MOUDULE-1

1. What is forensic science? What is computer forensics? How is it different from other related fields?

Forensic science is the application of science to criminal and civil laws, mainly on the criminal side,during criminal investigation, as governed by the legal standards of admissible evidence and criminal procedure.

Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation. While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals.

Computer Forensics is the science of obtaining, preserving, and documenting evidence from digital electronic storage devices, such as computers, PDAs, digital cameras, mobile phones, and various memory storage devices.

Computer Forensics is primarily concerned with the proper acquisition, preservation and analysis of digital evidence, typically after an unauthorized access or use has taken place.

With Computer Security the main focus concerns the prevention of unauthorized access, as well as the maintenance of confidentiality, integrity and availability of computer systems.

2. What is steganography? How can steganography files be identified?

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

Visual detection
By looking at repetitive patterns, you can detect hidden information in stego images. These repetitive patterns might reveal the identification or signature of a steganography tool or hidden information. Even small distortions can reveal the existence of hidden information.
You can analyze these patterns by comparing the original cover images with the stego images and try to see differences. This is called a known-cover attack. By comparing numerous images, patterns become possible signatures to a steganography tool. A few of these signatures might identify the existence of hidden information and the tools used to embed the messages. With this information, if the cover images are not available for comparison, the derived known signatures are enough to imply the existence of a message and identify the tool used to embed the message.

Detecting hidden information with various tools

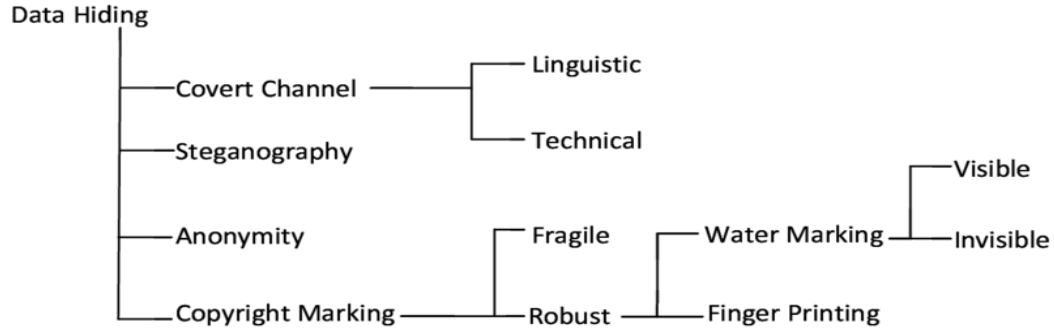
1)Guidance Software, Inc.

2) ILook Investigator
3)Comparing the MD5 hash values of two files with the program, md5sum.exe.
4)Detecting hidden information with Stegdetect and Xsteg (freeware)
5)Detecting hidden information with file compression
6)Detecting hidden information with Stego Watch from WetStone Technologies Inc. (commercial product).Spam mimic

transforms a text message into e-mail spam
8)Foundstone

3. State and explain different data hiding techniques.

Methods Of Hiding Data



A covert channel is a type of computer security attack that provides a channel for transfer of information in a way that violates the computer security policy. Robustness and imperceptibility are the important characteristics of a covert channel.
Linguistic Steganography uses text as the cover media to hide the
secret message whereas the technical covert channels work by exploiting the loopholes in the OS, network model, protocols etc.
Copyright marking
is a procedure that is used to protect the intellectual properties. In this method a logo or a mark is embedded into a piece of information to show the originality of the work. The copyright can be robust or fragile depending upon the requirement. Fragile copyright marks are used to prove manipulations as the fragile marks cannot resist manipulations and lost upon slightest modifications. Robust copyright methods
are resistant against all sorts of statistical and other types of manipulations.

Finger printing and watermarking techniques are popular types of robust copyright marking methods and are used for authentication purposes.
Watermarking-
-Robustness
-Message Secrecy
Should be high
-Capacity not
important as a
small amount of
data need to be
embedded
-Impeccability Depends

Types-
Visible
Embedding is generally performed
into the higher order bit planes.
Impeccability is low as the watermark
is visible.
Robustness is high

Invisible
Embedding is generally performed into
selected pixels of the whole image
Impeccability is high.
Robustness is high
High security
against unauthorised
alteration of the watermark

Anonymity:
is a method of secret communication where the transmitter and the receiver remain anonymous so that
a third party, who is interested on the information but is not a legitimate user of the information, looses track of
it.
Steganography:
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video
Steganography is a process of secret communication where a piece of information (a secret message)is hidden into another piece of innocent looking information,popularly called a cover, in such a way that the very existence of the secret information remains concealed without raising any suspicion in the minds of the viewers.

4. What is extraction? What are its subfunctions? Explain.

5. What is a file system? Explain the computer boot sequence.

file system is a method of organizing and retrieving files from a storage medium, such as a hard drive. File systems usually consist of files separated into groups called directories. Directories can contain files or additional directories. Today, the most commonly used file system with Windows is NTFS.

Examples of file systems

- FAT (e.g., FAT16 and FAT32)
- GFS
- HFS
- NTFS
- UDF

sequence comprises of the following steps:

Turn on the Power button.

CPU pins are reset and registers are set to specific value.

CPU jump to address of BIOS (0xFFFF0).

BIOS run POST (Power-On Self Test) and other necessary checks.

BIOS jumps to MBR(Master Boot Record).

Primary Bootloader runs from MBR and jumps to Secondary Bootloader.

Secondary Bootloaders loads Operating System.

These are the tasks that are carried during booting process.

- The boot process is something that happens every time you turn your computer on. You don't really see it, because it happens so fast. You press the power button come back a few minutes later and Windows XP, or Windows Vista, or whatever Operating System you use is all loaded.
- The BIOS chip tells it to look in a fixed place, usually on the lowest-numbered hard disk (the boot disk) for a special program called a boot loader (under Linux the boot loader is called Grub or LILO). The boot loader is pulled into memory and started. The boot loader's job is to start the real operating system.
- **Functions of BIOS**

POST (Power On Self Test) The Power On Self Test happens each time you turn your computer on. It sounds complicated and thats because it kind of is. Your computer does so much when its turned on and this is just part of that.

It initializes the various hardware devices. It is an important process so as to ensure that all the devices operate smoothly without any conflicts. BIOSes following ACPI create tables describing the devices in the computer.

The POST first checks the bios and then tests the CMOS RAM. If there is no problems with this then POST continues to check the CPU, hardware devices such as the Video Card, the secondary storage devices such as the Hard Drive, Floppy Drives, Zip Drive or CD/DVD Drives.If some errors found then an error message is displayed on screen or a number of beeps are heard. These beeps are known as POST beep codes.

- **Master Boot Record**

The Master Boot Record (MBR) is a small program that starts when the computer is booting, in order to find the operating system (eg. Windows XP). This complicated process (called the Boot Process) starts with the POST (Power On Self Test) and ends when the Bios searches for the MBR on the Hard Drive, which is generally located in the first sector, first head, first cylinder (cylinder 0, head 0, sector 1).

- The bootstrap loader is stored in the master boot record (MBR) on the computer's hard drive. When the computer is turned on or restarted, it first performs the power-on self-test, also known as POST. If the POST is successful and no issues are found, the bootstrap loader will load the operating system for the computer into memory. The computer will then be able to quickly access, load, and run the operating system.

init

init is the last step of the kernel boot sequence. It looks for the file */etc/inittab* to see if there is an entry for *initdefault*. It is used to determine initial run-level of the system. A run-level is used to decide the initial state of the operating system.
Some of the run levels are:

- **Level**
  - 0 –> System Halt
  - 1 –> Single user mode
  - 3 –> Full multiuser mode with network
  - 5 –> Full multiuser mode with network and X display manager
  - 6 –> Reboot

6. What are the components of disk drives? Explain

Hard drive physical components

Disk platter
•Read/Write head
•Head arm/Head slider
•Head actuator mechanism
•Spindle motor
•Logic board
•Air filter
•Cables & Connectors

The Four Major Components of a Hard Drive

Disk Platter Storage

A hard drive's platters are the physical part of the hard drive responsible for storing data. Platters are circular, thin metal disks that have a diameter that's slightly smaller than the width of the device storage case. Modern hard drives can have more than one platter stacked on top of each other to expand storage capacity. Disc platters resemble optical discs with thicker metal and no protective plastic coating.

Spindle Controls Motion

The spindle is the part of the hard drive that's responsible for spinning the platters so the device's read and write arm can access and save data. Hard drive platters are stacked on top of each other on top on the spindle. The platters have a hole in the center for placement on the spindle and are held in place on the spindle itself with platter clamps. If the platters are not secured on the spindle, they may collide with other parts of the hard drive when moving and break.

Reading and Writing Heads

The read and write arm, also called the actuator arm, is the part of the hard drive that reads data already stored on the platter and writes new data on the platter. The actuator arm includes the read and write heads that float just microns away from the platter that perform the actual read and write tasks. The read and write heads physically read and record magnetic patterns stored on the platter.

Actuator Aligns the Heads

The actuator arm is connected to a part called the actuator that controls the positioning of the actuator arm relative to the disk platter. The actuator works with the spindle motor to position the actuator arm so it lines up with the platter to read and write data.

Other Parts Interface and Protect

Hard drives have other components that aren't central to the physical process of storing and accessing data. The other parts include the data connector, power connector, printed circuit board and device case. The data connector and printed circuit board are the parts that the computer uses for data requests from the hard drive whereas the the power connector handles the electrical current needed to run the device. The hard drive's case is an air-sealed component that protects the device and holds all the components in place.

7. Explain the Microsoft file structures

A computer running a Microsoft Windows operating system organizes its data like you would organize files in a file cabinet. Each cabinet has multiple drawers. Each drawer contains folders. Each folder contains important papers that you need to file away. The Windows file system structure parallels this type of organization.

Logical Drives and Cabinet Drawers

Based on the file cabinet scenario, each cabinet drawer is represented as a logical drive on a Windows computer. For example, the logical drive "C:" is usually where your personal and system data is stored. The "D:" drive may contain files used for computer recovery that should only be managed by a system administrator. The "E:" drive may give you access to a DVD player. When a digital camera is plugged into a Windows computer, a new logical drive "F:" may appear, which gives you access to the photo files on the camera.

Folders

Some common folders that come by default on a Windows environment include Documents, Pictures, Music, Videos and Downloads. The Documents folder is a logical place to store word-processing files, spreadsheets and presentations. The Pictures folder is appropriate for digital pictures that you created, copied or scanned from external sources such as email, scanner, Internet or digital camera. The Music folder is suitable for music files that you downloaded from the Internet, ripped from a CD or composed with a music program. The Videos folder is proper for videos downloaded from the Internet, copied from a camcorder or created from a movie maker software. The Downloads folder is recommended for programs and files downloaded from the Internet. You may also create folders and sub folders. Microsoft Windows uses a file naming convention such as "C:\Users\Sarah\Documents," where the file name is delineated by the backslash ("\") sign.

Files

Papers and items filed inside a physical file cabinet folder are represented as files in a Microsoft Windows environment. A file can be a spreadsheet, drawing, music or application program. A Windows file name can have up to 260 characters. A Windows file usually has a file extension, which helps Windows understand what type it is and how to read it. A regular word-processing file with a ".txt" file extension may invoke a Windows Notepad or Wordpad program to open it. A picture file with a JPG file extension may invoke a Windows picture-viewer program. In naming a Windows file, you should avoid these characters: \, /, ?, :, *, ", >, < and |.

Recycle Bin

When you delete a file on Microsoft Windows, rest assured that, by default, the file is not permanently deleted from the computer. A deleted file first gets recycled into the Recycle Bin

folder, which normally resides on the desktop. You can restore the deleted files from the Recycle Bin. You can also configure the Recycle Bin to increase its storage, remove the "Delete confirmation" dialog or not to recycle files to it. If you choose to do the last item, then Windows permanently deletes files without first recycling them into the bin.

8. What is a disk partition? State the hexadecimal codes in the partition table and the corresponding file systems

Disk partitioning or **disk slicing**[1] is the creation of one or more regions on a hard disk or other secondary storage, so that an operating system can manage information in each region separately.

Partition Table

The partition table is 64 bytes long and is located inside the MBR at sector 0x1BE.The partition table is an array of 4 partition table entries each of 16 bytes thus: 16x4 = 64.The format of each partition table entry is the following:

Offset	Size	Item
0x00	1	Boot indicator; 0x80 = Active partition / 0x00 Inactive partition (*boot_indicator*)
0x01	1	partition start: head (*chs_start.head*)
0x02	1	partition start: sector (*chs_start.sect*)
0x03	1	partition start: cylinder (*chs_start.cyl*)
0x04	1	Partition ID (example ID=1 for FAT12) (*system_indicator*)
0x05	1	partition end: head (*chs_end.head*)
0x06	1	partition end: sector (*chs_end.sector*)
0x07	1	partition end: cylinder (*chs_end.cyl*)
0x08	4	Number of sectors before the beginning of this partition (*sectors_before*)
0x0C	4	Number of sectos in this partition (*number_of_sectors*)

9. Explain the new technology file system.(or Explain the structure of NTFS disks)

NTFS (NT file system; sometimes New Technology File System) is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk. NTFS is the Windows NT equivalent of the Windows 95 file allocation table (FAT) and the OS/2 High Performance File System (HPFS). However, NTFS offers a number of improvements over FAT and HPFS in terms of performance, extendibility, and security.

Notable features of NTFS include:

- Use of a b-tree directory scheme to keep track of file clusters
- Information about a file's clusters and other data is stored with each cluster, not just a governing table (as FAT is)
- Support for very large files (up to 2 to the 64th power or approximately 16 billion bytes in size)
- An access control list (ACL) that lets a server administrator control who can access

specific files

- Integrated file compression
- Support for names based on Unicode
- Support for long file names as well as "8 by 3" names
- Data security on both removable and fixed disks

How NTFS Works

When a hard disk is formatted (initialized), it is divided into partitions or major divisions of the total physical hard disk space. Within each partition, the operating system keeps track of all the files that are stored by that operating system. Each file is actually stored on the hard disk in one or more clusters or disk spaces of a predefined uniform size. Using NTFS, the sizes of clusters range from 512 bytes to 64 kilobytes. Windows NT provides a recommended default cluster size for any given drive size. For example, for a 4 GB (gigabyte) drive, the default cluster size is 4 KB (kilobytes). Note that clusters are indivisible. Even the smallest file takes up one cluster and a 4.1 KB file takes up two clusters (or 8 KB) on a 4 KB cluster system.

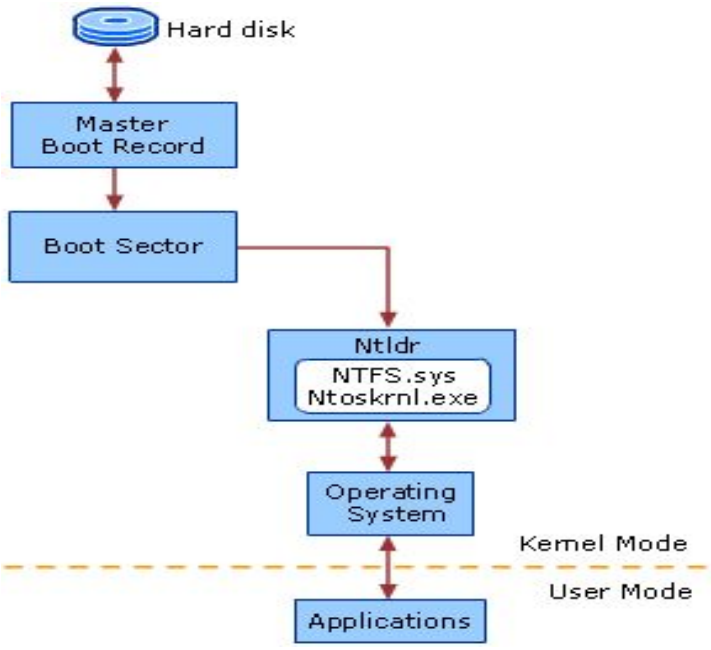
The selection of the cluster size is a trade-off between efficient use of disk space and the number of disk accesses required to access a file. In general, using NTFS, the larger the hard disk the larger the default cluster size, since it's assumed that a system user will prefer to increase performance (fewer disk accesses) at the expense of some amount of space inefficiency.

When a file is created using NTFS, a record about the file is created in a special file, the Master File Table (MFT). The record is used to locate a file's possibly scattered clusters. NTFS tries to find contiguous storage space that will hold the entire file (all of its clusters).

Each file contains, along with its data content, a description of its attributes (its metadata).

The figure NTFS Architecture shows the architecture of this process.

NTFS Architecture



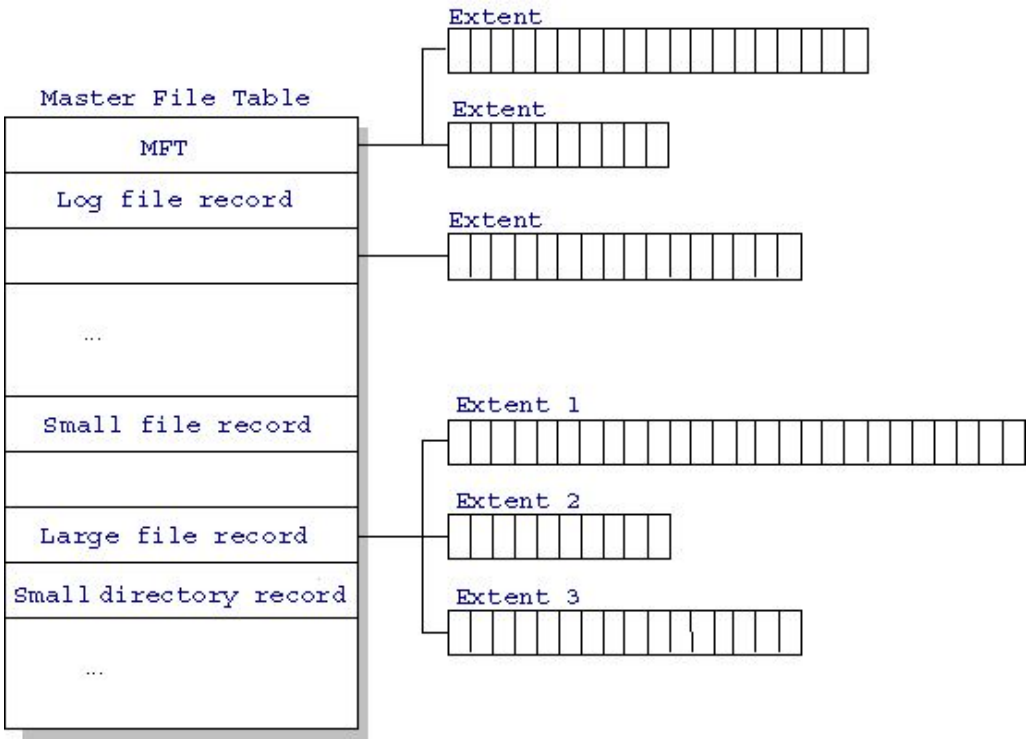
NTFS Architecture Components on an x86-based System

Component	Component Description
Hard disk	Contains one or more partitions.
Boot sector	Bootable partition that stores information about the layout of the volume and the file system structures, as well as the boot code that loads Ntdlr.
Master Boot Record	Contains executable code that the system BIOS loads into memory. The code scans the MBR to find the partition table to determine which partition is the active, or bootable, partition.
Ntldlr.dll	Switches the CPU to protected mode, starts the file system, and then reads the contents of the Boot.ini file. This information determines the startup options and initial boot menu selections.
Ntfs.sys	System file driver for NTFS.
Ntoskrnl.exe	Extracts information about which system device drivers to load and the load order.
Kernel mode	The processing mode that allows code to have direct access to all hardware and memory in the system.
User mode	The processing mode in which applications run.

10. What are the metadata records in the master file table of NTFS ?

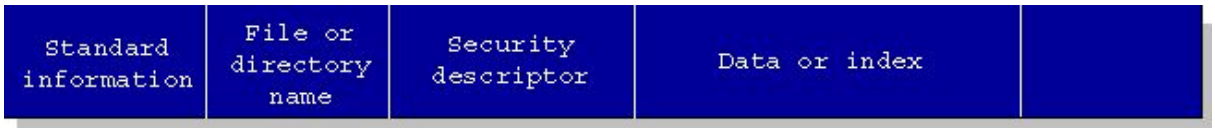
NTFS Master File Table (MFT)
Each file on an NTFS volume is represented by a record in a special file called the master file table (MFT). NTFS reserves the first 16 records of the table for special information.The first record of this table describes the master file table itself, followed by a MFT mirror record.If the first MFT record is corrupted, NTFS reads the second record to find the MFT mirror file, whose first record is identical to the first record of the MFT. The locations of the data segments for both the MFT and MFT mirror file are recorded in the boot sector.Figure provides a simplified illustration of the MFT structure:

MFT Structure



The master file table allocates a certain amount of space for each file record. The attributes of a file are written to the allocated space in the MFT. Small files and directories (typically 512 bytes or smaller), such as the file illustrated in next figure, can entirely be contained within the master file table record.

MFT Record for a Small File or Directory:



This design makes file access very fast. Consider, for example, the FAT file system, which uses a file allocation table to list the names and addresses of each file. FAT directory entries contain an index into the file allocation table.

When you want to view a file, FAT first reads the file allocation table and assures that it exists. Then FAT retrieves the file by searching the chain of allocation units assigned to the file. With NTFS, as soon as you look up the file, it's there for you to use.

Directory records are housed within the master file table just like file records. Instead of data, directories contain index information.

Small directory records reside entirely within the MFT structure. Large directories are organized into B-trees, having records with pointers to external clusters containing directory entries that could not be contained within the MFT structure.

11. Explain the attributes in the master file table.

The master file table (MFT) stores the information required to retrieve files from an NTFS partition.

A file may have one or more MFT records, and can contain one or more attributes. In NTFS, a file reference is the MFT segment reference of the base file record. For more information, see **MFT_SEGMENT_REFERENCE**.

The MFT contains file record segments; the first 16 of these are reserved for special files, such as

the following:

- 0: MFT ($Mft)
- 5: root directory (\)
- 6: volume cluster allocation file ($Bitmap)
- 8: bad-cluster file ($BadClus)

Each file record segment starts with a file record segment header. For more information, see **FILE_RECORD_SEGMENT_HEADER**. Each file record segment is followed by one or more attributes. Each attribute starts with an attribute record header. For more information, see **ATTRIBUTE_RECORD_HEADER**. The attribute record includes the attribute type (such as $DATA or $BITMAP), an optional name, and the attribute value. The user data stream is an attribute, as are all streams. The attribute list is terminated with 0xFFFFFFFF ($END).

The following are some example attributes.

- The $Mft file contains an unnamed $DATA attribute that is the sequence of MFT record segments, in order.
- The $Mft file contains an unnamed $BITMAP attribute that indicates which MFT records are in use.
- The $Bitmap file contains an unnamed $DATA attribute that indicates which clusters are in use.
- The $BadClus file contains a $DATA attribute named $BAD that contains an entry that corresponds to each bad cluster.

12. Explain the NTFS encrypting file system. Explain the EFS recovery agent.

An Encrypting File System (EFS) is a functionality of the New Technology File System (NTFS) found on various versions of Microsoft Windows. EFS facilitates the transparent encryption and decryption of files by making use of complex, standard cryptographic algorithms.

The cryptographic algorithms are used in EFS to provide useful security countermeasures, whereby only the intended recipient can decipher the cryptography. EFS uses symmetric and asymmetric keys during the encryption process, but it does not protect data transmissions. Rather, it protects data files within systems. Even if someone has access to a certain computer, whether authorized or not, he still cannot unlock the EFS cryptography without the secret key.

Techopedia explains Encrypting File System (EFS)

EFS is actually a transparent public key encryption technology that operates with NTFS permissions to allow or deny user access to files and folders in various Windows operating systems (OS), including NT (excluding NT4), 2000 and XP (excluding XP Home Edition).

Key EFS features are as follows:

- The encryption process is easy. Select the check-box in the file or folder's properties to turn on the encryption.
- EFS offers control over who can read the files.
- Files selected for encryption are encrypted once they are closed but are automatically ready to use once opened.
- The file's encryption feature may be removed by clearing the check-box in the file properties.

Although used by many organizations, EFS must be handled with caution and knowledge, to avoid

encrypting content that should be transparent, rather than secure. This is compounded by the fact that it may be difficult to decrypt data content that was not meant to be encrypted in the first place.

EFS developers remind users that once a folder is marked encrypted, all files contained in that folder are encrypted as well, including future files transported to that particular folder. However, a custom setting for encrypting “this file only” is available.

Encryption passwords are identity specific, so it is important for employees to avoid sharing passwords and equally important that users remember their passwords.

Data Recovery Agents (DRAs)

Once a file has been encrypted, only the user who encrypted it or a DRA can access it. DRAs are users who are designated as **recovery agents** for encrypted files. They can decrypt any encrypted file and they can log on to a system and decrypt files and folders, making them accessible again to other users.

The default DRAs are as follows:

- Members of the local Administrators group for Windows XP Professional non-domain member computers or Windows 200X Server non-domain member servers
- Members of the Domain Administrators group for Windows 200X domain controllers, Windows domain member servers, and Windows XP Professional domain member computers.

If you remove all the DRAs are removed from a standalone Windows XP computer or from a Windows Active Directory domain, EFS will not allow users to encrypt files and folders, as there is no Data Recovery policy in place.

The EFS recovery policy for the local Windows XP computer is managed via the Group Policy snap-in for the Microsoft Management Console (MMC) as follows:

1. Expand the Group Policy snap-in node for **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**, then select the **Encrypting File System** subnode.
2. Right-click the **Encrypting File System** subnode and select **Add Data Recovery Agent**, or select **Properties** to enable or disable EFS on the computer.

Creating a DRA

As we've already noted, if the user who has encrypted folders or files is unavailable to decrypt them when required, a **Data Recovery Agent (DRA)** can be used to access the encrypted files. If a Windows XP Professional computer is are part of an Active Directory domain, the domain Administrator user account is automatically

assigned the role of DRA, but Windows XP Professional computers that are installed as stand-alone computers or are part of a workgroup have no default DRA assigned.

You can create a DRA manually, using the ***Cipher***command-line utility as follows:

Cipher /R:filename

The ***/R*** switch specifies that two files should be generated, a ***.pfx*** file which is used for data recovery and a ***.cer*** file which includes a self-signed EFS recovery agent certificate. The recovery agent can be imported into the local security policy and the private key stored in a safe place. Go ahead and do this, choosing a relevant filename, eg: your surname or username.

Once you have created these files, you can specify the DRA using **Local Security Policy**, as follows:

1. Access **Local Security Policy** via **Administrative Tools** or the **Local Computer Policy MMC snap-in** and expand **Public Key Policies Encrypting File System.**
2. Right-click **Encrypting File System** and select **Add Data Recovery Agent**. The **Add Recovery Agent Wizard** will start. Click **Next** to continue.
3. The **Select Recovery Agents** dialog box will appear. Click the **Browse Folders** button to access the ***.cer*** file you created above with the ***Cipher /R:filename*** command. Select the certificate and click **Next**.
4. The **Completing the Add Recovery Agent Wizard** dialog box will appear. Check that the settings are correct and click **Finish**.
5. You will now see the **Data Recovery Agent** listed in the **Local Security Settings** dialog box, under Encrypting File System.

If the DRA has the private key to the DRA certificate created through ***Cipher /R:filename*** then it can decrypt files just like the user who originally encrypted the file. Once the encrypted files have been opened by a DRA, they are available as unencrypted files and can be stored as either encrypted or unencrypted files.

13. What is master boot record? Explain the FAT file systems

The Master Boot Record (MBR) is the information in the first sector of any hard disk or diskette that identifies how and where an operating system is located so that it can be boot (loaded) into the computer's main storage or random access memory. The Master Boot Record is also sometimes called the "partition sector" or the "master partition table" because it includes a table that locates each partition that the hard disk has been formatted into. In addition to this table, the MBR also includes a program that reads the boot sector record of the partition containing the operating system to be booted into RAM. In turn, that record contains a program that loads the rest of the operating system into RAM.

File Allocation Table, **FAT** is a method of keeping track of the contents of a hard drive used by early Microsoft operating systems that was first introduced in 1977. The table is a chart of numbers that correspond to cluster addresses on the hard drive. Below is a listing of the different types of FAT that have been used and the operating systems using them.

Tip: Today, later versions of Microsoft Windows, such as Windows XP, Vista, 7, and 10 are using NTFS and not FAT.

FAT8

The oldest FAT, FAT8 was used on 8-inch floppies with the 8086 processor.

FAT12

A File Allocation Table that uses 12-bit binary system that was derived from FAT8. A hard drive formatted using FAT12 can use a maximum of approximately 16,736,256 volume size, and today is no longer used. If your computer is running Windows 95 or above and your FAT within FDISK is being displayed as FAT12 your hard drive is corrupted, bad, or has a computer virus.

FAT16

FAT utilizing a 16-bit binary system. Used with Windows 3.x to Windows 95.

FAT32

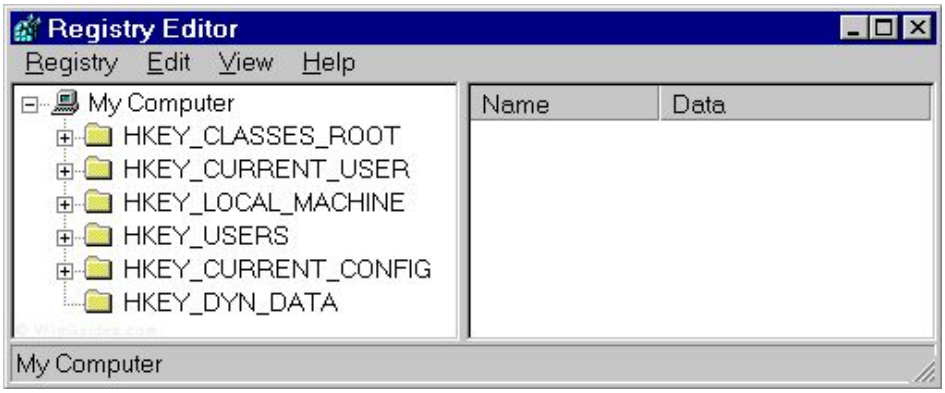
Enhanced File Allocation Table utilizing a 28-bit binary system, first used in Windows 95 OSR2 and Windows 98, that saves disk space by using 4 k Cluster. See FAT32 Page for extended

information about FAT32.

14. What is windows registry? Explain the following terms of windows registry: Registry editor, HKEY, Key, Subkey, branch, value, default value, hives.

The **registry** is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry. the registry or Windows Registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. For example, when a program is installed, a new subkey containing settings like a program's location, its version, and how to start the program, are all added to the Windows Registry.

The Registry Editor :: is included with most version of Windows (although you won't find it on the Start Menu) it enables you to view, search and edit the data within the Registry. There are several methods for starting the Registry Editor, the simplest is to click on the **Start** button, then select **Run**, and in the **Open** box type "regedit", and if the Registry Editor is installed it should now open and look like the image below.



HKEY::The keys at the root level of the hierarchical database are generally named by their Windows API definitions, which all begin "HKEY"

KEYS:: Keys are referenced with a syntax similar to Windows' path names, using backslashes to indicate levels of hierarchy. Keys must have a case insensitive name without backslashes.

Hive:: A *hive* is a logical group of keys, subkeys, and values in the registry that has a set of supporting files containing backups of its data.

15. Explain the functions of the following registry HKEYs:

i. HKEY_CLASS_ROOT

ii. HKEY_CURRENT_USER

iii. HKEY_LOCAL_MACHINE

iv. HKEY_USERS

v. HKEY_CURRENT_CONFIG

vi. HKEY_DYN_DATA

Root Key	***Description***
HKEY_LOCAL_MACHINE	This is the root key that contains the most interesting information. It contains information on the hardware such as processor type, bus

	architecture, video, and disk I/O hardware. It also contains software information for the operating system, including information on device drivers, services, security, and installed software.
HKEY_CLASSES_ROOT	This key is similar to the functionally limited Registry included with Windows 3.x. It contains information on files associations (matching a file extension to an application), as well as acts as the repository for OLE classes. This root key points to data stored in the HKEY_LOCAL_MACHINE\SOFTWARE\Classes subkey.
HKEY_CURRENT_USER	This key contains the profile information for the user currently logged onto the console. It contains user-level preferences for the operating system, as well as for applications installed on the computer. This key is a pointer to one of the subkeys stored in HKEY_USERS.
HKEY_USERS	This key contains a pointer to the hive for the user currently logged on at the console , as well as a pointer to the hive for the default user. In neither case does HKEY_USERS contain profiles for users who log on remotely.
HKEY_CURRENT_CONFIG	This is a new root key in Windows NT 4.0. It contains the current hardware configuration information, as specified by the current hardware profile. It actually points to the same contents as the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current subkey.
HKEY_DYN_DATA	This branch points to the part of HKEY_LOCAL_MACHINE, for use with the Plug-&-Play features of Windows, this section is dymanic and will change as devices are added and removed from the system.

16. What are typical computer supported crimes that occur in corporates? How can these be prevented? (or Write a short note on Corporate Investigations.)

A **corporate investigation** is the thorough **investigation** of a **corporation** or business in order to uncover wrongdoing committed by management, employees, or third parties. There are many aspects of **corporate investigations** and they can vary significantly based on your needs.

17. What are the different formats for digital evidence? Explain

- Three formats

Raw format:

- This is what the Linux dd command makes
- Bit-by-bit copy of the drive to a file
- Advantages
  - Fast data transfers
  - Can ignore minor data read errors on source drive
  - Most computer forensics tools can read raw format
- Disadvantages
  - Requires as much storage as original disk or data
  - Tools might not collect marginal (bad) sectors
    - Low threshold of retry reads on weak media spots
    - Commercial tools use more retries than free tools
  - Validation check must be stored in a separate file
    - Message Digest 5 (MD5)
    - Secure Hash Algorithm (SHA-1 or newer)
    - Cyclic Redundancy Check (CRC-32)

Proprietary Formats:

- Features offered
  - Option to compress or not compress image files
  - Can split an image into smaller segmented files
    - Such as to CDs or DVDs
    - With data integrity checks in each segment
  - Can integrate metadata into the image file
    - Hash data
    - Date & time of acquisition
    - Investigator name, case name, comments, etc.
- Disadvantages
  - Inability to share an image between different tools
  - File size limitation for each segmented volume
    - Typical segmented file size is 650 MB or 2 GB
- Expert Witness format is the unofficial standard

- Used by EnCase, FTK, X-Ways Forensics, and SMART
- Can produce compressed or uncompressed files
- File extensions **.E01**, **.E02**, **.E03**, …

Advanced Forensics Format (AFF):

- Developed by Dr. Simson L. Garfinkel of Basis Technology Corporation
- Design goals
  - Provide compressed or uncompressed image files
  - No size restriction for disk-to-image files
  - Provide space in the image file or segmented files for metadata
  - Simple design with extensibility
  - Open source for multiple platforms and Oss
- Design goals (continued)
  - Internal consistency checks for self-authentication
- File extensions include **.afd** for segmented image files and **.afm** for AFF metadata
- AFF is open source

18. State and explain the general tasks that the investigators perform when working with digital evidence.

- General tasks investigators perform when working with digital evidence:
  - Identify digital information or artifacts that can be used as evidence
  - Collect, preserve, and document evidence
  - Analyze, identify, and organize evidence
  - Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.

19. Identify 5 different types of volatile evidence

20. Identify the different data acquisition methods we use in digital forensics.

Four methods

Bit-stream disk-to-image file:

- Most common method
- Can make more than one copy
- Copies are bit-for-bit replications of the original drive

  Tools: ProDiscover, EnCase, FTK, SMART, Sleuth Kit, X-Ways, iLook
  - Bit-stream disk-to-disk
- Used when disk-to-image copy is not possible
  - Because of hardware or software errors or incompatibilities
  - This problem is more common when acquiring older drives

- Adjusts target disk's geometry (cylinder, head, and track configuration) to match the suspect's drive
- Tools: EnCase, SafeBack (MS-DOS), Snap Copy

Logical and Sparse:

- When your time is limited, and evidence disk is large
- Logical acquisition captures only specific files of interest to the case
  - Such as Outlook **.pst** or **.ost** files
- Sparse acquisition collects only some of the data

21. Explain the tasks to be completed before searching for evidence

- Preparing for a computer search and seizure
  - Probably the most important step in computing investigations
- You might need to get answers from the victim and an informant
  - Who could be a police detective assigned to the case, a law enforcement witness, or a manager or coworker of the **person of interest** to the investigation
- Identifying the nature of the case
  - Including whether it involves the private or public sector
  - The nature of the case dictates how you proceed
  - And what types of assets or resources you need to use in the investigation
- Identifying the Type of Computing System
  - If you can identify the computing system
  - Estimate the size of the drive on the suspect's computer and how many computers to process at the scene
  - Determine which OSs and hardware are involved
- Determining Whether You Can Seize a Computer
  - The type of case and location of the evidence
  - Determine whether you can remove computers
  - Law enforcement investigators need a warrant to remove computers from a crime scene and transport them to a lab
- If you aren't allowed to take the computers to your lab
  - Determine the resources you need to acquire digital evidence and which tools can speed data acquisition
- Determining the Tools You Need
- Preparing the Investigation Team

22. Why is it necessary to maintain professional conduct during computer investigation? How can this be maintained?

23. What do we need to conduct an investigation involving Email abuse? Enumerate the steps for processing of an Email abuse case.

26. What are the steps executed when a NTFS computer is switched on? What are the startup files of windows XP? What are the system files of windows XP?

When a hard disk is formatted (initialized), it is divided into partitions or major divisions of the total physical hard disk space. Within each partition, the operating system keeps track of all the files that are stored by that operating system. Each file is actually stored on the hard disk in one or more clusters or disk spaces of a predefined uniform size. Using NTFS, the sizes of clusters range from 512 bytes to 64 kilobytes. Windows NT provides a recommended default cluster size for any given drive size. For example, for a 4 GB (gigabyte) drive, the default cluster size is 4 KB (kilobytes). Note that clusters are indivisible. Even the smallest file takes up one cluster and a 4.1 KB file takes up two clusters (or 8 KB) on a 4 KB cluster system.

The selection of the cluster size is a trade-off between efficient use of disk space and the number of disk accesses required to access a file. In general, using NTFS, the larger the hard disk the larger the default cluster size, since it's assumed that a system user will prefer to increase performance (fewer disk accesses) at the expense of some amount of space inefficiency.

When a file is created using NTFS, a record about the file is created in a special file, the Master File Table (MFT). The record is used to locate a file's possibly scattered clusters. NTFS tries to find contiguous storage space that will hold the entire file (all of its clusters).

Each file contains, along with its data content, a description of its attributes (its metadata).

The figure NTFS Architecture shows the architecture of this process.

NTFS Architecture