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 DNS server requesting the IP address of yummyrecipes.com. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: The third and fourth line show that the UDP packet was undeliverable. The port noted in the error message is used for: Port 53 of the DNS server The most likely issue is: the port is not traced.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24pm Explain how the IT team became aware of the incident: Several Custers of the client reported that they were not able to access the website. Explain the actions taken by the IT department to investigate the incident: Troubleshoot the issue, load the network analyzer tool, tcpdump and attempt to load the webpage again, Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The identification number that appeared in the first line of the error log. The sign after the query Identifcation “A”? Note a likely cause of the incident: destination port unreachable