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 port 53 was unreachable when customers tried to access the client company website “www.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 protocol. The most likely issue is the UDP message requesting an IP address for the domain name "www.yummyreceipesforme.com" did not go through to the DNS server because 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.
The incident occurred around 1:24pm, 32.192571 seconds when the client reported that they were unable to access the client's website. The network security team responded by troubleshooting the issue using the network analyzer tool tcpdump. The IT team found out that port 53 which is used for the DNS server was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to successful Denial of Service attack or a misconfiguration