Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
A network traffic analysis revealed an issue with the DNS and ICMP protocols affecting the accessibility of the website yummirecipesforme.com. Port 53, which is commonly used for DNS services, was found to be unreachable. This issue was identified through the ICMP echo replies, which returned the error message: UDP port 53 unreachable. Port 53 is essential for DNS servers to resolve domain names into IP addresses, and its unavailability prevented users from accessing the website. The most likely cause of this issue is a Denial of Service (DoS) attack, which could have overwhelmed the DNS server or blocked access to port 53.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 13:24:32, when several customers reported that they were unable to access the website. They saw error messages after waiting for the page to load. The IT team became aware of the issue after receiving these customer complaints. To investigate, the IT department attempted to access the website themselves and confirmed the problem. They used network analysis tools, specifically tcpdump, to track packet movement and found that the ICMP protocol was returning error messages indicating that port 53 was unavailable. The IT team discovered that port 53, responsible for DNS resolution, was being overwhelmed, which led to the failure of DNS queries. Based on these findings, the IT department concluded that the most likely cause of the incident was a Denial of Service (DoS) attack.