BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – B.Sc.(ANCS)-Hons-2022
Course Name – Digital Forensics
Course Code - BNCSC401
(Semester IV)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Select the term that refers to unauthorized access to computer systems with malicious intent.
a) Hacking b) Phishing
c) Spoofing d) Cyberbullying

(ii) Define ransomware.
a) Malicious software that steals personal information b) Malware that encrypts files and demands payment for their release
c) A type of computer virus d) Software used for ethical hacking

(iii) Identify a step in the cyber forensics process.
a) Preparing the crime scene b) Conducting background interviews
c) Collecting and preserving evidence d) All of these

(iv) What is the term used in the IT Act 2000 for the person responsible for maintaining electronic records?
a) Record Keeper b) Data Custodian
c) System Administrator d) Certifying Authority

(v) State the primary purpose of digital signature certificates as outlined in the IT Act 2000.
a) Ensuring data confidentiality b) Ensuring data availability
c) Ensuring data integrity d) Ensuring data authenticity

(vi) Explain the term "metadata" in digital forensics.
a) Data that is encrypted b) Data about data
c) Unrecoverable data d) Compressed data

(vii) Explain the purpose of a write blocker in digital forensics.
a) Preventing unauthorized access b) Reading data from a storage device
c) Protecting evidence from being altered d) Generating hash values

(viii) Choose the option that best exemplifies covert communication:
a) Clear text messages b) Encrypted emails

c) Steganographic images
d) Publicly shared documents

(ix) In network traffic analysis, what is the function of a packet sniffer?

a) To create a firewall
b) To capture and analyze network packets
c) To establish secure connections
d) To encrypt data

(x) Identify a task NOT considered a primary goal of computer forensics.

a) Data recovery
b) Network optimization
c) Legal evidence preservation
d) Investigating cybercrimes

(xi) Explain the primary purpose of critiquing a computer forensic case.

a) To identify weaknesses in the investigator's approach
b) To prove the innocence of the suspect
c) To delay legal proceedings
d) To destroy evidence

(xii) Define network forensics.

a) Physical security of networks
b) The process of monitoring and analyzing computer network traffic to identify and investigate security incidents.
c) Database management
d) Software development

(xiii) Describe the main function of a network scanner in cybersecurity.

a) To prevent unauthorized access attempts
b) To identify devices and services on a network and assess potential vulnerabilities.
c) To monitor network traffic for suspicious activity
d) To recover lost data from compromised systems

(xiv) Select the volatile data source in mobile forensics:

a) SIM card
b) Hard drive (assuming removable storage)
c) External SD card
d) Cloud storage

(xv) Choose the primary advantage of 5G over previous cellular generations:

a) Faster data transfer rates
b) Better call quality
c) Longer battery life
d) Enhanced GPS accuracy

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the significance of Metadata in digital forensics. (3)
3. Illustrate how data is organized on a hard disk. (3)
4. Explain how network traffic analysis contributes to cybersecurity. (3)
5. State the definition of social engineering and give an example of a social engineering attack. (3)
6. Differentiate between IPv4 and IPv6 in terms of the length of their addresses. (3)

OR

Explain the function of a Virtual Private Network (VPN) in network security. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Describe the key steps involved in a cyber forensics' investigation and how does the process differ from traditional forensic investigations and challenges that may arise in collecting and preserving digital evidence. (5)
8. Illustrate the data storage hierarchy and it's impact on data retrieval speed. (5)
9. Discuss the techniques and tools commonly used in mobile forensics to retrieve and analyze data from mobile devices. (5)
10. Explain the process of evidence identification in a computer forensics investigation. (5)
11. Validate the criticality of unbroken Chain of Custody for the admissibility of evidence in court. (5)

12. Compare the functionalities of FTK Imager and EnCase in computer forensics investigations. (5)

OR

Critique the role of password cracking tools in computer forensics investigations. (5)

****