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 destinated port 53 in the DNS server is unreachable. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The port noted in the error message is used for: The UDP port 53 is used to send and receive DNS queries and responses. The most likely issue is: The most likely issue may be a network problem , firewall problem, or any attack on 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 p.m., 32.192571 seconds. Explain how the IT team became aware of the incident: The team started taking action when the HR department reported the issue. Explain the actions taken by the IT department to investigate the incident: The network incident response team started running tests through tcpdump and got the relevant details. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The team found that the port 53 of the DNS server became unreachable.

Note a likely cause of the incident:
The cause maybe a network crash, issues in the firewall, or any threat actor initiating an attack.