b. During 2020 pandemic, zero day attacks were reported against sophisticated firewalls, globally affecting the cyber space causing great economic and digital loss. Suggest the list of procedures that could have been followed for corporate high-tech investigations and its consequences based on the evidence collected. 10 3 3 1,8

29. a. Highlight the difference between a civil and criminal investigation while reviewing a cyber incidence. 10 2 4 1

(OR)

b. Discuss the requirements of a cyber case that in under investigation. 10 2 4 1,8

30. a. Describe the tasks in investigating e-mail crimes like email bombing and its violations, that may result in illegal data acquisition. 10 3 5 1,8

(OR)

b. Elaborate the procedures for acquiring data from any mobile device, which may lead to a punishable cyber crime under law. 10 3 5 1,8

* * * * *

Reg. No. □□□□□□□□□□□□□□□

B.Tech. DEGREE EXAMINATION, MAY 2022

Sixth & Seventh Semester

18CSE461T – INTERNET SECURITY AND CYBER FORENSICS

(For the candidates admitted from the academic year 2018-2019 to 2019-2020)

Note:

(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

(ii) **Part - B** should be answered in answer booklet.

Time: 2½ Hours Max. Marks: 75

PART – A (25 × 1 = 25 Marks)

Answer **ALL** Questions

Marks BL CO PO

1. _____ header is designed to provide security services in IPv4 and IPv6. 1 1 1 1
(A) IP AH (B) IP ESP
(C) IP IKE (D) OAKLEY

2. An SSL connection occurs in _____ layer of OSI model. 1 1 1 1
(A) Transport (B) Network
(C) Session (D) Physical

3. The size of alert messages in SSL alert protocol is ______. 1 1 1 1
(A) 2 bytes (B) 2 bits
(C) 4 bytes (D) 4 bits

4. TLS utilizes _______ to expand secrets into blocks of data for key generation or validation. 1 1 1 1
(A) Random function (B) Pseudo random function
(C) Hash function (D) Non hash function

5. ______ is based on SSL V_3 protocol specification as published by Netscape 1 1 1 1
(A) TLSV1 (B) MD5
(C) SHA (D) MAC

6. _____ relays a user's TCP and UDP session over firewall. 1 1 2 1
(A) Socks (B) Choke point
(C) Proxy server (D) Bastion host

7. _____ has ability to provide Network Address Translation (NAT) 1 1 2 1
(A) Circuit level gateway (B) Packet filter
(C) Application level gateway (D) Session gateway

8. _____ is a protocol designed for protecting credit card transactions over the internet. 1 1 2 1
(A) SET (B) NET
(C) TCP (D) UDP

9. _______ protocol provides point to point encryption. 1 1 2 1
(A) SET (B) SSL
(C) NET (D) SHA

10. ______ is ensured by digital signature. 1 1 2 1
(A) Integrity (B) Confidentiality
(C) Authentication (D) Sharing

11. ______ route the evidence from time you find it until the case is closed and goes for court trail. 1 1 3 1
(A) Chain of evidence (B) Chain of custody
(C) Chain of proof (D) Chain of investigation

12. During acquisition of RAID drives, ______ are designed for data recovery. 1 1 3 1,8
(A) RAID 0 (B) RAID 1
(C) NON RAID 0 (D) NON RAID 1

13. Comparing the current biometric data with historical data is called _____. 1 1 3 1
(A) Identification (B) Verification
(C) Validation (D) Recognition

14. SSL provides ______ encryption. 1 1 3 1
(A) Point to point (B) End to end
(C) Point to end (D) End to point

15. Which of the following is NOT a storage format for digital evidence? 1 1 3 1
(A) Raw format (B) Properity format
(C) Advanced forensics format (D) Digital format

16. _____ are known program files used to identify illegal files. 1 1 4 1
(A) Known file filters (B) Unknown file filters
(C) File frame (D) Doc frames

17. _____ format image files (.dd ext) do not contain meta data 1 2 4 1
(A) Raw (B) Processed
(C) Media (D) Textual

18. Steganography tools are used to protect ______ materials. 1 2 4 1
(A) Copy righted (B) Trademarked
(C) Patented (D) Digitally approved

19. ________ is designed to recover encrypted data if users forget their pass phrases. 1 2 4 1
(A) Key escrow (B) Hash escrow
(C) Force escrow (D) Password escrow

20. _____ enables different email applications to work together in Microsoft email server. 1 2 4 1
(A) MAPI (B) API
(C) DAPI (D) CAPI

21. Digital evidence can be stored or transmitted in digital form for 1 1 5 1,8
(A) Specific information (B) Specific data
(C) Only numeric data (D) Any information

22. Computer records used as evidence must be ______. 1 1 5 1,8
(A) Authentic only (B) Trustworthy only
(C) Trustworthy and authentic (D) Non trustworthy and confidential

23. When will attorneys challenge a digital evidence? 1 1 5 1,8
(A) Record alternation and damage (B) Record creation and damage
(C) Record sharing and creation (D) Record sharing and damage

24. For private sector incident scenes, evidences will be collected from ______. 1 1 5 1,8
(A) Business agencies (B) Government agencies
(C) Business and government that are not involved in law enforcement (D) Business and government that are involved in law enforcement

25. Which amendment under Indian law issues warrants for search and persons or things that are to be seized 1 1 5 1,8
(A) First (B) Second
(C) Third (D) Fourth

PART – B (5 × 10 = 50 Marks)

Answer **ALL** Questions

Marks BL CO PO

26. a. Internet security association and key management protocol (ISAKMP) defines several types of payloads, that are used to transfer information like security association data or key exchange data in DOI-defined formats. Elaborate on any five types of ISAKMP payloads of your choice. 10 1 1 1

(OR)

b.i. Sketch the seven group documents describing the set of IPsec protocols involving the protocols and related algorithms. 5 1 1 1

ii. Differentiate the modes or type of security association (SA) in IPsec protocol during its communication. 5 2 1 1

27. a. Suggest the general types of firewalls used for any organization's digital communication and their features depicting the implementation and need. 10 2 2 1

(OR)

b. Enlist the cryptographic operation principles to be followed by every payee and payer during a digital financial transaction. 10 3 2 1

28. a. The Indian computer emergency response team found evidence of Chinese hackers against Indian transportation sector. Enumerate the list of steps that can be suggested to the computer forensic specialists to trace the cyber incident. 10 3 3 1,8

(OR)