DEUSOP02 – Mobile Device Acquisition

Table of Contents

1. Scope

1.1. This standard operating procedure is utilized for the acquisition of a mobile device.

2. Background

2.1. To establish the practices for documenting the examination of evidence to conform to the requirements of the Department of Forensic Sciences (DFS) Digital Evidence Unit *Quality Assurance Manual*, the accreditation standards under ISO/IEC 17025:2017, and any supplemental standards.

3. Safety

3.1. If necessary due to condition of evidence received (e.g. hazardous and/or biological substances), wear appropriate personal protective equipment (e.g., lab coat, gloves, mask, eye protection), when carrying out standard operating procedures.

3.2. Refer to DEUSOP01 – Handling Digital Evidence for additional precautions and requirements when examining evidence items.

4. Materials Required

4.1. Forensic examination workstation; forensic software; storage media; cable kits associated with each forensic suite (including SIM card adaptors, write blockers, charging kits); digital camera; toolkit.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

There are many different makes and models of mobile devices. Each has their own unique characteristics that will be used to determine the “best” forensic strategy to preserve the data on the device. However, this procedure articulates the general considerations necessary in order to ensure the data is captured in a forensically defensible manner. Not all steps in this procedure may be applicable or relevant.

The following applies to all mobile acquisitions:

7.1. Refer to DEUSOP01 – Handling Digital Evidence and DEUSOP04 – DEU Case Creation for initial procedures regarding handling of evidence and creating a case. DEUF01 Mobile Device Acquisition should be used to record mobile device data.

7.2. Phones

7.2.1. Before opening the evidence package per DEUSOP01 – Handling Digital Evidence try to determine the make/model and the power state (on/off) of the device.

7.2.2. Per DEUSOP01, remove device from packaging. Photograph and record information off device, storage in device and any peripherals that were included. If the device is powered on, ensure that it is set to airplane mode (if possible). If airplane mode is not possible, the device should be placed into a Faraday box, if possible. Information should be recorded on DEUF01 Mobile Device Acquisition.

7.2.3. Based on the make/model of device, consider the following factors for mobile device acquisition:

- Power state / Battery life / charging capability
- Password / PIN Protected
- Encryption
- Memory Cards, SIM Cards

- Forensic tools and their capabilities/limitations relating to the device
- Acquisition types

7.2.4. Perform acquisitions of any memory card(s) and SIM card(s) stored within or packaged with the mobile device. Refer to DEUSOP03 – SIM Card Acquisition and DEUSOP05 – Digital Device Acquisition, and document the process on DEUF01.

7.2.5. Determine what type of acquisition(s) are supported by the device. Follow the forensic tool instructions for acquisition(s) selected. Acquisition considerations should begin with a physical, then file system, and then logical. All supported acquisitions should be attempted. Document further process, if applicable.

7.2.6. If the device is locked and access to the device is obtained using another tool or method, document the process, tool, and results on DEUF01. Then proceed with 7.2.3-7.2.4.

7.2.7. If the device is not supported by physical, file system, or logical acquisitions, is PIN/Password protected and cannot be examined without the password/PIN, or is damaged, consider photography, manual transcription, and advanced mobile device techniques such as JTAG/Chip-Off. For advanced techniques, see DEUSOP09 – Using JTAG for Mobile Phone Examinations or DEUSOP10 – Using Chip-off for Mobile Phone Examinations. The device's software for synchronization/backup may be considered for preserving the evidence electronically (e.g., iTunes, Google Drive).

7.2.8. Create two copies of the original evidence: a best evidence copy and a working copy. Ensure working copy of the device is on DEUNet, in the correct case folder. The working copy should be found in the "Evidence" folder inside a folder labeled with the appropriate evidence identification number (e.g., Item 0006). The best evidence copy should be saved to appropriate storage media (CD, DVD, USB drive, etc.), marking it appropriately with the DFS Case number for DEU storage. Enter the Best Evidence copy into LIMS under the appropriate case number.

7.2.9. Refer to DEUSOP07 – Analysis, Interpretation and Reporting of Results.

7.3. Tablets/iPads

7.3.1. Before opening the evidence package try to determine the make/model, power state (on/off) and whether the device is passcode protected.

7.3.2. If the tablet device is supported by mobile forensic software, follow items 7.2.2-7.2.6. Alternately, follow DEUSOP05 – Digital Device Acquisition.

7.3.3. Follow items 7.2.7-7.2.8.

7.4. Media Players / iPod / Kindles / Watches

7.4.1. Before opening the evidence package try to determine the make/model, power state (on/off), and whether the device is passcode protected.

7.4.2. If the media player device is supported by mobile forensic software, follow items 7.2.2-7.2.6. Alternately, follow DEUSOP05 – Digital Device Acquisition.

7.4.3. Follow items 7.2.7-7.2.8.

7.5. GPS Devices

7.5.1. Record/Document the make/model, serial number and any accessories provided.

7.5.2. If the GPS device supports “disk mode”, follow DEUSOP05 – Digital Device Acquisition.

7.5.3. If the GPS device is supported by mobile forensic software, follow items 7.2.2-7.2.8.

8. Sampling

8.1. Not applicable.

9. Calculations

9.1. Not applicable.

10. Uncertainty of Measurement

10.1. Not applicable.

11. Limitations

11.1. Due to damage or other factors, some or all of the above examinations might not be possible. It is at the discretion of the analyst as to what examinations are necessary and if they should be conducted.

11.2. It may be necessary to conduct multiple examinations utilizing different equipment and acquisition methods.

11.3. In most instances, the data stored on the device will be forensically acquired in total. However, not all of the data will necessarily be made available for review or reported as specified in the scope or associated search warrant.

12. Documentation

12.1. DEUF01 Mobile Device Acquisition

12.2. DEUSOP01 – Handling Digital Evidence

12.3. DEUSOP03 – SIM Card Acquisition

12.4. DEUSOP04 – DEU Case Creation

12.5. DEUSOP05 – Digital Device Acquisition

12.6. DEUSOP07 – Analysis, Interpretation and Reporting of Results

12.7. DEUSOP09 – Using JTAG for Mobile Device Examinations

12.8. DEUSOP10 – Using Chip-Off for Mobile Device Examinations

13. References

13.1. Digital Evidence Unit Quality Assurance Manual (Current Version).

13.2. DFS Departmental Operations Manuals (Current Versions).

13.3. Forensic Science Laboratory (FSL) Laboratory Operations Manuals (Current Versions).

13.4. Digital Evidence Unit Laboratory Operations Manuals (Current Versions).

13.5. SWDGE Best Practices for Mobile Phone Forensics (v2.0 Feb 11, 2013).

13.6. SWDGE Standards and Controls Position Paper (v1.0 Jan 30, 2008).