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 when attempting to access the website yummurecipesforme.com This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: 203.0.113.2 udp port 53 unreachable length 254. The port noted in the error message is used for: port 53 is used by DNS to resolve numerical IP addresses to human readable hostnames. The most likely issue is: This could be an issue with the DNS server called BIND which has a history of security problems. BIND and port 53 are frequent targets for couple worms.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred at 1:24:36 pm **Explain how the IT team became aware of the incident:** several people who tried to access the website yummyrecipes.com website reported the error message “destination port unreachable” after waiting for the page to load. **Explain the actions taken by the IT department to investigate the incident:** The IT department after getting the complaints they immediately assigned cybersecurity analyst to analyze the situation and determine which protocol was affected during the incident. In this case UDP port is affected. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): The key findings of the IT department are the possible attack originated at the DNS server on UDP port 53 or there might be a misconfiguration on the firewall settings as there is no port listening to the service request. Note a likely cause of the incident: improper firewall configuration or a possible worm attack.