ITDO6014
ETHICAL HACKING AND FORENSICS

Module 6: Report Generation

Forensic Report

- 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

- 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.

Goals of Forensic Report

- **Documentation of Evidence**: A forensic report aims to document all relevant evidence collected during the investigation. This includes physical evidence, digital artifacts, witness statements, and any other pertinent information.
- **Analysis and Interpretation**: The report should provide an analysis of the evidence collected, including any examinations, tests, or analyses conducted. It should interpret the findings in the context of the case and relevant forensic methodologies.

Goals of Forensic Report

- **Clarity and Precision**: Forensic reports need to be clear, concise, and written in a language that is easily understood by non-technical stakeholders such as lawyers, judges, or jurors. Precision in language and terminology is crucial to avoid ambiguity.
- **Objectivity and Impartiality**: It is essential for forensic reports to maintain objectivity and impartiality. They should present findings without bias or prejudice, allowing the reader to form their own conclusions based on the evidence presented.

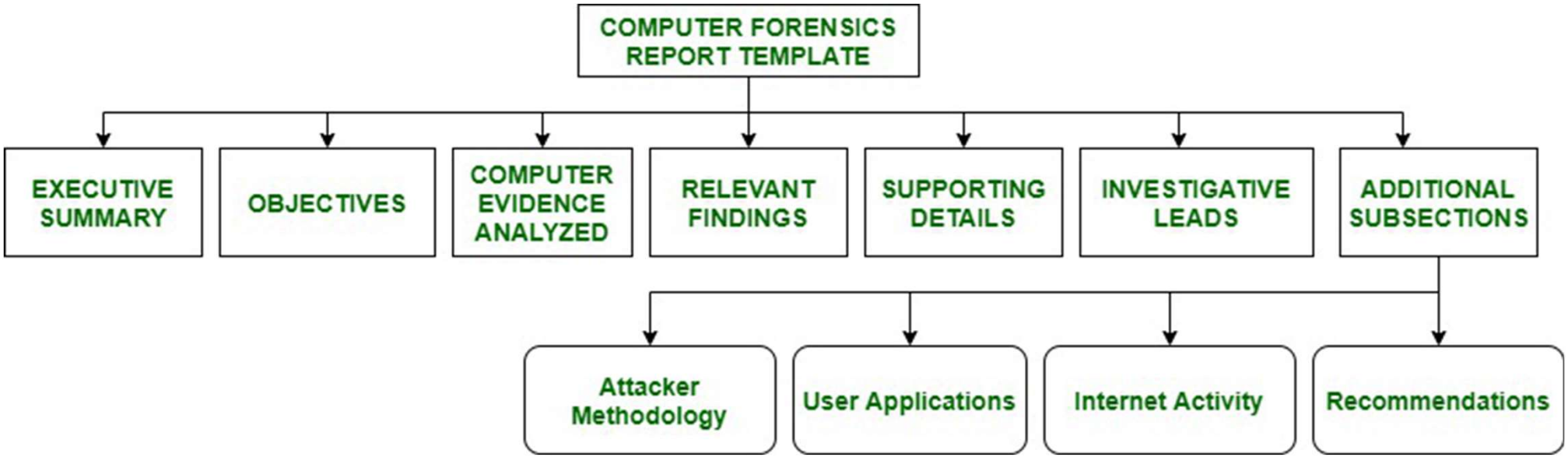
Goals of Forensic Report

- **Compliance and Standards**: Depending on the jurisdiction and the nature of the investigation, forensic reports may need to adhere to specific legal standards, regulations, or professional guidelines. Compliance with these standards ensures the admissibility and reliability of the report in legal proceedings.
- **Support for Legal Proceedings**: Forensic reports often serve as crucial pieces of evidence in legal proceedings, providing support for prosecutors, defense attorneys, or other parties involved in the case. The report should be structured and formatted in a way that facilitates its use in court.

Goals of Forensic Report

- **Transparency and Accountability**: Transparency in the methodology used and the rationale behind conclusions is vital for maintaining the credibility of the forensic report. It should clearly outline the steps taken during the investigation and justify the conclusions reached.
- **Risk Mitigation**: In cases where the forensic analysis involves potential risks or uncertainties, the report should communicate these effectively. It is important to identify limitations, assumptions, and uncertainties associated with the findings to avoid misinterpretation or misunderstanding.

Layout of Forensic Report



Forensic Report Format

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- **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

- 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

- Do determine the structure of your report beforehand according to your case.
- Do answer the referral question clearly.
- Don’t use too technical language, jargon words, and lengthy wordy sentences.
- Do write the report keeping in mind the targeted audience.
- Do avoid grammatical errors.
- Don’t put needless information in the report.
- 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.

Sample Report

- Consider a scenario of a forensic investigation involving a digital security breach at a company called TechSecure Inc.
- (Refer PDF Report)