**YOUR LOGO HERE**

**Mobile Device Forensic Analysis**

**Technical 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Field Response / Evidence Preservation Protocol 4](#_Toc403588560)

[Subscriber Identity Module Examination 6](#_Toc403588561)

[General Cellular Phone Examination Protocol 7](#_Toc403588562)

[Removable/External Media Imaging Protocol 9](#_Toc403588563)

[Forensic Imaging Protocol of Removable Flash Media 10](#_Toc403588564)

[Creation of Results Report 12](#_Toc403588565)

|  |
| --- |
| Field Response / Evidence Preservation Protocol |

**1. Purpose**

The purpose of this procedure is to provide direction to laboratory personnel when preserving digital evidence in the field. This protocol applies to all staff within the laboratory.

**2. Equipment Needed**

1. Digital camera
2. Evidence containers/bags
3. Faraday bag/box
4. Gloves
5. Paper/pen
6. Permanent pen

**3. Calibration**

All hardware and software used in this protocol shall be validated and the validation documented within the [Agency Name] Validation Manual.

**4. Procedures**

1. Immediately take control over the device and restrict access.
2. If possible, photograph the device in the condition it was found.
3. Immediately isolate the device from the cellular network. This may be accomplished by the use of a Faraday bag or box, aluminum foil, placing the device into airplane mode, or turning the device off.
4. Prior to turning the device off, the investigator should attempt to determine if there are any passwords or PIN’s on the device. Turning a device off that has a PIN will lock the device.
5. The device should be delivered to the forensics laboratory as soon as possible to reduce the chances of the battery running low.
6. If a mobile device is found in the off position, the device should be left off and transported in that condition.
7. Any charging cables located should be transported with the device to the laboratory.

**5. Important Notes**

Cellular phone devices constantly communicate with cell towers, which actively change the data on the device. Investigations must take precautions to preserve evidence on cellular devices and isolate them from radio frequency.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| Subscriber Identity Module Examination |

**1. Purpose**

The purpose of this protocol is to discuss the proper methods for conducting a forensic examination of a Subscriber Identity Module (SIM) card. This protocol is to be used by all laboratory members who conduct forensic examinations.

**2. Equipment Needed**

1. Forensic computer or CelleBrite unit
2. USB or serial SIM card reader if not using CelleBrite
3. Storage media

**3. Calibration**

All hardware and software used in this protocol shall be validated and the validation documented within the [Agency Name] Validation Manual.

**4. Procedures**

1. Remove the SIM card from the cellular phone and photograph the SIM to obtain all nomenclature.
2. Place the SIM card into the CelleBrite unit or the USB/Serial SIM card reader.
3. Launch the appropriate software application and select to extract data from the SIM card.
4. Review the findings of the forensic software application and report the findings.
5. If the SIM is locked, attempt to determine the PIN. If the PIN cannot be determined, consider obtaining the PUK from the cell phone provider.

**5. Important Notes**

None.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| General Cellular Phone Examination Protocol |

**1. Purpose**

This purpose of this protocol is to assist the examiner with the forensic examination of a cellular device. This protocol is to be used by all laboratory staff members who conduct mobile device forensic examinations.

**2. Equipment Needed**

1. Faraday isolation device
2. Approved cellular phone forensic software/hardware
3. Forensic computer
4. Charging cables
5. Data cables

**3. Calibration**

All hardware and software used in this protocol shall be validated and the validation documented within the [Agency Name] Validation Manual.

**4. Procedures**

1. Ensure the cellular phone has been isolated from the network. This can be accomplished by using a Faraday device or by placing the phone in airplane mode.
2. Determine if the phone has adequate battery life to conduct an examination. Generally
3. ¼ of battery life or more is required for an examination. If needed, charge the device prior to the exam or simultaneous to the exam if the model of phone supports charging via USB.
4. Photograph the phone prior to examination. Ensure to photograph the SIM card, any flash media expansion cards, and all relevant nomenclature of the phone.
5. If a SIM exists, first examine the SIM card using the protocol in this manual.
6. If a flash card exists, remove the card, photograph it, and examine it pursuant to the protocol in this manual.
7. At the conclusion of the SIM examination, replace the SIM into the phone and prepare to conduct the phone examination.
8. Determine what examination will be accomplished; Physical analysis or Logical analysis.
9. Determine what software applications support the model of phone and what options are available.
10. If a physical analysis is available, conduct the physical dump of the phone and examine that information. After the physical dump is done, do a normal logical dump.
11. If needed, extract the complete file system of the phone and import it into a forensic application such as FTK and data carve the file system.
12. It may be required to use multiple applications for a single device to obtain all possible evidence.
13. At the conclusion of the forensic examination, manually browse the phone to compare the results of the forensic exam with the information displayed on the phone and note any inconsistencies in the examination report.
14. If needed, manually document the phone’s contents using a digital camera or Project‐a‐Phone device.

**5. Important Notes**

Forensic examiners should ensure the cellular device has adequate battery life to conduct the examination. If needed, the examiner should charge the phone prior to the examination using the charging tips within the forensics laboratory or a supplied cable by the case agent. Examiners must also ensure the cellular device has properly been isolated from the cellular network prior to beginning the examination.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| Removable/External Media Imaging Protocol |

**1. Purpose**

The purpose of this protocol is to provide information to forensic examiners on how to image various types of removable media. This protocol is to be used by all laboratory staff members who conduct mobile device forensic examinations.

**2. Equipment Needed**

1. Forensic computer
2. Prepared target hard drive or network storage
3. Validated forensic imaging software

**3. Calibration**

All hardware and software used in this protocol shall be validated and the validation documented within the [Agency Name] Validation Manual.

**4. Procedures**

1. If possible write protect any removable media. Some media will have a write blocking switch, or a hardware write blocker should be used.
2. Forensically imaging the device should occur, generally with FTK Imager and the image file should be stored on the network storage or a target hard drive.

**5. Important Notes**

Battery powered devices such as MP3 players and PDA’s should be treated carefully to ensure the battery does not go dead prior to examination as data loss can occur.6. References

1. Validation manual
2. Administrative manual

|  |
| --- |
| Forensic Imaging Protocol of Removable Flash Media |

**1. Purpose**

This protocol describes the steps to be taken by computer forensic examiners during forensic imaging of removable flash media. This protocol applies to all members of the laboratory who performs mobile device forensic analysis.

**2. Equipment Needed**

1. Forensic computer
2. Prepared target hard drive or network storage
3. Validated forensic imaging software

**3. Calibration**

All hardware and software used in this protocol shall be validated and the validation documented within the [Agency Name] Validation Manual.

**4. Procedures**

1. Attach the evidence flash media device to a hardware write blocker.
2. Attach the write blocker to a forensic computer.
3. Boot the forensic computer into Windows.
4. Using an approved software application create an MD5 hash of the evidence flash drive prior to any imaging or other work.
5. Create a forensic image using the approved imaging software onto the target hard drive or network storage.

If using FTK Imager:

1. Open FTK Imager and click the “Create Disk Image” button on the toolbar.
2. Select the type of disk (generally Physical Drive).
3. Select the evidence hard drive.
4. Select to verify images after they are created, precalculate progress statistics, and to create a directory listings of all files in the image after they are created.
5. Press the “add” button.
6. Select a “raw dd” image.
7. Enter case specifics such as case number, evidence number and examiner name.
8. Browse to the target hard drive.
9. Name the image.
10. Set the image size to “0” if imaging to the network storage.
11. Press “start”

**5. Important Notes**

This protocol is for removable flash media found commonly in mobile devices such as MicroSD cards and SD cards.

**6. References**

1. Validation manual
2. Administrative manual

|  |
| --- |
| Creation of Results Report |

**1. Purpose**

This protocol describes the steps to be taken when creating an evidence results report for forensic examinations. This protocol applies to all laboratory members who perform forensic analysis.

**2. Equipment Needed**

1. Forensic computer
2. CD/DVD Duplicator

**3. Calibration**

None.

**4. Procedures**

1. Within the laboratory electronic cases folder for the specific case being worked on a folder called “CD” is created.
2. Within the “CD” folder is all the html files needed for the CD as well as the files exported as exhibits for the evidence.
3. The examiner must test all hyperlinks prior to burning the “CD” folder to a CD/DVD using the CD/DVD duplicator machine.
4. Once everything has been tested and works the entire contents of the “CD” folder should be transferred to the CD/DVD duplicator machine and the needed number of discs created.
5. The standard laboratory label shall be printed on the discs which include the examiner’s name, date of creation, case number and other warnings about possible disturbing content.

**5. Important Notes**

This protocol discusses how to create forensic examination result reports for the submitting agency. In the event that the CD/DVD Duplicator and printer are not functioning a CD can be created using the forensic machine and a laser printer label can be affixed to the evidence disc.

This protocol is also for cases that require an optical disc for evidence. In rare situations only a cover page is required which is printed out and signed by the examiner and later scanned in to the laboratory electronic case jacket.

**6. References**

1. Validation manual
2. Administrative manual