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 yummyrecipesforme.com was not accessible to users and network analyser logs reveal that port 53 was unreachable. 53 is used for DNS service - it became evident from logs that the 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”.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred in the afternoon at 1.28pm. The IT team became aware of the incident because several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The IT department began investigations by attempting to access the website themselves to receive the same error message “destination port unreachable”. The team then attempted to load the website using the network analyser tool tcpdump that reported that UDP port 53, which is used for DNS service, was unreachable still after ICMP packets were sent three times. These requests did not go through to the DNS server because no service was listening on the receiving DNS port. This may be as a result of an ICMP flood attack.