NAME: SAYED MOHAMMED OWAIS

CLASS: MSc CS(Part-II)

ROLL NO: 532   DIV: F

SUBJECT: CYBER FORENSICS & LAW

Unit- I

Q Explain computer forensics technologies and its fields.

⟹ Computer forensics is the science of obtaining, preserving and documenting evidence from digital devices such as electronic storage devices (computers, PDA's, digital cameras, mobile phones) and various memory storage devices. Computer forensics technologies are made use of in different fields like military, law enforcement and computer analysts to serve the very purpose of identifying computer crime.

- Military computer forensics technology:
  - The features of military computer forensics involves discovering, evidence and gauging the effect on the victim and access the nature and motto of the attacks.
  - The emergence of CFX 2000 (computer forensics Experiment 2000) has transformed forensics technology from military research and development laboraties into being used by laws enforcement.
  - The idea of CFX 200 is that it is possible to accurately determine, the motives, intents, targets, sophistication, identity and location of the cyber criminals and cyber terriorists by deploying and integrated forensics analysis framework
  - The framework uses the concept of SI-FI platform which enables cyber forensics investigations to be captured and analyzed using digital evidance bays meant for storing electronic evidence.

- Law enforcement computer forensics technology:
  - Evidence is usually captured and stored by the computer without the users knowledge; in order to retrieve and analyze the evidence, forensics tools capable of gathering hidden information from the computer is needed.
  - Such procedures should always confirm to legal standards.
  - Evidence from computers is succeptible to change and possibly be earesed, so trainees are trained in backing up the evidence.
  - The law enforcement officials should also be trained in the following:
    - Trojan horse programs.
    - Computer forensics documentation.
    - File stack.
    - Data hiding technologies
    - e-commerce investigations.
    - Text search techniques.
    - Disk structures
    - Data encryption.
    - Data compression.
    - Erased files.
    - Boot process and memory resident programs.

- Business Computer forensics technology:
  - Remotely monitoring computers : This is amethod used by andlysts to capture evidence without being in close proximity of the offender's computer.
  - Creating electronic documents which can be tracked These tools enable agents to track views of offenders pertaining to certain documents. The tools identify the connection to the documents that have been stolen.
  - Recovery softwore for computer theft: These tools will locate your stolen computers once the software is installed on Computer.
  - Forensics services: Forensics expert can track crime anywhere in the world and be able to recover the lost data or track misappropriation of your valuable resources.

Q. Why do individuals and organizations need to pay attention to computer forensics?

⟹ • In recent years, more and more people are using computers and devices with computing. ability. Many businessman and personal transactions are conducted electronically.

- According to a university of california study, 93% of all information generated was in digital form. Morever, a significant of computer created documents might never be printed on paper.

- Need for computer forensics:
  - • Consider a hypothetical scenario where a criminal is broken into an organizations premises and stolen critical assets. A responsible executive would have no hesitation calling in professional forensics examiner and extending Them all necessay cooperation.
  - • Such cooperation might involve coording of the crime scene to ensure that:
  - • The area is not disturbed.
  - • Evidence is not accidently contaminated or tampered with.
  - • Forensic professionals have access to the necessay information or location.

- The executive would do this because if is in his/her organizations best interest. This would be done with the intent for collecting relevant evidence, if the criminal is to be caught, assests are to be recovered or if cant action is to succesfull court prosecution will vanish.
- Now, lets suppose the criminal had committed the theft electronically - for example he/she hacked into an organizations computers to steal valuable data. Or perhaps, the criminal is an insider commiting a white collar crime or fraud using organization computers.
- A responsible executive similarly would know that it was in his/her personal interest to call in the appropriate computer forensics specialist and extend them as much cooperative assistance as possible because if there is to be any chance of recovering property, locating and successfully prosecuting the criminal, there must be evidence of sufficient quantity and qualify.

Q. What is digital data and where can it be found?

⟹ Types of data:

- Active data:
  Active data consists of data created by The user. (Including temporay files.

- Metadata: Many users are aware That important data is kept within data files. However, many users may not be aware of The other information about the files which may be useful for investigation. This data is called metadata.
- Operating System data: Data from the computers operating system can be a rich source of details about what a user has been doing.
- Temporary Files: When a user runs a program, data may be temporarily stored on The hard drive.
- Communications data: Whenever a person uses a computer, mobile phone or other device to communicate, a digital trail is created that can yield information regarding whom the user communicated with, what was discussed, when it occured, who was privy to it, what documents were transmitted and even attempts to erase the record of that communication.

- Residual data:
  - When a user deletes a file, the operating system does not remove the file data.
  - Rather the operating system only indicates that the space is available.
  - A person who knows how to access these released-but-not erased areas and who has the proper tools can recover these contents.
  - Residual data can also include portions of files distributed on the drive surface or embedded within other file.
    - Slack space: Data can be found in what is known as the stack area of the hard disk. slack space is an area at the end of the space allocated to a file not occupied by data belonging to that file.

- Backup data:

  Backup data typically consists of information copied to portable media to provide users with all access to their data.

- Sources of data:
  - One obvious source of data is the user's computer; yet potential sources of digital data within a computer are not always obvious.
  - while digital data obviously exists on a computer hard drive, digital data may also be located on media devices attached or inserted to a computer as well as within the cache memories of the computer.

Q. Why is knowledge of computer Forensics are important?

=> Computers and networks are becoming widely used with every passing day and hence the opportunity for criminals to employ these facilities to commit crimes is increasing.

- Preservation of evidence:
  - The ability to retrieve and preserve data plays a pivotal role in the prosecution of a case and it is important that anyone gathering data know.
    - where to find
    - How to find
    - Gather
    - Preserve such evidence
  - There are several reasons why a specially trained, qualified computer Forensics specialist should be called in to investigate a potential cyber crime.
    - To handle issues specific to digital date.
    - To maintain the change of custody.
    - To avoid the dangers of mishandling digital data.

- Need for computer forensics and important of gathering and preserving evidence:
  - While the process of digital forensics may be addmittedly time consuming and disptive, the potential cost of not conducting a proper digital forensics examination may be substantial if not disastrous.

- Loss of evidence may hamper any efforts to recover lost digital assests or affect the viability of the any future legal action - Even if the criminal were caught, without proper evidence he/she could not be charged.
- By avoiding a proper examination, an organization risks losing a valuable opportunity to identify and correct security weakness. As a ~~se~~ result, not only would an organization remain vulnerable to future attacks, such failure to take positive corrective action might also damage an organization image and reputation potentially resulting in loss of customer confidence in the organization - and loss of business.
- Loss of valuable information such as customer files, private data or other confidential information, may potentially render an organization vulnerable to legal or other action.
- For companies whose business models depend on protection of intellectual properties, maintaining confidentially or whose business data is a highly sought after commodity, such losses could be castastrophic particurlay if the data were not recovered in a timely manner.

Q. What does a computer forensics specialist do?

⟹ - The job of computer forensic specialist is to help determine if a computer disk, media or other device contains potential evidence and secure from any seized material, be it hard disks, floppy disks, tape or any storage media, a true copy of the data contained therein. If it does, he/she must oversee the extraction of information from the computer media to ensure that this process is conducted properly and that evidence is obtained without compromising The original data.

- Once the data has been extracted and properly processed the computer forensics specialists must evaluate the information for its evidentiary value.

- All this should be done in accordance with internationally accepted best practices to ensure the probative value of the evidence obtained.

- Evidence handling principles:
  - First the general rules of evidence should be applied to all digital evidence.
  - It is important that forensic specialists, upon seizing digital evidence ensure that the evidence is not changed and that the only persons who are suitably trained should be allowed to access original digital evidence should be need arises.

- Initial assessment:
  - In the event that a computer forensics specialist must go to a site to acquire evidence, his/her first task is to attempt to determine the types of computer systems in use so that he/she can then bring the appropriate tools to the scene.

- Evidence gathering considerations:
  - In general, items for forensics examination should be preserved securely as soon as possible with all items taken, examined in laboratory or forensic workspace rather than at the scene.
  - Whenever practicable, an image copy should be made of the entire target device through partial or selective file copying may be acceptable. in certain circumstances.

- Image copy:
  - In most computer forensics examinations, the next step is to make an exact copy of the data residing on the evidence hard disk. The need to create such a copy is consistent with the essential concern not to change the evidence.

- Analysis:
  - With the image copy, the forensic specialist can now commence his/her following SOP.
  - In performing the analysis, the forensic specialists need to consider.