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 packet was undeliverable to port 53. This is based on the results of the network analysis, which show that the ICMP echo reply returned an error message indicating that the UDP packet was undeliverable to port 53. The port noted in the error message is used for: DNS The most likely issue is: Possible threat actor or faulty DNS server. Will contact the sysadmin at that company and alert them to the unresponsive server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24:32pm Explain how the IT team became aware of the incident: Customers of the client company made us aware that they were receiving the error message “destination port unavailable”. Explain the actions taken by the IT department to investigate the incident: Ran a network analyzer to find further info on the issue. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Port 53 (DNS) is unresponsive. Note a likely cause of the incident: Threat actor, misconfigured server, power outage