UNIT- 5

Q.1 what is forensic science? What is the need of it?

Ans:

- Forensic science is generally defined as the application of science to the law.
- Digital forensics, also known as computer and network forensics.
- Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

➢ **The Need for Forensics:**

- Over the last decade, the number of crimes that involve computers has grown, spurring an increase in companies and products that aim to assist law enforcement in using computer-based evidence to determine the who, what, where, when, and how for crimes.
- Forensic tools and techniques are most often thought of in the context of criminal investigations and computer security incident handling used to respond to an event by investigating suspect systems, gathering and preserving evidence, reconstructing events, and assessing the current state of an event.
- However, forensic tools and techniques are also useful for many other types of tasks, such as the following:
  - **Operational Troubleshooting:** Many forensic tools and techniques can be applied to troubleshooting operational issues, such as finding the virtual and physical location of a host with an incorrect network configuration.
  - **Log Monitoring:** Various tools and techniques can assist in log monitoring, such as analyzing log entries and correlating log entries across multiple systems. This can assist in incident handling, identifying policy violations, auditing, and other efforts.
  - **Data Recovery**: There are dozens of tools that can recover lost data from systems, including data that has been accidentally or purposely deleted or otherwise modified.
  - **Data Acquisition:** Some organizations use forensics tools to acquire data from hosts that are being redeployed or retired.
  - **Regulatory Compliance:** Existing and emerging regulations require many organizations to protect sensitive information and maintain certain records for audit purposes.

Q.2 who are the primary users of forensic tools and techniques? Also state the various factors to be considered when selecting an external or internal party?

Ans:

- The primary users of forensic tools and techniques within an organization usually can be divided into the following three groups:
    - **Investigators:** Investigators within an organization are most often from the Office of Inspector General (OIG), and they are responsible for investigating allegations of misconduct. The OIG typically uses many forensic techniques and tools.
    - **IT Professionals**: This group includes technical support staff and system, network, and security administrators. They use a small number of forensic techniques and tools specific to their area.
    - **Incident Handlers**: This group responds to a variety of computer security incidents, such as unauthorized data access, inappropriate system usage, malicious code infections, and denial of service attacks. Incident handlers typically use a wide variety of forensic techniques and tools during their investigations.
- When deciding which internal or external parties should handle each aspect of forensics, organizations should keep the following factors in mind:
    - **Cost:** There are many potential costs. Software, hardware, and equipment used to collect and examine data may carry significant costs.
    - **Response Time:** Personnel located on-site might be able to initiate computer forensic activity more quickly than could off-site personnel.
    - **Data Sensitivity:** Because of data sensitivity and privacy concerns, some organizations might be reluctant (doubtful) to allow external parties to image hard drives and perform other actions that provide access to data.

Q.3 what are the different groups in which primary users of forensic tools and techniques within an organization usually can be divided into?

Ans:

- The primary users of forensic tools and techniques within an organization usually can be divided into the following three groups:
    - **Investigators:** Investigators within an organization are most often from the Office of Inspector General (OIG), and they are responsible for investigating allegations of misconduct. The OIG typically uses many forensic techniques and tools.
    - **IT Professionals**: This group includes technical support staff and system, network, and security administrators. They use a small number of forensic

techniques and tools specific to their area of expertise during their routine work (e.g., monitoring, troubleshooting, data recovery).

- **Incident Handlers**: This group responds to a variety of computer security incidents, such as unauthorized data access, inappropriate system usage, malicious code infections, and denial of service attacks. Incident handlers typically use a wide variety of forensic techniques and tools during their investigations.

Q.4 what are the key recommendations of establishing and organizing a forensic capability?

Ans: The key recommendations on establishing and organizing a forensic capability are as follows:

1. **Organizations should have a capability to perform computer and network forensics**
   - Forensics is needed for various tasks within an organization, including investigating crimes and inappropriate behavior, reconstructing computer security incidents, troubleshooting operational problems.
2. **Organizations should determine which parties should handle each aspect of forensics**
   - Most organizations rely on a combination of their own staff and external parties to perform forensic tasks.
   - Organizations should decide which parties should take care of which tasks based on skills and abilities, cost, response time, and data sensitivity.
3. **Incident handling teams should have robust forensic capabilities**
   - More than one team member should be able to perform each typical forensic activity.
4. **Many teams within an organization should participate in forensics**
   - Individuals performing forensic actions should be able to reach out to other teams and individuals within an organization, as needed, for additional assistance.
   - Examples of teams that may provide assistance in these efforts include IT professionals, management, legal advisors, human resources personnel, auditors, and physical security staff.
5. **Forensic considerations should be clearly addressed in policies**
   - At a high level, policies should allow authorized personnel to monitor systems and networks and perform investigations for legitimate reasons under appropriate circumstances.
   - Everyone who may be called upon to assist with any forensic efforts should be familiar with and understand the forensic policy.

6. **Organizations should create and maintain guidelines and procedures for performing forensic tasks**
    - The guidelines should include general methodologies for investigating an incident using forensic techniques, and step-by-step procedures should explain how to perform routine tasks.
    - The guidelines and procedures should also be reviewed regularly and maintained so that they are accurate.

Q.5 Write a note on forensic process.

Ans: The most common goal of performing forensics is to gain a better understanding of an event of interest by finding and analyzing the facts related to that event.
Forensic Process describes the basic phases of the forensic process are as follows:

1. Collection
- During collection, data related to a specific event is identified, labeled, recorded, and collected, and its integrity is preserved.

2. Examination
- In examination phase, forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity.
- Examination may use a combination of automated tools and manual processes.

3. Analysis
- In analysis phase analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

4. Reporting
- The final phase involves reporting the results of the analysis, which may include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process.

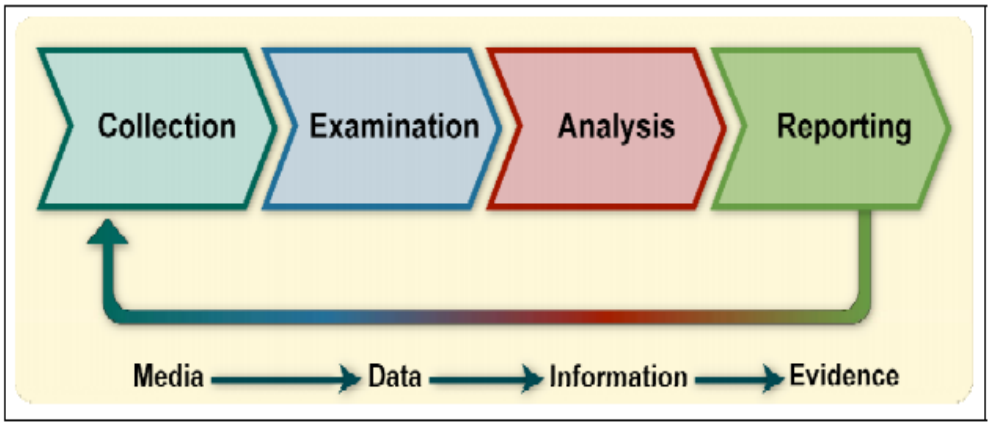

Figure: Forensic Process

Q.6 Write a note on forensic toolkit

Ans:

- The forensic toolkit should contain applications that can accomplish data examination and analysis in many ways and can be run quickly and efficiently from floppy disks, CDs, or a forensic workstation.
- The following processes are among those that an analyst should be able to perform with a variety of tools:

1. Using File Viewers

- Using viewers instead of the original source applications to display the contents of certain types of files is an important technique for scanning or previewing data,

2. Uncompressing Files

- Uncompressing files should be performed early in the forensic process to ensure that the contents of compressed files are included in searches and other actions.

3. Graphically Displaying Directory Structures

- This practice makes it easier and faster for analysts to gather general information about the contents of media.
- Most products can display Windows, Linux, and UNIX directory structures, whereas other products are specific to Macintosh directory structures.

4. Identifying Known Files

- The benefit of finding files of interest is obvious, but it is also often beneficial to eliminate unimportant files, such as known good OS and application files, from consideration.

5. Performing String Searches and Pattern Matches

- String searches aid in perusing large amounts of data to find key words or strings.

- Various searching tools are available that can use Boolean, fuzzy logic, synonyms and concepts, stemming, and other search methods.

6. Accessing File Metadata

- File metadata provides details about any given file.
- For example, collecting the metadata on a graphic file might provide the graphics creation date, copyright information, and description, and the creator's identity.

Q.7 Write a note on Examining data files

Ans:

- After a logical backup or bit stream imaging has been performed, the backup or image may have to be restored to another media before the data can be examined.
- This is dependent on the forensic tools that will be used to perform the analysis. Some tools can analyze data directly from an image file, whereas others require that the backup or image be restored to a medium first.
- Regardless of whether an image file or a restored image is used in the examination, the data should be accessed only as read-only to ensure that the data being examined is not modified and that it will provide consistent results on successive runs.
- After restoring the backup the analyst begins to examine the collected data and performs an assessment of the relevant files and data by locating all files, including deleted files and hidden files.
- The analyst may need to extract the data from some or all of the files, which may be complicated by such measures as encryption and password protection.

Q.8 Explain the two different techniques used for copying files from media.

Ans: Files can be copied from media using two different techniques:

1. Logical Backup

- A logical backup copies the directories and files of a logical volume.
- It does not capture other data that may be present on the media, such as deleted files or residual data stored in slack space.

2. Bit Stream Imaging

- Bit Stream Imaging is also known as disk imaging.
- Bit stream imaging generates a bit-for-bit copy of the original media, including free space and slack space.
- Bit stream images require more storage space and take longer to perform than logical backups.
- When a bit stream image is executed, either a disk-to-disk or a disk-to-file copy can be performed.

- A disk-to-disk copy, as its name suggests, copies the contents of the media directly to another media.
- A disk-to-file copy copies the contents of the media to a single logical data file.
- A disk-to-disk copy is useful since the copied media can be connected directly to a computer and its contents readily viewed.

Q.9 What is NESSUS? Why is it considered as the most popular vulnerability scanner?
Ans:

- Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.
- Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans.
- Significant capabilities of Nessus include:
    - Compatibility with computers and servers of all sizes.
    - Detection of security holes in local or remote hosts.
    - Detection of missing security updates and patches.
    - Simulated attacks to pinpoint vulnerabilities.
    - Execution of security tests in a contained environment.
    - Scheduled security audits.
- The Nessus server is currently available for UNIX, Linux and FreeBSD. The client is available for UNIX- or Windows-based operating systems.

Q.11 what are the control objectives of ISO 17799 standard?
Ans: ISO 17799 is an information security code of practice.

- The control objectives of ISO 17799 standard are as follows:
    1. **Risk Assessment and Treatment:**
        - Deals with the fundamentals of security risk analysis.
    2. **System Policy:**
        - To provide management direction and support for information security.

3. Organizing Information Security:

- To manage information security within the organization.
- Maintain the security of information and processing facilities with respect to external parties.

4. Asset Management:

- Achieve and maintain appropriate protection of organizational assets.
- Ensure that information receives an appropriate level of protection.

5. Human Resources Security:

- Ensure that employees, contractors and third parties are suitable for the jobs they are considered for, understand their responsibilities, and to reduce the risk of abuse.

6. Physical and Environmental Security:

- Prevent unauthorized physical access, interference and damage to the organization's information and premises.
- Prevent loss, theft and damage of assets
- Prevent interruption to the organization's activities.

7. Communications and Operations Management:

- Minimize the risk of systems failures
- Protect the integrity of information and software
- Ensure the security of e-commerce services
- Detect unauthorized information processing activities

8. Access Control

- Control access to information
- Ensure authorized user access
- Prevent unauthorized access to information systems

Q.13 State the features of NMAP.

Ans: Nmap features include:

- **Host discovery**: Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- **Port scanning:** Enumerating the open ports on target hosts.
- **Version detection**: Interrogating network services on remote devices to determine application name and version number.
- **OS detection:** Determining the Operating System and hardware characteristics of network devices.
- **Scriptable interaction with the target:** Using Nmap Scripting Engine (NSE) and Lua programming language. Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Q.14 what are the basic phases of forensic process? Give a brief overview of it.

Ans: Refer Question no: 5

Q.15 Write **a short note on File Systems.**

Ans:

- A file system defines the way that files are named, stored, organized, and accessed on logical volumes.
- However, all file systems share some common traits.
- First, they use the concepts of directories and files to organize and store data. Directories are organizational structures that are used to group files together. In addition to files, directories may contain other directories called subdirectories.
- Second, file systems use some data structure to point to the location of files on media.
- Some commonly used file systems are as follows:

1. FAT12:
  - FAT12 is used only on floppy disks and FAT volumes smaller than 16 MB.
  - FAT12 uses a 12-bit file allocation table entry to address an entry in the file system.

2. FAT16:
  - FAT16 is also commonly used for multimedia devices such as digital cameras and audio players.
  - FAT16 uses a 16-bit file allocation table entry to address an entry in the file system.
  - FAT16 volumes are limited to a maximum size of 2 GB in MS-DOS and Windows 95/98.

3. FAT32:
  - FAT32 uses a 32-bit file allocation table entry to address an entry in the file system.
  - The maximum FAT32 volume size is 2 terabytes (TB).

4. NTFS:
  - NTFS is a recoverable file system, which means that it can automatically restore the consistency of the file system when errors occur.
  - The maximum NTFS volume size is 2 TB.

5. Compact Disk File System (CDFS):
  - As the name indicates, the CDFS file system is used for CDs.

6. Universal Disk Format (UDF):
  - UDF is the file system used for DVDs and is also used for some CDs.

Q.16 how is the collection of files done in forensic science?

Ans:

- During data collection, the analyst should make multiple copies of the relevant files or file systems typically a master copy and a working copy.
- The analyst can then use the working copy without affecting the original files or the master copy.

- **Copying Files from Media**
  - **1. Logical Backup**
    - A logical backup copies the directories and files of a logical volume.
    - It does not capture other data that may be present on the media, such as deleted files or residual data stored in slack space.
  - **2. Bit Stream Imaging**
    - Bit Stream Imaging is also known as disk imaging.
    - Bit stream imaging generates a bit-for-bit copy of the original media, including free space and slack space.
- **Data File Integrity**
  - During backups and imaging, the integrity of the original media should be maintained.
  - To ensure that the backup or imaging process does not alter data on the original media, analysts can use a write-blocker while backing up or imaging the media.
  - A write-blocker is a hardware or software-based tool that prevents a computer from writing to computer storage media connected to it.
- **File Modification, Access, and Creation Times**
  - **Modification Time**: This is the last time a file was changed in any way, including when a file is written to and when it is changed by another program.
  - **Access Time:** This is the last time any access was performed on a file (e.g., viewed, opened, printed).
  - **Creation Time:** This is generally the time and date the file was created; however, when a file is copied to a system, the creation time will become the time the file was copied to the new system.
- **Technical Issues**
  - Several technical issues may arise in collecting data files.
  - The primary issue is the collection of deleted files and remnants of files existing in free and slack space on media.
  - Another common issue is the collection of hidden data.
  - Another issue that may arise is collection of data from RAID arrays that use striping.

Q.17 what is the need for forensics?

Ans: Refer Question no: 1

Q.18 what are the key recommendations on establishing and organizing a forensic capability?

Ans: Refer Question no: 4

Q.19 List various phases in forensics process. Explain in short.

Ans: Refer Question no: 5

Q.20 Explain the two techniques used to copy files from media.
Ans: Refer Question no: 8