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 DNS requests were sent from the client's computer to the DNS server on port 53 but failed to receive valid responses. Analysis of the network traffic shows that each request was met with ICMP error messages stating "udp port 53 unreachable," indicating that the DNS server did not accept or respond to the UDP packets. Port 53 is used for DNS services, which are responsible for translating domain names into IP addresses so that web clients can reach websites. The most likely issue is that the DNS service on the server is offline, misconfigured, or blocked by a firewall, preventing clients from resolving the domain name and accessing the website.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident first occurred at approximately 13:24:32 (1:24 PM), according to the timestamps in the tcpdump log. The IT team became aware of the issue after multiple customers reported that they could not access the website *www.yummyrecipesforme.com*, and the analyst also encountered the "destination port unreachable" error when attempting to load the site. To investigate, the IT department captured network traffic using tcpdump and observed that DNS requests sent via UDP to port 53 consistently resulted in ICMP "udp port 53 unreachable" responses. Key findings indicate that UDP packets for DNS queries failed to reach a listening service on port 53 of the DNS server (IP: 203.0.113.2), and the failure was persistent across multiple attempts. The likely cause of the incident is that the DNS server is not responding on port 53, potentially due to a service outage, misconfiguration, or firewall rules blocking DNS traffic.