32. a. Explain the process of investigating e-mail crimes and violation. 12 3 5 3

(OR)

b. Describe the acquisition procedure for cell phones and mobile devices. 12 3 5 3

* * * * *

Reg. No.															

B.Tech. DEGREE EXAMINATION, JUNE 2023

Sixth Semester

18CSE461T – INTERNET SECURITY AND CYBER FORENSICS

(For the candidates admitted during the academic year 2018-2019 to 2021-2022)

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 & Part - C** should be answered in answer booklet.

Time: 3 hours Max. Marks: 100

PART – A (20 × 1 = 20 Marks)

Answer **ALL** Questions

Marks BL CO PO

1. The combination of key exchange, hash and encryption algorithms defines a ______ for each SSL session. 1 1 1 1
   (A) List of protocols (B) List of keys
   (C) Hashed message authentication code (D) Cipher suite

2. IP security operates in which layer of the OSI model? 1 1 1 1
   (A) Network (B) Transport
   (C) Application (D) Physical

3. Which two types of encryption protocols can be used to secure the authentication of computers using IPsec? 1 1 1 2
   (A) Kerberos V5 (B) SHA
   (C) MD5 (D) Both SHA and MD5

4. _______ is actually an IETF version of ________. 1 1 1 2
   (A) TLS, TSS (B) SSL, TLS
   (C) TLS, SSL (D) SSL, SLT

5. _______ uniquely identifies the MIME entities uniquely with reference to multiple contexts. 1 1 2 2
   (A) Content description (B) Content-ID
   (C) Content type (D) Content transfer encoding

6. The cryptography algorithms used in S/MIME are ________. 1 1 2 1
   (A) IDEA (B) RC4
   (C) RSA, DES-3 (D) RC5

7. What is the key size allowed in PGP? 1 1 2 2
   (A) 1024-1056 (B) 1024-4056
   (C) 1024-4096 (D) 1024-2048

8. ______ is a software that blocks unauthorized users from connecting to the computer. 1 1 2 2
   (A) Firewall (B) Quick laucm
   (C) One login (D) Centrify

9. ______ can makes or breaks investigation 1 1 3 2
(A) Crime (B) Security
(C) Digital forensic (D) Evidence

10. _______ is known as father of computer forensic. 1 1 3 2
(A) G.Pacmar (B) J.Korn
(C) Michael Anderson (D) S.Ciardhuain

11. Which of the tasks the investigators will not perform when working with digital evidence? 1 1 3 2
(A) Identity digital information or artifacts that can be used as evidence (B) Collect, preserve and document evidence
(C) Analyze, identify and organize evidence (D) Inform the victim about the recent development

12. FAT stands for 1 1 3 2
(A) File access table (B) File allocation table
(C) Federal assessment team (D) Forensic assistant tool

13. A mathematical formula that translates a file into a hexadecimal code value or a hash value 1 1 4 2
(A) CRC (B) DES
(C) MD5 (D) SHA-1

14. When a file is deleted in windows XP, 1 1 4 2
(A) The OS renames it (B) OS renames it and moves it to the recycle bin
(C) The OS removes it totally from system (D) It evaporates

15. Write blockers protect _______ by preventing data from being written to them. 1 1 4 2
(A) Compact disks (B) DVD's
(C) Evidence disks (D) Pen drives

16. In web based E-mail, messages are displayed and saved as web pages in ______. 1 2 4 2
(A) Cache folders (B) History
(C) Cookies (D) Desktop shortcut

17. Which gives the configuration information for send mail? 1 1 5 2
(A) /etc/sendmail/cf (B) /etc/syslog.conf
(C) /var/log/maillog (D) Config.sys

18. Administrators can recover lost or deleted emails from these files? 1 1 5 2
(A) History (B) Cookies
(C) Bookmarks (D) Favorites

19. ________ scans email database files 1 1 5 2
(A) Sawmill-GroupWise (B) Final Email
(C) Fookes Aid4mail (D) R-tools R-mail

20. Disk explorer and HDhost are what kinds of tools? 1 1 5 2
(A) Password recovery (B) Remote DBMS
(C) Remote acquisition (D) Compression

PART – B (5 × 4 = 20 Marks)
Answer **ANY FIVE** Questions

	Marks	BL	CO	PO
21. Draw the encapsulation security payload format and list all the fields.	4	2	1	2
22. Define hashed message authentication code (HMAC) algorithm.	4	2	1	1
23. What is a firewall? Write the role of firewalls.	4	2	2	2
24. List the benefits of computer forensics methodology.	4	2	3	2
25. List out any four forensics tool for evidence collection.	4	2	4	1
26. Explain the multipurpose internet mail extension (MIME) format in detail.	4	2	2	2
27. Discuss the RAID data acquisition.	4	2	3	1

PART – C (5 × 12 = 60 Marks)
Answer **ALL** Questions

	Marks	BL	CO	PO
28. a. Write short notes on		3	1	1
(i) Transport layer security	6			
(ii) ISAKMP key determination protocol	6			
(OR)				
b. Explain in detail on secure socket layer protocol and its types.	12	3	1	2
29. a. Describe in detail on different types of firewalls and firewall designs.	12	3	2	3
(OR)				
b. Discuss in detail on Pretty Good Privacy confidentiality and authentication.	12	3	2	2
30. a. Explain in detail on data acquisition techniques.	12	2	3	3
(OR)				
b. Summarize on the following		3	3	3
(i) Network disaster recovery systems	6			
(ii) Instant messaging (IM) security systems	6			
31. a. Explain in detail on file systems and examining NTFS disks.	12	3	4	3
(OR)				
b. Discuss in detail on storing digital evidence and obtaining a digital hash.	12	3	4	3