**YOUR LOGO HERE**

**Mobile Device 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 laboratory who are assigned to mobile device 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:

* BK Forensics Mobile Phone Seizure Certification
* SEARCH Cell Phone Investigations
* SANS 585
* CelleBrite Logical Operator Course
* CelleBrite Physical Analyst Course

**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 Mobile Device Knowledge**

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

Assigned tasks:

1. The trainee shall be able to explain the differences between communication modes used on cellular devices such as GSM, CDMA, and TDMA.
2. The trainee shall understand what a SIM card is, how it’s used, and what kind of information can be contained on a SIM card.
3. The trainee shall be able to describe how to make a cellular device safe from outside RF signals and the various technologies and equipment used to do so.
4. The trainee shall be familiar with various models of phones and common terminology used with cellular devices as well as web resources to research additional information.
5. The trainee shall demonstrate knowledge of the Faraday box and articulate how it functions.
6. The trainee shall demonstrate his or her general cellular device knowledge by successfully completing a written or practical examination on the topic.
7. The trainee shall be able to explain terms such as IMEI, DEC, ESN, MIN, MDN, etc.
8. The trainee shall be familiar with various external storage devices used with cellular phones such as MicroSD cards and how to handle them.

**Section 3 – Policies and Procedure in Mobile Device 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 mobile devices.

Assigned Tasks:

1. The trainee shall read and understand the Mobile Device 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.

**Section 4 – Mobile Device Forensic Tools**

The objective of this section is to give the trainee a working knowledge of the different mobile device forensic software applications utilized within the [Agency name] Digital Evidence Forensic Laboratory.

Tasks Assigned:

1. The trainee shall demonstrate working knowledge of the CelleBrite UFED Physical Pro and understand when it is appropriate to use it.
2. The trainee shall demonstrate how to use the password bypass feature of the CelleBrite unit.
3. The trainee shall understand the difference between a physical and logical acquisition of the mobile device and how to conduct both exams.
4. The trainee shall show how to use different targets for the CelleBrite including PC, USB device, SD card, etc.
5. The trainee shall show competency with the CelleBrite software including the report manager and physical acquisition software.
6. The trainee shall understand how different mobile forensic software applications may obtain different information.
7. The trainee shall understand how to properly manually browse a phone and use the Project-­‐a-­‐Phone device.
8. The trainee shall demonstrate proficiency in the use of Paraben Device Seizure.
9. The trainee shall demonstrate proficiency in the use of Susteen Data Pilot.

**Section 5 – Forensic Imaging**

The objective of this section is to train the new examiner on how to properly forensically image removable media contained within a mobile device.

Tasks Assigned:

1. The trainee shall assist in preparing mobile 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 task force. 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 removable flash media, including but not limited to MicroSD cards.
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 6 – Supervised Casework**

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

Assigned Tasks:

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 one month 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, MPSC, NW3C STOP, etc.
2. 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.
3. 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 video forensics.

Trainee not released to perform video forensics.