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: my host device IP 192.51.100.15 is trying to translate the domain name for yummyrecipesforme.com to its IP address through the websites DNS server 203.0.113.2. Port 53 is used for DNS traffic. Based on the ICMP echo reply, 'udp port 53 unreachable', the DNS server for the website is unresponsive. The DNS server has received a lot of traffic beyond its capacity to resolve at a go. It may likely be that there is a problem in the firewall configuration or the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred in the afternoon around 1:24pm. The incident was reported by several customers of our client, www.yummyrecipesforme.com, stating that the client website was unreachable. The network security team responded by running tests using network protocol analyzer tool, tcpdump.The resulting logs indicated that port 53, the DNS server used to translate the domain name to IP address, is unreachable. Now that we are aware the challenge lies in the DNS server, we are trying to resolve the issue.