DEUSOP13 - Live Imaging a Device

Table of Contents

1. Scope
2. Background
3. Safety
4. Materials Required
5. Standards and Controls
6. Calibration
7. Procedures
8. Sampling
9. Calculations
10. Uncertainty of Measurement
11. Limitations
12. Documentation
13. References

1. Scope

1.1. This standard operating procedure addresses how to image a device “live” or while the device is turned on and functioning.

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 the conditions of the device or the environment where the imaging process will take place, wear personal protective equipment (e.g., lab coat, gloves, mask, eye protection), when carrying out standard operating procedures.

4. Materials Required

4.1. Imaging software, storage media, connection materials such as cables or a hard drive dock, software/hardware write-blocker.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. On first examining the digital device, observe and document the following, if applicable:

- Operating system(s)
- Number of drives in the system
- System configuration (ex: RAID)
- Connection to network (network cable or wireless)
- Ensure there is no encryption service running
- Number and types of interfaces available on the digital device

7.2. If device is connected to a network via a network cable, remove the network cable. If device is connected to the network via a wireless interface, disable network connection or turn off wireless access. Document action taken on DEUF02 – Digital Device Acquisition.

7.3. If business continuity must be maintained or the network connection is part of the investigation, leave network connection.

7.4. Record and document any processes and applications open and running. Example: QuickBooks accounting software is open and running on the system. Documentation can be done via photography and/or documentation on the DEUF02 – Digital Device Acquisition.

7.5. For memory/RAM acquisition, connect memory collection device/tool/software/connection (i.e. Netcat to an open port). Collect RAM according to software/device protocols, saving onto prepared storage media.

7.6. Determine the best imaging software and hardware solution based on observations and documentation. If necessary, consult the technical leader for guidance.

7.7. Acquire the device using the selected hardware/software solution. Ensure that a write-blocker is used when possible.

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. 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 Capture of Live Systems (2014 September 5).