CYBER FORENSIC CHALLENGES FOR LAW ENFORCEMENT

Computer Forensics

Computer forensics is considered to be the use of analytical and investigative techniques to identify, collect, examine, preserve and present evidence or information which is magnetically stored or encoded

A better definition for law enforcement would be the scientific method of examining and analyzing data from computer storage media so that the data can be used as evidence in court.

Media = computers, mobile phones, PDA, digital camera, etc.

Cyber Crimes

Real-world & Virtual- world

- Current approaches evolved to deal with real-world crime

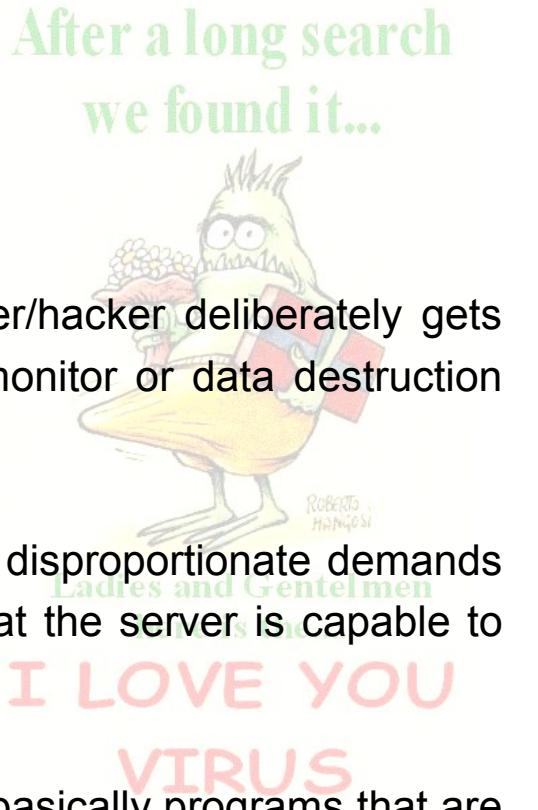
- Cybercrime occurs in a virtual-world and therefore presents different issues

Example : Theft

- **Real-world theft:**
  Possession of property shifts completely from A to B, i.e., A had it now B has it

- **Theft in Virtual-world (Cyber-theft):**
  Property is copied, so A "has" it and so does B

Common scenarios in Cyber Crime



Unauthorized access: This occurs when a user/hacker deliberately gets access into someone else's network either to monitor or data destruction purposes

Denial of service attack: It involves sending of disproportionate demands or data to the victims server beyond the limit that the server is capable to handle and hence causes the server to crash

Virus, Worms and Trojan attacks: Viruses are basically programs that are attached to a file which then gets circulated to other files and gradually to other computers in the network. Worms unlike Viruses do not need a host for attachments they make copies of themselves and do this repeatedly hence eating up all the memory of the computer. Trojans are unauthorized programs which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

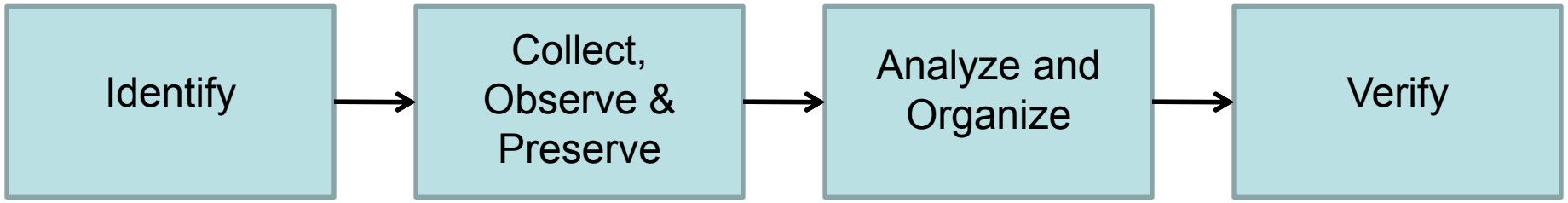
Email Bombing It refers to sending a large number of emails the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing

Internet Time Thefts This connotes the usage by an unauthorized person of the Internet hours paid for by another.

Web Jacking This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website

Theft and Physical damage of computer or its peripherals This type of offence involves the theft of a computer, some parts of a computer or a peripheral attached to the computer. and physically damaging a computer or its peripherals

Handling of Evidences by Cyber Analysts



Four major tasks for working with digital evidence

Identify: Any digital information or artifacts that can be used as evidence.

Collect, observe and preserve the evidence

Analyze, identify and organize the evidence.

Rebuild the evidence or repeat a situation to verify the same results every time. Checking the hash value.

Challenges faced by Law Enforcement

Awareness: Technology is changing very rapidly. So does the increase in Cyber crimes, No proper awareness shared with regard to crime and latest tools. People are so ignorant that makes it effortless for cyber criminals to attack. People fear to report crimes and some crimes are not properly recorded. The reason behind this is that the victim is either scared of police harassment or wrong media publicity. For minority and marginalised groups who already bear the brunt of media bias, reporting online harassment to the police may simply draw further unwanted attention. The public is not aware of the resources and services that law enforcement could provide them if being a victim of crime or witness.

Technical Issues: Large amount of storage space required for storing the imaged evidences and also for storing retrieved evidence after analysis. Retrieved evidence might contain documents, pictures, videos and audio files which takes up a lot of space. Technical issues can further be categorised into software and hardware issues.

Software and Hardware Issues: The growth of Cyber crime as given rise to numerous Forensic software vendors. The challenge being to choose among them and no single forensic tool solves the entire case, there are loads of third party tools available. So is the case with Hardware tools, Most common and liable h/w tool is the FRED. But when it comes to Mobile forensics it is a challenge to decide the compatibility of different phones and which h/w to rely on..

Recently China has been manufacturing mobile phones that have cloned IME numbers which is a current challenge faced in Mobile forensics.

Information sharing: Information sharing is a best practice and can be accomplished by a variety of means such as interacting with industry groups, attending briefings, meetings, seminars and conferences, and working actively with forensic bodies like CDAC..

Inadequate Training and Funds: Due to the growing of cyber forensic tools law enforcement does not get adequate training and awareness on innovative tools. Training bodies are limited and are pricey. Insufficient funding in order to send officers for training and investing on future enhancements. Transfers and recruiting officers adds to the loss of experienced staff and spending for training the newcomers. Cases become pending in such circumstances.

Global Issues: Most of the IP addresses retrieved during investigation leads to servers or computers located abroad which have no identity, hence further investigations are blocked and closed. Correspondence with bodies such as Google, Yahoo, Hotmail is quite time consuming and prolong the investigations.

Wireless or Wi-Fi, Bluetooth, Infrared Issues: Latest wireless technologies which provide internet connections causes exploitation especially when it is not secured. This is the present technology terrorists and radical activists exploit. This is another vulnerability that law enforcement faces.

Judiciary and IT Act 2000

The judicial bodies are not fully aware of Cyber crime and the way in which investigations are carried out.

Although Cyber law courses available in India, it is difficult to find a experienced cyber lawyer who is aware of Forensic analysis and technical terms.

It is difficult to convince judicial bodies including judges and the tribunal when evidence is in a digital format.

There is no legal procedure for collecting, analyzing and presenting evidence in the court of law. Hence the defense lawyer can always anticipate a ambiguity.

There are certain shortcomings of the Information Technology Act, 2000 with regard to identity theft, spamming, pornography, data protection and internet banking.

Current and Emerging Cyber Forensic Tools of Law Enforcement

Guidance Software

EnCase

AccessData

CDCC
The Supercomputing People

CyberCheck Suite

Cyber forensics Tools

Data Recovery

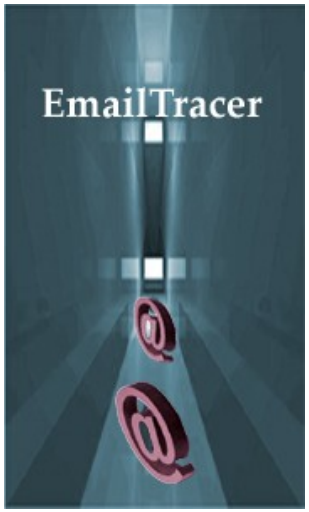
Data Analysis

Disk Imaging

TrueBack

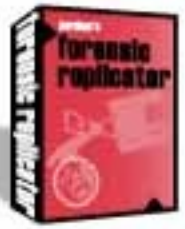
- Seize
- Acquire
- Seize & Acquire

EmailTracer



paraben's

forensic replicator



paraben corporation

paraben's

device seizure toolbox

Think before you Click

THANK YOU

Sri.Loknath Behera.IPS