

ITDO6014

ETHICAL HACKING AND FORENSICS

Module 4: Report Generation

Forensic Report

2

- ❑ Forensic science refers to the use of scientific methods or the application of science to help the court of law in solving crimes.
- ❑ These scientific techniques are applied by experts like forensic experts, forensic scientists, criminal investigators, etc. in collecting evidence that might be useful in the case.
- ❑ Basically, forensics is the application of science to investigations more particularly criminal investigations. The result of these forensic-related investigations is detailed in a forensic report.
- ❑ These reports are often used for several purposes, including billing, affidavits, and as proof of what was found or not found. These reports are very important to a case.

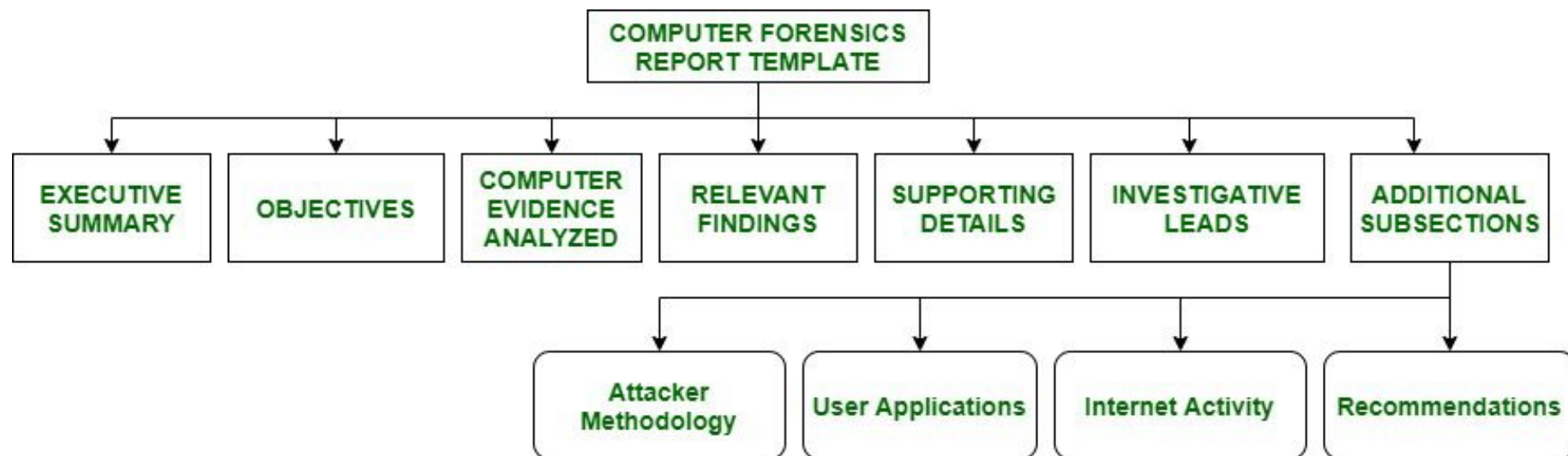
Forensic Report

3

- Basic components of a forensic report include articulating a referral question, and sources of information, presenting relevant data and then giving an expert opinion without being biased, grammatically correct text, and avoiding jargon, opinions, and data should be linked or related.
- A forensic report is usually related to or about the subject and not for the subject. This forensic report proves useful in court proceedings and can also influence the decision of the court.

Purpose of Forensic Report

4



Forensic Report Format

5

- **Executive Summary :**

Executive Summary section of computer forensics report template provides background data of conditions that needs a requirement for investigation. Executive Summary or the Translation Summary is read by Senior Management as they do not read detailed report. This section must contain short description, details and important pointers.

Forensic Report Format

6

- This section could be one page long. Executive Summary Section consists of following :
 - Taking account of who authorized the forensic examination.
 - List of the significant evidences in a short detail.
 - Explaining why a forensic examination of computing device was necessary.
 - Including a signature block for the examiners who performed the work.
 - Full, legitimate and proper name of all people who are related or involved in case, Job Titles, dates of initial contacts or communications.

Forensic Report Format

7

■ Objectives :

Objectives section is used to outline all tasks that an investigation has planned to complete. In some cases, it might happen that forensics examination may not do a full fledged investigation when reviewing contents of media. The prepared plan list must be discussed and approved by legal council, decision makers and client before any forensic analysis. This list should consist tasks undertaken and method undertaken by an examiner for each task and status of each task at the end of report.

Forensic Report Format

8

- **Computer Evidence Analyzed :**

The Computer Evidence Analyzed section is where all gathered evidences and its interpretations are introduced. It provides detailed information regarding assignment of evidence's tag numbers, description of evidence and media serial numbers.

Forensic Report Format

9

■ **Relevant Findings :**

This section of Relevant Findings gives summary of evidences found of **probative Value** When a match is found between forensic science material recovered from a crime scene e.g., a fingerprint, a strand of hair, a shoe print, etc. and a reference sample provided by a suspect of case, match is widely considered as strong evidence that suspect is source of recovered material. However, probative value of evidence can vary widely depending on way in which evidence is characterized and hypothesis of its interest. It answers questions such as “What related objects or items were found during investigation of case ?”.

Forensic Report Format

10

■ **Supporting Details :**

Supporting Details is section where in-depth analysis of relevant findings is done. ‘How we found conclusions outlined in Relevant Findings?’, is outlined by this section. It contains table of vital files with a full path name, results of string searches, Emails/URLs reviewed, number of files reviewed and any other relevant data. All tasks undertaken to meet objectives is outlined by this section. In Supporting Details we focus more on technical depth. It includes charts, tables and illustrations as it conveys much more than written texts. To meet outlined objectives, many subsections are also included. This section is longest section. It starts with giving background details of media analyzed. It is not easy to report number of files reviewed and size of hard drive in a human understandable language. Therefore, your client must know how much data you wanted to review to arrive at a conclusion.

Forensic Report Format

11

□ **Investigative Leads :**

Investigative Leads performs action items that could help to discover additional information related to the investigation of case. The investigators perform all outstanding tasks to find extra information if more time is left. Investigative Lead section is very critical to law enforcement. This section suggests extra tasks that discovers information needed to move on case. e.g. finding out if there are any firewall logs that date any far enough into past to give a correct picture of any attacks that might have taken place. This section is important for a hired forensic consultant.

Forensic Report Format

12

▣ **Additional Subsections :**

Various additional subsections are included in a forensic report. These subsections are dependent on clients want and their need. The following subsections are useful in specific cases : **Attacker**

Methodology –

Additional briefing to help reader understand general or exact attacks performed is given in this section of attacker methodology. This section is useful in computer intrusion cases. Inspection of how attacks are done and what bits and pieces of attacks look like in standard logs is done here.

Forensic Report Format

13

▣ **User Applications –**

In this section we discuss relevant applications that are installed on media analyzed because it is observed that in many cases applications present on system are very relevant. Give a title to this section, if you are investigating any system that is used by an attacker .e.g Cyber Attack Tools.

Forensic Report Format

14

▣ **Internet Activity –**

Internet Activity or Web Browsing History section gives web surfing history of user of media analyzed. The browsing history is also useful to suggest intent, downloading of malicious tools, unallocated space, online researches, downloading of secure deleted programs or evidence removal type programs that wipe files slack and temporary files that often harbor evidence very important to an investigation.

Forensic Report Format

15

▣ **Recommendations –**

This section gives recommendation to posture client to be more prepared and trained for next computer security incident. We investigate some host-based, network-based and procedural countermeasures are given to clients to reduce or eliminate risk of incident security.

Forensic Report Format

16

- There really isn't a de-facto standard or format per-se. Formatting and layout options are up to the examiner/analyst, or they may be defined by organizational policies or jurisdictional court rules. The report may include something similar or a slightly different flavor to the following:
- Title Page
- Table of Contents
- Overview/Case/Executive Summary
- Evidence
- Objectives
- Forensic Analysis (Steps Taken)
- Relevant Findings
- Conclusion
- Exhibit

Do's and Don'ts

17

- Do determine the structure of your report beforehand according to your case.
- Do answer the referral question clearly.
- Don't use too technical language, flowery language, and lengthy wordy sentences.
- Do write the report keeping in mind the targeted audience.
- Do avoid grammatical errors and jargon.
- Don't put needless information in the report. Try to answer the referral question only.
- Do consider the length of the report by asking the party for guidance.
- Do report relevant sources in the report and include all the data related to the referral question.
- The test conducted should be comprehensible by the court and the test should be valid and reliable.
- Don't rely on only one source of data.