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: Request sent in a UDP Packet to the IP address for yummyrecipesforme.com Error connecting to the DNS server, This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The error message indicated that the UDP packet was undeliverable to the port, port 53 being unreachable. The port noted in the error message is used for: was port 53 of the DNS server The most likely issue is: port 53 is used for DNS communications so it being unreachable means there's probably been a DoS attack against the DNS server..

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 pm 36.098564 seconds Explain how the IT team became aware of the incident: Several Customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com. Explain the actions taken by the IT department to investigate the incident: Troubleshooted the problem, load network analyzer tool, use tcpdump to figure out the issue. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Port 53 was affected showing that the DNS servers was attacked, meaning a DoS attack most likely happened since port 53 was unreachable. Note a likely cause of the incident: Denial of Service Attack (DoS) was most likely the culprit since port 53 is for the DNS servers meaning the service was unreachable. They attacked it with a DoS attack by overloading the DNS server.