**Cyber Forensics**

Brief by – Harsh Sharma

**Introduction**

**Cyber Forensics**

Analysis of electronic data to determine the criminal activity and malicious attempts for legal purposes is known as Cyber Forensics. Cyber Forensics is also known as Computer Forensics. Cyber forensics is mostly done in cybercrime investigations.

**Cyber forensics is classified into several categories:**

1. Disk Forensics
2. Network Forensics
3. Wireless Forensics
4. Database Forensics
5. Malware Forensics
6. Mobile Forensics
7. GPS Forensics
8. Email Forensics
9. Memory Forensics

**Disk Forensics**

Disk Forensics is the process of extracting information from storage devices such as hard disk, USB drive, CD, DVD, flash drive or floppy disk.

Step in Disk Forensics are as follows:

1. Identification of evidence: The step locates the sources of evidence at the crime scene.
2. Seizure and acquisition of evidence: The hash value of the original evidence is computed with a forensic tool. The hash value is stored, and the evidence is packed and sealed. Acquisition is the process of taking bit-by-bit copy of the original evidence which itself is write protected. This is done in a forensics laboratory.
3. Authentication of the analysis of evidence: The step is required to check the hash value of both the evidence are same or not i.e. the original evidence and the forensic copy of the evidence.
4. Preservation of the evidence: After acquisition and authentication of evidence, it is kept in a place that is secured from magnetic and other radiations.
5. Analysis of the evidence: Collecting information from the evidence.
6. Report on the findings and documenting the whole process.

**Network Forensics**

The process of capturing, recording and analysis of network events so as to find any malicious activity, security attack or any violation is known Network Forensics.

Tools for analysis

1. IDS - Intrusion Detection System: It is a device or software application that monitors networks and the systems under it for malicious activity or policy violations and maintains the record of the activity. Any detected activity or violation will be reported to the administrator of the network.
2. Logging obtained from the IDS can be used to reconstruct the security incident.
3. Packet capturing tools can be used to gather and record every bit exchanged between any two designated hosts.

**Wireless Forensics**

Wireless Forensics is a part of Network Forensics, analysis of network captures using forensic tools like Wireshark, network-grep, text-based tcpdump and tshark sniffer used to automate and script the analysis of certain task.

**Database Forensics**

A database is a collection of records. To determine the security breach to a database , reverting any unauthorized manipulation is a primary goal in this type of forensics.

Objectives of database forensics:

1. To flag the database breach
2. To identify the data before and after the security breach
3. To recover previously deleted database
4. To retrace user DML and DDL operations

**Malware Forensics**

Malware is a malicious software : Once the presence of malware is identified , the hard disk is cleared and the machine is re-imaged so as to prevent other systems in the network from getting affected.

Data is collected from the machine and the user and includes logs from anti-malware(antivirus), browser cookies, history, and email history. This information can be used to figure out the origin of malware and to alert others users in the network and protect other machines in the network.

**Mobile Forensics**

Recovery of digital evidence from mobile devices. It is a branch of digital forensics. Process of mobile forensics is same as Disk Forensics.

Stages:

1. Possession of the devices
2. Preparing the environment for mobile forensics.
3. Acquisition
4. Evidence examination
5. Presentation and reporting

**GPS Forensics**

GPS Forensics is now very important to trace down drug traffickers, murderers and cyber criminals. As a part of forensic examination, live and deleted data can be recovered from different navigation devices. Forensic tools can be used to extract information from trip logs which hold information about the devices.

**Email Forensics**

Most of the cyber-attacks happens through email. Email forensics is a process to find potential information like email headers, sender IP address. The goal of email forensics is to identify the person behind the crime, collect evidence and present the findings to build a strong case. Email tracing and email tracking can be achieved with email forensics, where the former aims to determine the source.

Tracing is done when an email header is available, whereas tracking is done even when no information is available about an email id.