A Technical Executive Summary on

Establishing Digital Forensics Labs - India and USA(Standards)

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

Information technology law (also called "cyberlaw") concerns the law of information technology, including computing and the internet in the US. It is related to legal informatics and governs the digital dissemination of both (digitalized) information and software, information security, and electronic commerce. aspects and it has been described as "paper laws" for a "paperless environment".

A Computer Forensics Lab (CFL) is a designated location for conducting computer-based investigations on collected evidence. It is an efficient computer forensics platform that is able to investigate any cybercrime event. The objective of this lab is to provide expert knowledge about the tools used in computer forensics for:

- Recovering deleted files from a hard disk
- Gathering evidence
- Viewing files of various formats
- Locating files needed for a forensics investigation
- Performing image and file conversions
- Handling evidence data
- Creating a disk image file of a hard disk partition

For better research and investigation, developers have created many computer forensics tools. Police departments and investigation agencies select the tools based on various factors including budget and available experts on the team.

- Disk and data capture tools
- File viewers
- File analysis tools
- Registry analysis tools
- Internet analysis tools
- Email analysis tools
- Mobile devices analysis tools
- Mac OS analysis tools
- Network forensics tools

- Database forensics tools

Few important and popular data forensics tools are:

- Digital Forensics Framework
  https://github.com/arxsys/dff
- Open Computer Forensics Architecture
  http://sourceforge.net/projects/ocfa/
- CAINE
  http://www.caine-live.net/
- X-Ways Forensics
  http://www.x-ways.net/forensics/
- EnCase
  https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
- Registry Recon
  http://arsenalrecon.com/apps/recon/
- The Sleuth Kit
  http://www.sleuthkit.org/
- Llibforensics
  http://code.google.com/p/libforensics/
- Volatility
  http://code.google.com/p/volatility/
- WindowsSCOPE
  http://www.windowsscope.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=35&category_id=3&option=com_virtuemart
- The Coroner's Toolkit
  http://www.porcupine.org/forensics/tct.html
- Oxygen Forensic Suite
  http://www.oxygen-forensic.com/en/features
- Bulk Extractor
  http://digitalcorpora.org/downloads/bulk_extractor/
- Xplico
  http://www.xplico.org/about
- Mandiant RedLine
  https://www.mandiant.com/resources/download/redline
- Computer Online Forensic Evidence Extractor (COFEE)
  https://cofee.nw3c.org/
- P2 eXplorer
  https://www.paraben.com/p2-explorer.html

- PlainSight
  http://www.plainsight.info/index.html
- XRY
  http://www.msab.com/xry/what-is-xry
- HELIX3
  http://www.e-fense.com/h3-enterprise.php
- Cellebrite UFED
  http://www.cellebrite.com/Mobile-Forensics

Choosing a workstation configuration is an important step. The effectiveness of digital examiners depends on the way the workstation is configured. The nature of the cases in which digital evidence is involved is generally borderless and the offense happens in a split second; the findings derived from electronic evidence must, therefore, follow a standard set of guidelines to ensure that it is admissible not only in a specific country's court of law, but also in the international criminal justice system.