**ESTABLISHING DIGITAL FORENSIC LABS [US AND INDIA STANDARDS]**

All of us are very well aware about the fact that of the era being a digital era and so with the increase in advancement, an increment in the crime rate has also been observed. Computer forensics in the most -simplest terms could be explained as the branch of science involving computer and a computer; network related crime. The very first requirement is the establishment of a digital forensic lab includes, a RAM with at least 4 gigabyte so as for visualization, an octa or quad core CPU, onboard graphics, DVD/CD-RW , USB 1 and 2, dual monitor , printer and the network equipment.

Moving on the next step is the tool that are needed. The methodology of the tools used for examination are so classified on the type of analysis they exhibit, namely:

* **Disk and data capture tools** (examples- autopsy, Encrypted disk detector, wireshark etc., having the major focus on checking the physical drives and penetration testing etc. )
* **Mac OS analysis tools** (example- OnyX, Memtest86 etc. though lesser prone to windows ,machines but still prone to malware.
* **Registry analysis tools** (example-Encase forensics, FTK imager etc. basically stores the low level setting of windows OS in SAM)
* **Database forensic tools** (example- SQLite forensic browser; file system metadata often is used to navigate the propagation of event triggerance and further reconstruction of the timeline.
* **Network forensic tools** (example -Xplico, network miner, tcpdump etc. enables identification of the suspicious event triggering functions)
* **Mobile device analysis tools** (example- cellebrite touch, in-case forensics etc. enables the investigator to work with terminal and main mobile OS)
* **File analysis tools** (examples-SANS SIFT, the sleuth kit, CAINE, exiftool etc., includes the in-depth analysis and incident response investigation of an event)

Establishing a digital forensics lab, not only is a matter of the expertise of the investigator but also a nice toolkit to be his companion. All of us are very well known that Sherlock could never be a detective, without Dr. Watson! Here I have our digital forensic lab, including some of the most important tools so as to make system, either malware proof or protect the system against further damage and can also enable tracking the hacker.

1. **CELLEBRITE UFED**

The solution offers combined and unified workflow for all the levels so as to preserve, collect and enact as per the mobile data that has varied speed and accuracy as per the demand of the situation. Being user friendly, it enables speedy extraction of data from devices. A type of cellphone forensics tool enabling extraction and decoding of information of interest including, images, call logs, applications, calendar information, SMS messages and chats and call logs. With the help of Cellebrite premium, extraction of files from many recent androids, iOS could be done. Being an advanced logical extraction technique, it combines the logical and file system extraction where physical extraction cannot be implemented.

1. **HELIX3**

A live CD- based digital forensic suite on top of ubuntu that is usually created for incident response. Helix3 is user friendly and customizable as per the need which has easy integration. Helix3 is a multi-platform LIVE side, suitable for all; Mac OS X, Linux and windows. Having a bootable and a sound environment that can boot any x86 system. Helix3 Pro has the capability of automounting storage devices in both read/write mode.

The basic functioning procedure involves data collection from physical memory, network, scheduled jobs and the other stored information on the system, which are then analyzed and reviewed becoming the basis of report formulation. The link that can be used to download the live CD-based forensic suite is here! Go and grab your forensic tool! <https://e-fenseinc.sharefile.com/d/sda4309a624d48b88>

1. **XRY**

A digital and a mobile forensic tool that enables analyzation and retrieval of crucial information from various mobile devices. The components comprise of a hardware device connected to PC , extracting the data of interest using a software. The most significant advantage of XRY being the allowance for both logical and physical examination. Physical information is useful in the recovery of any deleted information from the source system. The data thus recovered from XRY is admissible in the court of law adding onto the forensic significance of the tool.

To gather more information, related to XRY! Open the link shown here: <http://www.msab.com/xry/what-is-xry>

1. **CAINE**

Computer aided investigative environment linux has built-in investigative tools adding on to its tight security. The only issue related to CAINE lies it’s technicality. Latest version of CAINE 6.0 dark matter is based on ubuntu 14.04.1 64-bit supporting Legacy/Bios/secure boot/UEFI. The procedure involved in investigation includes: seizure, acquisition, analyzation and report formation. GUI has a digital platform onto Sleuth kit , allowing recovery of images from a camera’s memory card.

CAINE menu has a subtotal of 18+ applications, involving identification of memory forensics, database, mobile forensics and network database. CAINE enables the user a safe and a secure computation environment in Linux, so as to enable further identification. To know more about the open-source tool, log: <http://www.caine-live.net/>

1. **THE SLEUTH KIT**

Autopsy being a digital tool having a GUI to sleuth kit based on unix and windows based tool system. The tool basically enables analyzation of disk images enabling an in-depth analysis of the file system, strengthening the stand while investigation.

1. **REGISTRY RECON**

A paid tool having a cost of $399, registry recon is a type of registry analysis tool. The tool enables registry representation based on the data extracted from the evidence or the source device.

1. **X-WAYS FORENSICS**

The security device, runs on all the Windows available versions. The features provided by X-ways forensics includes, disk imaging and cloning of cloud, RAM analysis, generating a automated registry report, authentication of data, binary data structure view and lots more! The basic idea lies between the sharing of data and it’s collaboration with the investigator increase efficiency.

The ones discussed above, includes some of the digital forensic tools permitted to be used by the criminal investigation agencies. With the increment in the use of digital media , cyber crimes are also increasing day-by-day and so it is the need of the hour, for not only the investigator but also the institutions involved so as to match up to the increasing technological advancements of the culprit.