Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that: when attempting to access the domain "yummyrecipesforme.com" it's not reachable.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ICMP 203.0.113.2 udp port 53 unreachable length 254.

The port noted in the error message is used for: Port 53 is normally used for DNS traffic.

The most likely issue is: it's possible that this is an indication for malicious attract on DNS server.

Part 2: Explaining analysis of the data and providing at least one cause of the incident.

Time incident occurred: afternoon at 1:24 PM IST.

Explain how the IT team became aware of the incident: when users started reporting that our website is not reachable.

Explain the actions taken by the IT department to investigate the incident: The network security team responded and began running tests with the network protocol analyser tool tcpdump.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): the resulting log revealed that port 53 which is used for DNS traffic, is not reachable. Our next steps include checking the DNS server configuration for security breach. Network security team believes that the attacker is trying to harm the organization by not letting users access our website.

Note a likely cause of the incident: The network security team suspects this attack might be launched by some international hacker groups.