CHAPTER 1

Unit I

Computer Forensics

Syllabus Topic : Introduction to Computer Forensics and Standard Procedure

1.1 Introduction to Computer Forensics and Standard Procedure

Q. 1.1.1 What is computer forensics ? Why computer forensics important ? *(Ref. Sec. 1.1)* **(5 Marks)**

Computer Forensic

Computer forensic is collection, preservation, analysis and presentation of computer-related evidence. It determines the past actions that have taken place on a computer system using computer forensic techniques. Computer forensics is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.

Why Is Computer Forensics Important ?

1. A few criminals are becoming smarter. So data-hiding techniques which includes ***encryption*** and ***steganography***. The evidence of criminal activity is placed in such a way where traditional search methods cannot able to find it.
   - **Encryption :** Scrambling data, for example an e-mail message, so that it cannot be readable to the interceptor.
   - **Steganography :** It is nothing but hiding a message into a larger file, typically in a photographic image or sound file.
2. Computer forensics isn't just about "detective work" – searching for and trying to find out information. Computer forensics is also worried with :
   - Sensitive data handling responsibly and confidentially.
   - Taking precautions to not nullify findings by corrupting data.

- Taking precautions to make certain the integrity of the information.
- Staying within the regulation and guidelines of evidence.

1.1.1 Computer Forensic Process Steps

Q. 1.1.2 Explain the process of computer forensics ? *(Ref. Sec. 1.1.1)* **(5 Marks)**

There are 4 common steps for forensic investigation, these steps are as follows :

1. Collection
2. Examination
3. Analysis
4. Reporting

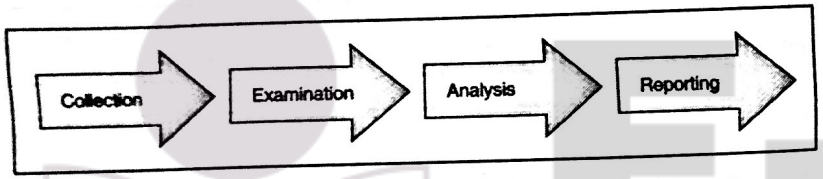

Fig. 1.1.1 : The forensic process

➜ 1. Collection

This is the first phase in forensic process. In this phase data is identified, labelled and recorded and gathering the data and physical evidence related to the incident being invested is done. Simultaneously integrity of the chain of custody is also preserved.

➜ 2. Examination

In this phase from the collected data identify and extract the pertinent information, using proper forensic tools and techniques and also maintain integrity of the evidence.

➜ 3. Analysis

In this phase results of the examination phase are analyzed. From the analysis useful answers to the questions are generated which are presented in the previous phases. Most probably the case gets solved in this phase.

➜ 4. Reporting

In the reporting phase the results of the analysis are done, which contains :

- The information pertinent to the case.

- Actions that have been accomplished actions left to be performed.
- Moves left to be performed.
- Advocated enhancements to processes and tools.

☛ What things are we investigating?

- Investigating the identity theft.
- Investigating the fraud and embezzlement.
- Investigating the software piracy and hacking.
- Investigating the blackmail and extortion.
- Investigating the child pornography and exploitation.
- Investigating the prostitution, infidelity, domestic violence.
- Investigating the terrorism and national security.
- Investigating the theft of intellectual property and trade secrets.

1.1.2 What Evidence Can We Recover at the Time of Investigation?

1. Investigation of Computer Fraud

While investigating the computer fraud we recover following information :

- Credit card data.
- Financial and asset records.
- E-mail, notes, and letters.
- Accounting software and files.
- Account data from online auctions.

2. Investigation of Child Exploitation

While investigating the Child exploitation we recover following information :

- Photos and digital camera software.
- Internet activity logs.
- Movie files.
- User-created directory and file names to classify images.
- Chat logs.

- Graphic editing and viewing software.

3. Investigations of Network Intrusion and Hacking

While investigating the network Intrusion and hacking we recover the following information.

- Names of the Network users.
- Internet Protocol (IP) addresses.
- Executable files which also includes viruses and spyware.
- Security logs and Configuration files.
- Text files and other documents containing sensitive information such as passwords.

4. Investigation of Identity Theft

Investigation of Identity Theft will recover the following information.

- Credit card numbers and the credit card readers, writers and scanners.
- Identification Templates such as driving license, birth certificates etc.
- Images of the electronic signatures
- Information of online trading.

5. Investigation of Harassment and Stalking

While investigating the Harassment and Stalking we recover following information :

- Research of the victims background.
- Victim's location maps.
- Photos of the victim.
- Diaries of the victim.
- Internet activity logs.
- E-mails, notes, and letters.

6. Investigation of Software Piracy

While investigating the software piracy we recover following information :

- Serial numbers of the software.

- Utilities for the software cracking.
- Image files of software licenses.
- Binary files which are required for software installation.
- Chat logs and Internet activity logs.

Syllabus Topic : Incident Verification and System Identification

1.2 Incident Verification and System Identification

1.2.1 Introduction to Incident

Q. 1.2.1 What is Incidence ? What are the goals of incidence response ? *(Ref. Sec. 1.2.1)* **(5 Marks)**

Computer security Incident is any unlawful, unauthorized, or unsuitable activity that includes a computer system or a computer network. Such an activity can incorporate any of the following events :

1. Theft of the trade secrets.
2. Email spam or harassment.
3. Embezzlement.
4. Unauthorized or unlawful intrusions into computing systems.
5. Denial-of-service (DoS) attacks.
6. Extortion.
7. Any unlawful action when the evidence of such action may be stored on computer media for example fraud, threats, and traditional crimes.
8. Possession or dissemination of child pornography.

1.2.1.1 Goals of Incident Response

The goals of the Incident response are as follows :

1. To prevent a disconnected, no cohesive response.
2. Confirms or dispels whether an incident happened.

3. Promotes gathering of accurate information.
4. Establishes controls for proper retrieval and handling of evidence.
5. Protects privacy rights established by law and policy.
6. Minimizes damage to business and network operations.
7. Allows for criminal or civil action against culprits.
8. Provides accurate reports and useful recommendations.
9. Provides quick detection and containment.
10. Minimizes exposure and compromise of proprietary data.
11. Protects your organization's reputation and assets.
12. Educates senior management.
13. Promotes quick detection and/or prevention of such incidents in the future.

1.2.1.2 Who is Involved in the Incident Response Process ?

In the incident response method there is inclusion of :

- Technical specialist, Human resources personnel, legal counsel, security professionals, corporate security officers, business managers, end users, helpdesk workers, and other employees.
- Some organizations establish a team of people. This team is referred as a ***Computer Security Incident Response Team (CSIRT)***.
- This team responds to any computer security incident. The CSIRT consist of proper technical, legal and other specialist necessary to resolve an incident.

1.2.2 Incident Response Methodology

Q. 1.2.2 Explain the Incidence Response methodology or explain the components of Initial Response or explain the steps of initial response ? **(5 Marks)**

(Ref. Sec. 1.2.2)

- Computer security incidents are often complicated, multifaceted troubles like any complex engineering problem. Black box approach is used to solve the incident problem. In this approach divide the larger problem of incident resolution into components and test the inputs and outputs of each component.

- Fig. 1.2.1 illustrates our approach to incident response.

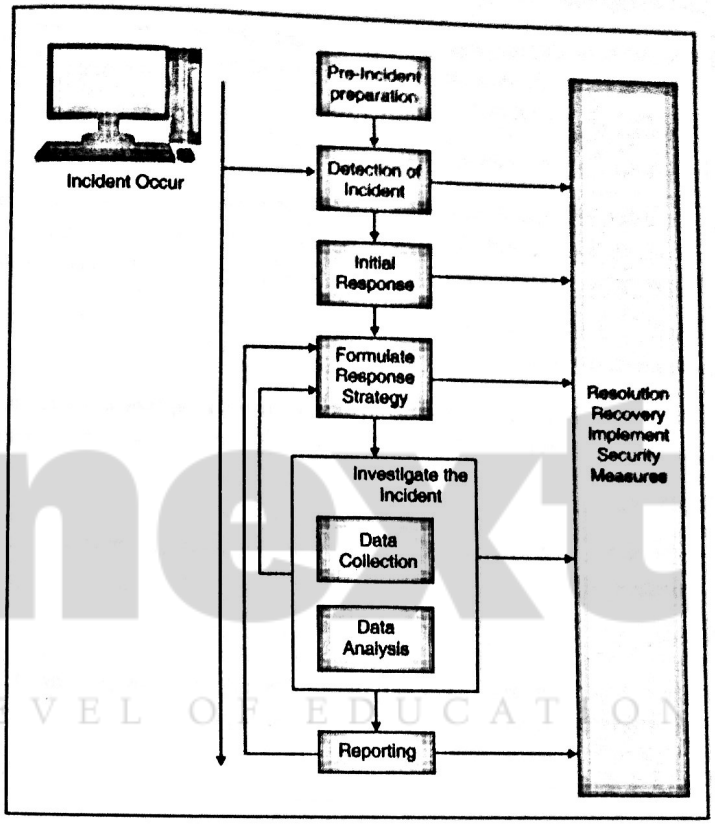

Fig. 1.2.1 : Incident Response Seven Components

In our methodology, there are seven important components of incident response :

1. Pre-incident preparation

In this phase actions are taken to prepare the organization and the CSIRT before an incident occur.

2. Detection of incidents

In this phase potential computer security incident is identified.

➜ 3. Initial response

In this phase an initial investigation is performed. The basic details surrounding the incident are recorded. The incident response team is assembled and individuals who need to know about the incident are notified.

➜ 4. Formulate response strategy

In this phase best response is determined and the management approval is taken based on the results of all the known facts. What types of civil, criminal, administrative, or other actions are appropriate to take are determined, based on the conclusions got from the investigation.

➜ 5. Investigate the incident

In this phase thorough collection of data. To determine what happened, when it happened, who did it, and how it can be prevented in the future is reviewed from the collected data.

➜ 6. Reporting

In this phase information is accurately reported about the investigation in a manner useful to decision makers.

➜ 7. Resolution

In this phase security measures are employed. For any problem procedural changes record lessons learned, and develop long-term fixes are identified.

1.2.3 Steps

1. Pre-Incident Preparation
   (a) Organization (b) CSIRT
2. Detection of Incidents
3. Initial Response
4. Formulate a response strategy
5. Investigate the incident
6. Reporting
7. Resolution

➜ 1. Pre-Incident Preparation

Preparation leads to successful incident response. Incident response is reactive in nature. In this phase there is need to prepare :

(a) Organization
(b) CSIRT

➜ (a) Preparing the Organization

Preparing the organization contains developing all of the company-wide strategies you want to employ to better pose your organization for incident response. This contains the following :

(a) Applying host-based security measures.
(b) Applying network-based security measures.
(c) Training end users.
(d) Hire an Intrusion Detection System (IDS).
(e) Creating strong access control.
(f) Performing timely vulnerability examination.
(g) Ensuring backups are done on a regular basis.

➜ (b) Preparing the CSIRT

The organization will gather a team of specialists to handle any incidents that arise. Preparing the CSIRT consists of considering at least the following :

(a) The hardware required to investigate computer security incidents.
(b) The software required to investigate computer safety incidents.
(c) The documentation like forms and reports required to investigate computer safety incidents.
(d) The ideal guidelines and operating tactics to implement your response techniques.
(e) The training required to perform the incident response to staff or employees.

2. Detection of Incidents

- The detection of incidents phase is one of the maximum critical elements of incident reaction.
- Detection of incident is a most decentralized phase. In this phase the incident response expertise have the least control.
- If any unauthorized or illegal thing happened involving organization computer network or data processing unit, the computer security incident are identified.
- At the initial stage the incident may be reported by an end user, detected by a system administrator, recognized by intrusion detection system or discovered by means of much other method.
- In most groups, end users may additionally document an incident through certainly one of three ways :
  (a) Their immediately supervisor,
  (b) The company help desk.
  (c) An incident hotline controlled by the Information Security entity.
- Normally technical issues are reported to the help desk by the end users. Issues related to the employee are reported to the Human Resource department.
- Prepare an initial response checklist to record the pertinent facts. This checklist list includes :
  - Current time and date of the incident
  - Who reported the incident ?
  - Nature of the incident
  - When the incident happened ?
  - What Hardware/software involved ?
  - Points of contact for involved personnel.
- This information is used by CSIRT from the initial response checklist to begin the next phase of the response process which is the initial response.

3. Initial Response

- Initial response is the first step of investigation. In this investigation step gather enough information to determine the proper response.

- The initial response phase consist of gathering the CSIRT, gathering network-based and other data, determining what type of incident that has occurred, and assessing the impact of the incident. The initial response phase document steps that must be taken.
- The individuals who are involved with detecting an incident actually begin the initial response phase. Whoever will detect or notify the incident this is their duty to document the details surrounding the incident.
- At the early stage in the process the control of the response should be forwarded to the CSIRT to take benefit the team's expertise; the more steps in the initial response phase performed by the CSIRT, the better. Initially initial response do not poke the affected system .
- The data collected during this phase consist of reviewing network-based and other evidence. This phase does the following tasks :
  - Interviewing system administrators.
  - Interviewing business unit personnel.
  - Reviewing intrusion detection reports and network-based logs to identify data that would support that an incident has happened.
  - The network topology reviewing and access control lists to determine if any ways of attack can be ruled out.
- The team must have to verify :
  - Incident has actually occurred,
  - Which systems are directly or indirectly affected,
  - Which users are involved,
  - The potential business impact.

4. Formulate a Response Strategy

- The goal of the response strategy formulation is to determine appropriate response strategy, given the circumstances of the incident.
- The strategy must have to take into account the political, technical, legal, and business factors that surround the incident. The final result depends on the objectives of the group or individual with responsibility for selecting the strategy.

Considering the Totality of the Circumstances

- Circumstances of the computer security incident affect the response strategies. Some factors need while deciding the resources required for investigating an incident.
- So the strategy must have to take into account whether to make a forensic duplication of pertinent systems, whether to make a criminal referral, whether to accompany civil litigation, and added aspects of your response strategy :
  - How critical are the affected systems ?
  - How sensitive is the compromised or stolen information ?
  - Who are the abeyant perpetrators ?
  - Is the incident known to the public ?
  - What is the level of unauthorized access achieved by the attacker ?
  - What is the obvious skill of the attacker ?
  - How many system and user downtime is required ?
  - What is the overall dollar loss ?

Considering Appropriate Responses

- The response strategy has consideration the organization's business objectives.
- The prepared business strategy should be approved by upper-level management and response strategy options should be quantified with advantages and disadvantages relative to the following :
  - Estimated dollar loss.
  - Network downtime and its impact to operations.
  - User downtime and its impact to operations.
  - Whether or not your organization is legally compelled to take certain actions.
  - Public announcement of the incident and its effect on the organization's reputation/business.
  - Theft of intellectual property and its potential economic impact.

Taking action

Organizations have to take action to discipline an employee. The organization also has to respond to a malicious act done by an outsider.

Legal action

There are two legal choices, one is to file a civil complaint or another is to notify law enforcement. Law enforcement involvement will results in reducing the autonomy that the organization has in dealing with an incident and cautious deliberation ought to arise earlier than you have interaction the precise government. The following standards have to be considered while identifying whether or not to include law enforcement in the incident response :

- Does the damage/cost of the incident merit a criminal referral ?
- Is it likely that civil or criminal action will accomplish the outcome desired by your organization ?
- Has the reason of the incident been reasonably established ?
- Does your organization have proper documentation and an organized report that will be conducive to an effective investigation ?
- Can tangible investigative leads be given to law enforcement officials for them to act on ?
- Does your organization know and have a working relationship with local or federal law enforcement officers ?
- Is your organization wishing to risk public exposure ?
- Does the previous performance of the individual merit any legal action ?
- How will law enforcement involvement impact business operations ?

Administrative Action

The administrative of an organization can discipline or terminate employees instead of initiating civil or criminal actions.

Following are some administrative actions to discipline internal employees :

- Letter of scolding.
- Immediate dismissal.
- Mandatory leave of absence for a specific length of time.
- Reassignment of job duties.

- Temporary reduction in pay to account for losses/damage.
- Public/private apology for actions conducted.
- Withdrawal of certain privileges, such as network or web access.

5. Investigate the Incident

The investigation phase involves determining who, what, when, where, how, and wh surrounding an incident. One can also conduct the investigation by, reviewin host-based evidence, network-based evidence, and evidence gathered traditionally.

Incident Action

- At the point when there is a DoS attack Contact upstream suppliers to endeavour recognize the possible wellspring of the DoS attack. On the off chance that t source is distinguished, consider informing law requirement to penetrate t obscurity of the attacker and/or end the activity. Your organization might likew look for the assistance of the source.
- ISP by asking for a break of "Terms of Service" of the ISP by the attacker. Outs attacker identify an IP address as the conceivable source and consider utilizing l requirement to puncture the secrecy behind the IP address.
- Ownership of tyke erotic entertainment your organization might be required inform law implementation. Contact legitimate direction and Human Resour promptly.

Computer security investigation can be divided into two phases :

(a) Data collection
(b) Forensic analysis

(a) Data Collection

- Data collection is the gathering of facts and clues that are considered during forens analysis. The data you gather forms the basis of your conclusions. Information gatheri includes a few extraordinary forensic challenges :
  - o You should gather electronic information in a forensically stable way.
  - o You are frequently gathering more information than you can read in your lifetime
  - o You should handle the information you gather in a way that ensures its integrity.

- The data you get amid the information accumulation stage can be partitioned into three key ranges : host-based data, system based data and other.

Host-based Information

- Host-based evidence contains logs, records, documents, and any other information that you get on a system and not gathered from network-based nodes. Host-based information might be a system backup.
- Host-based data collection is done in two ways: ***live data collection*** and ***forensic duplication***. In few cases, the evidence that is required to understand an incident is temporary or lost when the victim/relevant system is powered down. Such type of volatile data can give critical information when attempt to understand the nature of an incident.
- The first step of data collection is the collection of any volatile information from a host before this information is lost. This volatile data gives a "snapshot "of a system at the time you respond. The following volatile information is recorded :
  - o Date and time of the system.
  - o The applications currently running on the system.
  - o Network connections which are currently.
  - o Sockets which are currently open.
  - o The applications listening on the open sockets.
  - o The state of the network interface.
- Live response is performed to collect this information. A live response is can be performed when a computer system is still powered on and running.
- It means you can collect the information contained in these areas without impacting the data on the compromised device. There are three types of live response :

(i) Initial live response
(ii) In-depth response
(iii) Full live response

➜ **(i) Initial live response**

Initial live response collect only the volatile data from a target or victim system. An initial live response is usually done when you have wanted to conduct a forensic duplication of the media.

➜ **(ii) In-depth response**

In this response the CSIRT gather enough additional information from the target/victim system to decide a valid response strategy. Even the Non volatile information is collected like log files d to help understand the nature of the incident.

➜ **(iii) Full live response**

It is a full investigation on a live system. For forensic duplication all data for the investigation is collected from the live system which requires the system to be powered off.

☛ **Network-based Evidence**

Network-based evidence contains information gathered from the following sources :

- Intrusion Detection System logs.
- Consensual tracking logs.
- Non-consensual wiretaps.
- Pen-register/trap and traces.
- Router logs.
- Firewall logs.
- Authentication servers.

– An organization frequently performs network surveillance acquire evidence, and perceiv co-conspirators involved in an incident. It may be possible host-based auditing get fai network surveillance may fill in the gaps.

– Network surveillance permits an organization to accomplish a number of tasks :

- Confirm or dispel suspicions surrounding an alleged computer security incident.
- Gather additional evidence and information.
- Verify the scope of a compromise.

- Identify any other parties involved.
- Form a timeline of events happening on the network.
- Ensure compliance with a desired activity.

☛ **Other Evidence**

– It is the other information obtained from the people. Other evidences follow the traditional investigative techniques to collect the evidence.

– Other evidence you get when you collect personnel files, interview employees, interview witnesses, interview character witnesses, and document the information gathered.

➜ **(b) Forensic analysis**

– Forensic analysis reviews all the collected data. Forensic analysis review includes log files review, system configuration files, trust relationships, web browser history files, email messages and their attachments, installed applications, and graphic files.

– When you perform software analysis, review time/date stamps, perform keyword searches, and take any other necessary investigative steps.

– Forensic analysis also examines the information which has been logically deleted from the system to determine if deleted files, slack space, or free space contain data fragments or entire files that may be useful to the investigation.

➜ **6. Reporting**

– The most difficult phase in incident response process is reporting. The big challenge in reporting is to create reports that precisely describe the details of an incident.

– This reports should be understandable to decision makers, that can bear the wall of legal scrutiny, and that are produced in a timely manner. The guidelines for reporting are :

(i) Document immediately
(ii) Write concisely and clearly
(iii) Use a standard format
(iv) Use editors.

➜ **(i) Document immediately**

Document all investigative steps and conclusions which are necessary to document as early as possible It results in time saving and ensure that can be communicated more clearly to others at any time.

➜ **(ii) Write concisely and clearly**

Write down everything in such a way that it is easy to understand to everyone. Try to avoid the shorthand or shortcuts.

➜ **(iii) Use a standard format**

Build up a format for your reports and stick to it. Make forms, outlines, and layouts that sort out the response process and cultivate the recording of all relevant information. This makes report writing versatile, spares time, and advances exactness.

➜ **(iv) Use editors**

Recruit technical editors to read the forensic reports. This helps to develop reports that are conceivable to nontechnical personnel who affect your incident response procedure and resolution.

➜ **7. Resolution**

The objective of the resolution stage is to execute host-based, network-based, and procedural countermeasures to keep an incident from creating additional harm and to give back your organization to a protected, solid operational status.

The accompanying steps are frequently taken to determine a computer security incident :

- Identify your organization's top needs.
- Determine the way of the incident in enough detail to understand how the security occurred and what host-based and network-based remedies are required to address it.
- Determine if there are basic or systemic reasons for the incident that need to be addressed.
- Restore any affected or compromised systems.
- Apply corrections required to address any host-based vulnerabilities.

- Apply network-based countermeasures, for example access control lists, firewalls, or IDS.
- Assign responsibility for correcting any systemic issues.
- Track progress on all corrections that are required.
- Validate that all remedial steps or countermeasures are viable.
- Update your security policy and methods as needed to improve your response process.

1.2.4 Activities in Initial Response and Phase after Detection/Identification of an Incident

Q. 1.2.3 Explain the phase after detection of incident. *(Ref. Sec. 1.2.4)* **(5 Marks)**

The phase after detection of the Incident is Initial Response which is depicted in Fig. 1.2.2. This section discusses the activities of the initial response which is the phase after detection of an incident. In this section we will see what actions the organization will take after detecting the computer security incident.

Initial Response Phase

When computer security incident occurred the organization will face many challenges. So there is a need of process that supports the following :

- Quick and effective decision making.
- Quick gathering of information in a forensically sound manner.
- Proper escalation of the incident.
- Quick notification of the participants required to assemble your CSIRT.
- To meet the challenges, a documented and well-rehearsed process is required. Fig. 1.2.2 illustrates the initial response steps.

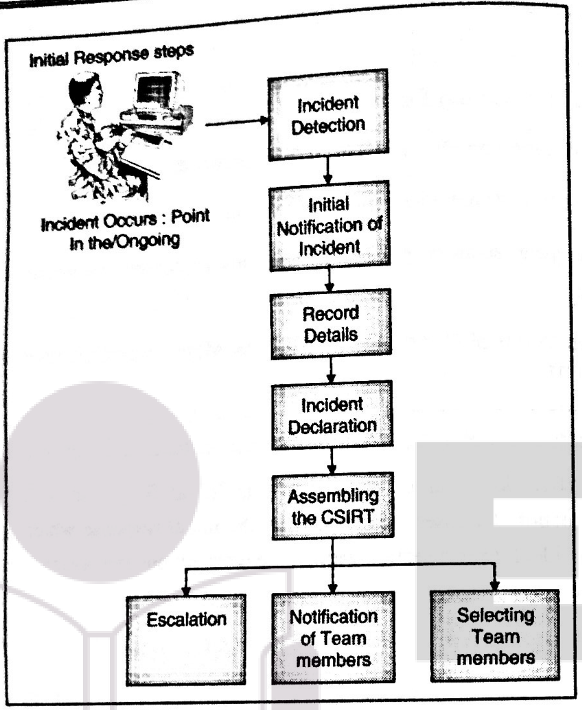

Fig. 1.2.2 : Initial response Phases

Obtaining Preliminary Information

The initial steps of any investigation are to get enough data to decide a proper respon That is the objective of the initial response stage. Your organization's initial response ought incorporate exercises, for example, the accompanying :

1. Receiving the initial notification of an incident.
2. Recording the details after the initial notification.
3. Assembling the CSIRT.
4. Performing traditional investigative steps.
5. Conducting interviews.
6. Determining whether the incident is highlighted or not.

Documenting steps to take

- The other reason for the initial response stage is to document steps that should be taken. By recording the subtle elements of an incident in a composed manner, your organization will have an exact number of the kind of attacks that happen, their recurrence, the harm brought about by these attacks, and the impacts these attacks had on your organization.
- Such measurements are basic to measuring the Return On Investment (ROI) for having a formalized incident response program.

1. Establishing an incident notification procedure

- To fabricate a strong incident response program participation of every one of your employees is required. In your organization incident response ought to be everybody's top priority. It is fundamental to build up a notification technique for clients to report potential computer security incidents.
- As a major aspect of your current security awareness program, you ought to advise the end clients of how to report incidents (by telephone, email, intranet site, or other system).
- Likewise, think about making as a computer security awareness notice that has the suitable instrument to report a potential computer security incident. Making the incident response handle clear to clients will maintain a strategic distance from confusion.

2. Recording the details after initial detection

To develop an organized incident response program checklists are required. So initial response checklist is there to record the details after the initial notification of an incident.

Initial response checklists

The initial response checklist is a mechanism of recording the circumstances surrounding a reported incident. The initial response checklist is divided into two separate sections :

(a) General information

(b) More specific details

(a) General information

General Information does not contain more technical information. This information is used to respond the end user the following information :

- Date the incident was detected.

- Contact information of the person completing the form.
- Contact information of the person who detected the incident.
- The type of incident.

➜ **(b) More specific details**

The members of the CSIRT use the checklist to address the technical details surrounding the incident. It is important for the CSIRT members to personally respond to obtain and record this information.

The initial response checklist is used to address the following issues :

- Make and model of the relevant system(s).
- System details.
- Operating system.
- The systems primary user.
- System administrator for the system(s).
- Network address or IP address of the relevant systems.
- The systems network name.
- Whether there is a modem connection to the system(s).
- Critical information that may have resided on the system(s).
- Incident containment.
- Whether the incident is in progress or ongoing.
- Whether network monitoring is required or being conducted.
- Whether the system is still connected to the Internet/network; if not, who authorized the removal of the system from the network and when it will be put back online.
- Whether backup tapes exist for the relevant systems.
- Whether there is a requirement to keep knowledge of the incident on a "need-to-know" basis.
- Whether any remedial steps have been taken so far (such as packet filtering, new access control lists, new firewall rules, or some other countermeasure).
- Whether the information collected is being stored in a protected, tamper-proof manner.

- Preliminary investigation.
- The IP addresses involved in the incident.
- Whether any investigative steps or actions have already been taken.
- Whether a forensic duplication of the pertinent systems needs to be made or a logical copy of the relevant system will do.

☛ **Case Notes**

- Checklists are too complicate. The alternative to checklist is case notes. Case notes is a documentation which records the steps that are taken during your incident response process.
- This is the duty of the member of CSIRT to maintain well-written notes of the details surrounding of the incident.

➜ **3, Incident Declaration**

It is important to understand that the reported activity is computer security incident. If you come across a suspicious activity which presents an incident but you are not sure about it then consider it as an incident until it is proven.

To avoid spending time on no incident, there are a few questions that can be considered :

- Was there a scheduled system or network outage that caused resources to be unavailable during the time the incident was reported ?
- Was there an unscheduled and unreported outage of a network service provider that caused resources to be unavailable during the time the suspected incident was reported ?
- Was the affected system recently upgraded, patched, reconfigured, or otherwise modified in such a way as to cause the suspicious activity that was reported ?
- Was testing being performed on the network that would lock out accounts or cause resources to be unavailable ?
- For insider incidents, are there any justifications for the actions an employee has taken that remove or lessen the suspicions ?

In case when incident is occur and you are not able to tell it immediately at this time assign the incident a case or incident number, making it a real incident worth investigating.

4. Assembling the CSIRT

- Several organizations form the e CSIRTs. Some CSIRTs are formed dynamically according a particular response to an incident, instead of an established, centralized team which is dedicated to responding to incidents.
- To prepare a team for a particular incident, organization have to identify the types of skills and resources required from the rest of the organization to respond to that particular incident.
- There is no need to go through notification procedures and increase of an incident until a certain incident occurred. Preparing the CSIRT requires the following activities :

(a) Determining increase procedures
(b) Implementing notification procedures
(c) Scoping an Incident and Assembling the appropriate resources.

(a) Determining escalation procedures

- There is no need of absolute response for every incident with an international CSIRT mobilized for the worst-case scenario.
- An assurance is required whether the incident handle at local level or at the corporate level. If there is an involvement of the internal employee in the incident then it will damage only local business unit.
- It does not include theft of trade secrets or disclose the data of client which is handled at local level. If outsider is involved in the incident then it affect multiple locations, so it is be handled at the corporate level.

(b) Implementing notification procedures

- The organization must a central point of contact for all detected or suspected incidents. Make this point of contact a permanent member of CSIRT who is well versed in your organization's acceleration and notification procedures.
- The points of contact for organization's CSIRT individuals should be set up much sooner than an incident happens. Maintain this information in a notification checklist. The notification checklist contains the information required to contact all the team members.

- The CSIRT members must have to know at what time use the recorded contact information recorded organization's notification checklist and when to notify the proper people an ongoing incident.
- Internal investigations often require diverse rules of notification than external security incidents. If you notify maximum people about the internal investigation then there are chances that the subject of investigation will find he/she is the centre of an investigation.
- Notification should involve only people that :
  - Need to know about the investigation.
  - Can really help with the investigation.
  - Will not be confused, panicked, or otherwise hinder the investigation.
  - Are not dear friend of the suspect.

(c) Scoping an incident and assembling the appropriate resources

Incident response needs quick decisions, and the speed at which you act regularly saves your organization time and money as well as reflects on its reputation. When you assemble the CSIRT the first step is to determine the specialist required for the work. The number and type of peoples on the team depend on these factors :

- How many workstations involved in the incident ?
- How many operating systems involved in the incident ?
- How many systems that are involved, vulnerable, or exploited ?
- Timeframe in which the investigation needs to be performed Potential exposure or profile of the case.
- Your organization's desire for a big or small investigative team.
- Whether or not litigation is probable?
- Whether it is an internal investigation?
- Whether the subject of the investigation is aware of the investigation?

5. Assigning a team leader

Organizations must have to select a team leader because all computer-related investigations require professionals who understand technical aspects of the incident as well as the investigative process for computer security incidents. To ensure that you have chosen an effective team leader, you should select someone who can perform the following tasks :

- Manage the organization's CSIRT during the entire response process.
- Manage the interview process when talking to witnesses, system administrators, end users, legal counsel, managers, and others.
- Provide status reports and communicate effectively to management on the progress of the response.
- Ensure that best practices and proper response techniques are used.
- Provide overall analysis of the incident.
- Protect the evidence gathered during the investigation in a manner consistent with your evidence guidelines and instructions.
- Take responsibility for verifying the chain of custody of evidence.
- Perform forensic duplication and analysis if necessary.
- Compile, manage, and present the investigative report and offer recommendations to management.
- Understand the legal issues and corporate policies.
- Provide an unbiased investigation with no conflict of interest.

Assigning Technical Staff

Smaller organizations that cannot have full-time CSIRT need to assign technical staff. There is a need to request support from other business units and create a CSIRT composed of the appropriate technical advisors. The technical advisors are employees or contractors who understand the details of the systems and the technologies involved in the investigation. These people want to possess the following characteristics :

- Knowledge of Complete operating system.
- Ability to review logs, audit trails, and other trace evidence and to clearly report findings.
- Knowledge of proper evidence-handling techniques.
- Ability to perform proper damage assessments.
- Ability to assist in determining the scope of an incident.
- Ability to determine the nature of the incident and identify the specific technical details that support their conclusions.
- Ability to make recommendations of how to remedy the situation.

- Capacity to maintain the perspective that technological evidence including audit trails, logs, core dumps, or live data collection may be critical to resolve the incident.
- Documentation skills to record all investigative steps clearly and concisely.
- Ability to support the team leader.
- Ability to perform interviews when needed.
- Once the CSIRT or investigative team is assembled, you are ready to begin the investigation.

6. Performing traditional investigative steps

The investigation phase involves determining the surrounding of an incident in the form of "who, what, when, where, how. There are two ways to simplify a technical investigation is to divide the evidence you collect into three categories :

(i) Host-based evidence
(ii) Network-based evidence
(iii) Other evidence

(i) Host-based evidence

For the host based evidence data is collected from Windows or Unix machines, or from the device actually involved in the incident.

(ii) Network-based evidence

Network-based evidence is collected from routers, IDS, network monitors. It may be possible that some network node not immediately involved in the incident.

(iii) Other evidence

Other evidence means testimonial data that contributes to the case, for example motive, intent and or some other digital evidence. It also consists of other information gathered from the people. This is when you gather personnel files, interview employees, interview incident witnesses, interview character witnesses, and document the information gathered. Other information can include voicemail systems, time cards, card swipe data, physical security logs, video camera tapes, employee records, telephone call logs, and fax logs.

7. Conducting interviews

When your CSIRT come across of a suspected incident, the first step is to start asking the questions like what, who, when, where, and how". These questions helps you to determine some facts surrounding the incident, for example the location of relevant systems, administrative contacts, what may have occurred and when etc. it may be possible that there may be no answer for some questions but if you gather more answers it helps to assess the situation. Some few important questions to ask while forming your initial assumptions about an incident :

- What happened ?
- When did it happen ?
- What systems are relevant/compromised/involved ?
- Who may have done it ?
- Who uses the affected/relevant systems ?
- What actions have already been taken ?
- What is the corporate policy on such an incident ?

Getting Contact Information

- During the interview collect each individual's information like Full name, Job title, Company name, Phone number, Email address.
- This identifying data is critical if you need to contact these people for additional information. When you prepare your report, you should include all the contact information for each person who provided you with information.

Interviewing System Administrators

- Many incidents results in failure after a discussion with the system administrator or the user. This is true when notification of the suspected incident comes from firewall logs, for example IDS detecting failed login attempts, at that point a fruitful login by means of telnet.
- The source address is registered to a home DSL provider. The notification checklist questions are helpful, but do not analyze the situation.
- The user may easily resolve the situation by describing that a telnet privy was made up to implement administrative duties. Conversely, if the system administrator has no idea of the logins, and remarks that telnet was not build to allow connections from the Internet, an incident has occurred and a response is necessary.

Here are some random questions for system administrators :

- Have you noticed any recent inappropriate activity?
- How many of them have administrator access to the system?
- Which applications provide isolated access on the system?
- What are the logging capabilities of the network and system?
- What safety measures for security of the system are taken?

Interviewing Managers

Managers regularly have advantageous bits of knowledge into the business impact and harm caused by security incidents interviewing manager is often critical to determine what risks are involved with the security incident and what damage was truly done. Following are some sample questions for managers :

- Is there anything particularly sensitive about the data and applications on the system?
- Are there any personnel issues of which we should be aware?
- Was any type of penetration testing authorized for the system or network?
- What is the worst case scenario that can play out based on what you know about this incident?

Interviewing End Users

End users may provide pertinent information when he reports the suspicious activity. End users describe anomalous behaviour on the system in a helpful way.

8. Formulating a response strategy

Here we consider the steps to recover from the incident. It also includes initiating adverse action against an internal employee or an external attacker.

Response Strategy Considerations

- Response strategy considers everything you know about the incident. Response strategy changes over time, and then factor in the legal, political, technical, and business influences that should be considered.
- Response strategy is an iterative process. Final response strategy is implemented after going through so many options.
- For determining your response strategy following are some common factors you have to consider.

- Does your organization have a formal/public posture on responding to attacks that it must adhere to in order to appear consistent to customers and the media?
- Is the suspected attack from overseas, making it more difficult to pursue technically and legally ?
- Is the strategy worth pursing from a cost/benefit standpoint?
- Are there any legal considerations that may affect the response?
- Can you risk public disclosure of the incident to clients or to the public?
- How have you enforced same incidents in the past?
- What is the past record/work performance of the individual(s) involved?
- Will the investigation cost more than merely allowing the incident to continue?

Policy Verification

- In the initial assessment first steps taken is to determine the existing policy. The policy which addresses the two fundamental needs of the investigator: network monitoring and computer forensics examination of computer systems got the highest priority.
- Monitoring may be limited, without appropriate policy or banners on systems. It is also necessary to make sure that any existing acceptable use and consent to monitoring policies apply to your situation.

Syllabus Topic : Recovery of Erased and Damaged Data

1.3 Recovery of Erased and Damaged Data

Q. 1.3.1 Explain the techniques used to recover erased or damaged data. **(5 Marks)**

(Ref. Sec. 1.3)

- In computer forensics it is necessary to recover information that is erased, deleted and damaged. Users, companies/organizations, and government Agencies use data recovery for different reason. data recovery is an important part of Computer forensic.
- There are different data recovery techniques available, but maximum of the techniques are not related to the computer systems. Nowadays data recovery is most often related to the computer system.

- There are many misconceptions related to deleted/erased or damaged files.
  1. When the data is removed from the system that data is deleted or overwritten, but there are different techniques available to recover the deleted data.
  2. Deleting the file doesn't means the data is gone permanently, operating system simply remove the pointer of that file but data is still present there and the new data can be written in this place.
  3. On the magnetic media data is recorded in the form of zeros and ones when this data is overwritten, the disk detects only the new data leaving only remnants of the old data. Reading the remnant is time consuming and the old data would not be read correctly. this is very problematic and impossible to solve.

There are different reasons of different users behind data recovery:

End users

The end users wanted to recover the files which they have deleted accidentally and the files that have been compromised due to **Hardware failure and**

Malicious activity

Companies/organizations

Companies wanted to recover the data from the ex-employees computer or to recover the lost files due to Hardware failure and Compromised or lost due to network problem.

Government Agencies

Government Agencies wanted to recover the data from the ex-employees computer or to recover the lost files due to Hardware failure or network problem.

Law Enforcement Agencies

Law Enforcement Agencies needs to recover evidence from a suspect's computer, recover data from hard drive, find out the motive of the crime, to find out the any co-conspirator and to support **forensic analysis of computers.**

Techniques used to recover erased or damaged data :

- Carry out a forensic analysis of the computer.
- Search for single file type.
- Attack encryption methods.
- Use the existing image to restore the disk.

- Inspect data in Random Access Memory (RAM)
- Inspect disk at the cluster level or sector level
- Analyze data using hex editor
- create hash of whole disk and export it in another tool for use.

Types of Damages

There are two types of damages :

1. Physical damage
2. Logical damage.

1. Physical damage

- Physical damage means scratches on CD's, breaking of tapes and mechanical problem i hard disk.

2. Logical Damage

- Logical damage is mainly caused by power interruption that does not let the file to b completely written to the storage device. It results in an inconsistent state of file, total dat loss, system crash, Strange behavior and Partial storage of data.

Tools used for data recovery are :

- WinHex
- Forensic Tool Kit (FTK)
- Encase

1.3.1 Recovering Deleted Files on Windows Systems

Q. 1.3.2 How Linux tools use to recover files on FAT file systems **(5 Marks**
(Ref. Sec. 1.3.1)

Q. 1.3.3 How deleted files recover on Windows systems **(5 Marks**
(Ref. Sec. 1.3.1)

- Many times you want to clear the unallocated space on a restored forensic image in ord to undelete or recover as many files or file fragments as possible. You also want recover the evidence which was deleted by attacker.

- In this section, we going to study different ways to obtain files, for all intents and purposes, suspects would believe no longer exist. As you probably know, deleted files are not truly deleted; they are merely ***marked*** for deletion.
- For example, when a file or directory is deleted from a FAT file system, the first letter of its filename is set to the sigma character (Ó), or, in hex, 0xE5. This means that these files will remain intact until new data has overwritten the physical area where these deleted files are located on the hard drive.
- Special tools can find these "intact" deleted files and recover them for review. After a file has been marked for deletion, each hard drive I/O could overwrite the data you want to recover.
- To recover the file on windows system we use following tools :

1. Windows based tools : Encase, FTK
2. Linux tools: Fatback, TASK, and Foremost

1. Windows-Based Tools to Recover Files on FAT File Systems

EnCase and FTK are the tools of the windows system for recovering files on FAT filesystems. Both EnCase and FTK have this capability built-in, and they automatically recover any files they can.

2. Linux Tools to Recover Files on FAT File Systems

Three Linux utilities that can recover data : Fatback, TASK, and Foremost.

FatBack to Recover Deleted Files

Fatback is used to recover the deleted files from the Fat System. Fatback also performs file recovery on FAT12, FAT16, and FAT32 file systems from a Linux forensics platform. Following are the features of Fatback :

(a) It supports the Long filename.

(b) There is recursive undeletion of directories.

(c) Lost cluster chain recovery.

(d) It can work within single partitions or entire disks.

Fatback is flexible because it works on image files as well as devices Fatback installation is easily on Linux and FreeBSD systems.

To recover the deleted file from an image of an evidence floppy, the following Fatback command-line options are used :

(a) -a : This option runs Fatback in automatic undelete mode.

(b) -o : This option places recovered files into the specified directory

(c) -s : This option tells Fatback to treat the input file *evidencefloppy.bin* as a single Partition, since all floppy drives have only one partition.

Using TASK to Recover Deleted Files

- TASK is a tool used to recover the deleted files. It is open-source forensic toolkit. It is used to analyze Microsoft and Unix file systems. TASK can recover files from different file systems, including FAT, FAT12, FAT16, FAT32, FreeBSD, EXT2, EXT3, OpenBSD, and UFS. TASK can work on binary images which do not have embedded checksum values.
- TASK cannot work on EnCase evidence files and SafeBack files. TASK works with only a single partition so image each partition on a drive separately in order to use this tool. TASK is used to recover previously deleted files in your binary image file created by dd.
- One can also use autopsy forensic browser for analyzing allocated files, previously deleted files, directories, data units, and metadata of forensic images in a read-only environment.

Using foremost to Recover lost files

- Foremost is a Linux program used to recover or files based on the file headers and footers. Foremost is a portable, exceptional tool for data recovery. Foremost can work on forensic image files such as those generated by dd, SafeBack, and Encase, or act directly on a device.
- Foremost consults a configuration file at runtime. This configuration file specifies the headers and footers that Foremost is looking for, so you can choose which ones you want to look for simply by editing the *foremost.conf* file.
- The Foremost can find GIF files, JPG files, common Microsoft Office documents, email repositories, HTML pages, PDF files, ZIP files, Windows Registry files, WordPerfect files, and even America Online (AOL) mail files.

1.3.2 Recovering Deleted Files on Unix Systems

- *Recovering previously deleted files on Unix systems can be quite a challenge. Since most of the files you attempt to recover on Unix systems are flat text files.*

- For recovering previously deleted files in Unix system you can use **debugfs** on files stored on the ext2 (second extended file system) file system.
- Debugfs is a very powerful tool in the hands of the computer forensic examiner. It is an interactive file debugger used to examine and to change the state of the ext2 file systems.
- The debugfs provides the best means for recovering files on media using the ext2 file system.

1.3.3 Recovering Unallocated Space, Free Space and Slack Space

- After doing the forensic duplication of media and recovering as many files as you can, there is still data left on the evidence media that you will want to review.
- The remaining data is stored in ***slack space***, ***unallocated space***, and ***free space***. In order to understand slack space and unallocated space, we must first review what an ***allocation unit*** or ***cluster*** is.

Cluster

- Operating systems arrange all data stored on a hard drive into segments called allocation units (also called *clusters*). For example, an operating system that uses 32K clusters reads and writes data from a hard drive 32K at a time. It cannot read less than 32K of data from a hard drive, and it cannot write less than 32K at a time to the hard drive.
- However, very few files have the exact amount of data to occupy an entire cluster or set of clusters. Therefore, when an operating system that writes 32K clusters to a hard drive is being asked to save a 20K Microsoft Word document, there is 12K of unused space called ***file slack***. In our example, there may be remnants of previous files in this 12K of file slack.

Unallocated space

- Unallocated space is the area of the hard drive which is not currently allocated to a file. Sections of deleted files are frequently scattered crosswise over unallocated space on a hard drive. ***Free space*** is the segment of the hard drive media that is not inside of any currently active partition.
- MS-DOS tools have been written that examine the information on a hard drive and create files that contain all the information inside of the unallocated space, free space, and slack space on a drive. To write the contents of slack space and free space to a file the NTI'S tools are used.

- These tools are powerful and simple. The tools EnCase and FTK automatically uncove slack space and unallocated space on the qualified forensic duplication. The advantage o these tools is there is no need to restore the original evidence to its own hardware.

Syllabus Topic : Disk Imaging and Preservation

1.4 Disk Imaging / File duplication and Preservation

Q. 1.4.1 What is disk imaging ? *(Ref. Sec. 1.4)* (5 Marks)

Q. 1.4.2 What is mirror image ? *(Ref. Sec. 1.4)* (5 Marks)

- Disk Imaging makes a large compressed file of your drive. You can restore this data t drive. Image file is large in size and maximum people store it to external drives or file shares. The disk imaging software's creates the exact copy of the hard disk. The forensi image consists of Deleted files, system files, slack space and executables.
- ***A disk imaging/ duplication*** is a file that contains every bit of information from th source, in a raw bit stream format. A 5GB hard drive would result in a 5GB forensi duplicate.
- No extra data is stored within the file, except in the case where errors occurred in a rea operation from the original. When this occurs, a placeholder is put where the bad dat would have been. A forensic duplicate may be compressed after the duplication process.
- The tools that create a forensic image are :
  1. Unix dd command
  2. dfcldd (U.S. Department of Defense (DoD) Computer Forensics Lab version of th dd command).
  3. open-source Open Data Duplicator (ODD) e.g. FTK imager

1. Qualified Forensic Duplicate

- A qualified forensic duplicate is a file that contains every bit of information from th source, but may be stored in an altered or changed form. Two examples of altere paperwork are in-band hashes and Empty Quarter compression.
- A few equipments will examine in some of sectors from the supply, generate a has from that group of sectors, and write the world organization, accompanied via th hash value to the output document.

- This approach works very well if something is going wrong in the course of the duplication or recovery of the reproduction. If a quarter groups fail to fit the hash cost generated for it, the recovery can continue, and the analyst is conscious that records from that area organization may be invalid. If a similar state of affairs came about with a forensic duplicate file, the place of the mistake may be unknown, probable invalidating the entire reproduction.
- Empty Quarter compression is a not unusual technique for minimizing the dimensions of the output document.
- If the tool comes throughout 500 sectors, all filled with zeros, it will make a unique entry inside the output file that the healing application will recognize.
- Three tools that create qualified forensic duplicate output files are :
  1. SafeBack
  2. EnCase.
  3. FTK imager

2. Restored Image

- A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium. The restoration process is more complicated than it sounds.
- For example, one method involves a blind sector-to-sector copy of the duplicate file to the destination hard drive. If the destination hard drive is the same as the original hard drive, everything will work fine. The information in the partition table will match the geometry of the hard drive.
- Partition tables will be accurate; if the table says that partition 2 starts on cylinder 20, head 3, and sector 0 that is where the data actually resides. But what if the destination hard drive is not the same as the original hard drive? If you restore the forensic duplicate of a 2.1GB drive to a 20GB drive, then the geometries do not match.
- In fact, all of the data from the original drive may occupy only three cylinders of the 20GB destination drive. The partition that started on cylinder 20, head 3, and sector 0 on the original drive may actually start on cylinder 2, head 9, and sector 0.
- The software would look in the wrong location and give inaccurate results. How does the restoration software compensate for this? As the forensic duplicate is restored to the destination hard drive, the partition tables (in the master boot record and partition boot sectors) are updated with the new values.

- Is the restored image an exact duplicate of the original? If the analyst generates hashes of the restored image, will they match the original?
- The answer is no in both cases. Is the data on the restored image still a true and accurate representation of the original? For the purposes of analysis, yes.
- The method of updating the partition tables on the destination hard drive is not reliable. When hard drives grew beyond 512MB, the PC-BIOS manufacturers were scrambling to update their software to recognize such huge drives. Hard drive manufacturers came up with a way around the problem.
- Instead of forcing everyone to buy new motherboards with updated BIOS code, they released software that emulated modern BIOS. This software would "push" all of the real data on the drive down one sector and store its program and information in sector 1. The real partition table would be at cylinder 0, head 0, and sector 2.
- When the software restored the forensic duplicate to a large destination drive, it would not update the correct table, leaving the restored image relatively useless. Most forensic processing software will detect this drive overlay software and create a valid restored image.
- The following tools are used to create a restored image from the qualified forensic duplicate :
  1. SafeBack,
  2. EnCase,
  3. dd
- Depending on your method of analysis, EnCase and dd images may not need to be restored. EnCase, the Forensic Toolkit, treats the images as virtual disks, eliminating the need for restoration.

3. Mirror Image

- A mirror image is created from hardware that does a bit-by-bit copy from one hard drive to another. Hardware solutions are very fast, pushing the theoretical maximum data rate of the IDE or SCSI interfaces.
- Investigators do not make a mirror image very often, because it introduces an extra step in the forensic process, requiring the examiner to create a working copy in a forensically sound manner. If your organization has the ability to keep the original drive, seized from the computer system being investigated, you can easily make working copies.

- If the original drive must be returned (or never taken offsite), the analyst will still be required to create a working copy of the mirror image for analysis.
- The small amount of time saved onsite is overshadowed by the overhead of making a second working copy. We will not cover the process of creating a mirror image of evidence here. Most hardware duplicators are relatively simple to set up and operate.
- Two such duplicators are Log cube's Forensic SF-5000 and Intelligent Computer Solutions' Image MASSter Solo-2 Professional Plus. You do need to ensure that the hardware duplicator actually creates a true mirror image.
- Many duplicating machines on the market are made for systems integration companies who use them for installing operating systems on large numbers of hard drives. When used in this capacity, the hardware device will typically alter items in the boot and partition blocks to ensure that the partitions fall on cylinder boundaries.
- This alters the resulting image, which means that you do not walk offsite with an exact duplicate of the original. As with any process, test it thoroughly before you need to rely on it.

1.4.1 Forensic Duplication/Disk Imaging Tool Requirements

Q. 1.4.3 What are the forensic duplication tool requirements ? *(Ref. Sec. 1.4.1)* (5 Marks)

- Expanding on the legal standards that are set up to control the tolerability of expert affirmation, we trust that a legal duplication tool must prove itself in the accompanying areas :
  1. The tool must be able to image all of information on the storage medium.
  2. The tool must make a forensic duplicate or mirror image of the original storage medium.
  3. The tool must handle read errors in a vigorous and elegant way. In the event that a process fails after repeated endeavours, the error is noted and the imaging process proceeds. A placeholder might be placed in the output file with the same dimensions as the portion of the input with errors. The contents of this placeholder must be archived in the tool's documentation.
  4. The tool must not make any changes to the source medium.
  5. The tool must be able to be involved to scientific and peer review. Results must be repeatable and certain by a third party, if essential.

– Action and error logs are crucially important also. The more data logged by the tool amid operation, the less demanding your occupation will be the point at which you record the procedure.

1.4.2 Creating a Forensic Duplicate of Hard Drive

Q. 1.4.4 How to create a forensic duplicate of hard drive. *(Ref. Sec. 1.4.2)* **(5 Marks)**

To create the forensic duplicate of hard drive the following tools are used.

1. dd and dcfldd
2. ODD (Open Data Duplicator)

➜ **1. Creating forensic duplicate using dd and dcfldd**

– The dd tool is the part of the GNU software suite, afterwards dd was improved by th programmers and re-released as dcfldd. The dd tool is very reliable to create the tru forensic duplicate.

– The dd tool performs a complete bit-by-bit copy of the original. While using the tool simply transposing a single character may destroy evidence, so one must have t be familiar with the dd tool before using it as well as with the Unix environme address storage devices.

– The steps require for duplicating hard drive using dd are :

1. Create a boot media
2. Perform the duplication with dd. In some situations the duplication is stored the series of the files which are sized to fit on a specific media type or f system type, we call this as segmented image. So do the following things perform the duplication.
   - o Write the script to perform hard drive duplication.
   - o Write down the source device name.
   - o Write down the output file name and set the output file size.
   - o Use the dd command.

– It is also possible to create the duplicate without splitting the output file in Linux. create such type of duplicate calculate MD5 sum of the entire drive in one pass o the source hard drive.

➜ **2. Creating forensic duplicate with Open Data Duplicator (ODD)**

– The Open Data Duplicator (ODD) is an open-source tool which follows the client server model. This client server model allows the investigator to perform forensic duplications on a number of computer systems simultaneously over a local LAN.

– We can use the software on a single forensic system because both halves can be run on the same computer system. ODD can perform additional functions on the data as it is being processed. ODD includes modules (plug-ins) that will calculate checksums and hashes, perform string searches, and extract files based on the file headers.

– The ODD package is having three portions :

- o **Bootable CD-ROMs :** These are similar to the Trinux Linux distribution.
- o **Server-side application :** The server will perform most of the processing of the duplicate image, including the calculation of hashes, string searches, and the storage of the true forensic duplication.
- o **Client-side application :** This portion may be run locally if you are duplicating drives on a forensic workstation.

– When we perform the forensic duplication of hard drive using ODD. Firstly it detects the location of the ODD server. Then the ODD server detects the device and files which we can use to direct ODD for the duplication of some portions. After detecting the device the next step is processing.

– The process stores the forensic image and performs simple string searches and extracts certain types of files based on their file headers. We also manage some notes using the Notes plug in which give the information like the case number, the computer's date and time, the actual date and time, and the system description.

– Then we use the Carv plug-in to extract a certain number of bytes from the incoming data stream, based on file headers. For example, we have selected gif and jpg for extraction, once the duplication has completed, the carved files may be found in a directory on the ODD server.

1.4.3 Creating Qualified Forensic Duplicate of a Hard Drive

Q. 1.4.5 How to create a qualified forensic duplicate of hard drive ? *(Ref. Sec. 1.4.3)* **(5 Marks)**

– It is must to know as an investigator that never boot from the evidence drive. Many items on the evidence media can be altered; starting from the moment the BIOS executes the boot block on the hard drive.

- In the initial boot process, file access timestamps, partition information, the Registry configuration files, and important log files may be changed in a matter of seconds. The qualifier "forensic" implies that the copy is a true copy, that is, the bit stream from the original and the duplicate are the same.
- In order to certify this, one can compare the original and duplicate bit-by-bit, or one can speed up the process by using signatures, also known as a hash. A signature is a small piece of data, typically between 4 and 22 bytes long calculated from the contents of a sector, a track, a file, or a whole hard drive.
- 32-bit cyclic redundancy codes SHA1 use an algorithm to generate the signatures that is so complicated that it is computationally impossible (i.e. it just takes too long) to generate a sector, block , track, or file that has the same signature as a given sector, block, track, or file.
- A good duplication tool will have some way of proving that the duplicate is true, typically by calculating the signature.

1. Creating a Boot Disk

- A clean operating environment is required for imaging a system. For doing this imaging DOS applications like SafeBack or EnCase is used it means that you must create an MS DOS boot disk. The following command will format and copy the system files to a floppy :

```
C:\format a:\ /s
```

- There should be four files in the root directory of the floppy. These files contain the code to get the computer running a minimal operating system and these four file are IO.SYS, MSDOS.SYS, and COMMAND.COM. DRVSPACE.BIN.
- The computer first process the IO.SYS file and then the code in IO.SYS loads the contents of MSDOS.SYS and begins to initialize device drivers, tests and resets the hardware, and loads the command interpreter, COMMAND.COM.
- During the process of loading device drivers, if a disk or partition connected to the machine uses compression software then IO.SYS loads the DRVSPACE.BIN driver file.
- When the driver loads it mount the compressed volume and present the operating system with an uncompressed view of the file system.
- When it mounts the compressed volume, it changes the time/date stamps on the compressed file; it means that the evidence will be altered. These files are required to you.

- When you boot from your clean boot disk, you want to make sure that the loading of the DRVSPACE.BIN driver file fails. Simply removing the file is a good start, but IO.SYS is smart enough to check the root directories of all active partitions for the file.
- The most effective way to prevent the loading of DRVSPACE.BIN is to load IO.SYS into a hex editor and alter the strings manually. Perform the string search operation in word space.
- Notice that the period in the filename is not represented in the executable file. Continue to search the file for the SPACE string. There are four instances in IO.SYS that will need to be changed. When you are finished, save the file and exit the hex editor.
- On the safer side remove the DRVSPACE.BIN file from the floppy as well. After you've created the clean boot floppy, copy over any DOS mode drivers that you will need to access the hard drives on the computer system under investigation.
- The best source for DOS drivers is the web site for each hardware manufacturer, rather than on the driver CD that ships with the product.

2. Use Encase tool

- Encase is a totally high-priced, but very surprising windows based Forensics suite that consists of the making of certified forensics duplicates.
- Being home windows based totally makes Encase easy to apply, however it additionally introduces a few issues, approximately the OS spotting suspect drives and inside the procedure changing their contents. This doesn't imply of direction - that Encase should ever generate person information.
- Encase strength lies in their seamless integration of all forensics investigation obligations. Encase generates a certified forensics duplicate.

3. Use Safe back tool

- Safe back is small software program software that is positioned on a DOS boot disk (normally a floppy, however this could be changing as floppy drives die out).
- It offers options on the kind of duplicate, a real forensics duplicate or a reflect. We will need to have a clean DOS

Syllabus Topic : Data Encryption and Compression

1.5 Data Encryption and Compression

Q. 1.5.1 Explain data encryption and compression ? *(Ref. Sec. 1.5)* **(5 Marks)**

A few criminals are becoming smarter. So data-hiding techniques which includes ***encryption*** and ***steganography***. The evidence of criminal activity is placed in such a way where traditional search methods cannot able to find it.

Encryption

- Scrambling data, for example an e-mail message, so that it cannot be readable to the interceptor. Many publically available programs permit the user to create virtual encrypted disks which are opened by selected key. It is not possible to read the encrypted data without the key.
- When you encrypt a file, only contents of the file get encrypted but the name of the file, size and the timestamps are unencrypted. It is possible to build the parts of the content of the file from other locations, such as swap file, temporary files, and deleted, unencrypted copies.
- In computer forensics many encryption program with extra function makes the investigation difficult. Few functions include use of a key file, plausible deniability, and full-volume encryption.

Steganography

- It is nothing but hiding a message into a larger file, typically in a photographic image or sound file. Steganography has the capability of disrupting the forensic process when used correctly.
- In computer forensics to preserve the data evidence MD5 is used for data integrity and cryptcat is used to encrypt the data which is transferred via net.

Data Compression

- Many computer users use the compression tools like WinZip, Alzip and WinRAR. These are the widely used compression tools and support many compressed formats. These tools are mainly used for archiving purposes.
- DEFLATE algorithm is the main compression algorithm for WinZip and Alzip. WinRAR uses a modified version of this DEFLATE algorithm.

- For example, .zip, .gz and .alz are extensions of the given compression algorithms which use the DEFLATE data compression algorithm.
- The dual algorithm for decompression is known as INFLATE. Since the DEFLATE and INFLATE algorithms are common among compression utilities these are used for damaged compressed file recovery methodology.

Syllabus Topic : Automated Search Techniques

1.6 Automated Search Techniques

Q. 1.6.1 Write short note on automated search techniques. *(Ref. Sec. 1.6)* **(5 Marks)**

The searching techniques are used to find out whether the given type of object, such as hacking tools, or pictures of specific type, are there in the collected information.

There are two levels of search automation techniques, they are :

1. Manual browsing
2. Automated searches
   - (i) keyword search,
   - (ii) regular expression search,
   - (iii) approximate matching search,
   - (iv) custom searches,
   - (v) Search of modifications.

1. Manual browsing

- In manual browsing the forensic analyst browses gathered information and selects objects of preferred type.
- The single tool used in manual browsing is a watcher of some type. It takes a data object, for example, file, decodes it and gives the result in a human-comprehensible form.
- Manual browsing is time consuming and slow as there is large amount of data is gathered in maximum investigations.

➜ **Automated searches**

➜ **(i) Keyword search**

- Keyword search is an automatic search of digital information that consists of specifi keywords. It is easy and widely used technique and it speedup manual browsing. Th output of keyword search is the list of found data objects.

There are two problems with keyword search :

(a) False positive

Keyword searches do not precisely gives the required type of data objects, due t this, output of keyword search can have false positives, it mean the objects that d not belong to the specific type even though they contain specified keywords Forensic analyst has to browse the keyword search data objects manually to remov false positives

(b) False negative

False negative means there are objects of given type but they are missed by search. I the search utility cannot correctly interpret the data objects then it results in fals negative. This may happen due to encryption, compression, or lack of ability of th search utility to interpret new data.

It set (1) to select words and phrases highly precise to the objects of the required typ like particular names, address, bank account number, etc and (2) to give ever possible variation of these words

➜ **(ii) Regular expression search**

- Regular expression (RE) search gives more expressible language for describing objects o interest than keywords. RE is an extension of keyword search. RE searches are also use to specify searches for e-mail addresses, and files of precise type.
- Encase tool is used to perform regular expression searches. As not all the type of data ca be sufficiently described using regular expressions, like keyword searches it also results i false positives and false negatives.

➜ **(iii) Approximate matching search**

- Approximate matching search is an expansion of regular expression search. It us matching algorithm. These algorithms allow character mismatches while searching f keyword.

- Here user has to specify the degree of mismatches allowed. This search detects the misspelled words, but it gives mismatches and raises the number of false positives. The agrep is used for approximate search.

➜ **(iv) Custom searches**

- The regular expressions have limited expressiveness. The programs are written for the more complex searches, for example, the FILTER_1 tool from new Technologies Inc.
- This tool uses heuristic procedure to find full names of persons in the gathered information. FILTER_1 tool also suffers from false positives and false negatives.

➜ **(v) Search of modifications**

- Search of modification is used for data objects that have been modified since specified instant in the past.
- The modification of the data objects that are not frequently, such as operating system utilities, these utilities are detected by comparing their current hash with their expected hash. Before the search a library of expected hashes is built.
  - Some tools for building libraries of expected hashes are given in the "file hashes" Modification of a file can likewise be construed from adjustment of its timestamp. Albeit conceivable in many cases, this adjustment is circumstantial.
  - Investigator assumes that a file is constantly modified concurrently with its timestamp, and since the timestamp is adjusted, he induces that the file was changed as well. This is a type of event reconstruction

Syllabus Topic : Forensics Software

1.7 Forensics Software

Q. 1.7.1 Explain the forensic softwares. *(Ref. Sec. 1.7)* **(5 Marks)**

The computer forensic tools performs the tasks : collection, preservation, analysis and presentation of computer-related evidence. The following are some forensic tools: (https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/)

1. SANS SIFT

- The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu based Live CD which includes all the tools you need to conduct an in-depth forensic or incident response investigation.
- It supports analysis of Expert Witness Format (E01), Advanced Forensic Format (AFF), and RAW (dd) evidence formats. SIFT includes tools such as log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.

2. CrowdStrike CrowdResponse

- CrowdResponse is a lightweight console application that can be used as part of an incident response scenario to gather contextual information such as a process list, scheduled tasks, or Shim Cache.
- Using embedded YARA signatures you can also scan your host for malware and report if there are any indicators of compromise.

3. Volatility

- Volatility is a memory forensics framework for incident response and malware analysis that allows you to extract digital artefacts from volatile memory (RAM) dumps.
- Using Volatility you can extract information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives, process IDs, and more.

4. The Sleuth Kit (+Autopsy)

- The Sleuth Kit is an open source digital forensics toolkit that can be used to perform in-depth analysis of various file systems. Autopsy is essentially a GUI that sits on top of The Sleuth Kit.
- It comes with features like Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching out of the box, with the ability to add other modules for extended functionality.

5. FTK Imager

- FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images or memory dumps.

- Using FTK Imager you can also create SHA1 or MD5 hashes of files, export files and folders from forensic images to disk, review and recover files that were deleted from the Recycle Bin (providing that their data blocks haven't been overwritten), and mount a forensic image to view its contents in report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.

6. ExifTool

- ExifTool is a command-line application used to read, write or edit file metadata information. It is fast, powerful and supports a large range of file formats (although image file types are its speciality).
- ExifTool can be used for analysing the static properties of suspicious files in a host-based forensic investigation, for example.

7. Free Hex Editor Neo

- Free Hex Editor Neo is a basic hex editor that was designed to handle very large files.
- While a lot of the additional features are found in the commercial versions of Hex Editor Neo, I find this tool useful for loading large files (e.g. database files or forensic images) and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.

8. Bulk Extractor

- bulk_extractor is a computer forensics tool that scans a disk image, file, or directory of files and extracts information such as credit card numbers, domains, e-mail addresses, URLs, and ZIP files.
- The extracted information is output to a series of text files (which can be reviewed manually or analysed using other forensics tools or scripts).

9. DEFT

- DEFT is another Linux Live CD which bundles some of the most popular free and open source computer forensic tools available.
- It aims to help with Incident Response, Cyber Intelligence and Computer Forensics scenarios. Amongst others, it contains tools for Mobile Forensics, Network Forensics, Data Recovery, and Hashing.

10. Xplico

- Xplico is an open source Network Forensic Analysis Tool (NFAT) that aims to extract applications data from internet traffic (e.g. Xplico can extract an e-mail message from POP, IMAP or SMTP traffic).
- Features include support for a multitude of protocols (e.g. HTTP, SIP, IMAP, TCP, UDP), TCP reassembly, and the ability to output data to a MySQL or SQLite database, amongst others.

11. LastActivityView

- LastActivityView allows you to view what actions were taken by a user and what events occurred on the machine.
- Any activities such as running an executable file, opening a file/folder from Explorer, an application or system crash or a user performing a software installation will be logged. The information can be exported to a CSV / XML / HTML file.
- This tool is useful when you need to prove that a user (or account) performed an action he or she said they didn't.

12. DSi USB Write Blocker

- DSi USB Write Blocker is a software based write blocker that prevents write access to USB devices.
- This is important in an investigation to prevent modifying the metadata or timestamps and invalidating the evidence.

13. FireEye RedLine

- RedLine offers the ability to perform memory and file analysis of a specific host.
- It collects information about running processes and drivers from memory, and gathers file system metadata, registry data, event logs, network information, services, tasks, and Internet history to help build an overall threat assessment profile.

14. PlainSight

PlainSight is a Live CD based on Knoppix (a Linux distribution) that allows you to perform digital forensic tasks such as viewing internet histories, data carving, USB device usage information gathering, examining physical memory dumps, extracting password hashes, and more.

15. HxD

- **HxD is one of my personal favourites.** It is a user-friendly hex editor that allows you to perform low-level editing and modifying of a raw disk or main memory (RAM). HxD was designed with easy-of-use and performance in mind and can handle large files without issue.
- Features include searching and replacing, exporting, checksums/digests, an in-built file shredder, concatenation or splitting of files, generation of statistics and more.

16. HELIX3 Free

- HELIX3 is a Live CD based on Linux that was built to be used in Incident Response, Computer Forensics and E-Discovery scenarios.
- It is packed with a bunch of open source tools ranging from hex editors to data carving software to password cracking utilities, and more.

17. Paladin Forensic Suite

- Paladin Forensic Suite is a Live CD based on Ubuntu that is packed with wealth of open source forensic tools.
- The 80 + tools found on this Live CD are organized into over 25 categories including Imaging Tools, Malware Analysis, Social Media Analysis, Hashing Tools, etc.

18. USB Historian

- USB Historian parses USB information, primarily from the Windows registry, to give you a list of all USB drives that were plugged into the machine. It displays information such as the name of the USB drive, the serial number, when it was mounted and by which user account.
- This information can be very useful when you're dealing with an investigation whereby you need to understand if data was stolen, moved or accessed.

1.8 Exam Pack (Review Questions)

☞ **Syllabus Topic : Introduction to Computer Forensics and Standard Procedure**

Q. 1 What is computer forensics ? Why computer forensics important ? *(Refer section 1.1)* **(5 Marks)**

Q. 2 Explain the process of computer forensics ? *(Refer section 1.1.1)* **(5 Marks)**

Q. 3 What Evidence Can We Recover at the Time of Investigation ? *(Refer section 1.1.2)* **(5 Marks)**

Syllabus Topic : Incident Verification and System Identification

Q. 4 What is Incidence? What are the goals of incidence response ? *(Refer section 1.2.1)* **(5 Marks)**

Q. 5 Explain the Incidence Response methodology or explain the components of Initia Response or explain the steps of initial response ? *(Refer section 1.2.2)* **(5 Marks)**

Q. 6 Explain the phase after detection of incident. *(Refer section 1.2.4)* **(5 Marks)**

Syllabus Topic : Recovery of Erased and Damaged Data

Q. 7 Explain the techniques used to recover erased or damaged data. *(Refer section 1.3)* **(5 Marks)**

Q. 8 How Linux tools use to recover files on FAT file systems. *(Refer section 1.3.1)* **(5 Marks)**

Q. 9 How deleted files recover on Windows systems ? *(Refer section 1.3.1)* **(5 Marks)**

Syllabus Topic : Disk Imaging and Preservation

Q. 10 What is disk imaging ? *(Refer section 1.4)* **(5 Marks)**

Q. 11 What is mirror image ? *(Refer section 1.4)* **(5 Marks)**

Q. 12 What are the forensic duplication tool requirements ? *(Refer section 1.4.1)* **(5 Marks)**

Q. 13 How to create a forensic duplicate of hard drive ? *(Refer section 1.4.2)* **(5 Marks)**

Q. 14 How to create a qualified forensic duplicate of hard drive ? *(Refer section 1.4.3)* **(5 Marks)**

Syllabus Topic : Data Encryption and Compression

Q. 15 Explain data encryption and compression. *(Refer section 1.5)* **(5 Marks)**

Syllabus Topic : Automated Search Techniques

Q. 16 Write short note on automated search techniques. *(Refer section 1.6)* **(5 Marks)**

Syllabus Topic : Forensics Software

Q. 17 Explain the forensic softwares. *(Refer section 1.7)* **(5 Marks)**

Chapter Ends

Unit I

CHAPTER 2

Network Forensic

Syllabus Topic : Introduction to Network Forensics and Tracking Network Traffic

2.1 Introduction to Network Forensics and Tracking Network Traffic

Q. 2.1.1 What is network forensics ? *(Ref. Sec. 2.1)* **(5 Marks)**

Q. 2.1.2 What is mean by securing a network ? *(Ref. Sec. 2.1)* **(5 Marks)**

- **Network forensics** is the process of collecting and analyzing raw network data and tracking network traffic systematically to find out how an attack was carried out or how an event occurred on a network.
- Network attacks are increasing day by day. Few of the attacks are unintentional which happens because of lack of knowledge. Attacks can be done without gaining entry to the network or system, for example DoS attacks.
- The DoS attacks overload network resources to make the network unavailable to genuine users, but the attacker never gains access to any computer on the network. It's imperative, then, to be exact when we mention particular computer crimes.
- DoS attackers ought not to be referred to as intruders when no interruption happens. In like manner, not all intruders can precisely be named attackers inspite of the fact that the individuals who get access and then destroy information or plant viruses are legitimately called by both names.
- Network forensic helps you to find out that the attacks on the network are done intentionally or unintentionally.
- When the intruders attack the network they leave a trace behind. So, it is necessary to find out the variation in network traffic to track the intrusions. It is important to know the typical pattern of your network, for example, the peak hours of using internet in the city are between 6 a.m. and 6 p.m.