

Forensic Report Guidelines

Reporting is the process of preparing a detailed summary of all the steps taken and conclusions reached in the investigation of a case. Reporting depends on maintaining a careful record of all actions and observations, describing the results of tests and examinations, and explaining the inferences drawn from the data. A good report relies on solid documentation, notes, photographs and tool-generated content.

Reporting occurs once the data has been thoroughly searched and relevant items bookmarked. Many forensic tools come with a built-in reporting facility that usually follows predefined templates and may allow customization of the report structure. Permitted customizations include allowing for organization logos and report headers and selection of styles and structure to provide a more professional look tailored to the organization's needs. Reports generated by a forensic tool typically include items from the case file, such as the specialist's name, a case number, a date and title, the categories of evidence, and the relevant evidence found. Report generation typically either outputs all of the data obtained or allows examiners to select relevant data (i.e., bookmarked items) for the final report. Including only relevant findings in the report minimizes its size and lessens confusion for the reader.

The software-generated contents are only one part of the overall report. The final report contains the software-generated contents along with data accumulated throughout the investigation that summarizes the actions taken, the analysis done, and the relevance of the evidence uncovered. Ideally, the supporting documentation is in electronic form and able to be incorporated directly into the report.

Reporting facilities vary significantly across mobile device acquisition applications. Report generation typically can render a complete report in one of several common formats (e.g., .txt, .csv, .doc, .html, .pdf) or at least provide a means to export out individual data items to compose a report manually. A few tools include no means of report generation or data export and instead require examiners to capture individual screenshots of the tool interface for later assembly into a report format. Regardless of how reports are generated, checking that the finalized report is consistent with the data presented in the user interface representation is vital to identify and eliminate any possible inconsistencies that may appear (Ayers, R).

The ability to modify a pre-existing report and incorporate data (e.g., images, video stills) captured by alternative means is advantageous. Auxiliary acquisition techniques are sometime required to recover specific data types, as mentioned earlier. For example, video recording a manual examination documents the recovery of data that the automated forensic tool may not have acquired. Video editing software allows still images to be captured for inclusion into the report. Pictures could also be taken of

Forensic Report Guidelines

the manual exam using a digital camera; though this process is less efficient and may not document the entire process, it may be the only method available.

The type of data determines whether it is presentable in a hard-copy format. Today, many popular mobile devices are capable of capturing audio and video. Such evidentiary data (e.g., audio, video) cannot easily be presented in a printed format and instead should be included with the finalized report on removable media (e.g., CD-R, DVD-R, or flash drive) along with the appropriate application for proper display.

Forensic Report Guidelines

Reports of forensic examination results should include all the information necessary to identify the case and its source, outline the test results and findings, and bear the signature of the individual responsible for its contents. In general, the report may include the following information (E.S.C.I):

- Identity of the reporting agency
 - Case identifier or submission number
 - Case investigator
 - Identity of the submitter
 - Date of evidence receipt
 - Date of report
 - Descriptive list of items submitted for examination, including serial number, make, and model
 - Identity and signature of the examiner
 - The equipment and set up used in the examination
 - Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.
 - Supporting materials such as printouts of particular items of evidence, digital copies of evidence, and chain of custody documentation
- Details of findings:
 - Specific files related to the request
 - Other files, including deleted files that support the findings
 - String searches, keyword searches, and text string searches
 - Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity
 - Graphic image analysis
 - Indicators of ownership, which could include program registration data
 - Data analysis
 - Description of relevant programs on the examined items

Forensic Report Guidelines

- Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions and file name anomalies

- Report conclusions

Digital evidence, as well as the tools, techniques and methodologies used in an examination is subject to being challenged in a court of law or other formal proceedings. Proper documentation is essential in providing individuals the ability to re-create the process from beginning to end. As part of the reporting process, making a copy of the software used and including it with the output produced is advisable when custom tools are used for examination or analysis, should it become necessary to reproduce forensic processing results.

Bibliographic Citations

Ayers, R. Computer Forensic Tool Testing (CFTT) Program<URL:
http://www.cftt.nist.gov/mobile_devices.htm>.

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, NCJ 219941, April 2008, <URL: <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>

Forensic Report Guidelines