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 client attempted to perform a DNS query using UDP port 53 to resolve the domain name `www.yummyrecipesforme.com`, but the query was unsuccessful. 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", meaning that the DNS server at IP `203.0.113.2` was not reachable on the expected DNS port. The port noted in the error message is used for: omain Name System (DNS) resolution, which maps domain names to IP addresses. The most likely issue is: The DNS server is either down, not listening on UDP port 53, or a firewall is blocking access to that port, preventing the DNS resolution process.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident was first observed at **13:24:32**, according to the tcpdump log timestamp. Explain how the IT team became aware of the incident: Several users reported that they were unable to access the website `www.yummyrecipesforme.com`. All users experienced an error stating “destination port unreachable” when attempting to load the page. Explain the actions taken by the IT department to investigate the incident: The IT department replicated the issue by attempting to access the website and captured the network traffic using the `tcpdump` tool. This analysis focused on DNS and ICMP traffic between the client and the DNS server. Note key findings of the IT department's investigation (i.e., details related to the port

affected, DNS server, etc.): The network capture revealed that the DNS query was sent using **UDP port 53** to the DNS server at IP address **203.0.113.2**. In response, the server sent an **ICMP message** indicating **"udp port 53 unreachable"**, confirming that the DNS server was not accepting traffic on the expected port.

Note a likely cause of the incident: The most likely cause is that the DNS server is either **offline**, **misconfigured**, or **a firewall is blocking access to UDP port 53**, preventing DNS resolution.