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 port 53 can't be accessed. 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". This port is commonly used for DNS service. The most likely issue is that the DNS service is down at 203.0.113.2. It is also possible that there may be a problem in the firewall or a misconfiguration.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The time the incident occurred was at 1:24 p.m., 32.192571 seconds. The IT team became aware of the problem when several clients reported that they saw the error "destination port unreachable" when visiting the company website. The actions taken by the IT team were the following: First they confirm the issue by visiting the website and confirming the error the clients reported. Then, the team used a network analyzer tool called "tcpdump", that showed logs of the ICMP packets received when sending UDP packets to the DNS server. The investigation revealed that all DNS requests from the internal IP address 192.51.100.15 to the DNS server 203.0.113.2 on UDP port 53 failed. The repeated queries were attempting to resolve the domain yummyrecipesforme.com. Each request resulted in an ICMP "Port Unreachable" message from the DNS server, indicating that port 53 is either closed, not listening, or being blocked by a firewall. This consistent failure suggests that the DNS server is not properly configured or accessible for DNS resolution, preventing successful domain name lookups. The likely cause of the incident is that UDP port 53 is closed, blocked, or the DNS service is down on 203.0.113.2