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 the UDP protocol shows port 53 can't be reached when a client is trying to access the website. The ICMP echo reply indicates "port 53 is unreachable". Port 53 is used for DNS server to request IP address of the website. The error message indicates that the UDP message requesting an IP address for the domain www.yummyrecipesforme.com did not go through to the DNS server because no service was listening on the receiving DNS port. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the "A?" symbol indicates flags with performing DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident was discovered in the afternoon at 1:24 pm when multiple clients reported that they could not access the website www.yummyrecipesforme.com .The network security team responded and began running tests with the network protocol analyzer tool tcpdump. We the security team are continuing to investigate the root cause of the issue to restore access to the website. The next step is to find out if possible cause could be that the DNS server is offline. The DNS server might be down due to a successful Denial of Service or a misconfiguration