Reporting

Objectives

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

Impact of Reports

- 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

Impact of Reports (Cont.)

- 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

Impact of Reports (Cont.)

- 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

Specificity

- 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
  - Provide explanations as appropriate

Report Types

- Formal
- Preliminary / Verbal
- Examination Plan

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

Examination Plan Example

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

Preliminary / Verbal Report

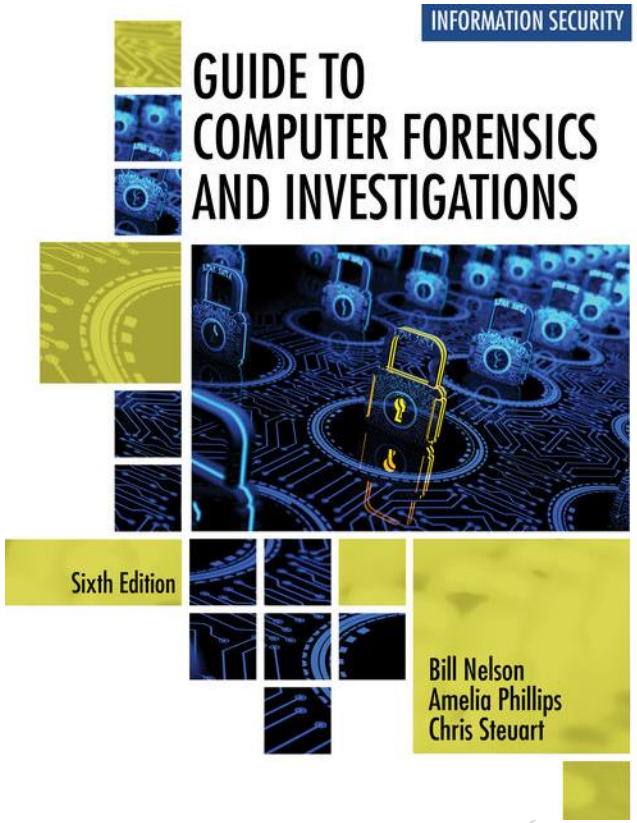
- Less structured
- Attorneys cannot be forced to release verbal reports
  - Preliminary reports can be discovered
- Addresses areas of investigation yet to be completed
  - Tests that have not been concluded
  - Interrogatories
  - Document production
  - Depositions

Written Report

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

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Writing Reports

Report Guidelines

- 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

Expert Witnesses

- 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

Preliminary Reports

- 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)

Preliminary Reports (Cont.)

- 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

Sample Report Structure

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

Report Structure Notes

- An abstract condenses the report to concentrate on the essential information
  - Write this after completing all other components of the report
- 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

Clarity

- Communicative quality
  - Make the report easy to read for those that will consume it
  - Use active voice
- Ideas and organization
  - Make sure all included information is relevant and in a logical order
- Grammar and vocabulary
  - Language should be simple without repetitive text
  - Technical terms used must be used consistently (include a glossary if necessary)
- Punctuation and spelling
  - Consistency and accuracy are important here as well

Be Objective

- Communicate calm, detached observations
- Your job is to describe what happened based on your technical expertise
  - Identify deviations from this yourself and fix them before presenting the report

Layout & Presentation

Headings & Numbering

- Clearly identify your headings and sub headings with both font adjustments and formal numbering
  - How you format is less important than formatting consistently
- 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

Supporting Material

- Use material such as figures, tables, data, and equations to help tell the story as it unfolds
- This can include screenshots of artifacts and tools used as long as context is provided
  - It's likely you'll also include those items as attachments to the report

Explanations (Data Collection & Examination)

- Explain how you studied the problem, which should follow logically from the report's purpose
  - Try and leave the reader without any questions about your approach
- If you summarize the data collection process or examination within your report, you should still include a full log of your notes as an appendix
- Calculations included should have citations to demonstrate validity
  - Previous use of tool in a case
  - Use in a well-known resource (Text ex: NSRL)

Uncertainty & Error Analysis

- Most results of a computer forensics investigation are absolutes
- Be sure to include a statement of limitations of knowledge and uncertainty to protect credibility
  - Example: timestamp on a file

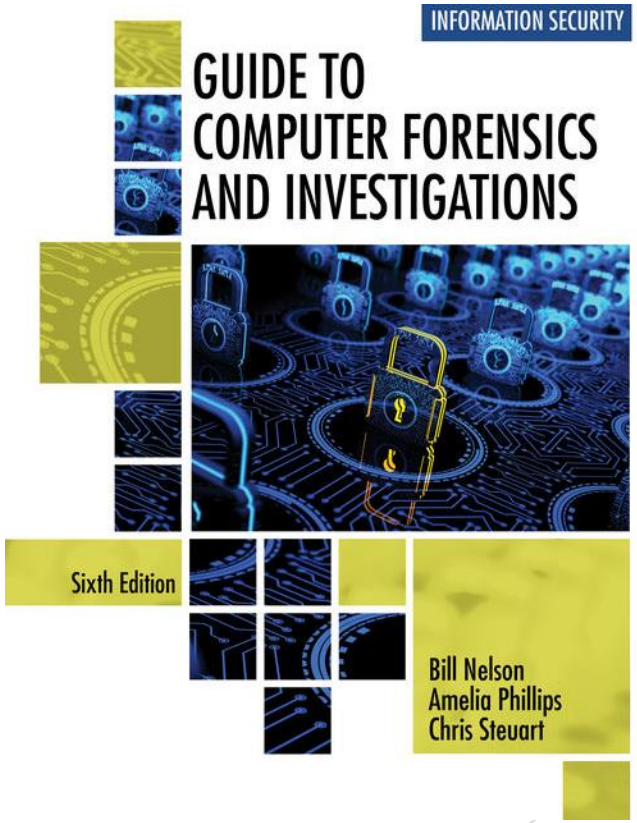
Results, Conclusions, & References

- Explain your findings, using subheadings to divide the discussion into logical parts
  - What you actually found, not what you expected to find or wanted to find
  - Which questions have been answered and which have not
- Save broader generalizations and summaries for the report's conclusion
- Providing references
  - Cite references by author's last name and year of publication
  - Follow a standard format

Tool Reports

References

- *Guide to Computer Forensics and Investigations*
  - *ISBN: 9780357688595*



Windows Artifacts

A Non-Exhaustive List

What is an artifact?

- Within computer forensics:

An object of digital archaeological interest.

Where digital archaeology roughly refers to computer forensics without the forensic (legal) context.

https://forensicswiki.xyz/wiki/index.php?title=Artifacts

Examples of Windows Artifacts

- Prefetch
- MRU (Most Recently Used)
  - Last-Visited
  - Open/Save
- Jump Lists
- UserAssist
- Browser History
  - Cookies
- Thumbcache / Thumbs.db
- Recycle Bin
- Shell Bags
- System Logs
- USB / USBSTOR

Revisiting the Registry

Table 5-6 Registry file locations and purposes

Filename and location	Purpose of file
Users*user-account*\Ntuser.dat	User-protected storage area; contains the list of most recently used files and desktop configuration settings
Windows\system32\config\Default.dat	Contains the computer's system settings
Windows\system32\config\SAM.dat	Contains user account management and security settings
Windows\system32\config\Security.dat	Contains the computer's security settings
Windows\system32\config\Software.dat	Contains installed programs' settings and associated usernames and passwords
Windows\system32\config\System.dat	Contains additional computer system settings
Windows\system32\config\systemprofile	Contains additional NTUSER information

Defined

- The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that **opt** to use the registry.

https://en.wikipedia.org/wiki/Windows_Registry

Investigating the Registry

- Going to be dependent on what you're looking for
  - https://www.dfir.training/ultimate-registry-forensics-cheat-sheet
- Other artifacts originate in the registry – extraction may or may not be automated by your tool
  - Persistence: https://forensicswiki.xyz/wiki/index.php?title=Windows_Registry#Persistence_keys

MRU Lists

- Most Recently Used (MRU) Lists
  - Most Recently Used (MRU) is a term used in computing to refer to the list of programs or documents that were last accessed. It is a feature of convenience allowing users to quickly see and access the last few used files and documents…
- Open/Save – lists files that are opened or saved with Windows Explorer or similar dialogs
- Last-Visited – lists executable used by an application to open a file and the location of the most recently opened file

https://forensicswiki.xyz/wiki/index.php?title=MRU

MRU Lists

- Paths (Win7+):
  - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDlMRU
  - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU

https://forensicswiki.xyz/wiki/index.php?title=MRU

Prefetch

- We've discussed this before
  - Prefetch helps speed up application and OS start time
- Can tell us when application was last executed
  - CreateTime: First execution
  - ModifiedTime: Most recent execution
  - .pf includes count
- Path: C:\Windows\Prefetch
- Autopsy Addon: https://github.com/markmckinnon/Autopsy-Plugins/tree/master/Process_Prefetch_Files_V41

Jump Lists

- Feature added in Windows 7+ to allow you to select files recently used in an application from the taskbar
- Path: C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- Creation Time: First time item added
- Modification Time: Last time item added

UserAssist

- Applications launched from the desktop are tracked here
  - ROT-13 encoded application name
  - Executable: CEBFF5CD
  - Shortcut: F4E57C4B

- Hive: NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\ {GUID}\Count

Browser History

- Chrome: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History
- IE: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat
- Firefox: %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\<random text>.default\places.sqlite
  - Table:moz_annos

Thumbcache / Thumbs.db

- Each Windows user has a thumbcache contains thumbnails of documents, pictures, and folders
  - Path: C:\%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer
- Thumbs.db is a hidden file in a directory that keeps track of image thumbnails even if they're deleted
  - Not created by default on Windows 7+ systems

Recycle Bin

- Files deleted by users end up here before being deleted
- Path: C:\$Recycle.bin

Shell Bags

- Information related to how files are displayed in a particular directory
- Identify recently accessed directories

- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
- USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU
- NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

https://www.sans.org/blog/computer-forensic-artifacts-windows-7-shellbags/

System Logs

- Windows event logs can be a rich source of info related to system access and usage
- Path: %system root%\System32\winevt\logs\

USB / USBSTOR

- USB Device Info
  - SYSTEM\CurrentControlSet\Enum\USB
  - SYSTEM\CurrentControlSet\Enum\USBSTOR

References

- https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download
  - © 2021 Rob Lee
- https://github.com/ForensicArtifacts/artifacts