Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
As part of the DNS protocol, the UDP protocol was used to contact the DNS server and to get the IP address of our client's website that has the domain name www.yummyrecipesforme.com. The server responded with an ICMP message indicating that port 53 is unreachable. Since we know that port 53 is used by the DNS protocol, we know that there is an issue with the DNS server. The ICMP error message contains "A?", which indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. Due to the ICMP message, we highly believe that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The organization received reports from our clients indicating that they were not able to access the client company website www.yummyrecipesforme.com, and they saw the error "destination port unreachable" after waiting for the page to load. Our network security experts started immediately to investigate the root of the problem. The tcpdump network analyzer tool has shown that port 53 is unreachable, which is the port used by the DNS protocol. Our team is now investigating whether the DNS server itself is down or if traffic to port 53 is being blocked by a firewall. We suspect that the DNS server went down due to a denial-of-service attack or a misconfiguration.