**Guru Ghasidas Vishwavidyalaya**

**Department of Forensic Science**

**Model answers AS-2334**

**M.Sc. Forensic Science Semester III**

**Paper-I (Computer Forensics and Digital Investigations)**

## Section A

1. i) (a) Windows Vista
   ii) (c) WAN
   iii) (d) All of these
   iv) (b) Point matching
   v) (b) Service provider
   vi) (a) Faraday bag
   vii) (a) Amplified
   viii) (d) All of these
   ix) (c) Android
   x) (c) Firefox

## Section B

2. A computer is a machine/electronic device that receives input, stores and manipulates data, and provides output in a useful format. A basic computer consists of three major components: CPU (Central Processing Unit), IO (Input / Output), and Memory.

PARTS OF A COMPUTER:

1. Keyboard: It is an input device. It translates numbers, letters and special characters into machine understandable language.
2. Mouse: It is an input device. It is a handheld pointing device.
3. Scanner: It is an input device which converts a hard copy into digital format.

4. Printer: It is an output device which converts digital file into hard copy. Forensically important data can be obtained from its spooler or memory chip.
5. Monitor: It is an output device which displays data on a screen.
6. CPU (Central Processing Unit): It carries out all processes and logical operations of the computer. It includes
    - Motherboard- it is a circuit board, physically connecting many components
    - Microprocessor- it executes processes
    - Memory- it stores all data. Major artifact for dead forensics.
    - System clock-maintains date and time
    - Expansion slots

3. **NETWORK ARCHITECTURE**

| | |
|---|---|
| 7 | Application layer |
| 6 | Presentation layer |
| 5 | Session layer |
| 4 | Transport layer |
| 3 | Network layer |
| 2 | Data Link layer |
| 1 | Physical layer |

Network architecture includes Open Systems Interconnection model (OSI model). It is a way of sub-dividing a communications system into smaller parts called layers. A layer is a collection of similar functions that provide services to the layer above it and receives services from the layer below it.

a) Physical layer

The Physical Layer defines the electrical and physical specifications for devices.

b) Data link layer

The Data Link Layer provides the functional and procedural means to transfer data between network layer and physical Layer.

c) Network layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network. Protocols: IP (Internet Protocol) and ARP (Address Resolution Protocol).

d) Transport layer

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. Protocols: TCP (Transmission Control Protocol).

e) Session layer

This Layer provides a user interface to the network where the user negotiates to establish a connection.

f) Presentation layer

The presentation layer transforms data into the form that the application accepts.

g) Application layer

The Application Layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. Protocols: Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Hyper Text Transfer Protocol (http).

4. i) **CYBER TERRORISM**

Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Cyber terrorism is a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic.

Cyber terrorism can also be defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives. Objectives may be political or ideological since this is a form of terrorism.

Cyber terrorism includes:

- Use of viruses to disrupt information
- Destroy network infrastructure
- Use cyber space to threaten
- Hacking
- Creating DoS and DDos attacks: Denial of Service attack involves flooding the target resource with external communication requests. This overload prevents the resource from responding to legitimate traffic, or slows its response so significantly that it is rendered effectively unavailable. A DDoS attack, uses many devices and multiple Internet connections, often distributed globally into what is referred to as a botnet. A DDoS attack is, therefore, much harder to deflect, simply because there is no single attacker to defend from, as the targeted resource will be flooded with requests from many hundreds and thousands of multiple sources.

**4. ii) SPAMMING**

Spam is the use of electronic messaging systems to send unsolicited bulk messages, especially advertising, indiscriminately. Spams are a waste of resources, storage space and time.

Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high.

Spam can be used to spread computer viruses, Trojan horses or other malicious software. The objective may be identity theft, or worse. It can be used for political advertising. Spamming can be done through:

- Email
- Instant messaging
- Newsgroups and forums
- Mobile phones
- Social networking
- Blogs

## 5. **COMPUTER FORENSICS**

Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

A Computer Forensics investigation, involves four major areas:

1. Acquisition: Obtaining the original evidence.
2. Preservation: Protecting the original evidence.
3. Analysis: Finding relevant evidence.
4. Presentation: Presenting the evidence in court.

### 1. <u>Acquisition</u>

This involves the evidence search, evidence recognition, evidence collection and documentation at the crime scene. Appropriate procedures should be followed and documented to ensure that the electronic evidence collected is not altered or destroyed. All potential sources of evidence should be identified and labeled properly before packing. First responders should be trained to handle digital evidence because it is fragile. Digital evidence is easily altered if not handled properly. Simply turning a computer on or operating the computer changes and damages evidence.

– Evidence can be easily modified.
– Evidence can be easily destroyed.

Evidence collection of the digital or mobile devices is an important step and requires proper procedures or guidelines to make it work. We can categorize evidence collection of the digital devices into two categories:

A. Volatile Evidence Collection
B. Non-Volatile Evidence Collection

**A. Volatile Evidence Collection**

Majority of the evidence involving mobile devices will be of volatile nature. Collecting volatile evidence presents a problem as the device state and memory contents may be changed. If the device is running out of battery power, the entire information will be lost soon. In that case, adequate power needs to be maintained if possible by using the power adaptor or replacing batteries. If maintaining the battery power seems doubtful, the contents of the memory should be imaged using appropriate tools as quickly as possible. RAM (Random Access Memory) contains data only while the computer is on. It is temporary storage and is cleared when the computer shuts down or restarts.

**B. Non-volatile Evidence Collection**

This phase involves collecting evidence from external storage media such as USB memory sticks, SD cards etc. All power cables, adaptors, cradle and other accessories should also be collected. Care should be taken to look for evidence of non-electronic nature, like written passwords, hardware and software manuals and related documents, computer printouts etc.
Hard disk drives (HDDs) can hold thousands of Documents, Pictures, Music files, Movies, Passwords, and Emails etc.

2. <u>Preservation</u>

This phase includes packaging, transportation and storage of evidence before analysis. Use of ordinary plastic bags may cause static electricity. Hence anti-static packaging of evidence is essential. The device and accessories should be put in an envelope and sealed before placing it in

the evidence bag. The evidence bag must be kept in a radio frequency isolation container to avoid further communications with any other device. All the containers holding these evidence bags must also be properly labeled. Adequate precautions are necessary as the sources of evidence could be easily damaged while transportation because of shock, excessive pressure, humidity or temperature. Afterwards the device can be moved to a secure location where a proper chain of custody can be maintained and examination and processing of evidence can be started. The evidence should be stored in a secure area and should be protected from electromagnetic radiations, dust, heat and moisture. Unauthorized people should not have access to the storage area.

3. Analysis

The data should be analyzed while keeping its integrity intact. This phase involves examining the contents of the collected evidence by forensic specialists and extracting information, which is critical for proving the case. Finding evidence for system tampering, data hiding or deleting utilities, unauthorized system modifications etc. should also be performed. Detecting and recovering hidden or obscured information is a major tedious task involved. Data should be searched thoroughly for recovering passwords, finding unusual hidden files or directories, file extension and signature mismatches etc. It is required to prove that the evidence has not been altered after being possessed by the forensic specialist and hence hashing techniques (MD5 or SHA) must be used for mathematical authentication of data.

4. Presentation

This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation. After extracting and analyzing the evidence collected, the results may need to be presented before a wide variety of audience including law enforcement officials, technical experts, legal experts, corporate management etc. A report consisting of a detailed summary of the various steps in the process of investigation and the conclusions reached must be provided. In many cases, the forensic specialist may have to give an expert testimony in court. The complex terms involved in various stages of investigation process needs to be explained in

layman's terminology. The expertise and knowledge of the forensic examiner, the methodology adopted, tools and techniques used etc. are all likely to be challenged before a jury. Along with the report, supporting materials like copies of digital evidence, chain of custody document, printouts of various items of evidence etc. should also be submitted.

## 6. **Symmetric encryption**

In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption.

Two basic components of classical ciphers:

1. Substitution

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns. The substitution encryption can be carried out in one of two ways:

i. Stream algorithm

It encrypts bits of information one at a time. It operates on one bit of data at a time and encrypts data bit by bit.

ii. Block algorithm

It encrypts data in blocks i.e. encrypts information by breaking it down into blocks and encrypting data in each block. Block cipher encrypts data in fixed size blocks (64 bits).

2. Transposition

A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher where letters are arranged in a different order.

**Asymmetric encryption**

Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

As long as a user's private key remains protected and secret, incoming communication is secure. At any time, a system can change its private key and publish the companion public key to replace its old public key.

## 7. **REPRESENTATION IN COURT**

As digital forensic examiners/analysts, we must report and present our findings on a very technical discipline in a simplistic manner.

Presenting electronic evidence in court presents many technical and practical challenges.
Some courts are already wired for electronic presentation, but many courts are not. A courtroom presentation system typically consists of a projector screen or large flat panel monitors for the jury, individual monitors for the judge, witness, clerk, and counsel tables. In addition CD/DVD players may be present.
Before a presentation, determine where the electric outlets are located and prepare a short checklist of standard courtroom display equipment that may be required:

- Laptop (Primary and Backup)
- Projector
- Audio Speaker (if audio is needed)
- Projector Screen
- Cables and Extension Cord
- Power Strips

The two most common tools for the presentation of electronic evidence are Microsoft's PowerPoint and trial presentation software such as TrialDirector and Sanction. Trial Presentation Software has the ability to bring up an exhibit on-the-fly and call-out a specific portion of the exhibits, as well as high-light and annotate. In addition you can show multiple exhibits at once, which is an invaluable tool for comparing documents or linking evidence. Lastly you can present a variety of media, including deposition video and electronic exhibits in native format such as Excel and Word documents.

Demonstratives are almost necessities for any arbitration, mediation, or trial. Presenting arguments at trial is much like telling a story or putting on a play; there is hardly a case that doesn't warrant the use of visuals. They educate and can persuade. They can help you as an attorney to present your arguments and evidence visually; and they can also help your experts convey what can often be a very complicated concept in a visual way. There are many types of visual aids including static graphics, 2D and 3D drawings, 2D and 3D animations, and Interactive graphics such as Adobe Flash. The main benefits of interactive graphics are that they are incredibly flexible and can be presented in a non-linear dynamic fashion. A typical example of an interactive Flash demonstrative is a timeline. Interactive graphic gives the operator the ability to click on any event to instantly locate the supporting exhibit(s) to support that event. These interactive demonstratives can be a perfect tool for presenting evidence piece by piece in a very organized fashion. People learn much more visually.

**Advantages of using software**

1. Show specific portions of exhibits
2. Highlight
3. Compare
4. Link evidences
5. Present a variety of media in original format e.g. video, excel, doc
6. Present arguments and evidences visually

Three broad categories of digital evidence raise issues that are especially important to address in a pretrial meeting:

**1. Background evidence**

These types of evidences provide background evidence to understand the technical issues in the case. These act as supportive evidences and not as direct evidences.

**2. Substantive evidence.**

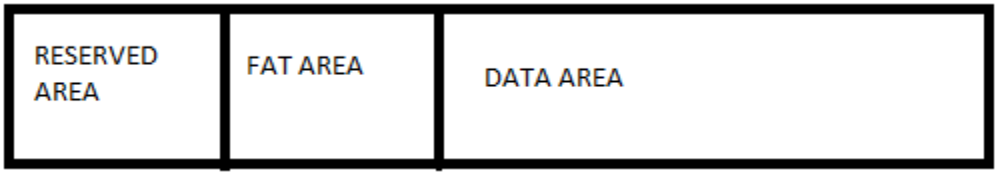
These are direct evidences in a case. Substantive evidences may be live, static or use of internet in the Court. The presentation of substantive evidence will raise tactical and technical considerations.

**3. Illustrative evidence.**

Illustrative evidence may be used as examples to help in understanding the case. For example, animations or pictures which are designed to better understand the happenings of the case.

**8. Windows file systems**

**FAT (File Allocation Table)**



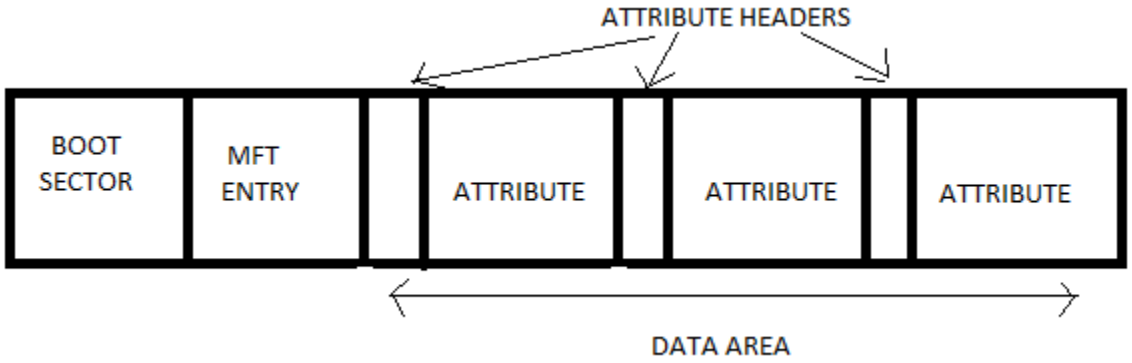

Reserved area contains the boot code. FAT area contains the sector address and cluster chaining information. The data area contains the file contents.

In FAT 12 and FAT 16, the FAT area is immediately followed by the root directory (in the data area). There is no backup of boot sector.

In FAT 32, the root directory can be present anywhere in the data area. There is a backup of boot sector.

**2. NTFS (New Technology File System)**

This is a Windows file system which allows encryption and disk compression. NTFS is not supported below Windows 98.




MFT (Master File Table) itself is a file and itself has an entry $MFT that describes on-disk location of MFT. MFT contains the metadata. Attribute header identifies the type of attribute, its size, name, compression, encryption etc.

The header of attribute identifies if the attribute is resident or on-resident. If an attribute is resident, the contents will immediately follow the header. If the attribute is non-resident, the header will give cluster addresses. Resident attribute stores its contents in MFT entry with attribute header. Non-resident attribute stores its contents in an external cluster in file system.