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: There was an attempt to query the DNS server for the IP of yummyrecipesforme.com.

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

The port noted in the error message is used for: DNS queries.

The most likely issue is: the DNS server of IP 203.0.113.2 is not reachable or is denying queries.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred: 13:24:32, 13:26:32, and 13:28:32.

Explain how the IT team became aware of the incident: The repeated “destination port unreachable” ICMP error responses were observed while attempting to DNS query.

Explain the actions taken by the IT department to investigate the incident: Analyzed the traffic with the use of tcpdump.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): UDP port 53 (commonly used for DNS) on the destination server 203.0.113.2 is unreachable, preventing DNS queries from resolving the domain name.

Note a likely cause of the incident: Server might be down, misconfigured or blocking requests.