Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
Several of our client’s customers complained they were unable to reach yummyrecipesforme.com. I attempted to reach the website and the tcpdump log has indicated that port 53 is unreachable. Port 53 is used for DNS services. This may indicate that the server has an ongoing issue or may be the result of a malicious attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The same “udp port 53 unreachable” message was received 3 times in a row at 2 minute intervals starting at 13:24:32. Several of our client’s customers complained they were unable to reach yummyrecipesforme.com. An attempt was made to reach the website but was ultimately unsuccessful due to the issue with port 53 as stated by tcpdump. It appears that the website's DNS server is having an ongoing issue that may be malicious in nature. This may be due to a sustained flood of DNS queries resulting in a DoS attack.