15906

# BRAINWARE UNIVERSITY

LIBRARY
Brainware University
Barasat, Kolkata -700125

**Term End Examination 2025-2026**
**Programme – Dip.CSE-2023**
**Course Name – Network Forensics**
**Course Code - DCSE-PE502B**
**( Semester V )**

**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) Identify the protocol used for secure communication over a network.
a) FTP b) HTTP
c) SSH d) Telnet

(ii) Choose the OSI layer where routing is performed.
a) Data Link b) Network
c) Session d) Application

(iii) Select the main purpose of a firewall in a network.
a) Encrypt data b) Forward packets
c) Filter traffic d) Assign IP

(iv) Identify the protocol responsible for assigning IP addresses.
a) TCP b) FTP
c) DHCP d) DNS

(v) Identify what a packet sniffer does.
a) Blocks malware b) Monitors CPU
c) Captures network packets d) Encrypts messages

(vi) Choose the protocol used for transferring files.
a) DNS b) FTP
c) ICMP d) SMTP

(vii) Select the reason to preserve chain of custody.
a) Maintain file size b) Legal validity
c) Avoid viruses d) Improve bandwidth

(viii) Identify a non-volatile evidence source.
a) RAM b) CPU register
c) Network packet d) Hard drive

(ix) Choose the tool best used for live packet capture.
a) Netcat b) Ping



148- 4

c) Wireshark
d) Traceroute

(x) Choose the correct statement about Promiscuous Mode.

a) It only captures broadcast packets
b) It captures only TCP packets
c) It filters traffic by default
d) It captures all packets passing through the NIC

(xi) Select the technique used to collect logs from network devices.

a) Syslog
b) Netstat
c) Traceroute
d) Ping

(xii) Identify the tool used for analyzing PCAP files.

a) Netcat
b) Wireshark
c) Netstat
d) Traceroute

(xiii) Choose the correct output format for Syslog messages.

a) CSV
b) JSON
c) Plain Text
d) XML

(xiv) Select the technique used to duplicate traffic to another interface.

a) ARP Poisoning
b) Port Mirroring
c) Switching
d) Subnetting

(xv) Choose the correct meaning of PCAP in Wireshark.

a) Packet Capture Protocol
b) Packet Connection and Processing
c) Packet Collection and Analysis Protocol
d) Packet Capture

## Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain the role of Syslog in network forensics. (3)
3. Describe the concept of network port mirroring and its application in forensic investigations. (3)
4. Compare active and passive network monitoring techniques. (3)
5. Describe the role of the Physical Layer in data communication. (3)
6. Explain the role of packet sniffers in network forensics. (3)

**OR**

Illustrate a real-life case study where network forensics helped solve a cybercrime. (3)

## Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the OSI Model and its significance in network communication. (5)
8. Describe the key differences between TCP and UDP protocols. (5)
9. Describe the key components of a network forensic investigation. (5)
10. Explain the structure and function of a firewall log, and how it enhances network security. (5)
11. Evaluate the role of anonymization tools (like Tor) in complicating network forensic investigations. (5)
12. Illustrate with examples how combined log analysis (server, proxy, browser) can enhance incident response. (5)

**OR**

Analyze the implications of privacy laws on conducting network forensic investigations. (5)

**********

LIBRARY
Brainware University
Barasat, Kolkata -700