM PH:	

EXHIBIT 61

CLASSIFIED

Exhibit(s) 62

Page(s) 000327 thru 000327c referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 63

Page(s) 000328 thru 000328b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 64

Page(s) 000329 thru 000329b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 65

Page(s) 000330 thru 00330d referred to:

Defense Intelligence Agency
ATTN: DAN-1A (FOIA)
200 MacDill Blvd
Washington, DC 20340-5100

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

DETAILS

Examination and Contents:

On 14 June 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Digital Forensics and Research Branch, CCIU, conducted a preliminary examination of a Samsung SGH-T229 cellular phone, recorded on DA Form 4137, Document Number (DN) 067-10. All times shown in this report are in relation to UTC/GMT unless otherwise noted.

SA (b)(6)(b)(7)(C) used a Cellebrite Universal Forensic Extraction Device (UFED) to obtain text messages from the SIM card. SA (b)(6)(b)(7)(C) attempted to power the cellular phone with the battery provided and with the UFED, both with no success.

Cell Phone:	Samsung SGH-T229
Serial number:	RPRS303202D
SIM	8901260520008043773

The text messages from the SIM card are provided below.

#	Number	Name	Date & Time	Status	Index	Type	Text
1	(b)(6)(b)(7)(C)	N/A	10/11/09 04:36:06 (GMT-4)	Read	1	Incoming	(b)(6)(b)(7)(C)
2		N/A	05/14/09 17:40:54 (GMT-4)	Read	9	Incoming	(b)(6)(b)(7)(C)
3		N/A	05/14/09 17:42:39 (GMT-4)	Read	10	Incoming	(b)(6)(b)(7)(C)
4		N/A	10/09/09 17:38:53 (GMT-4)	Read	18	Incoming	(b)(6)(b)(7)(C)
5		N/A	05/16/09 17:13:51 (GMT-4)	Read	19	Incoming	(b)(6)(b)(7)(C)
6		N/A	10/09/09 19:14:48 (GMT-4)	Read	22	Incoming	(b)(6)(b)(7)(C)
7		N/A	10/09/09 21:29:11 (GMT-4)	Read	25	Incoming	(b)(6)(b)(7)(C)

SA (b)(6)(b)(7)(C) imported the files created by the UFED into EnCase version 6.16 and created a Logical Evidence File (LEF). The LEF was written to Compact Disc – Recordable (CD-R). About 1500, 14 June 2010, SA (b)(6)(b)(7)(C) collected the CD-R as evidence, which was documented on a DA Form 4137, DN 075-10.

Leads:

None.

//LAST ENTRY//

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 14 June 2010	EXHIBIT 66

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

[redacted]NUMBER CAF# 0028-10-CID361
ROI# 0028-10-CID221-10117

DETAILS

Between 14-16 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Digital Forensics and Research Branch, CCIU, conducted a preliminary forensic examination of a Kodak EasyShare M380 digital camera and Sandisk memory card, taken as evidence on DA Form 4137, Evidence Property Custody Document (EPCD), Document Number (DN) 067-10, Item 7, and reported to belong to PFC MANNING.

FINDINGS:

Kodak EasyShare M380 Camera:

Examination of the camera's internal memory revealed it did not appear to contain any data pertinent to this investigation.

Sandisk Memory Card:

A 2GB Sandisk-brand memory card (S/N BE0828613591D) was found within the Kodak M380 camera.

Examination of the memory card revealed that despite the fact that it was removed from a Kodak camera, it carried a volume label of "NIKON D40".

Volume	
File System	FAT16
Sectors per cluster	64
Bytes per sector	512
Total Sectors	3,858,489
Total Capacity	1,975,287,808 Bytes (1.8GB)
Total Clusters	60,281
Unallocated	1,175,846,912 Bytes (1.1GB)
Free Clusters	35,884
Allocated	799,440,896 Bytes (762.4MB)
Volume Name	NIKON D40
Volume Offset	135
Drive Type	Fixed

Figure 1 – Volume information for Sandisk memory card

The Defense Cyber Crime Institute's (DCCI) StegCarver tool was used to carve digital images from the allocated and unallocated space on the memory card. Numerous images were located depicting the same Caucasian male (shown below).

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	
SIGNATU(b)(6)(b)(7)(C) [redacted]	DATE 16 Jun 10	EXHIBIT 67

DETAILS

Figure 2 – Example of one of many pictures of Caucasian male from memory card

Other images recovered from the memory card included depictions of a Caucasian male in underwear, a variety of outdoor activities, other military personnel, and pages of PFC MANNING's Article 15 paperwork.

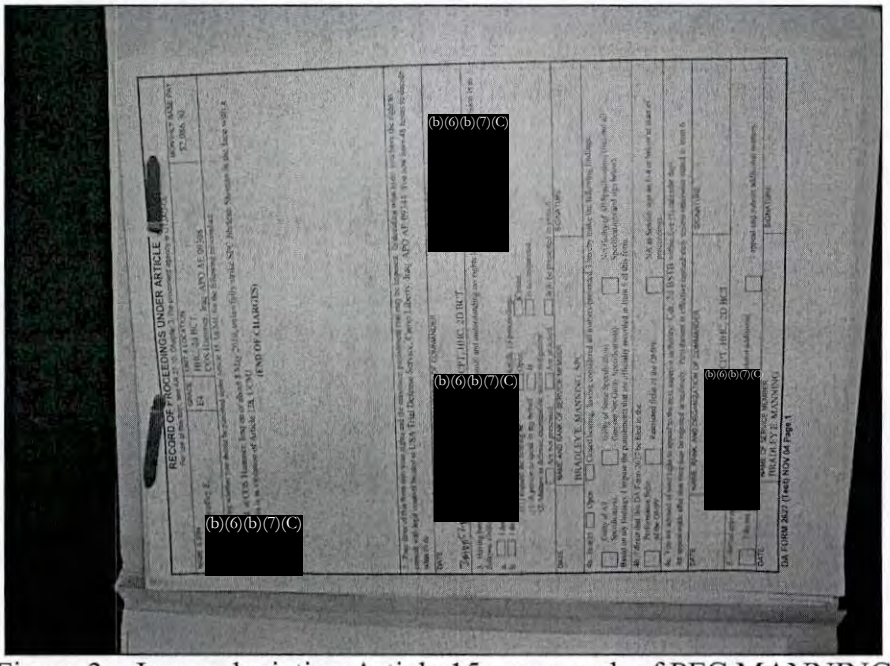


Figure 3 – Image depicting Article 15 paperwork of PFC MANNING

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 16 Jun 10	EXHIBIT 67

DETAILS

No classified material was located on either the Kodak M380 or the Sandisk memory card.

LEADS:

1. Attempt to locate the NIKON D40 camera used to format the Sandisk memory card, as it may belong to PFC MANNING and might contain additional removable media that could be used to store or transfer data.

----------///LAST ENTRY///----------

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: 16 Jun 10 / EXHIBIT: 67

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

DETAILS

Examination and Contents:

Between 15 and 16 June 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Digital Forensics and Research Branch, CCIU, conducted a preliminary examination of the U.S. Government computer named N2D10MTNBDE7019, assigned Internet Protocol (IP) Address 144.107.17.19, property of the 4th Brigade, 10th Mountain Division and recorded on DA Form 4137, Document Number (DN) 068-10. All times shown in this report are in relation to UTC/GMT unless otherwise noted.

File Verification:
Supply Annex NIPR Computer –
Hitachi 111.8 Gigabyte (GB) Hard Disk Drive (HDD), SN#070817DP0C10DSG2J1DP
The files were verified to be exact copies of the files obtained from Item 2, DN 068-10, through a comparison of the message digest-5 (MD5) algorithm (i.e., hash) values, with no errors.

Original File Hash: b0b530ea63552253e0dc814db4b618f2
Verification Hash: b0b530ea63552253e0dc814db4b618f2

A review of the Hard Drive using Anti-Virus:
The examined hard disk was scanned using Symantec Endpoint Protection (SEP) Version 11.0.5002.333, Definitions 6/14/2010 rev. 40.
No threats were identified by SEP.

Pertinent Information:
Examination of the Internet History for the "Bradley Manning" user profile revealed visits to the Google website to search for the term 'wikileaks'.

Url Name	Profile Name	Visit Count	Last Accessed
http://news.google.com/news/search?aq=f&pz=1&cf=all&ned=us&hl=en&q=wikileaks	bradley.manning	7	05/21/10 11:23:17AM
http://news.google.com/news/search?pz=1&cf=all&ned=us&hl=en	bradley.manning	1	05/21/10 11:23:07AM
http://news.google.com/news/search?pz=1&cf=all&ned=us&hl=en&q=wikileaks&cf=all&as_qdr=d&as_drrb=q	bradley.manning	16	05/21/10 11:23:48AM
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	bradley.manning	1	05/21/10 11:23:25AM
http://news.google.com/news?pz=1&cf=all&ned=us&hl=en&q=wikileaks&cf=all&output=rss	bradley.manning	1	05/21/10 11:23:16AM

Examination of the Internet History for the "Bradley Manning" user profile revealed visits to the "About.com: US Military" website for web pages detailing Non-Judicial Punishment (Article 15).

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 16 June 2010	EXHIBIT 68

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

DETAILS

Url Name	Profile Name	Visit Count	Last Accessed
http://usmilitary.about.com/od/justicelawlegislation/a/article152.htm	bradley.manning	4	05/21/10 10:00:43AM
http://usmilitary.about.com/od/justicelawlegislation/a/article152_2.htm	bradley.manning	4	05/21/10 10:02:57AM

Examination of the Internet History for the "Bradley Manning" user profile revealed visits to the Google website searching for "closed open article 15 hearing".

Url Name	Profile Name	Visit Count	Last Accessed
http://www.google.com/search?hl=en&source=hp&q=closed+open+article+15+hearing&aq=o&aqi=&aql=&oq=&gs_rfai=	bradley.manning	7	05/21/10 10:00:35AM

Examination of the Internet History for the "Bradley Manning" user profile revealed visits to the Google webmail web site. It is unknown what Gmail account was accessed.

Url Name	Profile Name	Visit Count	Last Accessed
https://mail.google.com/mail/?hl=en&safe=on&shva=1	bradley.manning	94	05/22/10 03:34:15PM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:dad.1e.2.0&view=tl&start=0&num=70&lhop=1367&ltup=^r&slmm=128ba1907a68b241&scid=rr4fr9-47adbe8a...	bradley.manning	2	05/21/10 09:50:49AM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:ex.29.2.1&view=cv&th=128bf80386ce98af&msgs=128bc9336156877f&rt=h&search=inbox	bradley.manning	2	05/22/10 03:34:28PM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:ex.29.3.0&view=cv&th=128bf80386ce98af&msgs=128bea6ff39ea6fb&rt=h&search=inbox	bradley.manning	1	05/22/10 03:34:36PM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:ex.29.3.0&view=cv&th=128bf80386ce98af&msgs=128bea6ff39ea6fb&rt=h&search=inbox	bradley.manning	2	05/22/10 03:34:37PM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.1e.1.0&view=tl&start=0&num=70&rt=h&search=drafts	bradley.manning	2	05/21/10 09:50:43AM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.1e.3.0&view=tl&start=0&num=70&rt=h&search=trash	bradley.manning	2	05/21/10 09:51:03AM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.1e.4.0&view=tl&start=0&num=70&lhop=1367&ltup=^i&slmm=0&scid=rr4fr9-47adbe&rt=h&search=inbox	bradley.manning	2	05/21/10 09:55:58AM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.22.1.0&view=tl&start=0&num=70&lhop=1368&ltup=^i&slmm=0&scid=d11y0r-ijdxbn&rt=h&search=inbox	bradley.manning	2	05/21/10 11:09:29AM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.23.1.0&view=tl&start=0&num=70&lhop=1368&ltup=^i&slmm=0&scid=fpramk-1k8qjt&rt=h&search=inbox	bradley.manning	2	05/21/10 11:42:30AM
https://mail.google.com/mail/?ui=2&ik=eccd5dd524&rid=mail:lc.23.2.0&view=tl&start=0&num=70&lhop=1368&ltup=^i&slmm=0&scid=fpramk-1k8qjt&rt=h&search=inbox	bradley.manning	2	05/21/10 11:46:06AM
https://mail.google.com/mail/feed/atom	bradley.manning	11	05/22/10 03:34:09PM
https://mail.google.com/mail/feed/atom	bradley.manning	12	05/22/10 03:34:15PM

Examination of the "Cookies" folder for the (b)(6)(b)(7)(C) user profile revealed a Gmail account name for Bradley Manning.

From C:\Documents and Settings(b)(6)(b)(7)(C) Cookies(b)(6)(b)(7)(C) google[1].txt
Created Date 05/22/10 03:34:10PM
gmailchat(b)(6)(b)(7)(C)

Leads:

1. None.

//LAST ENTRY//

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 16 June 2010	EXHIBIT 68

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

DETAILS

Imaging:

Between 0934 and 1058, 18 Jun 10, SA (b)(6)(b)(7)(C) created a digital forensic image (.E01) of the Fujitsu hard disk drive (property of Mr. (b)(6)(b)(7)(C) , taken as evidence on Evidence Property Custody Document (EPCD), DA Form 4137, Document Number (DN) 076-10, Item #1, utilizing AccessData's FTK Imager v2.9.0.1385.

Computer Make	N/A
Computer Model	N/A
Computer Serial Number	N/A
Hard Drive Make	Fujitsu
Hard Drive Model	MHY2120BH
Hard Drive Serial Number	K404T812MF4D
Source MD5 checksum:	ca670499c7607d539b991793e5830008
Verification MD5 checksum:	ca670499c7607d539b991793e5830008
Source SHA1 checksum:	f39ba0bdf1b72da40e126dc933bbfdf22da4e31a
Verification SHA1 checksum:	f39ba0bdf1b72da40e126dc933bbfdf22da4e31a

Between 1103 and 1213, 18 Jun 10, SA (b)(6)(b)(7)(C) created a digital forensic image (.E01) of Seagate hard disk drive (property of Mr. (b)(6)(b)(7)(C) , taken as evidence on EPCD, DA Form 4137, DN 077-10, Item #1, utilizing AccessData's FTK Imager v2.9.0.1385.

Computer Make	HP
Computer Model	HP2133
Computer Serial Number	CNU90513VT
Hard Drive Make	Seagate
Hard Drive Model	ST9120817AS
Hard Drive Serial Number	SRE2C1QK
Source MD5 checksum:	b9314be0ef75d9d878f6b6ba12b2d55d
Verification MD5 checksum:	b9314be0ef75d9d878f6b6ba12b2d55d
Source SHA1 checksum:	91e55b9d3180277d2f30a243e48cbab093de272a
Verification SHA1 checksum:	91e55b9d3180277d2f30a243e48cbab093de272a

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SAC (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
S (b)(6)(b)(7)(C) [redacted]	DATE 18 Jun 10	EXHIBIT 69

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) 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	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATU (b)(6)(b)(7)(C)	DATE: 18 Jun 10 / EXHIBIT: 70

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
199.56.188.121	AN ICESAVE REFERENDUM
199.56.188.122	Mr. Company Computer Guy
199.56.188.53	ncd.state.sgov.gov
199.56.188.71	Net-Centric Diplomacy Version
199.56.188.73	NOFORN
199.56.188.75	NTNCDDOSWS1SB
199.56.188.76	NTNCDDOSWS2S
199.56.188.79	NTNCDDOSWS3SB
88.80.12.160	NTNCDPRODSTAT
88.80.2.32	NTNCDSQL2S
\\22.225.53.205\QDrive	NTNCDSQL4s
\\22.225.53.20S\TDrive	NTNCDSQL5S
adrianlamo	osc_youtube-cm
assange	REYKJAVIK
backup.xlsx	S//NF
bradass87	schmiedl
breanna.jpg	SECRET//
collateral murder	SIGURDARDOTTIR
dates.csv	SIPDIS
dump2.csv	SIPDIS
farah	SKARPHEDINSSON
files.zip	wget -O
gmail.com	wikileaks
Gunnarsson	

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: 18 Jun 10 / EXHIBIT: 70

DETAILS

Figure 3 – Text showing interaction with the Facebook page associated with (b)(6)(b)(7)(C)

References to (b)(6)(b)(7)(C) were found in numerous locations on the disk, such as in a text fragment found in PS 308287245:

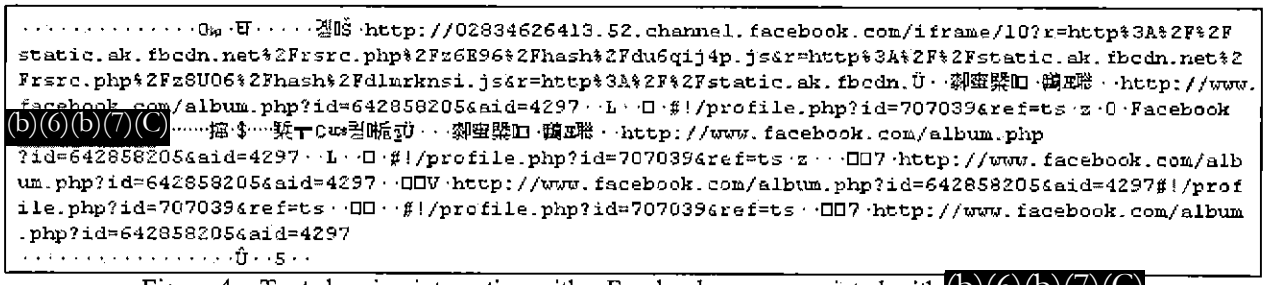


Figure 4 – Text showing interaction with a Facebook page associated with (b)(6)(b)(7)(C)

References to "Collateral Murder" were found in numerous locations on the disk. In one instance, the NTUSER.DAT file for the "swamp rat" user showed evidence of the user account having searched for "collateral murder" on YouTube.com.

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 18 Jun 10	EXHIBIT 70

DETAILS

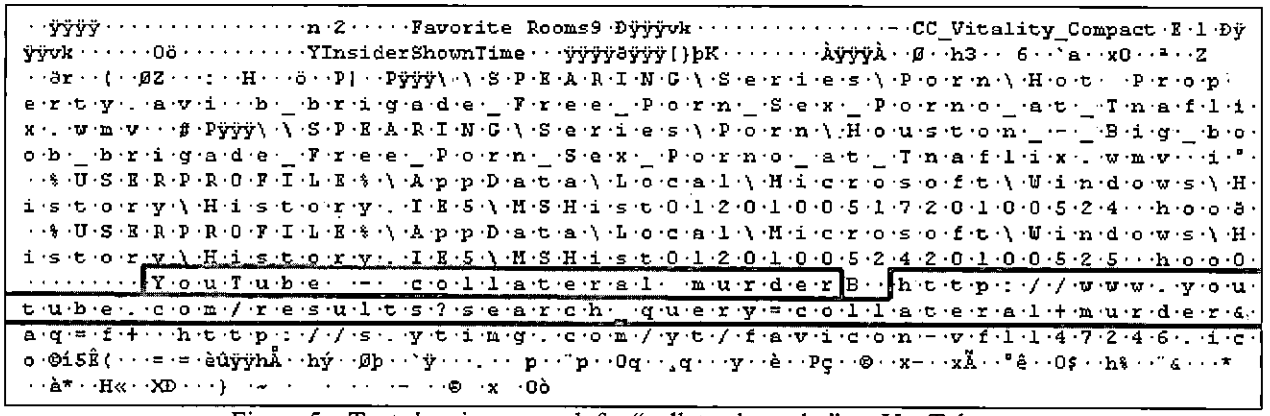


Figure 5 – Text showing a search for "collateral murder" on YouTube.com

Other references to "collateral murder" were found in the system's restore point files. Two of the more significant references are shown below.

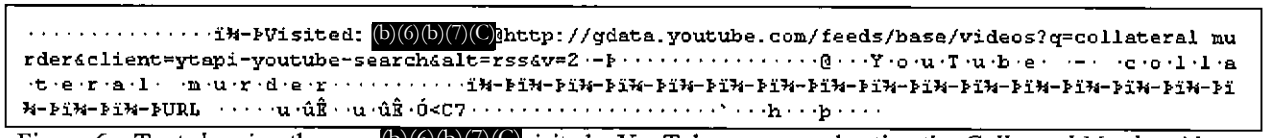


Figure 6 – Text showing the user (b)(6)(b)(7)(C) visited a YouTube.com page hosting the *Collateral Murder* video

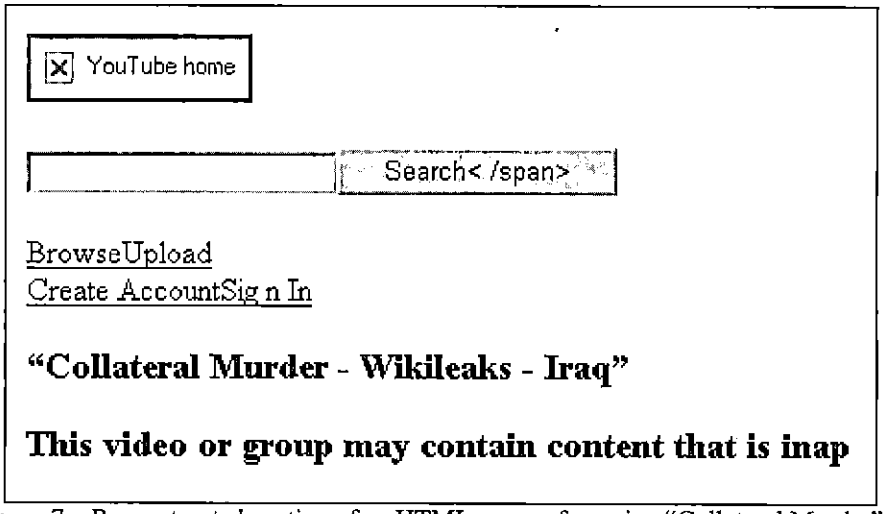


Figure 7 – Reconstructed portion of an HTML page referencing "Collateral Murder"

Reference to Mr. (b)(6)(b)(7)(C) was located in several locations on the disk, including in a rant against Wikileaks and the Formspring conversation below. Formspring is a social networking site that allows participants to anonymously ask questions of Formspring users and receive responses. In the conversation below

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: 18 Jun 10 / EXHIBIT: 70

DETAILS

(reconstructed from HTML found in unallocated space), the questioner (or questioners) is unknown, but Mr. (b)(6)(b)(7)(C) appeared to be providing the answers.

Figure 8 – Formspring conversation between Mr. (b)(6)(b)(7)(C) and unknown questioner(s)

References to "breanna.e.manning" were found in several locations on the disk, including in the system's restore point files. Two of those references provided information pertaining to Gmail and Twitter accounts are shown below.

```
Visited: swamp rat@https://mail.google.com/mail/?hl=en&shva=1·-þ·····"···G·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·····ï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-Þï¾-ÞURL ····
"¢V·üÊ·"¢V·üÊ·Ô<Ld·····`···h···þ····· ·"·····¹<Ld·····i
```

Figure 9 – Text referencing Gmail and Twitter accounts believed to belong to PFC MANNING as "Breanna"

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: 18 Jun 10 / EXHIBIT: 70

DETAILS

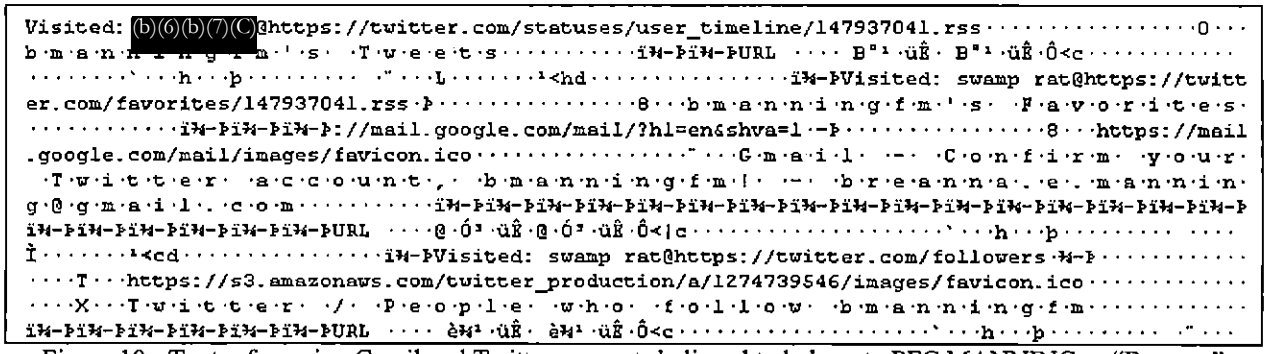


Figure 10 - Text referencing Gmail and Twitter accounts believed to belong to PFC MANNING as "Breanna"

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 '(b)(6)(b)(7)(C) ' 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(b)(6)(b)(7)(C) \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%2web.w` file appear to relate to PFC MANNING's interests.

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 18 Jun 10	EXHIBIT 70

DETAILS

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

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

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: 18 Jun 10 / EXHIBIT: 70

DETAILS

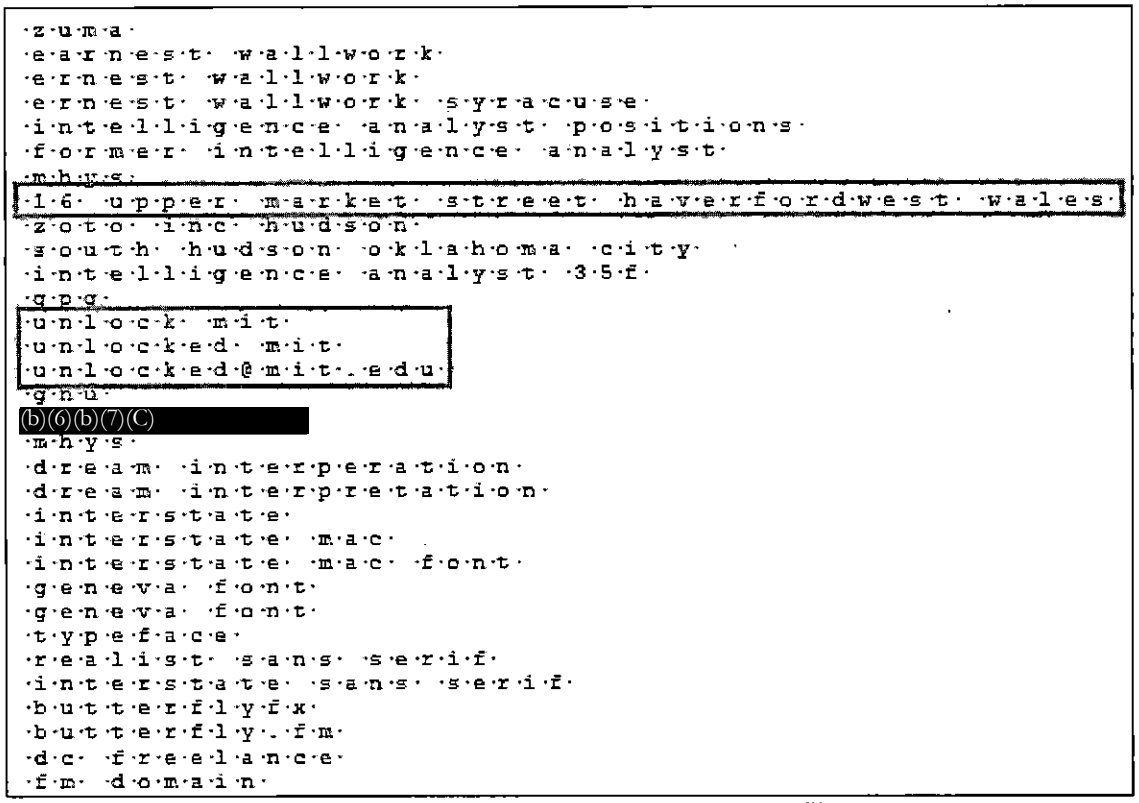


Figure 12 – Excerpt from `google%2web.w` file

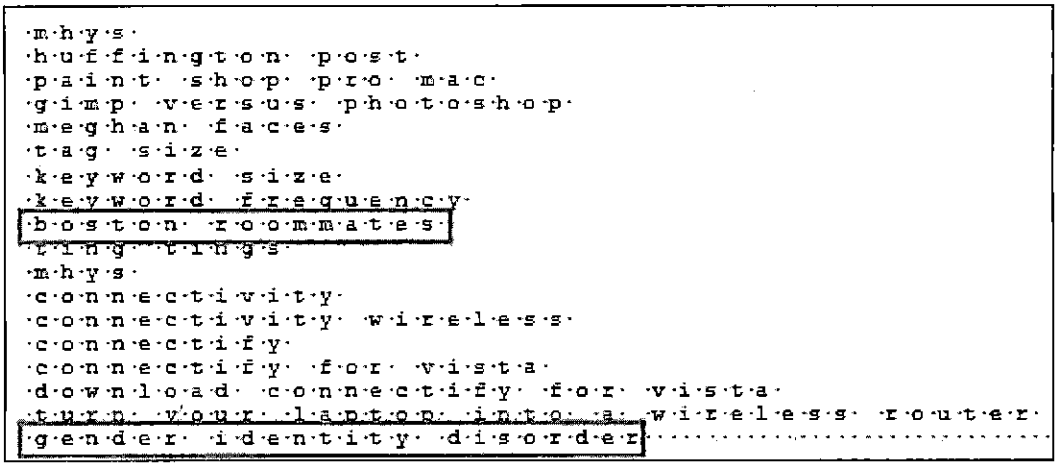


Figure 13 – Excerpt from `google%2web.w` file

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	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: 18 Jun 10 / EXHIBIT: 70

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	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: 18 Jun 10 / EXHIBIT: 70

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

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), previously collected as evidence on Evidence/Property Custody Document (EPCD), Document Number (DN) 079-10, Item 1, 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 Ultabay 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 : verified

SHA1 Acquisition Hash: a3ee6a82a19408b64a1de1ce2aa3e204498475d2
SHA1 Verification Hash: a3ee6a82a19408b64a1de1ce2aa3e204498475d2 : verified

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), previously collected as evidence on EPCD, DN 079-10, Item 2, 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 Ultabay 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 : verified

SHA1 Acquisition Hash: cdbdfb82874030f387cd46b3fffc3d77b2c3f91b
SHA1 Verification Hash: cdbdfb82874030f387cd46b3fffc3d77b2c3f91b : verified

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).

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
SIGNATU (b)(6)(b)(7)(C) [redacted]	DATE: 18 Jun 10 / EXHIBIT: 717

DETAILS

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-created files, all of which are listed below.

Name	File Created	Logical Size	MD5 Hash Value
bradass87.html	5/25/2010 18:40	90,314 bytes	420f99b1217fd7c614f256fa4665bed7
LOG1.RTF	5/25/2010 21:55	14,656 bytes	6bb7a4b60b44101e1f215c7465bb72b3
LOG2.RTF	5/25/2010 21:56	37,159 bytes	cc41ed2a8d4dc4cfd8f0022aa0754d25
otr_print	5/25/2010 18:43	36 bytes	cf2fb64659ed129fe46066b437b11609

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

Name	File Created	Logical Size	MD5 Hash Value
5-21LOG4.RTF	5/27/2010 18:54	1,082 bytes	a5b5b4e9f6dbb42ff28bf9580753a84c
5-22LOG3.RTF	5/27/2010 18:54	37,155 bytes	e840bf939a59ae287395f67507048856
5-23LOG2.RTF	5/27/2010 18:53	37,159 bytes	cc41ed2a8d4dc4cfd8f0022aa0754d25
5-24LOG1.RTF	5/27/2010 18:53	14,656 bytes	6bb7a4b60b44101e1f215c7465bb72b3
b-523logX.rtf	5/27/2010 19:14	14,656 bytes	6bb7a4b60b44101e1f215c7465bb72b3
Hackers Wanted.mp4.mp4	5/27/2010 19:43	729,574,543 bytes	1d710b7d0f5c4858d73e1f00088a0a6e
manning_pgp_jan_2010	5/27/2010 21:53	1,768 bytes	de6a9675395fe39fd45acc1f29a1190f
Screenshot-1.png	5/27/2010 19:34	116,127 bytes	b359e4475b790efe2381a5b638e96a51

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

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

DATE
18 Jun 10

EXHIBIT
71

DETAILS

Based on matching hash values, the files `LOG1.RTF` (on the "Corner Office" thumb drive) and `5-24LOG1.RTF` and `b-523logX.rtf` (on the "DANE_ELEC" thumb drive) were determined to be identical files. Similarly, based on matching hash values, the files `LOG2.RTF` (on the "Corner Office" thumb drive) and `5-23LOG2.RTF` (on the "DANE_ELEC" thumb drive) were determined to be identical files.

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	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: 18 Jun 10 / EXHIBIT: 71

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

DETAILS

WEBSITE CAPTURE:

About 1120, 17 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) Digital Forensics and Research Branch, CCIU, conducted a Web site capture using the covert network, Adobe Acrobat Professional and HT Track Website Copier to capture portions of the web sites "http://wikileaks.org/" and "http://www.collateralmurder.com".

SA (b)(6)(b)(7)(C) captured the following Web sites using Adobe Acrobat Professional:

http://wikileaks.org/
http://wikileaks.org/wiki/Draft:Presser - (Inactive Press release about 6 Jun10 Wired Magazine release)
http://wikileaks.org/wiki/Draft:CM

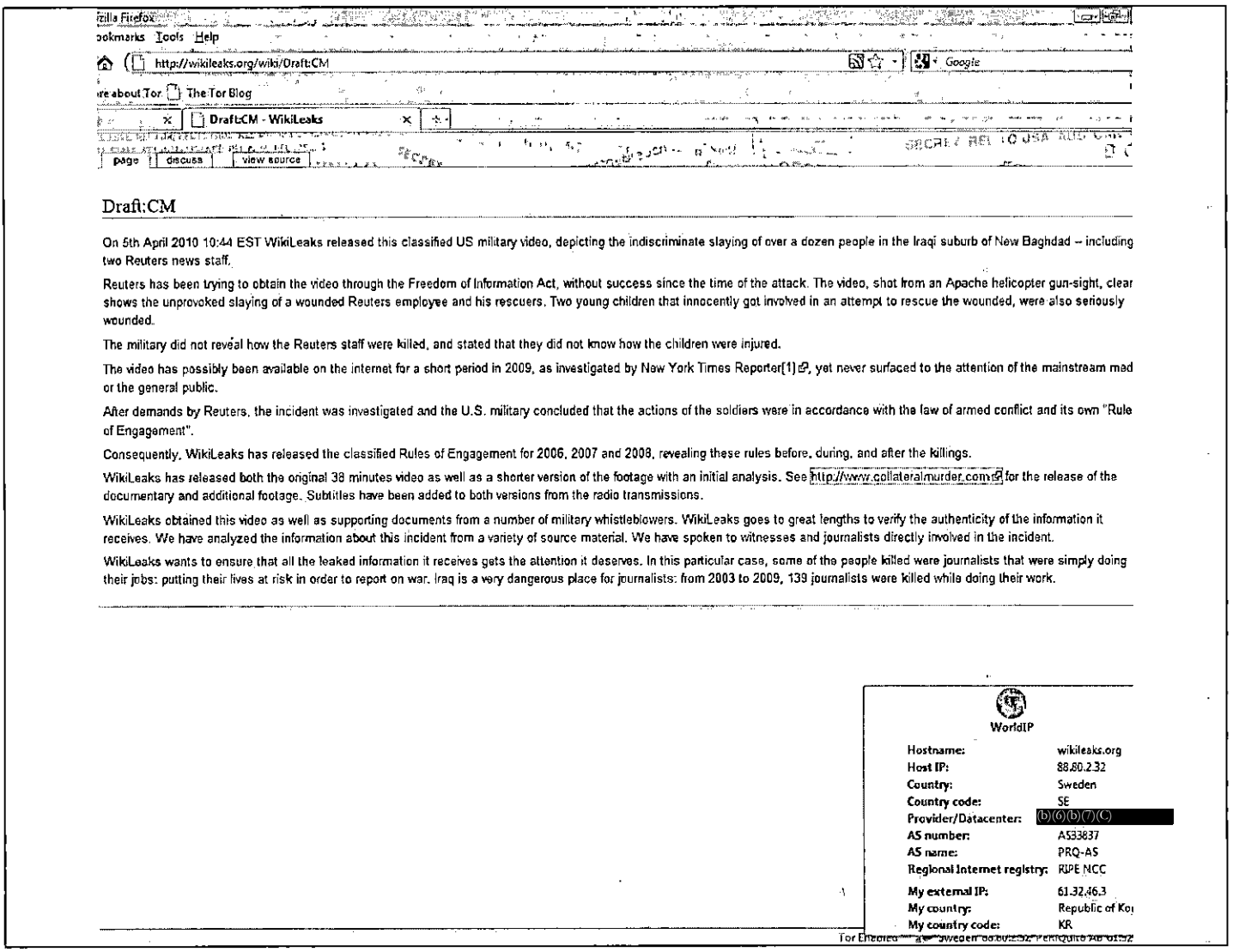
SA (b)(6)(b)(7)(C) captured the following Web sites (with attachments on each page) using Adobe Acrobat Professional:

http://wikileaks.org/wiki/Classified_cable_from_US_Embassy_Reykjavik_on_Icesave,_13_Jan_2010 Attachment – "us-watson1-2010.txt"
http://wikileaks.org/wiki/U.S._Embassy_profiles_on_Icelandic_PM,_Foreign_Minister,_Ambassador Attachment – "iceland-profiles.pdf"
http://wikileaks.org/wiki/U.S._Intelligence_planned_to_destroy_WikiLeaks,_18_Mar_2008 Attachment – "us-intel-wikileaks.pdf"
http://wikileaks.org/wiki/Final_UK-NL_offer_to_the_government_of_Iceland,_19_Feb_2010 Attachment – "icesave1.pdf"
http://wikileaks.org/wiki/Icelandic_Icesave_offer_to_UK-NL,_25_Feb_2010 Attachment – "icesave2.pdf"

The Internet Protocol (IP) address reported for "http://wikileaks.org" (shown below) was 88.80.2.32.

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) [redacted]	DATE 18 June 2010	EXHIBIT 72

DETAILS



zilla Firefox
ookmarks Tools Help
http://wikileaks.org/wiki/Draft:CM
Google
re about Tor The Tor Blog
Draft:CM - WikiLeaks
page discuss view source

Draft:CM

On 5th April 2010 10:44 EST WikiLeaks released this classified US military video, depicting the indiscriminate slaying of over a dozen people in the Iraqi suburb of New Baghdad – including two Reuters news staff.

Reuters has been trying to obtain the video through the Freedom of Information Act, without success since the time of the attack. The video, shot from an Apache helicopter gun-sight, clear shows the unprovoked slaying of a wounded Reuters employee and his rescuers. Two young children that innocently got involved in an attempt to rescue the wounded, were also seriously wounded.

The military did not reveal how the Reuters staff were killed, and stated that they did not know how the children were injured.

The video has possibly been available on the internet for a short period in 2009, as investigated by New York Times Reporter[1], yet never surfaced to the attention of the mainstream mad or the general public.

After demands by Reuters, the incident was investigated and the U.S. military concluded that the actions of the soldiers were in accordance with the law of armed conflict and its own "Rule of Engagement".

Consequently, WikiLeaks has released the classified Rules of Engagement for 2006, 2007 and 2008, revealing these rules before, during, and after the killings.

WikiLeaks has released both the original 38 minutes video as well as a shorter version of the footage with an initial analysis. See http://www.collateralmurder.com for the release of the documentary and additional footage. Subtitles have been added to both versions from the radio transmissions.

WikiLeaks obtained this video as well as supporting documents from a number of military whistleblowers. WikiLeaks goes to great lengths to verify the authenticity of the information it receives. We have analyzed the information about this incident from a variety of source material. We have spoken to witnesses and journalists directly involved in the incident.

WikiLeaks wants to ensure that all the leaked information it receives gets the attention it deserves. In this particular case, some of the people killed were journalists that were simply doing their jobs: putting their lives at risk in order to report on war. Iraq is a very dangerous place for journalists: from 2003 to 2009, 139 journalists were killed while doing their work.

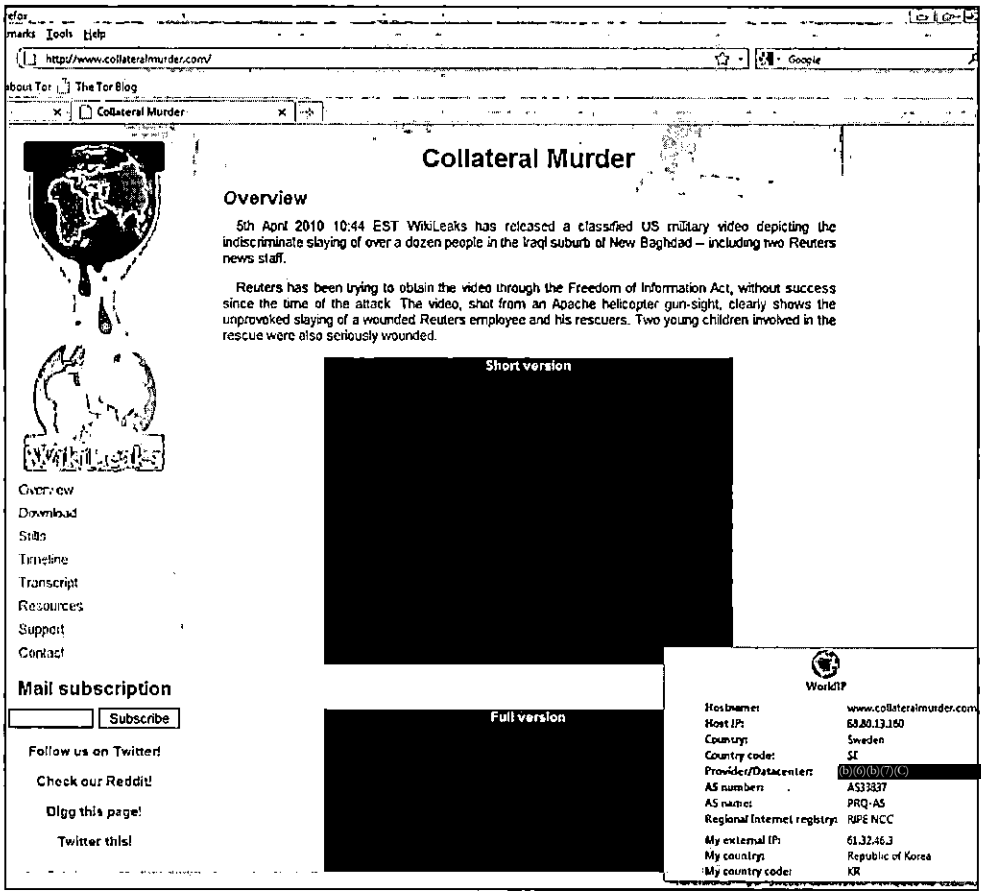
WorldIP

Hostname:	wikileaks.org
Host IP:	88.80.2.32
Country:	Sweden
Country code:	SE
Provider/Datacenter:	(b)(6)(b)(7)(C)
AS number:	AS33837
AS name:	PRQ-AS
Regional Internet registry:	RIPE NCC
My external IP:	61.32.46.3
My country:	Republic of Ko
My country code:	KR

About 1200, 17 Jun 10, SA (b)(6)(b)(7)(C) captured the web site "http://www.collateralmurder.com" using HT Track Website Copier. The IP Address reported for "http://www.collateralmurder.com" (shown below) was 88.80.13.160.

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 18 June 2010	EXHIBIT 73

DETAILS



The collected folders/files from each website were imported into EnCase v6.16.2 and a logical evidence file was created. The original files from the collected folders were hashed using the message digest-5 (MD5) algorithm (i.e., hash), and the resulting values compared to those of the files within the logical evidence file. The hash values matched.

The logical evidence file was recorded to a Digital Versatile Disc – Recordable (DVD-R).

About 1200, 18 June 10, SA (b)(6)(b)(7)(C) collected the DVD-R as evidence on a DA Form 4137, Evidence Property Custody Document (EPCD), Document Number (DN) 084-10.

//LAST ENTRY//

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 18 June 2010	EXHIBIT 72

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

DETAILS

Imaging:

Between 09:34:32 and 10:58:41, 18 Jun 10, SA (b)(6)(b)(7)(C) created a digital forensic image of Department of the Army Form 4137, Evidence Property Custody Document (EPCD), Document Number (DN) 076-01, Item #1, utilizing the Access Data FTK Imager Version 2.9.0.1385 and saved as in the EnCase file format.

Computer Make	N/A
Computer Model	N/A
Computer Serial Number	N/A
Hard Drive Make	Fujitsu
Hard Drive Model	MHY2120BH
Hard Drive Serial Number	K404T812MF4D
Source MD5 checksum:	ca670499c7607d539b991793e5830008
Verification MD5 checksum:	ca670499c7607d539b991793e5830008
Source SHA1 checksum:	f39ba0bdf1b72da40e126dc933bbfdf22da4e31a
Verification SHA1 checksum:	f39ba0bdf1b72da40e126dc933bbfdf22da4e31a

Between 11:03:21 and 12:13:40, 18 Jun 10, SA (b)(6)(b)(7)(C) created a digital forensic image of DA Form 4137, DN 077-01, Item #1, utilizing the Access Data FTK Imager Version 2.9.0.1385 and saved as in the EnCase file format.

Computer Make	HP
Computer Model	HP2133
Computer Serial Number	CNU90513VT
Hard Drive Make	Seagate
Hard Drive Model	ST9120817AS
Hard Drive Serial Number	SRE2C1QK
Source MD5 checksum:	b9314be0ef75d9d878f6b6ba12b2d55d
Verification MD5 checksum:	b9314be0ef75d9d878f6b6ba12b2d55d
Source SHA1 checksum:	91e55b9d3180277d2f30a243e48cbab093de272a
Verification SHA1 checksum:	91e55b9d3180277d2f30a243e48cbab093de272a

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SSA (b)(6)(b)(7)(C), (b) (7)(E)	Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SI (b)(6)(b)(7)(C) [redacted]	DATE 18 Jun 10	EXHIBIT 73

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1730, 18 Jun 10, SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C), this office; SA (b)(6)(b)(7)(C) Diplomatic Security Service (DSS), U.S. Department of State (DoS),10 Causeway Street, Suite 1001, Boston, MA 02222; and SA (b)(6)(b)(7)(C) 902 Military Intelligence Group, U.S. Army Intelligence and Security Command, 4 Lexington Street, Devens, MA 01434; interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) who related he first met PFC Bradley E. MANNING around January of 2010, during a visit to the Techniques Office at the Massachusetts Institute of Technology (MIT), in which he believed PFC MANNING was on leave from the U.S. Army. Mr. (b)(6)(b)(7)(C) related he spoke with PFC MANNING for approximately 40 minutes, during which time PFC MANNING divulged he was an intelligence officer and discussed the history of American Intelligence. Additionally, Mr. (b)(6)(b)(7)(C) related he discussed security containers and physical security with PFC MANNING and subsequently received an email pertaining to the security of storage facilities in which himself and PFC MANNING were Carbon Copied (CC), and in which Mr. (b)(6)(b)(7)(C) elaborated on the use of a "Robo Dialer". Mr. (b)(6)(b)(7)(C), did not clarify who sent the aforementioned email. Mr. (b)(6)(b)(7)(C) related he subsequently exchanged email with PFC MANNING, but he refused to comment on the content of some of the email; however, Mr. (b)(6)(b)(7)(C) related he would discuss the email that he believed to be relevant to this investigation, and he would subsequently forward relevant email to SA (b)(6)(b)(7)(C)

When asked about how he learned about PFC MANNING's disclosure of classified information, Mr. (b)(6)(b)(7)(C) related some time after speaking with PFC MANNING he traveled to the Dominican Republic where he became aware of PFC MANNING's apprehension by U.S. Army authorities though an email received from the news web sites "slashdot.org" and the "Washington Post", which revealed PFC MANNING released documents obtained from the "Iraq Database" that included "airstrike videos" and State Department documents. Subsequently, Mr. (b)(6)(b)(7)(C) related he conducted research and found the "Wired.com" articles pertaining to Mr. (b)(6)(b)(7)(C) disclosure of his chats logs with PFC MANNING detailing PFC MANNING's disclosure of classified information. When asked about what PFC MANNING would have to do to accomplish the disclosure of classified material, Mr. (b)(6)(b)(7)(C) related he believed that he recalled in the "Wired.com" article Mr. (b)(6)(b)(7)(C) related that PFC MANNING zero filled or erased the classified information that he had previously stored in a digital format under a codename.

When asked about his acquaintances, Mr. (b)(6)(b)(7)(C) related he would not comment about any of his acquaintances or anyone associated with PFC MANNING. Additionally, Mr. (b)(6)(b)(7)(C) related he would not comment on whether he knew Mr. (b)(6)(b)(7)(C) or Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related he knew of Mr. Julian ASSANGE, but was not personally acquainted with Mr. ASSANGE. Mr. (b)(6)(b)(7)(C) related when in Amsterdam he stays at the townhouse of Mr. (b)(6)(b)(7)(C) who agents knew through news articles was a close associate of Mr. ASSANGE. Mr. (b)(6)(b)(7)(C) subsequently related he hoped Mr. (b)(6)(b)(7)(C) would distance himself from Mr. ASSANGE and Wikileaks, which he expressed, had better security then the American Intelligences apparatus, because of the attention drawn to Wikileaks after the revelation of PFC MANNING's disclosure of 260,000 State Department documents, which he characterized as an irresponsible action on the part of PFC MANNING.

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Quantico, VA 22134	
S (b)(6)(b)(7)(C)	DATE 18 Jun 10	EXHIBIT 74

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

Mr. (b)(6)(b)(7)(C) was subsequently advised that PFC MANNING did release classified information and if any of the information released by PFC MANNING is in Mr. (b)(6)(b)(7)(C) possession, he should not store, transfer, or discuss the information with anyone, and should immediately turn over the information to SA (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) responded relating PFC MANNING did not reveal anything classified to him, but he would provide SA (b)(6)(b)(7)(C) with any information he deemed to be relevant to the investigation. Additionally, SA (b)(6)(b)(7)(C) requested, if Mr. (b)(6)(b)(7)(C) knows either Mr. (b)(6)(b)(7)(C) or Mr. (b)(6)(b)(7)(C) that he communicate with them requesting that they contact SA (b)(6)(b)(7)(C) to coordinate a meeting.

AGENT'S COMMENT: Mr. (b)(6)(b)(7)(C) subsequently forwarded SA (b)(6)(b)(7)(C) email from the account, (b)(6)(b)(7)(C) and (b)(6)(b)(7)(C) pertaining to the release of Mr. (b)(6)(b)(7)(C)'s chat logs with PFC MANNING and "Apache Helicopter" video, none which originated from PFC MANNING. Additionally, Mr. (b)(6)(b)(7)(C) coordinated with SA (b)(6)(b)(7)(C) via email, relating, "since you asked me to try and get in touch with (b)(6)(b)(7)(C) – (b)(6)(b)(7)(C) left me a message that you should get in touch via his attorney, (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) (Mr. (b)(6)(b)(7)(C) Good & Cormier, 83 Atlantic Avenue, Boston, MA 02110, 617-523-5933, Cell: (b)(6)(b)(7)(C) Fax: 617-523-7554, (b)(6)(b)(7)(C) @goodcormier.com). ///LAST ITEM///

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Quantico, VA 22134
SIG (b)(6)(b)(7)(C)	DATE: 18 Jun 10 / EXHIBIT: 74

Exhibit 75

Page(s) 000356 and 000357 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

PAGE 1 OF 1 PAGES

DETAILS

About 1703, 14 Jun 10, SA (b)(6)(b)(7)(C) sent Ms. (b)(6)(b)(7)(C) Supervisory Freedom of Information/ Privacy Act Specialist, Office of Personnel Management (OPM), Freedom of Information/Privacy Act Group, 1137 Branchton Road, P.O. Box 618, Boyers, PA 16017, an official request for the OPM Security Clearance Background Investigation results, Standard Form (SF) 86 documents, adjudication and other relevant documents related to the background investigation of PFC MANNING.

AGENT'S COMMENT: SA (b)(6)(b)(7)(C) noted that under exception (B)(7) of the Privacy Act, it allows for record holders, such as OPM, to release their records to a requestor if the purpose of the request relates to a civil or criminal law enforcement activity, as authorized by law.

About 0930, 23 Jun 10, SA (b)(6)(b)(7)(C) received a sealed envelope from the OPM containing approximately 69 pages of documents related to the processing of PFC MANNING's Security Clearance Background Investigation by OPM. A review of these documents reveal they include the Electronic Questionnaire for Investigation Processing (e-QIP) completed by PFC MANNING, dated 26 Sep 07; and the OPM results of checks and interviews of persons associated with PFC MANNING, dated 15 Jan 08.

//LAST ENTRY//

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	
SIGN (b)(6)(b)(7)(C) [redacted]	DATE 23 Jun 10	EXHIBIT 76

EXHIBIT(s) 77

Page(s) 000359 thru 000427 referred to:

FOI/P, OPM-FIPC
P.O. Box 618
1137 Branchton Road
Boyers, PA 16018-0618

CLASSIFIED

Exhibit(s) 78

Page(s) 000428 thru 000428b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 79

Page(s) 000429 thru 000429b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 80

Page(s) 000430 thru 000430b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

CLASSIFIED

Exhibit(s) 81

Page(s) 000431 thru 000431b referred to:

Commander
INSCOM
ATTN: IAMG-C-FOIA
4552 Pike Road
Fort Meade, MD 20755-5995

Exhibit(s) 82

Page(s) 000432 thru 000446 referred to:

FORT BLISS
FOIA Office (IMWE-BLS-HRF)
Building 503A - Pershing Road
Fort Bliss, Texas 79916

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER
0028-10-CID221-10117

DETAILS

About 1249, 12 Jul 10, SA (b)(6)(b)(7)(C), SA (b)(6)(b)(7)(C) U.S. Department of State – Diplomatic Security Service, 1801 N. Lynn Street, Arlington, VA 22209; SA (b)(6)(b)(7)(C) National Capital Region Military Intelligence Detachment, 902nd Military Intelligence Group, 9805 Lowen Road, Fort Belvoir, VA 22060; and SA (b)(6)(b)(7)(C) National Security Agency (NSA), 9800 Savage Road, Fort Meade, MD 20755, interviewed Ms. (b)(6)(b)(7)(C) GS-14, National Security Agency/Central Security Service Representative (NCR) - Iraq Staff, Camp Victory, Iraq, APO AE 09342, as she was identified as an NSA employee who previously worked with PFC MANNING while assigned to the S-2 Section of the 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq. Ms. (b)(6)(b)(7)(C) explained how she met PFC MANNING, her interactions with him, and the general conditions under which PFC MANNING worked under while in Iraq. Ms. (b)(6)(b)(7)(C) related she was assigned as an NSA liaison with the 3rd BCT of the 82nd Airborne Division at Joint Security Station (JSS) Loyalty, Iraq, beginning in July 2009; but due to the draw-down/movement of American forces within Iraq, she was later reassigned to FOB Hammer. Ms. (b)(6)(b)(7)(C) explained around November of 2009, the 2nd BCT, 10th Mountain Division rotated into FOB Hammer and replaced the 3rd BCT, 82nd Airborne Division, which is when she first met PFC MANNING. Ms. (b)(6)(b)(7)(C) said PFC MANNING was working in the area of All-Source Analysis and that she would have to walk past him and/or his area within the facility they worked in, in order to reach her own work area. Ms (b)(6)(b)(7)(C) said she remembered PFC MANNING primarily worked the night shift, which was a 12-hour shift beginning at 2200 and ending at 1000 the following morning. Ms. (b)(6)(b)(7)(C) explained she would generally see PFC MANNING during the hand-over meetings held twice daily; wherein the out-going shift personnel would brief the on-coming shift personnel of progress made on operations, indicators, and other intelligence related matters the unit was responsible for. Ms. (b)(6)(b)(7)(C) described PFC MANNING as immature but also as bright and intelligent. Ms. (b)(6)(b)(7)(C) mentioned at the hand-over briefings she noticed PFC MANNING appeared to have trouble speaking in front of others and would get choked up; often due to what she described as vicious verbal comments and gestures from other unit members. Ms. (b)(6)(b)(7)(C) specifically related MSG (b)(6)(b)(7)(C) Noncommissioned Officer in Charge (NCOIC) of the S-2 Section, as one of the main personnel who seemed to be the leader of these attacks which occurred while PFC MANNING was attempting to brief his projects in front of the group. Ms. (b)(6)(b)(7)(C) described the culture of the S-2 Section under which the soldiers worked as unsupportive and compared this atmosphere as being like sharks. Ms. (b)(6)(b)(7)(C) said she had talked to PFC MANNING on a couple of occasions in order to give him some encouragement from all of the personnel who would make fun at his expense during the briefings. Ms. (b)(6)(b)(7)(C) explained she made comments to personnel in the Signals Intelligence (SIGINT) Section about the poor working environment created by the other soldiers, but noticed this appeared to be the same atmosphere when the previous unit, the 3rd BCT, 82nd Airborne Division was there - so she did not pursue the matter. Ms. (b)(6)(b)(7)(C) stated she felt she should have possibly done or said more; however, stated there still wasn't any excuse for what PFC MANNING is alleged to have done. Ms. (b)(6)(b)(7)(C) stated PFC MANNING's access should have been limited to the Secure Internet Protocol Router (SIPR) and Non-secure Internet Protocol Router (NIPR) networks, as Ms. (b)(6)(b)(7)(C) noted FOB Hammer did not have any Joint Worldwide Intelligence Communications System (JWICS) access during the time she was assigned there. Ms. (b)(6)(b)(7)(C) further explained FOB Hammer did have NSA Network (NSANet) access. Ms. (b)(6)(b)(7)(C)

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C) [redacted]	DATE 12 Jul 10	EXHIBIT 83

DETAILS

explained NSANet is a system different, but similar to, the level of access provided by JWICS; and it is possible to connect to JWICS using NSANet. Ms. (b)(6)(b)(7)(C) related NSANet was limited to the work area which she worked in, and that this area was somewhat controlled by personnel working in her section. Ms. (b)(6)(b)(7)(C) stated if someone who was not assigned to this area entered it, they would likely be challenged by personnel from the SIGINT Section until it was determined they were clear to be in this area. Ms. (b)(6)(b)(7)(C) admitted that PFC MANNING would not likely have been challenged if he was in this area for a short period of time, as it was his job to interact with personnel from the SIGINT section due to his projects. Ms. (b)(6)(b)(7)(C) stated as far as she knew, PFC MANNING should not have had access to NSANet while he was assigned to Iraq. Ms. (b)(6)(b)(7)(C) mentioned that because people often don't know what NSA does, it would not be uncommon for personnel like herself to take time to answer questions and/or educate others about NSA systems. Ms. (b)(6)(b)(7)(C) related PFC MANNING would ask questions of the SIGINT Analysts, but didn't appear to have any overt agenda behind the questions he asked. Ms. (b)(6)(b)(7)(C) said PFC MANNING asked a lot of questions initially, but appeared to stop asking as many questions due to the unit dynamics she mentioned earlier. Ms. (b)(6)(b)(7)(C) when questioned about other personnel PFC MANNING may have been friends with, explained there was another male soldier who she said appeared to have emotional issues and who was assigned to the SIGINT Platoon. Ms. (b)(6)(b)(7)(C) said she remembered this soldier, who she could not immediately recall the name of, having arrived late to Iraq due to being stuck in Kuwait after reportedly testing positive for the H1N1Virus. Ms. (b)(6)(b)(7)(C) said this other soldier, who she believed was a Specialist (Pay Grade E-4), was also very intelligent and into computers. Ms. (b)(6)(b)(7)(C) said she did not believe FOB Hammer had certain capabilities related to cellular phone systems as discussed by PFC MANNING in his Internet chats, based on the remote location of FOB Hammer and lack of need for this capability. Ms. (b)(6)(b)(7)(C) said she had no knowledge of any penetration testing being conducted by any military personnel on any computer networks while at FOB Hammer, and was not aware of the website WikiLeaks.org until this investigation of PFC MANNING was made public. Ms. (b)(6)(b)(7)(C) related she did not have any contact with PFC MANNING while outside of her work environment, but did identify several other personnel who may have worked with PFC MANNING more closely. Ms. (b)(6)(b)(7)(C) identified these personnel as: Senior Airman (SrA) (b)(6)(b)(7)(C) whom she believed may have already ETS'ed; SrA (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) who was in the SIGINT Section and also worked the night shift; U.S. Air Force Senior Master Sergeant (SMSgt) (b)(6)(b)(7)(C) who was the Cryptological Support Team 5 (CST5) NCOIC and also spent time on the night shift; and WO1 (b)(6)(b)(7)(C), who appeared to have knowledge of the physical altercation incident between PFC MANNING and SPC (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) related that she left FOB Hammer in January 2010, and had not interacted with PFC MANNING after her departure.

AGENTS COMMENT: The soldier Ms. (b)(6)(b)(7)(C) identified as having arrived to Iraq later than the rest of his unit after being delayed in Kuwait, is believed to be SPC (b)(6)(b)(7)(C) Ms. (b)(6)(b)(7)(C) identified that in approximately 4 months, she would be redeploying and would be returning to her position at NSA.

// **LAST ENTRY** //

TYPED AGENT'S NAME AND SEQUENCE NUMBER	ORGANIZATION	
SA (b)(6)(b)(7)(C), (b) (7)(E)	Washington Metro RA, Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060	
SIGNATURE (b)(6)(b)(7)(C)	DATE 12 Jul 10	EXHIBIT 83

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER 0028-10-CID221-10117

DETAILS

About 1400, 20 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) and SA (b)(6)(b)(7)(C), (b) (7)(E) both assigned to Washington Metro Resident Agency (WMRA), Computer Crime Investigative Unit (CCIU), Fort Belvoir, VA 22060, interviewed Mr. (b)(6)(b)(7)(C) who related his last contact with PFC MANNING was in May 10, and he confirmed that he had exchanged email communication with PFC MANNING. Mr. (b)(6)(b)(7)(C) related he knows Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) but does not know Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related PFC MANNING did not send him any packages or leave anything with him, and he does not know if PFC MANNING sent any packages to any other people, or had any safety deposit boxes or storage facilities in the Boston area. Mr. (b)(6)(b)(7)(C) related he believes PFC MANNING stored all of his important information on his laptop computer and primarily utilized the following accounts, Gmail (bradley.e.manning@gmail.com) and Facebook. Mr. (b)(6)(b)(7)(C) related he was not a U.S. Citizen, however, he stated he had his green card.

About 0915, 23 Jun 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) Diplomatic Security Service (DSS), U.S. Department of State (DoS), Boston, MA 02222, interviewed Mr. (b)(6)(b)(7)(C) in the presence of Mr. (b)(6)(b)(7)(C) attorney, Mr. (b)(6)(b)(7)(C) Nelson Mullins Riley & Scarborough LLP, One Boston Place, Boston, MA 02108, in a conference room at Mr. (b)(6)(b)(7)(C) office. Mr. (b)(6)(b)(7)(C) related he first met PFC MANNING in person, about Jan 09, when he picked him up at the Hancock International Airport in Syracuse, NY, while PFC MANNING was travelling on leave. Mr. (b)(6)(b)(7)(C) related at the time he knew PFC MANNING was in the U.S. Army; however, Mr. (b)(6)(b)(7)(C) was unaware of PFC MANNING's occupation as an intelligence analyst. Mr. (b)(6)(b)(7)(C) related he and PFC MANNING had previously chatted online via an online chat/dating service, but later used AOL Instant Messenger (AIM) to chat, and Skype to speak. Mr. (b)(6)(b)(7)(C) related when they initially met, PFC MANNING had a Toshiba laptop with him that was stolen during a subsequent trip to Boston, MA, in 2009; however, PFC MANNING subsequently purchased a MacBook Pro, which he did not receive until after Sep 09. Mr. (b)(6)(b)(7)(C) related after meeting he began dating PFC MANNING, but moved to Boston to attend Brandeis University, and PFC MANNING subsequently traveled to Boston around Feb or Mar 09; in May 09; and about three other weekends during the summer of 2009, in order to visit Mr. (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related after moving to Boston he met Mr. (b)(6)(b)(7)(C) around Mar 09, and developed a friendship with him, and late during the summer of 2009, Mr. (b)(6)(b)(7)(C) introduced PFC MANNING to Mr. (b)(6)(b)(7)(C) as he expected they would get along well due to their common interest in computers. Mr. (b)(6)(b)(7)(C) related he knew Mr. (b)(6)(b)(7)(C) and PFC MANNING subsequently became Facebook friends and began chatting. Mr. (b)(6)(b)(7)(C) related in Aug 09, Mr. (b)(6)(b)(7)(C) met PFC MANNING for the first time in Watertown, NY, and in subsequent trips to Boston, PFC MANNING and Mr. (b)(6)(b)(7)(C) would spend time together while Mr. (b)(6)(b)(7)(C) was in class or otherwise unavailable. Mr. (b)(6)(b)(7)(C) was unaware of what Mr. (b)(6)(b)(7)(C) and PFC MANNING did while they were together or where they went. Mr. (b)(6)(b)(7)(C) frequented a living group near Massachusetts Institute of Technology (MIT) called pika, and Mr. (b)(6)(b)(7)(C) believed it was likely Mr. (b)(6)(b)(7)(C) introduced PFC MANNING to other pika participants. Mr. (b)(6)(b)(7)(C) related he stopped dating PFC MANNING in Sep 09, however, continued their friendship and Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) travelled to Fort Drum, NY, to visit PFC MANNING prior to his

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 13 Jul 10
	EXHIBIT 84

DETAILS

deployment to Iraq. During this trip, Mr. (b)(6)(b)(7)(C) recalled he and Mr. (b)(6)(b)(7)(C) traveled to Wal-Mart, just outside of Fort Drum, with PFC MANNING who purchased a Seagate brand 1 or 2 terabyte external hard drive. Mr. (b)(6)(b)(7)(C) related Mr. (b)(6)(b)(7)(C) helped PFC MANNING move his personal items from Fort Drum to Potomac, MD where he believes that Mr. (b)(6)(b)(7)(C) met PFC MANNING's (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) related he believed PFC MANNING used the following accounts: (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) and possibly (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) further related he believed PFC MANNING used Google chat and Facebook chat. Mr. (b)(6)(b)(7)(C) related that he used Skype account (b)(6)(b)(7)(C) and email account (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) was unaware of any storage facilities PFC MANNING had or used. Mr. (b)(6)(b)(7)(C) believed PFC MANNING stored some of his belongings with (b)(6)(b)(7)(C) NFI, the wife of one of PFC MANNING's (b)(6)(b)(7)(C) Mr. (b)(6)(b)(7)(C) stated his computer was password protected, and he never provided PFC MANNING the password. Mr. (b)(6)(b)(7)(C) related he gave PFC MANNING access to his computer for simple tasks such as checking the weather or scheduling trips. PFC MANNING used his own computer when he was doing other tasks. Mr. (b)(6)(b)(7)(C) related PFC MANNING never sent Mr. (b)(6)(b)(7)(C) encrypted emails; however, PFC MANNING did try to send Mr. (b)(6)(b)(7)(C) his PGP key, but Mr. (b)(6)(b)(7)(C) was unable to use it. Mr. (b)(6)(b)(7)(C) related PFC MANNING used long, complicated passwords, and he could not recall any of the passwords he used. Mr. (b)(6)(b)(7)(C) stated he never used PFC MANNING's computer. Mr. (b)(6)(b)(7)(C) related in Jan 10, while PFC MANNING was in Boston, he asked Mr. (b)(6)(b)(7)(C) how he would handle it if he knew or saw something bad or wrong. Mr. (b)(6)(b)(7)(C) related PFC MANNING spent a substantive amount of time with Mr. (b)(6)(b)(7)(C) during his trip to Boston in Jan 10. Mr. (b)(6)(b)(7)(C) related PFC MANNING never mentioned classified material. Mr. (b)(6)(b)(7)(C) related he did not know Mr. (b)(6)(b)(7)(C) and that PFC MANNING did not mail anything to him or leave anything at his residence, other than a shirt.

About 1430, 23 Jun 10, SA (b)(6)(b)(7)(C) received an access log from SA (b)(6)(b)(7)(C) which detailed Mr. (b)(6)(b)(7)(C) access to Metropolitan Moving and Storage Unit, number 0354, 134 Massachusetts Avenue, Cambridge, MA 02139. The access log detailed Mr. (b)(6)(b)(7)(C) access dates for Jul 09 - May 10, revealing a last accessed date of 25 May 10. SA (b)(6)(b)(7)(C) related the address on file for the unit matched the address pertaining to Mr. (b)(6)(b)(7)(C) in the state of Washington. SA (b)(6)(b)(7)(C) related the management did not have a record of storage units for Mr. (b)(6)(b)(7)(C) PFC (b)(6)(b)(7)(C) or Mr. (b)(6)(b)(7)(C)

AGENT'S COMMENT: A preliminary examination of PFC MANNING's personal computer identified an email sent on May 20, 2010, from (b)(6)(b)(7)(C) to Mr. (b)(6)(b)(7)(C) in which Mr. (b)(6)(b)(7)(C) and PFC MANNING (b)(6)(b)(7)(C) were Carbon Copied (CC). The email discussed the security of storage facilities and whether anyone was renting one. In the email Mr. (b)(6)(b)(7)(C) indicated he was a renting storage at Metropolitan Moving and Storage, 134 Massachusetts Avenue, Cambridge, MA 02139.

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: 13 Jul 10 / EXHIBIT: 84

DETAILS

About 1530, 21 Jun 10, this office received the response to Search Warrant, 10-330-M-01, issued by the U.S. District Court, District of Columbia, for all records, stored email, and electronic file storage associated with the (b)(6)(b)(7)(C) @gmail.com. (See Search Warrant)

About 1221, 24 Jun 10, SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, collected as evidence one compact disc (CD), which contained the results of the Search Warrant, 10-330-M-01, for the contents of PFC MANNING's Gmail account, (b)(6)(b)(7)(C) @gmail.com, from Gmail via FedEx, tracking number 9590 2760 8044, which was documented on Evidence/Property Custody Document (EPCD), Document Number (DN) 089-10.

About 1820, 24 Jun 10, SA (b)(6)(b)(7)(C) SA (b)(6)(b)(7)(C) and SA (b)(6)(b)(7)(C) interviewed Mr. (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) who related the purpose of his cooperation with this interview was to defame Mr. (b)(6)(b)(7)(C) as a witness, and to avoid anything that may further incriminate PFC MANNING. Mr. (b)(6)(b)(7)(C) related he first met PFC MANNING around Jan or Feb 10. Mr. (b)(6)(b)(7)(C) related he felt what PFC MANNING had done was noble, and that he felt all information should be freely available. Mr. (b)(6)(b)(7)(C) related he had talked to Mr. (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) concerning the investigation of PFC MANNING. Mr. (b)(6)(b)(7)(C) related PFC MANNING sent him an email with his PGP key, and requested that he communicate via PGP encrypted emails. Mr. (b)(6)(b)(7)(C) declined PFC MANNING's request for encrypted email exchange. Mr. (b)(6)(b)(7)(C) related that in his experience, if someone wants to communicate via encrypted channels, they would likely be disseminating sensitive information that may have repercussions. Mr. (b)(6)(b)(7)(C) related he did not like to discuss that type of information over electronic communication, and that he would only discuss that type of information in private, face to face. Mr. (b)(6)(b)(7)(C) related while PFC MANNING was in the Boston area; he attended a Free Software Foundation event. Mr. (b)(6)(b)(7)(C) related he did not know Mr. Julian P. ASSANGE, founder and Director of WikiLeaks, Townsville, Queensland, AU, personally, and had never communicated with him directly; however, Mr. (b)(6)(b)(7)(C) commented that WikiLeaks was not well organized and that Mr. ASSANGE had little control over all associates or editors assisting WikiLeaks in the disclosure of classified information.

About 1645, 25 Jun 10, SA (b)(6)(b)(7)(C) and Mr. (b)(6)(b)(7)(C) Forensic Examiner, Digital Forensic and Research Branch (DFRB), CCIU, Fort Belvoir, VA 22060, examined the MBOX file collected on EPCD, DN 089-10, which was provided by Google, Inc., in response to Search Warrant, 10-330-M-01, in regard to the email account of (b)(6)(b)(7)(C) @gmail.com. A keyword search was conducted based on the keywords listed in the Search Warrant. SA (b)(6)(b)(7)(C) extracted messages which contained any of the searched keywords and collected these messages as evidence, which were document on an EPCD, DN 091-10.

About 1501, 28 Jun 10, SA (b)(6)(b)(7)(C) collected as evidence the files: "bradley.e.manning.pdf", "bradley.e.manning@gmail.com.vcard", "bradley.e.manning_preserved.pdf", and "bradley.e.manning@gmail.com_preserved.vcard", which contained the log files and address book

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	
SIGNATU (b)(6)(b)(7)(C)	DATE 13 Jul 10	EXHIBIT 84

DETAILS

information related to the Gmail account of "(b)(6)(b)(7)(C) gmail.com", from the CD provided by Google in response to Search Warrant, 10-330-M-01, which was document on an EPCD, DN 092-10.

About 1330, 1 Jul 10, SA (b)(6)(b)(7)(C) reviewed the IP logs obtained as part of the Google search warrant on PFC MANNING's Gmail account. The logs revealed 10 IP addresses that accessed PFC MANNING's Gmail account between 4 May 10 and 28 May 10. Five of the IP addresses were registered to Horizon Satellite Services, United Arab Emirates; two were registered to Earthlink, Iraq; one was registered to the DoD network; and one was registered to IABG mbH, Germany.

About 0810, 6 Jul 10, SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, CCIU, Fort Belvoir, VA 22060, received the results of the Department of Defense, Office of Inspector General DoDIG subpoena, 2010233-10427, from AOL for the AOL Instant Messenger (AIM) account (b)(6)(b)(7)(C) via facsimile. The account was created 15 Dec 08, with the following registration information: email address (b)(6)(b)(7)(C) @brandeis.edu, (b)(6)(b)(7)(C) (b)(6)(b)(7)(C) (See Subpoena)

About 1040, 6 Jul 10, SA (b)(6)(b)(7)(C) received the results of the DoDIG subpoena, 2010233-10431, from Microsoft for the MSN Hotmail account (b)(6)(b)(7)(C)@hotmail.co.uk" via Email in a password protected Zip file. The account was registered to (b)(6)(b)(7)(C) and was registered on 10 Sep 08 from IP address 81.109.149.110. (See Subpoena)

About 1410, 6 Jul 10, SA (b)(6)(b)(7)(C) received the results of the DoDIG subpoena, 2010233-10430, from Microsoft for the MSN Hotmail account (b)(6)(b)(7)(C)@hotmail.com". The results from Microsoft stated that no such account existed. (See Subpoena)

About 0935, 7 Jul 10, SA (b)(6)(b)(7)(C) eceived the results of the DoDIG subpoena, 2010233-10432, from Microsoft for the MSN Hotmail account (b)(6)(b)(7)(C)@hotmail.com" via Email in a password protected Zip file. The account was registered to (b)(6)(b)(7)(C) and was registered on 14 Mar 10 from IP address 82.205.133.7. (See Subpoena)

About 1120, 9 Jul 10, SA (b)(6)(b)(7)(C) received the results of DoDIG subpoena, 2010247-10457, from Skype Communications Sarl for the Skype accounts (b)(6)(b)(7)(C) bradley.e.manning and bradley.manning. The records contained 5 Excel spreadsheets showing registration information, detailed call logs and instant message (IM) information. (See Subpoena)

About 1300, 9 Jul 10, SA (b)(6)(b)(7)(C) received the results of the following subpoenas results via facsimile:

2010233-10424 from AOL for the AIM account (b)(6)(b)(7)(C) The account was created 19 Nov 06, with the following registration information: email address (b)(6)(b)(7)(C) @pobox.com, (b)(6)(b)(7)(C) (See Subpoena)

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 13 Jul 10	EXHIBIT 84

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

	LOI NUMBER 0028-10-CID221-10117
	PAGE 5 OF 5 PAGES

DETAILS

2010233-10425 from AOL for the AIM account (b)(6)(b)(7)(C) The account was created 10 Feb 99, with the following registration information: email address (b)(6)(b)(7)(C)@pobox.com. (See Subpoena)

2010233-10426 from AOL for the AIM account leboheme1115. The account was created 11 Oct 02, with the following registration information: email address (b)(6)(b)(7)(C)@nerdparadise.zzn.com, DOB 17 Apr 86. (See Subpoena)

About 1030, 13 Jul 10, SA (b)(6)(b)(7)(C), (b) (7)(E) WMRA, Fort Belvoir, VA 22060, collected as evidence one Seagate Baracuda hard drive, model number ST3400832AS, serial number 3NF0DXW3, 400 GB in capacity, containing images of hard drives collected as evidence from Mr. (b)(6)(b)(7)(C) on EPCD DN 0076-10 and 0077-10, from the forensic computer, which was documented on EPCD, DN 095-10.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER SA (b)(6)(b)(7)(C), (b) (7)(E)	ORGANIZATION Computer Crime Investigative Unit U.S. Army CID, Fort Belvoir, VA 22060
SIGNATURE (b)(6)(b)(7)(C)	DATE: 13 Jul 10 / EXHIBIT: 84

Exhibit(s) 85

Page(s) 000454 thru 000466

Documents

SEALED

by the

U.S. District Court
for the Northern District of California

Exhibit 86 thru 93

Page(s) 000467 thru 000664 referred to:

Department of Defense

Office of Inspector General
DoD IG FOIA Requester Service Center
4800 Mark Center Drive – Suite 14L24
Alexandria, VA 22350-1500