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 the UDP packet was unreachable, which means 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. 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 communicating with the DNS service. The most likely issue is that the ICMP service is not communicating with the DNS service, so the main problem comes with the error message displayed on the web page because it doesn't send the right package or even it doesn't have any communication.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred in the afternoon at 1:24 pm. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The first thing was looking at the type of error and especially the port that was involved in that error, it was also essential to look at the time and the source and destination IP's. After that, they realized that the port 53 of DNS service was affected and the UDP was unreachable, but the ICMP of the computer was trying to access the web page. The problem of this cause could be a DoS that floods all the DNS service so it sends that error.