Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs show that DNS queries sent using the UDP protocol received ICMP error messages stating “udp port 53 unreachable.” This indicates that when a user attempted to visit the website www.yummyrecipesforme.com, their browser sent DNS queries to resolve the domain name, but the DNS server was not accessible on port 53. As a result, the webpage could not load due to failed DNS resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred in the afternoon when users reported that the website www.yummyrecipesforme.com failed to load. The network team captured the traffic using tcpdump, and analysis showed that the browser first attempted a DNS query using UDP. The DNS request had an ID of 35084. In response, the DNS server sent back an ICMP message saying “udp port 53 unreachable.” This confirms that the DNS server was either down or misconfigured, with no active service listening on port 53. Because DNS resolution failed, the browser could not obtain the website’s IP address and could not proceed to make an HTTPS connection.