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 port 53 is unreachable. 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 length [x]" The port noted in the error message is used for: Port 53 is used for Domain Name System (DNS) services. The most likely issue is: There request did not go through to the DNS server because no service was listening on the receiving DNS port. This possibly indicates a problem with the the server, the DNS service or with the firewall configuration.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13:24:32.192571 Explain how the IT team became aware of the incident: The IT team became aware of the problem after being contacted by several customers reporting 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: The IT team started investigating the incident by visiting the website, which caused the team to receive the same error message. To troubleshoot the issue the team used a network analyzer tool, *tcpdump*, to capture the same message from the website. Note key findings of the IT department's investigation: During the investigation the team found port 53 was unreachable when using an udp connection, which affected the server's ability to fulfill DNS requests. Note a likely cause of the incident: This issue could have been caused by a server shutdown, due to power supply issues or hardware related problems. It could have been caused by a server crash, due to excess traffic reaching the device, likely a DoS (Denial of Service) or lastly the server could have been compromised by a malicious actor that altered the integrity of the system, causing the service to stop working.