Unit-5

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

**Ans:**

* **Forensic Science**:

Forensic science is generally defined as the application of science to the law. Digital forensics, also known as computer and network forensics, has many definitions. 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.
* As a result, computer and network forensics has evolved to assure proper presentation of computer crime evidentiary data into court.
* 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:

**1.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, resolving a functional problem with an application, and recording and reviewing the current OS and application configuration settings for a host.

**2.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.

**3.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. The amount of data that can be recovered varies on a case-by-case basis.

**4.Data Acquisition:**

* Some organizations use forensics tools to acquire data from hosts that are being redeployed or retired.
* For example, when a user leaves an organization, the data from the users workstation can be acquired and stored in case it is needed in the future. The workstations media can then be sanitized to remove all of the original users data.

**5.Due Diligence/Regulatory Compliance:**

* Existing and emerging regulations require many organizations to protect sensitive information and maintain certain records for audit purposes.
* Also, when protected information is exposed to other parties, organizations may be required to notify other agencies or impacted individuals.
* Forensics can help organizations exercise due diligence and comply with such requirements.

**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:**

* Many organizations rely on a combination of their own staff and external parties to perform forensic tasks. For example, some organizations perform standard tasks themselves and use outside parties only when specialized assistance is needed.
* Even organizations that want to perform all forensic tasks themselves usually outsource the most demanding ones, such as sending physically damaged media to a data recovery firm for reconstruction, or having specially trained law enforcement personnel or consultants collect data from an unusual source (e.g., cell phone).
* Such tasks typically require the use of specialized software, equipment, facilities, and technical expertise that most organizations cannot justify the high expense of acquiring and maintaining.
* When deciding which internal or external parties should handle each aspect of forensics, organizations should keep the following factors in mind:

**1.Cost:**

* There are many potential costs. Software, hardware, and equipment used to collect and examine data may carry significant costs (e.g., purchase price, software updates and upgrades, maintenance), and may also require additional physical security measures to safeguard them from tampering.
* Other significant expenses involve staff training and labor costs, which are particularly significant for dedicated forensic specialists.
* In general, forensic actions that are needed rarely might be more cost-effectively performed by an external party, whereas actions that are needed frequently might be more cost-effectively performed internally.

2.**Response Time:**

* Personnel located on-site might be able to initiate computer forensic activity more quickly than could off-site personnel.
* For organizations with geographically dispersed physical locations, off-site outsourcers located near distant facilities might be able to respond more quickly than personnel located at the organizations headquarters.

**3.Data Sensitivity:**

* Because of data sensitivity and privacy concerns, some organizations might be reluctant to allow external parties to image hard drives and perform other actions that provide access to data.
* For example, a system that contains traces of an incident might also contain health care information, financial records, or other sensitive data; an organization might prefer to keep that system under its own control to safeguard the privacy of the data.
* On the other hand, if there is a privacy concern within the team. For example, if an incident is suspected to involve a member of the incident handling team use of an independent third party to perform forensic actions would be preferable.

**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:5

**1.Investigators:**

* Investigators within an organization are most often from the Office of Inspector General (OIG), and they are responsible for investigating allegations of misconduct.
* For some organizations, the OIG immediately takes over the investigation of any event that is suspected to involve criminal activity. The OIG typically uses many forensic techniques and tools.
* Other investigators within an organization might include legal advisors and members of the human resources department.
* Law enforcement officials and others outside the organization that might perform criminal investigations are not considered part of an organizations internal group of investigators.

**2.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).

**3.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, supporting due diligence for audit record maintenance, and recovering from accidental system damage.
* Without such a capability, an organization will have difficulty determining what events have occurred within its systems and networks, such as exposures of protected, sensitive data.
* Also, handling evidence in a forensically sound manner puts decision makers in a position where they can confidently take the necessary actions.

**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. Hands-on exercises and IT and forensic training courses can be helpful in building and maintaining skills, as can demonstrations of new tools and technologies.

**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.
* Members of these teams should understand their roles and responsibilities in forensics, receive training and education on forensic related policies, guidelines, and procedures, and be prepared to cooperate with and assist others on forensic actions.

**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.
* Organizations may also have a separate forensic policy for incident handlers and others with forensic roles that provide more detailed rules for appropriate behavior.
* Everyone who may be called upon to assist with any forensic efforts should be familiar with and understand the forensic policy. Additional policy considerations are as follows:
* Forensic policy should clearly define the roles and responsibilities of all people performing or assisting with the organizations forensic activities. The policy should include all internal and external parties that may be involved and should clearly indicate who should contact which parties under different circumstances.
* The organizations policies, guidelines, and procedures should clearly explain what forensic actions should and should not be performed under normal and special circumstances and should address the use of anti-forensic tools and techniques. Policies, guidelines, and procedures should also address the handling of inadvertent exposures of sensitive information.
* Incorporating forensic considerations into the information system life cycle can lead to more efficient and effective handling of many incidents. Examples include performing auditing on hosts and establishing data retention policies that support performing historical reviews of system and network activity.

**6.Organizations should create and maintain guidelines and procedures for performing forensic tasks:**

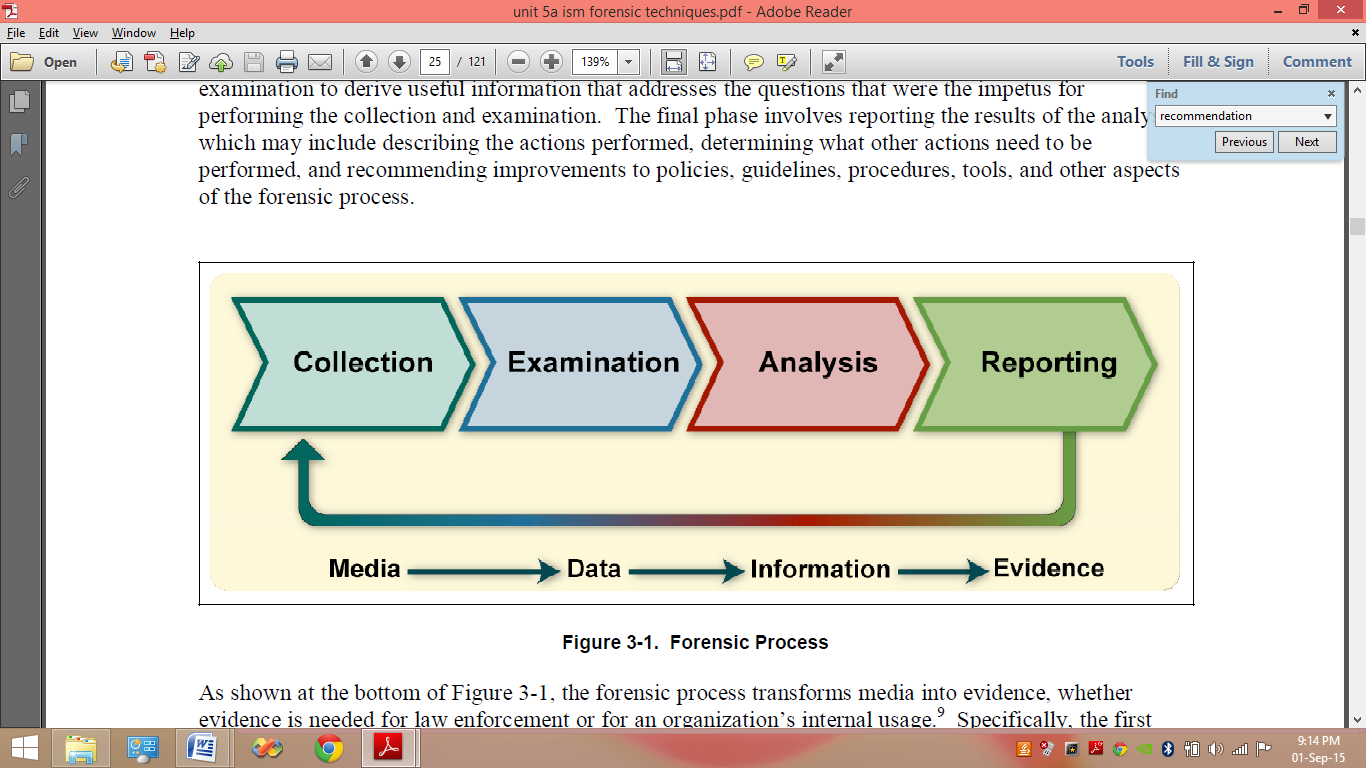
* The guidelines should include general methodologies for investigating an incident using forensic techniques, and step-by-step procedures should explain how to perform routine tasks.
* The guidelines and procedures should support the admissibility of evidence into legal proceedings. Because electronic logs and other records can be altered or otherwise manipulated, organizations should be prepared, through their policies, guidelines, and procedures, to demonstrate the reliability and integrity of such records.
* 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:**

* **Forensic Process:**

The basic phases of the forensic process: collection, examination, analysis, and reporting.



**1.Collection:**

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

### a.Identifying Possible Sources of Data :

* It describes the variety of data sources available and discusses actions that organizations can take to support the ongoing collection of data for forensic purposes.

### b.Acquiring the Data:

* It describes the recommended steps for collecting data, including additional actions necessary to support legal or internal disciplinary proceedings.

### c.Incident Response Considerations:

* It discusses incident response considerations, emphasizing the need to weigh the value of collected data against the costs and impact to the organization of the collection process.

**2.Examination:**

* After data has been collected, the next phase is to examine the data, which involves assessing and extracting the relevant pieces of information from the collected data.
* In the second phase, **examination**, 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.
* This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms.
* An acquired hard drive may contain hundreds of thousands of data files; identifying the data files that contain information of interest, including information concealed through file compression and access control, can be a daunting task. In addition, data files of interest may contain extraneous information that should be filtered.

**3.Analysis:**

* Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it.
* The next phase, **analysis**, involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
* For instance, a network intrusion detection system (IDS) log may link an event to a host, the host audit logs may link the event to a specific user account, and the host IDS log may indicate what actions that user performed. Tools such as centralized logging and security event management software can facilitate this process by automatically gathering and correlating the data.

**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.

Many factors affect reporting, including the following:

* Alternative Explanations.
* Audience Consideration.
* Actionable Information.
* As shown at the bottom of Figure 3-1, the forensic process transforms media into evidence, whether evidence is needed for law enforcement or for an organizations internal usage.
* Specifically, the first transformation occurs when collected data is examined, which extracts data from media and transforms it into a format that can be processed by forensic tools.
* Second, data is transformed into information through analysis.
* Finally, the information transformation into evidence is analogous to transferring knowledge into action using the information produced by the analysis in one or more ways during the reporting phase.
* For example, it could be used as evidence to help prosecute a specific individual, actionable information to help stop or mitigate some activity, or knowledge in the generation of new leads for a case.

**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, and is more efficient because the analyst does not need native applications for viewing each type of file.
* Various tools are available for viewing common types of files, and there are also specialized tools solely for viewing graphics.
* If available file viewers do not support a particular file format, the original source application should be used; if this is not available, then it may be necessary to research the files format and manually extract the data from the file.

**2.Uncompressing Files.**

* Compressed files may contain files with useful information, as well as other compressed files. Therefore, it is important that the analyst locate and extract compressed 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. However, analysts should keep in mind that compressed files might contain malicious content, such as compression bombs, which are files that have been repeatedly compressed, typically dozens or hundreds of times.
* Compression bombs can cause examination tools to fail or consume considerable resources; they might also contain malware and other malicious payloads.
* Although there is no definite way to detect compression bombs before uncompressing a file, there are ways to minimize their impact.

**3.Graphically Displaying Directory Structures.**

* This practice makes it easier and faster for analysts to gather general information about the contents of media, such as the type of software installed and the likely technical aptitude of the user(s) who created the data.
* 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.
* Analysts should use validated hash sets, such as those created by NIST.s National Software Reference Library (NSRL) projector personally created hash setsthat have been validated, as a basis for identifying known benign and malicious files.
* Hash sets typically use the SHA-1 and MD5 algorithms to establish message digest values for each known file.

**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.
* Examples of common searches include searching for multiple words in a single file and searching for misspelled versions of certain words.
* Developing concise sets of search terms for common situations can help the analyst reduce the volume of information to review.

**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 creators identity.
  + Metadata for graphics generated by a digital camera might include the make and model of the digital camera used to take the image, as well as F-stop, flash, and aperture settings.
  + For word processing files, metadata could specify the author, the organization that licensed the software, when and by whom edits were last performed, and user-defined comments. Special utilities can extract metadata from files.

**Q.7.Write a note on Examining data files.**

**Ans:**

The processes involved in examining files and data, as well as techniques that can expedite examination are:

### 1.Locating the Files:

* The first step in the examination is to locate the files. A disk image can capture many gigabytes of slack space and free space, which could contain thousands of files and file fragments.
* Manually extracting data from unused space can be a time-consuming and difficult process, because it requires knowledge of the underlying file system format.
* Fortunately, several tools are available that can automate the process of extracting data from unused space and saving it to data files, as well as recovering deleted files and files within a recycling bin.
* Analysts can also display the contents of slack space with hex editors or special slack recovery tools.

### 2.Extracting the Data:

* The rest of the examination process involves extracting data from some or all of the files. To make sense of the contents of a file, an analyst needs to know what type of data the file contains.
* The intended purpose of file extensions is to denote the nature of the files contents; for example, a jpg extension indicates a graphic file, and an mp3 extension indicates a music file.
* However, users can assign any file extension to any type of file, such as naming a text file **mysong.mp3** or omitting a file extension.
* In addition, some file extensions might be hidden or unsupported on other OSs. Therefore, analysts should not assume that file extensions are accurate.

### 3.Using a Forensic Toolkit:

* Analysts should have access to various tools that enable them to perform examinations and analysis of data, as well as some collection activities.
* Many forensic products allow the analyst to perform a wide range of processes to analyze files and applications, as well as collecting files, reading disk images, and extracting data from files.
* Most analysis products also offer the ability to generate reports and to log all errors that occurred during the analysis. Although these products are invaluable in performing analysis, it is critical to understand which processes should be run to answer particular questions about the data.
* An analyst may need to provide a quick response or just answer a simple question about the collected data. In these cases, a complete forensic evaluation may not be necessary or even feasible.
* 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.

**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.**

* 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.
* If evidence may be needed for prosecution or disciplinary actions, the analyst should get a bit stream image of the original media, label the original media, and store it securely as evidence.
* All subsequent analysis should be performed using the copied media to ensure that the original media is not modified and that a copy of the original media can always be recreated if necessary.
* All steps that were taken to create the image copy should be documented. Doing so should allow any analyst to produce an exact duplicate of the original media using the same procedures.
* In addition, proper documentation can be used to demonstrate that evidence was not mishandled during the collection process. Besides the steps that were taken to record the image, the analyst should document supplementary information such as the hard drive model and serial number, media storage capacity, and information about the imaging software or hardware that was used (e.g., name, version number, licensing information). All of these actions support the maintenance of the chain of custody.
* 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. However, a disk-to-disk copy requires a second media similar to the original media.A disk-to-file copy allows the data file image to be moved and backed up easily.
* Numerous hardware and software tools can perform bit stream imaging and logical backups. Hardware tools are generally portable, provide bit-by-bit images, connect directly to the drive or computer to be imaged, and have built-in hash functions.
* Hardware tools can acquire data from drives that use common types of controllers, such as Integrated Drive Electronics (IDE) and Small Computer System Interface (SCSI).
* Software solutions generally consist of a startup diskette, CD, or installed programs that run on a workstation to which the media to be imaged is attached of files or partitions and may ignore free or unallocated drive space, whereas others create a bit-by-bit image copy of the media.

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

**Ans:**

* Nessus is a [proprietary](http://en.wikipedia.org/wiki/Proprietary_software) comprehensive [vulnerability scanner](http://en.wikipedia.org/wiki/Vulnerability_scanner) which is developed by [Tenable Network Security](http://en.wikipedia.org/wiki/Tenable_Network_Security). It is free of charge for personal use in a non-enterprise environment.
* According to surveys done by sectools.org, Nessus is the world's most popular vulnerability scanner, taking first place in the 2000, 2003, and 2006 security tools survey. Tenable Network Security estimates that it is used by over 75,000 organizations worldwide.
* This free tool offers a surprisingly robust feature set and is widely supported by the information security community. It doesn't take long between the discovery of a new vulnerability and the posting of an updated script for Nessus to detect it.
* In fact, [Nessus](http://searchnetworking.techtarget.com/definition/Nessus) takes advantage of the Common Vulnerabilities and Exposures (CVE) architecture that facilitates easy cross-linking between compliant security tools.
* The Nessus tool works a little differently than other scanners. Rather than purporting to offer a single, all-encompassing vulnerability database that gets updated regularly, Nessus supports the Nessus Attack Scripting Language (NASL), which allows security professionals to use a simple language to describe individual attacks.
* Nessus administrators then simply include the NASL descriptions of all desired vulnerabilities to develop their own customized scans.
* **Nessus is now closed-source**. The base product is still available for free. With the introduction of Nessus 3, however, Tenable moved Nessus from an open source to a commercial licensing model. In other words, while the software itself remains free, updated vulnerability information will come with a fee, at least for enterprises (home users may download updates for free). Tenable cites the need to invest in the future of Nessus as the motivation for moving to a proprietary license scheme.
* **Significant speed enhancements**. In benchmarking tests performed by Tenable, Nessus 3 scans systems at about twice the speed of Nessus 2. This is due to optimizations in the scan engine and a complete overhaul of NASL.
* **Dramatic reduction in resource requirements.** Nessus 3 uses significantly less memory and CPU cycles than Nessus 2, allowing simultaneous scanning of a larger number of hosts.
* Nessus uses a modular architecture consisting of centralized servers that conduct scanning and remote clients that allow for administrator interaction. You may deploy Nessus scanning servers at various points within your enterprise and control them from a single client.
* This allows you to effectively scan segmented networks from multiple vantage points and conduct scans of large networks that require multiple servers running simultaneously.

**Q.10.What types of vulnerabilities are scanned by NESSUS?**

**Ans:**

Nessus allows scans for the following types of vulnerabilities:

* Vulnerabilities that allow a remote [hacker](http://en.wikipedia.org/wiki/Hacker_(computer_security)) to control or access sensitive data on a system.
* Misconfiguration (e.g. [open mail relay](http://en.wikipedia.org/wiki/Open_mail_relay), missing patches, etc.).
* [Default passwords](http://en.wikipedia.org/wiki/Default_password), a few common [passwords](http://en.wikipedia.org/wiki/Password), and blank/absent passwords on some system accounts. Nessus can also call [Hydra](http://en.wikipedia.org/w/index.php?title=Hydra_(software)&action=edit&redlink=1) (an external tool) to launch a [dictionary attack](http://en.wikipedia.org/wiki/Dictionary_attack).
* [Denials of service](http://en.wikipedia.org/wiki/Denial-of-service_attack) against the [TCP/IP stack](http://en.wikipedia.org/wiki/TCP/IP_stack) by using [mangled packets](http://en.wikipedia.org/wiki/Mangled_packet)
* Preparation for [PCI DSS](http://en.wikipedia.org/wiki/PCI_DSS) (Payment Card Industry Data Security Standard) audits.

**Q.11.What are the control objectives of ISO 17799 standard?**

**Ans:**

ISO 17799 is an information security code of practice. It includes a number of sections, covering a wide range of security issues. Broadly (very) the objectives of these are as follows:

**1. Risk Assessment and Treatment:**  
This section was an addition to the latest version, and deals with the fundamentals of security risk analysis.

**2. System Policy:**  
Objective:  To provide management direction and support for information security

**3. Organizing Information Security:**  
Objectives:

a) To manage information security within the organization

b) Maintain the security of information and processing facilities with respect to external parties.

**4. Asset Management:**  
Objectives:

a) Achieve and maintain appropriate protection of organizational assets.

b) Ensure that information receives an appropriate level of protection.

**5. Human Resources Security:**  
Objectives:

a) 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 (theft, misuse, etc).

b) Ensure that the above are aware of IS threats and their responsibilities, and able to support the organization's security policies

c) Ensure that the above exit the organization in an orderly and controlled manner.

**6. Physical and Environmental Security:**  
Objectives:

a) Prevent unauthorized physical access, interference and damage to the organization's information and premises.

b) Prevent loss, theft and damage of assets

c) Prevent interruption to the organization's activities.

**7. Communications and Operations Management:**  
Objectives:

a) Ensure the secure operation of information processing facilities

b) Maintain the appropriate level of information security and service delivery, aligned with 3rd party agreements

c) Minimize the risk of systems failures

d) Protect the integrity of information and software

e) Maintain the availability and integrity of information and processing facilities

f) Ensure the protection of information in networks and of the supporting infrastructure

g) Prevent unauthorized disclosure, modification, removal or destruction of assets.

h) Prevent unauthorized disruption of business activities.

i) Maintain the security of information and/or software exchanged internally and externally.

j) Ensure the security of e-commerce services

k) Detect unauthorized information processing activities

**8. Access Control:**  
Objectives:

a) Control access to information

b) Ensure authorized user access

c) Prevent unauthorized access to information systems

d) Prevent unauthorized user access and compromise of information and processing facilities

e) Prevent unauthorized access to networked services

f) Prevent unauthorized access to operating systems

g) Prevent unauthorized access to information within application systems

h) Ensure information security with respect to mobile computing and teleworking facilities

**9. Information Systems Acquisition, Development and Maintenance:**  
Objectives:

a) Ensure that security is an integral part of information systems

b) Prevent loss, errors or unauthorized modification/use of information within applications

c) Protect the confidentiality, integrity or authenticity of information via cryptography

d) Ensure the security of system files

e) Maintain the security of application system information and software

f) Reduce/manage risks resulting from exploitation of publiched vulnerabilities

**10. Information Security Incident Management:**  
Objectives:

a) Ensure that security information  is communicated in a manner allowing corrective action to be taken in a timely fashion

b) Ensure a consistent and effective approach is applied to the management of IS issues

**11. Business Continuity Management:**  
Objectives:

a) Counteract interruptions to business activities and protect critical processes from the effects of major failures/disasters

b) Ensure timely resumption of the above

**12. Compliance:**  
Objectives:

a) Avoid the breach of any law, regulatory or contractual obligation and of any security requirement.

b) Ensure systems comply with internal security policies/standards

c) Maximize the effectiveness of and minimize associated interference from and to the systems audit process

**Q.12.What is the functionality of NMAP tool?**

**Ans:**

* Nmap ("Network Mapper") is a free and open source ([license](http://nmap.org/data/COPYING)) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.
* Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.
* It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.
* In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer ([Zenmap](http://nmap.org/zenmap/)), a flexible data transfer, redirection, and debugging tool ([Ncat](http://nmap.org/ncat/)), a utility for comparing scan results ([Ndiff](http://nmap.org/ndiff/)), and a packet generation and response analysis tool ([Nping](http://nmap.org/nping/)).

**Q.13.State the features of NMAP.**

**Ans:**

Nmap features are:

* **Flexible**:
* Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many [port scanning](http://nmap.org/nmap/nmap_doc.html) mechanisms (both TCP & UDP), [OS detection](http://nmap.org/book/osdetect.html), [version detection](http://nmap.org/book/vscan.html), ping sweeps, and more.
* **Powerful**:
  + Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
* **Portable**:
* Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
* **Easy**:
  + While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
* **Free**:
* The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks.
* Nmap is available for [free download](http://nmap.org/download.html), and also comes with full source code that you may modify and redistribute under the terms of the [license](http://nmap.org/data/COPYING).
* **Well Documented**:
* Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages [here](http://nmap.org/docs.html).
* **Supported**:
* While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the [Nmap mailing lists](http://nmap.org/#lists). Most bug reports and questions should be sent to the [nmap-dev list](http://seclists.org/nmap-dev), but only after you read the [guidelines](http://nmap.org/book/man-bugs.html).
* **Acclaimed**:
* Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series.
* **Popular**:
* Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc).
* It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

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

**Ans:**

The forensic process comprises the following basic phases:

**1.Collection.**

* The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data.
* Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered devices (e.g., cell phones, PDAs).

**2.Examination.**

* Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.

**3.Analysis.**

* The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

**4.Reporting.**

* The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process.
* The formality of the reporting step varies greatly depending on the situation.

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

**Ans:**

* **Filesystems**:
* A filesystem defines the way that files are named, stored, organized, and accessed on logical volumes. Many different filesystems exist, each providing unique features and data structures. However, all filesystems 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, filesystems use some data structure to point to the location of files on media. In addition, they store each data file written to media in one or more file allocation units.
* These are referred to as clusters by some filesystems (e.g., File Allocation Table [FAT], NT File System [NTFS]) and as blocks by other filesystems (e.g., UNIX and Linux). A file allocation unit is simply a group of sectors, which are the smallest units that can be accessed on media.

Some commonly used filesystems 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 filesystem.

**2.FAT16**:

* MS-DOS, Windows 95/98/NT/2000/XP, Windows Server 2003, and some UNIX OSs support FAT16 natively. 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 filesystem.
* FAT16 volumes are limited to a maximum size of 2 GB in MS-DOS and Windows 95/98. Windows NT and newer OSs increase the maximum volume size for FAT16 to 4 GB.

**3.FAT32**:

* Windows 95 Original Equipment Manufacturer (OEM) Service Release 2 (OSR2), Windows 98/2000/XP, and Windows Server 2003 support FAT32 natively, as do some multimedia devices.
* FAT32 uses a 32-bit file allocation table entry to address an entry in the filesystem. The maximum FAT32 volume size is 2 terabytes (TB).

**4.NTFS**:

* Windows NT/2000/XP and Windows Server 2003 support NTFS natively. NTFS is a recoverable filesystem, which means that it can automatically restore the consistency of the filesystem when errors occur.
* In addition, NTFS supports data compression and encryption, and allows user and group-level access permissions to be defined for data files and directories.The maximum NTFS volume size is 2 TB.

**5.High-Performance File System (HPFS)**:

* HPFS is supported natively by OS/2 and can be read by Windows NT 3.1, 3.5, and 3.51. HPFS builds on the directory organization of FAT by providing automatic sorting of directories.
* In addition, HPFS reduces the amount of lost disk space by utilizing smaller units of allocation. The maximum HPFS volume size is 64 GB.

**6.Second Extended Filesystem (ext2fs)**:

* ext2fs is supported natively by Linux. It supports standard UNIX file types and filesystem checks to ensure filesystem consistency. The maximum ext2fs volume size is 4 TB.

**7.Third Extended Filesystem (ext3fs)**:

* ext3fs is supported natively by Linux. It is based on the ext2fs filesystem and provides journaling capabilities that allow consistency checks of the filesystem to be performed quickly on large amounts of data. The maximum ext3fs volume size is 4 TB.

**8.ReiserFS**:

* ReiserFS is supported by Linux and is the default filesystem for several common versions of Linux.
* It offers journaling capabilities and is significantly faster than the ext2fs and ext3fs filesystems. The maximum volume size is 16 TB.

**9.Hierarchical File System (HFS)**:

* HFS is supported natively by Mac OS. HFS is mainly used in older versions of Mac OS but is still supported in newer versions. The maximum HFS volume size under Mac OS 6 and 7 is 2 GB.
* The maximum HFS volume size in Mac OS 7.5 is 4 GB. Mac OS 7.5.2 and newer Mac OSs increase the maximum HFS volume size to 2 TB.

**10.HFS Plus**:

* HFS Plus is supported natively by Mac OS 8.1 and later and is a journaling filesystem under Mac OS X.
* It is the successor to HFS and provides numerous enhancements, such as long filename support and Unicode filename support for international filenames. The maximum HFS Plus volume size is 2 TB.

**11.UNIX File System (UFS):**

* UFS is supported natively by several types of UNIX OSs, including Solaris, FreeBSD, OpenBSD, and Mac OS X. However, most OSs have added proprietary features, so the details of UFS differ among implementations.

**12.Compact Disk File System (CDFS)**.

* As the name indicates, the CDFS filesystem is used for CDs.

**13.International Organization for Standardization (ISO) 9660 and Joliet**:

* The ISO 9660 filesystem is commonly used on CD-ROMs. Another popular CD-ROM filesystem, Joliet, is a variant of ISO 9660.
* ISO 9660 supports filename lengths of up to 32 characters, whereas Joliet supports up to 64 characters. Joliet also supports Unicode characters within filenames.

**14.Universal Disk Format (UDF)**:

* UDF is the filesystem 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 filesystems 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.

### 1.Copying Files from Media:

Files can be copied from media using two different techniques:

**a.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.

**b.Bit Stream Imaging:**

* 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.

### 2.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.
* Hardware write-blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.
* Software write-blockers are installed on the analysts forensic system and currently are available only for MS-DOS and Windows systems. (Some OSs [e.g., Mac OS X, Linux] may not require software write-blockers because they can be set to boot with secondary devices not mounted.
* However, attaching a hardware write-blocking device will ensure that integrity is maintained.) MS-DOS based software write-blockers work by trapping Interrupt 13 and extended Interrupt 13 disk writes.
* Windows-based software write-blockers use filters to sort interrupts sent to devices to prevent any writes to storage media.

### 3.File Modification, Access, and Creation Times:

* It is often important to know when a file was created, used, or manipulated, and most OSs keep track of certain timestamps related to files. The most commonly used timestamps are the modification, access, and creation (MAC) times, as follows:

**a.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.

**b.Access Time:**

* This is the last time any access was performed on a file (e.g., viewed, opened, printed).

**c.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. The modification time will remain intact.