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 computer attempted to query the DNS server at IP 203.0.113.2 on port 53. However, the server was unreachable, resulting in multiple failed ICMP packets. **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:** 'udp port 53 unreachable' **The port noted in the error message is used for:** Port 53, as mentioned in the provided context, is a well-known port primarily used for DNS (Domain Name System) service requests and responses. **The most likely issue is:** The DNS server is either not running or there's a firewall or network configuration preventing access to port 53. This may indicate a problem with the web server or present of a malicious attack on the web server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13:24. **Explain how the IT team became aware of the incident:** Through the DNS and ICMP logs, which highlighted error messages and indicated unsuccessful communication attempts with the DNS server. **Explain the actions taken by the IT department to investigate the incident:** Customers reported difficulty accessing the website, seeing a "destination port unreachable" error. Using the tcpdump network analyzer, an error response was confirmed. ICMP packets were sent two more times, but the same delivery error was received both times. N**ote key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):** Initial outgoing request from computer (192.51.100.15.52444) to the DNS server (203.0.113.2.domain) was performed, requesting the IP address of yummyrecipesforme.com. The start of the error message of the ICMP packet (203.0.113.2) was undeliverable to port 53 of the DNS server. **Note a likely cause of the incident:** While configuration issues or server malfunctions are common causes for such errors, it's crucial to consider the possibility of malicious

activities and thoroughly investigate the incident.