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: The browser sent DNS queries over UDP to resolve the domain "yummyrecipesforme.com" to an IP address.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The DNS query to port 53 on the DNS server returned the error “udp port 53 unreachable.”

The port noted in the error message is used for: Port 53 is used for DNS (Domain Name System) services, which map domain names to IP addresses.

The most likely issue is: The DNS server is either down or not listening on port 53, resulting in the DNS query failing and the ICMP error “port unreachable” being generated.

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

Time incident occurred: The incident began at 13:24:32 and was repeated at intervals, as shown in the log.

Explain how the IT team became aware of the incident: Users reported that they were unable to access the website "www.yummyrecipesforme.com" and received the error “destination port unreachable.”

Explain the actions taken by the IT department to investigate the incident: The IT department used a network analyzer tool (tcpdump) to capture traffic between the client device and the DNS server. They identified that the UDP DNS request resulted in an ICMP error message.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The key finding was that the DNS server (203.0.113.2) returned an ICMP error message stating "udp port 53 unreachable," meaning it wasn’t responding to DNS queries over UDP on port 53.

Note a likely cause of the incident: A likely cause is that the DNS server is either misconfigured, down, or not listening on port 53, which is preventing DNS resolution for the domain "yummyrecipesforme.com."