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: Logs show repeated queries of client to DNS but instead of the proper DNS response client received ICMP error “udp port 53 unreachable”. This is either do to the server being down / misconfigured, firewall or network policy blocking port 53 traffic or just a simple routing issue.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 pm 32.192571 seconds and persisted for several minutes Explain how the IT team became aware of the incident: Likely due to parameters in place sending alert to IT team of port unreachable errors , Someone reported it, or log analysis Explain the actions taken by the IT department to investigate the incident: Review logs, firewall and configurations, and overall server health Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Isolated incident that could be patched quickly and easily Note a likely cause of the incident: Failure or misconfiguration of dns server 203.0.113.2 most likely due to network policy or firewall or possible network / routing issues.