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: 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 The port noted in the error message is used for: when DNS does not return IP address for the domain. The most likely issue is: there is no service listening to the request on the receiving DNS port

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24:322 pm Explain how the IT team became aware of the incident: Customers reported being unable to access the website. Explain the actions taken by the IT department to investigate the incident: Network analyzer tcpdump was used to determine the issue. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): UDP port 53 was unreachable, which is used for DNS. Note a likely cause of the incident: No service was listening on the receiving DNS port