Exhibit(s) 456

Page(s) 017270 thru 017270aaaa
withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 457

Page(s) 017271 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 458

Page(s) 017272 thru 017272vvv
withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 459

Page(s) 017273 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 460

Page(s) 017274 thru 017274m withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 461

Page(s) 017275 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 462

Page(s) 017276 thru 017276f withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 463

Page(s) 017277 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 464

Page(s) 017278 thru 017278l withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 465

Page(s) 017279 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 466

Page(s) 017280 thru 017280dd
withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 467

Page(s) 017281 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 468

Page(s) 017282 thru 017282i withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 469

Page(s) 017283 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 470

Page(s) 017284 thru 017284m withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 471

Page(s) 017285 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

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

REPLY TO
ATTENTION OF

CISA-CCI-DF

22 Sep 11

1. (U) **Case Number**: CAF# 0028-10-CID361 / ROI# 0028-10-CID221-10117

2. (U) **Investigating Office**: Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134

3. (U) **Date of Report**: 22 Sep 11

4. (U) **Examiner**: SAC (b)(6)(b)(7)(C), (b) (7)(E)

5. (U//FOUO) **Summary of Analysis**: Examination of the U.S. Army SIPRNET computer assigned IP 22.225.28.216 and primarily utilized by SPC (b)(6)(b)(7)(C) (a coworker of PFC MANNING) disclosed the following:

A) (U) Examination of the file `C:\Document and Settings\`(b)(6)(b)(7)(C) `\`(b)(6)(b)(7)(C)`.pst` revealed an incoming email dated 28 May 10 sent from an HP Digital Sender scanner device, which contained a scanned DA Form 268, Report to Suspend Favorable Personnel Actions (Flag), pertaining to PFC Bradley MANNING.

Exhibit 472

TABLE OF CONTENTS

Exhibit 472

1. (U) Case Number:

(U) CAF# 0028-10-CID361 / ROI# 0028-10-CID221-10117

2. (U) Investigating Office:

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

3. (U) Date of Report:

(U) 22 Sep 11

4. (U) Examiner:

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

5. (U) Definitions of Technical Terms:

5.1 (U) Internet Protocol (IP) Address:

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

5.2 (U) Message Digest-5 (MD5):

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

5.3 (U) Secure Hash Algorithm-1 (SHA-1):

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

Exhibit 472

6. (U) Analysis:

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

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

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

6.1 (U) Examination of the hard disk drive (HDD), Serial Number Z5FX1422S 6P2 EC A:

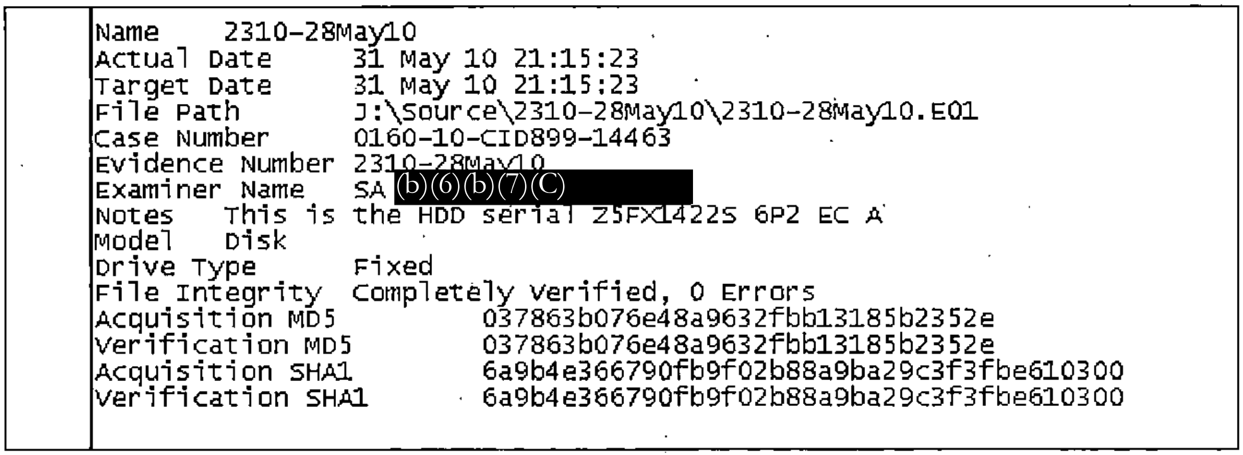
(U//FOUO) Examination of the HDD removed from the primary SIPRNET computer of SPC (b)(6)(b)(7)(C) (coworker of PFC MANNING) revealed it had the Microsoft XP Professional operating system, installed at 17:24:19, 5 May 08. It was assigned the computer name S2D10MTNBDE840 and IP 22.225.28.216.

Encase File Name	2310-28May10
Operating System Installed	05 May 08 17:24:19
IP address	22.225.28.216
Operating System	Microsoft Windows XP (SP2)
Computer Name	S2D10MTNBDE840
Time Zone	(GMT+03:00) Baghdad
Domain	2BCT10MTN (Primary)
Date bradley.manning first logged on	N/A
Date bradley.manning last logged off	N/A
Number of times bradley.manning logged on	N/A

(U) Figure 1 - System information for SPC (b)(6)(b)(7)(C) primary SIPRNET computer

Exhibit 472

6.1.1 (U) Imaging:



```
Name    2310-28May10
Actual Date      31 May 10 21:15:23
Target Date      31 May 10 21:15:23
File Path        J:\Source\2310-28May10\2310-28May10.E01
Case Number      0160-10-CID899-14463
Evidence Number  2310-28May10
Examiner Name    SA (b)(6)(b)(7)(C)
Notes    This is the HDD serial Z5FX1422S 6P2 EC A
Model    Disk
Drive Type       Fixed
File Integrity   Completely Verified, 0 Errors
Acquisition MD5          037863b076e48a9632fbb13185b2352e
Verification MD5         037863b076e48a9632fbb13185b2352e
Acquisition SHA1         6a9b4e366790fb9f02b88a9ba29c3f3fbe610300
Verification SHA1        6a9b4e366790fb9f02b88a9ba29c3f3fbe610300
```

(U) Figure 2 - Imaging and verification data for HDD, serial number Z5FX1422S 6P2 EC A

6.1.2 (U) Time Zone information:

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

6.1.3 (U) Voucher Information:

(U) Item 1, EPCD DN 070-10.

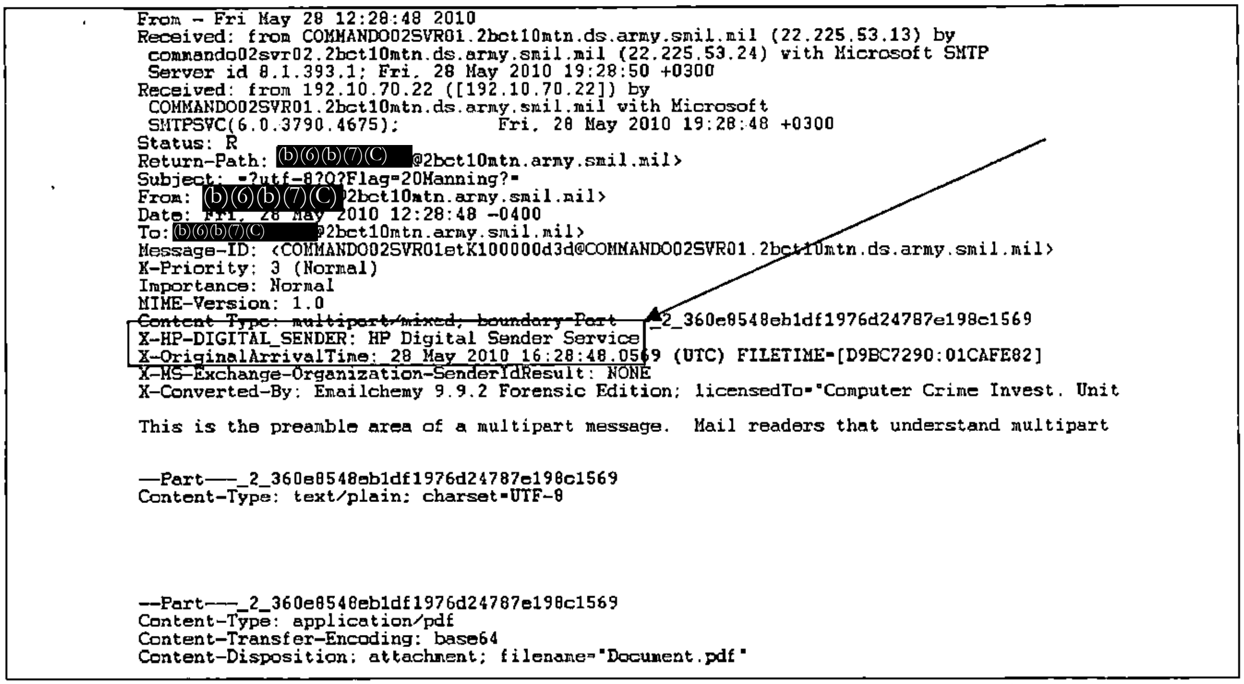
6.1.4 (U) A review of the HDD using Anti-Virus:

(U) The examined HDD was scanned using Symantec Endpoint Protection Version 11.0.4000.2295 with Definitions dated June 09, 2010 r22. No malicious files were located.

6.1.5 (U) Examination of the file `C:\Document and Settings \(b)(6)(b)(7)(C) pst`:

(U) Examination of the file `C:\Document and Settings\(b)(6)(b)(7)(C) \(b)(6)(b)(7)(C) pst` revealed an incoming email (excerpt shown in Figure 3 below) dated 28 May 10, received from an HP Digital Sender scanning device, which contained a scanned DA Form 268, Report to Suspend Favorable Personnel Actions (Flag), pertaining to PFC MANNING (shown in Figure 4 below). See Attachment A on Enclosure 1 to this report for the complete file. The email was sent to SPC(b)(6)(b)(7)(C)on 28 May 10, was delivered to her email box, and was deleted on and known date. This message was recovered from SPC(b)(6)(b)(7)(C)deleted email folder.

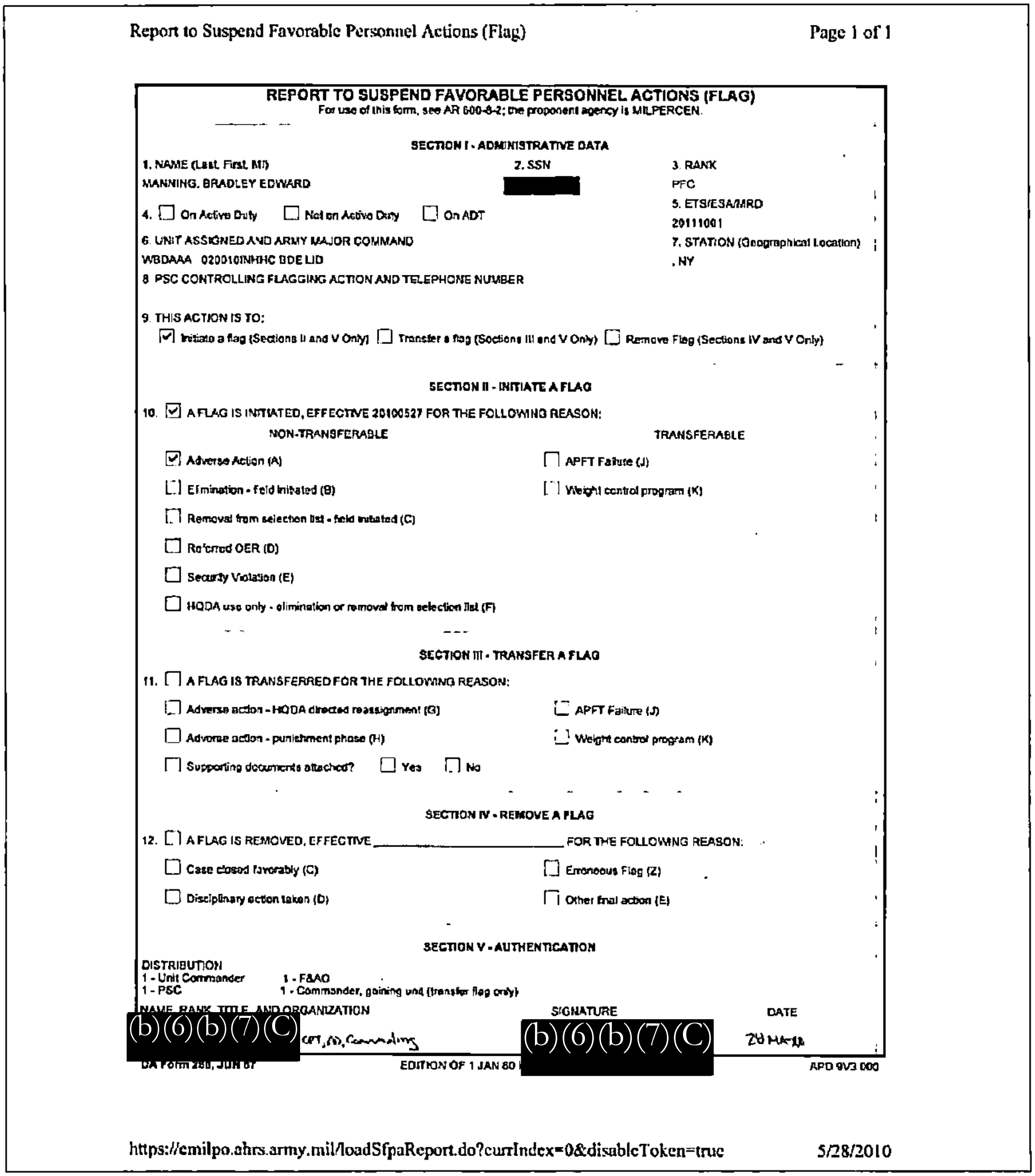
Exhibit 472



```
From - Fri May 28 12:28:48 2010
Received: from COMMANDO02SVR01.2bct10mtn.ds.army.smil.mil (22.225.53.13) by
 commando02svr02.2bct10mtn.ds.army.smil.mil (22.225.53.24) with Microsoft SMTP
 Server id 8.1.393.1; Fri, 28 May 2010 19:28:50 +0300
Received: from 192.10.70.22 ([192.10.70.22]) by
 COMMANDO02SVR01.2bct10mtn.ds.army.smil.mil with Microsoft
 SMTPSVC(6.0.3790.4675);         Fri, 28 May 2010 19:28:48 +0300
Status: R
Return-Path: (b)(6)(b)(7)(C)@2bct10mtn.army.smil.mil>
Subject: =?utf-8?Q?Flag=20Manning?=
From: (b)(6)(b)(7)(C)2bct10mtn.army.smil.mil>
Date: Fri, 28 May 2010 12:28:48 -0400
To: (b)(6)(b)(7)(C)@2bct10mtn.army.smil.mil>
Message-ID: <COMMANDO02SVR01etK100000d3d@COMMANDO02SVR01.2bct10mtn.ds.army.smil.mil>
X-Priority: 3 (Normal)
Importance: Normal
MIME-Version: 1.0
Content Type: multipart/mixed; boundary=Part ___2_360e8548eb1df1976d24787e198c1569
X-HP-DIGITAL_SENDER: HP Digital Sender Service
X-OriginalArrivalTime: 28 May 2010 16:28:48.0569 (UTC) FILETIME=[D9BC7290:01CAFE82]
X-MS-Exchange-Organization-SenderIdResult: NONE
X-Converted-By: Emailchemy 9.9.2 Forensic Edition; licensedTo="Computer Crime Invest. Unit

This is the preamble area of a multipart message.  Mail readers that understand multipart


—Part——_2_360e8548eb1df1976d24787e198c1569
Content-Type: text/plain; charset=UTF-8




--Part——_2_360e8548eb1df1976d24787e198c1569
Content-Type: application/pdf
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Document.pdf"
```

(U//FOUO) Figure 3 - Email message header for an email sent to (b)(6)(b)(7)(C)@bct10mtn.army.smil.mil from an HP Digital Sender scanning device (box and arrow added by the exmainer for emphasis)

Exhibit 472



Report to Suspend Favorable Personnel Actions (Flag) Page 1 of 1

REPORT TO SUSPEND FAVORABLE PERSONNEL ACTIONS (FLAG)
For use of this form, see AR 600-8-2; the proponent agency is MILPERCEN.

SECTION I - ADMINISTRATIVE DATA

1. NAME (Last, First, MI)
MANNING, BRADLEY EDWARD

2. SSN
[redacted]

3. RANK
PFC

4. □ On Active Duty □ Not on Active Duty □ On ADT

5. ETS/ESA/MRD
20111001

6. UNIT ASSIGNED AND ARMY MAJOR COMMAND
WBDAAA 0200101NHHC BDE LID

7. STATION (Geographical Location)
, NY

8. PSC CONTROLLING FLAGGING ACTION AND TELEPHONE NUMBER

9. THIS ACTION IS TO:
☑ Initiate a flag (Sections II and V Only) □ Transfer a flag (Sections III and V Only) □ Remove Flag (Sections IV and V Only)

SECTION II - INITIATE A FLAG

10. ☑ A FLAG IS INITIATED, EFFECTIVE 20100527 FOR THE FOLLOWING REASON:

NON-TRANSFERABLE

☑ Adverse Action (A)
□ Elimination - Field initiated (B)
□ Removal from selection list - field initiated (C)
□ Referred OER (D)
□ Security Violation (E)
□ HQDA use only - elimination or removal from selection list (F)

TRANSFERABLE

□ APFT Failure (J)
□ Weight control program (K)

SECTION III - TRANSFER A FLAG

11. □ A FLAG IS TRANSFERRED FOR THE FOLLOWING REASON:

□ Adverse action - HQDA directed reassignment (G) □ APFT Failure (J)
□ Adverse action - punishment phase (H) □ Weight control program (K)
□ Supporting documents attached? □ Yes □ No

SECTION IV - REMOVE A FLAG

12. □ A FLAG IS REMOVED, EFFECTIVE ______________ FOR THE FOLLOWING REASON:

□ Case closed favorably (C) □ Erroneous Flag (Z)
□ Disciplinary action taken (D) □ Other final action (E)

SECTION V - AUTHENTICATION

DISTRIBUTION
1 - Unit Commander 1 - F&AO
1 - PSC 1 - Commander, gaining unit (transfer flag only)

NAME, RANK, TITLE, AND ORGANIZATION	SIGNATURE	DATE
(b)(6)(b)(7)(C) CPT, IN, Commanding	(b)(6)(b)(7)(C)	28 May 10

DA Form 268, JUN 87 EDITION OF 1 JAN 80 (b)(6)(b)(7)(C) APD 9V3 000

https://emilpo.ahrs.army.mil/loadSfpaReport.do?currIndex=0&disableToken=true 5/28/2010

(U) Figure 4 - PFC MANNING's flag paperwork (SSN masked by the examiner to protect PII)

7. (U) Non-Lead Observations:

(U) None.

8. (U) Summary of Examination:

(U//FOUO) Examination of the U.S. Army SIPRNETcomputer assigned IP 22.225.28.216 and primarily utilized by SPC (b)(6)(b)(7)(C) (a coworker of PFC MANNING) disclosed the following:

A) (U) Examination of the file `C:\Document and Settings\`(b)(6)(b)(7)(C) `\`(b)(6)(b)(7)(C) `.pst` revealed an incoming email dated 28 May 10 sent from an HP Digital Sender scanner device, which contained a scanned DA Form 268, Report to Suspend Favorable Personnel Actions (Flag), pertaining to PFC Bradley MANNING.

9. (U) Investigative Leads:

(U) None.

10. (U) Evidence Disposition:

(U) All evidence was placed into the evidence room of this office.

REPORT PREPARED \ APPROVED BY:

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

(b)(6)(b)(7)(C)
SPECIAL AGENT IN CHARGE

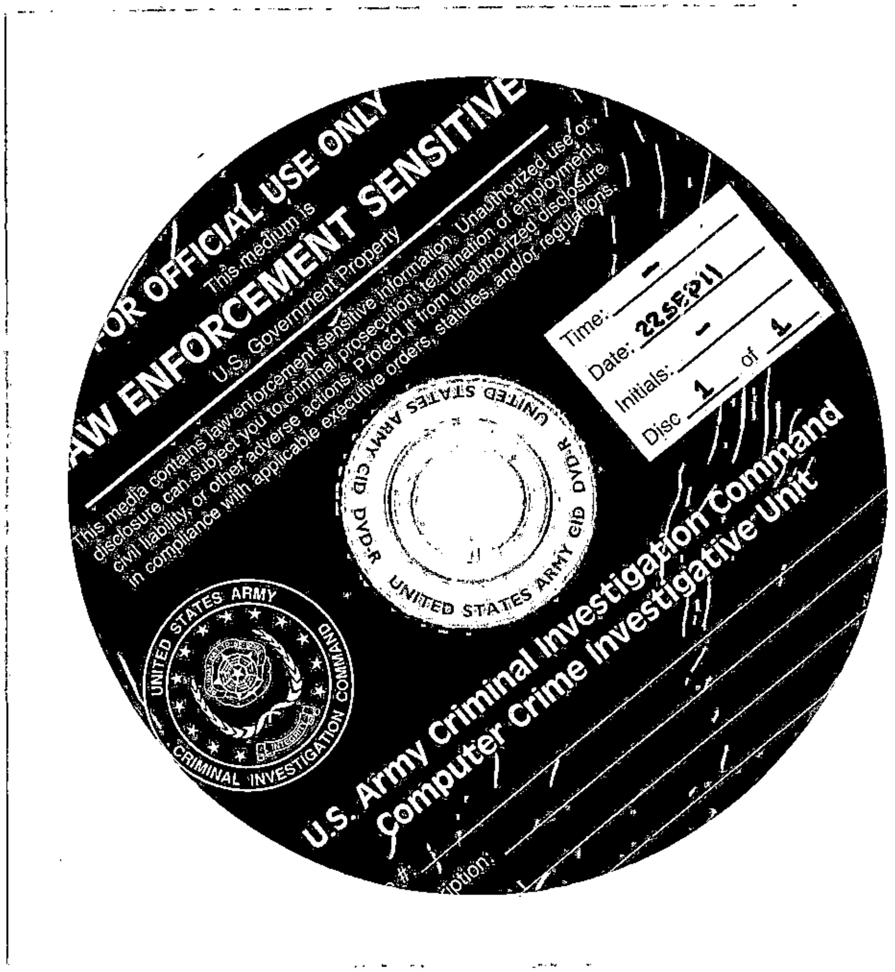
11. (U) Appendices:

(U) Attachment A, Enclosure 1 (*Report to Suspend Favorable Personnel Actions (FLAG) for PFC MANNING* with PII redacted)

Exhibit 472

Forensic Examination Report Date: 22 Sep 11
Forensic Report Author: SSA(b)(6)(b)(7)(C)

ENCLOSURE 1


FOR OFFICIAL USE ONLY
This medium is
LAW ENFORCEMENT SENSITIVE
U.S. Government Property
This media contains law enforcement sensitive information. Unauthorized use or disclosure can subject you to criminal prosecution, termination of employment, civil liability, or other adverse actions. Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and/or regulations.
Time: -
Date: 22SEP11
Initials: -
Disc 1 of 1
UNITED STATES ARMY CID DVD-R
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND
U.S. Army Criminal Investigation Command
Computer Crime Investigative Unit
Description:

REPORT TO SUSPEND FAVORABLE PERSONNEL ACTIONS (FLAG)

For use of this form, see AR 600-8-2; the proponent agency is MILPERCEN.

SECTION I - ADMINISTRATIVE DATA

1. NAME (Last, First, MI) MANNING, BRADLEY EDWARD	2. SSN [redacted]	3. RANK PFC
4. □ On Active Duty □ Not on Active Duty □ On ADT		5. ETS/ESA/MRD 20111001
6. UNIT ASSIGNED AND ARMY MAJOR COMMAND WBDAAA 020010INHHC BDE LID		7. STATION (Geographical Location) , NY

8. PSC CONTROLLING FLAGGING ACTION AND TELEPHONE NUMBER

9. THIS ACTION IS TO:

☑ Initiate a flag (Sections II and V Only) □ Transfer a flag (Sections III and V Only) □ Remove Flag (Sections IV and V Only)

SECTION II - INITIATE A FLAG

10. ☑ A FLAG IS INITIATED, EFFECTIVE 20100527 FOR THE FOLLOWING REASON:

NON-TRANSFERABLE	TRANSFERABLE
☑ Adverse Action (A)	□ APFT Failure (J)
□ Elimination - field initiated (B)	□ Weight control program (K)
□ Removal from selection list - field initiated (C)	
□ Referred OER (D)	
□ Security Violation (E)	
□ HQDA use only - elimination or removal from selection list (F)	

SECTION III - TRANSFER A FLAG

11. □ A FLAG IS TRANSFERRED FOR THE FOLLOWING REASON:

□ Adverse action - HQDA directed reassignment (G)	□ APFT Failure (J)
□ Adverse action - punishment phase (H)	□ Weight control program (K)
□ Supporting documents attached? □ Yes □ No	

SECTION IV - REMOVE A FLAG

12. □ A FLAG IS REMOVED, EFFECTIVE ____________________ FOR THE FOLLOWING REASON:

□ Case closed favorably (C)	□ Erroneous Flag (Z)
□ Disciplinary action taken (D)	□ Other final action (E)

SECTION V - AUTHENTICATION

DISTRIBUTION

1 - Unit Commander	1 - F&AO
1 - PSC	1 - Commander, gaining unit (transfer flag only)

NAME, RANK, TITLE, AND ORGANIZATION	SIGNATURE	DATE
(b)(6)(b)(7)(C) CPT, AD, Commanding	(b)(6)(b)(7)(C)	28 MAY 10

DA Form 268, JUN 87 EDITION OF 1 JAN 80 is APD 9V3.000

Exhibit(s) 474

Page(s) 017296 thru 017296w withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 475

Page(s) 017297 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 476

Page(s) 017298 thru 017298n withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 477

Page(s) <u>017299 </u>withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 478

Page(s) 017300 thru 017300i withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 479

Page(s) 017301 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 480

Page(s) 017302 thru 017302n withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 481

Page(s) 017303 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 482

Page(s) 017304 thru 017304u withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 483

Page(s) 017305 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 484

Page(s) 017306 thru 017306m withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 485

Page(s) 017307 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 486

Page(s) 017308 thru 017308x withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 487

Page(s) 017309 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 488

Page(s) 017310 thru 017310e withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 489

Page(s) 017311 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

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

REPLY TO
ATTENTION OF

CISA-CCI-DF

22 Sep 11

1. (U) **Case Number**: CAF# 0028-10-CID361 / ROI# 0028-10-CID221-10117

2. (U) **Investigating Office**: Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA 22134

3. (U) **Date of Report**: 22 Sep 11

4. (U) **Examiner**: SAC (b)(6)(b)(7)(C), (b) (7)(E)

5. (U) **Summary of Analysis**: Examination of the rewritable compact disc (CD-RW), which was marked SECRET and recovered from the personal quarters of PFC MANNING, FOB HAMMER, Iraq, revealed the following:

A) (U) The CD-RW was located in the back of a case labeled "Starting out in Arabic. All the Arabic you need to get started in a simple audio-only program. 3 Audio CDs. No books necessary" in an apparent attempt to hide the disc.
B) (U) The data on the CD-RW was recorded by a Macintosh computer at 21:03, 27 Apr 10 (GMT+0:00) and contained a partial video (12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv) of an Apache helicopter airstrike.
C) (U) References to the file 12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv found on this CD-RW were also located within 12 different restore points (created between 2 Mar 10 and 7 May 10) linked to the user profile bradley.manning during the previous forensic examination of PFC MANNING's primary SIPRNET computer.

Exhibit 490

TABLE OF CONTENTS

Exhibit 490

1. (U) Case Number:

(U) CAF# 0028-10-CID361 / ROI# 0028-10-CID221-10117

2. (U) Investigating Office:

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

3. (U) Date of Report:

(U) 22 Sep 11

4. (U) Examiner:

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

5. (U) Definitions of Technical Terms:

5.1 (U) Message Digest-5 (MD5):

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

5.2 (U) Restore Point:

(U) A restore point is a Microsoft method to allow a user with administrative privileges on the system to undo changes made to the operating system (such as the installation of a new program or a scheduled backup). Restore points can capture filenames, registry information and file locations in the users accounts. The restore points will usually reside in the hidden, protected System Volume Information folder and are enabled by default for most modern Windows operating systems.

5.3 (U) Secure Hash Algorithm-1 (SHA-1):

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

Exhibit 490

5.4 (U) Security Identifier (SID):

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

6. (U) Analysis:

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

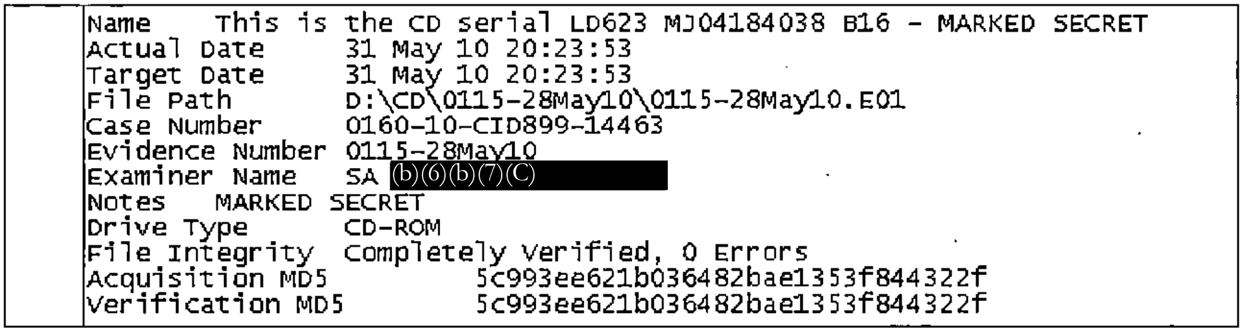
(U) EXAMINER's NOTE: Upon receipt by this office, DN 0585-10 was assigned the local CCIU DN 073-10. These items collected as evidence pertained to PFC Bradley E. MANNING in connection with the following offenses:

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

6.1 (U) Examination of CD-RW, Serial Number LD623 MJ04184038 B16:

(U) Examination of the CD-RW revealed it contained the digital movie file `12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv`.

6.1.1 (U) Imaging:



```
Name    This is the CD serial LD623 MJ04184038 B16 - MARKED SECRET
Actual Date      31 May 10 20:23:53
Target Date      31 May 10 20:23:53
File Path        D:\CD\0115-28May10\0115-28May10.E01
Case Number      0160-10-CID899-14463
Evidence Number  0115-28May10
Examiner Name    SA (b)(6)(b)(7)(C)
Notes    MARKED SECRET
Drive Type       CD-ROM
File Integrity   Completely Verified, 0 Errors
Acquisition MD5          5c993ee621b036482bae1353f844322f
Verification MD5         5c993ee621b036482bae1353f844322f
```

(U) Figure 1 - Imaging and verification data for CD-RW, serial number LD623 MJ04184038 B16

6.2 (U) Time Zone information:

(U) All times shown in this report are in relation to UTC (+0:00 GMT) unless otherwise noted.

6.3 (U) Voucher Information:

(U) Item 6, EPCD DN 067-10.

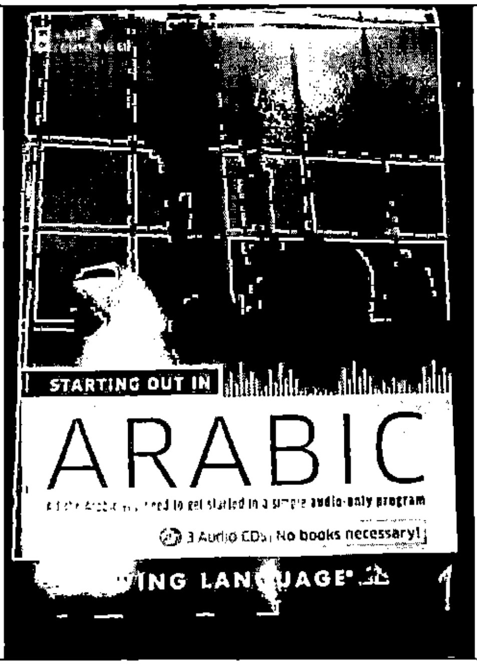
Exhibit 490

6.4 (U) A review of the CD-RW using Anti-Virus:

(U) The examined CD-RW was scanned using Symantec Endpoint Protection Version 11.0.4000.2295 with Definitions dated June 09, 2010 r22. No malicious files were located.

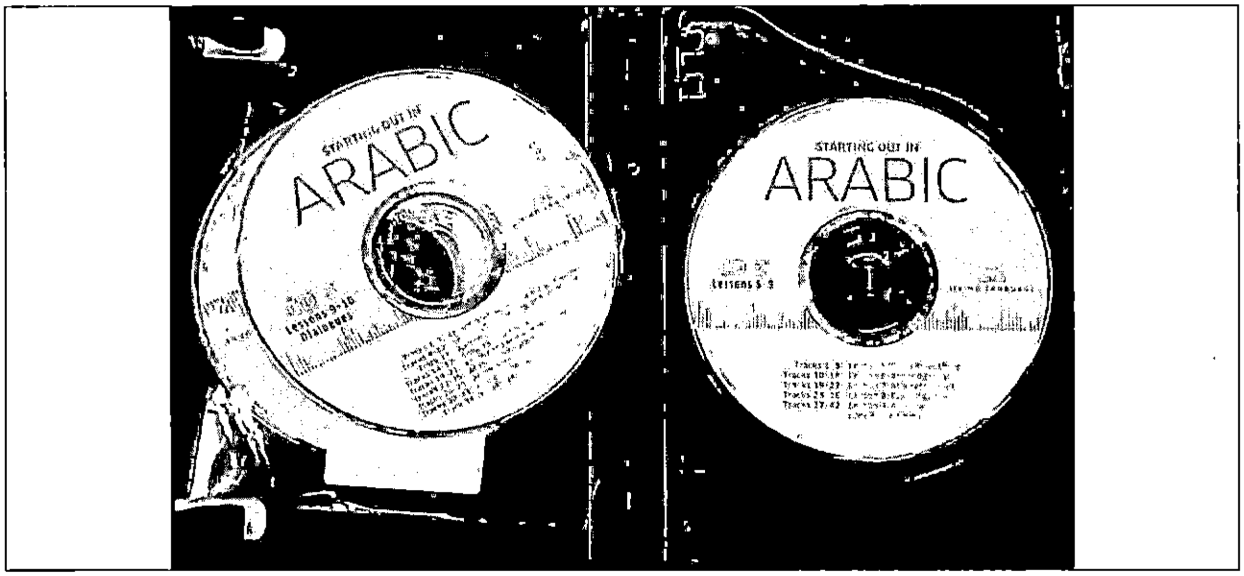
6.5 (U) A visual inspection of Item 6:

(U) A review of Item 6 revealed it was a hard plastic CD case (shown in Figure 2 below) labeled "Starting out in Arabic. All the Arabic you need to get started in a simple audio-only program. 3 Audio CDs. No books necessary!" There were four (4) discs contained within the case, of which three (3) were production audio CDs for learning the Arabic language. The fourth disc (a CD-RW) was placed in this case in an apparent attempt to conceal its true nature (see Figures 2-5 below). SA (b)(6)(b)(7)(C) noted the CD case was located within PFC MANNING's quarters at FOB HAMMER, Iraq.

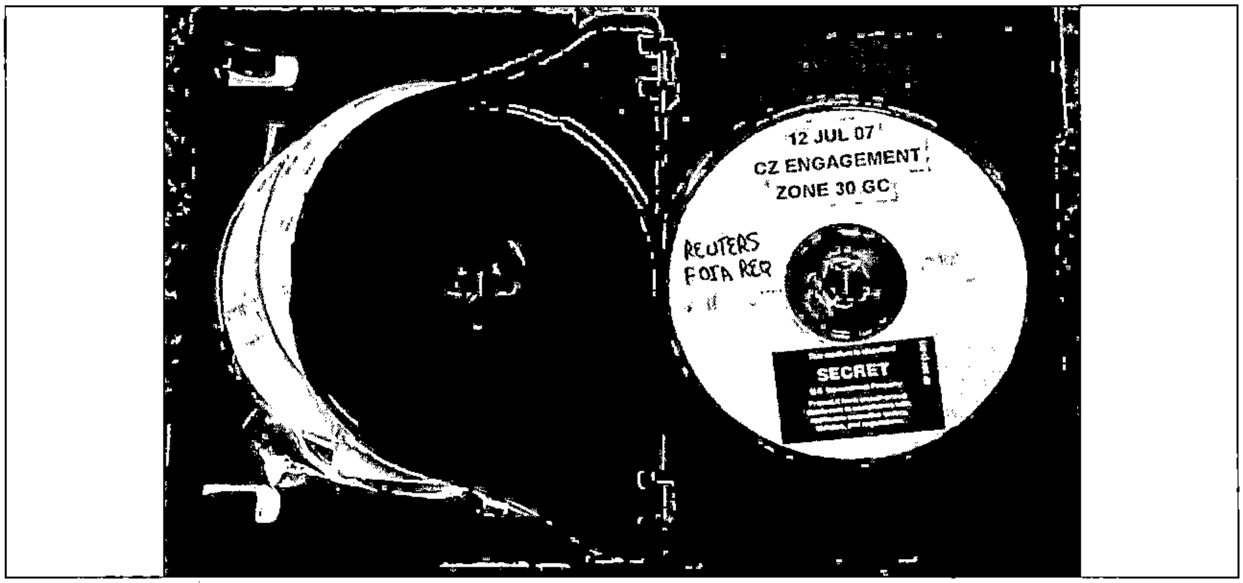


(U) Figure 2 - CD case seized from PFC MANNING's quarters at FOB HAMMER, Iraq

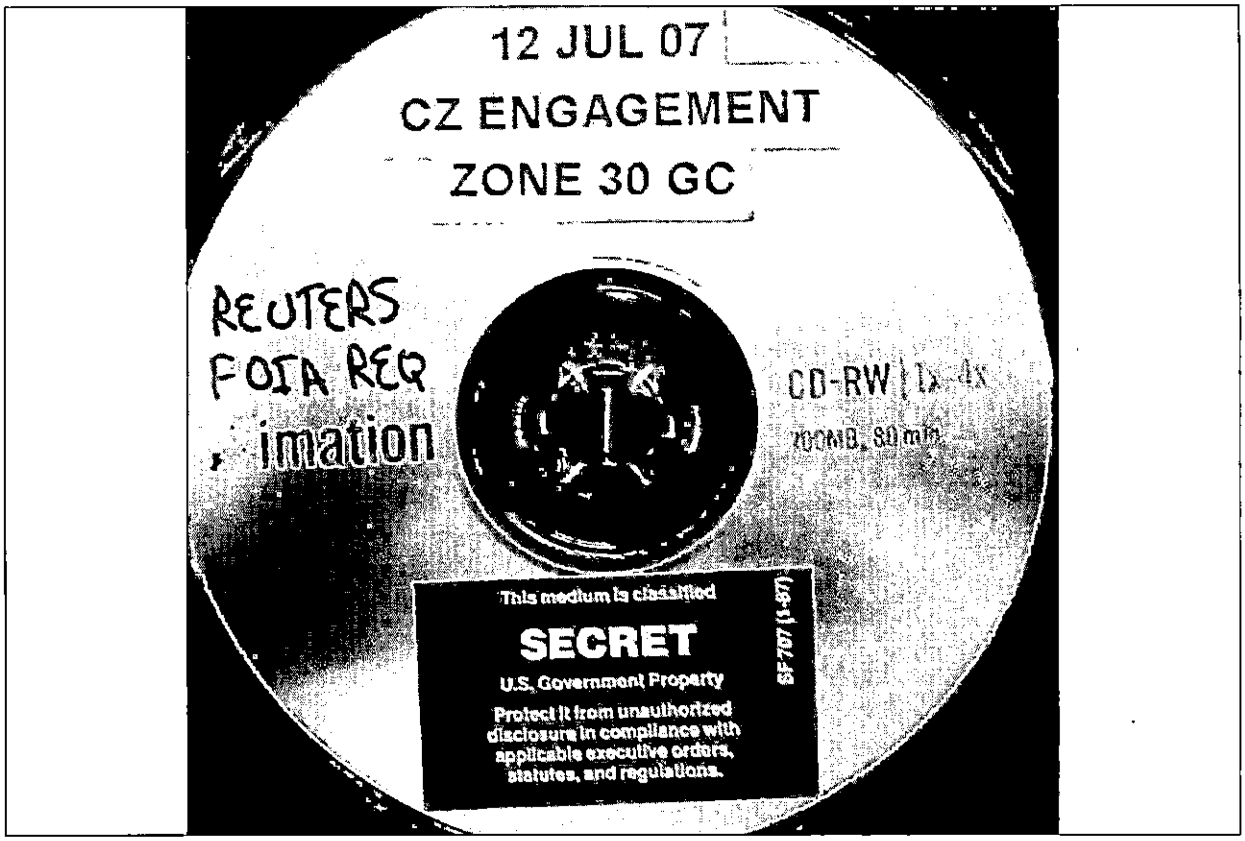
Exhibit 490



(U) Figure 3 - Contents of the CD case seized from PFC MANNING's quarters at FOB HAMMER, Iraq



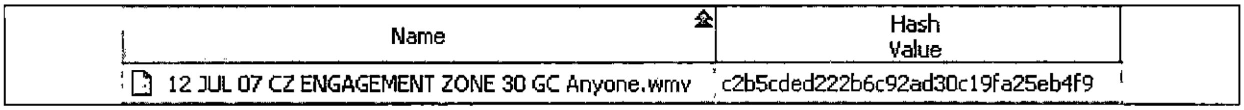
(U) Figure 4 - Contents of the CD case seized from PFC MANNING's quarters at FOB HAMMER, Iraq


12 JUL 07
CZ ENGAGEMENT
ZONE 30 GC
REUTERS
FOIA REQ
imation
CD-RW 1x-4x
700MB, 80 min
This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.
SF 707 (1-87)

(U) Figure 5 - CD-RW containing 12 Jul 07 CZ ENGAGEMENT ZONE GC Anyone.wmv located in the CD case seized from PFC MANNING's quarters at FOB Hammer, Iraq

6.6 (U) Examination of the CD:

(U//FOUO) The data on the CD-RW shown in Figure 5 above was created at 21:03, 27 Apr 10 (GMT+0:00) on a Macintosh computer. The CD-RW was labeled with "12 Jul 07 CZ ENGAGEMENT ZONE 30 GC", handwritten "Reuters FOIA Req" and had a SF 707 (1-87) SECRET sticker applied to its front. Further examination of the CD-RW revealed it contained a Microsoft Windows-format video file called 12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv. Attempts to view the video file revealed it may have been improperly burned to the CD-RW (see Figures 6 through 8). The video file on the CD-RW ended about the 24:28 mark, short of the full 38:21 length of the original video file identified during the previous forensic examination of the U.S. Army computer assigned the IP 22.225.41.22 (PFC MANNING's primary SIPRNET computer). See Attachment A on Enclosure 1 to this report for the full content of the video file found on the CD-RW.

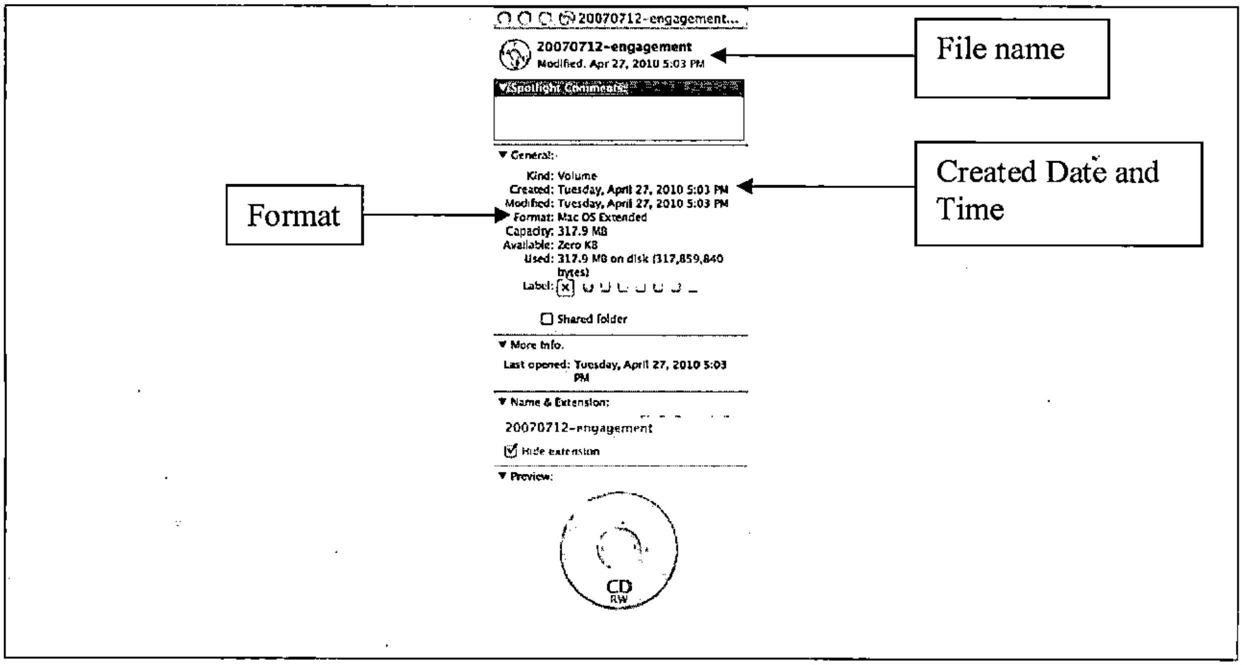


Name	Hash Value
12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	c2b5cded222b6c92ad30c19fa25eb4f9

(U) Figure 6 - Hash value for 12 Jul 07 CZ ENGAGEMENT ZONE GC Anyone.wmv located on the CD-RW

Exhibit 490

(U) Figure 7 - Screenshot from the digital video 12 Jul 07 CZ ENGAGEMENT ZONE GC Anyone.wmv on the CD-RW at the 00:01 minute mark



20070712-engagement...

20070712-engagement
Modified. Apr 27, 2010 5:03 PM

▼Spotlight Comments:

▼ General:

Kind: Volume
Created: Tuesday, April 27, 2010 5:03 PM
Modified: Tuesday, April 27, 2010 5:03 PM
Format: Mac OS Extended
Capacity: 317.9 MB
Available: Zero KB
Used: 317.9 MB on disk (317,859,840 bytes)
Label: ☒

□ Shared folder

▼ More Info.

Last opened: Tuesday, April 27, 2010 5:03 PM

▼ Name & Extension:

20070712-engagement

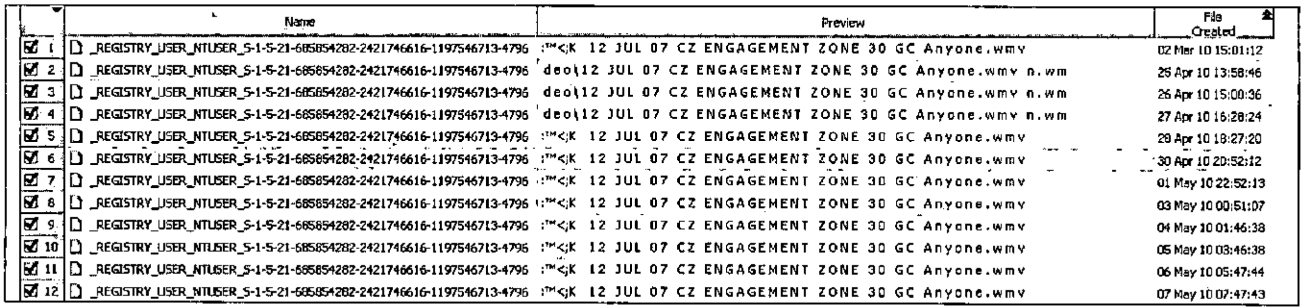
☑ Hide extension

▼ Preview:

(U) Figure 8 - Metadata for the CD-RW

(U//FOUO) EXAMINER's NOTE: References to the file `12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv` found on this CD-RW were also located within 12 different restore points (created between 2 Mar 10 and 7 May 10) linked to the security identifier (SID) for the user profile `bradley.manning` during the previous forensic examination of the U.S. Army computer assigned IP 22.225.41.22 (PFC MANNING's primary SIPRNET computer). (See the forensic report for PFC MANNING's primary SIPRNET computer for details.)

Exhibit 490



	Name	Preview	File Created
☑ 1	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	02 Mar 10 15:01:12
☑ 2	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	deo\12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv n.wm	25 Apr 10 13:58:46
☑ 3	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	deo\12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv n.wm	26 Apr 10 15:00:36
☑ 4	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	deo\12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv n.wm	27 Apr 10 16:28:24
☑ 5	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	28 Apr 10 18:27:20
☑ 6	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	30 Apr 10 20:52:12
☑ 7	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	01 May 10 22:52:13
☑ 8	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	03 May 10 00:51:07
☑ 9	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	04 May 10 01:46:38
☑ 10	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	05 May 10 03:46:38
☑ 11	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	06 May 10 05:47:44
☑ 12	_REGISTRY_USER_NTUSER_S-1-5-21-685854282-2421746616-1197546713-4796	:™<;K 12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv	07 May 10 07:47:43

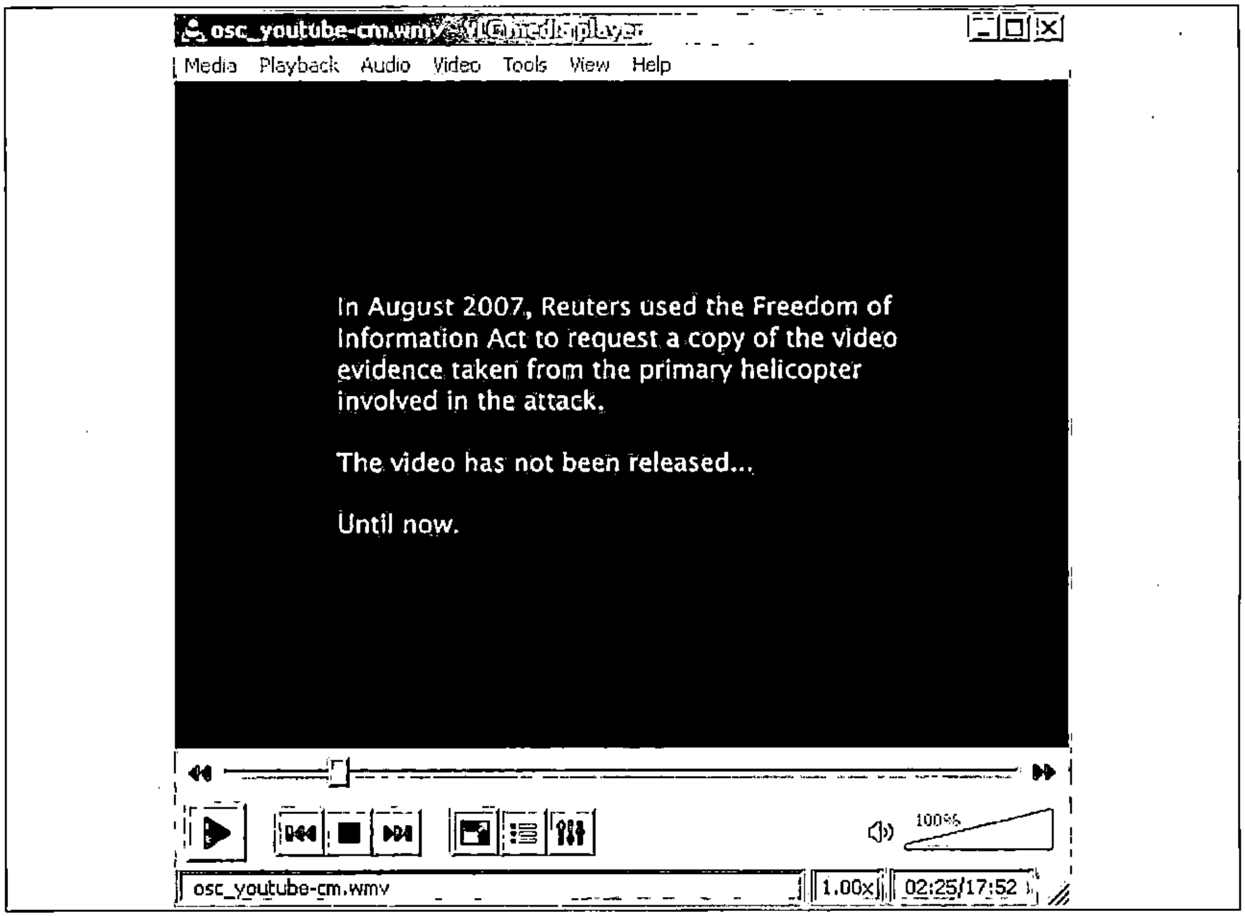
(U//FOUO) Figure 9 - The file 12 Jul 07 CZ ENGAGEMENT ZONE GC Anyone.wmv present on PFC MANNING's primary SIPRNET computer

6.7 (U) International news agency Thomson Reuters:

(U) Handwritten portions of the CD-RW label stated "REUTERS FOIA REQ," which appeared to indicate this CD-RW was destined for the Reuters news service pursuant to a Freedom of Information Act (FOIA) request. It is unknown whether such a request was ever made by international news agency Thomson Reuters, but the screenshot shown in Figure 10 below (from the 2:25 mark within the "Collateral Murder" video) specifically mentioned the news service.

(U//FOUO) EXAMINER's NOTE: A movie similar to the one located on this CD-RW was the basis for the movie "Collateral Murder", which was created by Wikileaks.org. The movie in Figure 10 below (`osc_youtube-CM.wmv`) was located within the user profile of PFC MANNING during the previous forensic examination of the U.S. Army computer assigned IP 22.225.41.22 (PFC MANNING's primary SIPRNET computer).

Exhibit 490


osc_youtube-cm.wmv - VLC media player
Media Playback Audio Video Tools View Help
100%
osc_youtube-cm.wmv
1.00x
02:25/17:52

In August 2007, Reuters used the Freedom of Information Act to request a copy of the video evidence taken from the primary helicopter involved in the attack.

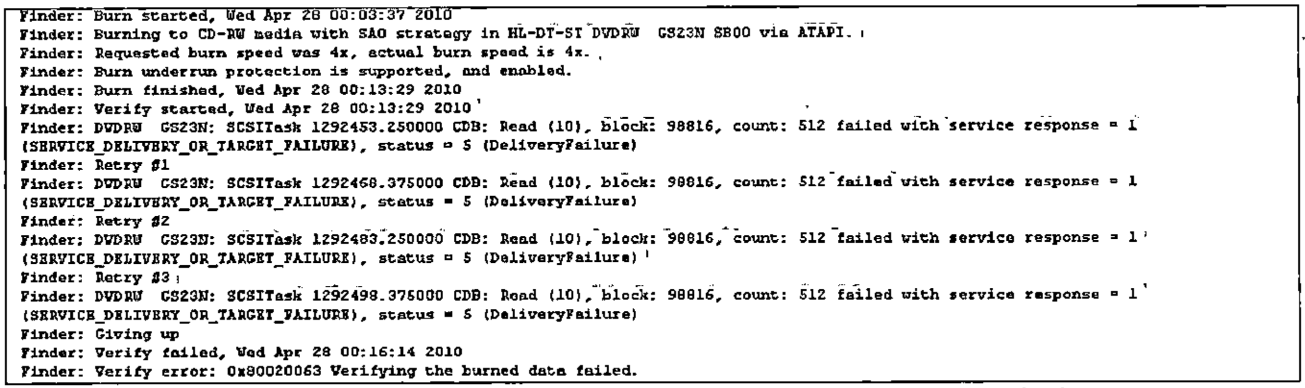
The video has not been released...

Until now.

(U) Figure 10 - Screenshot from the "Collateral Murder" video (osc_youtube-cm.wmv) at minute mark 2:25

6.8 (U) Previous forensic examination of PFC MANNING's personal Macintosh computer:

(U) Previous forensic examination of PFC MANNING's personal Macintosh computer (users\bmanning\Library\Logs\DiscRecording.log) revealed a CD-RW was burned at 00:03, 28 Apr 10 (GMT+3:00) and the CD-RW verification failed (see Figure 11). Data may have been successfully burned to a CD-RW, despite the failed verification.



```
Finder: Burn started, Wed Apr 28 00:03:37 2010
Finder: Burning to CD-RW media with SAO strategy in HL-DT-ST DVDRW  GS23N SB00 via ATAPI.
Finder: Requested burn speed was 4x, actual burn speed is 4x.
Finder: Burn underrun protection is supported, and enabled.
Finder: Burn finished, Wed Apr 28 00:13:29 2010
Finder: Verify started, Wed Apr 28 00:13:29 2010
Finder: DVDRW  GS23N: SCSITask 1292453.250000 CDB: Read (10), block: 98816, count: 512 failed with service response = 1
(SERVICE_DELIVERY_OR_TARGET_FAILURE), status = 5 (DeliveryFailure)
Finder: Retry #1
Finder: DVDRW  GS23N: SCSITask 1292468.375000 CDB: Read (10), block: 98816, count: 512 failed with service response = 1
(SERVICE_DELIVERY_OR_TARGET_FAILURE), status = 5 (DeliveryFailure)
Finder: Retry #2
Finder: DVDRW  GS23N: SCSITask 1292483.250000 CDB: Read (10), block: 98816, count: 512 failed with service response = 1
(SERVICE_DELIVERY_OR_TARGET_FAILURE), status = 5 (DeliveryFailure)
Finder: Retry #3
Finder: DVDRW  GS23N: SCSITask 1292498.375000 CDB: Read (10), block: 98816, count: 512 failed with service response = 1
(SERVICE_DELIVERY_OR_TARGET_FAILURE), status = 5 (DeliveryFailure)
Finder: Giving up
Finder: Verify failed, Wed Apr 28 00:16:14 2010
Finder: Verify error: 0x80020063 Verifying the burned data failed.
```

(U) Figure 11 - The DiscRecording.log file pertaining to CD creation at 00:03, 28 Apr 10 (GMT +3:00)

7. (U) Non-Lead Observations:

(U) None.

8. (U) Summary of Examination:

(U) Examination of the rewritable compact disc (CD-RW), which was marked SECRET and recovered from the personal quarters of PFC MANNING, FOB HAMMER, Iraq, revealed the following:

A) (U) The CD-RW was located in the back of a case labeled "Starting out in Arabic. All the Arabic you need to get started in a simple audio-only program. 3 Audio CDs. No books necessary" in an apparent attempt to hide the disc.
B) (U) The data on the CD-RW was recorded by a Macintosh computer at 21:03, 27 Apr 10 (GMT+0:00) and contained a partial video (12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv) of an Apache helicopter airstrike.
C) (U) References to the file 12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv found on this CD-RW were also located within 12 different restore points (created between 2 Mar 10 and 7 May 10) linked to the user profile bradley.manning during the previous forensic examination of PFC MANNING's primary SIPRNET computer.

9. (U) Investigative Leads:

(U) None.

10. (U) Evidence Disposition:

(U) All evidence was placed into the evidence room of this office.

REPORT PREPARED \ APPROVED BY:

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

(b)(6)(b)(7)(C)
SPECIAL AGENT IN CHARGE

11. (U) Appendices:

(U) Attachment A, Enclosure 1 (Video file `12 Jul 07 CZ ENGAGEMENT ZONE 30 GC Anyone.wmv`)

Exhibit(s) 491

Page(s) 017324 withheld.

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

Exhibit(s) 492

Page(s) 017325 thru 017325s withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

Exhibit(s) 493

Page(s) 017326 withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes

0028 10-CID221-10117

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

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

PAGE 1 OF 3 PAGES

DETAILS

Basis for Investigation:

On 07 Dec 11, SAC (b)(6)(b)(7)(C) received a written request from SA (b)(6)(b)(7)(C) Federal Bureau of Investigation, Washington Field Office, 601 4th Street Northwest, Washington DC 20535 to conduct a preliminary examination of the digital media seized as Item 1, Evidence/Property Custody Document (EPCD), Document Number (DN) 179-11. Item #1 consisted of a United States Department of Energy, Brookhaven National Laboratory computer which was assigned to Mr. (b)(6)(b)(7)(C) and utilizing the Linux operating system. Specifically it was requested to examine the file `b.zip` to determine if it was same file identified as the file `BE22 PAX.zip` originally located on EPCD, DN 123-10, Item #1, which was a classified U.S. Army computer.

Examination Date and Contents:

Between 08 Dec 11 and 09 Dec 11, SAC (b)(6)(b)(7)(C) conducted a preliminary investigation of the computer in question. All times shown in this preliminary report are in relation to Eastern Standard Time (EST -5:00 UTC) unless otherwise noted.

A review of the Acquisition and Verification hash values showed they did match, see Figure 1 below.

```
MD5 Acquisition Hash Value:  b3fcfc178c3e2c7bf577a21a6c8f93d9
MD5 Verification Hash Value: b3fcfc178c3e2c7bf577a21a6c8f93d9
SHA1 Acquisition Hash Value:  0720ce13812dea2b7b7336b74c057d9636bdc80f
SHA1 Verification Hash Value: 0720ce13812dea2b7b7336b74c057d9636bdc80f
```

Figure 1, the acquisition and verification hash values

Pertinent Information:

Examination of the file system determined there was only one user account named `kupo`.

Examination of the file `\home\kupo\b.zip` revealed it was created at 11:28:25, 15 Dec 09. A comparison between `b.zip` and `BE22 PAX.zip` revealed they did not have the same hash value, see Figure 2 below.

```
EPCD, DN 179-11, Item #1, b.zip:  c2ba26766091b62526c57b4bc9ac69ae
EPCD, DN 123-10, Item #1, BE22 PAX.zip:  a07f7a4c3ba6301748af6b18da2b1b41
```

Figure 2, the hash values of the files in question.

Examination of the two zip files revealed they both were password protected zip files and they contained a file named `BE22 PAX.wmv`. Examination of the file `BE22 PAX.wmv` from both zip files revealed they had the same hash value, see Figure 3 below.

TYPED AGENT'S NAME AND SEQUENCE NUMBER SAC (b)(6)(b)(7)(C), (b) (7)(E)	ORGANIZATION CCIU-Digital Forensics and Research Branch U.S. Army CID, Quantico, VA 22136
SI (b)(6)(b)(7)(C)	DATE 09 Dec 11
	EXHIBIT 494

# AGENT'S INVESTIGATION REPORT	ROI NUMBER CAF: 0028-10-CID361 ROI: 0028-10-CID221-10117
CID Regulation 195-1	PAGE 2 OF 3 PAGES

DETAILS

```
EPCD, DN 179-11, Item #1, b.zip (BE22 PAX.wmv):  35c8b3eafe8e341457ffbf329cedeeb4
EPCD, DN 123-10, Item #1, BE22 PAX.zip (BE22 PAX.wmv):  35c8b3eafe8e341457ffbf329cedeeb4
```

Figure 3, the hash values of the files in question.

In an attempt to determine what the user kupo was doing with the file `b.zip` the `\home\kupo\.bash_history` file was examined. The `.bash_history` file disclosed it was a history of the commands typed into the computer for the user kupo. There are no times and dates associated with individual commands. It was disclosed there were 54 commands issued which concerned the attempted decryption of the file `b.zip`, see Figure 4 below for a partial list.

```
./fcrackzip -p  -D -u ../../b.zip
./fcrackzip -p D8.DIC -D -u ../../b.zip
./fcrackzip -p D8.DIC -D -u ../../b.zip
./fcrackzip -p D8.DIC -D  ../../b.zip
./fcrackzip -p dic-0294.txt -D  ../../b.zip
./fcrackzip -p dic-0294.txt -D  -u ../../b.zip
./fcrackzip -p dic-0294.txt -D   ../../b.zip
```

Figure 4, partial list of the command issued concerning decryption

In an attempt to determine how the classified file b.zip arrived onto this computer, an examination of the file `\home\kupo\.bash_history` revealed there were 73 SSH (Secure Shell) connections to IP address 173.68.194.47. It is of note there were two SCP (Secure Copy) sessions to the IP 173.68.194.47 downloading the files `d8.zip` and `dic-0294.zip` which appeared to aid the user kupo in the decryption effort, see Figure 5 below for a partial list.

```
ssh  -Y 173.68.194.47
ssh  -Y 173.68.194.47
scp 173.68.194.47:~/d8.zip ./
scp 173.68.194.47:~/dic-0294.zip ./
ssh  -Y 173.68.194.47
ssh  -Y 173.68.194.47
ssh   173.68.194.47
ssh  -Y 173.68.194.47.
ssh -Y  173.68.194.47
ssh  -Y 173.68.194.47
```

Figure 5, partial list of connections initiated by the user kupo.

The file `\home\kupo\CODE\fdcrackzip-1.0\D8.DIC` was a text file dictionary of words used to help decrypt files, see Figure 6 below for segment of the file.

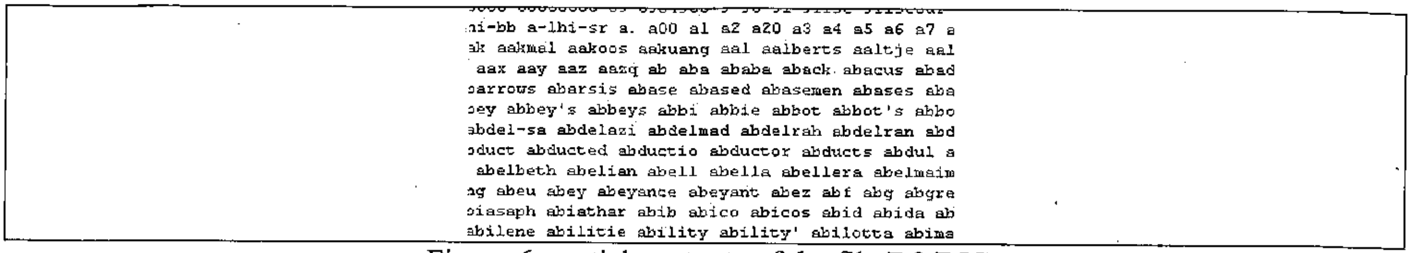
TYPED AGENT'S NAME AND SEQUENCE NUMBER SAC(b)(6)(b)(7)(C), (b) (7)(E)	ORGANIZATION CCIU-Digital Forensics and Research Branch U.S. Army CID, Quantico, VA 22136	
S(b)(6)(b)(7)(C)	DATE 09 Dec 11	EXHIBIT 494

AGENT'S INVESTIGATION REPORT

CID Regulation 195-1

ROI NUMBER	CAF: 0028-10-CID361 ROI: 0028-10-CID221-10117
	PAGE 3 OF 3 PAGES

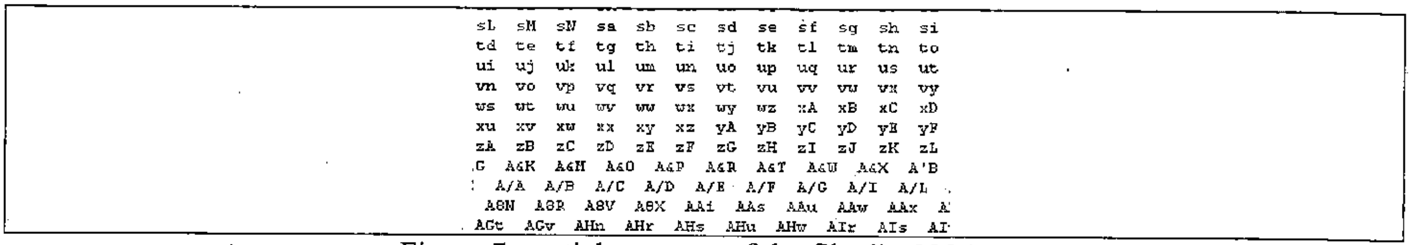
DETAILS



```
ni-bb a-lhi-sr a. a00 al a2 a20 a3 a4 a5 a6 a7 a
ak aakmal aakoos aakuang aal aalberts aaltje aal
 aax aay aaz aazq ab aba ababa aback abacus abad
barrows abarsis abase abased abasemen abases aba
bey abbey's abbeys abbi abbie abbot abbot's abbo
abdel-sa abdelazi abdelmad abdelrah abdelran abd
bduct abducted abductio abductor abducts abdul a
 abelbeth abelian abell abella abellera abelmaim
ag abeu abey abeyance abeyant abez abf abg abgre
biasaph abiathar abib abico abicos abid abida ab
abilene abilitie ability ability' abilotta abima
```

Figure 6, partial contents of the file D8.DIC

The file `\home\kupo\CODE\fdcrackzip-1.0\dic-0294.txt` was a text file dictionary of words used to help decrypt files, see Figure 7 below for segment of the file.



```
sL   sM   sN   sa   sb   sc   sd   se   sf   sg   sh   si
td   te   tf   tg   th   ti   tj   tk   tl   tm   tn   to
ui   uj   uk   ul   um   un   uo   up   uq   ur   us   ut
vn   vo   vp   vq   vr   vs   vt   vu   vv   vw   vx   vy
ws   wt   wu   wv   ww   wx   wy   wz   xA   xB   xC   xD
xu   xv   xw   xx   xy   xz   yA   yB   yC   yD   yE   yF
zA   zB   zC   zD   zE   zF   zG   zH   zI   zJ   zK   zL
.G   A&K   A&M   A&O   A&P   A&R   A&T   A&U   A&X   A'B
:  A/A   A/B   A/C   A/D   A/E   A/F   A/G   A/I   A/L
 A8N   A8R   A8V   A8X   AAi   AAs   AAu   AAw   AAx   A
AGt   AGv   AHn   AHr   AHs   AHu   AHw   AIr   AIs   AI
```

Figure 7, partial contents of the file dic-0294.txt

Summary:

The file `\home\kupo\b.zip` contained the exact same file copy of the file `BE22 PAX.zip` which was a classified password protected zip file containing a video named `BE22 PAX.wmv`. The file `BE22 PAX.zip` was originally located on classified server available only to users of the SIPRNET. This preliminary examination could not determine the source of the file `b.zip`, however it was likely the IP address 173.68.194.47 was involved. Further the user of the U.S. Government computer (kupo) had actively attempted to decrypt the password of `b.zip`.

//LAST ENTRY//

TYPED AGENT'S NAME AND SEQUENCE NUMBER SAC (b)(6)(b)(7)(C), (b) (7)(E)	ORGANIZATION CCIU-Digital Forensics and Research Branch U.S. Army CID, Quantico, VA 22136	
SIG (b)(6)(b)(7)(C)	DATE 09 Dec 11	EXHIBIT 494

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

REPLY TO
ATTENTION OF

CISA-CCI-DF 4 Jan 12

1. **Case Number:** CAF 0028-10-CID361/ROI 0028-10-CID221-10117

2. **Investigating Office:** Washington Metro Resident Agency, Computer Crime Investigative Unit, Quantico, VA

3. **Date of Report:** 4 Jan 12

4. **Examiner:** SAC (b)(6)(b)(7)(C), (b) (7)(E)

5. **Summary of Analysis:** Evidence/Property Custody Document (EPCD), Document Number (DN) 119-10, Items #2 and #3, consisting of two PST files from the bradley.manning user profile. One PST file was from the NIPRNET email server from FOB Hammer, Iraq and the other PST file was from the SIPRNET email server from FOB Hammer, Iraq. The items in question were not of evidentiary value.

EXHIBIT 495

Table of Contents

For Official Use Only
Law Enforcement Sensitive

Exhibit 495

1. Case Number

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

2. Investigating Office

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

3. Date of Report

4 Jan 12

4. Examiner

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

5. Analysis

5.1 Examination of the Log Files

5.1.1 Voucher information

EPCD, DN 119-10, Items #2 and #3 consisting of two PST files from the bradley.manning user profile. One PST file was from the NIPRNET email server from FOB Hammer, Iraq and the other PST file was from the SIPRNET email server from FOB Hammer, Iraq.

5.1.2 Pertinent Information

The items in question.were not of evidentiary value.

6. Summary of Examination

The item in question was of no evidentiary value.

7. Evidence Disposition:

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

Exhibit 495

Report Prepared/ Approved By:

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

Special Agent-in-Charge

Exhibit 495

Exhibit(s) 496

Page(s) 017334 thru 017334j withheld:

5 U.S.C. § 552(b)(1)
Permits withholding information that
is classified for
National Security purposes