Guide to Computer Forensics and Investigations Sixth Edition

Chapter 14

Report Writing for High-Tech Investigations

Objectives

- Explain the importance of reports
- Describe guidelines for writing reports
- Explain how to use forensics tools to generate reports

Understanding the Importance of Reports (1 of 3)

- Communicate the results of your investigation
  - Including expert opinion
- Forensic reports can:
  - Provide justification for collecting more evidence
  - Be used at a probable cause hearing
  - Communicate expert opinion
- U.S. district courts require expert witnesses to submit written reports
  - State courts are starting to also require them

Understanding the Importance of Reports (2 of 3)

- Rule 26, Federal Rules of Civil Procedure requires submission of the expert's written report that includes:
  - Testimony is based on sufficient facts or data
  - Testimony is the product of reliable principles and methods
  - Witness has applied the principles and methods reliably to the facts of the case
- Written report must specify fees paid for the expert's services
  - And list all other civil or criminal cases in which the expert has testified

Understanding the Importance of Reports (3 of 3)

- Keep a copy of any deposition notice or subpoena so that you can include the following:
  - Jurisdiction
  - Style of the case
  - Cause number
  - Date and location of the deposition
  - Name of the deponent
- **Deposition banks**
  - Examples of expert witness' previous testimonies

Limiting a Report to Specifics

- All reports to clients should start with the job mission or goal
  - Find information on a specific subject
  - Recover certain important documents
  - Recover certain types of files with specific dates and times
- Before you begin writing, identify your audience and the purpose of the report

Types of Reports (1 of 4)

- Digital forensics examiners are required to create different types of reports
- **Examination plan**
  - What questions to expect when testifying
  - Attorney uses the examination plan to guide you in your testimony
  - You can propose changes to clarify or define information
  - Helps your attorney learn the terms and functions used in computer forensics

Types of Reports (2 of 4)

WITNESS EXAMINATION PLAN

WITNES: Joseph Friday /Factors: Expert Digital Forensic Examiner.

Direct Examination: Expert Testimony Objective/Rule/

Testimony CV

Identity and Address Iowa Bureau of Criminal Investigations

Position (Current) Digital Forensic Examiner

Undergraduate Iowa State University summa cum laude 1990 BS Computer Science

Master's Degree Purdue University, 1992 MS Electrical Engineering

Summer Internship 1989 Des Moines Police Department

Academic Appointments

Lecturer, Dept. of Computer Science, University of Iowa 1998-Current

Instructor, Iowa Police Academy

Professional Society Certifications

P.E. 1990

CISSP 2001

Memberships

American Society of Industrial Security

Publications

Journal of the Iowa State Bar Association, May 1999, "Computer Forensics on RAID Servers-Testifying to Reasonable Certainty"

Experience

How many systems have you conducted forensic examinations on?

The Client

What is your relationship to the Plaintiff? Retained by his attorney to examine the hard drive of his computer for all financial records. I have never actually met or talked to Mr. Smith.

The Specific Examination

How long does it take you to conduct this examination?

What type of files were you looking for? Why those types of files? Where did you find those files?

What condition were the files in?

What is your opinion as to the cause of that condition?

Can you say for a reasonable certainty that the financial data files were deleted intentionally? Yes.

Are you able to state to a reasonable certainty who deleted the financial data files? Yes.

What is your fee for examining the hard drive, preparing a report and testifying?

Anticipated Cross Examination – Expert Testimony

How many times have you worked for Mr. Sawyer as an expert witness? I've done 16 contracts as a consultant expert or expert witness.

Have you ever previously testified that overwriting utilities are not 100% reliable? Yes, but that was in 1994 and utilities are so far as I can tell are 100% reliable today.

Figure 14-1 A sample examination plan

Types of Reports (3 of 4)

- Verbal report
  - Less structured
  - Attorneys cannot be forced to release verbal reports
  - Preliminary report
  - Addresses areas of investigation yet to be completed
    - Tests that have not been concluded
    - Interrogatories
    - Document production
    - Depositions

Types of Reports (4 of 4)

- Written report
  - Affidavit or declaration
  - Limit what you write and pay attention to details
    - Include thorough documentation and support of what you write

Guidelines for Writing Reports (1 of 2)

- Hypothetical questions based on factual evidence
  - Guide and support your opinion
  - Can be abused and overly complex
- Opinions based on knowledge and experience
- State the facts needed to answer the question
  - Don’t include any unnecessary facts

Guidelines for Writing Reports (2 of 2)

- As an expert witness, you may testify to an opinion or conclusion, if four basic conditions are met:
  - Opinion, inferences, or conclusions depend on special knowledge, skills, or training
  - Witness should qualify as a true expert in the field
  - Witness must testify to a reasonable degree of certainty
  - Experts must know facts on which their opinions are based, or they must testify to a hypothetical question

What to Include in Written Preliminary Reports (1 of 2)

- Anything you write down as part of your examination for a report
  - Subject to discovery from the opposing attorney
  - **Discovery**: the process of opposing attorneys seeking information from each other
- Written preliminary reports are considered **high-risk documents**
  - It's better if there's no written report to provide
- Destroying the report could be considered destroying or concealing evidence (spoliation)

What to Include in Written Preliminary Reports (2 of 2)

- Include the same information as in verbal reports
- Additional items to include in your report:
  - Summarize your billing to date and estimate costs to complete the effort
  - Identify the tentative conclusion (rather than the preliminary conclusion)
  - Identify areas for further investigation and get confirmation from the attorney on the scope of your examination

Report Structure (1 of 2)

- Structure
  - Abstract (summary)
  - Table of contents
  - Body of report
  - Conclusion
  - References
  - Glossary
  - Acknowledgements
  - Appendixes

Report Structure (2 of 2)

- An abstract condenses the report to concentrate on the essential information
- The body consists of the introduction and discussion sections
- 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 (1 of 3)

- Consider
  - Communicative quality
  - Ideas and organization
  - Grammar and vocabulary
  - Punctuation and spelling
- Lay out ideas in logical order
- Build arguments piece by piece
- Group related ideas and sentences into paragraphs
  - Group paragraphs into sections

Writing Reports Clearly (2 of 3)

- Avoid jargon, slang, and colloquial terms
- Define technical terms
  - Consider your audience
- Considering writing style
  - Use a natural language style
  - Avoid repetition, vague language, and generalizations
  - Use active rather than passive voice
  - Avoid presenting too many details and personal observations

Writing Reports Clearly (3 of 3)

- Considering writing style (cont'd)
  - Project objectivity
    - Communicate calm, detached observations
- Including signposts
  - Draw reader's attention to a point
  - Assist readers in scanning the text quickly by highlighting the main points and logical development of information

Designing the Layout and Presentation of Reports (1 of 4)

- Two numbering systems are typically used
- Decimal numbering structure
  - Divides material into sections
  - Readers can scan heading
  - Readers see how parts relate to each other
- Legal-sequential numbering
  - Used in pleadings
  - Roman numerals represent major aspects
  - Arabic numbers are supporting information

Designing the Layout and Presentation of Reports (2 of 4)

- Providing supporting material
  - Use material such as figures, tables, data, and equations to help tell the story as it unfolds
- Formatting consistently
  - How you format text is less important than being consistent in applying formatting
- Explaining examination and data collection methods
  - Explain how you studied the problem, which should follow logically from the report's purpose

Designing the Layout and Presentation of Reports (3 of 4)

- Including calculations
  - If you use any hashing algorithms, be sure to give the common name
- Providing for uncertainty and error analysis
  - Protect your credibility
- Explaining results and conclusions
  - Explain your findings, using subheadings to divide the discussion into logical parts
  - Save broader generalizations and summaries for the report's conclusion

Designing the Layout and Presentation of Reports (4 of 4)

- Providing references
  - Cite references by author's last name and year of publication
  - Follow a standard format
- Including appendixes
  - 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

Generating Report Findings with Forensics Software Tools

- Forensics tools generate reports when performing analysis
  - It is still your responsibility to explain the significance of the evidence
- Report formats
  - Plaintext
  - Word processor
  - Spreadsheet
  - HTML format

Using Autopsy to Generate Reports (1 of 4)

- Follow Activity steps starting on page 575

Using Autopsy to Generate Reports (2 of 4)

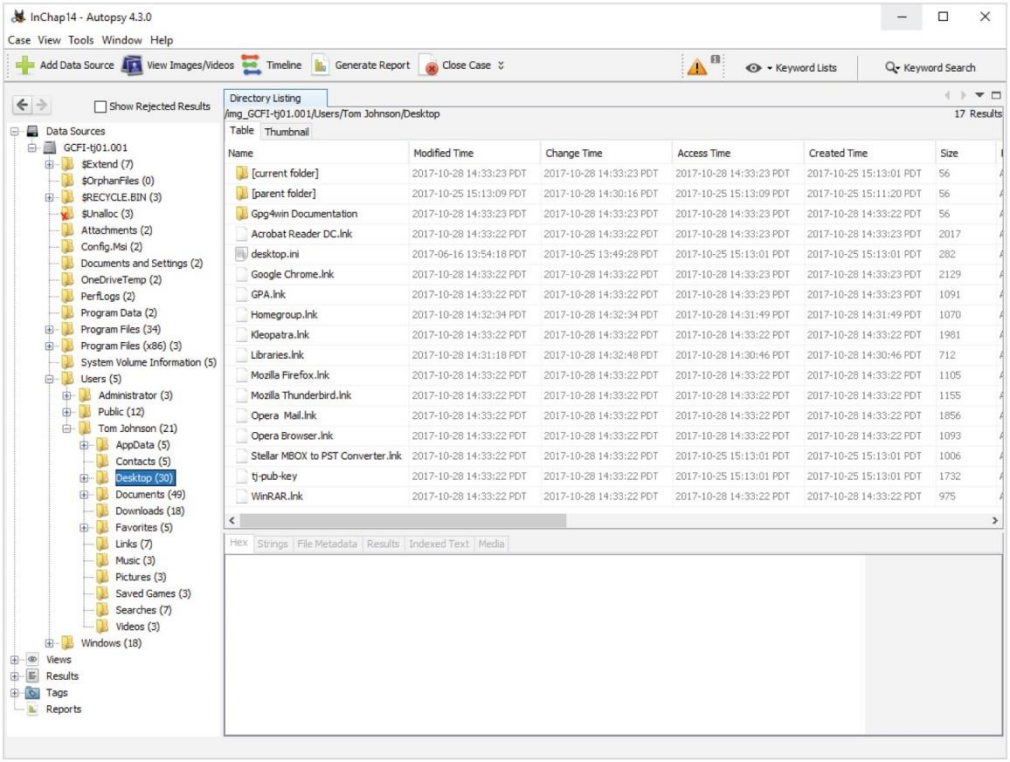

Figure 14-2 Viewing the Desktop folder

Source: *www.sleuthkit.org*

Using Autopsy to Generate Reports (3 of 4)

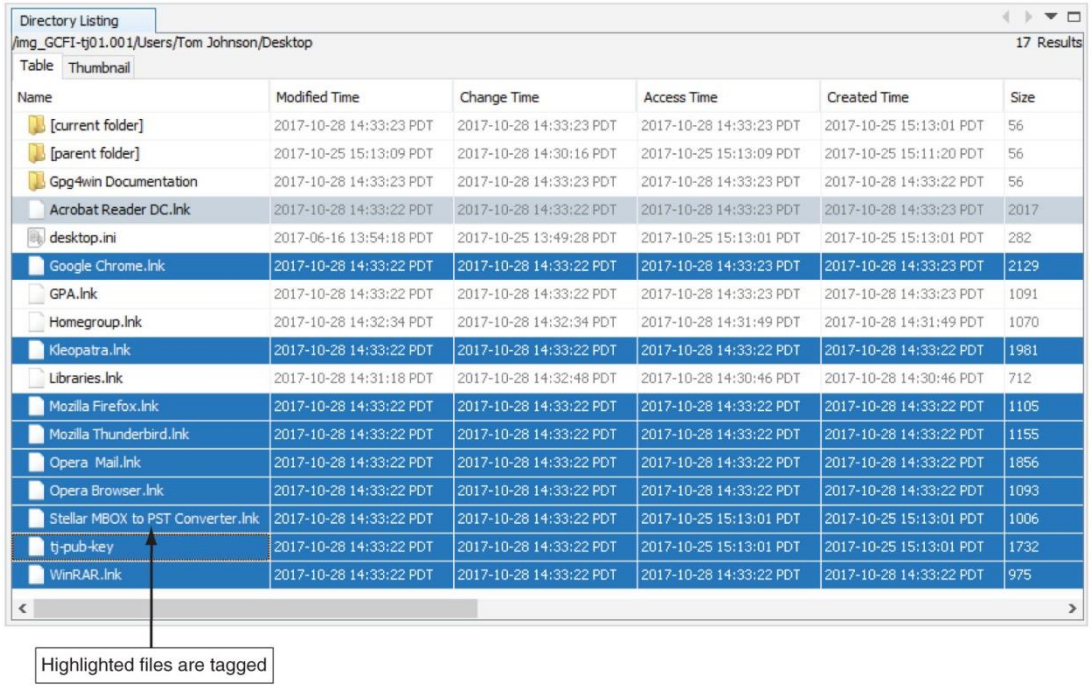

Figure 14-3 Tagged files in the Desktop folder

Source: *www.sleuthkit.org*

Using Autopsy to Generate Reports (4 of 4)

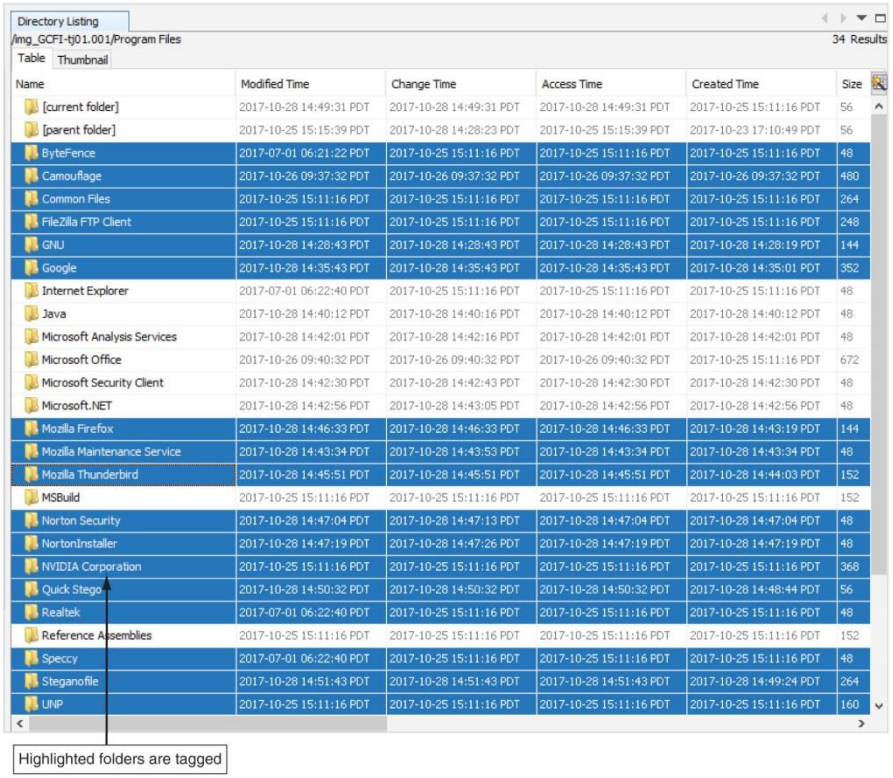

Figure 14-4 Tagged application folders under Program Files

Source: *www.sleuthkit.org*

Summary (1 of 2)

- All U.S. district courts and many state courts require expert witnesses to submit written reports
- Rule 26 of the FRCP requires expert witnesses who anticipate testifying to submit written reports
- Attorneys use deposition banks to research expert witnesses' previous testimony
- Reports should answer the questions you were retained to answer

Summary (2 of 2)

- A well-defined report structure contributes to readers' ability to understand the information you're communicating
- Clarity of writing is critical to a report's success
- Convey a tone of objectivity and be detached in your observations