Chapter 7

Real Forensic Cases and It’s Tools

A forensic report is the primary work product of a forensic psychologist. The aim of a forensic report is to inform and influence the court. These kinds of errors were used to discuss best practices in forensic report writing like as failure to answer the referral question, organization problems, language problems, mixed data and interpretation, inclusion of irrelevant data, over-reliance on a single source of data, improper psychological test use, failure to consider alternative hypotheses, and opinions without sufficient explanation.

Goals of Report :

The report writing requires documented process according to golden rule set by the organization. If your investigative reports to be accurate, written in timely manner and understandable to your audience then following goals to be achieved:

1. Accurately describe the details of an incident.
2. Be understandable to decision makers.
3. Be able to withstand a barrage of legal scrutiny.
4. Be unambiguous and not open to misinterpretation.
5. Be easily reference.
6. Contain all information required to explain your consideration.
7. Offer valid conclusions, opinions or

Recommendations when needed.

8. Report should be ready in time.

Layout of an Investigative Report

1. Executive Summary : The contextual information of the state of affairs that bought the essential for an investigation is the "executive summary" unit. This is the section that senior management just might read so things that matter should be included in short like as a) Include who authorized the forensic examination.

   b) Describe why a forensic examination of computer media is necessary.

c) List what the significant findings.

d) Include signature block for examiner who performed the work.

2. Objective : This section outline all the tasks that our investigation intended to accomplish i.e. forensic examination of media may include criteria that focuses and narrow your examination.

3. Computer Evidence analysed : While creating the investigative report, all the evidence that was collected and interpreted are included and represented into tabular or image format for reference.

4.Relevant findings: When describing the results of the investigation, relevant findings provides the quick reference that high level decision makers need and make use of. The fine details supporting these findings should be written in a different section.

5.Supporting Details : An in-depth look and analysis of the relative findings is provided in listing along with following relevant information.

a) Tables listing with full details
b) Pathnames of important files
c) The number of files reviewed
d) String search results
e) E-mails or URLs reviewed.

To meet the objective outlined , it also included many subsections to tailor organization of the report. It also included background details about actual media analysed.

6. Investigative List : In this section, we outline action items that could be performed to discover additional information pertinent to the investigation.

If more time or additional resources were provided to the examiner or investigator, these are the outstanding tasks that could be completed.

For example : The Linux partition on the laptop contained Palm Pilot files. A review of the data stores for the Palm Pilot personal digital assistant can be conducted.

7. Additional Report Subsection : Depend upon needs of circumstances or customer the additional subsections are included

a) Attacker Methodology : To understand the how and what kind of attack conducted , standard logs examine how the attack was executed and what remnants of the attack look like.

b) User applications: This section deals with application present on the system are relevant or not. Any relevant application that were installed on the media analysed.

c) Internet Activity or Web browsing history : The data that often harbor evidence vital to an investigation, browser history can also be used to suggest intent, online research/predisposition , downloads of secure delete program or evidence elimination type program.

d) Recommendations : It provides some recommendations to postures our consumer or client to be more prepared and trained.

Guidelines for Writing a Report

1. Document investigative steps immediately and clearly : These represent general principle that should be followed to ensure your organization can exceed expectation with your investigative reports. Do not use short form, unclear notations, incomplete scribbling or unclear documentation which are hard to comprehend.

2. Know the goals of your analysis : Your report must be more focused based on in-depth analysis of evidences to address all necessary issues of crimes.

It gives all information regarding sample size of investigative data and mode of collecting samples and whether evidence collected via verbal or written mode etc.

3. Organize your report : Organize your forensic reports to start at high level and have complexity of your report increase as your audience continues to read it. For longer reports include a table of contents to show what the report accomplishes.

4.Follow a template : The standardized report template should be follows to make report writing scalable, establishes a repeatable standard and save time.

5. Use consistent identifiers : There can be confusion created in a report by referreing to an item in different ways. Developing a consistent, unwaving way to reference each item throughout your report is critical to eliminate such ambiguity.

6. Use attachments and appendices : In your report, you can also include a brief reference to appendix to maintain the flow of your report by attaching information ,files and file fragments that you point out in your reports.

7. Have coworkers read your reports : To read your forensic reports , employ other coworker, it will help in developing report that are comprehensible to nontechnical personnel so that it can impact on your incident response strategy and resolutions. Knowledge of your audience and technical capability should be taken into consideration.

8.Use MD5 hashes : Performing MD5 hashes for all evidence provides support to the claim that you are diligent and attentive to the special requirements

Of forensic examination. The MD5 hashes calculated for a given set of a data will remain the same if evidences handled properly and remain tamper proof.

9. Include metadata : Record and include the metadata for every file or file fragments cited in your report. This metadata includes the time/date stamps, full path of the file size and the file’s MD5 sum.

Computer Forensic Tools

Computer forensics also uses some tools to perform investigations. Some of them are

- Digital Forensics
- Open Computer Forensics Architecture
- Caine
- X-Ways Forensics
- EnCase
- Registry Recon
- Volatility and many more…

These tools can be further classified into:

- Disk and Data Capture Tools
- Database Forensics Tools
- File Viewers
- Network Forensics Tools
- File Analysis Tools
- MacOS Analysis Tools
- Internet Analysis Tools
- Mobile Devices Analysis Tools
- Email Analysis Tools
- Registry Analysis Tools

Digital forensic tools make our work much more efficient or even possible. There are tools for specific purposes as well as tools with broader functionality. They can come in the form of both hardware or software. They can be commercial tools that must be purchased or they can be open source that are freely available. There are advantages and disadvantages to all. Keep in mind, no single tool does everything or does everything exceedingly well. As such, it's a good practice to have multiple tools available. Using multiple tools is also a great way to validate your findings. The same results, with two different tools, significantly increase the reliability of the evidence.

FTK Tool

Computers are the backbone of any digital forensics lab, so, as an examiner, you will need the best computer workstation you can afford. Digital forensic exams require quite a bit of computing power. These jobs can tax even the best systems and crush those that don't measure up. A good exam machine has multiple, multicore processors; as much RAM as you can get (the more the better); and large, fast hard drives. Forensic software manufacturers provide detailed lists of minimum and suggested hardware requirements. Straying below the minimums is done at your own risk. To get a better understanding, let's look at the minimum and recommended system requirements (as of press time) for AccessData's Forensic Tool Kit (FTK).

AccessData’s FTK has four distinct components and or applications. They are:

1.Oracle Database

2.FTK Client User Interface (UI)

3.Client-side Processing Engine

4.Distributed Processing Engine

The minimums and recommended specifications will vary with each component, but suffice it to say that you can never have too much RAM or computing power. For example, on a machine running the Oracle database, the FTK user interface, and the primary processing engine,

AccessData recommends the requirements shown in Tabl

Table

	Minimum	Recommended
Processor	Intel® i7 or AMD equivalent	Intel® i9 Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
RAM	12GB (DDR3) 8GB (DDR2)	12GB (DDR3) 8GB (DDR2)
Operating System	Vista, 2008, Windows 7 (64 bit)	Vista, 2008, Windows 7 (64 bit)

Helix :

Helix is a Ubuntu live CD customized for computer forensics. Helix has been designed very carefully to *not* touch the host computer in any way and it is forensically sound. Helix will not auto mount swap space, or auto mount any attached devices. Helix also has a special Windows autorun side for Incident Response and Forensics. Downloading of the live CD is only provided as a complement to membership in the e-fense members-only forum. An unsupported, older, no-cost version is available as well.

Autopsy

Autopsy is the graphical user interface (GUI) used in The Sleuth Kit to make it simpler to operate, automating many of the procedures, and so easier to identify, sort and catalogue pertinent pieces of forensic data. As the name implies, The Sleuth Kit—a collection of command lines and a C library—allows users to collect, parse and analyse forensic data on computer systems and mobile phones. The website claims that the system can even recover photos from your camera.[1] Layering a GUI over text-based and command line interfaces might not appeal to purists who love their simplicity, but Autopsy allows an ease of use those who grew up with GUI interfaces will appreciate

1.Easy to Use

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the intuitive page for more details.

2.Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.

- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Indicators of Compromise - Scan a computer using STIX.

3. Fast

Everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder. See the fast results page for more details.

4.Cost Effective

Autopsy is free. As budgets are decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis, that other commercial tools do not provide.