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 it did not reach the DNS server while requesting the IP address of a website 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 service. The most likely issue is: No service was listening on the receiving DNS port.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 p.m. Several clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The IT department responded and began running tests with the network protocol tool, tcpdump. The resulting logs revealed that port 53, which is used for DNS service, is not reachable. The tests were repeated two more times, but each time the same ICMP responding message occurred. The query identification number on the sent UDP message appears as: 35084 with associated flag “A”, which means that there is an issue of mapping an IP address to the domain name. The most likely cause for this incident is that the UDP message requesting an IP address for the domain yummyrecipesforme.com did not go through to the DNS server because no service was listening on the receiving DNS port. The incident is now being handled by the security engineering team.