FORENSICS REPORT

Understanding the Importance of Reports

You write a report to communicate **the results of your forensic examination** of a computer, network system, or digital device.

A forensic report **presents evidence** that might support further investigation and, in some situations, be **admissible in court**, at an administrative hearing, **or as an affidavit** to support issuing an arrest or a search warrant.

Besides presenting facts, **reports can communicate expert opinion**. You should look at your report as your first testimony in a case.

A report can also provide justification for collecting more evidence and be used at a probable cause hearing, as evidence in a grand jury hearing, or at a motion hearing in civil or criminal cases.

Necessary information in reports are :

Jurisdiction (the official power to make legal decisions and judgements:for example, U.S. District Court for Eastern District of Washington)

Style of the case (the format used for official court documents—for example, using a header such as John Smith, Plaintiff v. Paul Jones, Defendant)

Cause number

Date and location of the deposition

Name of the deponent (the person testifying at deposition)

Types of Reports

Digital forensics examiners are required to create different types of reports, such as

- a formal report consisting of facts from your findings
- a preliminary written or verbal report to your attorney
- an examination plan for the attorney who has retained you.

Examination Plan

An examination plan is a document that serves as a guideline for knowing what questions to expect when you're testifying

Your attorney uses the examination plan as an outline and a guide for your testimony.

You can propose changes to clarify or define information or to include substantive information the attorney might have omitted.

You can also use the examination plan to help your attorney learn the terms and functions used in digital forensics.

Verbal Report

A verbal report is less structured than a written report.

Typically, it takes place in an attorney's office, where the attorney requests the consultant's report.

An expert hired as a trial consultant uses verbal reports often.

Keep in mind that others can't force your attorney to repeat what you've told him or her in a verbal report.

A verbal report is usually a preliminary report and addresses areas of investigation yet to be completed, such as the following:

- Tests that haven’t been concluded
- Interrogatories that the lawyer might want to address to opposing parties
- Document production, either requests for production (to parties) or subpoenas (to nonparties, people who have information but aren’t a named party in the case)
- Determining who should be deposed and the plan for deposing them

Preliminary Report

With preliminary reports, mention to your client that your factual statement and opinion are still tentative and subject to change as more information comes in.

A written report is frequently an affidavit or a declaration.

Guidelines for Writing Reports

Accurate

relevant

ethical.

Reports should answer the questions you were retained to answer and keep information that doesn’t support specific questions to a minimum.

A well-defined report structure contributes to readers’ ability to understand the information you’re communicating.

Make sure your report includes clearly labeled sections and follows a numbering scheme consistently. Ensure that supporting materials, such as figures and tables, are numbered and labeled clearly.

Clarity of writing is critical to a report’s success. Make sure to include signposts to give readers clues about the sequence of information, and avoid vague wording, jargon, and slang.

Report Structure

Abstract (or summary)

Table of contents

Body of report

Conclusion

References

Glossary

Acknowledgments

Appendixes

Abstract

If **the report is long and complex**, you should include an abstract.

Typically, more people read the abstract than the entire report, so writing one for your report is important.

The abstract and table of contents give readers an overview of the report and its points so that they can decide what parts they need to review.

An abstract simply condenses the report's key points to focus on the **essential information**.

It should be one or two paragraphs totaling about 150 to 200 words.

Remember that the abstract should describe the examination or investigation and present the report's main ideas in a summarized form.

The Body

The body consists of the introduction and discussion sections.

The introduction should state the report’s purpose (the questions to be answered) and show that you’re aware of its terms of reference.

Two other main sections are the conclusion and supporting materials (references and appendixes).

The conclusion starts by referring to the report’s purpose, states the main points, draws conclusions, and possibly renders an opinion.

References and appendixes list the supporting material to which your work refers.

Writing Reports Clearly

Communicative quality—Is it easy to read? Think of your readers and how to make the report appealing to them.

Ideas and organization—Is the information relevant and clearly organized?

Grammar and vocabulary—Is the language simple and direct so that the meaning is clear and the text isn’t repetitive? However, technical terms should be used consistently; you shouldn’t try to use variety for these terms. Using different words for the same thing might raise questions.

Punctuation and spelling—Are they accurate and consistent?

Designing the Layout and Presentation of Reports

Layout and presentation involve many factors, including using clear titles and section headings.

A numbering system is also part of the layout.

Typically, report writers use one of two numbering systems: **decimal numbering or legal-sequential numbering.**

After you choose a system, be sure to follow it consistently throughout the report.

A report using the decimal numbering system divides material into sections and restarts numbering with each main section.

Providing Supporting Material

Use supporting material such as figures, tables, data, and equations to help tell the story as it unfolds.

Refer to this material in the text and integrate the points they make into your writing.

Number figures and tables sequentially as they're introduced (for example, Figure 1, Figure 2, and so forth with another sequence for Table 1, Table 2, and so on).

Formatting Consistently

How you format text is less important than being consistent in applying formatting.

- For example, if you indent paragraphs, be sure all are indented. Use fonts consistently, and use consistent heading styles throughout (for example, major headings in bold with initial capitals, minor headings in italics, and so forth). Follow the same guideline throughout for units of measure;

Explaining Examination and Data Collection Methods

Explain **how you studied the problem**, which should follow logically from the report's purpose.

Depending on the kind of data, this section might contain **subsections on examination procedures**, materials or equipment, data collection and sources, and analytical or statistical techniques.

Supply enough detail for readers to understand what you did.

Without good data recording in a lab notebook or file, completing a report beyond this point is futile.

Data collection is a critical portion of the report.

If your data collection process becomes the subject of discovery or examination, presenting data in a well-organized manner is important.

Use tables in your report to illustrate how data was handled and examined.

Including Calculations

In most cases, hashing algorithms are calculated in digital forensics investigations.

- If you use any hashing algorithms, be sure to give the common name, such as “Message Digest 5 (MD5) hash.” Generally, you don’t need to give examples of each type of hash if you’re using standard tools; you explain generally what they do and cite the authority or policy you rely on for using the tool. For example, to explain why you’re using the MD5 hash, you might cite the National Software Reference Library (NSRL; www.nsrl.nist.gov) as an authority

Explaining Results and Conclusions

Explain your findings, using subheadings to divide the discussion into logical parts.

Make comments on results as they're presented, discussing the importance of what you found in light of the overall report objectives.

Take a step back from the details and synthesize what has been learned about the problem and what the information means.

Describe what you actually found, not what you hoped to find. Including this discussion as you present results can often improve clarity and readers' understanding.

Link your discussion to figures and tables as you present results, and describe and interpret what these supporting materials show.

If you have many similar figures, select representative examples for the main report and put the rest in an appendix.

Save broader generalizations and summaries for the report's conclusion.

The conclusion should restate the objectives, aims, and key questions and summarize your findings with clear, concise statements.

Keep the conclusion brief and to the point.

Providing References

When you write a report, you must cite references to all material you have used as sources for the content of your work.

These citations are made wherever you quote, paraphrase, or summarize someone else's opinions, theories, or data.

References can include books, periodicals, newspapers, Web sites, conference proceedings, personal communications, and interviews.

Including Appendixes

If necessary, you can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits.

Arrange them in the order referred to in the report.

They are considered additional material and might not be examined by readers.

Some portions of appendixes might be considered optional, but others are required.

Ethics for the Expert Witness

For digital forensics examiners, maintaining the highest level of ethical behavior in their work is essential.

Forensics examiners are responsible for meeting the highest standards when conducting examinations, preparing reports, and giving testimony to ensure that evidence is accurate, reliable, and impartial.

In addition, you must know when to disqualify yourself from an investigation. Knowing what to look for when taking a new case helps you avoid potential ethical problems.

Applying Ethics and Codes to Expert Witnesses

Ethics are the rules you internalize and use to measure your performance.

The standards that others apply to you or that you're compelled to adhere to by external forces, such as licensing bodies, can be called ethics, but they're more accurately described as rules of conduct.

Many professions now call these rules codes of professional conduct or responsibility .

People need ethics to help maintain their balance, especially in difficult and contentious situations, and for guidance on their values. Ethics also help you maintain self-respect and the respect of those in your profession. Because forensics examiners don’t have the same formal, detailed codes of conduct that professions such as medicine and the law have, relying on an internal code of ethics might be more critical.

Expert witnesses are expected to present unbiased, specialized, and technical evidence to a jury. However, experts, like the attorneys who hire them, have biases and other ethical failings. As a professional, you must control your biases, not allow them to control you. Ethics are a tool you can use to identify and control your biases or prejudices.

Forensics Examiners' Roles in Testifying

Forensics examiners have two roles in testifying:

- testifying to facts found during evidence recovery (fact witness)
- rendering an opinion based on education, training, and experience (expert witness).

As an expert witness, you can testify even if you weren’t present when the event occurred or didn’t handle the data storage device personally. Because of an expert’s important role in litigation, attorneys often shop for experts who can support their cases, and experts’ fees might be only a secondary consideration. Criticism of expert witnesses is widespread in the legal community because it’s possible to find and hire an expert to testify to almost any opinion on any topic. As a result, the impartiality of expert testimony and the potential for misconduct have become concerns.

Opinion shopping is **the practice of searching for an outside auditor willing to provide a favorable view of a company's financial condition**.

If you’re going to have a long and productive career as an expert witness, beware of attorneys’ opinion shopping. An attorney might be willing to risk your career to improve the prospect of success in a case—and can always find another expert for the next case. The most effective way to prevent opinion shopping is to require that the attorney retaining your services send you enough material on the case for you to make an evaluation. Distinguishing opinion shopping from the process of attempting to disqualify experts by creating conflicts can be difficult, however.

Considerations in Disqualification

One of the effects of violating court rules or laws is disqualification . This outcome isn’t usually punitive, but it can be embarrassing for you as a professional and potentially for the attorney who retained you. A disqualification based on an ethical lapse could effectively be a death sentence for a career as an expert witness, as you can expect it to come up in any case you’re involved in.

Opposing counsel might attempt to disqualify you based on any deviations from opinions you've given in previous cases. Any testimony you give at trials or depositions is on record and available to attorneys.

If there's a change in your position on a point, be sure to explain why you have changed it, such as recent developments in technology, new tools with new capabilities, or the facts of the current case differing from a previous case. An apparent change of position could be a subject for cross-examination, and you must be able to explain what appears to be contradictory opinions, or you'll be seen as tailoring testimony to your client's needs.