

Prepared by Dr. Nermin Ewais

CYB 770
IT Forensics

Lecture 10



The Report

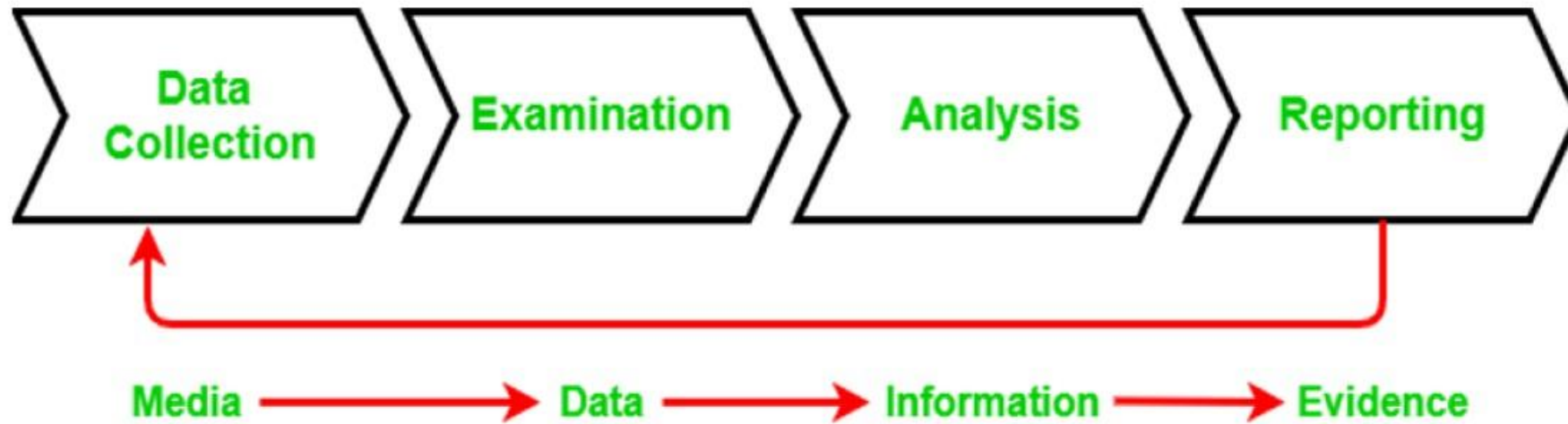
Lecture 10

CYB 770
IT Forensics

Prepared by
Dr. Nermin Ewais

- Investigative Reports
- Report Preparation
- Digital Forensic Report Format
- Report Classification
- Witness
- Example Cases

- Investigative reports are the records of actions performed during the investigation process starting from obtaining the first incident report till the derived conclusions.
- The report should provide every minute detail of the performed actions, reasons behind the actions , and the results.
- As a result, the non-technical people involved in the case can easily understand the case detail.



Data Collection: This is where chain of custody process is initiated. It involves identification, labeling, recording, and the acquisition of data from all the possible relevant sources that preserve the integrity of the data and evidence collected.

Examination: During this process, the chain of custody information is documented outlining the forensic process undertaken. It is important to capture screenshots throughout the process to show the tasks that are completed and the evidence uncovered.

Analysis: This stage is the result of the examination stage. In the Analysis stage, legally justifiable methods and techniques are used to derive useful information to address questions posed in the particular case.

Reporting:

This is the documentation phase of the Examination and Analysis stage. Reporting includes the following:

- Statement regarding Chain of Custody.
- Explanation of the various tools used.
- A description of the analysis of various data sources.
- Issues identified.
- Vulnerabilities identified.
- Recommendation for additional forensics measures that can be taken.

Report Preparation

- One of the forensic analyst's primary functions is the dissemination of the forensic process to the intended audience.
- To do their jobs successfully. They must write forensic reports that are both **technically accurate and easy to read**.
- A great investigation can be rendered largely ineffective if the resulting report is poor .
- If the report is disorganized and poorly written may actually hinder their case.

- Forensic information has limited value if it is not collected and reported in a usable form and presented to those who need to apply the information. The standard way to document
- Why the computer system was reviewed ?
- How the computer data was reviewed?
- What conclusions were arrived at?

The computer forensic report should achieve the following goals :

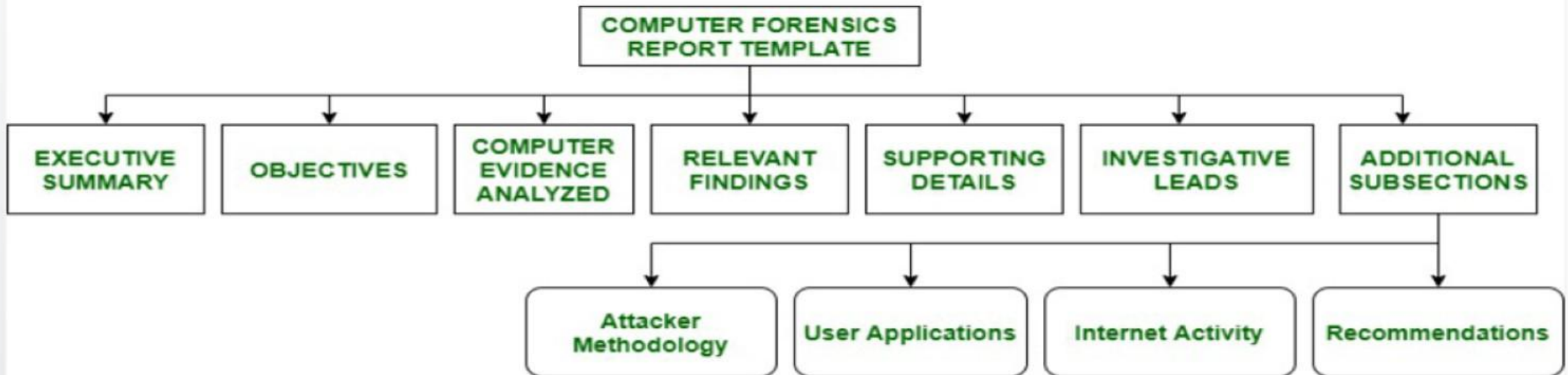
- Accurately describe the details of an incident
- Be understandable to decision-makers
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain your conclusions
- Offer valid conclusions options or recommendations when needed
- Be created in a timely manner

Most forensic report follow the general guideline below for a table of contents:

1. Brief summary of information
2. Tools used in investigation process including their purpose and any underlying assumptions associated with the tool
3. Repository (For example A's work computer)
 - A. Summary of evidence found on Employee A's work computer
 - B. Analysis of relevant portions of Employee A's work computer
 - Email history
 - Internet search history
 - USB registry analysis

- C. Repetition of above steps for other evidence items (which may include other computers and mobile devices, etc.)
- 4. Recommendations and next steps for counsel to continue or cease investigation based on the findings in the reports.

Digital Forensic Report Format



1. Executive Summary
2. Investigation Objectives
3. Computer Evidence Analyzed
4. Relevant Findings
5. Supporting Details
6. Investigative Leads
7. Additional Subsections

1. Executive Summary Section consists of following :

1. Case Number
2. Names and social Security number of the authors, investigators, and examiners
3. Purpose of investigation : Explaining why a forensic examination of computing device was necessary.
4. Full, legitimate and proper name of all people who are related or involved in case, Job Titles, dates of initial contacts or communications.

5. Significant finding: List of the significant evidences in a short detail.
6. Significant analysis : Including a signature block for the examiners who performed the work.

2. Investigation Objectives

1. The Objectives is used to outline all tasks that an investigation has planned to complete.
2. The prepared plan list must be discussed and approved by legal council, decision makers and client before any forensic analysis.
3. Write in the end the used Tools.

3. The Computer/IT 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. (List of the collected evidences)
-)

- Tools involved in the collected the evidence
- Preservation of the evidence
- Date and time investigation was assigned
- Location of the evidence

- Allocated investigator
- Natural of claim and information provided to the investigators

4- Relevant Findings

- This section gives summary of evidences found of probative Value e.g., a fingerprint, a strand of hair, a shoe print, etc.
- It answers questions such as “What related objects or items were found during investigation of case ?”.

5- Supporting Details

- where in-depth analysis of relevant findings is done.
- ‘How we found conclusions outlined in Relevant Findings?’, .
- 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.

- 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.

6- Investigative Leads

- Investigative Leads performs action items that could help to discover additional information related to the investigation of case.
- 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.

7- Additional Subsections

- Various additional subsections are included in a forensic report.
- Attacker Methodology
- User Applications
- Internet Activity
- Recommendations

Report Classification

- **Reports can be categorized as the following:**
 - Verbal
 - Written
- **These categories are further divided into the following:**
 - Formal
 - Informal

- Structured report delivered in person to a board of directors or managers or to a jury.

- A report that is less structured than a formal report and is delivered in person, usually in an attorney's office.

- A document that contains sensitive information that could create an advantage for the opposing attorney

As you write your report, keep the following guidelines in mind:

- Don't make any assumptions.
- Don't identify leads.
- Check your spelling before the report leaves your office; don't wait for a supervisor or the attorney to proofread your report.
- Double-check the media that you have stored findings to.
- If you create a findings CD, make sure the data is on it before you send it out.

Witness

Witness

- Expert witness
- Technical witness

- An expert witness is a person with specialized skill sets whose opinion may help a jury make sense of the factual evidence of a case.
- Offers opinions based on observation
- Works for attorney.

To be expert witness, you may testify to an opinion, or conclusion, if basic conditions are met:

- The opinion, inferences, or conclusions, depend on special knowledge, skill, or training not within the ordinary experience of lay jurors.
- The witness must be shown to be qualified as a true expert in the particular field of expertise.
- Expert witness's must first describe the data on what the opinion, inference, or conclusion, is based or, in the alternative, he or she must testify in response to a hypothetical question that sets forth the underlying evidence.

- Does the actual fieldwork
- Submit the result of his finding
- Identify the "processes and procedures" of obtaining the evidence and, if needs be, explain how the "thing" works, so to speak.
- Expert opinion is to provide an "explanation" or "possible conclusions" that might be drawn from the evaluation of the evidence overall.
- Prepare testimony شهادة

Example Cases

Background

- A local bank fired their IT manager after several of the bank's tellers filed sexual harassment complaints against him.
- When the bank executives arrived at work the morning after his termination, they found their computer networks inoperable and their servers erased.
- The IT manager was immediately suspected, but surveillance cameras showed no sign of his entry into the building after he was let go.
- The bank wanted to find out what happened, so they contacted their attorneys and hired forensics experts to collect images of the servers and the IT manager's computer.

Investigation

- A forensics investigator made forensic images of the manager's workstation at the bank, as well as the server computers.
- When the imaging process was complete, the forensic copies were brought back to the laboratory for investigation.
- Once all of the evidence was collected, the bank hired a local IT firm to begin repair of the network and computer problems. Since no one was physically present at the time of the destruction, the forensics examiners searched for evidence of a remote connection to the bank's servers.
- The examiner also took note of the specific times the files were deleted.

- The examiner found that the user “administrator” had logged into the server approximately one hour after the IT manager left the bank, and the connection had originated from a web address that was eventually traced to the general location of his house.
- The former IT manager was one of two people with knowledge of the “administrator” password. Further expert investigation revealed that the method used to delete files suggested it was someone with knowledge of the server’s file structure and location.

Outcome

- Taken together, each of these pieces of information was used to build a case that the former manager had remotely logged in to the bank's computers and maliciously deleted key business data.
- These results were reported to the bank and their attorneys, who brought formal charges against the former IT manager.

Background

- Six months after firing their lead project manager, a local construction company heard rumors that their former employee was soliciting their two best clients for his new consulting company.
- The replacement project manager also discovered that several proprietary building plans for their most popular model homes were missing from the former manager's desktop computer.

Investigation

- The construction company's attorneys ordered an investigation of the project manager's computer.
- A forensic specialist was dispatched to the construction company's corporate headquarters to make a forensics image of the computer hard drive.
- Once back at the laboratory, an examination was performed on the forensics image based on a list of keywords provided by the construction company provided.
- The forensics examiners were directed to investigate the edit history and metadata for all of the files in the "My Documents" and "Corporate Documents" folders. Furthermore, the investigators were asked to look for evidence that any of those files had been copied to CD, thumb drive or any other external media.

- The forensics examiners discovered that the former manager had indeed taken proprietary information from the company and had a pattern of misusing company time.
- The most recent edits to the company's client list showed that the document was copied to a thumb drive four hours before he was fired: his user profile was logged into the computer during the transfer time. He also deleted all of the documents in the "My Documents" folder and removed them from the recycle bin approximately one hour before leaving the company.
- On several other occasions during the last month of his employment, he copied the proprietary specifications for the newest model home onto a CD. Moreover, the investigators discovered that he spent three to five hours every day on the Internet shopping for handguns, ATV accessories and construction job opportunities.

Outcome

- All this information was compiled into a report and all the relevant documents were produced to the construction company's attorneys.
- The former project manager was charged with theft of proprietary information and was ordered to cease all communications with the company's clients and return the stolen information.

<https://ufediscoveryconference.com/wp-content/uploads/2016/03/Avansic-Digital-Forensics-Case-Studies.pdf>

Case study

- A new start-up SME (small-medium enterprise) based in Luton with an E-government model has recently begun to notice anomalies in its accounting and product records.
- It has undertaken an initial check of system log files, and there are a number of suspicious entries and IP addresses with a large amount of data being sent outside the company firewall.
- They have also recently received a number of customer complaints saying that there is often a strange message displayed during order processing, and they are often re-directed to a payment page that does not look legitimate.

Case study

- The company makes use of a general purpose eBusiness package and has a small team of six IT support professionals, but they do not feel that they have the expertise to carry out a full scale malware/forensic investigation.
- The task is to investigate the team's suspicions and to suggest to the team how they may be able to disinfect any machines affected with malware, and to ensure that no other machines in their premises or across the network have been infected. The team also wants you to carry out a digital forensics investigation to see whether you can trace the cause of the problems, and if necessary, to prepare a case against the perpetrators.

Case study

Data collection

- The forensic workstation must be located in same LAN where the target machine, in this case the Windows NT Server, is located.
- 'Cryptcat' tools can be used in the forensic workstation to listen to the port of the Windows NT server.
- Volatile data
- Non-Volatile data

```
cryptocat -l -p 6543 -k key >> <file name>
```



Figure 2: Volatile data collection setup

Source: Reino, A., (2012)

The following table shows the Graphic User Interface tools, and their usage and outcome can be used in the computer forensic investigation.

Tools	Usage	Outcome
Rootkit Revealer	Detects user mode and Kernel mode root kits	System date and time, Stored in information in memory
Process Explorer	Useful information about running process, loaded libraries, used resources, etc.,	Running Process, logged on users
Tcpview	Displays network connection and associated application	Network Connection, Open ports,

Table 1: Volatile Data Forensic Tools and their usage and outcome

Examination

- Once we have gathered all the available evidences, we need to conduct the examination by the help of various computer forensic investigation tools. We also examine the file system, Windows registry, Network and Database forensic examination, as follows:
- Files system examination
- Windows registry examination
- Network forensics examination
- Database forensics examination

Analysis

- Initially we need to analyze the evidences which we gathered and examined.
- Malware analysis

Reporting

- A forensic report highlights the evidences in the court and it also helps for gathering more evidences and can be used in court hearings.
- A computer forensic investigator must be aware of the type of computer forensic reporting such as formal report, written report and verbal report.
- A formal report contains the facts from the investigation findings.
- A written report is like a declaration or an affidavit which can be sworn to under oath so that it must be clear, precise and detailed.
- A verbal report is less structured and is a preliminary report that addresses the areas of investigation not covered yet.

<https://resources.infosecinstitute.com/topic/computer-forensics-investigation-case-study/>

- **Internet of Things (IoT) Forensics**
- There are mainly three IoT components that need to be secured to provide a safe, interactive environment between devices
- These components are:
 - IoT devices,
 - IoT networks,
 - and cloud infrastructures.

- **Internet of Things (IoT) Forensics**
- The implementation of the IoT has undergone considerable changes in the field of investigation
- **Data Location.** Most IoT data distributed over various locations are beyond the control of the user.
- **Device Type.** Investigators are required to determine and collect evidence from a remote crime scene during the identification process of forensics.

- **Data Format.** The data produced by IoT devices have a different format from that of data stored in the cloud.
- **Data Loss.** It is easy and possible to overwrite the data of IoT devices because of the short lifespan of IoT data and the limitation of the device storage.
- **Cloud Service Requirements.** The cloud service provider does not request accurate information from users when signing up for their services
- **Forensic Tool Limitations** The current tools in the field of digital forensics are not compatible with the IoT environment

- **Artificial Intelligence and ML in Forensics**
- **Identification :: NLP**
- **Analysis : metadata for videos**

- Asia ALJAHDALI, Hanan ALDISSI, Shoroq BANAFEE, Sundos SOBAHI, Wafaa NAGRO, "**IoT Forensic models analysis**", *Romanian Journal of Information Technology and Automatic Control*, ISSN 1220-1758, vol. 31(2), pp. 21-34, 2021



Thank You