1. COMPUTER FORENSIC INVESTIGATION PROCESS – FIRST RESPONSE

Incident response or first response constitutes the method carried out to respond to an incident or crime involving computers or any related devices. An incident related to crime or security violation can be due to several reasons like security breach alarm from an IDT (intrusion detection tool), several unsuccessful login attempts, Unknown new user creation or new file creation, modification or deleting of data, modification of system files and many other frauds.

1.1. Categories of Incidents

All incidents are not similar and it is highly necessary to tailor-make incident response plan to each incident. Response is always better with a good Incident Response Plan categorized by the state of difficulty, in terms of vast and changing systems, identifying various platforms used, securely handling each evidence collected, and not damaging the critical systems in process. Investigation team members should ensure proper seizure and evidence handling at scene of crime.

There are 3 categories of incidents: Low- Level incidents, Mid-Level incidents, High-Level incidents.

1.1.1. Low Level

Low level incidents are the least severe kind of incidents. They should be handled within one working day after the event has occurred. They can be identified by several ways, some of which are: when there is a loss of personal password, suspected sharing of organization's accounts or emails or data, unsuccessful scans and probes or otherwise due to the presence of any computer virus or worms.

1.1.2. Mid Level

Mid-Level incidents are relatively more serious and thus, should be handled the same day the event has occurred. These kinds of incidents can be identified by the method of observation. Some of the observations may be a violation of special access to a computer or computing facility, unfriendly employee termination, unauthorized storing and processing of data, destruction of property related to a computer incident, personal theft, and large intensity of computer viruses or worms.

1.1.3. High Level

High-Level incidents are the most serious incidents. These kinds of incidents should be handled immediately after the incident has occurred. Some of the incidents include: Denial of Service attacks, computer virus or worms of highest intensity, changes to system hardware, firmware or software without authentication, suspected computer break-in, illegal electronic fund transfer or download, any kind of pornography, human trafficking, gambling or violation of any law.

1.2. FIRST RESPONSE BY FORENSIC STAFF

First Response by forensic investigators involves 6 major steps:

1. Secure and evaluate electronic crime scene
2. Conducting preliminary interviews
3. Documenting electronic crime scene
4. Collecting and preserving electronic evidences
5. Packaging electronic evidence
6. Transporting electric evidence

1.2.1. First Response Step 1,2 - Secure and Evaluate Electronic Crime Scene and Conducting Preliminary Interviews

Forensic investigators should prevent people making any attempt to restore or recover information from the computers or any devices at the scene of crime. They should ensure the security of responders. People, when they are caught or suspect they might be caught, can have unpredictable or desperate and violent behaviours. Physical location of the crime including place of crime, building, floor, room, access method used for internet, location of computers, number of computers involved etc should be documented. Investigators should conduct personnel interviews and record them and identify criminal histories, employment status, hour of operation of business. They should also isolate the suspects from computers and ultimately gather maximum information about suspects.

The forensic investigator should plan the 'search and seizure' by identifying the location of the incident, equipment (type and number of equipment) involved. Once done, he/she must detail everything (make, model, location etc) that is to be seized, check devices where unauthorized hardware (like modem, key loggers) are connected. Search warrants should be obtained from the court to enter the organization where the crime has occurred, to access rooms, devices or any company-owned property, and seize all or part of a computer system.

1.2.1.1. Evidences and Electronic Evidences

Evidences provide proof. Computer evidence after an incident may be in the form of some files, which can provide evidence of an incident, contents of files, such as log files, picture files, executable files. The first step in the evidence collection process is to recognize and identify hardware, software, and data. Before

starting any forensic investigation, it is recommended to have skilled professionals, a workstation, a data recovery lab, support from management, and defined methodology.

"*Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device*" (Marcella et al). Electronic evidence can also be hidden such as fingerprint evidence or DNA evidences. Electronic evidences can be broken, altered, damaged or destroyed by improper handling. It can expire within a pre-set time.

Electronic evidence goes through following procedures:

- Collection: Searching, recognizing, collecting and documenting
- Examination: Discovering evidence from crime scene, describes about its origin & importance
- Analysis: Relating evidence found after examination to actual crime, provides proof for the case
- Reporting: summary of examination process & relevant data recovered

Investigators should search the electronic crime scene to recognise and collect potential evidences like:

Smart card	Portable device (microprocessor – stores encryption key or password & digital certificate).
Dongle Smart Cards -	Copy protection device provided with software that plugs into a computer port.
Biometric scanner	**C**onnected to a computer system to identify users.
Dongle -	Recognize or authenticate information and user, level of access, configurations permissions.
Answering Machine	Evidence is found in voice recordings like deleted messages, last number called, Memo, phone numbers, tapes.
Digital Camera	Evidence is found in images, removable cartridges, video, sound, time and date stamp.
Handheld Devices	For example Digital Assistants (PDAs) and electronic Organizers-Evidence is found in the Address book, appointment calendars or information, documents, e-mail, handwriting, password, phone book, text messages & voice messages.
Modem	Evidence is found in the device itself.
Pager	Contains volatile evidence such as address information, text messages, e-mail, voice messages & phone numbers
Printer	Evidence is found through usage logs, time and date information and network identity information, ink cartridges, time and date stamp.
Scanner	Evidence is found by looking at the marks on the glass of the scanner.
Telephones	Evidence is found through names, phone numbers, Caller Identification Information, appointment info, electronic mail and pages.
Copiers	Evidence is found in documents, user usage logs, time and date stamps.
Network Interface Card (NIC) -	Evidence is found in MAC (Media Access Control) address, routers (evidence in configuration files), hubs and switches (evidence is found on the devices themselves).
Network Cables and Connectors	Evidence is found on the devices themselves (e.g. how they are connected, type of connection etc)

Credit Card Skimmers	Information that is present on the tracks of the magnetic stripe is read. Evidence is found through card expiration date, User's address, credit card numbers, User's name
Digital Watches	Evidence is found through Address book, Notes, Appointment calendars, phone numbers and emails
Facsimile (Fax) Machines	Evidence is found through documents, phone numbers, film cartridge, Send or Receive logs
Global Positioning Systems (GPS)	Evidence is found through previous destinations, way points, routes and Travel Logs.

Investigators may use specific tools and equipment (cameras, notepads, sketchpads, evidence forms, crime scene tape and markers) to collect the evidences. Other categories of tools include:-

- **Documentation Tools**: Cable tags, indelible felt tip markers, Stick-on labels
- **Disassembly and Removal Tools**: Screwdrivers and pliers (different types), small tweezers, wire cutter.
- **Package and Transport Supplies**: Antistatic bags, antistatic bubble wrap, cable ties, evidence bags, evidence tape, packing materials, sturdy boxes of various sizes.
- **Other tools**: Gloves (for health and safety reasons and so as not to add fingerprints), hand truck, magnifying glass, printer paper, seizure disk, unused floppy diskettes.

1.2.2. First Response Step 3 - Documenting Electronic Crime Scene

Before anything is touched or removed, the electronic crime scene is documented and recorded through a combination of field notes, sketches, video, or still images, to as to show how things were initially found before seizure.

- **Record:** Take detailed notes of everything seized.
- **Photographer:** Photograph all items in place before they are seized, including connections at the back of the computer case, computer screen.
- **Search & seizure specialist:** Search and seize the bags and tag traditional evidence (documents, pictures, drugs, weapons, etc).
- **Digital evidence search & seizure specialist:** Search and seize and then bag and tag digital evidence of all types.

1.2.3. First Response Step 4 - Collecting and Preserving Electronic Evidences

Forensic investigators should perform the following instruction while collecting and preserving electronic evidences.

1. **Physical evidences:** Avoid contamination through the use of hand gloves and breathing masks while collecting data of fingerprints on keyboard, CDs, mouse, and hard disk, and hair, fibres or body tissues on computer parts. It is important to protect evidences and the investigator from bacteria or viruses.
2. **Data contained in RAM:** Collect information of running processes, network connections and other important data when the system is live (if ever). Never jeopardize the evidence by directly looking into the computer or devices by searching or browsing files.

   Collection of evidences should proceed from the most volatile to the least volatile. Start with the volatile data as this may be lost. Order of volatility for a typical system is as follows:

   a. Registers, Cache Memory
   b. Routing tables, ARP cache, process tables, and kernel statistics, memory
   c. Temporary file systems
   d. Onboard memory of system peripherals such as the video card or NIC
   e. Disk or other storage media
   f. Remote logging & monitoring data relevant to the system in question
   g. Physical configuration, network topology
   h. Archival media

3. **Dealing with Power ON/OFF at seizure time - If a computer is switched OFF, leave it in OFF state.**

- If a computer is switched ON and the screen is viewable, then the following must be done:
  - Record the programs running on screen.
  - Document the condition of the evidence.
  - Take photographs (screen, computer front and back, and area around the computer to be seized) and/or make a sketch of the computer connections and surrounding area.
  - Connections of external components should be noted.
- Disconnect the computer from network connections by removing the network cable. It prevents the possible remote destruction of data.
- Memory (volatile data) imaging & Live data analysis

- Consider the potential of encryption software being installed on the computer or as part of the operating systems. If it is present then appropriate forensic methods should be utilised to capture the encrypted data before the computer is powered down.

4. Computer shutdown procedures: How a computer/laptop is shut down depends upon the operating system, and its function.

- If there is a stand-alone computer/laptop which is not on network, then pull out the power cord and disconnect all power sources by unplugging from the back of the computer. Place evidence tape over power plug connector on the back of computer.
- If a computer or laptop is on network, remove power connector from the back of the computer. Place evidence tape over power plug connector on back of the computer.
- In the case of servers (if necessary), capture volatile data if necessary and perform a normal shutdown procedure.

1.2.4. First Response Step 5 - Packaging Electronic Evidences

Each piece of evidence should be protected from changes and a chain-of-custody should be maintained. Collected electronic evidences are documented, labelled and listed before packaging. Appropriate packaging of evidence may include plastic/paper bags or sleeves, computer case sealed with evidence tape over case access points and power connectors. Devices with volatile memory should be packaged appropriately to allow for power to be maintained to the device. Make sure that all containers that hold evidences are labelled in an appropriate way.

1.2.5. First Response Step 6 - Transporting Electronic Evidences

Special care should be taken with transportation of digital evidence material. Avoid physical damage, vibration and effects of magnetic fields, electrical static and large variations of temperature and humidity. Keep electronic evidence away from magnetic sources while transporting. Magnetic media should also be kept away from Radio Frequency (RF) energy emitted by police radio transmitters located in police cars. Avoid storing electronic evidence in vehicles for long periods. Proper bagging should be done for transportation to avoid items being shifted and damaged. When evidence arrives at the forensic lab, update chain of custody for evidence every time it is accessed for analysis.

2. CASE WORK

Case 1: Employee Intellectual Property Information Theft

John is working for a company involved in selling beauty products to individual customers, beauty parlour and international customers. John has been given a laptop which allows him to get access to highly confidential information on customers, business practices, sale strategies and supplier reports. Some of the information resides only in John's laptop while other data are regularly backup and available on the company server.

However after some time, John's employer notices that the company sale is declining and later on John offers his resignation. Soon after, his former employer learns that John has joined the direct competitor of the company.

His former employer suspects that John has stolen the company confidential data and trade secrets for the benefits of the competitor.

You have been asked to conduct a computer forensic investigation to discover evidences of misuse. To proceed with the investigation the following steps should be followed:

- Identification and Collection of Digital Evidence
- Preservation of Electronic Evidence
- Examination of digital Evidence
- Reporting the Result/Findings.

1. Identification and Collection of Digital Evidence

The first thing is to know which evidence is present, where it resides and in which state it is stored. This will determine the appropriate process to recover the evidence. Furthermore, the computer forensic investigator should identify the data stored in the device and its format so that appropriate tools can be applied to extract the information - for example, the operating system running on the device and the general configuration such as disk format. After the evidence has been identified, the investigator should create an image of the hard disk or storage media.

Casework Scenario

From the scenario, we can identify that John's laptop is the main device to be collected. Furthermore, the company server is also another device which will help in providing evidence since regular back up are being performed as well as email log.

Computer forensic tools such as FTK imager can be used to make an image of the laptop

2. Preservation of Electronic Evidence

One of the starting points of the investigation would be to forensically preserve the digital information present on the employee's workstation. The goal is to make an exact copy of the hard disk as soon as possible after the electronic device has been seized. This process is known as ***forensic imaging***. As a result, the computer forensic investigator will generate a chain of custody documentation, take photographic images of the device, and check the integrity of the preserved information. These steps are important in order to ensure that the digital evidence obtained during the investigation will be admissible in court and that no alteration of the original data has occurred. Use of forensic tools such as FTK, Helix, EnCase and SafeBack can be used to acquire the data and preserve them.

Casework Scenario

Before any analysis can be performed, a hash of the digital device (John's laptop) is performed, so as to detect any alteration.

A chain of custody form such as below can be used:

Chain of Custody Form	
Details of the Digital Evidence	
Crime Number	
Name of Investigating Officer	
Date of Seizure	
Time	
Technical Details	
Manufacturer	
Make/Model	
Serial Number	
Additional Description	

Chain of Custody Details					
Action	Received From	Received By	Date	Time	Addition Details

Figure 4.1: Chain of Custody Form

Preservation of Evidence:

Below is a list of data which can be preserved in addition to the laptop:

- Logs files, backups, access registers, calendars and appointment books can be preserved.
- Storage devices such as hard drives, CD, DVD, flash drives can be preserved.
- Emails and other communication data can be preserved.
- Address Resolution Protocol cache, login session, contents in the RAM memory
- Recent Internet activity
- Files recently opened or deleted
- Cloud storage

3. Examination of digital Evidence

This involves the extraction, processing and interpretation of the digital information in order to provide a timeline analysis. The latter will provide information such as when a file was modified, accessed, changed or deleted. That information is gathered using a variety of computer forensic tools as discussed in UNIT 3. Besides timeline analysis, data recovery, string and keyword search, volatile evidence analysis and system file analysis are performed.

Casework Scenario

From the scenario perspective, we can infer that John could have deleted the confidential files (thus the use of computer forensics tools to restore the deleted files).

Furthermore, to copy the confidential files, we can assume that an external USB device could have been employed. Thus it is important to know the serial number and the make of the USB device as well as when

the USB device has been connected to the laptop. Hence an in-depth registry analysis will provide valuable information on external devices used on the laptop.

Besides an analysis of recently opened files could also provide an indication on the type of document John was working on.

Also the use of cloud storage on the laptop should be investigated. It may happen that no external drive (USB) was connected to the laptop. However the data can be transferred through the use of cloud application such as Google Drive and Dropbox. Therefore it is important to look for those application and verify the log activities to know which type of files has been transferred.

Email activities should also be scrutinized. Important information could be sent using the company email, via attachment, to personal email account such as Yahoo or Google mail.

4. Reporting the Result/Findings.

Once all the digital evidence has been analyzed, the results should be provided in a clear and understandable manner.

For the above case study, you are required to follow the computer forensic investigation in order to obtain evidences.

Casework Assessment

Write a report discussing how you would conduct the computer forensic investigation for the Employee Intellectual Property Information Theft scenario. You make wish to expand in detail~~ed~~ each of the individual steps involved during the investigation, providing reasonable argument as to why you have chosen such approach, tools and methodology. Use the knowledge which you have acquired from Units 1 to 4.