CS6004-CYBER FORENSICS

UNIT 1

NETWORK LAYER SECURITY & TRANSPORT LAYER SECURITY

SYLLABUS

IPSec Protocol - IP Authentication Header - IP ESP - Key Management Protocol for IPSec. Transport layer Security: SSL protocol, Cryptographic Computations – TLS Protocol.

COURSE OBJECTIVE:

Learn the security issues network layer and transport layer.

PART – A

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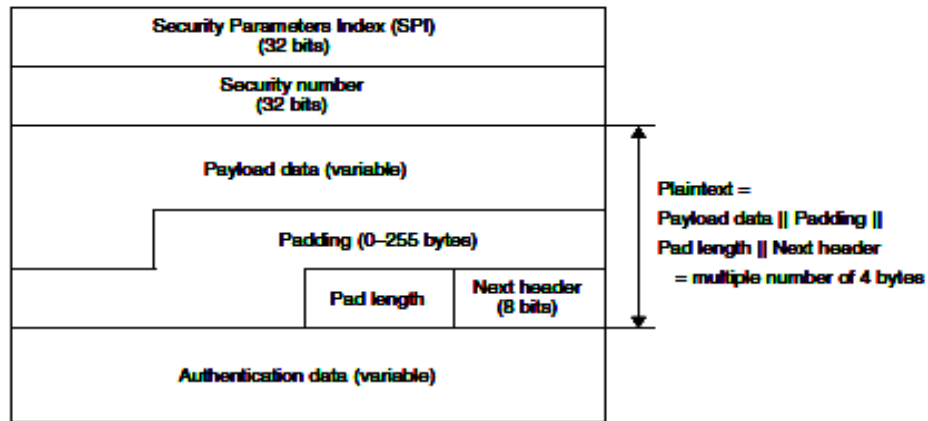
12. What is ISAKMP?
- **ISAKMP** (Internet Security Association and Key Management Protocol) defines a framework for Security Associations management and cryptographic key establishment for the Internet. This framework consists of defined exchange, payloads and processing guidelines.

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

17. Give the format of the SSL Record Protocol?

Content type	Major version	Minor version	Compressed length
Plain text(Optimality compressed)			
MAC 0,16,or 20 bytes.			

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.
  - o Diffie-Hellman key exchange
  - o RSA

- o Fortezza
- o RC2, RC4, 3DES, DES40

22. What is PRF?
- o TLS utilizes a pseudo-random function (PRF) to expand secrets into blocks of data for the purposes of key generation or validation.
- o 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.
- o

23. State the purpose of alert messages.
- o 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?
- o 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?
- o 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.

PART B

1. Explain in detail functionalities of IP sec protocol documents(**U**)
2. Identify the framework for SA management and cryptographic key establishment for the Internet and Expalin.(**R & U**)
3. Explain Transport mode of before and after applying ESP(**U&Ap**)
4. Explain in detail about the Payload Types for ISAKMP(**U**)
5. Explain the Payload type for the Vendor ID (**U**)
6. Discuss the overall operation of the SSL Record Protocol(**U**)
7. Explain how series of message is exchanged between client and server by Handshake Protocol.(**U & Ap**)

COURSE OUTCOME
Discuss the security issues network layer and transport layer.

UNIT II
E-MAIL SECURITY & FIREWALLS

SYLLABUS
PGP - S/MIME - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions.

COURSE OBJECTIVE

Be exposed to security issues of the application layer.

PART A

1. **Define PGP.**
   o PGP stands for **Pretty Good Privacy**.
   o PGP uses a combination of symmetric secret-key and asymmetric public-key encryption to provide security services for electronic mail and data files.
   o 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.**
   o MIME stands for **Multipurpose Internet Mail Extension**.
   o 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.**
   o **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?**
   o **Huffman compression** is a statistical data compression technique which reduces the average code length used to represent the symbols of an alphabet.
   o Huffman code is an example of a code which is optimal when all symbols probabilities are integral powers of 1/2.
   o A technique related to Huffman coding is **Shannon–Fano coding**.

5. **What is a Shannon–Fano coding?**
   o 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.
   o The first subset is assigned a binary 0, the second a binary 1.

6. **Define Radix-64 Conversion.**
   o 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.**
   o The data fields contained in ASCII Armor format are
      o An Armor head line,
      o Armor headers,
      o A blank line,
      o ASCII-Armored data,
      o Armor checksum and
      o Armor tail.

8. **Define an Armor head line.**
   o An armor head line consists of the appropriate header line text surrounded by five dashes ('-', 0x2D) on either side of the header line text.
   o 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.**
   o **BEGIN PGP MESSAGE** – used for signed, encrypted or compressed files.
   o **BEGIN PGP PUBLIC KEY BLOCK** – used for armouring public keys.
   o **BEGIN PGP PRIVATE KEY BLOCK** – used for armouring private keys.
   o **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.
   o **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.
   o **BEGIN PGP SIGNATURE** – used for detached signatures, PGP/MIME signatures and natures following clear-signed messages.

10. **Define Armor headers.**
    o 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.
    o 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.
    o 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.**
    o 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 (=).
    o The CRC is computed by using the generator 0x864cfb and an initialization of 0xb704ce.
    o The accumulation is done on the data before it is converted to radix-64, rather than on the converted data.
    o The checksum with its leading equals sign may appear on the first line after the base 64 encoded data.

12. **Define packet headers.**
    o A PGP message is constructed from a number of packets. A packet is a chunk of data which has a tag specifying its meaning.
    o Each packet consists of a packet header of variable length, followed by the packet body.

13. **Define packet tag.**
    o The packet tag denotes what type of packet the body holds. The defined tags (in decimal) are:
      ❖ 0–Reserved
      ❖ 1–Session key packet encrypted by public key

- ❖ 2–Signature packet
- ❖ 3–Session key packet encrypted by symmetric key
- ❖ 4–One-pass signature packet
- ❖ 5–Secret-key packet
- ❖ 6–Public-key packet
- ❖ 7–Secret-subkey packet
- ❖ 8–Compressed data packet
- ❖ 9–Symmetrically encrypted data packet
- ❖ 10–Marker packet
- ❖ 11–Literal data packet
- ❖ 12–Trust packet
- ❖ 13–User ID packet
- ❖ 14–Public sub key packet
- ❖ 60 ~ 63–Private or experimental values

14. List out the components of PGP packet structure.
- o A PGP file consists of a **message packet**, a **signature packet** and a **session key packet**.

15. Define Message digest (or hash code).
- o A hash code or message digest represents the 160-bit SHA-1 digest, encrypted with sender a's private key.
- o The hash code is calculated over the signature timestamp concatenated with the data portion of the message component.

16. Define Session Key Packets.
- o This component includes the session key and the identifier of the receiver's public key that was used by the sender to encrypt the session key.

17. Define Key Material Packet.
- o A key material packet contains all the information about a public or private key.
- o There are four variants of this packet type namely,
  - ▪ Public-key packet
  - ▪ Public sub key packet
  - ▪ Secret-key packet
  - ▪ Secret-sub key packet

18. Define SMTP.
- o SMTP is a simple mail transfer protocol by which messages are sent only in NVT (Network Virtual Terminal) 7-bit ASCII format.

19. Define Content Transfer Encoding.
- o This header defines the method to encode the messages into ones and zeros for transport.
- o There are the five types of encoding: 7 bit, 8 bit, binary, Base64 and Quoted-printable.

20. Define MIC.
- The **Message Integrity Check** (MIC) is the quantity computed over the body part with a message digest or hash function, in support of the digital signature service.

21. Define fingerprint.
- The **fingerprint** of a v3 key is formed by hashing the body (excluding the two-octet length) of the MPIs that form the key material with MD5.

22. List out the S2K specifiers.
- Salted S2K
- Iterated and salted S2K

23. What is meant by quoted-printable encoding?
- In quoted-printable encoding, if a character is ASCII, it is sent as it is; if a character is not ASCII it is sent as three characters.

24. Define Base64 encoding.
- Base64 encoding is a solution for sending data made of bytes when the highest bit is not necessarily zero.
- Base64 transforms this type of data of printable characters which can be sent as ASCII characters.

25. Define ASN.1
- ASN.1 stands for Abstract Syntax Notation One, as defined in ITU-T X.680– 689.

26. Define BER.
- BER stands for Basic Encoding Rules for ASN.1, as defined in ITU-T X.690.

27. Define DER
- DER stands for Distinguished Encoding Rules for ASN.1, as defined in ITU-T X.690.

28. Define Certificate.
- A certificate is a type that binds an entity's distinguished name to a public key with a digital signature.
- This type is defined in the PKIX certificate and CRL profile.
- The certificate also contains the distinguished name of the certificate issuer (the signer), an issuer-specific serial number, the issuer's signature algorithm identifier, a validity period and extensions also defined in that certificate.

29. Define CRL.
- The Certificate Revocation List that contains information about certificates whose validity the issuer has prematurely revoked.
- The information consists of an issuer name, the time of issue, the next scheduled time of issue, a list of certificate serial numbers and their associated revocation times, and extensions. The CRL is signed by the issuer.

30. **Define Attribute certificate.**
   o An X.509 AC is a separate structure from a subject's PKIX certificate.
   o A subject may have multiple X.509 ACs associated with each of its PKIX certificates.
   o Each X.509 AC binds one or more attributes with one of the subject's PKIXs.

31. **Define Cryptographic Message Syntax (CMS).**
   o 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.
   o CMS provides additional details regarding the use of the cryptographic algorithms.

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

33. **Define SignatureAlgorithmIdentifier.**
   o Sending and receiving agents must support id-dsa defined in DSS. Receiving agents should support rsaEncryption, defined in PRCS-1.

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

35. **What is meant by Enveloped-data content type ?**
   o An application/prcs7-mime subtype is used for the enveloped-data content type.
   o 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.

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

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

38. **Define firewall.**
   o A firewall is a device or group of devices that controls access between networks.

- o A firewall generally consists of filters and gateway(s), varying from firewall to firewall.
- o 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 untrusted internet.

39. What are the three main categories of firewalls?
- o Firewalls can be classified into three main categories:
    - o Packet filters,
    - o Circuit-level gateways and
    - o Application-level gateways.

40. Bastion Host
- o 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.
- o 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.

41. List out the bastion host's roles.
- o Single-homed bastion host
- o Dual-homed bastion host
- o Multihomed bastion host

42. What is meant by a proxy server?
- o Proxy servers are used to communicate with external servers on behalf of internal clients.
- o A proxy service is set up and torn down in response to a client request, rather than existing on a static basis.
- o The term proxy server typically refers to an application-level gateway, although a circuit-level gateway is also a form of proxy server.

43. Define SOCKS.
- o The SOCKS protocol version 4 provides for unsecured firewall traversal for TCP-based client/server applications, including HTTP, TELNET and FTP.

44. Define choke point.
- o A choke point is the point at which a public internet can access the internal network.

45. Define De-militarised Zone (DMZ).
- o The DMZ is a network that lies between an internal private network and the external public network.
- o DMZ networks are sometimes called perimeter networks. A DMZ is used as an additional buffer to further separate the public network from the internal network.

46. Define screening router.
- o The type of router used in a packet-filtering firewall is known as a screening router.

- o The screening router is configured to filter packets from entering or leaving the internal network.
- o The routers can easily compare each IP address to a filter or a series of filters.

47. What are the two basic forms of proxies ?
- o Proxies are classified into two basic forms:
    - o Circuit-level gateway
    - o Application-level gateway

48. What is meant by circuit-level gateways?
- o The circuit-level gateway represents a proxy server that statically defines what traffic will be forwarded.
- o A circuit-level gateway operates at the network level of the OSI model.
- o This gateway acts as an IP address translator between the Internet and the internal system.

49. Define Network Address Translation (NAT).
- o NAT hides the internal IP address from the Internet.
- o NAT is the primary advantage of circuit-level gateways and provides security administrators with great flexibility when developing an address scheme internally.

50. What is meant by Application-Level Gateways?
- o The application-level gateway represents a proxy server, performing at the TCP/IP application level.
- o Application proxies forward packets only when a connection has been established using some known protocol.
- o When the connection closes, a firewall using application proxies rejects individual packets, even if the packets contain port numbers allowed by a rule set.

51. What is meant by SET?
- o The Secure Electronic Transaction (SET) is a protocol designed for protecting credit card transactions over the Internet.
- o It is an industry-backed standard that was formed by MasterCard and Visa (acting as the governing body) in February 1996.

52. List out the major business requirements for SET.
- o Confidentiality of information.
- o Integrity of data.
- o Cardholder account authentication.
- o Merchant authentication.
- o Security techniques.
- o Creation of brand-new protocol.
- o Interoperability

53. List out the SET system participants.
- o Cardholder,

- o Issuer,
- o Merchant,
- o Acquirer,
- o Payment gateway, and
- o Certification Authority,

54. What are the cryptographic principles of SET?
- o Confidentiality,
- o Integrity, and
- o Authentication.

55. Define dual signature.
- o SET introduced a new concept of digital signature called dual signatures.
- o A dual signature is generated by creating the message digest of two messages: order digest and payment digest.

PART B

1. Explain about the enhanced Security Services for S/MIME.(**U**)
2. Explain in detail about PGP.(**U**)
3. Explain in detail about MIME.(**U**)
4. Explain about S/MIME.(**U**)
5. Explain in detail about the Cryptographic Message Syntax (CMS) Options in S/MIME(**An &Ap**).
6. Explain in detail about the basic terminologies required to design and configure a firewall.(**C&U**)
7. Elaborate in detail about the types of firewall.(**U**)
8. Identify the business requirements for SET and explain it in detail.(**R&U**)
9. Explain about the SET system participants.(**U**)
10. Discriminate about dual signature and signature verification in SET (**An & U**).
11. Explain in detail about authentication and message integrity.(**U**)
12. Describe in detail about payment processing.(**U**)
13. Describe in detail about the firewall designs.(**C**)

COURSE OUTCOME

  To apply security principles in the application layer.

UNIT III
INTRODUCTION TO COMPUTER FORENSICS

SYLLABUS

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

COURSE OBJECTIVE

Learn computer forensics.

PART A

1. **Define the term "Computer Forensics".**
   o 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?**
   o 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.**
   o 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?**
   o Criminal Prosecutors
   o Civil litigations
   o Corporations
   o Law enforcement officials

5. **List few services offered by computer forensics.**
   o Data seizure
   o Data duplication and preservation
   o Data recovery
   o Document searches
   o Media conversion
   o Expert witness services
   o Computer evidence service options

6. **Mention some problems with Computer Forensic Evidence.**
   o Computer data changes moment by moment.
   o Computer data is invisible to the human eye; it can only be viewed indirectly after appropriate procedures.
   o The process of collecting computer data may change it—in significant ways.
   o The processes of opening a file or printing it out are not always neutral.
   o Computer and telecommunications technologies are always changing so that forensic processes can seldom be fixed for very long

7. **Define Computer Crime and digital crime.**
   o 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.

8. **List the categories of computer crime.**
   - There are three general categories of computer crime:
        - Targets,
        - Means, and
        - Incidentals.

9. **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.

10. **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.).

11. **List the contents of an investigation plan.**
    - Any case begin with the creation of an investigation plan that defines the:
        - Goal and scope of investigation
        - Materials needed
        - Tasks to perform

12. **State the types of computer records.**

Computer records are usually divided into:
- Computer-generated records
- Computer-stored records

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

14. **List the basic steps for all digital forensics investigations.**
- For target drives, use recently wiped media that have been reformatted and inspected for viruses.

- o Inventory the hardware on the suspect's computer, and note condition of seized computer
- o For static acquisitions, remove original drive and check the date and time values in system's CMOS
- o Record how you acquired data from the suspect drive

15. What are the Steganalysis methods?
- o Stego-only attack
- o Known cover attack
- o Known message attack
- o Chosen stego attack
- o Chosen message attack

16. What methods are available for recovering passwords?
- o The three ways to recover passwords:
  - ❖ Dictionary attacks
  - ❖ Brute-force attacks
  - ❖ Rainbows tables

17. Give the hierarchy of Contemporary Cybercriminals
There are five general categories of cybercriminals in today's society:
1. Script kiddies,
2. Cyberpunks,
3. Hackers/crackers,
4. Cybercriminal organizations, and
5. Hacktivists.

18. List some digital forensics tools.
- – DriveSpy and Image
- – FTK
- – X-Ways Forensics

19. What is CMOS?
- o CMOS denotes Complementary Metal Oxide Semiconductor. The Computer stores system configuration and date and time information in the CMOS.

20. List the tasks of a Computer Forensics Examination Protocol
- o Perform the investigation with a GUI tool
- o Verify your results with a disk editor
- o Compare hash values obtained with both tools

PART B

1. How would you identity theft and identity fraud explain in details(**Ap&U**).

2. Elaborate about forensics technology and systems.(**C & U**)

3. Describe the process involved in the preparation of IR.(**Ap**)

4. Explain about the concept of data acquisition methods and how would you work in a case of clustering(**Ap**)

5. Describe Access Data FTK imager in detail and list out some applications.(**U,Ap&An**)

6. How would you get different types data using windows data acquisition tool.(**Ap,An&U**)

7. Explain about the various types of CF techniques and how to apply the CF techniques in various application (**Ap &An**).

8. Write short notes on :

    a. Forensic duplication(**An**)

    b. Forensic investigation.(**An**)

COURSE OUTCOME

To Explain computer forensics.

UNIT IV
EVIDENCE COLLECTION AND FORENSICS TOOLS

SYLLABUS

Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

COURSE OBJECTIVE

Be familiar with forensics tools

PART A

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.
   o Zoned bit recording (ZBR)
   o Track density
   o Areal density
   o 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.**
   o FAT12
   o FAT16
   o FAT32
   o 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.**
    o TrueCrypt
    o CrossCrypt
    o 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.**
18. 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.

19. **Give examples for Computer crimes.**
    o Fraud
    o Check fraud
    o Homicides

20. **Write down the Tasks for planning your investigation.**
    o Identify the case requirements
    o Plan your investigation
    o Conduct the investigation
    o Complete the case report
    o Critique the case

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?**
    o Identifies the evidence
    o Identifies who has handled the evidence
    o 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.**
    o You can't predict the hash value of a file or device,
    o No two hash values can be the same ,
    o If anything changes in the file or device, the hash value must change.

28. **List out the functions of FTK.**
    o Extract the image from a bit-stream image file
    o 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
- Remote acquisition
- Verification

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.

36. 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.

PART B

1. Describe about the process of collecting evidence in private-sector incident scenes.(**Ap**)

2. Explain about the process of preparing for a search.(**Ap**)

3. Elaborate about the concept of securing a computer incident or crime scene.(**An&U**)

4. Explain about the concept of reviewing a case.(**Ap**)

5. Describe about windows registry.(**U**)

6. Explain about the steps involved in examining NTFS disks.(**Ap &U**)

7. List out the computer forensic hardware and software tools and to solve the different types of forensics(**Ap**)

8. Elaborate about the validation and testing of forensic software.(**An**)

COURSE OUTCOME
       To understand the Use of forensics tools

UNIT V
ANALYSIS AND VALIDATION
SYLLABUS
Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics.
COURSE OBJECTIVE
 Learn to analyze and validate forensics data.
PART A

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)?**
   AccessData 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 forgets 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,

- o People,
- o Technology,
- o 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.
- o Mantech Memory DD
- o Win32dd
- o winen.exe from Guidance Software
- o 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:
- o RegMon shows Registry data in real time
- o Process Explorer shows what is loaded
- o Handle shows open files and processes using them
- o 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. List out some of the Knoppix-STD tools
- o Dcfldd, the U.S. DoD dd version
- o memfetch forces a memory dump
- o photorec grabs files from a digital camera
- o snort, an intrusion detection system
- o oinkmaster helps manage your snort rules
- o john
- o chntpw resets passwords on a Windows PC
- o tcpdump and ethereal are packet sniffers

29. Write a short note on The Auditor – Linux tool.

The Auditor – robust security tool that had a Trojan warrior for its logo. It has been replaced by BackTrack which has tools for network scanning, brute-force attacks, Bluetooth and wireless networks, and more. It includes forensics tools, such as Autopsy and Sleuth and it is easy to use and frequently updated.

30. Define BackTrack.

BackTrack includes built-in web browsers, editors and graphics tools so the you can generate reports. It also contains word lists from many languages that you can use for password cracking.

31. Define packet sniffers.

Packet sniffers are devices and/or software placed on a network to monitor traffic. Most network administrators use sniffers for increasing security and tracking bottlenecks.

32. What is the purpose of Tcpslice?

Tcpslice is a good tool for extracting information from large Libpcap files; by specifying the time frame you want to examine. It's also capable of combining files.

33. Define Tcpdstat.

The Tcpdstat tool generates Libpcap statistics and break packets down by protocol so that you can get a quick overall view of network traffic, including average and maximum transfer rates.

34. Define Netdude.

Netdude is a GUI tool designed as an easy – to- use interface for inspecting and analyzing large Tcpdump files.

35. Define Argus.

Argus is a session data probe, collector and analysis tool. This real-time flow monitor can be used for security, accounting and network management.

36. What is meant by Zero day attacks?

A zero day attacks is another major threat in which the attackers look for holes in networks and OSs and exploit these weaknesses before patches are available.

37. Distinguish between Honeypot and Honeywalls.

Honeypot are normal looking computer that lures attackers to it.

Honeywalls are monitor what's happening to honeypots on your network and record what attackers are doing.

38. 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.

39. Define ESMTP.

An enhanced simple mail transfer protocol is used for sending and receiving e-mail messages. ESMTP number stands for enhanced simple mail transfer protocol number in the message's header of an e-mail is unique to each message an e-mail server transmits.

40. Give examples for e-mail server program.
- Microsoft Exchange Server,
- Novell GroupWise,
- UNIX SendMail.

41. Define Web-based e-mail.

Web-based e-mails are messages displayed and saved as Web pages in the browser's cache folders. Many Web-based e-mail providers also offer instant messaging (IM) services.

42. 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

43. What is the significance of e-mail forensics tools?

The tools allow you to find:
- E-mail database files
- Personal e-mail files
- Offline storage files
- Log files

44. What is the use of FINALeMAIL tool?
- Scans e-mail database files
- Recovers deleted e-mails
- Searches computer for other files associated with e-mail

45. Define spoofing.

Transmitting an e-mail message with its header information altered so that its point of origin appears to be from a different sender. Spoofed e-mail is also referred to as forged e-mails.

46. Define mbox.

A method of storing e-mail messages in a flat plain text file.

47. What is drive slack?
- Unused space in a cluster between the end of an active file and the end of the cluster is called drive slack.

48. Define MIME.

MIME stands for multipurpose internet mail extensions. A specification for formatting non-ASCII messages such as graphics, audio, and video, for transmission over the internet.

49. Write down the bandwidth of 3G with other technologies.

3G offers increased bandwidth such as,
- o 384 kbps for pedestrian use.
- o 128 kbps in a moving vehicle,
- o 2 Mbps in fixed locations.

50. Define EDGE.

EDGE stands for Enhanced Data GSM Environment.

51. Define GSM.

GSM stands for Global system for mobile communications. It uses the Time Division Multiple Access (TDMA) technique, so multiple phones take turns sharing a channel.

52. List out the technologies supported by 4G networks.
- o Orthogonal Frequency Division Multiplexing (OFDM),
- o Mobile Wi Max,
- o Ultra Mobile Broadband (UTMS)
- o Multiple Input Multiple Output (MIMO)
- o Long Term evolution (LTE)

53. Define Orthogonal Frequency Division Multiplexing (OFDM).

The Orthogonal Frequency Division Multiplexing (OFDM) technology uses radio waves broadcast over different frequencies, uses power more efficiently, and is more immune to interference.

54. Write down the main components used for mobile communication.

The three main components used for mobile communication are
- o Base transceiver station (BTS)
- o Base station controller (BSC)
- o Mobile switching center (MSC)

PART B

1. Explain in detail about the process of validating forensic data.(**Ap**)

2. List out the data hiding techniques and how to apply the data hiding techniques in various applications(**Ap, An&U**)

3. Elaborate about the process of performing remote acquisition. (**U**)

4. Describe in detail about the steps involved in securing a network.(**Ap**)

5. Elaborate about the network tools.(**U**)

6. What were some of the roles of the client and server and how would apply in e-mail.(**An , Ap &U**)

7. List out the steps involved in examining in Microsoft e-mail server logs and Explain it in detail .(**Ap**, **An,&U**)

8. Describe in detail about specialized E-mail forensic tools.(**An**)

9. Elaborate about mobile device forensics.(**C**)

COURSE OUTCOME

To Analyze and To validate forensics data.

Course Name   **: CS6004-CYBER FORENSICS**

Year/Semester   **:** IV / VIII

Year of Study   **:** 2016 –2017 (R – 2013)

On Completion of this course student will be able to

COURSE OUTCOMES

CO	OUTCOMES
CO1	Discuss the security issues network layer and transport layer
CO2	Apply security principles in the application layer
CO3	Explain computer forensics
CO4	Use forensics tools
CO5	Analyze and validate forensics data

CO – PO MATRIX:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C411.1	3	-	2	-	2	-	-	-	2	-	2	-
C411.2	3	-	2	-	2	2	-	--	2	-	2	1
C411.3	3	-	2	1	2	2	-	-	2	-	2	-
C411.4	3	-	2	1	2	2	-	-	2	-	2	1
CO411.5	3	1	2	1	2	-	-	-	2	-	2	1
AVG	3	1	2	1	2	2			2		2	1

COURSE OUTCOMES AND PROGRAM SPECIFIC OUTCOMES MAPPING

CO – PSO MATRIX:

CO	PSO1	PSO2	PSO3
C411.1	2	1	2
C411.2	2	1	2
C411.3	3	2	2
C411.4	2	1	2
CO411.5	2	2	2
AVG	2.2	1.4	2