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 protocol was used to contact dns server to retrieve the IP address for the domain name of 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: an issue with the DNS server. The most likely issue is: The DNS server is not responding. And is supported by flags associated with the outgoing UDP message and domain name retrieval.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: today at 1:24pm Explain how the IT team became aware of the incident: Customers notified the organization that they received the message “destination port unreachable” Explain the actions taken by the IT department to investigate the incident: they conducted packet sniffing tests using tcpdump. In the resulting log file, they found that the DNS port 53 was unreachable, & the next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. Note a likely cause of the incident: DNS server down due to a successful DDOS attack.