Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicate that port 53 is unreachable when attempting to resolve the domain **yummyrecipesforme.com**. Port 53 is normally used for DNS queries. This may indicate a problem with the DNS server, a firewall configuration issue, or a network misconfiguration preventing DNS resolution.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24 PM when the system attempted to resolve the domain yummyrecipesforme.com but failed to receive a response from the DNS server. The network security team analyzed the traffic using the tcpdump tool and found that port 53, which is used for DNS queries, is unreachable. The logs show repeated ICMP "udp port 53 unreachable" error messages, indicating that the DNS server at 203.0.113.2 is either down, misconfigured, or blocked by a firewall. As a result, the client at 192.51.100.15 is unable to resolve the domain name, preventing access to the requested website. We are continuing to investigate the root cause of the issue to determine how we can restore DNS functionality. Our next steps include checking whether the DNS service is running on the server, reviewing firewall settings to ensure UDP traffic on port 53 is allowed, and testing DNS resolution from another client to determine if the issue is network-wide. The network team suspects that the DNS server may be misconfigured or down due to a successful Denial of Service attack, causing it to reject requests. Restarting the DNS service and adjusting firewall rules may help restore normal operation.