

**PUNE VIDYARTHI GRIHA'S
COLLEGE OF SCIENCE & TECHNOLOGY**

**Final Examination Sept-2020
T.Y.BSc.Computer Science (Semester-VI)**

Subject – Cyber Forensics

(USCS603)

Date:

1. Which of the following is not a type of cybercrime?
 - a) Data theft
 - b) Forgery
 - c) Damage to data and systems
 - d) Installing antivirus for protection

2. ----- is the process of making an archival or back up copy of the entire contents of a hard drive.
 - a) Investigation
 - b) Disk imaging
 - c) Formatting
 - d) S/w Installation

3. Valid definition of digital evidence is:
 - a) Data stored or transmitted using a computer
 - b) Information of probative value
 - c) Digital data of probative value
 - d) Any digital evidence on a computer

4. Computer forensics involves all of the following stated activities except:
 - a) extraction of computer data.
 - b) preservation of computer data.
 - c) interpretation of computer data
 - d) manipulation of computer data

5. In this phase from the collection data identify and extract the pertinent information using proper forensic tools.
 - a) Collection
 - b) Examination
 - c) Analysis
 - d) Reporting

6. What things are not recovered while investigating the computer fraud?
 - a) Financial and asset record
 - b) Accounting software and files
 - c) Photos and diaries of the victim
 - d) Credit card data

7. Which of the following route the evidence takes from the time you find it until the case is closed or goes to court?
- a) Chain of Custody
 - b) Chain of validity
 - c) Chain of Verification
 - d) Chain of Investigation
8. Which of the following are the steps for problem solving?
- a) Identify the risks
 - b) Mitigate or minimize the risks
 - c) Test the design
 - d) All of the mentioned
9. What is meant by repeatable findings?
- a) Image file
 - b) File containing the bit stream copy of all data on a disk
 - c) Repeat the steps and produce the same result
 - d) A report
10. Which of the following are especially useful when you're dealing with active network intrusions or attacks
- a) Live Acquisitions
 - b) Static acquisitions
 - c) Logical Acquisitions
 - d) Partly Acquisitions
11. _____ determines how long a piece of information lasts on the system.
- a) Order of Volatility
 - b) Order of appearance
 - c) Order of Performance
 - d) Order of measurement
12. What is the full form of DiD?
- a) Defense in Depth
 - b) Depth in Defensec
 - c) Data integrity Detection
 - d) None
13. _____ e-mails contain links to text on a Web page.
- a) Phishing
 - b) Pharming
 - c) Both a & b
 - d) None
14. _____ e-mail can be used to commit fraud.
- a) Phishing
 - b) Pharming
 - c) Spoofing
 - d) None
15. E-mail can be sent and received in which of the given environments?
- a) Internet
 - b) Intranet

- c) Supernet
 - d) Both a & b
16. Which of the following is a crime involving emails?
- a) Domestic Violence
 - b) Murder
 - c) Terrorism
 - d) None
17. Determining email message origin is referred to as _____
- a) Tracking
 - b) Tracing
 - c) Finding
 - d) None
18. E-mail logs generally identify which of the following:
- a) Email-messages an account received
 - b) Sending IP addresses
 - c) Email content
 - d) All of the above
19. block cypher used by PGP to encrypts data...
- a) international data encryption algorithm
 - b) internet data encryption algorithm
 - c) private data encryption algorithm
 - d) All of the above
20. Pretty good privacy PGP(Pretty Good Privacy) is used in...
- a) browser security
 - b) email security
 - c) FTP security
 - d) none of the mentioned
21. The extensible authentication protocol is an authentication framework used in...
- a) wired local area network
 - b) wireless networks
 - c) wired personal area network
 - d) all of the above
22. What is used to carry traffic of one protocol over the network that does not support that protocol directly...
- a) Tunnelling
 - b) Trafficking
 - c) Transferring
 - d) Switching
23. In which Mode the authentication header is inserted immediately after the IP header...
- a) Tunnel
 - b) Transport
 - c) Authentication

- d) Both A and B
24. Which of the following is an extension of an enterprise private intranet across a public Network that creates a secure private connection...
- a) VNP
 - b) VSPN
 - c) VSN
 - d) VPN
25. What term is considered as a basis for most robust authentication schemes...
- a) Registration
 - b) Identification
 - c) Encryption
 - d) Refine information