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 indicate that port 53 unreachable when attempting to access the client company website port 53 is normally used for both tcp and udp communication.This may indicate a problem with the web server or the firewall configuration.It is possible that this is an indication of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred when 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 time is 1:24 p.m., 32.192571 seconds.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 connection,the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack.The network security team suspect might have launched an attack to crash the web.