Computer Forensics

Week 12: Report Writing for High-Tech Investigations

Lecturer: Lemi Agrey Oliver

codingissweet@gmail.com

KUMI UNIVERSITY

Content

- Understanding the Importance of Reports
- Guidelines for Writing Reports
- Generating Report Findings with Forensics Software Tools

Understanding the Importance of Reports

Purpose of Reports

- Reports communicate findings from forensic examinations of digital devices.
- They provide evidence supporting further investigations, sometimes admissible in legal proceedings.
- Reports can justify collecting more evidence and support disciplinary actions in cases of employee misconduct.

Understanding the Importance of Reports+

Content and Requirements

- Reports present facts and expert opinions, akin to testimony in a case.
- In civil cases, U.S. district courts mandate expert witnesses to submit detailed written reports.
- Rule 26 of the Federal Rules of Civil Procedure specifies the content required in reports.
- Federal courts generally require reports from all fact or expert witnesses in civil cases.
- The Daubert standard, followed in many states, emphasizes reliable methodology and factual basis for testimony.

Understanding the Importance of Reports++

Components of a Report

- Reports should include all opinions, their basis, information considered, and related exhibits.
- Expert witnesses' curriculum vitae, listing publications, is required.
- Details on fees, past testimonies, and case involvements of the expert must be provided.
- Additional information such as jurisdiction, case style, and deposition details should be included if applicable.

Understanding the Importance of Reports+

➢Expert Witness Awareness

- ➢Lawyers utilize deposition banks to access previous testimonies of expert witnesses.
- ➢Transcripts of previous testimonies might be requested to ensure consistency.
- ➢Electronic mailing lists within legal associations facilitate sharing of expert witness depositions.

Limiting a Report to Specifics

Define Investigation Goals

- Determine the specific mission or objective of the investigation, which could involve locating information, retrieving documents, or recovering specific types of files with designated dates and times.
- Clearly outlining these goals minimizes time and costs, especially considering the growing complexity of digital storage systems.

Identify Audience and Purpose

- Before drafting the report, understand the intended readership and the report's purpose.
- This understanding helps in tailoring the report to focus on relevant specifics.

Limiting a Report to Specifics+

Consider Audience Knowledge

- If the audience lacks technical expertise, anticipate the need to include educational content on technical matters.
- Maintain a set of standard paragraphs for this purpose, updating them periodically to ensure accuracy and relevance.

Types of Reports in Digital Forensics

Formal Report

- Detailed documentation of factual findings obtained during the examination process.
- Typically includes comprehensive information regarding the forensic analysis conducted, the evidence collected, and the conclusions drawn from the investigation.
- Primarily serves as a means of presenting objective facts and findings to relevant parties, such as attorneys, judges, or clients.
- Often considered a crucial piece of evidence in legal proceedings and may be subject to scrutiny by opposing parties.

Preliminary Report

- Can be presented in either written or verbal form and is typically provided to the attorney before formal legal proceedings commence.
- Functions as a preliminary overview of the forensic examination, outlining initial findings and potential areas of focus for further investigation.
- Serves as a guide for the examiner's testimony during legal proceedings, helping both the examiner and the attorney prepare for questioning.
- Allows for the exchange of information between the examiner and the attorney, facilitating clarification of technical terms and concepts.
- Enables the examiner to propose changes or additions to ensure clarity and completeness in subsequent reports.

Verbal Report

- A less formal mode of communication compared to written reports, often delivered in-person within an attorney's office.
- Typically serves as a preliminary update on ongoing investigation activities and findings.
- Covers aspects such as pending tests, potential interrogatories for opposing parties, document production requests, and deposition plans.
- Provides an opportunity for real-time discussion and clarification between the examiner and the attorney.
- Not legally compelled to be repeated verbatim by the attorney in subsequent proceedings, but serves as valuable background information for case preparation.

Written Report

- Often takes the form of an affidavit or declaration, which is a formal legal document sworn under oath.
- Requires meticulous attention to detail and adherence to legal standards, as it may be subject to scrutiny in court.
- Must accurately and comprehensively document all aspects of the forensic examination process, including methodologies, findings, and conclusions.
- Demands thorough documentation and support for all assertions made within the report, often accompanied by relevant evidence and exhibits.
- Subject to specific guidelines and standards outlined in legal statutes and professional codes of conduct to ensure reliability and credibility.

What to Include in Written Preliminary Reports

Risk Factors in Report Creation for Civil Litigation:

- Anything documented during examination for a civil litigation report is subject to discovery by opposing attorneys.
- Discovery involves attorneys seeking information from each other, meaning written reports can be demanded by opposing counsel.
- Written preliminary reports pose a high risk as they can be used to discredit testimony if they differ from the final report or testimony.

What to Include in Written Preliminary Reports+

- Avoid using terms like "preliminary copy" or "draft copy" in preliminary reports to prevent giving opposing counsel grounds for discrediting.
- Destruction of preliminary reports before case resolution could be considered spoliation, leading to potential sanctions.
- If listed as a witness, all work related to the case is subject to discovery, including preliminary reports.

Content Guidelines for Written Preliminary Reports

- Restate the assignment to ensure alignment with the client's focus.
- Summarize completed tasks, including systems examined, tools used, and observations made.
- Outline evidence preservation or protection processes employed.
- Include a summary of billing to date and estimated costs to complete the examination.
- Provide a tentative conclusion rather than a preliminary one.
- Identify areas for further investigation and confirm the scope of examination with the attorney.

Report Structure

- A report usually includes the sections shown in the following list, although the order varies depending on organizational guidelines or case requirements:
- Abstract (or summary)
- Table of contents
- Body of report
- Conclusion
- References
- Glossary
- Acknowledgments
- Appendixes

Title and Abstract Importance

- The title of your report should succinctly convey its subject matter, such as "Investigation Findings for Superior Bicycles, Inc.: Intellectual Property Theft."
- An abstract provides a condensed overview of the report's key points, typically totaling about 150 to 200 words.
- It summarizes the examination or investigation and presents the main ideas in a concise form, without duplicating references or results tables.
- Writing the abstract last ensures it accurately reflects the report's content.

Body Structure

- The body of the report comprises the introduction and discussion sections.
- The introduction should:
  - State the report's purpose and questions to be addressed.
  - Demonstrate awareness of terms of reference, methods used, and any limitations.
  - Justify why the report is written and provide a structured overview of its contents.
  - Introduce the problem, progressing from broader issues to specific concerns, and outline the report's aims.

Body Structure

- Craft this section carefully to logically present the processes used in developing information.
- Reference relevant facts, ideas, theories, and related research by other authors.

➢ Discussion sections should be logically organized under headings to classify information and ensure relevance to the investigation.

Conclusion and Supporting Materials

- The conclusion: Refers to the report's purpose and restates main points.
- Draws conclusions and may offer opinions based on findings.
- Supporting materials include references and appendixes:
  - References list supporting materials following a style manual's guidelines, such as Gregg Reference Manual, The Chicago Manual of Style, or MLA Style Manual.
  - Appendixes provide additional resource material not included in the body of the report.

Writing Reports Clearly

- To produce clear and concise reports, evaluate your writing based on the following criteria:
- **Communicative Quality,** Ensure the report is easy to read.
- Consider your audience and make the report appealing to them.
- **Ideas and Organization,** Ensure the information is relevant and clearly organized.
- **Grammar and Vocabulary,** Use simple and direct language to convey meaning clearly and avoid repetition.
- Consistently use technical terms without trying to vary them, as different words for the same concept can cause confusion.
- **Punctuation and Spelling,** Ensure accuracy and consistency in punctuation and spelling.

Characteristics of Good Expert Reports

- **Logical Structure:**
- Present ideas in a logical order to facilitate clear thinking.
- Ensure each sentence logically follows the previous one, building the argument piece by piece.
- Group related ideas and sentences into paragraphs, and organize paragraphs into sections to create a coherent flow from the beginning to the end of the report.

Characteristics of Good Expert Reports+

Clarity and Precision

- Ensure the report is grammatically sound and free of spelling errors and writing mistakes.
- Avoid using jargon, slang, or informal terms.
- Define technical terms in ordinary language or refer readers to a glossary, as most lawyers, judges, and jurors are not technically trained.
- Spell out all acronyms the first time they are used and define any abbreviations that are not standard measurement units.
- Be cautious of potential misinterpretations of abbreviations. For example, "m" is often used for "meter" in scientific writing but could be misunderstood as "mile" by nontechnical readers, especially in the United States.

Considering Writing Style

- Natural Language Style: Use first-person language (e.g., "I") instead of third-person formalities like "your affiant" when appropriate, but avoid excessive repetition of "I."
- Employ a conversational tone to keep readers engaged, while adhering to formal writing guidelines regarding word usage, grammar, and spelling.
- Avoid Vagueness and Generalizations: Provide specific descriptions rather than vague statements.
- Clearly articulate problems encountered and actions taken to address them.
- Mindful of Repetition: Repeat only necessary key words or technical terms to avoid redundancy
- Tense and Voice Usage: Use past tense for describing actions taken during the investigation, but employ present or future tense as applicable.
-

Considering Writing Style+

- Prefer active voice over passive voice for clarity and engagement.
- Balance Detail and Objectivity: Include pertinent details without overwhelming the report with unnecessary information or personal observations.
- Maintain objectivity and focus solely on uncovering the truth, avoiding advocacy or bias towards any particular outcome.
- Project Objectivity: Maintain a sense of detachment and neutrality throughout the report.
- Identify and address any flaws or limitations in your analysis to preempt potential criticisms or challenges.

Including Signposts

Purpose of Signposts:

- Signposts help guide readers to understand what you're communicating.
- They draw attention to key points and indicate the order of processes.

Benefits of Signposts:

- Assist in quickly scanning the text.
- Highlight main points and logical progression.

Examples of Using Signposts:Begin a report section with clear statements like, “This is the report of findings from the forensic examination of computer SN 123456.”

Including Signposts+

- Indicate the sequence of procedures with phrases like, “The first step in this examination was…” followed by “The second step in this examination was…”
- Use words like “First” and “Second” to show the order of tasks or information.

Evaluating Points: Use signposts to evaluate issues, such as “The problem with this is…”

- **Drawing Conclusions**: Introduce conclusions with phrases like, “This means that…” or “The result shows that…”
- By using such signposts, you make your writing clearer and more structured for your readers.

Providing Supporting Material

- Use figures, tables, data, and equations to enhance your narrative.
- Refer to these materials within your text and integrate their points into your writing.
- Number figures and tables sequentially as they appear (e.g., Figure 1, Figure 2, Table 1, Table 2).
- Provide descriptive captions for figures.
- Label all axes in charts and include units of measure.
- Insert a figure or table immediately after the paragraph where it is first mentioned.
- Alternatively, gather all supporting material in one section after the references, before any appendixes.

Formatting Consistently

- Ensure all formatting choices are applied uniformly throughout the document.
- If you indent paragraphs, make sure every paragraph is indented.
- Use the same font style and size consistently.
- Apply consistent heading styles, such as major headings in bold with initial capitals and minor headings in italics.
- Use a single format for units of measure consistently; for example, choose either “%” or “percent” and use it throughout the document.
- Establish a template for formatting and adhere to it throughout the document.

Explaining Examination and Data Collection Methods

- Clearly explain how you studied the problem, ensuring it aligns with the report's purpose.
- Depending on the data type, include subsections on:
  - ✓ Examination procedures
  - ✓ Materials or equipment used
  - ✓ Data collection and sources
  - ✓ Analytical or statistical techniques
- Provide enough detail for readers to fully understand your methods
- Data collection is a crucial part of the report. Accurate data recording in a lab notebook or file is essential.

Explaining Examination and Data Collection Methods+

- If your data collection is scrutinized, presenting data in an organized manner is vital.
- Use tables to show how data was handled and examined.
- Ensure tables are clearly labeled regarding their content and are numbered sequentially for easy reference.

Including Calculations

- Hashing algorithms are commonly calculated in digital forensics.
- Specify the common name of the algorithm used, like "Message Digest 5 (MD5) hash."
- Generally, explaining the purpose of the hashing tool and citing authoritative sources or policies suffices.
- For instance, citing the National Software Reference Library (NSRL) or court cases can justify the tool's usage.

Providing for Uncertainty and Error Analysis

- Acknowledge limitations and uncertainties in your findings to maintain credibility.
- For example, if using file timestamps, note the potential for PC clock resets.
- Highlight alternative indicators like timestamps of related files or creation orders.

Explaining Results and Conclusions

- Structure your discussion with clear subheadings.
- Comment on results as presented, emphasizing their significance in relation to the report's objectives.
- Avoid bias by describing actual findings rather than expectations.
- Link discussions to supporting materials like figures and tables for clarity.
- If necessary, include similar figures in an appendix, selecting representative examples for the main report.
- Save broader generalizations for the conclusion, which should succinctly summarize findings and key points.

Providing References

- Cite all sources used in the report, including books, websites, and personal communications.
- In-text citations typically follow the author's last name and year of publication.
- List references alphabetically in a separate section, providing enough detail for others to locate the sources.

Including Appendixes

- Appendices can contain supplementary material like raw data and additional figures, arranged in the order referenced in the report.
- Some elements, like exhibits and curriculum vitae, might be mandatory depending on legal requirements or organizational standards.

Generating Report Findings with Forensics Software Tools

- To generate reports using Autopsy, an open-source digital forensics platform, follow these steps:

Installation and Setup:

- Download and install Autopsy on your computer.
- Set up the necessary configurations and options according to your investigation requirements

Case Creation:

- Create a new case in Autopsy and provide relevant details such as case name, investigator's name, and case number..

Generating Report Findings with Forensics Software Tools+

Data Acquisition

- Add evidence sources to the case, such as disk images, files, or directories.
- Autopsy supports various file formats and acquisition methods, including disk images, logical files, and network acquisitions.

Analysis and Examination

- Perform analysis using Autopsy's built-in tools, including keyword search, timeline analysis, file categorization, and hash analysis.
- Use Autopsy's features to examine file metadata, internet activity, chat logs, and deleted files.

Generating Report Findings with Forensics Software Tools++

Generating Reports

- Navigate to the reporting section within Autopsy.
- Customize the report template based on the specific requirements of your investigation or organization.
- Include relevant details such as case information, evidence sources, analysis findings, and conclusions.
- Autopsy allows for the inclusion of visual aids such as charts, graphs, and tables to enhance the clarity of the report.
- Export the report in the desired format, such as PDF or HTML, for sharing or presentation purposes.

Generating Report Findings with Forensics Software Tools+++

Review and Validation

- Review the generated report to ensure accuracy, completeness, and compliance with investigative standards.
- Validate findings and conclusions through peer review or additional analysis if necessary.

Documentation and Archiving

- Document any additional notes or observations related to the investigation process.
- Archive the report, along with any supporting documentation or evidence, in a secure location for future reference or legal proceedings

Sample Investigation Report

- **Investigation Findings for Superior Bicycles, Inc.: Intellectual Property Theft**

Abstract

- This report summarizes the investigation into the alleged intellectual property theft at Superior Bicycles, Inc.
- The examination focused on identifying unauthorized access to proprietary designs and documents. Key findings indicate that a former employee accessed and transferred sensitive data.
- This report presents the investigation's methods, findings, and conclusions, providing a comprehensive overview of the digital forensic analysis conducted.

Sample Investigation Report+

Table of Contents

Sample Investigation Report++

Introduction

- The purpose of this report is to investigate the alleged intellectual property theft at Superior Bicycles, Inc. Specifically, it seeks to determine whether proprietary designs and documents were accessed and transferred without authorization.
- This report outlines the methods used in the investigation, discusses the findings, and presents the conclusions drawn from the analysis.

Methods

- The investigation employed various digital forensic techniques to analyze the suspected data breach. These methods included:

Sample Investigation Report+++

- **Data Collection:** Imaging of hard drives and relevant storage devices.
- **Data Analysis:** Use of forensic tools such as EnCase and FTK to examine file access logs and data transfers.
- **Network Analysis:** Review of network logs to identify unauthorized access attempts.
- **Interviews:** Conducting interviews with key personnel to gather additional context and information.

Sample Investigation Report++++

Findings

- The investigation revealed several key findings:
- **Unauthorized Access:** Evidence shows that a former employee accessed proprietary designs on multiple occasions.
- **Data Transfer:** Forensic analysis identified multiple instances of data being transferred to external storage devices.
- **Email Correspondence:** Review of email logs indicated communication between the former employee and a competitor.
- **File Deletion:** Attempts were made to delete logs and files to cover the tracks of unauthorized activities.

Sample Investigation Report+++++

Discussion

- The findings indicate a deliberate attempt to steal intellectual property.
- The former employee's access to sensitive data and subsequent data transfers suggest a breach of company protocols.
- The email correspondence with a competitor raises further concerns about the misuse of the stolen information.
- The investigation faced certain limitations, such as incomplete network logs and the lack of physical access to some devices used by the former employee.
- Despite these limitations, the collected evidence provides a strong basis for concluding that intellectual property theft occurred.

Sample Investigation Report++++++

- **Conclusion**
- This investigation confirms that intellectual property theft took place at Superior Bicycles, Inc.
- The former employee accessed and transferred sensitive designs and documents, violating company policies and potentially causing significant business harm.
- The evidence supports taking legal action against the responsible individual and implementing stronger security measures to prevent future incidents.

Sample Investigation Report+++++++

References

- Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley.
- Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
- Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to Computer Forensics and Investigations. Cengage Learning.

Sample Investigation Report++++++++

Appendixes

- **Appendix A: Glossary of Terms**
- **FTK:** Forensic Toolkit, a digital investigations software.
- **EnCase:** A suite of digital forensic tools used for data acquisition and analysis.

Appendix B: Evidence Summary

- **Exhibit 1:** Screen capture of unauthorized access logs.
- **Exhibit 2:** Data transfer logs to external devices.
- **Exhibit 3:** Email correspondence between the former employee and a competitor.

Reference

1. Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning.
2. Sun, J. R., Shih, M. L., & Hwang, M. S. (2015). A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure. *Int. J. Netw. Secur.*, *17*
3. Oettinger, W. (2020). *Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence*. Packt Publishing Ltd.