



QP CODE: 26019168



26019168

Reg No :

Name :

M.Sc DEGREE (CSS) EXAMINATION, MARCH 2026

Fourth Semester

MSc CYBER FORENSICS

ELECTIVE - CF800402 - NETWORK FORENSIC ANALYSIS

2019 Admission Onwards

EC2FD605

Time: 3 Hours

Weightage: 30

Part A (Short Answer Questions)

*Answer any **eight** questions.*

Weight 1 each.

1. Explain Application Logs.
2. Explain major factors when remote event logging is employed in a network forensic.
3. What is URI Filtering?
4. How TLS/SSL Works?
5. Describe Common features of enterprise-class WAPs.
6. What is Skyhook?
7. What is Protocol Analysis?
8. What is Flow Analysis?
9. What are the goals of malware forensics?
10. List common vectors for propagation for malware.

(8×1=8 weightage)

Part B (Short Essay/Problems)

*Answer any **six** questions.*

Weight 2 each.

11. Explain the functionalities of NIDS/NIPS.
12. What is strategies for Collecting and Analyzing Evidence?
13. Explain Types of Routers.
14. Explain Types of Firewalls.





15. Discuss the 802.11 Frame Analysis.
16. What is Rogue Wireless Access Points?
17. Explain Flow Record Analysis Techniques.
18. Explain the term in detail Inter-Switch Link (ISL).

(6×2=12 weightage)

Part C (Essay Type Questions)

*Answer any **two** questions.*

Weight 5 each.

19. What is snort ?Explain snort rule language.
20. Explain in detail Squid.
21. Describe Spectrum Analysis,.
22. Describe ICMP Tunnels and different tools used in ICMP tunnels?

(2×5=10 weightage)

