Computer - Meaning and its main parts.

The important component of cyber crime is computer, though Internet, mobile phones are also used as tools of commit cyber crime. Therefore, let us know what a computer is? Computer is an electronic machine with four main parts i.e., CPU, monitor, keyboard and mouse, and it takes input from the user, process it and gives output in a systematic manner. Among the four main parts, keyboard and mouse are input devises and monitor is the output devise. The Central Processing Unit (CPU) is in between the input devices and the output device. The CPU is in fact chasses, a cabinet or a metallic frame on which other electronic items and storage media that are connected or fitted together to have a shape. Such electronic items are mother board, processor, random access memory (RAM), Hard Disk, CD Drive, floppy drive etc. These items are also called as system hardware. Among all these the processor is very important for the point of view of a computer because it has computing ability and all the computations, processes that are performed by the computer are carried out by this item. However from the investigation purposes hard disk is essential because it is a storage device as it holds data or information i.e., electronic evidence to establish a cyber offence. Therefore, seizure of hard disk of a computer is primary concern of investigating officer.

It shall also be noted that apart from hardware, computer system will also has software which is a set of instructions that makes a computer work. There are two major types of software: system software and application software. System software provides the basic functionality of the computer. For example operating systems (OSs), device drivers etc, whereas application software is a programme that makes computer to perform specific type functionality. For example MS Office, Excel Spread Sheets etc.

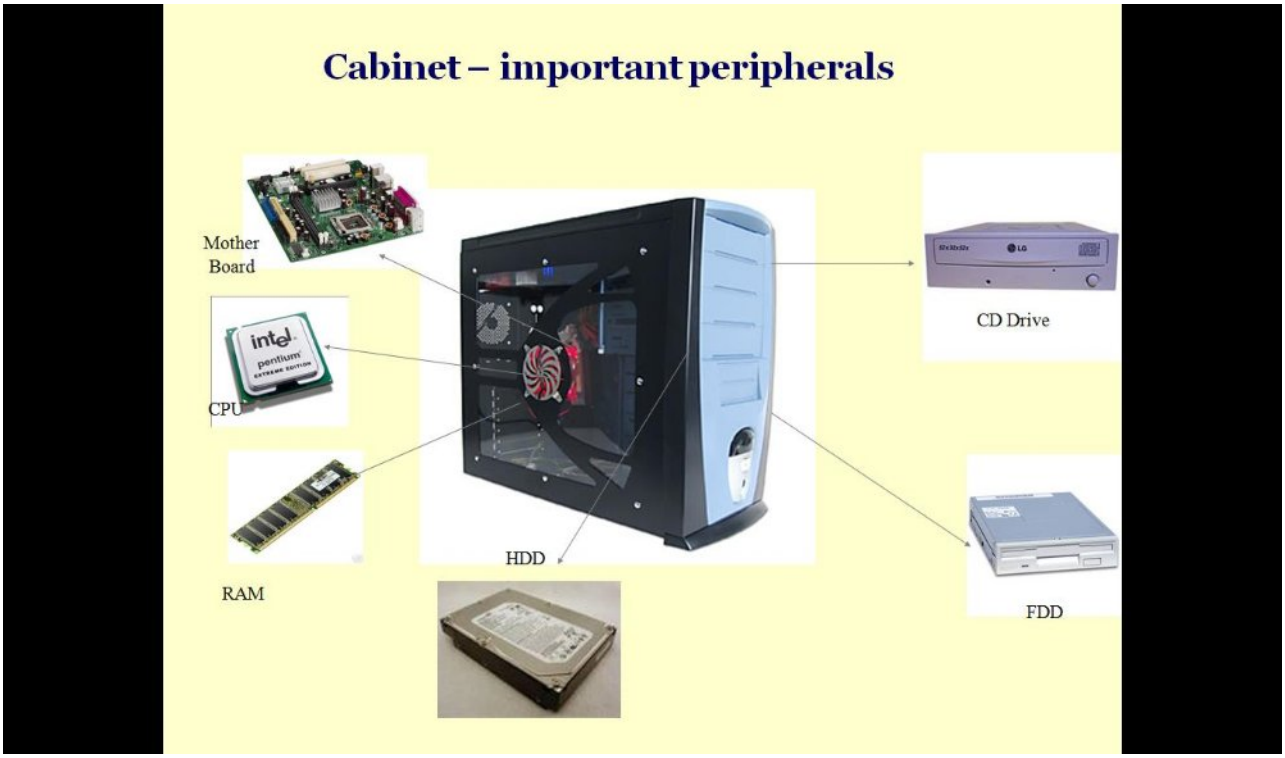
Computer

Cabinet - Central Processing Unit (CPU)

Monitor

Keyboard

Mouse



Other storage media:-

Apart from hard disk there are other storage devices like pen drives, floppy disks, compact disks, mobile phones, SIM cards, memory sticks, digital cameras etc also will have memory that also contain data (electronic evidence). Depending on the requirement of the case, the Investigating Officer shall recover any of these electronic devices if he feels that they contain electronic evidence to establish the case.

Hard Disk

Pendrive

Zip floppy

Mobile phone

DVD

Recovery /Seizure of electronic material objects:-

As per the requirement of the case computers or other electronic storage media will be recovered either from the scene of offence under cover of observation-cum-seizure panchnama / report or from the scene of offence

at the instance of the accused in pursuance of confession-cum-seizure panchanama / report or while conducting searches and seizure.

The main steps that are to be followed in cybercrime scene of offence are:-

- Identification and securing by cordoning the scene of offence.
- Documentation of the scene of offence.
- Collection of electronic evidences from systems that either switched-on or switched-off state.
- Examination of witnesses who are acquainted with the facts of the case at scene of offence.
- As per the requirement of the case making on-sight analysis of material objects, forensic duplication or imaging of the hard disks etc.
- Documentation of evidences that are recovered.
- Packing, labelling and transportation of the evidences that are recovered.

The scenes of offences in cybercrime mostly, but not limited to, are located in the following places.

- Residence.
- Cyber Café
- Offices of organisation, institutions with or without networks

The Investigating Officer while going to scene of offence may be ready with, not limited to, the following

- Two independent mediators, seizure forms / proformas, search warrant.
- For documentation required papers, cable tags, stick-on labels, markers, cameras, notepads etc.
- Required toolkits for disassembling the computers and servers.

- Packing materials like antistatic bags, air bubble tape, hard board boxes.

- If available on-sight cyber forensic analysis tools like EnCase Prtable.

If the scene of offence is a cyber café then IO shall make an effort to identify the computer that was used by the accused by questioning the person who was manning the cyber café, collect CC camera footage/ web camera clippings if so, collect the log register of the Internet users for the relevant period, verify there is any user management software is installed, check for the formatting or replacement policy with regard to the storage devices. If the scene of offence is office premises then apart from the said investigative steps the topology (client –server), many be known, the colleagues of the suspect can be examined to identify the computer used in the offence. If the scene of offence is a home then the type of Internet connection (Wi-Fi/ cable) may be verified.

Another challenge that the I.Os may come across in the scene of offence is the state of the computer whether it is switched-on or off. If the computer is switched-off, to make sure by observing the hard drive and monitor lights, which may indicate that the machine is switched-on. Never switch-on the computer that was already switched-off. Unplug the power and other devices from the sockets. If the computer is switched-on then record what is on the computer screen by making a written note of the contents and photograph the screen. If the screen is blank or screen saver is active, as per the advice of an expert can make small movement of the mouse, get the screen restore then complete the process. If password protected is shown, then take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory i.e., RAM. If such support is not available,

then for windows system remove the power supply from the back of the computer, without closing down the programme. However for UNIX systems gracefully shutting down the system with shut down command is recommended.

The general belief is that in most of the cyber offences if hard disk of the computer is recovered that is sufficient, but it is advisable to seize to CPU/Cabinet because the hard disk would inside safely, and it will also reveal other information for forensic purpose. But what to recover and what is not to be recovered depend on the case that is under investigation. Further to recover hard disk the cabinet / chasses shall be opened and the hard disk shall be carefully taken out and it's description like make, model, serial number, capacity etc shall be noted in the seizure report. Hard disk shall also be carefully packed and preserved. First it shall be kept in anti static polythene cover, then it shall be wrapped in air bubble roll and then it shall be kept in think hard board box. If the investigating officer (IO) does not have the skill to open the cabinet / chasses then it may also not incorrect that the whole cabinet / chasses is recovered so that the hard disk will be there in side of the cabinet safely. In the latter case the description like colour, make of the cabinet shall only be noted in seizure report. If the cabinet is recovered it can be wrapped in white cloth and tied with twine and seals can be put on the knots. It shall be kept in mind that while recording the seizure report complete description of the whole computer like how it is placed, what kind of peripherals like keyboard, mouse, monitor, printer etc are attached to it shall also be noted descriptively in the seizure report and from such state what actually (hard disk or cabinet) has been recovered shall be clearly mentioned in seizure report. The other procedure like following the provisions of Criminal Procedure Code (Cr.P.C), Police Manual etc are all as they are adhered to while investigating the regular conventional cases. The only recommended thing will be care may be

taken that at least one among the independent mediators is with computer knowledge so that they will be in a position to identify various electronic objects. Further, any other storage media i.e., pendrive, compact disk (CD) that IO comes across in the scene of offence and he feels that it also contain evidence relating to the case under investigation, such storage media may also be recovered. If more than one electronic device is recovered, then they shall be allotted a serial number each and all such details are incorporated in the seizure report.

While a pen drive is recovered then also the detailed description of the state, location where it was found may be incorporated in the seizure report. Further its description like make, colour, size shall be incorporated in the seizure report.

Imaging of hard drives and network acquisition:

Imaging of hard drives and network acquisition can be done with the support of experts with required forensic tools. Forensic duplication is also known as disk imaging of cloning or bit stream imaging. In this process a bit by bit transfer of every bit of the hard drive to a new hard drive including free space and slack space.

There will be certain occasions the IO cannot recover hard drive in original because the computer / server may be required for the other public purposes then the process of imaging is done and the original is collected for the investigation purpose leaving the image for the functioning of the computer / server. For imaging special forensic imaging tolls e.g., Falcon Disk Imager and sterile hard drive that has the equal space or higher space that of the original are required. The imaging tool will also generate hash value which is an indicator of data integrity. Hash value is 32 digit alphanumeric value and IT Act allows both MD5 and SHA1 algorithms.

For imaging network drives and file collection network acquisition process is followed. This is done by connecting the evidence computer to the forensic computer via special Ethernet cable called cross over network cable.

	MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual. The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity.	
	In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long. However, SHA-1 is no longer considered secure against well-funded opponents. In 2005, cryptanalysts found attacks on SHA-1 suggesting that the algorithm might not be secure enough for ongoing use, and since 2010 many organizations have recommended its replacement by SHA-2 or SHA-3. But, the available standard is on date SHA-1	

* * *