1. COMPUTER CRIME

Computer crime is often described as a crime or illegal act committed with the use of computer-related technologies. A computer generally plays several roles in computer crime: a computer can be the target of a crime, a computer can be used to commit crime, and a computer can be the one containing evidences.

1.1. CYBER CRIME

Cybercrime is broadly used to describe the criminal activities where computers, networks or related tools are either used illegally to perform a crime directed against a device or a crime where the device contains evidences or a crime where the device itself is used as a tool to commit the crime. A cybercrime is always intentional and never accidental.

2. COMPUTER FORENSICS

Computer forensics is "*acquiring, preserving, retrieving and presenting data that has been processed electronically and stored on computer media*" (Allen, 2005). Analyzing digital data and examining computers or digital devices routinely within the organization can save time and money during an investigation process. Computer forensics can be extended to acquiring and processing data from other digital devices like smart phones, PDAs, cameras, smart watches and more.

2.1. ROLE OF COMPUTER FORENSICS

Information is generally stored on computers or other digital devices and this information can be manipulated. Digital evidences can be used in investigation of criminal cases like financial fraud, child pornography, human trafficking and others. It can also be used for investigating information regarding security breaches, discrimination cases, and harassment cases. Forensic techniques are required to investigate and analyze data that are required for confirmation of cybercrime.

2.2. DIGITAL FORENSIC INVESTIGATION PROCESS

Digital Forensic investigation process involves five steps to achieve the best outcome of the examination case. Briefly the steps are as follows:

1. Identification is the first step in an investigation process. Before starting any forensic investigation process, it is important to identify the aim and scope of action being carried out, key players, source of evidences.
2. Conducting Interviews with suspects, users and others can be a key parameter for a successful investigation.
3. Identify source of crime and document related evidential data
4. Collect all related information and electronic evidences from the scene of crime.
5. Preserve evidences by different means of method.
6. Analyzing involve extracting relevant information obtained in the previous stage to ensure quality of information in terms of accuracy.
7. Presentation involves in presenting a detailed report on findings, activities involved and all other information acquired from the scene of crime.

2.3. FORENSIC READINESS

Digital evidences can be easily destroyed and modified and which in turn an lead to non-admissible evidence in the court of law. Evidence being presented in court should be collected and documented using a legally accepted method. Forensic readiness follows procedures and rules for collecting, preserving, protecting and analyzing evidences so that these evidences can be used for any legal matters, security investigations or in a court of law. Post incident activities after cybercrime can be optimized by forensic readiness for minimized cost, saved time, and effort during a forensic investigation. Originations can benefit using the method of forensic readiness.

3. COMPUTER HARDWARE

Computer hardware are the components of the computer system which includes central processing units, monitors, keyboard, mouse, power supply, motherboard, memory, drives etc.

3.1. COMPUTER HARDWARE COMPONENTS

Components	Description
Motherboard	Motherboard connects all parts of the computer together. Every connection seen behind the computer casing is connected to the motherboard. Modern motherboards include USB ports, HDMI that allow compatible devices like digital cameras, printers etc, connect to your computer when required.
Central Processing Units(CPU)	CPU processes and executes all commands from the computer's hardware and software.
Random Access Memory (RAM)	RAM is a hardware that stores data temporarily. It facilitates the read and write access to the storage media in a faster way. All data that a user uses during the working on a computer is temporarily stored in RAM. Upon shutdown of the computer, the content of RAM is always erased. All data in RAM are often written to hard drive in a file called the *swap file*. In Windows, swap files can grow and shrink. If a computer is in the hibernate mode, then the entire contents of RAM are written to a file named hiberfil.sys so that contents of RAM can be restored from disk. Huberfil.sys is normally inaccessible but with the help of forensic tools, data from this file can be accessed from hard disk. Pagefile.sys contains windows system file of virtual memory or swap files. Using the forensic tools, some of the data can be obtained from swap files.

Hard Drive	Hard Drive serves as the main data storage device in a computer. Hard drive secures the data even when the computer is shut down. It stores, bootable data, operating system files, and programs. Hard drive consists of series of thin magnetized platters. Hard drive ***platters*** have an addressing scheme so that the various locations of file on the disk where data are stored can be located for reads & write. A ***track*** is a circular ring on one side of the platter. A track is always numbered for identification. A ***sector*** is the smallest storage unit in the hard disk holding a storage capacity of 512 bytes. If a data of 1000bytes have to be stored in the hard disk, the data will be written on 2 sectors of 512bytes each. Sectors are found in tracks and each track contains equal number of sectors. Track and sector numbers are used by operating systems and to identify and retrieve the stored information.
Solid State Drive (SSD)	Solid State Drive is a storage device similar to hard drive. Data are stored on flash memory instead of platters. Advantage of SSD over traditional hard drive is based on the faster read or write, less energy and smaller in size. Flash memory is divided into pages of 2Kbytes or larger. Each page can be rewritten a limited number of times compared to a hard disk drive.
Optical Drive	Hardware that uses laser to read or write data to an optical disc. Examples of optical discs are CDs, DVDs and Blue-ray discs.
Power Supply	Hardware that transforms alternating current from the outlet to the direct current (DC) required for different system components.

Network Interface Card (NIC)	NIC is a hardware or extension card in a computer used for communication with other computers in a network. Each NIC has a unique hardware address coded into its memory - MAC (Media Access Control) address. MAC address is a 6- sets of hexadecimal values where the first three hexadecimal values identify the manufacturer and the second set of three hexadecimal values is a unique serial number applied by the manufacturer.
Wireless Network Interface Card	A network interface controller used in wireless communication to send data using radio waves.

3.1.1. Hard Drive Performances

The performance of a hard disk drive is measured by the rate at which the data are read or written from/to a hard drive. Seek times, buffer size and rotational speed are the three important specifications to measure the drive performances. Defragmentation is one method used to improve the performance of a hard drive.

3.1.2 Defragmentation

Generally hard drives store data in a sequential order in sectors. Upon deletion of files, folders, programs or other files, sectors become empty leaving spaces. Defragmenting is one method to reorganize the hard disk drive back to its sequential sectors.

4. FILES SYSTEMS

File system is a method of storing, retrieving and managing files from the hard disk. File systems are independent from any specific computer but must be consistent between systems using the same file systems. Examples of Linux files systems are EXT (Extended File System), EXT2 (Second Extended File System), EXT3 (Third Extended File System), EXT4 (Fourth Extended File System). Examples of Windows file systems are FAT (File allocation Table), FAT32 (32 bit FAT), NTFS (New Technology File Systems). A file system needs its own structural files and data.

1.1. TYPES OF FILE SYSTEMS

- **Disk file system:** Manages data and files on permanent storage devices.
- **Network file system –**Mechanism for storing files on a network. It allows users to locate and access files on remote computers.
- **Database file system (DBFS):** Files are identified by their characteristics, such as type of file, topic, author, or similar metadata.

1.1.1. File System Categories

Each file system has a general structure to them, but each instance of a file system is unique because it has a unique size.The data structures in this category frequently have unused values and storage locations that could be used to hide small amounts of data. Essential file system data are those that are needed to save and retrieve files. Essential file system data should be true for the user to open the file. Non-essential file system data are those that are there for convenience but are not needed for the basic functionality of saving and retrieving files.

1.1.1.1.Content Category

Content category contains data that includes the actual content of a file. Most of the data in a file system belong to this category and it keeps track of the allocation status of each data unit. Without this function, data could be overwritten. When a new file is created or any changes are made to an existing file, the operating system looks for an unallocated data unit and allocates it to a file. When a file is deleted, the data units that were allocated to the file are set to the unallocated state and can be allocated to new files. Most operating systems do not wipe the contents of the data unit when it is unallocated. In forensic investigation, analysis of the content category is conducted to recover deleted data and conduct low-level searches.

1.1.1.2.Metadata Category

Metadata category contains the data that describe a file and its data-like location of the content, size of the file, date and time the file was last read or written and access control information. When a file is deleted, metadata entry is set to an unallocated state. In forensic investigation, metadata category analysis is carried out to determine more details about a specific file or to search for a file that meets certain requirements.

1.1.1.3.File Name Category

File name category contains the data that assign a name to each file. File name analysis is to determine and to locate the root directory of a file. Each file system has its own way of defining the location of the root directory.

1.1.1.4.Application Category

Application category contains data that provide special features. These data are not needed during the process of reading or writing a file. These data can be useful during an investigation process but need not be trustworthy.

1.2. FILE SYSTEM BENEFITS IN FORENSIC EXAMINATION

In forensic investigation, it is necessary to carry out all file system category data analysis as it allows one to find the location of data structures in other categories like general layout, version of file system application that created the file system, creation date, and file system label. Volume ID or version might be useful when trying to determine on which computer a file system was created. If a file gets corrupted or is lost, additional analysis is more difficult because the examiner has to find backup copies or guess what the values were.