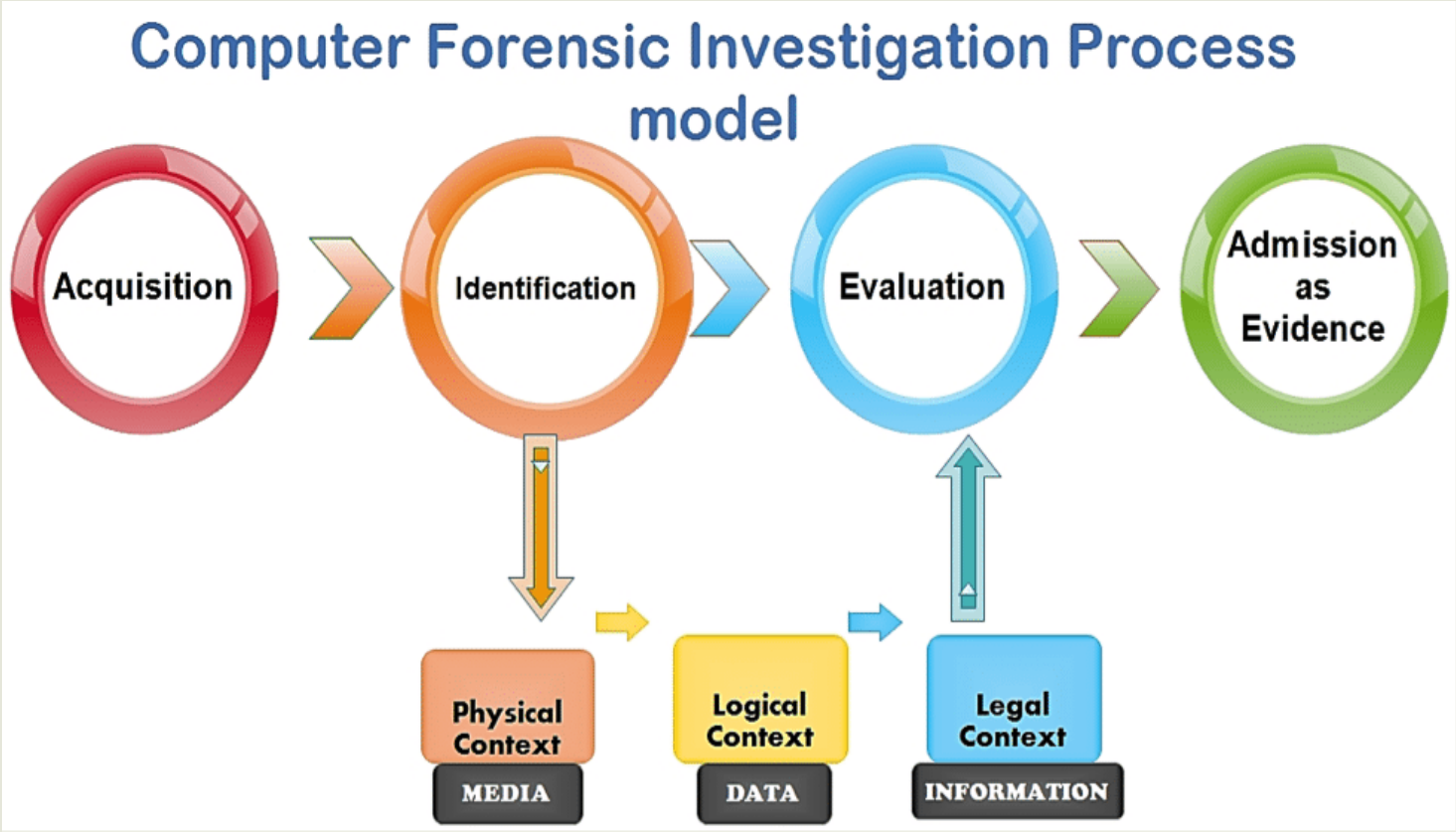
Cyber Forensic and IR

Subject Faculty – Ms. Hepi Suthar
Lecture - 4

Forensic Investigation Process

- Preservation
- Acquisition
- Analysis
- Discovery
- Documentation
- Presentation of Evidence
- Litigation



Forensic Investigation Process – Preservation

- Handling of **evidence** is the most important aspect in **digital forensics**.
- It is imperative that nothing be done that may alter **digital evidence**. This is known as **preservation**.
- The isolation and protection of **digital evidence** exactly as found without alteration so that it can later be analysed.

Forensic Investigation Process – Preservation

- – As a general rule, make sure you **do not turn ON a device if it is turned OFF**. For computers, make sure you **do not change** the current status of the device at all. If the device is OFF, it must be kept OFF. If the device is ON, call a forensics expert before turning it off or doing anything.
- – **If it is not charged, do not charge it**; for mobile phones, if the device is ON, power it down to prevent remote wiping or data from being overwritten.
- – Ensure that you **do not leave the device in an open area or other unsecured space**. Document where the device is, who has access, and when it is moved.
- – **Do not plug anything to the device**, such as memory cards, USB thumb drives, or any other storage media that you have, as the data could be easily lost.
- – **Do not open any applications, files, or pictures** on the device. You could accidentally lose data or overwrite it.
- – **Do not copy anything to or from the device**.
- **– Preserve any and all digital evidence** that you think could be useful for your case.
- **– Take a picture of the piece of evidence** (front, back, etc.) to prove its condition.
- – **Make sure you know the PIN/Password pattern of the device**.
- – Last but not least, **do not trust anybody without forensics training** to investigate or view files on the original device. They might cause the deletion of data or the corruption of important information.

Forensic Investigation Process – Acquisition

- The first digital **forensic process** model proposed contains four steps: **Acquisition**, Identification, Evaluation and Admission.
- Since then, numerous **process** models have been proposed to explain the steps of identifying, acquiring, analysing, storage, and reporting on the evidence obtained from various digital devices.

Forensic Investigation Process – Analysis

- **Forensic** digital **analysis** is the in-depth **analysis** and **examination** of electronically stored information (ESI), with the purpose of identifying information that may support or contest matters in a civil or criminal **investigation** and/or court proceeding.

Forensic Investigation Process – Documentation

- **Documentation** is a continuous **process** throughout the **investigation process**. It is important to precisely record location and status of computers, storage media, other electronic devices, and traditional evidence, although there are overlaps and similarities in the digital and physical **forensic investigation**.

Forensic Investigation Process – Presentation of evidence

- Forensic cases often present unique scenarios that require a customized process that utilizes all possible best practices. The presentation of digital analysis includes a formal written report on the identification of relevant information.
- Ultimately, the report and relevant information will be viewed by human resources, executives, law enforcement, lawyers, judges and juries. As such, the report should be clear and concise, yet still contain sufficient detail to describe a repeatable and defensible process.
- The information must be provided in an organized and easily accessible format. Depending on the ultimate use of the information, there may be the need to provide the same data in different formats.
- The most important overriding principle for a forensic report is that it is based on objective findings. It is acceptable to give opinions or examples when necessary. Any conjecture, however, should be clearly identified as such.
- As with any written document, the digital forensic report must be drafted for the intended reader/audience. Since it will be intended for multiple audiences, it is important to divide the report into sections that appeal to each. Audiences may include individuals, businesses, clients, legal counsel, opposing counsel, forensic experts, judges and/or juries.

Any Question ???

Thank You