DEUSOP05 – Digital Device Acquisition

Table of Contents

1. Scope

1.1. This standard operating procedure is utilized for the forensic acquisition (imaging) of a computer, server or other non-mobile device that has an operating system and/or a file system.

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. Toolkit(s); forensic examination workstation; forensic software; storage media; cable kits associated with each forensic suite (write blockers, charging kits); digital camera.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

The following procedure is provided as a guide to determine the appropriate strategy for forensically acquiring (imaging) and recording uniquely identifiable device and image details.

7.1. Refer to DEUSOP01 – Handling Digital Evidence for the proper handling and documenting of the digital device. Record this information on the DEUF02 Digital Device Acquisition.

7.2. Determine if device contains or is attached to other digital media.

7.2.1. Check all CD, DVD and/or BluRay drives for optical media.

7.2.2. Check all memory card slots/readers for memory cards.

7.2.3. Record/Document all other accessories and peripherals (e.g., USB devices) that are found in/attached to the device.

7.2.4. Record/Document the accessories/peripherals/optical media/memory cards identified on separate DEUF02 Digital Device Acquisition forms, one for each piece of media identified.

7.2.5. All devices associated with the original devices will be imaged separately following this SOP, DEUSOP8 – Encrypted Storage Examination, DEUSOP13 – Live Imaging a Device, or DEUSOP14 – Examining Unidentified Media.

7.2.6. Determine if the drive is a solid-state drive (SSD) as this might require specialized adapters for drive removal acquisition if necessary or, more commonly, imaging the drive using a “boot” device or program.

7.3. Record/Document on acquisition form the state of the device (ON/OFF/HIBERNATE) and follow procedure below.

7.3.1. If the device is powered on or in active sleep mode, record any accounts logged in (if applicable), application(s) running, date/time (if possible), and any encryption that might be employed.

7.3.2. If it is determined that the device needs to be imaged while turned on or "live" due to encryption or an SSD, refer to DEUSOP13 – Live Imaging a Device.

7.3.3. If the system is not encrypted, power the system off.

7.3.4. If the device is powered off, begin 7.4, 7.5, or 7.6.

7.3.5. Document acquisition information gathered from above on the DEUF02 Digital Device Acquisition.

7.4. Windows Operating Systems-Remove Hard Drive(s)

7.4.1. Using the toolkit(s), open the computer casing and identify the number of internal drives. Record/Document the state of the internal hard drives. This information can be documented photographically and/or on DEUF02 Digital Device Acquisition.

7.4.2. Remove hard drive(s) from the computer and attach the hard drive(s) to a write-blocking device and/or software.

7.4.3. Using forensic imaging software/hardware, create a forensic image file. E01 or Ex01 is the preferred DEU format but a DD/RAW or AD1 can also be created when an E01is not possible or appropriate.

7.4.3.1. Name the image file according to the evidence identification number. (e.g., Item 0006.E01).

7.4.3.2. 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).

7.4.3.3. Ensure that a hash value (MD5/SHA-1) has been generated along with the image. Use this to verify the integrity of the image once it is complete. Record/Document the hash algorithm and the hash value on DEUF02 Digital Device Acquisition.

7.4.4. Once the image is complete and verified successfully, return the hard drive(s) and reassemble the computer. If no disassembly was needed to access the drives, ensure the device is returned as received.

7.4.5. Finish recording acquisition information on DEUF02 Digital Device Acquisition.

7.4.6. Repackage the device in the original packaging, if possible. Seal with evidence tape (initial and date).

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

7.5. Imaging a Windows System-Boot Media

7.5.1. Using the toolkit(s), open the computer casing and identify the number of internal drives. Record/Document the state of the internal hard drives. This information can be documented photographically and/or with DEUF02 Digital Device Acquisition.

7.5.2. Boot the device into the BIOS setup and determine the current boot order. Document on DEUF02.

7.5.3. If necessary, change boot order to on device to ensure forensic boot media (e.g., USB, CD) will be first in the boot order. Additional BIOS settings may need to be changed. Document all changes made.

7.5.4. Insert/Attach forensic boot media to device.

7.5.5. Boot device into forensic operating system using forensic boot media.

7.5.6. Follow boot device instructions for imaging the hard drive(s). Follow steps 7.4.3-7.4.5.

7.5.7. Return the device's BIOS settings to the settings previously documented on DEUF02. Verify settings match what was previously recorded/documented.

7.5.8. Follow steps 7.4.6-7.4.7.

7.6. Apple Operating Systems-Target Disk Mode/Boot Media

7.6.1. Boot the Apple computer while holding down the "Option" key until the selection dialog is presented. If the computer presents a lock icon and a password dialog box (Figure 1), there is a firmware password in place and the drive cannot be imaged without the password. If icons for bootable partitions are visible, then there is no firmware password and the drive may be imaged.

Figure 1

7.6.2. If no firmware password exists, reboot the computer while holding down the "T" key until a FireWire logo is displayed (Figure 2). Selecting this boot option will place the evidence computer into Target Disk mode.

Figure 2

7.6.3. Attach the computer to the forensic computer unless using the boot CD/USB.

7.6.3.1. Boot the forensic computer into a forensically sound operating system environment.

7.6.3.2. If using a forensic Windows computer, the forensic computer must be booted with a forensically sound Linux variant (Boot Disk).

7.6.3.3. If using a forensic Apple computer, the examiner must mount the evidence computer in read-only mode. Disk Arbitration must be turned off in the forensic computer.

7.6.4. If using a boot CD/USB, attach storage media formatted as ExFat to the evidence system. Boot the computer, holding the “option” key down. When the system options appear, select the boot CD/USB and follow the prompts to create an image of the system.

7.6.5. Follow items 7.4.3 -7.4.7.

7.7. Hybrid / Tablet Computer Devices

7.7.1. Depending on the tablet device received, it may be possible to access the UEFI (Unified Extensible Firmware Interface) to provide details about the UUID (Universally Unique Identifier), serial number and boot order. Consult the device user manual/research obtained for the correct sequence to access the UEFI.

7.7.2. If the device is powered off, turn the device on. If the device is powered on, document/record the following actions:

7.7.2.1. Disable Internet access (wireless settings).

7.7.2.2. Turn off encryption (e.g., Bitlocker).

7.7.2.3. Disable password (if applicable).

7.7.2.4. With forensic acquisition software loaded on a USB device, create a “live” image of the tablet. Restore previous settings listed in 7.7.2. Follow items 7.4.3 -7.4.7.

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 digital evidence analyst as to what examinations are necessary and if they should be conducted.

12. Documentation

12.1. DEUF02 Digital Device Acquisition

12.2. DEUSOP01 – Handling Digital Evidence

12.3. DEUSOP07 – Analysis, Interpretation and Reporting of Results

12.4. DEUSOP08 – Encrypted Storage Examination

12.5. DEUSOP13 – Live Imaging a Device

12.6. DEUSOP14 – Examining Unidentified Media

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 Best Practices for Computer Forensics (v3.1, Sep 05, 2014).

13.6. SWGDE Mac OS X Tech Notes (v1.3 September 29, 2015).