SYED AMMAL ENGINEERING COLLEGE
(An ISO 9001: 2008 Certified Institution)
Dr. E.M.Abdullah Campus, Ramanathapuram – 623 502
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CS6004-CYBER FORENSICS

Two Marks Question with Answers

Unit-I

Network layer Security and Transport Layer security

1. **State the different protocols for securing communications in the Internet.**

- Cryptographic methods and protocols have been designed for different purposes in securing communication on the Internet. These include, for instance, the SSL and TLS for HTTP Web traffic, S/MIME and PGP for e-mail and IPsec for network layer security.

2. **What is the purpose of IPsec Protocol?**

- IPsec is designed to protect communication in a secure manner by using TCP/IP. The IPsec protocol is a set of security extensions developed by the IETF and it provides privacy and authentication services at the IP layer by using modern cryptography.

3. **Mention the two main transformation types that form the basis of IPsec.**
   - There are two main transformation types that form the basics of IPsec,

     1. The Authentication Header (AH) and

     2. The Encapsulating Security Payload (ESP).

- Both AH and ESP are two protocols that provide connectionless integrity, data origin authentication, confidentiality and an anti-replay service.

- These protocols may be applied alone or in combination to provide a desired set of security services for the IP layer. They are configured in a data structure called a Security Association (SA).

4. Specify the basic components of the IPsec security architecture.

- The basic components of the IPsec security architecture are explained in terms of the following functionalities:
  - ❖ Security Protocols for AH and ESP
  - ❖ Security Associations for policy management and traffic processing
  - ❖ Manual and automatic key management for the Internet Key Exchange (IKE), the
  - ❖ Oakley key determination protocol and ISAKMP.
  - ❖ Algorithms for authentication and encryption.

5. What is IPsec Protocol Document?

- In November 1998, the Network Working Group of the IETF published RFC 2411 for IP Security Document Roadmap. This document is intended to provide guidelines for the development of collateral specifications describing the use of new encryption and authentication algorithms used with the AH protocol as well as the ESP protocol.

6. What are the seven-group documents describing the set of IPsec protocols? o The seven-group documents describing the set of IPsec protocols are:

1. **Architecture:** The main architecture document covers the general concepts, security requirements, definitions and mechanisms defining IPsec technology.

2. **ESP:** This document covers the packet format and general issues related to the use of the ESP for packet encryption and optional authentication.

3. **AH:** This document covers the packet format and general issue related to the use of AH for packet authentication.

4. **Encryption algorithm:** This is a set of documents that describe how various encryption algorithms are used for ESP.

5. **Authentication algorithm:** This is a set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.

6. **Key management:** This is a set of documents that describe key management schemes.

7. **DOI:** This document contains values needed for the other documents to relate each other.

7. **Name the three parameters that uniquely identify the SA.**

- **Security Associations** (SAs) is uniquely identified by three parameters as follows:

Security Parameters Index (SPI): This is assigned to each SA

IP Destination Address: This is the address of the destination endpoint of the SA.

Security Protocol Identifier: This identifier indicates whether the association is an AH or ESP security association.

8. **What is a Security association database?**

- The **SAD** contains parameters that are associated with each security association. Each SA has an entry in the SAD. For outbound processing, entries are pointed to by entries in the SPD.

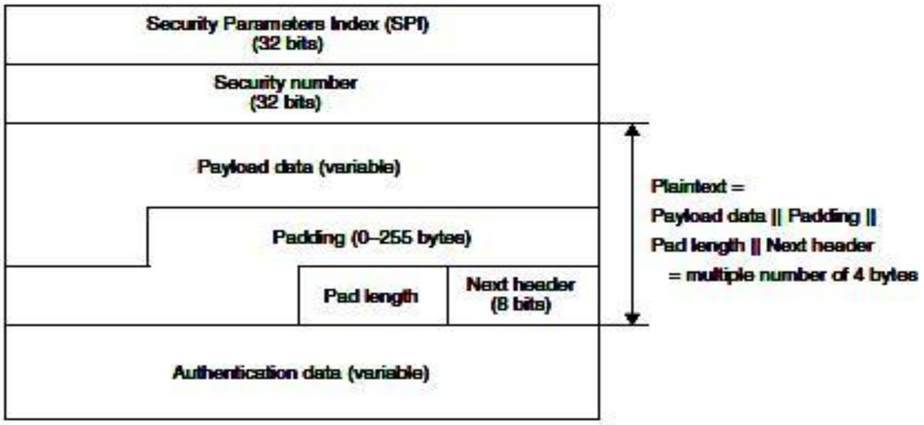
9. **List the types of SAs.**

- There are two types of SAs to be defined: a **Transport Mode SA** and a **Tunnel Mode SA**. A transport mode provides protection primarily for upper-layer protocols. Tunnel mode provides protection to the entire IP packet. A tunnel mode SA is essentially an SA applied to an IP tunnel.

10. **What is HMAC?**

- An HMAC mechanism can be used with any iterative hash functions in combination with a secret key. HMAC uses a secret key for computation and verification of the message authentication values

11. **Give the structure of the ESP Packet .**


Security Parameters Index (SPI)
(32 bits)
Security number
(32 bits)
Payload data (variable)
Padding (0–255 bytes)
Pad length
Next header
(8 bits)
Authentication data (variable)
Plaintext =
Payload data || Padding ||
Pad length || Next header
= multiple number of 4 bytes

12. What is ISAKMP?

- **ISAKMP** (Internet Security Association and Key Management Protocol) defines a framework for Security Associations management and cryptographic key establishment for the Internet. This framework consists of defined exchange, payloads and processing guidelines.

13. List the Payload Types for ISAKMP.

- Security Association Payload
- Proposal Payload
- Transform Payload
- Key Exchange Payload
- Identification Payload
- Certificate Payload
- Certificate Request Payload
- Hash Payload
- Signature Payload
- Nonce Payload
- Notification Payload
- Delete Payload
- Vendor ID Payload

14. What is a SSL Session?

- An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. An SSL session coordinates the states of the client and server.

15. List the elements of a session state.

- The session state is defined by the following elements:
    - Session identifier

- ❖ Peer certificate
- ❖ Compression method
- ❖ Cipher spec
- ❖ Master secret
- ❖ Is resumable

16. List the elements of a connection state.

- o The connection state is defined by the following elements:
    - ❖ Server and client random
    - ❖ Server write MAC secret
    - ❖ Client write MAC secret
    - ❖ Server write key
    - ❖ Client write key
    - ❖ Initialization vectors
    - ❖ Sequence numbers

18. Mention the use of CCS Protocol.

- o The change cipher spec protocol is used to change the encryption being used by the client and server. It is normally used as part of the handshake process to switch to symmetric key encryption.

- o The CCS protocol is a single message that tells the peer that the sender wants to change to a new set of keys, which are then created from information exchanged by the handshake protocol.

19. What is HMAC?

- o A Keyed-hashing Message Authentication Code (HMAC) is a secure digest of some data protected by a secret. Forging the HMAC is infeasible without knowledge of the MAC secret.

- o HMAC can be used with a variety of different hash algorithms, namely MD5 and SHA-1, denoting these as HMAC MD5(secret, data) and HMAC SHA-1(secret, data).

20. State the differences between SSL version 3 and TLS.

SSL	TLS
In SSL the minor version is 0 and major version is 3.	In TLS, the major version is 3 and the minor version is 1.
SSL use HMAC alg., except that the padding bytes concatenation.	TLS makes use of the same alg.
SSL supports 12 various alert codes.	TLS supports all of the alert codes defined in SSL3 with the exception of no _ certificate.

21. Name the SSL Cipher Suites.

- Diffie-Hellman key exchange
- RSA
- Fortezza
- RC2, RC4, 3DES, DES40

22. What is PRF?

- TLS utilizes a pseudo-random function (PRF) to expand secrets into blocks of data for the purposes of key generation or validation.
- The PRF takes relatively small values such as a secret, a seed and an identifying label as input and generates an output of arbitrary longer blocks of data.

23. State the purpose of alert messages.

- Alert messages convey the severity of the message and a description of the alert. Alert messages with a fatal level result in the immediate termination of the connection.

24. What are the parameters for key block computation?

- The computation of the key block parameters (MAC secret keys, session encryption keys and IVs) is defined as follows:

  key_block = PRF (master_secret,__key
  expansion‘‘,SecurityParameters.server_random||

  SecurityParameters.client_random)

25. How are errors handled in TLS?

- Error handling in the TLS Handshake Protocol is very simple. When an error is detected, the detecting party sends a message to the other party. Upon transmission or receipt of a fatal alert message, both parties immediately close the connection.

UNIT II

E-MAIL SECURITY & FIREWALLS

1. Define PGP.

- PGP stands for **Pretty Good Privacy**.
- PGP uses a combination of symmetric secret-key and asymmetric public-key encryption to provide security services for electronic mail and data files.
- It also provides data integrity services for messages and data files by using digital signature, encryption, compression (zip) and radix-64 conversion (ASCII Armor).

2. Define MIME.

- MIME stands for Multipurpose Internet Mail Extension.
- MIME is an extension to the RFC 2822 framework which defines a format for text messages being sent using e-mail.

3. Define S/MIME.

- **Secure/Multipurpose Internet Mail Extension (S/MIME)** is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.

4. What is meant by Huffman compression?

- **Huffman compression** is a statistical data compression technique which reduces the average code length used to represent the symbols of an alphabet.
- Huffman code is an example of a code which is optimal when all symbols probabilities are integral powers of 1/2.
- A technique related to Huffman coding is **Shannon–Fano coding**.

5. What is a Shannon–Fano coding?

- A technique related to Huffman coding is Shannon–Fano coding. This coding divides the set of symbols into two equal or almost equal subsets based on the probability of occurrence of characters in each subset.
- The first subset is assigned a binary 0, the second a binary 1.

6. **Define Radix-64 Conversion.**

- A radix-64 conversion is a wrapper around the binary PGP messages, and is used to protect the binary messages during transmission over non-binary channels, such as Internet e-mail.

7. **List out the data fields contained in ASCII Armor Format.** ○ The data fields contained in ASCII Armor format are

- An Armor head line
- Armor headers
- A blank line,
- ASCII-Armored data
- Armor checksum and
- Armor tail.

8. **Define an Armor head line.**

○ An armor head line consists of the appropriate header line text surrounded by five dashes (‗- ‘, 0x2D) on either side of the header line text.

○ The header line text is chosen based upon the type of data that is being encoded in Armor, and how it is being encoded.

9. **List out the strings contained in header line text.**

○ **BEGIN PGP MESSAGE** – used for signed, encrypted or compressed files.

○ **BEGIN PGP PUBLIC KEY BLOCK** – used for armouring public keys.

○ **BEGIN PGP PRIVATE KEY BLOCK** – used for armouring private keys.

○ **BEGIN PGP MESSAGE, PART X/Y** – used for multipart messages, where the armour is divided amongst Y parts, and this is the Xth part out of Y.

○ **BEGIN PGP MESSAGE, PART X** – used for multipart messages, where this is the Xth part of an unspecified number of parts; requires the MESSAGE-ID Armor header to be used.

○ **BEGIN PGP SIGNATURE** – used for detached signatures, PGP/MIME signatures and natures following clear-signed messages.

10. Define Armor headers.

- Armor headers are pairs of strings that can give the user or the receiving PGP implementation some information about how to decode or use the message.

- The Armor headers are a part of the armour, not a part of the message, and hence are not protected by any signatures applied to the message.

- The format of an Armor header is a (key, value) pair. A colon (_:‘ 0x38) and a single space (0x20) separate the key and value.

11 Define Armor checksum.

- Armor checksum is a 24-bit CRC converted to four characters of radix-64 encoding by the same MIME base 64 transformation, preceded by an equals sign (=).

- The CRC is computed by using the generator 0x864cfb and an initialization of 0xb704ce.

- The accumulation is done on the data before it is converted to radix-64, rather than on the converted data.

- The checksum with its leading equals sign may appear on the first line after the base 64 encoded data.

12. Define packet headers.

- A PGP message is constructed from a number of packets. A packet is a chunk of data which has a tag specifying its meaning.

- Each packet consists of a packet header of variable length, followed by the packet body.

13. Define Attribute certificate.

- An X.509 AC is a separate structure from a subject‘s PKIX certificate.

- A subject may have multiple X.509 ACs associated with each of its PKIX certificates.

- Each X.509 AC binds one or more attributes with one of the subject‘s PKIXs.

14. Define Cryptographic Message Syntax (CMS).

- CMS allows for a wide variety of options in content and algorithm support. This subsection puts forth a number of support requirements and recommendations in order

to achieve a base level of interoperability among all S/MIME implementations.

- CMS provides additional details regarding the use of the cryptographic algorithms.

15. Define Digest Algorithm Identifier.

- This type identifies a message digest algorithm which maps the message to the message digest.
- Sending and receiving agents must support SHA-1.
- Receiving agents should support MD5 for the purpose of providing backward compatibility with MD5-digested S/MIME v2 Signed Data objects.

16. Define Signature Algorithm Identifier.

- Sending and receiving agents must support id-dsa defined in DSS. Receiving agents should support rsa Encryption, defined in PRCS-1.

17. Define Key Encryption Algorithm Identifier.

- This type identifies a key encryption algorithm under which a content encryption key can be encrypted.
- A key-encryption algorithm supports encryption and decryption operations.
-

18. What is meant by Enveloped-data content type ?

- An application/prcs7-mime subtype is used for the enveloped-data content type.
- This content type is used to apply privacy protection to a message. The type consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.

19. Define digital envelope.

- The combination of encrypted content and encrypted content-encryption key for a recipient is called a **digital envelope** for that recipient.

20. What is meant by triple wrapped message?

- A **triple wrapped message** is one that has been signed, then encrypted and then signed again.
- The signers of the inner and outer signatures may be different entities or the same entity.
- The S/MIME specification does not limit the number of nested encapsulations, so there may be more than three wrappings

21. Define firewall.

- A firewall is a device or group of devices that controls access between networks.
- A firewall generally consists of filters and gateway(s), varying from firewall to firewall.
- It is a security gateway that controls access between the public Internet and an intranet (a private internal network) and is a secure computer system placed between a trusted network and an un trusted internet.

22. What are the three main categories of firewalls?

- Firewalls can be classified into three main categories:
- Packet filters,
- Circuit-level gateways and
- Application-level gateways.

23. Bastion Host

- A bastion host is a publicly accessible device for the network‘s security, which has a direct connection to a public network such as the Internet.
- The bastion host serves as a platform for any one of the three types of firewalls. Bastion hosts must check all incoming and outgoing traffic and enforce the rules specified in the security policy.

UNIT III

INTRODUCTION TO COMPUTER FORENSICS

1. Define the term "Computer Forensics".

- Computer forensic science, computer forensics, and digital forensics may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence. It also involves collection and presentation of computer-related evidence. Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

2. What are the roles of a Computer in a Crime?

- A computer can play one of three roles in a computer crime.
- A computer can be the target of the crime,
- It can be the instrument of the crime, or
- It can serve as an evidence repository storing valuable information about the crime.

3. State the objectives of Computer Forensics.

- The objective of Computer Forensics is to recover, analyze, and present computer-based material in such a way that it is useable as evidence in a court of law.

4. Who Can Use Computer Forensic Evidence?

- Criminal Prosecutors
- Civil litigations
- Corporations
- Law enforcement officials

5. Mention some problems with Computer Forensic Evidence.

- Computer data changes moment by moment.
- Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.

- The process of collecting computer data may change it—in significant ways.
- The processes of opening a file or printing it out are not always neutral.

- Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long

6. Define Computer Crime and digital crime.

- Computer crime has been traditionally defined as any criminal act committed via computer.
- Computer-related crime has been defined as any criminal act in which a computer is involved, even peripherally.
- Cybercrime has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses.
- Digital crime, a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data.

7 What Is Phreaking?

- Phreaking involves the manipulation of telecommunications carriers to gain knowledge of telecommunications, and/or theft of applicable services. It is also known as telecommunications fraud, and includes any activity that incorporates the illegal use or manipulation of access codes, access tones, PBXs, or switches.

8. State the motivations for computer intrusion or theft of information in contemporary society.

- Boredom (informational voyeurism)
- Intellectual challenge (mining for knowledge—pure hackers),
- Revenge (insiders, disgruntled employees, etc.),
- Sexual gratification (stalking (nuisance), harassment, etc.),
- Economic (criminals), and
- Political (Hacktivists, terrorists, spies, etc.).

9. List some digital forensics tools.

–Drive Spy and Image

–FTK

–X-Ways Forensics

10. What is CMOS?

○ CMOS denotes Complementary Metal Oxide Semiconductor. The Computer stores system configuration and date and time information in the CMOS.

11. What methods are available for recovering passwords?

○ The three ways to recover passwords:
  - Dictionary attacks
  - Brute-force attacks
  - Rainbows tables

12. Give the hierarchy of Contemporary Cybercriminals

There are five general categories of cybercriminals in today‘s society:

2. Script kiddies,
3. Cyberpunks,
4. Hackers/crackers,
5. Cybercriminal organizations, and

Hacktivists

13. State the types of computer records.

Computer records are usually divided into:

–Computer-generated records

–Computer-stored records

14. What is FIOA?

- FOIA: **Freedom of Information Act** , allows citizens to request copies of public documents created by federal agencies.

15. **List the tasks of a Computer Forensics Examination Protocol**

- Perform the investigation with a GUI tool
- Verify your results with a disk editor
- Compare hash values obtained with both tools

SYED AMMAL ENGINEERING COLLEGE
(An ISO 9001: 2008 Certified Institution)
Dr. E.M.Abdullah Campus, Ramanathapuram – 623 502
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNIT IV

EVIDENCE COLLECTION AND FORENSICS TOOLS

1. List out the disk drive components.

Geometry,

Head,

Tracks,

Cylinders, and
Sectors.

2. What is meant by ZBR?

ZBR stands for Zoned bit recording. In ZBR the platter‘s inner tracks are being shorter than its outer tracks. Grouping tracks by zones ensures that all tracks hold the same amount of data.

3. Define track density.

Track density is the space between each track.

4. List out the properties handled at the drive’s hardware.

- Zoned bit recording (ZBR)
- Track density
- Areal density
- Head and cylinder skew

5. Define Master boot record (MBT).

The boot disk contains a file called the Master Boot Record (MBR) which stores information about partitions on a disk and their locations, size and other important items.

6. Define FAT.

File allocation table is a file structure database that Microsoft originally designed for floppy disks. FAT is used on file systems before windows NT and 2000.

7. List out the versions of FAT.

- FAT12
- FAT16
- FAT32
- FATX

8. Define VFAT.

Microsoft developed virtual file allocation table (VFAT) to handle long file names when it released Windows 95 and Windows for workgroups.

9. Define data runs.

The MFT record provides cluster addresses where the file is stored on the drive‘s partition. It is referred to as data runs.

10. What is meant by logical cluster numbers?

When a disk is created as an NTFS file structure, the OS assigns logical clusters to the entire disk partition. These assigned clusters are called logical cluster numbers (LCNs).

11. What is meant by Encrypting File System (EFS)?

EFS were introduced with Windows 2000. It implements a public key and private key method of encrypting files, folders, or disk volumes.

12. Define recovery certificate.

When EFS is used in Windows Vista Business Edition or higher, XP Professional, or 2000, a recovery certificate is generated and sent to the local Windows administrator account. The users can apply EFS to files stored on their local workstations or a remote server.

13. What is meant by trusted platform module?

A Trusted Platform Module (TPM) microchip generates encryption keys and authenticates logins.

14. List out some of the open-source encryption tools.

- TrueCrypt
- CrossCrypt
- FreeOTFE

15. Define Registry.

A database that stores hardware and software configuration information, network connections, user preferences, and setup information.

16. Write down the two modes of Windows 9x Oss.

o DOS protected-mode interface (DPMI) o
Protected-mode GUI

17. **Define Virtual machine.**

A virtual machine allows you to create a representation of another computer on an existing physical computer. Virtual machines enable you to run other OSs from a Windows computer.

18. Give examples for Computer crimes.

- Fraud
- Check fraud
- Homicides

19. Write down the Tasks for planning your investigation.

- Identify the case requirements
- Plan your investigation

- Conduct the investigation
- Complete the case report
- Critique the case

20. **What is National Software Reference Library (NSRL) project ?**

NSRL collects all known hash values for commercial software applications and OS files. It uses SHA-1 to generate a known set of digital signatures called the Reference Data Set

(RDS). It helps filtering known information and can use RDS to locate and identify known bad files

21. What is meant by HAZMAT?

HAZMAT stands for hazardous materials. The recovery process includes decontaminating digital components needed for the investigation. It destroys the digital evidence.

22. What is the use of initial response field kit?

The initial response field kit should be a lightweight and easy to transport. With this kit, you can arrive at a scene, acquire the data you need, and return to the lab as quickly as possible.

23. What is meant by sparse acquisition?

The technique for extracting evidence from large systems. It extracts only data related to evidence for your case from allocated files.

24. What are the functions of evidence custody form?

- Identifies the evidence
- Identifies who has handled the evidence
- Lists dates and times the evidence was handles.

25. Define CRC.

CRC stands for cyclic redundancy check. It is a mathematical algorithm that determines whether a file‘s contents have changed.

26. Define message digest 5 (MD5).

It is a mathematical formula that translates a file in to a hexadecimal code value, or a hash value. If a bit or byte in the file changes, it alters the digital hash.

27. List out the three rules for forensic hashes.

- You can‘t predict the hash value of a file or device,
- No two hash values can be the same ,
- If anything changes in the file or device, the hash value must change.

28. List out the functions of FTK.

- Extract the image from a bit-stream image file
- Analyze the image

29. List out the types of computer forensics tools.

- Hardware forensic tools
- Software forensic tools

30. Write down the task performed by computer forensics tools.

- Acquisition
- Validation and discrimination
- Extraction
- Reconstruction
- Reporting

31. What is meant by acquisition and list out its functions?

Acquisition means making a copy of the original drive.
Acquisition sub functions are,

- Physical data copy

- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition

32. Give the types of data-copying methods used in software acquisitions.

The two types of data-copying methods are used in software acquisitions:

- Physical copying of the entire drive
- Logical copying of a disk partition

33. Distinguish between Validation and discrimination.

- Validation means ensuring the integrity of data being copied.
- Discrimination of data involves sorting and searching through all investigation data.

34. What is meant by reconstruction?

Reconstruction means re-creating a suspect drive to show what happened during a crime or an incident. Its sub functions are,

- Disk-to-disk copy
- Image-to-disk copy
- Partition-to-partition copy
- Image-to-partition copy

35. Define write-blocker.

Write-blocker prevents data writes to a hard disk. It is of two variants

- Software-enabled blockers
- Hardware options

Software write-blockers are OS dependant. Example: PDBlock from Digital Intelligence. Hardware options are ideal for GUI forensic tools. It act as a bridge between the suspect drive and the forensic workstation.

UNIT V

ANALYSIS AND VALIDATION

1. **List out the file systems in which FTK can perform forensic analysis.**

Microsoft FAT12, FAT 16 and FAT32, Microsoft NTFS (for Windows NT, 2000, XP and Vista) Linux Ext2fs and Ext3fs.

2. **Define scope creep.**

In the corporate environment, if litigation is involved, the company attorney often directs the investigator to recover as much information as possible. Satisfying this demand becomes a major undertaking with many hours of tedious work. These types of investigations results in scope creep, in which an investigation expands beyond the original description because of unexpected evidence you find, prompting the attorney to ask you to examine other areas to recover more evidence. Scope creep increases the time and resources needed to extract, analyze, and present evidence.

3. **What is meant by Known File Filters (KFF)?**

Access Data has a separate database called Known File Filters (KFF) which is available only with FTK. The KFF filters known program files from view, such as MSWord.exe, and identifies known illegal files, such as child pornography.

4. **What is meant by auto image checksum verification?**

Prodiscover‘s .eve files contain metadata that includes the hash value. When an image file is loaded in ProDiscover, it‘s hashed and compared to the hash value in the stored metadata. If the hashes don‘t match, ProDiscover notifies you that the acquisition is corrupt and can‘t be considered to be reliable evidence. This feature is called auto image checksum verification.

5. **What is meant by data hiding?**

Data hiding involves changing or manipulating a file to conceal information. It includes hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption and setting up password protection.

6. **List out some of the disk management tools.**

The disk management tools are,

Partition Magic,

Partition Master, and

Linux Grand Unified Bootloader (GRUB)

7. What is meant by bit-shifting?

Bit-shifting is a well known technique for hiding data by shifting bit patterns to alter the byte values of data. Bit-shifting changes data from readable code to data that looks like binary executable code.

8. Define steganography.

Steganography comes from the Greek word for ―hidden writing‖. Hiding messages in such a way that only the intended recipient knows the message is there.

9. Define Steganalysis.

Steganalysis is a term for detecting and analyzing steganography files.

10. Define Digital watermarking.

Digital watermarking has been developed as a way to protect file ownership. It is usually not visible when used for steganography.

11. List out the Steganalysis methods.

Stego-only attack Known
cover attack Known
message attack Chosen
stego attack Chosen
message attack

12. What is meant by key escrow?

Encrypted files are encoded to prevent unauthorized access. To decode an encrypted file, users supply a password or passphrase. Without the passphrase, recovering the contents of encrypted file is difficult. Hence key escrow is a commercial encryption program to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure.

13. List out some of the password cracking tools.

- Last Bit
- AccessData PRTK
- ophcrack
- John the Ripper
- Passware

14. Define rainbow table.

A rainbow table is a file containing the hash values for every possible password that can be generated from a computer‘s keyboard. No conversion necessary, so it is faster than a brute-force or dictionary attack.

15. Define salting passwords

A salting password alters hash values and makes cracking passwords more difficult.

16. List out the three ways to recover passwords.

- Dictionary attacks
- Brute-force attacks
- Rainbows tables

17. What is meant by remote acquisition?

Remote acquisitions are useful for making an image of a drive when the computer is far away from your location or when you don‘t want a suspect to be aware of an ongoing investigation.

18. Define network forensics.

Network forensics is a process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network.

Network forensics can also help you to determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program.

19. What is the use of network logs?

Network logs can be used in determining what happened on a machine and give clues on what to search for.

20. Define layered network defense network strategy.

A layered network defense network strategy sets up layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper in to the network an attacker gets, the more difficult access becomes and the more safeguards are in place.

21. Define Defense in Depth (DiD) strategy.

The National security agency (NSA) developed a simple approach called a defense in depth strategy (DiD) which has three modes of protection namely,

- People,
- Technology,
- Operations.

22. Define order of volatility (OOV).

The order of volatility means how long a piece of information lasts on a system. Data such as RAM and running processes might exist for only milliseconds; other data such as files stored on the hard drive might last for years.

23. List out the tools available to capture RAM.

- Mantech Memory DD
- Win32dd
- winen.exe from Guidance Software
- BackTrack 3

24. What is the purpose of Tcpdump program?

A common way for examining network traffic is running the Tcpdump program, which can produce hundreds or thousands of lines of records.

25. What is the usage of ethereal network analysis tool?

The ethereal network analysis tool could generate a list of the top 10 websites users in your network are visiting.

26. Define Sysinternals and give examples.

Sysinternals is a collection of free tools for examining Windows products

Examples of the Sysinternals tools:

- RegMon shows Registry data in real time
- Process Explorer shows what is loaded
- Handle shows open files and processes using them
- Filemon shows file system activity

27. Define Knoppix Security Tools Distribution (STD).

A Knoppix Security Tools Distribution (STD) is a bootable Linux CD intended computer and network forensics.

Knoppix STD contains several forensically sound tools put together by Klaus Knopper that are maintained and updated by Knoppix users.

28. Define phishing.

Phishing e-mails are in HTML format, which allows creating links to text on a web page. By using this technique, a phishing message could redirect the IRS‘s official address to a website in a foreign country.

29. List out some specialized e-mail forensics tools.

- AccessData‘s Forensic Toolkit (FTK)
- ProDiscover Basic
- FINALeMAIL
- Sawmill-GroupWise
- DBXtract
- Fookes Aid4Mail and MailBag Assistant
- Paraben E-Mail Examiner
- Ontrack Easy Recovery EmailRepair
- R-Tools R-Mail