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 browser attempted to contact the DNS server using port 53 to retrieve the IP address for the domain name yummyrecipesforme.com, but encountered issues performing the DNS protocol operations. **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,” indicating a problem reaching the DNS server. **The port noted in the error message is used for:** DNS protocol traffic, specifically port 53, which is the standard port for DNS queries and responses. **The most likely issue is:** that the DNS server is either down or misconfigured, preventing it from responding to requests made by the browser for domain name resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occurred at 1:24p,, during which attempts to resolve the domain name *yummyrecipesforme.com* were made. **Explain how the IT team became aware of the incident:** The IT team became aware of the incident through user reports of failed website access and monitoring alerts indicating unsuccessful DNS resolution attempts. These alerts were triggered by the repeated ICMP error messages indicating unreachable DNS port 53. **Explain the actions taken by the IT department to investigate the incident:** Upon receiving user reports, the IT department initiated an investigation by reviewing network logs to identify patterns of failed DNS queries. They analyzed the UDP messages sent to the DNS server and the ICMP error responses received. The team also checked

the status of the DNS server to confirm its operational state and inspected firewall settings to ensure that port 53 was correctly configured.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
The investigation revealed that the UDP messages from the browser were sent to port 53 of the DNS server, but were met with ICMP error responses stating that port 53 was unreachable. This indicated a communication failure with the DNS server. The analysis of logs showed consistent patterns of failure over a specific time frame, suggesting a possible ongoing issue with the DNS server.

Note a likely cause of the incident:
A likely cause of the incident is that the DNS server experienced an outage or misconfiguration, preventing it from processing requests on port 53. This could have been due to server hardware failure, software issues, or incorrect firewall settings that blocked incoming DNS queries.