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 UDP port 53 is unreachable.DNS protocol is further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding The most likely issue is: DNS Server Issue, Server down, firewall blocking the traffic or misconfigured network

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred this afternoon. 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 network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for UDP protocol We are continuing to investigate the root cause of the issue to determine how we can recover the destination website. Our next steps include checking the firewall configuration to see if port 53 is blocked, the firewall traffic, or DNS server issue