CYBER ENRICH TRAINING PROGRAM | MODULE II

Digital Forensics Standards

ISO/IEC 27037:2012

ISO/IEC 27037:2012 provides guidance on identifying, gathering, collecting, acquiring, handling and protecting, preserving digital forensic evidence, that is, "digital data that may be of evidential value" for use in court.

ISO/IEC 27037:2012

- It provides guidelines for specific activities in the **handling of digital evidence**, which are **identification, collection, acquisition and preservation** of potential digital evidence that can be of evidential value.

- It provides **guidance** to individuals with respect to common situations encountered throughout the digital evidence **handling process** and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

ISO/IEC 27037:2012

ISO/IEC 27037:2012 gives guidance for the following devices and circumstances:

- ✓ Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,
- ✓ Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,
- ✓ Mobile navigation systems,
- ✓ Digital still and video cameras (including CCTV),
- ✓ Standard computer with network connections,
- ✓ Networks based on TCP/IP and other digital protocols, and
- ✓ Devices with similar functions as above.

Scope & Purpose

- The standard provides detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of **electronic evidence**, particularly to maintain its **integrity**.
- It defines and describes the **processes** through which evidence is recognized and identified, **documentation** of the crime scene, collection and preservation of the evidence, and the **packaging** and **transportation** of evidence.
- The scope covers 'traditional' IT systems and media rather than vehicle systems, cloud computing etc. The guidance is **aimed primarily at first responders**.

Points to Note

- Every country has its own unique legislative system. A crime committed in one jurisdiction may not even be regarded as a crime in another. The challenge is to **harmonize processes across borders** such that cybercriminals can be prosecuted accordingly.
- Therefore, a means to allow and facilitate the exchange and use of reliable evidence is required.
- "Digital evidence", meaning information from digital devices to be presented in court, is interpreted differently in different jurisdictions.
- For the widest applicability, the standard will **avoid using jurisdiction-specific terminology**. It will not cover analysis of digital evidence, nor its admissibility, weight, relevance etc. It also will not mandate the use of particular tools or methods.