Homeland Security Investigations

Computer Forensics Handbook

HSI HB 20-03 / June 12, 2020

U.S. Immigration and Customs Enforcement

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Foreword

The Computer Forensics Handbook provides a uniform source of national policies, procedures, responsibilities, guidelines, and controls to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents, including Computer Forensics Agents, and Criminal Analysts, including Computer Forensics Analysts, when requesting or performing computer or mobile device forensics on electronic media or devices pursuant to ongoing HSI investigations. This Handbook contains instructions and guidance to help ensure uniformity and operational consistency across all HSI field offices. Oversight over the national Computer Forensics Program resides with the Unit Chief, Computer Forensics Unit.

This Handbook supersedes the Computer Forensics Handbook (HSI HB 11-01), dated April 27, 2011, and all other policy documents on computer forensics issued since April 27, 2011, with the exception of ICE Directive 10044.1 (former number: 7-6.1), "Border Searches of Electronic Devices," dated August 18, 2009; Office of Investigations (OI) memorandum, "Border Searches of Electronic Devices Directive," dated August 31, 2009; and OI memorandum, "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media," dated December 12, 2008.

The Computer Forensics Handbook is an internal policy of HSI. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Information Disclosure Unit, as well as the appropriate ICE Counsel and/or U.S. Attorney, are to be consulted so that appropriate measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure pursuant to the law enforcement privilege. Any further request for disclosure of this Handbook or information contained herein should be referred to the HSI Information Disclosure Unit.

The HSI Policy Unit is responsible for coordinating the development and issuance of HSI policy. All suggested changes or updates to this Handbook should be submitted to the HSI Policy Unit, which will coordinate all needed revisions with the Computer Forensics Unit.

Alysa D. Erichs

Alysa D. Erichs
Acting Executive Associate Director
Homeland Security Investigations

6/12/2020
Date

COMPUTER FORENSICS HANDBOOK

Table of Contents

Chapter 1. PURPOSE AND SCOPE 1

Chapter 2. INTRODUCTION 1

Chapter 3. DEFINITIONS 1

- 3.1 Computer Forensics 1
- 3.2 Electronic Device 1
- 3.3 Mobile Device 2
- 3.4 Non-Physical Evidence 2
- 3.5 Operating System 2
- 3.6 Physical Evidence 2

Chapter 4. AUTHORITIES/REFERENCES 2

- 4.1 Authorities 2
- 4.2 References 3

Chapter 5. RESPONSIBILITIES 4

- 5.1 Executive Associate Director, Homeland Security Investigations 4
- 5.2 Unit Chief, Computer Forensics Unit 4
- 5.3 Section Chiefs, Computer Forensics Unit 4
- 5.4 Computer Forensics Unit Program Managers 4
- 5.5 Special Agents in Charge 5
- 5.6 Computer Forensics Coordinator 5
- 5.7 Group Supervisors and Resident Agents in Charge 5
- 5.8 Special Operations Jump Teams 5
- 5.9 Computer Forensics Agents and Computer Forensics Analysts 6
- 5.10 Special Agents and Criminal Analysts 7
- 5.12 Human Exploitation Rescue Operative (HERO) Child Rescue Corps Operatives 7

Chapter 6. SELECTIONS FOR COMPUTER FORENSICS PROGRAM TRAINING ... 7

- 6.1 Prerequisites 7
- 6.2 Nomination Process for Computer Forensics Program Training 7
- 6.3 Selection for Training Process 8

- 6.4 Nomination of State or Local Law Enforcement Officers or Task Force Officers 8
- 6.5 Nomination of Individuals Who Have Prior Computer Forensics Training....9

Chapter 7. COMPUTER FORENSICS PROGRAM – TERMS OF SERVICE....9

- 7.1 Probationary Period in the Computer Forensics Program 9
- 7.2 Mentoring Program....9
- 7.3 Mandatory Term of Service....9
- 7.4 Extension of Service 10
- 7.5 Relocations and Promotions 10
- 7.6 Requests for Computer Forensics Agents and Computer Forensics Analysts to Provide Presentations and Training 10

Chapter 8. TRAINING AND CERTIFICATIONS....11

- 8.1 (b) (7)(E) 11
- 8.2 11
- 8.3 Computer Forensics Annual Training....11
- 8.4 Required Certifications 11
- 8.5 Optional Certifications....12
- 8.6 Advanced Training and Certifications 12
- 8.7 Proctoring....13
- 8.8 Continuing Education 13

Chapter 9. COMPUTER FORENSICS AGENT AND COMPUTER FORENSICS ANALYST PERFORMANCE STANDARDS 13

- 9.1 Computer Forensics Agent/Computer Forensics Analyst Status Guidelines 13
- 9.2 Minimum Workload Standardization 14
- 9.3 Computer Forensics Program Personnel Composition....14
- 9.4 Computer Forensics Levels of Expertise and Certifications....15

Chapter 10. REMOVAL FROM THE COMPUTER FORENSICS PROGRAM 16

- 10.1 Removal from the Computer Forensics Program During the Probationary Period 16
- 10.2 Removal from the Computer Forensics Program During the Initial 3-Year Term of Service 17
- 10.3 Removal from the Computer Forensics Program After the Initial 3-Year Term of Service 17

- 10.4 Notification of Change of Computer Forensics Agent/Computer Forensics Analyst Status and Return of Computer Forensics Unit Equipment....17
- 10.5 Reinstatement....17

Chapter 11. DEFENSE DISCOVERY PROCESS....18

- 11.1 Adam Walsh Act....18
- 11.2 Procedures for Defense Forensics Examiners....18

Chapter 12. CASE MANAGEMENT....19

- 12.1 Computer Forensics Case Documentation....19
- 12.2 Case Management and Reporting....19
- 12.3 Collateral Requests....19
- 12.4 Field Examination Report....19
- 12.5 Reports of Investigation....19
- 12.6 Other Reporting....20
- 12.7 Computer Forensics Assistance Requests....20
- 12.8 Case File Audits....21

Chapter 13. HANDLING OF COMPUTER FORENSICS EVIDENCE....21

- 13.1 Handling of Evidence....21
- 13.1.1 Documenting the Scene....21
- 13.1.2 Labelling and Submission of Digital Evidence....21
- 13.2 Processing Digital Evidence....22
- 13.3 Image Duplication....22
- 13.4 Storing Forensic Images....23
- 13.5 Archiving Forensic Images....23
- 13.6 Retention of Forensic Evidence Files....23
- 13.7 (b) (7)(E) 24
- 13.8 Returning Files or Equipment that Had Contained Evidence or Contraband to Third Parties....24

Chapter 14. ENCRYPTION OF FORENSIC LAPTOPS/TABLETS....25

- 14.1 (b) (7)(E) 25
- 14.2 25

Chapter 15. HARDWARE/SOFTWARE....25

- 15.1 (b) (7)(E) 25
- 15.2 Imaging Software....25

- 15.3 Analysis Software 26
- 15.4 Supplemental Software 26
- 15.5 Approval Process for New Hardware/Software....26
- 15.6 Validation Requirements/Procedures....27

Chapter 16. IMAGING PROCEDURES....27

- 16.1 Imaging Procedures 27
- 16.2 (b) (7)(E) 28
- 16.3 Mobile Devices 28
- 16.3.1 Seizure of Evidence 28
- 16.3.2 Intake of Evidence 28
- 16.3.3 (b) (7)(E) 29
- 16.3.4 Report of Findings 29
- 16.4 Encryption....29

Chapter 17. FORENSIC ANALYSIS PROCEDURES....29

Chapter 18. DOCUMENTATION AND REPORTING 30

Chapter 19. GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 31

- 19.1 Exigent Circumstances....32
- 19.2 Border Search....32
- 19.3 Consent 33
- 19.4 Privacy Protection Act 33

APPENDICES

Appendix A Examples of Recommended Performance Goals for Computer Forensics Agents and Computer Forensics Analysts.... A-i
Appendix B Adam Walsh Examination Worksheet.... B-i
Appendix C Computer Forensics Case File Folder Go-by.... C-i
Appendix D Computer Forensics Examination Worksheet .... D-i
Appendix E Example of a Computer Forensics Report of Investigation....E-i
Appendix F Computer Forensics Assistance Request Worksheet....F-i
Appendix G Computer Forensics Consent Worksheet.... G-i
Appendix H Computer Forensics Border Response Worksheet .... H-i
Appendix I Computer Forensics (b) (7)(E) I-i
Appendix J Computer Forensics Image Release Worksheet ....J-i
Appendix K Computer Forensic Validation and Testing Go-by.... K-i
Appendix L First Responders Checklist ....L-i
Appendix M Acronyms....M-i

COMPUTER FORENSICS HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Computer Forensics Handbook establishes policy and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) General Schedule (GS)-1811 Special Agents (SAs), including Computer Forensics Agents (CFAs), and GS-0132 and GS-1801 Criminal Analysts (CAs), including Computer Forensics Analysts (CFAs), when requesting or performing computer or mobile device forensics on electronic media or devices pursuant to an ongoing HSI investigation. (Notes: For the purposes of this Handbook, 1) previewing electronic devices with HSI-issued equipment or software is not considered to be performing a "forensic" function; 2) the acronym "CFA" will refer to both Computer Forensics Agents and Computer Forensics Analysts; and 3) Human Exploitation Rescue Operative (HERO) Child Rescue Corps Operatives will be referred to as CFAs.)

Chapter 2. INTRODUCTION

The successful investigation and prosecution of criminal violations by HSI is largely dependent on the ability to quickly assess, image, process, and analyze evidentiary digital data obtained from lawfully detained or seized electronic devices and digital media. As a result, computer forensics has become increasingly critical to HSI investigations due to its heavy reliance on digital data as evidence.

Chapter 3. DEFINITIONS

The following definitions are provided for the purposes of this Handbook:

3.1 Computer Forensics

Computer forensics is the use of tools and techniques to recover, preserve, and examine data stored or transmitted in binary form using the principles applied to the detection, collection, preservation, and analysis of evidence to ensure its admissibility in legal proceedings.

3.2 Electronic Device

An electronic device is any device capable of containing or storing electronic information, such as computers, disks, drives, tapes, mobile phones, and other communications devices, as well as cameras, music players, and any other electronic or digital devices.

3.3 Mobile Device

A mobile device is any device that can store and manipulate digital data, is easily portable, and runs a limited operating system. This can include, but is not limited to, cellular phones, smart phones, personal digital assistants (PDAs), iPods, iPads, music players, and satellite navigation systems.

3.4 Non-Physical Evidence

Non-physical evidence is any evidence retrieved from physical evidence that is not a material object. Examples include forensic images and digital copies of data.

3.5 Operating System

The Operating System (OS) is the computer's master control program. Examples of OSs include Windows, Mac OS, Microsoft Disk Operating System (MS-DOS), and Linux.

3.6 Physical Evidence

Physical evidence is any evidence in the form of a material object. Examples include electronic devices and mobile devices.

Chapter 4. AUTHORITIES/REFERENCES

4.1 Authorities

A. Title 8, United States Code (U.S.C.), § 1225(d), Authority relating to inspections.

B. 8 U.S.C. § 1357, Powers of immigration officers and employees.

C. 19 U.S.C. § 482, Search of vehicles and persons.

D. 19 U.S.C. § 507, Assistance for customs officers.

E. 19 U.S.C. § 1461, Inspection of merchandise and baggage.

F. 19 U.S.C. § 1462, Forfeiture.

G. 19 U.S.C. § 1496, Examination of baggage.

H. 19 U.S.C. § 1582, Search of persons and baggage; regulations.

I. 19 U.S.C. § 1589a, Enforcement authority of customs officers.

J. 19 U.S.C. § 1595a, Forfeiture and other penalties.

K. 22 U.S.C. § 2778, Control of arms exports and imports.

L. 22 U.S.C. § 2780, Transactions with countries supporting acts of international terrorism.

M. 22 U.S.C. § 2781, Transactions with countries not fully cooperating with United States antiterrorism efforts.

N. 31 U.S.C. § 5317, Search and forfeiture of monetary instruments.

O. Federal Rules of Criminal Procedure, Rule 41(e)(2)(B), Warrant Seeking Electronically Stored Information.

P. Federal Rules of Criminal Procedure, Rule 41(f)(1)(B), Inventory.

4.2 References

A. Department of Homeland Security (DHS) Management Directive (MD) 11042.1, "Safeguarding Sensitive but Unclassified (For Official Use Only) Information," dated January 6, 2005 (as amended by DHS Instruction 121-01-014, "Access to 'For Official Use Only' (FOUO) Information by the Private Sector, Foreign Governments, International Organizations, and Foreign Non-Governmental Individuals," dated July 7, 2014, or as updated).

B. DHS Instruction 121-01-011, "The Department of Homeland Security Administrative Security Program," dated April 25, 2011, or as updated.

C. ICE Directive 10044.1 (former number: 7-6.1), "Border Searches of Electronic Devices," dated August 18, 2009, or as updated.

D. ICE Directive 4003.2, "Safeguarding Law Enforcement Sensitive Information," dated May 20, 2014, or as updated.

E. Office of Investigations (OI) Memorandum, "Border Searches of Electronic Devices Directive," dated August 31, 2009.

F. OI Memorandum, "Recordkeeping Procedures Regarding Detentions of Documents and Electronic Media," dated December 12, 2008.

G. HSI Guidance, "Legal Update – Border Search of Electronic Devices," dated May 11, 2018.

H. OI Handbook (HB) 08-02, "Case Management Handbook," dated February 1, 2008, or as updated.

I. HSI HB 15-05, Evidence Handbook, dated November 9, 2015, or as updated.

J. U.S. Customs and Border Protection (CBP) HB 4400-01B, "Seized Asset Management and Enforcement Procedures Handbook" (SAMEPH), dated July 2011, or as updated.

Chapter 5. RESPONSIBILITIES

5.1 Executive Associate Director, Homeland Security Investigations

The Executive Associate Director (EAD) of HSI has the overall responsibility for the oversight and implementation of the provisions of this Handbook.

5.2 Unit Chief, Computer Forensics Unit

The Unit Chief of the Computer Forensics Unit (CFU), Cyber Crimes Center (C3), is responsible for providing policy, guidance, training, and technical assistance to HSI field offices to ensure the highest quality of computer forensic examinations and maintenance of evidence. This responsibility also includes coordinating and developing training for all CFAs and providing them with the initial equipment necessary to perform their duty. Since technology is ever-changing, the CFU Unit Chief is responsible for keeping abreast of those changes and for providing frequent equipment updates to field offices. This entails researching new software and hardware products that will enhance productivity. To that end, the CFU Unit Chief is responsible for maintaining a relationship with the leading vendors in the field and assisting in budgeting and contracting. The CFU Unit Chief is also responsible for the management and maintenance of the(b) (7)(E)

5.3 Section Chiefs, Computer Forensics Unit

The CFU is divided into two sections: the Operational and Field Support Section and the Forensic Programs Section, each managed by a Section Chief. The Section Chiefs are responsible for overseeing the Program Managers and other assigned personnel and for reporting to the Unit Chief.

5.4 Computer Forensics Unit Program Managers

CFU Program Managers are responsible for providing direct support to CFAs and for liaison between CFU and other components, agencies, and field offices. This can include forwarding requests for forensic assistance and replacing or acquiring new equipment for CFAs. CFU Program Managers are also responsible for coordinating with Special Operations Jump Teams.

5.5 Special Agents in Charge

Special Agents in Charge (SACs) are responsible for implementing the provisions of this Handbook within their respective areas of responsibility (AORs). SACs are also responsible for designating a Group Supervisor or a Program Manager at the GS-14 grade level as a Computer Forensics Coordinator (CFC) to coordinate, with first-line supervisors, all the computer forensics workload and assignments between offices within the SAC's AOR. This is not meant to reduce or eliminate the first-line supervisors' management of their personnel. The CFC is intended to be a conduit between CFU and the SAC office, and to coordinate workload between offices in the SAC's AOR, as necessary. **(b) (7)(E), (b) (2)**

The Group Supervisor for the CFAs located at the SAC office should be the CFC who could then coordinate with the Group Supervisors in the DSAC, ASAC, RAC, or RA offices for balancing the workload, as necessary.)

5.6 Computer Forensics Coordinator

The CFC is responsible for distributing work between offices, through the Group Supervisors/ RACs, to CFAs assigned to offices in the SAC's AOR, and for assessing, prioritizing, and balancing the volume of work, if required. When possible, the work should be assigned to a CFA in the same office as the case agent. Should SAC resources prove insufficient to handle the computer forensics workload, the CFC will contact CFU to make alternate arrangements and balance work among SAC offices nationwide. The CFC will be the primary point of contact with CFU in the SAC's AOR.

5.7 Group Supervisors and Resident Agents in Charge

Group Supervisors and RACs who have CFAs under their supervision are responsible for direct supervision of those personnel. If assistance outside of the local office is required, the supervisor should coordinate with the CFC to distribute computer forensics workload between offices within a SAC's AOR. Group Supervisors and RACs are responsible for reviewing computer forensics examinations and evidence in order to make recommendations as appropriate and for ensuring quality control. Group Supervisors and RACs without the requisite background in computer forensics are urged to contact CFU, through the CFC, for assistance with their reviews.

5.8 Special Operations Jump Teams

Special Operations Jump Teams are composed of CFAs from the Computer Forensics Program (CFP) who have received advanced training or possess specialized skills such as the ability to communicate in a foreign language or who have a unique set of forensic skills including incident response/network forensics training. **(b) (7)(E)**

5.9 Computer Forensics Agents and Computer Forensic Analysts

CFAs are responsible for the identification, preservation, acquisition, processing, analysis, and presentation of electronic evidence and media:

A. Identification refers to locating media that may contain digital evidence.

B. Preservation refers to using forensically sound methods in preserving the data in its original form, including properly documenting possession of the evidence on the chain-of-custody form. Original evidence may be needed throughout the course of the forensic examination for a variety of reasons. CFAs should make every effort to preserve the evidence as expeditiously as possible. When CFAs no longer require access to the original evidence, they will coordinate with the case agent for proper disposition of the evidence.

C. Acquisition refers to the creation of a forensically sound copy of the original digital evidence on a government-owned storage device. **(b) (7)(E)**

(b) (7)(E)

D. Processing refers to a systematic series of actions conducted in accordance with HSI policy for the examination and handling of electronic media.

E. Analysis refers to the examination of the digital media. The amount of work needed for a forensic examination varies and depends on the needs of the case. **(b) (7)(E)**

F. Presentation of the forensic examination refers to writing a report and presenting it to the case agent and prosecutor for review. CFAs may be called upon to present their findings in court. In some cases, further review of evidence may be needed. In these situations, the request must come either from the case agent or from the prosecutor.

5.10 Special Agents and Criminal Analysts

SAs and CAs are responsible for complying with the provisions of this Handbook.

5.11 Human Exploitation Rescue Operative (HERO) Child Rescue Corps Operatives

HEROs are responsible for complying with the provisions of this Handbook.

Chapter 6. SELECTIONS FOR COMPUTER FORENSICS PROGRAM TRAINING

6.1 Prerequisites

HSI SAs and CFAs must have been ICE employees for a minimum of 3 years in the GS-1811, GS-1801, or GS-0132 series prior to being nominated for CFP training. However, the CFU Unit Chief can waive this requirement. CFAs can be nominated only if they will be co-located with a CFA with 3 years of experience, or if assigned under the supervision of a forensically trained Group Supervisor.

Candidates must possess, at a minimum, basic computer knowledge and skills, including familiarity and functionality with computer components, operations, peripherals, interfaces, operating systems, and software applications, as well as the Internet and Internet Service Providers.

CFAs are required to testify in court. Nominees should be able to provide credible testimony as to their findings and must be free of any Giglio and Henthorn issues that might impair their ability to testify in court.

6.2 Nomination Process for Computer Forensics Program Training

Based on workload, CFU will determine which SACs are required to nominate candidates. These SACs will submit a memorandum addressed to the CFU Unit Chief, providing the following information for each candidate:

A. Name;

B. Contact information;

C. SAC Office;

D. DSAC/ASAC/RAC/RA office location, if applicable;

E. Candidate's entrance on duty date;

F. Brief biography of the candidate's computer knowledge and experience;

G. Acknowledgement of 3-year mandatory term of service;

H. Acknowledgement of 1-year probationary period;

I. Need of a CFA or an additional CFA for a specific office location;

J. Request for training; and

K. Substantiated Giglio and/or Henthorn issues, and a list of any disciplinary actions of record, obtained in consultation with the Office of the Principal Legal Advisor (OPLA) and Employee and Labor Relations that might raise Giglio and/or Henthorn issues, or letters from U.S. Attorney's Offices (USAOs) regarding such issues.

6.3 Selection for Training Process

SACs are encouraged to consult with their CFC and the CFU Unit Chief prior to recommending SAs and/or CAs to attend CFP training. CFA placement is based on the needs of HSI and/or statistical analysis.

SACs will submit their recommendations in a memorandum to the CFU Unit Chief. The CFU Unit Chief will make selections for CFP training based on the projected forensic needs of a specific office location, the candidate's knowledge and computer-based experience, and the candidate's time in service.

After a candidate has been nominated by the SAC for possible acceptance into the CFP, he or she will be required to complete a computer knowledge assessment administered by CFU. (b) (7)(E)

(b) (7)(E)

After the candidate has been selected for the CFP, he or she will be scheduled for training. (See Chapter 8.)

6.4 Nomination of State or Local Law Enforcement Officers or Task Force Officers

Upon receiving a request from the CFU for CFA nominations, SACs can, via memorandum (see Section 6.2), nominate state or local law enforcement officers (LEOs) or task force officers (TFOs) within their AOR. The memorandum must affirm that the state or local LEO or TFO will conduct forensic examinations in furtherance of HSI investigations according to policies and procedures established by HSI. Additionally, the SAC sponsoring the state or local LEO or TFO nominee is responsible for accepting and assigning an ICE employee as the custodian of any equipment issued to the LEO or TFO in the ICE property system. All equipment issued to the

LEO or the TFO remains the property of ICE and may be utilized only in a manner consistent with ICE policy and procedures. Procedures for removal from the CFP will be the same as those for SAs, in accordance with Chapter 10 of this Handbook.

6.5 Nomination of Individuals Who Have Prior Computer Forensics Training

At any time, a SAC can, via memorandum (see Section 6.2), nominate HSI employees or state or local LEOs or TFOs who have successfully completed training equivalent to the Basic Computer Evidence Recovery Training (BCERT) course for acceptance into the CFP program as a CFA. CFU will decide the viability of such candidates based on the needs of HSI and the information contained in the memorandum from the SAC.

Chapter 7. COMPUTER FORENSICS PROGRAM – TERMS OF SERVICE

7.1 Probationary Period in the Computer Forensics Program

After the selectee has completed the training program or has otherwise been accepted into the CFP, he or she is considered a CFA. The probationary period in the CFP begins upon completion of BCERT. The CFA will remain in probationary status for 1 year. During the probationary period, the new CFA will be teamed with a mentor CFA for peer review of reports and other questions pertaining to examinations. The mentor CFA will provide quarterly status updates to CFU. Failure to perform pursuant to the provisions of this Handbook may result in the CFA being removed from the CFP in accordance with Section 10.1 of this Handbook.

7.2 Mentoring Program

A mentor is a CFA who has achieved at least Level III proficiency (see Section 9.4). The mentor will normally be selected by the local supervisor from within the same office as that of the probationary CFA. If the probationary CFA is the only CFA in the office, the mentor CFA will be selected from within the SAC's AOR. If there is no qualified mentor CFA in the SAC's AOR, a mentor CFA in another SAC's AOR or in CFU will be selected by the CFU Section Chief overseeing training.

The mentor CFA will review reports and examinations for format and presentation prior to their submission. The mentor CFA will also be available to answer questions the CFA may have during the course of the examinations. When possible, the mentor CFA should observe the probationary CFA's first few examinations. If the mentor CFA is not located in the same office as the probationary CFA, the probationary CFA should provide the mentor CFA with any completed work products and associated files he or she produces during the mentoring process, in accordance with Chapter 13 of this Handbook.

7.3 Mandatory Term of Service

Because of the prohibitive costs of training, all CFAs must agree to a minimum term of service of 3 years with HSI and sign a continuing service agreement prior to commencing the training.

The term of service begins immediately upon completion of BCERT. This term of service applies to all CFAs.

SACs who wish to remove a CFA from the CFP prior to completion of the CFA's initial 3 years require the approval of the EAD of HSI. The CFU Unit Chief has the authority to remove a CFA from the CFP who does not meet the guidelines provided in this Handbook or if the CFP's mission changes.

7.4 Extension of Service

After the mandatory term of service has been reached, CFAs may continue to work in their current position as CFAs. Renewal into the CFP is automatic unless one of the following conditions apply:

1) The CFA requests removal from the CFP by routing a memorandum of intent to the SAC, through the Deputy Assistant Director (DAD), C3, at least 6 months prior to his or her requested date of removal from the CFP.

2) The SAC does not concur with or terminates the renewal.

3) The DAD, C3, with approval from the SAC, does not concur with or terminates the renewal.

7.5 Relocations and Promotions

When relocating to an office within the same SAC's AOR, the CFA can remain in the CFP at the SAC's discretion. The SAC should notify CFU as to the CFA's status in the CFP at the new location.

When transferring from one SAC's AOR to a different SAC's AOR, a CFA can remain in the CFP only at the receiving SAC's discretion. A memorandum must accompany this action from the receiving SAC to the CFU Unit Chief, acknowledging the CFA's continued participation in the CFP.

Any active CFA who has been promoted or placed into an acting supervisory status for more than 90 days must notify CFU. If the CFA continues to support the CFP mission or anticipates returning to CFA duties within a reasonable time period, the CFA will remain in the CFP.

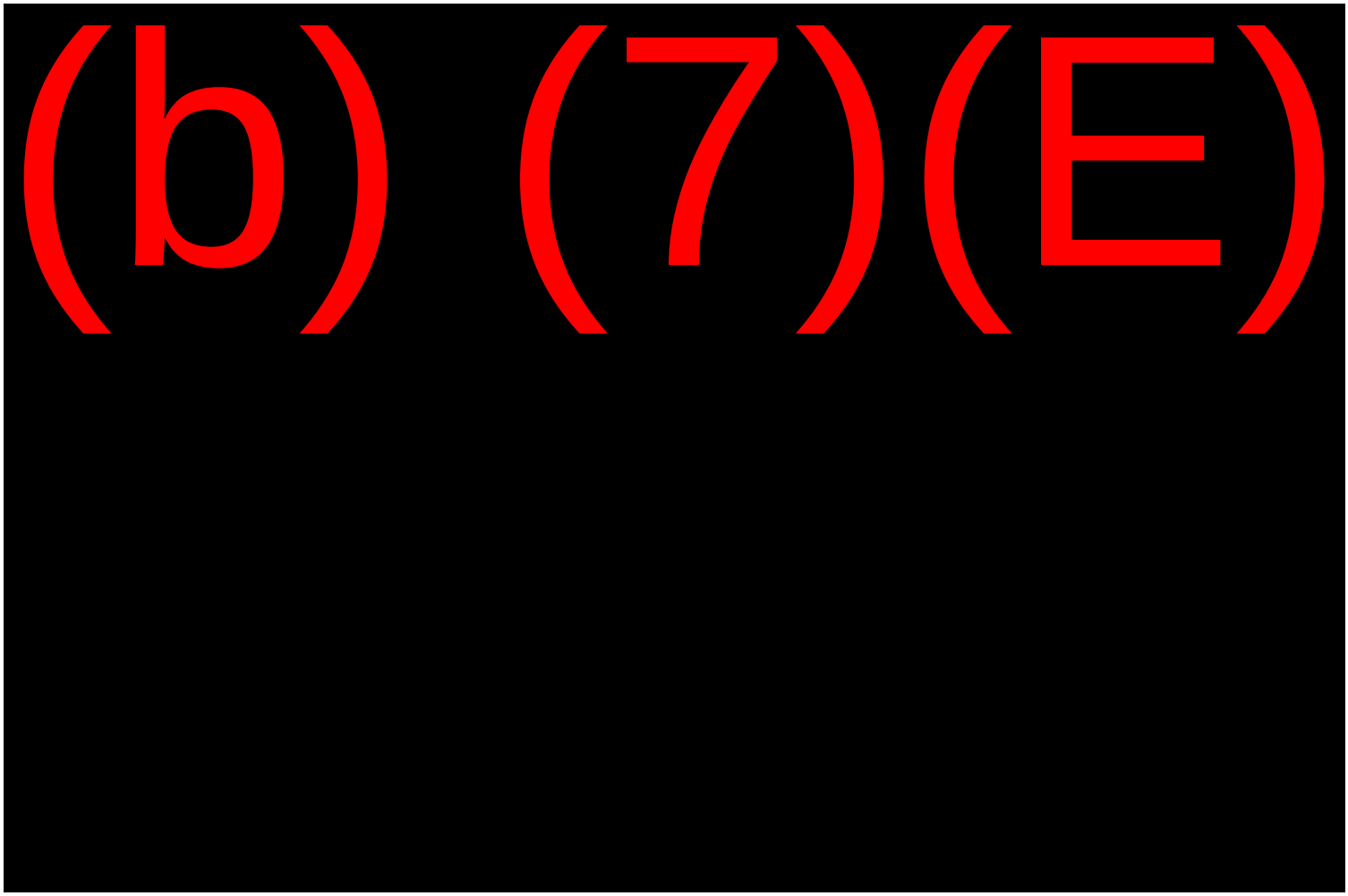
Understanding each situation is unique, the SAC, in consultation with the DAD, C3, will make final determinations about participants in the CFP within the SAC's AOR.

7.6 Requests for Computer Forensics Agents and Computer Forensics Analysts to Provide Presentations and Training

Any requests for a CFA to provide, conduct, or perform any type of computer forensics-related presentations or training must be approved by the SAC, or his or her designee, who can consult

with the CFU Unit Chief for assistance. The CFU tracks this information, so the CFA must notify the CFU Unit Chief regarding the type of presentation or training provided, including the number of associated participants.

Chapter 8. TRAINING AND CERTIFICATIONS



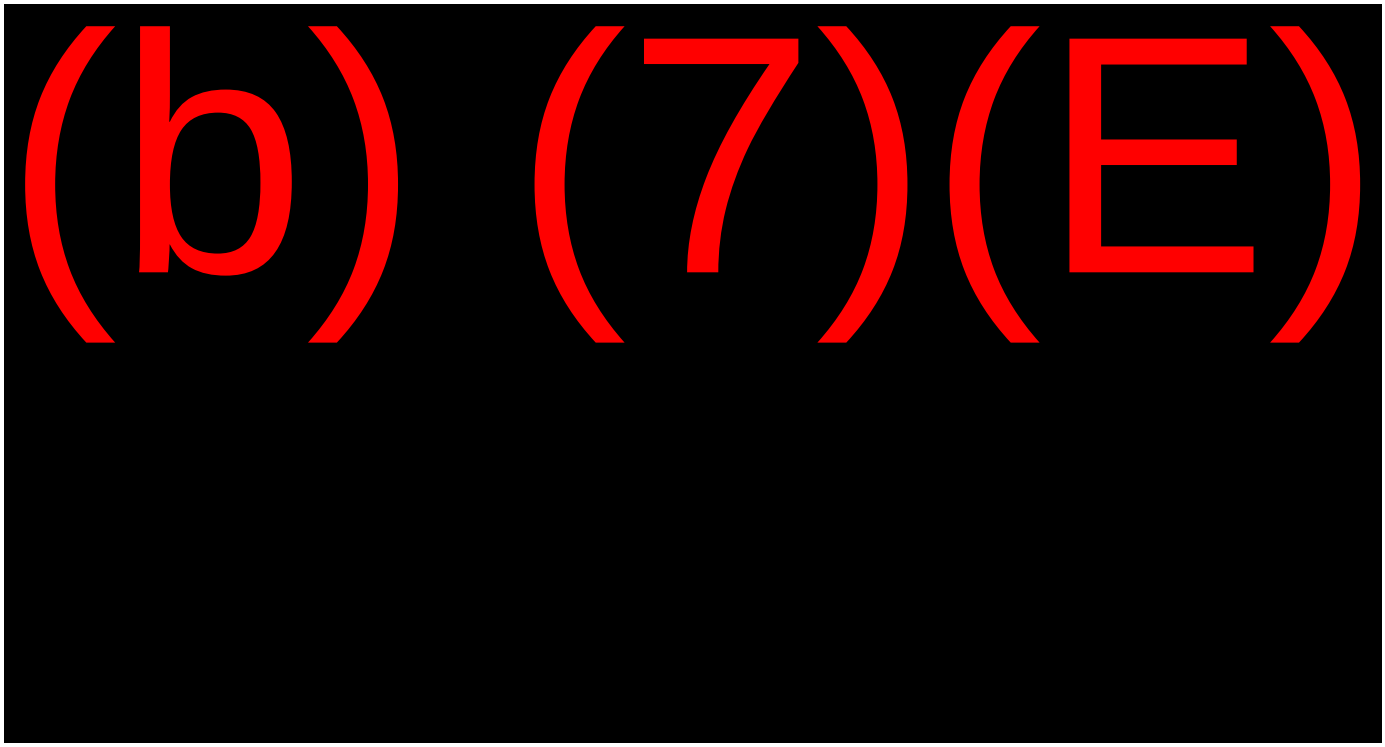
8.3 Computer Forensics Annual Training

CFU sponsors the Computer Forensics Annual Training (CFAT). CFAT topics include emerging technologies, basic training in new hardware and software, and advanced computer forensic techniques. CFAT will be held depending on the availability of funds.

8.4 Required Certifications

8.5 Optional Certifications

Industry-recognized certifications in computer forensics are strongly supported by CFU. These training programs and certifications enhance the CFA's computer knowledge and skills with certain computer forensics analysis tools. Programs approved by CFU include, but are not limited to, the following:



Failure to complete or acquire certification in any such requested course(s) may bar the CFA from future certifications and training, restrict the CFA's advancement to the next CFA level, and impact the CFA's ability to remain in the CFP. This decision lies solely with the CFU Unit Chief.

8.6 Advanced Training and Certifications

Only one advanced training or attempt at a certification process may be pursued at a time and it must be completed before another request can be made. At the discretion of CFU, the CFA may

be provided additional opportunities to successfully complete the training or certification process. Failure to complete or acquire certification could result in the denial of future training requests and may impact the CFA's ability to remain in the CFP.

CFAs who receive advanced certifications funded by CFU are a valuable resource to the CFP and to HSI and may be called upon as needed. CFAs in level of expertise V (see Section 9.4 (E)) cannot decline the request for assistance without just cause.

8.7 Proctoring

The education of new students is paramount to the success of the CFP. CFAs are encouraged to participate by proctoring basic and advanced courses within HSI and volunteering as proctors, instructors, mentors, or in any other similar position with other computer forensic organizations such as IACIS. Having CFAs represent HSI with these organizations enhances the reputation of the CFP and the agency.

8.8. Continuing Education

All CFAs are required to continue their education after the successful completion of BCERT. In order to maintain their active status, CFAs must receive 120 hours of CFU-approved training every 3 years, which can include CFAT, proctoring, and instructor hours. Continuing educational opportunities will be announced via the **(b) (7)(E)** and/or via e-mail. However, CFU will accept ad hoc training requests on an individual basis. Failure to complete this continuing education may result in the CFA being removed from the CFP. Continuing education is essential to maintaining a healthy and robust CFP skillset. All CFAs are encouraged to participate in instructional, educational, certification, and accreditation organizations such as IACIS. HSI representation in these organizations enhances the visibility of HSI and recognition of HSI's presence in the forensics community.

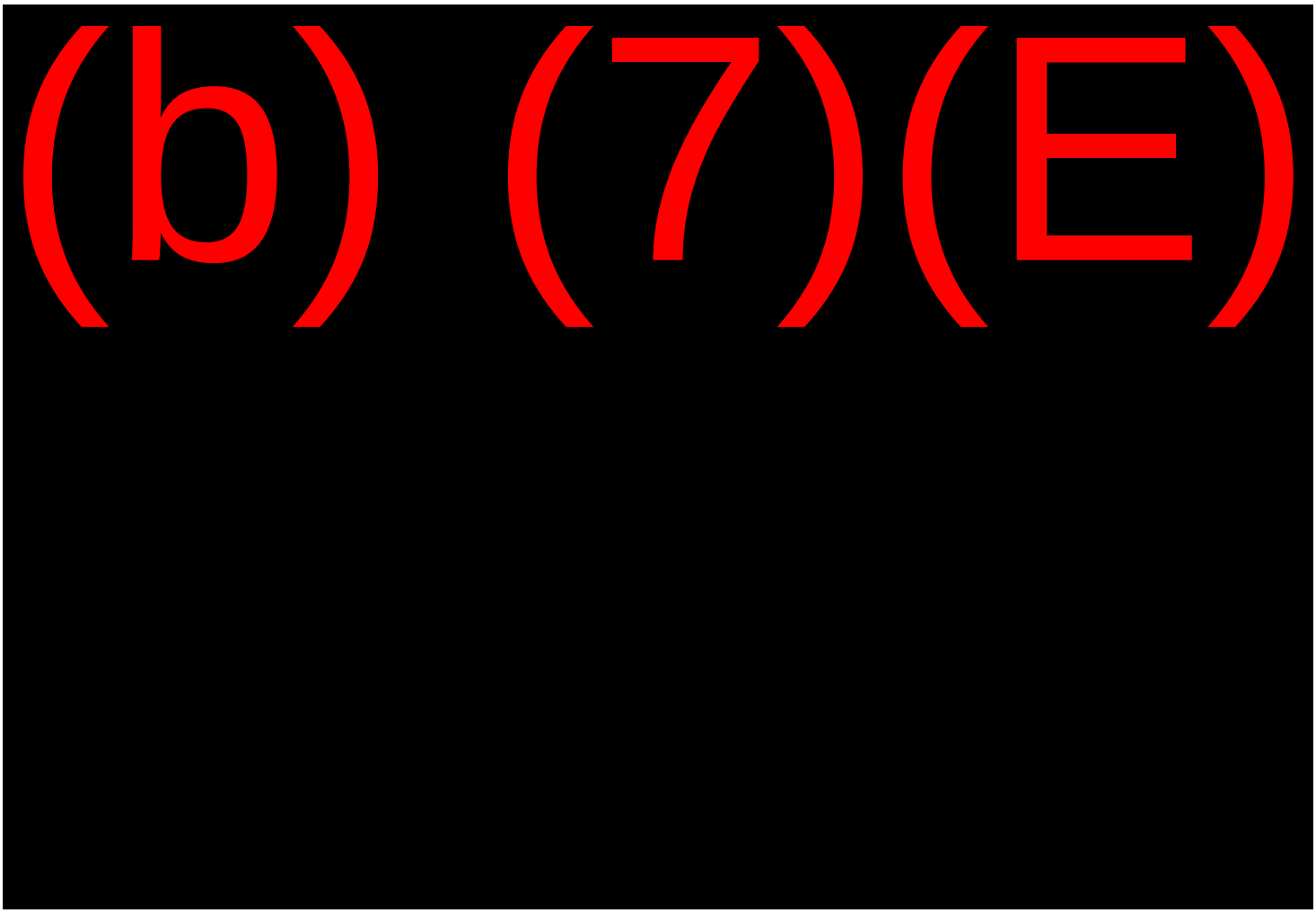
Chapter 9. COMPUTER FORENSICS AGENT AND COMPUTER FORENSICS ANALYST PERFORMANCE STANDARDS

9.1 Computer Forensics Agent/Computer Forensics Analyst Status Guidelines

To become CFAs, candidates must pass the BCERT forensic course. In order to remain in the CFP, CFAs are required to complete forensic examinations for their respective AOR. CFAs need to be committed to continuing education in the field of computers and computer forensics. Additional training and certifications are required for CFAs to maintain their position and stay up-to-date with advances in computer forensics and technology.

CFAs' immediate supervisors should include specific goals in the CFAs' annual Performance Plans that are relevant to CFAs' forensic duties. (See Appendix A for examples of recommended performance goals for CFAs.)

9.2 Minimum Workload Standardization



If CFAs are unable to maintain the number of case hours required, they may be removed from the CFP at the discretion of the CFU Unit Chief after consultation with the SAC.

9.3 Computer Forensics Program Personnel Composition

Given GS-1811 CFAs' law enforcement and investigative experience and mindset, HSI recognizes the importance and benefit of maintaining a robust core of GS-1811 CFAs assigned to the CFP. As a result, SAC offices should maintain at least a 1:1 ratio of SAs to non-SAs in the CFP within their AORs and should make every effort to ensure that GS-1801 and GS-0132 CFAs, collectively, do not outnumber GS-1811 CFAs assigned to the CFP. With the understanding that personnel requirements vary from office to office, this ratio may be modified by SACs on a case-by-case basis in coordination with the DAD, C3. In these instances, SACs may notify the DAD, C3 via memorandum if they intend to maintain a CFA composition entailing more personnel in a non-GS-1811 series than those in the GS-1811 series. This memorandum will ensure that the requesting SAC's future GS-1811 CFA selections are prioritized.

9.4 Computer Forensics Levels of Expertise and Certifications

A. Level I (Mobile Extraction Specialist): Has completed the baseline mobile acquisition training and has been accepted into the HSI CFP:

1) HSI or (b) (7)(E) or other mobile device data extraction forensics Certification.

B. Level II (Data Acquisition Specialist): Has met the requirements for Level I and has completed:

1) HSI or equivalent data acquisition course.

a) CFU First Responder Data Acquisition Course.

C. Level III (Computer Forensics Agent/Analyst): Has met the requirements for Level II and has:

1) Earned (b) (7)(E) and

2) Completed (b) (7)(E)

D. Level IV (Computer Forensics Agent/Analyst): Has met the requirements for Level III and has:

1) A minimum of 3 years' experience as a CFA;

2) Obtained the (b) (7)(E) or equivalent industry recognized computer forensic certification; and

3) Completed (b) (7)(E) or its equivalent.

E. Level V (Senior Computer Forensics Agent/Analyst): Has met the requirements for Level IV and:

1) Has 5 years' experience as a CFA;

2) Has attended advanced training classes in various disciplines;

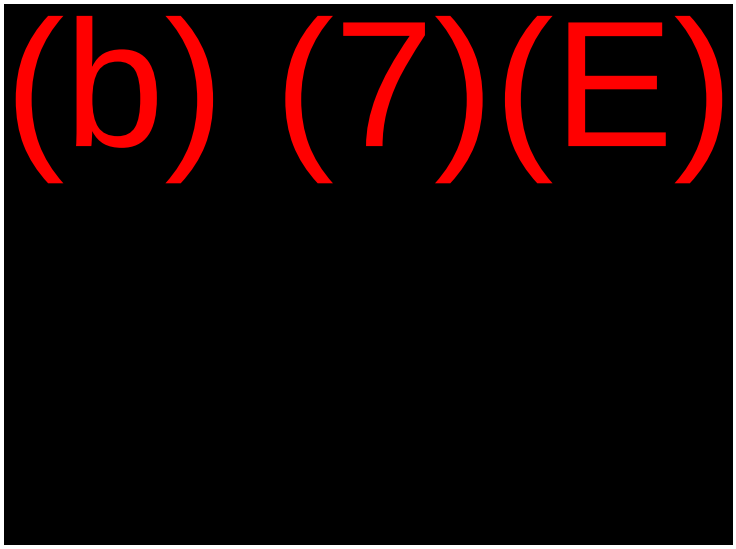
3) Has provided advice and assistance to other CFAs and SAs, or has been assigned as a Mentor (Section 7.2);

4) Has achieved an advanced industry-accepted certification in a computer science discipline, incident response, malware analysis, or equivalent;

5) Has obtained the approval of the CFU Unit Chief and the SAC if assigned within a SAC's AOR; and

6) Cannot refuse a request for assistance from CFU without just cause, as agreed upon by the SAC and the CFU Unit Chief.

CFU will determine the entry level of CFAs with prior experience, training, and certification. The CFU Unit Chief can alter or amend the levels' criteria due to the needs of HSI. Global discipline subject matter will be decided based on the needs of the CFP and may change from year to year. Examples of global disciplines include, but are not limited to:



Chapter 10. REMOVAL FROM THE COMPUTER FORENSICS PROGRAM

10.1 Removal from the Computer Forensics Program During the Probationary Period

During a new CFA's probationary period in the CFP, the CFA may be removed from the CFP by the CFU Unit Chief based on the needs of the CFP or if the CFA does not meet the requirements specified in this Handbook.

If the mentor CFA, any active CFA, or the supervisor determines that the probationary CFA is unable to complete examinations accurately and/or in a timely manner, or that the probationary CFA lacks the base level of knowledge required, the mentor CFA, active CFA, or supervisor can request that the CFU Unit Chief and/or the CFC conduct a secondary review of the probationary CFA's work product. If the CFU Unit Chief determines that the work product does not meet the standards of the program, he or she can remove the CFA from the CFP.

Upon removal, the CFA's equipment will be returned to, and reassigned by, CFU. CFAs can be removed from the CFP for prolonged inactivity, failure to complete assignments or training, or any performance issues as CFAs, as determined by the CFU Unit Chief. The CFU Unit Chief will make the final decision as to the permanent status of the CFA.

10.2 Removal from the Computer Forensics Program During the Initial 3-Year Term of Service

Due to the amount of time and money invested in their training, CFAs are required to remain in the CFP during their initial 3-year term of service (see Section 7.3). However, the SAC may remove a CFA from his or her duties as a CFA during the initial 3-year term of service. The SAC may accomplish this by notifying the Assistant Director, Operational Technology and Cyber Division.

CFAs transferred to another SAC's AOR should be placed in a position with CFA responsibilities through the duration of the 3-year term of service commitment. If the receiving SAC decides to remove the CFA from the CFP, this will not be considered a breach of the 3-year mandatory term of service by the employee.

Nothing in this Handbook prevents the promotion of CFAs into supervisory positions. Such a promotion would not be a breach of the term of service.

The DAD, C3, may remove a CFA from the CFP for any reason, with concurrence from the affected SAC.

10.3 Removal from the Computer Forensics Program After the Initial 3-Year Term of Service

After the initial 3-year commitment is fulfilled, the SAC may remove a CFA from his or her responsibilities as a CFA for any reason. The DAD, C3, should be notified as soon as practically possible prior to the CFA's removal from the CFP. Due to the amount of time and money invested in the training of the CFAs, there must be a documented reason to remove someone from the CFP.

After the initial 3-year commitment is fulfilled, CFAs may request removal from the CFP for any reason. The CFA must route a memorandum of intent to the SAC through the DAD, C3, at least 6 months prior to his or her requested date of removal from the CFP. This 6-month period is intended to provide the DAD, C3, and the SAC appropriate time to plan for a suitable replacement.

10.4 Notification of Change of Computer Forensics Agent/Computer Forensics Analyst Status and Return of Computer Forensics Unit Equipment

Upon a CFA's separation from service, retirement, or termination of active CFA status, the CFC must notify the CFU Unit Chief. The CFU Unit Chief will determine the final disposition of all issued computer forensics equipment.

10.5 Reinstatement

CFAs who leave the CFP in good standing are welcomed back into the program at the discretion of the CFU Unit Chief. If reinstatement occurs more than 2 years after leaving the CFP, the CFA

may be required to attend classes prior to conducting computer forensics examinations. The CFU Unit Chief will make the final determination concerning the training needs of the reinstated CFA. Any request for reinstatement must adhere to the procedures outlined in Section 6.5.

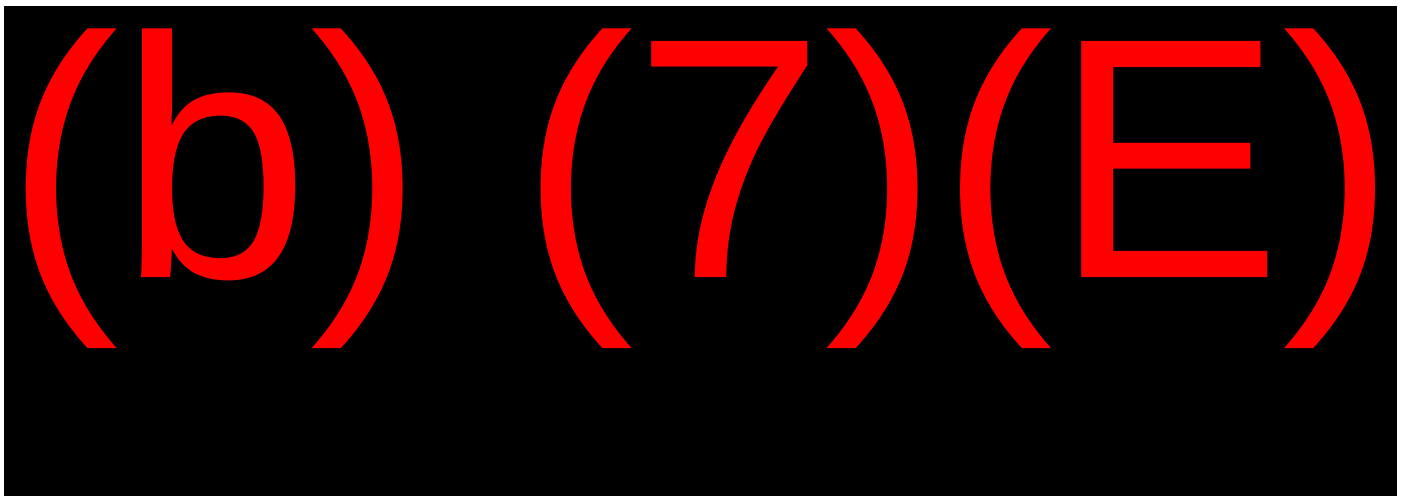
Chapter 11. DEFENSE DISCOVERY PROCESS

As part of the discovery process, CFAs are sometimes required to provide access to digital evidence obtained during analysis. Due to the unique nature of some of the content of such evidence **(b) (7)(E)**
pecial handling may be required.

11.1 Adam Walsh Act

In federal criminal proceedings, child pornography must remain in the care, custody, and control of the government or the court. Adam Walsh Child Protection and Safety Act of 2006 (codified at 18 U.S.C. § 3509(m)). Despite the general discovery rules set forth in the Federal Rules of Criminal Procedure, *the defendant and his or her representatives are not entitled to copies of such material.* In order to control such material during the examination of electronic devices by the defense, CFAs on site are required to ensure that defense examiners complete the Adam Walsh Examination Worksheet (see Appendix B) prior to the examination of a computer system. Prosecutions under state law are subject to state discovery rules; therefore, the Adam Walsh Act may not apply.

11.2 Procedures for Defense Forensics Examiners



Chapter 12. CASE MANAGEMENT

12.1 Computer Forensics Case Documentation

CFAs will maintain all original documents, including, but not limited to, worksheets, notes, forms, etc., related to a forensics exam. (Note: See Chapter 13 for procedures on handling work product containing contraband.)

12.2 Case Management and Reporting

CFAs will post their computer forensics Reports of Investigation (ROIs) to the originating case number. Computer forensics case hours will be recorded in (b) (7)(E) as stated in the (b) (7)(E) Quick Reference Guide on hours.

12.3 Collateral Requests

Collateral requests will be made via ICM in accordance with the Case Management Handbook (OI HB 08-02), dated February 1, 2008, or as updated, if the original case originates outside the SAC's AOR where the CFA is assigned. It is the prerogative of the SAC to determine if collateral requests are required to be initiated within his or her AOR.

12.4 Field Examination Report

The Field Examination Report (FER), located on the HSI **(b) (7)(E)** or its successor, is mandatory and must be completed within 10 business days after the completion of a forensic examination. Initial information (i.e., case number, seizure number, border search, number of computers, number of media, encryption, and capacity of media) must be input no later than the 5th business day of the following month after imaging has begun. For the purpose of the CFP, only one FER per CFA is entered per case regardless of the number of media the case may have. If an examination is performed pursuant to a collateral case, the CFA needs to enter only the actions he or she performed on that particular case. For instance, data acquisition trained personnel can submit a FER for imaging only and a CFA can submit a FER for analysis only. CFCs and/or first-line supervisors over CFAs in SAC offices will be given supervisory access to the system to ensure the timely entering of FERs. Once the FER has been completed, CFAs should ensure that the "FER Completed" check box has been checked in the Computer Forensics Examination Worksheet (see Appendix D).

12.5 Reports of Investigation

For every computer forensics examination, the CFA must complete an ROI. The ROI should be posted to the originating case or a collateral case. Forensic examination ROIs should be Type **(b) (7)(E)** The ROI should specify what initiated the investigation, the search authority computer identifiers, forensic equipment utilized, methods utilized, and a brief summary of findings. (See Appendix E for an example of a Computer Forensics ROI.)

12.6 Other Reporting

CFAs regularly create a variety of different work products to support the findings of their examinations. The work products can be in the form of optical media or typed pages from the forensic examination. CFAs should coordinate with the case agent and/or the prosecutor to determine what is needed for the final work product.

Any work product that is provided to the case agent and/or prosecutor should, at a minimum, be labelled with the original case number, the case agent's name, and the CFA's name. The CFA should also initial and date the items that are distributed. (Note: See Chapter 13 for procedures on handling work products containing contraband.)

12.7 Computer Forensics Assistance Requests

CFAs must ensure that all forensic assistance requests are accompanied by the appropriate Computer Forensics Assistance Request Worksheet (see Appendix F). This worksheet must be routed from the case agent to the case agent's supervisor for assignment with an office, or to the local CFC who is responsible for coordinating such assistance requests with the CFAs and first-line supervisors in other offices within the SAC's AOR. SAC offices may add additional fields or modify the formatting of this worksheet to suit their individual requirements.

CFAs should ensure that the Computer Forensics Assistance Request Worksheet is accompanied by all supporting documentation. This documentation should include a copy of the search warrant or a copy of the completed Computer Forensics Consent Worksheet (see Appendix G) or a copy of the completed Computer Forensics Border Response Worksheet (see Appendix H). Any CFA response to the U.S. border or a port of entry to provide forensic assistance requires the completion of a Computer Forensics Border Response Worksheet.

CFAs must complete a Computer Forensics Examination Worksheet (see Appendix D).

(b) (7)(E)

During a request by defense counsel to examine a forensic image that contains child pornography, CFAs must ensure that the defense counsel's computer forensic examiner completes the Computer Forensics Adam Walsh Examination Worksheet (see Appendix B). This worksheet, once completed, must remain in the case folder.

Any request for copies of a forensic image from an outside agency must be received on a completed Computer Forensics Image Release Worksheet (see Appendix J). Requests for copies of images obtained through border searches must comply with ICE Directive 10044.1 (former number: 7-6.1), "Border Searches of Electronic Devices," dated August 18, 2009, or as updated. The local OPLA embedded attorney should be contacted in situations where such a request stems from a border search or would result in the release of classified, privileged, or otherwise sensitive information (e.g., asylum information).

12.8 Case File Audits

CFU can audit a CFA's case files at any time to check for compliance with the provisions of this Handbook. An unfavorable audit of the case files, including failure to input completed FERs, can lead to removal from the CFP.

Chapter 13. HANDLING OF COMPUTER FORENSICS EVIDENCE

CFAs and SAs must ensure compliance with the Evidence Handbook (HSI HB 15-05), dated November 9, 2015, or as updated, and CBP's SAMEPH, dated July 2011, or as updated.

13.1 Handling of Evidence

(b) (7)(E)

13.1.1 Documenting the Scene

(b) (7)(E)

13.1.2 Labelling and Submission of Digital Evidence

All evidence that is submitted for forensic analysis is required to be properly labelled with the appropriate evidence label and accompanied by the appropriate DHS Form 6051 or other chain of custody form. (b) (7)(E)
(b) (7)(E)

Evidence labels should include the following information: FP&F number, seizure number, case number, date and time of seizure, line item number, case agent, and subject or owner. If the device is too large to fit into an evidence package, an evidence label should be affixed to the device. The original chain of custody form must accompany and remain with the digital evidence. Cellular phones and PDAs should be documented on a separate chain of custody form for mobile devices, separate and apart from the chain of custody used for other digital evidence.

When direct hand-to-hand transfer of evidence is not practical, an approved shipping company such as FedEx, Dalsey Hillblom Lynn (DHL), United Parcel Service (UPS), and United States Postal Service (USPS), with package tracking, must transport the evidence. The officer having custody of the evidence must write "Sent via FedEx (or DHL, UPS, or USPS)," as applicable, on the appropriate DHS Form 6051, in the Acceptance/Chain of Custody, Block C. In Block D, the officer having custody of the evidence will input the tracking number. This information should also be included when utilizing another chain of custody document.

13.2 Processing Digital Evidence

After evidence has been submitted for forensic examination, the CFA is required to ensure that the case agent or the submitting SA has included the Computer Forensics Assistance Request Worksheet (see Appendix F), along with the search authority documentation. This information needs to be received prior to conducting any forensic work on the digital evidence.

The CFA should photograph the computer and all associated components. The photographic images will be maintained with the CFA's forensic evidence image files. The CFA should record the pertinent information in the Computer Forensics Examination Worksheet (see Appendix D).

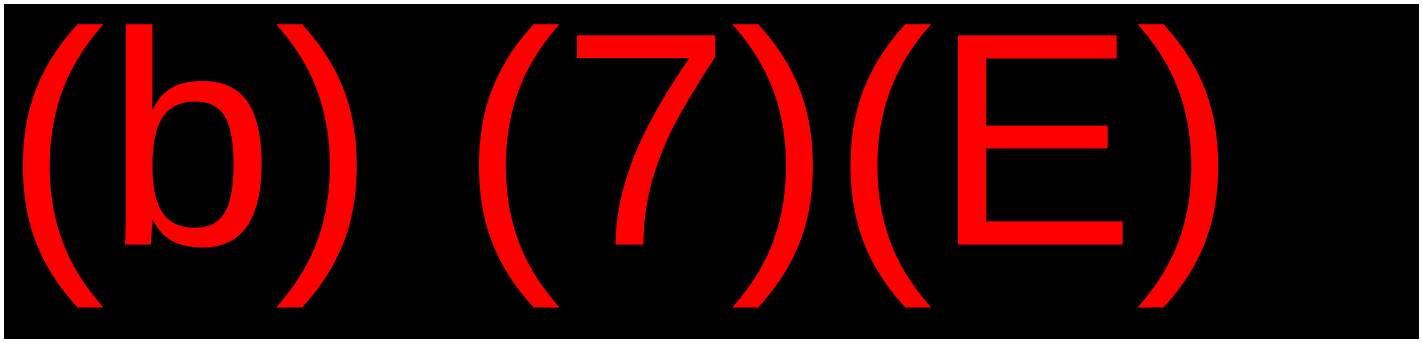
In compliance with the SAMEPH, original evidence should be secured post acquisition in an approved Seized Property facility. The original evidence should be returned to the case agent as soon as possible upon completion of imaging or viewing the item(s). CFAs need to ensure that all the labelling requirements have been met (see Section 13.1.2) and that the labels are still in place on the evidence. The case agent is responsible for the final disposition of the original evidence after the CFA determines that it is no longer required.

13.3 Image Duplication

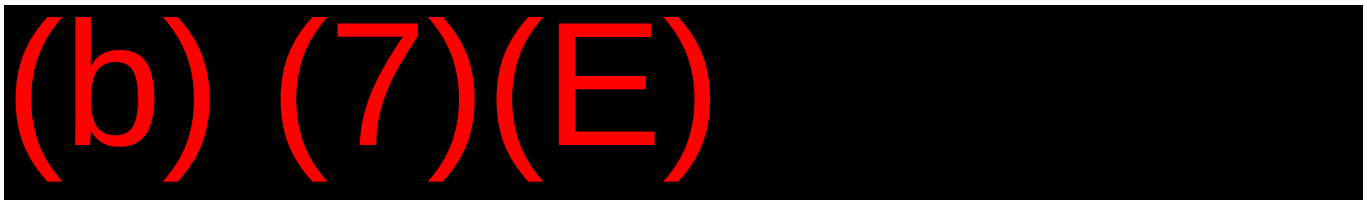
As of the date of issuance of this Handbook, there is no mechanism for entering or tracking non-physical evidence in **(b) (7)(E)**; therefore, CFAs should not enter the above-mentioned items into **(b) (7)(E)**. Computer forensics images or copies of information from electronic devices and media are not to be entered into **(b) (7)(E)**. Whenever HSI seizes a copy or image of electronic media, the seizing SA must initiate a chain of custody form and other appropriate documentation.

When providing images to agencies outside HSI, a Computer Forensics Image Release Worksheet (see Appendix J) must also be completed. This is in addition to the DHS Form 6051 or other chain of custody form.

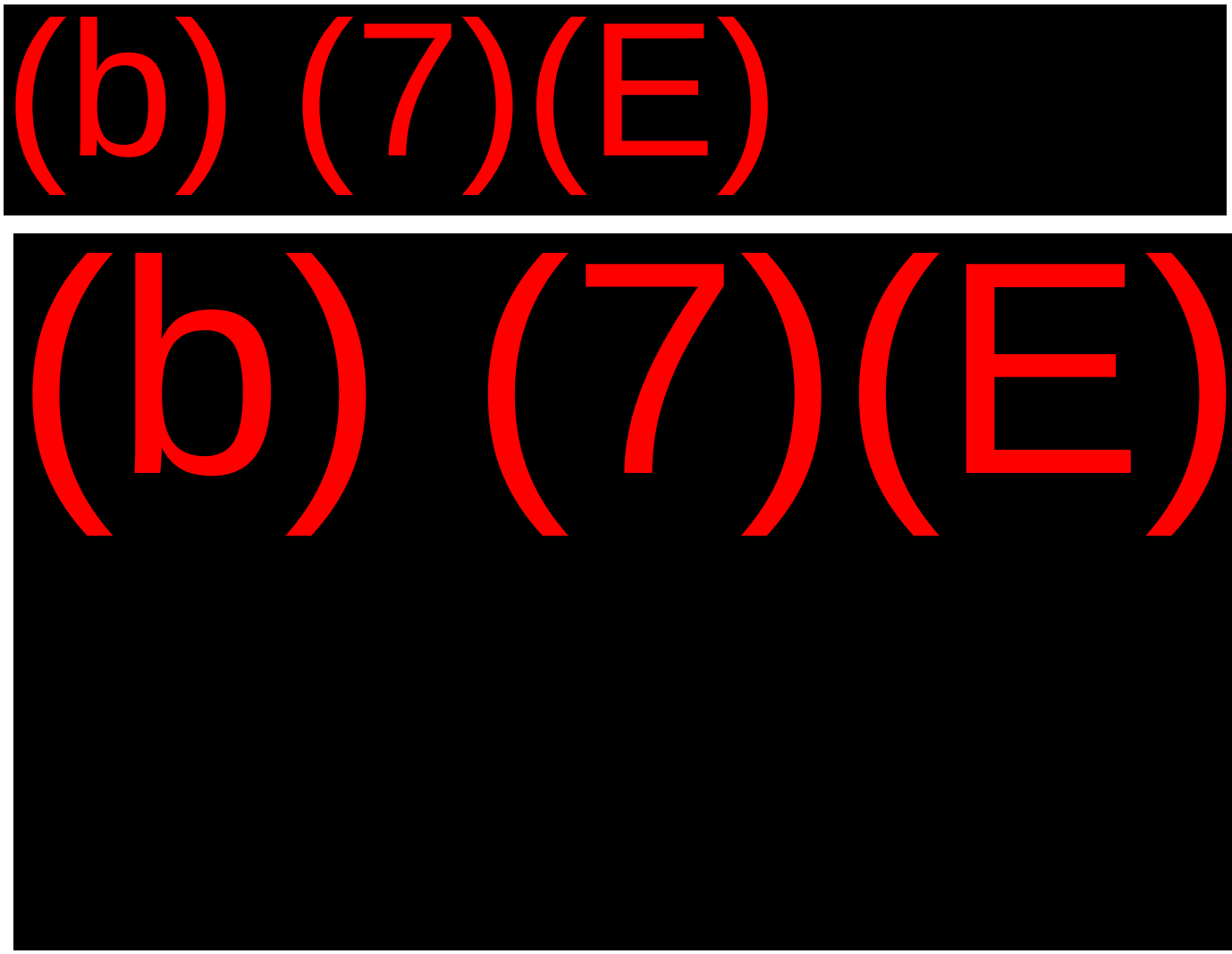
13.4 Storing Forensic Images



13.5 Archiving Forensic Images



13.6 Retention of Forensic Evidence Files



13.8 Returning Files or Equipment that Had Contained Evidence or Contraband to Third Parties

In certain situations, it may be necessary to return files or equipment that had contained child pornography or other evidentiary files. For example, a search warrant is executed on a business, and a computer is seized that contains both child pornography and a proprietary work product for the company. In such situations, every effort must be made to ensure that no child pornography is returned. The business or individual must supply to the CFA a list of files or directories needed by the business or individual, as well as the destination media preferred by the business or individual (e.g., Digital Versatile Disc (DVD)/CD, hard drive, or thumb drive). The CFA will ensure that the files requested do not contain any contraband and will transfer the files to the destination media. The media can then be returned to the business or individual.

Equipment that contains storage media can be returned at the CFA's discretion once the storage media has been removed. Discretion should be based upon whether the CFA needs the device to complete the examination. Original evidentiary storage media should not be returned before final adjudication of the case unless exigent circumstances apply. Exigent circumstances can

include, but are not limited to, severe financial hardship (e.g., inability to purchase replacement storage resulting in the loss of business revenue) and proprietary equipment (e.g., developing technology or a unique or irreplaceable device).

In cases where storage devices contained child pornography, CFAs must (b) (7)(E) the media one time and perform one verification. Once the case has been adjudicated and the storage media has been wiped, it may be returned to the owner.

Chapter 14. ENCRYPTION OF FORENSIC LAPTOPS/TABLETS

(b) (7)(E)

Chapter 15. HARDWARE/SOFTWARE

15.1 Write-Block/Imaging Devices

(b) (7)(E)

15.2 Imaging Software

(b) (7)(E)

(b) (7)(E)

15.3 Analysis Software

(b) (7)(E)

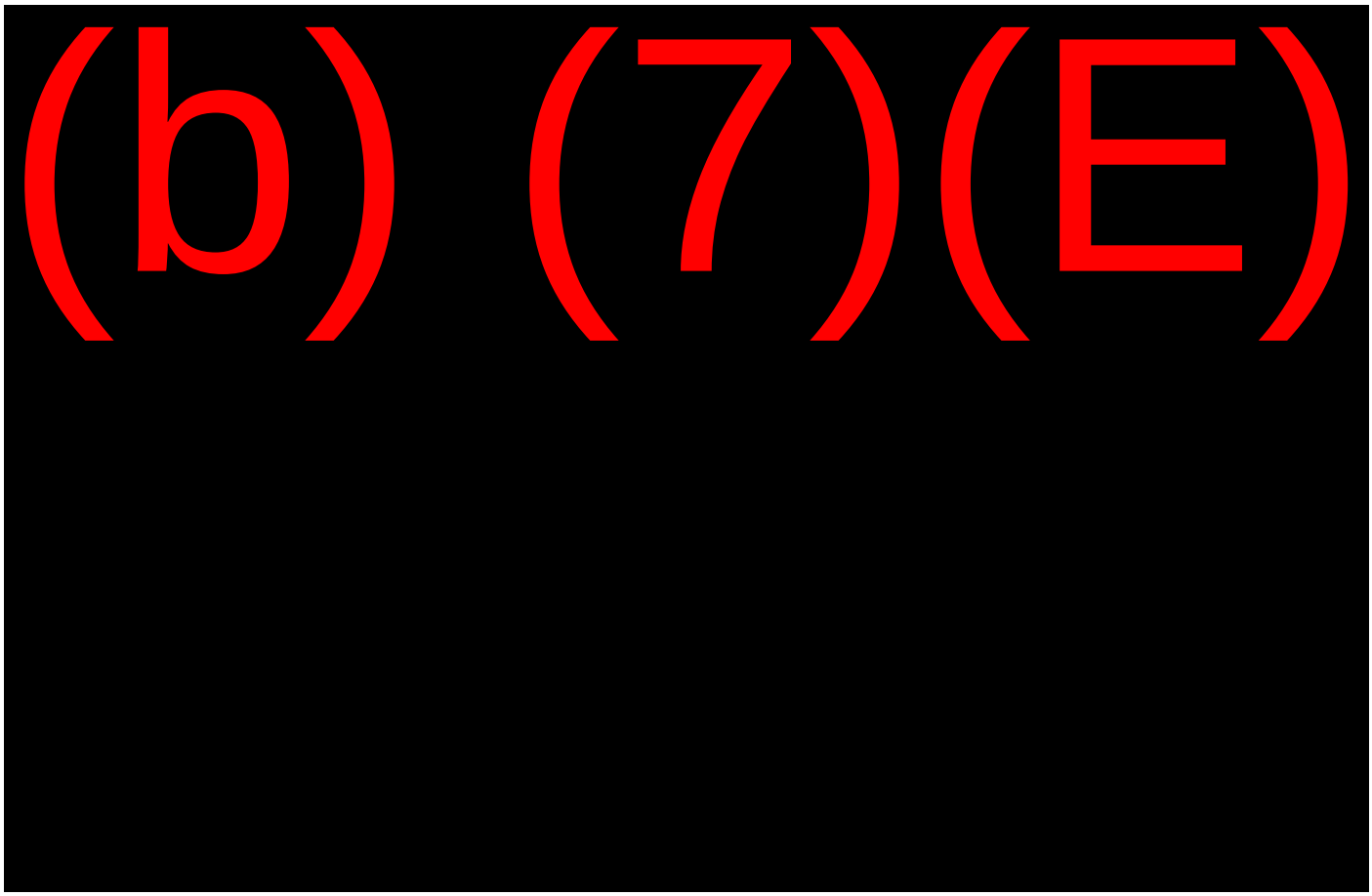
15.4 Supplemental Software

(b) (7)(E)

15.5 Approval Process for New Hardware/Software

(b) (7)(E)

15.6 Validation Requirements/Procedures



Chapter 16. IMAGING PROCEDURES

16.1 Imaging Procedures

16.2 Destination Drive Preparation

(b) (7)(E)

16.3 Mobile Devices

(b) (7)(E)

16.3.1 Seizure of Evidence

Trained personnel should follow all policies and procedures set forth in Chapter 13, as well as the guidelines provided below.

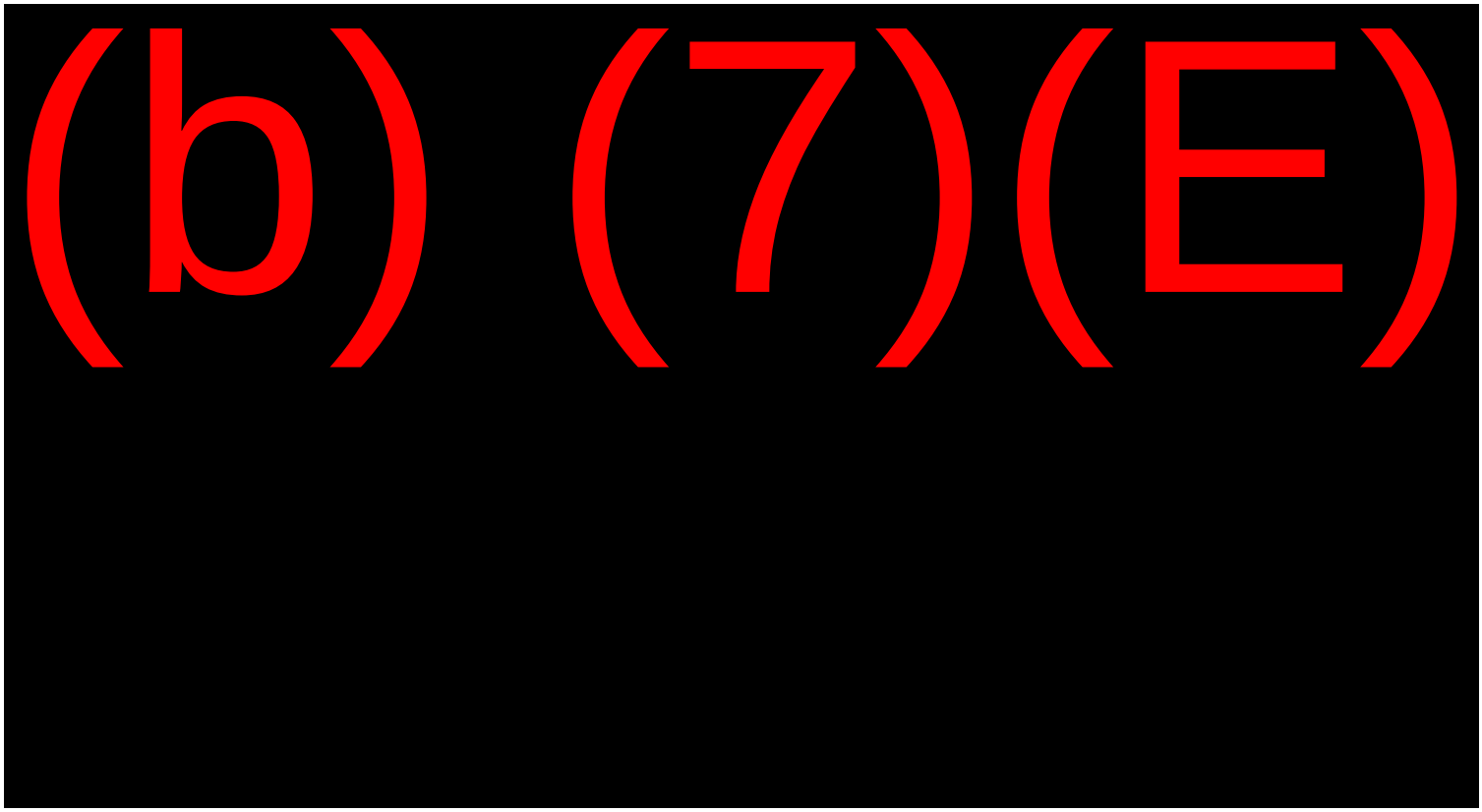
(b) (7)(E)

16.3.2 Intake of Evidence

Trained personnel should follow all policies and procedures set forth in Chapter 13. In addition,

(b) (7)(E)

(b) (7)(E)



16.3.4 Report of Findings

CFAs should follow all policies and procedures set forth in Chapter 12 of this Handbook.

16.4 Encryption

(b) (7)(E)

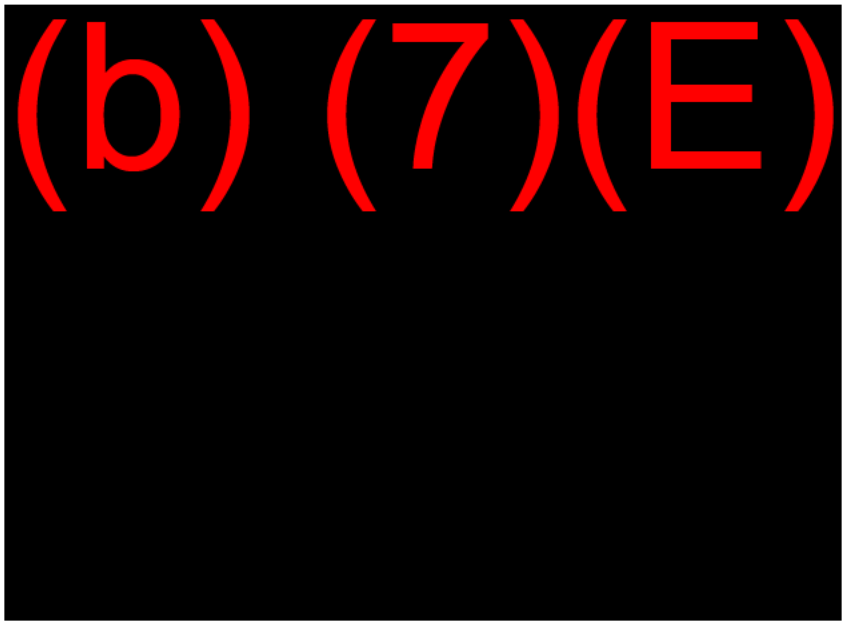
Chapter 17. FORENSIC ANALYSIS PROCEDURES

(b) (7)(E)

Chapter 18. DOCUMENTATION AND REPORTING

A standardized folder organization is necessary to provide uniformity throughout the CFP. By adopting such standardization, any CFA will be able to rapidly find the image files and work product of any other CFA at any point in the examination. The following is an example of the folder organization to be used:

(b) (7)(E)



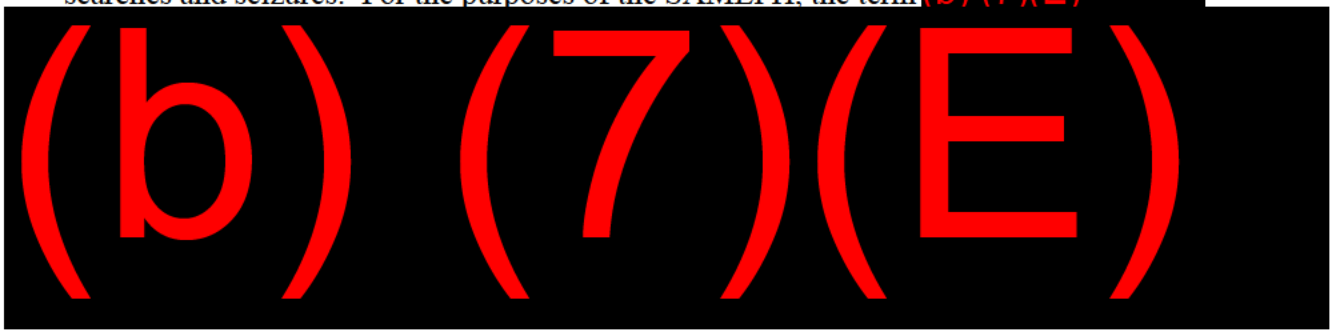
CFAs must ensure that all forensic assistance requests are accompanied by the Computer Forensics Assistance Request Worksheet (see Appendix F). This worksheet must be routed from the case agent, through the case agent's supervisor, to the local CFC who is responsible for assigning such assistance requests to CFAs.

Chapter 19. GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS

If SAs believe that electronic devices will be encountered and searched or seized, they must contact their local CFA. If a local CFA is not available, SAs should immediately contact their CFC to coordinate interim support. SAs must contact a CFA when conducting searches of electronic devices. If necessary, SAs should consult the local USAO or their local OPLA embedded attorney, since, outside of a border search or consent, such searches and/or seizures should be detailed in a warrant. If a CFA is not available, SAs executing the actual search and/or seizure must take precautions when disassembling and packing computer equipment. (b) (7)(E)

(b) (7)(E)

SAs must adhere to the SAMEPH, which provides policy and procedures relating to computer searches and seizures. For the purposes of the SAMEPH, the term (b) (7)(E) "



(b) (7)(E)

19.1 Exigent Circumstances

(b) (7)(E)

19.2 Border Search

Due to potential district-specific court rulings, SAs should coordinate with OPLA and local USAOs prior to conducting a border search of electronic devices to ensure adherence to agency policy and to the most recent case law. At the border (or its functional equivalent), ICE has the broad authority to conduct routine searches of persons and things upon their entry into or exit out of the United States without first obtaining a warrant and without suspicion. This authority stems from a long-standing and well recognized exception to the Fourth Amendment that is premised on the government's interest in protecting its citizens from the entry of persons and items harmful to U.S. interests. The U.S. Supreme Court has recognized that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." See *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

With respect to the border search of electronic devices, federal courts have concluded that the routine searching of electronic devices is within the broad border search exception exercised by ICE and have generally endorsed the view that laptop computers or other electronic devices are subject to suspicionless searches at the border. However, the U.S. Courts of Appeal for the Fourth and Ninth Circuits have held that use of forensic tools to search an electronic device is not a "routine search" and so, in those circumstances, some level of particularized suspicion is required. *See U.S. v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc). Accordingly, CFAs should only conduct a border search of an electronic device if there is reasonable suspicion that the device contains information relating to a violation of the laws enforced or administered by ICE. SAs and CFAs should consult ICE Directive 10044.1 (former number: 7-6.1), "Border Searches of Electronic Devices," dated August 18,

2009, or as updated, as well as the "Legal Update – Border Search of Electronic Devices" internal guidance message sent on May 11, 2018, for further direction on such searches.

As specified in ICE Directive 10044.1 (former number 7.6-1), border searches of electronic devices must be conducted by HSI SAs or other properly authorized officers with customs border search authority, such as persons cross-designated as customs officers (e.g., TFOs) under 19 U.S.C. § 1401(i). At any point during a border search, SAs may detain electronic media, or copies thereof, for further review, either on-site or at an off-site location, including an associated demand for assistance from a third agency, pursuant to 19 U.S.C. § 507. SAs must contact their local CFA for assistance in searching any electronic media. Computer Forensic Analysts can conduct border searches at the request of, and while assisting, HSI SAs. If a local CFA is not available, SAs must contact the CFC to coordinate interim support. For more information on border searches of electronic devices, including specific guidance regarding chain of custody requirements for detentions of originals or images, demands for assistance, and information sharing, SAs and CFAs should consult ICE Directive 10044.1 (former number: 7-6.1), "Border Searches of Electronic Devices," dated August 18, 2009, or as updated.

Authorities under the customs laws of the United States in no way limit authorities to search and retain evidence available to SAs under the Immigration and Nationality Act.

19.3 Consent

SAs may search a place or object without a warrant and without probable cause if a person with actual or apparent authority has consented, and such consent has been given voluntarily and without coercion or duress. A person who consents to a search may limit this consent to a certain area (e.g., if a suspect consents to share some of the information contained in his or her computer but attempts to prevent SAs from seeing the file password, this constitutes a limit to his or her consent; SAs who attempt to acquire the password have then exceeded the limitations of the consensual search). **(b) (7)(E)**

(b) (7)(E)

Questions regarding the scope of consent or any possible revocation of consent should be discussed with CFU or the local OPLA embedded attorney.

19.4 Privacy Protection Act

The Privacy Protection Act (PPA) (42 U.S.C. § 2000aa) prohibits the U.S. Government, in connection with an investigation or prosecution of a criminal offense, from searching and seizing work products or documentary materials that are intended for publication. Work products and documentary materials do not include contraband, fruits of the crime, or items otherwise criminally possessed. The purpose of the PPA is to provide the press and other innocent third parties who are not suspected of a crime with certain protections not provided by the Fourth Amendment. If there are materials protected by the PPA commingled with criminal evidence that is unprotected, there is no liability on LEOs for the seizure of PPA-protected materials. However, the PPA-protected materials that are incidentally seized may not be searched. SAs should address questions on this and, in particular, on searching such documents during a border search to CFU or their local OPLA embedded attorney.

Appendix A

Examples of Recommended Performance Goals for Computer Forensics Agents and Computer Forensics Analysts

(b) (7)(E), (b) (2)

(b) (7)(E)

Appendix B

Adam Walsh Examination Worksheet

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Adam Walsh Examination Worksheet

(b) (7)(E)

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Adam Walsh Examination Worksheet

Adam Walsh Child Protection and Safety Act of 2006

18 U.S.C. § 3509(m), Prohibition on Reproduction of Child Pornography

(1) In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court.

(2) (A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title), so long as the Government makes the property or material reasonably available to the defendant.

(B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing, and examination at a Government facility of the property or material by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial.

Appendix C

Computer Forensics
Case File Folder Go-by

INSIDE FRONT COVER

ADMINISTRATIVE ITEMS

-CASE CHRONOLOGY AND REVIEW SHEET
(ICE FORM 73-005)
-INVESTIGATIVE CASE RECORD (CASE OPENING)
-COMPUTER FORENSICS UNIT CASE REVIEWS

FIRST DIVIDER (FRONT)

COMPUTER FORENSICS REPORTS OF INVESTIGATION

-REPORTS OF INVESTIGATION (ROIs):
-THE MOST CURRENT ROI ON THE TOP
-ROI NUMBER 1 ON THE BOTTOM

FIRST DIVIDER (BACK)

COURT DOCUMENTS AND SEARCH AUTHORITY

-COMPUTER FORENSICS PROGRAM REQUEST WORKSHEET WITH ATTACHED AUTHORITY
-SEARCH WARRANT
-COMPUTER FORENSICS CONSENT WORKSHEET
-COMPUTER FORENSICS BORDER RESPONSE WORKSHEET

SECOND DIVIDER (FRONT)

HSI DOCUMENTS

-ANY RELEVANT HSI DOCUMENTS
-ANY RELEVANT ICM RECORDS
-SEACATS INCIDENT REPORTS
-MEMORANDA
-LETTERS
-CUSTODY RECEIPTS
-INVENTORY SHEETS

-COMPUTER FORENSICS AGENT/
COMPUTER FORENSICS ANALYST
OTHER WORKSHEETS
-ADAM WALSH EXAMINATION WORKSHEETS
-COMPUTER FORENSICS IMAGE RELEASE
WORKSHEETS

SECOND DIVIDER (BACK)

ORIGINATING CASE OR OTHER AGENCY DOCUMENTS

-CASE ROIs
-STATE AND LOCAL POLICE DOCUMENTS
-OTHER FEDERAL AGENCY DOCUMENTS

INSIDE BACK COVER

INVESTIGATIVE / EXAMINATION PAPERWORK

-MISCELLANEOUS DOCUMENTS
-INVESTIGATIVE/EXAMINATION NOTES
-PHOTOCOPIES
-DIGITAL COPIES OF FORENSICS REPORTS
-NO CONTRABAND
-COMPUTER FORENSICS EXAMINATION WORKSHEETS

Appendix D

Computer Forensics Examination Worksheet

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Computer Forensics Examination Worksheet

(b) (7)(E)

(b) (7)(E)

Appendix E

Example of a Computer Forensics Report of Investigation

(b) (7)(E)

(b) (7)(E)

Appendix F

Computer Forensics Assistance Request Worksheet

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Computer Forensics Assistance Request Worksheet

(b) (7)(E)

Appendix G

Computer Forensics Consent Worksheet

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Computer Forensics Consent Worksheet

(b) (7)(E)

Appendix H

Computer Forensics Border Response Worksheet

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Computer Forensics Border Response Worksheet

(b) (7)(E)

Appendix I

Computer Forensics (b) (7)(E) (b) (7)(E)

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Computer Forensics (b) (7)(E) [redacted]

(b) (7)(E)

Appendix J

Computer Forensics Image Release Worksheet

U.S. Immigration and Customs Enforcement

Homeland Security Investigations

CYBER CRIMES CENTER
Computer Forensics Unit

Computer Forensics Image Release Worksheet

(b) (7)(E)

Appendix K

Computer Forensic Validation and Testing Go-by

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Appendix L

FIRST RESPONDERS CHECKLIST

(b) (7)(E)

Appendix M

ACRONYMS

ACE	AccessData Certified Examiner
(b) (7)(E)	[redacted]
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
(b) (7)(E)	[redacted]
C3	Cyber Crimes Center
CA	Criminal Analyst
CBP	U.S. Customs and Border Protection
CD	Compact Disc
CFA	Computer Forensics Agent
CFA	Computer Forensics Analyst
CFAT	Computer Forensics Annual Training
CFC	Computer Forensics Coordinator
CFCE	Certified Forensics Computer Examiner
CFP	Computer Forensics Program
(b) (7)(E)	Computer Forensics Program Web Site
CFU	Computer Forensics Unit
DAD	Deputy Assistant Director
DHL	Dalsey Hillblom Lynn
DHS	Department of Homeland Security
DOS	Disk Operating System
DSAC	Deputy Special Agent in Charge
DVD	Digital Versatile Disc
EAD	Executive Associate Director
EAGLE	Enforcement Integrated Database Arrest Graphic User Interface for Law
(b) (7)(E)	[redacted]
FER	Field Examination Report
FOUO	For Official Use Only
FRCrP	Federal Rules of Criminal Procedure
(b) (7)(E)	[redacted] eitures
GB	Gigabyte
GCFA	GIAC Certified Computer Forensics Analyst
GCFE	GIAC Certified Computer Forensics Examiner
GIAC	Global Information Assurance Certification
GS	General Schedule
HB	Handbook
HERO	Human Exploitation Rescue Operative
HSI	Homeland Security Investigations

IACIS	International Association of Computer Investigative Specialists
ICE	U.S. Immigration and Customs Enforcement
(b) (7)(E)	[redacted]
IDE	Integrated Drive Electronics
LEO	Law Enforcement Officer
MB	Megabyte
MD	Management Directive
MD5	Message Digest Algorithm 5
MS-DOS	Microsoft Disk Operating System
NIST	National Institute of Standards and Technology
NTFS	New Technologies File System
OI	Office of Investigations
OPLA	Office of the Principal Legal Advisor
OS	Operating System
PALMS	Performance and Learning Management System
PDA	Personal Digital Assistant
PPA	Privacy Protection Act
RA	Resident Agent
RAC	Resident Agent in Charge
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
ROI	Report of Investigation
SA	Special Agent
SAC	Special Agent in Charge
SAMEPH	Seized Asset Management and Enforcement Procedures
SCSI	Small Computer System Interface
(b) (7)(E)	
SHA-1	Secure Hash Algorithm
SIM	Subscriber Identity Module
SPADA	System Preview and Data Acquisition
TFO	Task Force Officer
UPS	United Parcel Service
USAO	U.S. Attorney's Office
USB	Universal Serial Bus
U.S.C.	U.S. Code
USPS	U.S. Postal Service