ESTABLISHING DIGITAL FORENSICS LABS – INDIA & USA (STANDARDS)

The computer is a reliable witness that cannot lie. Digital evidence contains an unfiltered account of a suspect's activity, recorded in his or her direct words and actions. But some people say that using digital information as evidence is a bad idea. If it's easy to change computer data, how can it be used as reliable evidence?

To identify all the hidden details that are left after or during an incident, the computer forensics is used. The purpose of computer forensics techniques is to search, preserve and analyze information on computer systems to find potential evidence for a trial.

Computers are getting more powerful day by day, so the field of computer forensics must rapidly evolve. Previously, we had many computer forensic tools that were used to apply forensic techniques to the computer.

1. **SANS SIFT**
2. **ProDiscover Forensic**
3. **Volatility Framework**
4. **The Sleuth Kit (+Autopsy)**
5. **CAINE**
6. **Xplico**
7. **X-Ways Forensics**

SANS SIFT

The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu-based Live CD which includes all the tools you need to conduct an in-depth forensic or incident response investigation. The free SIFT toolkit that can match any modern incident response and forensic tool suite is also featured in SANS' Advanced Incident Response course (FOR 508). It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

PRODISCOVER FORENSIC

ProDiscover Forensic is a powerful computer security tool that enables computer professionals to locate all of the data on a computer disk and at the same time protect evidence and create quality evidentiary reports for use in legal proceedings.

It can recover deleted files, examine slack space, access Windows Alternate Data Streams, and dynamically allows a preview, search, and image-capture of the Hardware Protected Area (HPA) of the disk utilizing its own pioneered the

technology. It is not possible to hide data from a ProDiscover Forensic because it reads the disk at the sector level.

VOLATILITY FRAMEWORK

The Volatility Framework was released publicly at the BlackHat and based on years of published academic research into advanced memory analysis and forensics. Volatility framework introduced people to the power of analyzing the runtime state of a system using the data found in volatile storage (RAM). It also provided a cross-platform, modular, and extensible platform to encourage further work in this exciting area of research.

THE SLUETH KIT (+AUTOPSY)

The Sleuth Kit is a collection of command line tools that allows us to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

The core functionality of The Sleuth Kit (TSK) allows you to analyze volume and file system data. The plug-in framework allows you to incorporate additional modules to analyze file contents and build automated systems.

CAINE

CAINE (Computer Aided Investigative Environment) is a Linux Live CD that contains a wealth of digital forensic tools. The latest version of Caine is based on the Ubuntu Linux LTS, MATE, and LightDM. Compared to its original version, the current version has been modified to meet the standard forensic reliability and safety standards.

XPLICO

Xplico is a network forensics analysis tool, which is software that reconstructs the contents of acquisitions performed with a packet sniffer (e.g. Wireshark, tcpdump, Netsniff-ng). Xplico is able to extract and reconstruct all the Web pages and contents (images, files, cookies, and so on).

X-WAYS FORENSICS

X-Ways Forensics is an advanced work environment for computer forensic examiners. X-Ways Forensics is efficient to use, not a resource-hungry, often runs faster, finds deleted files and offers many features that the others lack. X-Ways Forensics is fully portable, runs off a USB stick on any given Windows system without installation.

The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) was a Missouri-based not-for-profit that "offers voluntary accreditation to public and private crime laboratories" around the world. Laboratories wishing to become accredited had go through a proficiency testing program as part of the accreditation process.

The main objectives of the ASCLD/LAB were

- **To improve the quality of laboratory services provided to the criminal justice system.**
- **To adopt, develop and maintain criteria which may be used by a laboratory to assess its level of performance and to strengthen its operation.**
- **To provide an independent, impartial, and objective system by which laboratories can benefit from a total operational review.**
- **To offer to the general public and to users of laboratory services a means of identifying those laboratories which have demonstrated that they meet established standards.**

The ASCLD/LAB was acquired by and merged into the ANSI-ASQ NATIONAL ACCREDITATION BOARD (ANAB) in April 2016.

Cyber law is any law that applies to the internet and internet-related technologies. Cyber law is one of the newest areas of the legal system. This is because internet technology develops at such a rapid pace. Cyber law provides legal protections to people using the internet. This includes both businesses and everyday citizens. Understanding cyber law is of the utmost importance to anyone who uses the internet. Cyber Law has also been referred to as the "law of the internet."

Areas that are related to cyber law include cyber crime and cyber security. With the right cyber security, businesses and people can protect themselves from cybercrime. Cyber security looks to address weaknesses in computers and networks. The International Cyber Security Standard is known as ISO 27001.

Cybersecurity policy is focused on providing guidance to anyone that might be vulnerable to cybercrime. This includes businesses, individuals,

and even the government. Many countries are looking for ways to promote cybersecurity and prevent cybercrime. For instance, the Indian government passed the Information Technology Act in 2000. The main goal of this law is to improve transmission of data over the internet while keeping it safe.

Information is another important way to improve cybersecurity. Businesses, for example, can improve cybersecurity by implementing the following practices:

- **Offering training programs to employees.**
- **Hiring employees who are certified in cybersecurity.**
- **Being aware of new security threats.**

Cybercrimes can be committed against governments, property, and people.

Most of these types of cybercrimes have been addressed by the IT ACT of 2000 and the IPC. Cybercrimes under the IT ACT include:

- **Sec. 65, Tampering with Computer Source Documents.**
- **Sec. 66, Hacking Computer Systems and Data Alteration.**
- **Sec. 67, Publishing Obscene Information.**
- **Sec. 70, Unauthorized Access of Protected Systems.**
- **Sec. 72, Breach of Confidentiality and Privacy.**
- **Sec. 73, Publishing False Digital Signature Certificates.**

Special Laws and Cybercrimes under the IPC include:

- **Sending Threating Messages by Email, Indian Penal Code (IPC) Sec. 503.**

- **Sending Defamatory Messages by Email, Indian Penal Code (IPC) Sec. 499**
- **Forgery of Electronic Records, Indian Penal Code (IPC) Sec. 463**
- **Bogus Websites & Cyber Fraud, Indian Penal Code (IPC) Sec. 420**
- **Email Spoofing, Indian Penal Code (IPC) Sec. 463**
- **Web-Jacking, Indian Penal Code (IPC) Sec. 383**
- **Email Abuse, Indian Penal Code (IPC) Sec. 500**