Writing Computer Forensic Reports

Objectives

- Understand the Importance of Reports
- List Procedural and Evidence Requirements
- List Report Types
- Determine What's Needed to Express an Opinion
- Express an Opinion
- Document a Report

Forensics Report

- A document that describes the examination of the contents of a system (or systems).

A standard way to document:

- Why the system was reviewed
- How the computer data was reviewed
- How conclusions were arrived at.

Expert Report

- A report that does not offer an opinion is not an expert report.
- Report writing requires a documented process to ensure a repeatable standard is met.

Expert Witness

- A person who is a specialist in a subject, often technical, who may present his/her expert opinion without having been a witness to any occurrence relating to the lawsuit or criminal case.
- It is an exception to the rule against giving an opinion in trial, provided that the expert is qualified by evidence of his/her expertise, training and special knowledge.
- If the expertise is challenged, the attorney for the party calling the "expert" must make a showing of the necessary background through questions in court, and the trial judge has discretion to qualify the witness or rule he/she is not an expert, or is an expert on limited subjects.
-

--http://legal-dictionary.thefreedictionary.com/Expert+opinion

Report Goals

- Accurately describe an incident's details
  - Attributes
    - Timely.
    - Understandable to decision makers
    - Able to withstand legal scrutiny
    - Unambiguous
    - Easily referenced
- Contains all information required to explain conclusions
- When needed, offers:
  - valid conclusion
  - Opinions
  - recommendations

Related Goals

- Clients desires.
  - Single or multiple reports
- Report, verbal or written?
- Reporting frequency?
- Interim reports verbal or written?
- Who signs off on final report?

Relevant Terms

Lay Witness
Witness not considered an expert in a particular field.

Verbal Formal Report
Structured report delivered in person to a board of directors or managers or to a jury.

Report Terms

Examination Plan
The plan laying out the strategy created by the attorney to try a case.

Verbal Informal Report
A report that is less structured than a formal report and is delivered in person, usually in an attorney's office.

Verbal Informal Reports

A verbal informal report may be appropriate, for areas of an investigation that are yet to be completed:

- Tests may not have been concluded
- Interrogatories
- Document production
- Deposition

Report Types

Written Formal Report

A written report sworn under oath, such as an affidavit or declaration.

Written Informal Report

A report that is less structured than a formal report and is delivered in person, usually in an attorney's office.

High-Risk Documents

A document that contains sensitive information that could create an advantage for the opposing attorney.

Legal Terms

Discovery

The efforts to obtain information before a trial by demanding documents, depositions, questions and answers written under oath, written requests for admissions of fact, and examination of the scene, for example.

Spoliation

Destroying or concealing evidence.

Note

Notes made during a civil or criminal case may be discoverable.

Expressing an Opinion

As an expert witness, you may testify to an opinion, or conclusion, if basic conditions are met

- The opinion, inferences, or conclusions, depend on special knowledge, skill, or training not within the ordinary experience of lay jurors.
- The witness must be shown to be qualified as a true expert in the particular field of expertise.
- Expert witness's must first describe the data on what the opinion, inference, or conclusion, is based or, in the alternative, he or she must testify in response to a hypothetical question that sets forth the underlying evidence.

Guidelines

As you write your report, keep the following guidelines in mind :

- Don’t make any assumptions.
- Don’t identify leads.
- Check your spelling before the report leaves your office; don’t wait for a supervisor or the attorney to proofread your report.
- Double-check the media that you have stored findings to. If you create a findings CD, make sure the data is on it before you send it out.

Writing Quality

- **Think about the criteria for assessment of English language skills in a written report.**
- **You should criticize and assess the quality of your writing. Consider the following criteria:**

 - Communicative quality – Is it easy to read?
 - Ideas and organization – Is the information appropriate and clearly organized?

Report Organization

- Start at a high, non technical level
- As report goes on, increase detail and technology.
- Include an appropriate table of contents.
- Use consistent identifiers.
- Use attachments and appendices to maintain the flow of the report.
- Use MD-5 Hashes.
- Include Meta Data

Investigation Reports

Provide lists or figures from the sources, as in the following:

- Personal (unpublished) communications
- Lecture notes
- Web sites
- Single author journal paper
- Multiple author journal paper
- Book
- Government/technical report
- Chapter in an edited volume

Sample Report Template

- Executive Summary
- Objectives
- Computer Evidence Analyzed
- Relevant Findings
- Supporting Details
- Investigative Leads
- Additional subsections
  - Attacker methodology
  - User apps
  - Internet Activity
  - Recommendations

Executive Summary

- Provides background information of the circumstances that brought about the need for an investigation.

Includes

- Who authorized project
- Why examination was necessary
- Significant findings
- Signature block for examiners who performed work

Objectives

- Outlines all investigative tasks.

Evidence Analyzed

- Introduces all the evidence that was collected and interpreted when creating the investigative report.

Relevant Findings

- Provides a summary of the findings of probative value.

Supporting Details

- Outlines all the tasks we undertook to meet the objectives.
- Provides background details about the media analyzed.

Investigative Leads

- Document steps, that although perhaps beyond the scope of your forensic report, could generate actions that lead to the successful resolution of the case.

Summary

- Timely
- Accurately describe incident details in a manner understandable to decision makers.
- Able to withstand legal scrutiny
- Unambiguous
  - Not open to misinterpretation.
- Easily referenced.
- Containing all information necessary to explain conclusions.
- When needed, offer valid conclusions, opinions, or recommendations.
  - Assists case.

Questions?