SNS COLLEGE OF TECHNOLOGY

(Autonomous)
COIMBATORE – 35

DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

UNIT II - CYBER FORESENICS

Topic Name : Cyber Forensics and Digital evidence

Cyber forensics is a process of extracting data as proof for a crime (that involves electronic devices) while following proper investigation rules to nab the culprit by presenting the evidence to the court. Cyber forensics is also known as computer forensics. The main aim of cyber forensics is to maintain the thread of evidence and documentation to find out who did the crime digitally. Cyber forensics can do the following:

- It can recover deleted files, chat logs, emails, etc
- It can also get deleted SMS, Phone calls.
- It can get recorded audio of phone conversations.
- It can determine which user used which system and for how much time.
- It can identify which user ran which program.

Why is cyber forensics important?

In todays technology driven generation, the importance of cyber forensics is immense. Technology combined with forensic forensics paves the way for quicker investigations and accurate results. Below are the points depicting the importance of cyber forensics:

- Cyber forensics helps in collecting important digital evidence to trace the criminal.
- Electronic equipment stores massive amounts of data that a normal person fails to see. For example: in a smart house, for every word we speak, actions performed by smart devices, collect huge data which is crucial in cyber forensics.
- It is also helpful for innocent people to prove their innocence via the evidence collected online.
- It is not only used to solve digital crimes but also used to solve real-world crimes like theft cases, murder, etc.
- Businesses are equally benefitted from cyber forensics in tracking system breaches and finding the attackers.

The Process Involved in Cyber Forensics

- Obtaining a digital copy of the system that is being or is required to be inspected.
- Authenticating and verifying the reproduction.
- Recovering deleted files (using Autopsy Tool).
- Using keywords to find the information you need.
- Establishing a technical report.

How did Cyber Forensics Experts work?

Cyber forensics is a field that follows certain procedures to find the evidence to reach conclusions after proper investigation of matters. The procedures that cyber forensic experts follow are:

- **Identification:** The first step of cyber forensics experts are to identify what evidence is present, where it is stored, and in which format it is stored.
- **Preservation:** After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.
- **Analysis:** After getting the data, the next step is to analyze the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the final conclusion.
- **Documentation:** Now after analyzing data a record is created. This record contains all the recovered and available(not deleted) data which helps in recreating the crime scene and reviewing it.
- **Presentation:** This is the final step in which the analyzed data is presented in front of the court to solve cases.

Types of computer forensics

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- **Network forensics:** This involves monitoring and analyzing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.
- **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.
- **Malware forensics:** This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, trojans to identify the hacker involved behind this.
- **Memory forensics:** This branch of forensics deals with collecting data from the memory(like cache, RAM, etc.) in raw and then retrieve information from that data.
- **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyze data from the mobile phone.
- **Database forensics:** This branch of forensics examines and analyzes the data from databases and their related metadata.
- **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Techniques that cyber forensic investigators use

Cyber forensic investigators use various techniques and tools to examine the data and some of the commonly used techniques are:

- **Reverse steganography:** Steganography is a method of hiding important data inside the digital file, image, etc. So, cyber forensic experts do reverse steganography to analyze the data and find a relation with the case.
- **Stochastic forensics:** In Stochastic forensics, the experts analyze and reconstruct digital activity without using digital artifacts. Here, artifacts mean unintended alterations of data that occur from digital processes.
- **Cross-drive analysis:** In this process, the information found on multiple computer drives is correlated and cross-references to analyze and preserve information that is relevant to the investigation.
- **Live analysis:** In this technique, the computer of criminals is analyzed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.
- **Deleted file recovery:** This includes searching for memory to find fragments of a partially deleted file in order to recover it for evidence purposes.

Advantages

- Cyber forensics ensures the integrity of the computer.
- Through cyber forensics, many people, companies, etc get to know about such crimes, thus taking proper measures to avoid them.
- Cyber forensics find evidence from digital devices and then present them in court, which can lead to the punishment of the culprit.
- They efficiently track down the culprit anywhere in the world.
- They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.

What are the required sets of skills needed to be a cyber forensic expert?

The following skills are required to be a cyber forensic expert:

- As we know, cyber forensic based on technology. So, knowledge of various technologies, computers, mobile phones, network hacks, security breaches, etc. is required.
- The expert should be very attentive while examining a large amount of data to identify proof/evidence.
- The expert must be aware of criminal laws, a criminal investigation, etc.
- As we know, over time technology always changes, so the experts must be updated with the latest technology.
- Cyber forensic experts must be able to analyse the data, derive conclusions from it and make proper interpretations.
- The communication skill of the expert must be good so that while presenting evidence in front of the court, everyone understands each detail with clarity.
- The expert must have strong knowledge of basic cyber security.

Digital forensics

Digital forensics is the application of analyses techniques to the reliable and unbiased collection, analysis, interpretation and presentation of digital evidence.

It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

It is difficult to provide a precise definition of "digital evidence" because the evidence is recovered from devices that are not traditionally considered to be computers. Some researchers prefer to expand the definition by including the "collection" and "examination" of all forms of digital data, including the data found in cell phones, PDAs, iPods and other electronic devices.

- Uncover and document evidence and leads.
- Corroborate evidence discovered in other ways.
- Assist in showing a pattern of events (data mining has an application here).
- Connect attack and victim computers.
- Reveal an end-to-end path of events leading to a compromise attempt, successful or not.
- Extract data that may be hidden, deleted or otherwise not directly available.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices. Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.

The typical scenarios involved are:

- Employee Internet abuse.
- Data leak/data breach.
- Industrial espionage.
- Damage assessment.
- Criminal fraud and deception cases;
- Criminal cases.
- Copyright violation – more about this is mentioned.

Using digital forensics techniques, one can:

- Corroborate and clarify evidence otherwise discovered.
- Generate investigative leads for follow-up and verification in other ways.
- Provide help to verify an intrusion hypothesis.
- Eliminate incorrect assumptions.