DEUSOP10 - Using Chip-Off for Mobile Device Examinations

Table of Contents

1. Scope

1.1. This standard operating procedure is utilized for the acquisition of mobile device memory using “chip-off.”

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. For proper handling of digital evidence see the DEUSOP01 – Handling Digital Evidence.

4. Materials Required

4.1. Forensic workstation with Internet access; chip removal equipment (e.g., micromill, T-862 Rework Station); chip card reader adapters; write blocker (if applicable); universal programmer; imaging software; microscope; storage device; soldering iron with accessories; toolkit; heat gun.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. Research the make and model of the mobile device.

7.2. Determine chip identification number and identify the ball grid array (BGA). Determine if the correct chip adapter is available to read the chip.

7.3. Remove the chip from the circuit board using available techniques such as heat or milling.

7.4. Ensure that the chip is in its best condition before contact with the programmer (i.e., re-tin the chip, clean the chip).

7.5. Acquire the data from the chip using a programmer, adapter, software and write-blocker, if applicable. If the programmer requires an Internet connection workstation, ensure the workstation is connected to the Internet.

7.6. Record all processes on DEUF02 – Digital Device Acquisition. If necessary, documentation can be done via photography.

7.7. Upon removal from the Internet connected forensic workstation, verify the acquisition hash value(s).

7.8. Create two copies of the original evidence: a best evidence and a working copy. Create a best evidence copy on appropriate storage media. Enter the item into LIMS and mark with appropriate DFS number for storage in DEU evidence. Create working copy and store the image on DEUNet. The image should be saved in the correct case folder. Within the case folder, the image should be

saved in the "Evidence" folder, inside a folder that has the same name as evidence identification (e.g., Item 0006/Item 0006.E01).

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.

12. Documentation

12.1. DEUSOP01 – Handling Digital Evidence

12.2. DEUF02 – Digital Device Acquisition

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

13.6. SWGDE Best Practices for Chip-Off (v1.0 February 8, 2016).