DEUSOP08 – Encrypted Storage Examination

Table of Contents

1. Scope

1.1. This standard operating procedure is utilized for the acquisition of encrypted storage, encrypted volumes and encrypted media.

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 imaging software; encryption software (e.g., TrueCrypt).

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. In exigent circumstances and if a known decryption solution exists (pass phrase, key, etc.), ensure that a forensic copy (image) of the source data is created before attempting to decrypt or access encrypted volumes.

7.2. Check if the forensic software can decrypt the drive by providing it with the password, passphrase or key. If so, use the forensic software to acquire a decrypted copy of the media/volume to create a best evidence copy and a working copy.

7.3. For encrypted media/volumes (removable, non-TPM, unsupported forensic software) where a known specialized software was used:

7.3.1. If not on the forensic workstation, install the encryption software.

7.3.1.1. Record/document the details of the software, include the developer and version number.

7.3.2. Using the working copy of the encrypted media/volume, mount the image as read only using the appropriate forensic software, if possible.

7.3.3. Using the encryption software installed, decrypt the mounted encrypted media/volume and open the media/volume using the provided passcode, passphrase or key.

7.4. For encrypted media/volumes (non-removable, TPM, WDE, unsupported forensic software) using unknown encryption software, mount the volume/media if possible to the forensic workstation. Attempt to use a technique/tool (e.g. brute force attack, bitlocker bypass, etc.) that is designed to “open” encrypted media.

7.5. If successful, using the appropriate forensic acquisition software, acquire the decrypted data from the mounted media/volume to storage media. Refer to DEUSOP05 – Digital Device Acquisition.

7.6. Verify the acquisition and verification hash values, the number of sectors (if applicable) and the total bytes that were acquired.

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

11.2. The results of this procedure are limited to the acquisition of the storage device; no forensic analysis is conducted on results from the acquisition of data.

12. Documentation

12.1. DEUSOP01 – Handling Digital Evidence

12.2. DEUSOP05 – Digital Device Acquisition

12.3. DEUF02 – Digital Device Acquisition

12.4. DEUF05 – Forensic Examination

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 (2015 September 05).

13.6. SWGDE Capture of Live Systems (2014 September 05).