**YOUR LOGO HERE**

**Computer Forensic Analysis**

**Training Manual**

**DOCUMENT CONTROL #**

**CLASSIFICATION LEVEL HERE**

May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552) exemption number and category: **7, Law Enforcement**

**Department of Name of Agency review required before public release**

Name/Org: Your name/org Date:

Guidance (if applicable):

**Record of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Pages Affected | Description | Author/Editor |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

All new trainees within the [Agency name] who are assigned to computer forensics shall be assigned to a Senior Forensic Examiner and fully complete this manual. This manual is broken into a series of sections and it is allowable for a trainee to work on different sections concurrently as the opportunities may arise. The trainer will meet regularly with the laboratory director to provide status updates. The trainer is also responsible for maintaining the training manual in an up-to-date fashion.

At the completion of the manual the trainer will prepare a memo for the laboratory director with their recommendation about the trainee’s status.

In addition to this training manual other outside training should be considered. This training includes:

* Basic Data Recovery and Analysis – National White Collar Crime Center
* Intermediate Data Recovery and Analysis – National White Collar Crime Center
* Advanced Data Recovery and Analysis – National White Collar Crime Center
* Basic Computer Forensic Examiner (BCFE) course – International Association of Computer Investigative Specialists
* SANS FOR408
* SANS FOR508

**Section 1 – General Laboratory Procedures**

The trainee should be familiar with the general practices and procedures used at the [Agency name] Digital Evidence Forensic Laboratory.

Assigned Tasks:

1. Read and become familiar with the [Agency name] Administrative Procedures Manual.
2. Receive training on the case management system to input case data.
3. Show familiarity with evidence handling and security procedures.
4. Be assigned key fob and alarm code and understand how to set burglar alarm.
5. The trainer should assign the trainee relevant reading from the library or from the [Agency name] digital resource library.

**Section 2 – General Computer Knowledge**

The objective of this section is to certify that the trainee can demonstrate the knowledge of computers that will be needed for casework.

Assigned tasks:

1. The trainee shall be able to explain the differences between file structures such as FAT16, FAT32, NTFS, EXT, and HFS.
2. The trainee shall be familiar with the various computer operating systems such as DOS, Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7, Apple, and Linux.
3. The trainee shall be able to identify the internal components of a computer system and understand their function. Examples include; RAM, hard drive, motherboard, CPU. Etc.
4. The trainee shall be familiar with various types of storage media such as hard drives, floppy disks, CD’s, DVD’s, Zip disks, and flash memory devices.
5. The trainee shall demonstrate his or her general computer knowledge by successfully completing a written or practical examination on the topic.

**Section 3 – Policies and Procedure in Computer Forensics**

The objective of this section is to give the trainee a working knowledge of the policies and procedures used in the forensic examination of computer evidence.

Assigned Tasks:

1. The trainee shall read and understand the Computer Forensics Technical Procedure Manual.
2. Study additional reading as assigned by the trainer. Examples may be verification papers, manuals, articles, books, website material, and whitepapers.
3. Attend an approved training session on the use of computer forensics software (such as AccessData bootcamp).

**Section 4 – Forensic Imaging**

The objective of this section is to allow the trainee to begin working with computer forensic evidence under the immediate supervision of a Senior Forensic Examiner.

Tasks Assigned:

1. The trainee shall assist in preparing computer evidence for examination under the direct supervision of a trained examiner.
2. The trainee shall have a working knowledge of the verification procedure within the forensic laboratory. The trainee shall be proficient in verifying equipment used during analysis.
3. The trainee shall understand how to forensically wipe a target drive and how to ensure a drive has been wiped.
4. The trainee shall become familiar with imaging various types of media including hard drives, USB drives, flash drives, optical drives and Zip disks.
5. The trainee shall demonstrate for the trainer how to completely image a device using forensically sound methods and pursuant to the laboratory technical procedures as a practical examination.

**Section 5 – Specific Forensic Knowledge, Skills, and Abilities**

The objective of this section is to ensure that the trainee has specific knowledge in key computer forensic methodologies, concepts, procedures, and information. This is certainly not a complete list, and the trainer should elicit additional questions and conversations based upon this list.

Tasks Assigned:

1. The trainee shall demonstrate their ability to successfully process a forensic image using an analysis tool of their choice (FTK or X-­‐Ways for example).
2. The trainee shall understand and describe what data carving is, how it works manually, and demonstrate how to use tools such as FTK and/or File Extractor Pro.
3. The trainee shall understand key concepts and terms such as bit, byte, nibble, word, dword, kilobyte, megabyte, gigabyte, terabyte, and hex.
4. The trainee shall understand the windows registry, describe what it is, where it’s located, how to forensically examine it, and what evidence may be located within the registry.
5. The trainee shall understand what a link file is, how they are created, and the forensic importance of them.
6. The trainee shall understand what prefetch files are, how to examine them, and what they are.
7. The trainee shall understand and describe the difference between allocated and unallocated space on a storage device.
8. The trainee shall demonstrate proficiency with various forensic software and hardware applications.
9. The trainee shall describe what .plist’s are, where they are located and how to forensically examine them.
10. The trainee shall describe what a file header and footer is, and how that information is used within a forensic examination.
11. The trainee shall understand and demonstrate proficiency with hash values and describe the differences between checksum 64, MD5, SHA1, SHA256, and others.
12. The trainee shall describe what printer spool files are and how to located them in a forensic examination.
13. The trainee shall describe what system restore points are and how they can be valuable in a forensic investigation.
14. The trainee shall describe what volume shadow copies are, how they are created, and how they can be used in a forensic examination.
15. The trainee shall demonstrate how to create a timeline and whythat information is so important in a forensic investigation.

**Section 6 – Supervised Casework**

The objective of this section is to allow the trainee to apply his or her knowledge of computer forensics to an actual case while being supervised.

Tasks Assigned:

1. The trainee shall assist in working cases under the direct supervision of a Senior Forensic Examiner. The trainee shall assist in all facets of the case.
2. If possible, the trainee should attend court with a trained examiner to watch them testify as an expert witness.
3. The trainee shall successfully complete a minimum of four months of casework under the Senior Forensic Examiner.

**Section 7 – Competency Tests**

The objective of this section is to ensure the trainee has the competency needed to conduct casework without the direct supervision of a Senior Forensic Examiner.

Assigned Tasks:

1. The trainee is encouraged to obtain a certification in the seizure of digital evidence, such as CEECS, DECT, etc.
2. The trainee is encouraged to attend forensic certification training such as IACIS CFCE, SCERS, FBI Cart, etc.
3. The trainee shall complete a mock forensic examination on a piece of media provided to them by the laboratory director. They shall find all pertinent information on the media and complete a report and submit that report to their trainer. The trainer will review it and also give it to the laboratory director for review.
4. The trainee shall meet with the laboratory director and become familiar with the accreditation process and other policies and procedures.

At the completion of this manual the trainer shall provide a written recommendation to the laboratory director as to the status of the trainee. The recommendations may include that they be allowed to handle casework on their own, have their training extended, be provided remedial training, or be terminated from the training program.

The trainer shall meet with the laboratory director on a regular basis to discuss the progress of the trainee.

**Signatures:**

|  |  |
| --- | --- |
| Trainer Printed Name: |  |
|  |  |
| Trainer Signature: |  |
|  |  |
| Date of manual completion: |  |

By signing this manual I acknowledge the trainee successfully completed the competencies in this manual and recommend the trainee be allowed to conduct casework.

|  |  |
| --- | --- |
| Trainee Printed Name: |  |
|  |  |
| Trainee Signature: |  |

By signing this manual I acknowledge that I fully understand the contents of the manual and each competency was explained to me by my trainer. I understand that by signing this manual I am stating that I understand the expectations for completing mobile device forensics and am expected to conduct forensic examinations pursuant to this training.

|  |  |
| --- | --- |
| Laboratory director Printed Name: |  |
|  |  |
| Laboratory director Signature: |  |
|  |  |
| Date Signed: |  |

Trainee released to perform computer forensics.

Trainee not released to perform computer forensics.