DEUSOP07 – Analysis, Interpretation, and Reporting of Results

Table of Contents

1. Scope

1.1. This standard operating procedure is utilized for the analysis and reporting of digital evidence.

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. Not applicable.

4. Materials Required

4.1. Forensic examination workstation; forensic software; DEU media, DEU forms, case file(s).

5. Standards and Controls

5.1. Not applicable.

6. Calibration

6.1. Not applicable.

7. Procedures

Digital Evidence Analysis

This is a general procedure for analysis conducted by the Digital Evidence Unit. For reporting and procedural purposes, analysis is not an extraction of data that is covered by acquisition SOPs. Analysis is an examination of the data once it has been extracted per the scope/requirements of the request.

7.1. Determine and document a Scope of Examination with the requestor. Use the search warrant provided, if applicable, and the request form submitted. This can be documented on DEUF05 – Forensic Examination.

7.2. Ensure that the forensic workstation is up to date with current DEU software and hardware. Ensure no other examination is being undertaken on this workstation.

7.3. Based on the scope of the analysis, determine what forensic tools are to be used. Record these items using DEUF05 – Forensic Examination. A basic analysis should include the following:

7.3.1. Add the working copy to forensic software.

7.3.2. If applicable to the image being analyzed, ensure that a verification hash is established prior to the commencement of the examination on the working copy. Log and record this as part of the case file. This can be documented on DEUF05 – Forensic Examination, screenshot, or other accessible documentation method.

7.3.3. If possible and applicable, ensure that any folders/files are recovered from the working copy image.

7.3.4. If possible and applicable, utilize the NSRL or other relevant hash libraries to perform a hash value and file signature analysis.

7.3.5. If possible and applicable, run the appropriate processing functions for type of image (Windows, Mac, Linux/UNIX, Android, iOS, etc.) for unique system software/hardware identifiers.

7.3.6. Based on the scope and predetermined tools, record methodology, tools, and actions taken to retrieve pertinent data from working copy.

7.3.7. During the examination, document any third party or internally generated functions, scripts ran, or code that was used to analyze the data.

7.3.8. If practical, extract/report any relevant data for later inclusion in the forensic report.

7.3.9. If tools used are not validated by DEU or validated by a standards body (NIST), the results must be verified using a secondary forensic tool and/or manually recalculated.

7.4. At the completion of the analysis, produce a verification hash of the digital working copy, if applicable. Record the action on the DEUF05 – Forensic Examination or note results in the electronic case file (e.g., log file).

7.5. Document a conclusion/finding based on the results of analysis and include references to the data used in determining the finding. Record items on DEUF05 – Forensic Examination for inclusion in report.

7.6. Follow steps in the appropriate section below to produce a report.

DEU Reporting

There are three types of reports and analysis that the DEU provides to requesting agencies: Report of Examination (Data Extraction), Report of Examination, and Discontinuation Report.

Report of Examination (Data Extraction)

This report is used when only the data extracted from an evidence item(s) is provided to the requestor. No forensic interpretation/analysis has been conducted and no forensic opinion is offered.

7.7. Using the DEUF04 – Report of Examination (Data Extraction) template, fill out the sections to include scope, evidence items, tools/methodology, extracted data details, disposition, and signature of analyst.

7.8. Copy the extracted data to media to be provided to the requestor. Files and folders can be compressed in an appropriate container (i.e. ZIP) if the data would be best transported in a compressed file. Extracted data can also be provided to requestor electronically per agreement with requestor/requesting agency.

7.9. In LIMS, mark the request “Draft Complete” for technical and administrative review.

7.10. Inform the technical leader or designee that the request is ready for technical and administrative reviews.

Report of Examination

This report is used when forensic interpretation and analysis of the evidence item(s) has been conducted, whether a forensic opinion has been offered or not.

7.11. Using the DEUF07 – Report of Examination template, fill out the sections to include the scope of examination, tools/versions used, methodology (e.g., recover folders, hash/signature analysis, etc.), the results and the conclusion / finding of the report. These items are recorded on DEUF05 – Forensic Examination for inclusion into the Report of Examination.

7.12. If applicable, use the DEUF11 – Digital Evidence Report template to create a report. This report template is used when the analysis requires an opinion from the analyst, interpretation of finding or more extensive reporting is requested or determined than on the Report of Examination.

7.13. In LIMS, mark the request “Draft Complete” for technical and administrative review.

7.14. Inform the technical leader or designee that the request is ready for technical and administrative reviews.

Discontinuation Report

This report is used when analysis/extraction requested cannot be completed, the requestor has cancelled the request, or the request/data/evidence is no longer available to the Digital Evidence Unit.

7.15. Using the DEUF08 – Discontinuation Report template, fill out the sections as appropriate.

7.16. In LIMS, mark the request “Draft Complete” for technical and administrative review.

7.17. Inform the technical leader or designee that the request is ready for technical and administrative reviews.

8. Sampling

8.1. Not applicable.

9. Calculations

9.1. Not applicable.

10. Uncertainty of Measurement

10.1. Not applicable.

11. Limitations

11.1. The scope of the report will be limited to the scope of the request for examination and the associated search warrants, if applicable.

12. Documentation

12.1. DEUF05 – Forensic Examination

12.2. DEUF04 – Report of Examination (Data Extraction)

12.3. DEUF07 – Report of Examination

12.4. DEUF11 – Digital Evidence Report Template

12.5. DEUF08 – Discontinuation Report

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).