# Contents that should be included in every Forensic Report

Table of Contents

[Forensic Reporting 2](#_Toc348356431)

[Forensic analysis reports 2](#_Toc348356432)

[Examiner notes 2](#_Toc348356433)

[Report format 2](#_Toc348356434)

[Scope and objectives 2](#_Toc348356435)

[Evidence listing format 3](#_Toc348356436)

[Examination details 3](#_Toc348356437)

[Conclusions 4](#_Toc348356438)

[Supporting documentation 4](#_Toc348356439)

[Best practices 5](#_Toc348356440)

# Forensic Reporting

## Forensic analysis reports

1. Should answer these questions:
   1. Why was analysis conducted?
   2. What evidence was analyzed?
   3. How was evidence integrity safeguarded?
   4. What process was used?
   5. What relevant information was found?

## Examiner notes

1. Document as you go – **NOT** after the fact
   1. Handwritten notes are acceptable
2. Provide enough detail for others to duplicate steps
3. Note ***any exam anomalies, fixes or workarounds*** put in place
4. Include dates, times, observations and actions taken

## Report format

1. Introduction
   1. Forensic reports typically include several key sections. Each section should aim to answer any questions a reviewer may have regarding your analysis
2. Executive summary
   1. Likely to be the most read component of your report. For some audiences, particularly decision makers within your business, it may be the only component of your report that is read. Your summary should rarely be more than one page and should include all of your key findings and conclusions.

### Scope and objectives

1. What were the stated goals of the analysis?
   1. Explain relevant case facts
2. Who authorized the examination?
3. What scope limitations are in place?
4. Format of this section:
   1. Introduction – important to identify the scope and objectives up front
   2. Objectives – work with your intended audience to identify what the goals of the investigation should be. What are you trying to prove/disprove? Law enforcement often structures their goals in terms of the Elements of Proof for the crime they are investigating.
   3. Authorization – every examination must be authorized, and this section is a good place to document where that authority came from.
   4. Scope – scope identifies the boundaries of your examination, including what you can examine, and in some cases, what examination methods can be used. Inherently tied to the authority to examine and is informed by requirements or covenants such as court orders, privacy policies and contracts.
   5. Summary – good best practice is to draft this section early and gather feedback from peers and those you are reporting to in order to ensure you have captured the essential elements of the investigation.

### Evidence listing format

1. Catalogs media analyzed during the forensic exam
   1. Includes
      1. Tag number
      2. Description
      3. Serial number
      4. Hash value
      5. Size of media
2. Sections:
   1. Introduction – gives the reader a quick snapshot of the media that was analyzed and should provide a means for the writer to refer back to that media within the report.
   2. Description of Evidence – ties pieces of physical evidence to your analysis. Should e thorough, including the type of device, the make, serial number, data capacity, any physical markings, and a hash value of the evidence if available. Allows investigator to refer to evidence without having to repeat the key information. Often labels are used to make it easy to indicate to the reader which piece of evidence yielded the given result.
   3. Summary – evidence listing is critical for ensuring that all evidence was taken into account during the exam.

### Examination details

1. Answers the questions:
   1. How evidence was safeguarded
   2. What forensic process was used
2. Can be structured:
   1. Chronologically
   2. By file system data layer
   3. According to tool output
   4. By specific exam objectives
3. Include forensic tools listing
4. Identify installed applications
5. Results of media analysis
   1. Internet activity, relevant keywords search findings, etc.
6. Anti-forensics indicators
7. Malware or hacker tool analysis
8. Sections
   1. Introduction – this is where the examiner will explain how the examination was conducted and what key results (if any) were discovered
   2. How to Structure the details
      1. Examiner preferences will dictate the overall structure and could be different for various types of cases
      2. Chronological may be the most common, but structuring according to tool output could be relevant in situations where procedures dictate a strict order of tool use.
      3. Organizing the report details by the stated goals or elements of proof within the objectives section could also be helpful to a particular audience.
   3. What to include
      1. List all steps taken to complete the investigation
      2. Steps to acquire the evidence
      3. Measures taken to ensure evidence integrity
      4. Entire forensic process used to conduct the media analysis and identify the results relevant to the goals in your objectives part of the report.
   4. Summary – examination details is the core of your report. Describes the entire investigation and the key findings and results. Other sections of the report should be built to support the information covered in this section.

### Conclusions

1. Conclusions must be supported by findings
   1. Opinions and inferences should be omitted
2. Should be clear and fully expressed
3. Simple enough to be understood by a non-technical audience
4. Can include recommendations
5. Sections
   1. Introduction
   2. Just the facts
   3. summary

### Supporting documentation

1. Use appendices for data output relevant to the exam and larger than half a page
2. Examples
   1. Forensic tool output
   2. Log file or install script printouts
   3. E-mail threads
   4. Keyword hits in unallocated space
3. Sections
   1. Introduction
   2. Why use supporting documentation?
      1. Anything over half a page long should be included in an appendix instead of the main report
   3. Keeping results in native form
      1. Reference can be made to ESI in your report
   4. Summary
4. Appendices should also be used to hold other case documentation:
   1. Search authority or permission to examine evidence
   2. Chain of custody forms
   3. User agreements
   4. Glossary of terms used

### Best practices

1. Hyperlink references to supporting docs
2. Include excerpts from appendices to support key findings
3. Use labels for frequent references
4. Introduction
   1. Tips and tricks: if a large number of reports are generated by your organization, it could be useful to create a series of guidelines for forensic reports
5. Packaging reports
   1. Reports are frequently delivered electronically, so take advantage of the inherent benefits of using a digital format
   2. Many burn their reports onto a CD/DVD-ROM including their supporting documentation
   3. Linking all documentation in the report increases usability for relevant parties
6. Increasing readability
   1. Provide snippets in the report that refers to labeled evidence and link to longer descriptions in the appendices
   2. Include graphics in your report – GUI-based tools provide an excellent opportunity to include screen captures to illustrate evidence/artifacts found
7. Other best practices
   1. When possible, reports should be peer-reviewed before they are released
   2. Work through your legal department to cover your report under attorney-client privilege
8. Summary
   1. Keep intended audience in mind, take pains to describe complicated topics in words and images, and provide ample documentation to support their results and conclusions