DEUSOP15 - Skimming Devices

Table of Contents

1. Scope

1.1. This standard operating procedure is for the acquisition of data from common skimming devices.

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 workstation with Internet access; chip removal equipment (i.e T-862 Rework Station); chip card reader adapters; write blocker (if applicable);

universal programmer; imaging software; microscope; storage device; soldering iron with accessories; toolkit; mobile phone cable kit.

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

7.1. As skimmers are often unique in design and implementation, examination processes vary depending upon the category and/or type of device. When considering retrieving stored account information, due to differences in acquisition and analysis, skimmers can be broken down into two general categories: analog or digital.

The following are procedures for both categories:

7.1.1. Record/Document the evidence packaging, noting the seal and markings (date/initials) on the evidence storage container (e.g. plastic bag, box, paper bag) per DEUSOP01 – Handling Digital Evidence.

7.1.2. If device contains an SD card or other known digital storage, reference DEUSOP05 – Digital Device Acquisition for acquisition and document using DEUF02 – Digital Device Acquisition.

7.1.3. Ensure appropriate media storage devices for the best evidence and working copies are prepared for acquisition and their uniquely identifiable information is recorded on DEUF02 – Digital Device Acquisition.

7.2. Analog Skimming Devices

7.2.1. Identify the architecture of the analog skimming device.

7.2.2. In order to acquire the information from the flash memory chips, a header may need to be soldered to the leads for acquisition through universal serial bus (USB) mode.

7.2.3. Once soldered and communication with a forensic workstation is established, reference DEUSOP05 – Digital Device Acquisition and record process/device information on DEUF02 – Digital Device Acquisition.

7.3. Digital Skimming Devices

7.3.1. After visually examining the chips located on the device, document/photograph the manufacturer and chip model numbers of both the microcontroller and flash chips.

7.3.2. Identify if you have the correct tools to read the data from the chip (i.e. chip adapter).

7.3.3. Refer to DEUSOP10 – Using Chip-Off for Mobile Device Examinations.

7.3.4. Remove the chip from the circuit board in a manner that ensures they are not damaged (i.e. IR Heat, Hot Air).

7.3.5. Read the data from the chip using the appropriate chip package and chip reader. The microcontroller might also need to be removed and read to understand the encoding or encryption methods used by the device.

7.3.6. 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).

7.3.7. If possible, return device pieces to original packaging, seal and initial.

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. DEUSOP05 – Digital Device Acquisition

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

12.4. 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 Best Practices for Examining Magnetic Card Readers (v2.0 September 29, 2015).

13.6. USSS Skimming Device Training Manual (Current Version).