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 was used to contact the DNS server to retrieve the IP address for the domain name yummyrecipesforme.com. ICMP protocol was used to respond with an error message, indicating issue contacting the DNS server. The UDP message going from your browser to the DNS server is indicated in the first two lines of every log event. The ICMP response from the DNS server with the error message “udp port 53 unreachable” is displayed in the third and fourth lines of every log event.Since port 53 is associated with DNS protocol traffic, we can infer that the issue lies with the DNS server. This conviction is further supported by the '+' sign after the query identification protocol number (35084), which indicates flags in the UDP message, and the 'A?' flag, which signifies a DNS protocol operation. For these reasons, 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.

The incident occurred today at 1:24 p.m. Several customers reported being unable to access the client company's website, www.yummyrecipesforme.com, encountering the error "destination port unreachable" after waiting for the page to load. The cybersecurity team providing IT services is actively investigating the issue to restore website accessibility. During our investigation, packet sniffing tests conducted with tcpdump revealed that port 53 was unavailable. This suggests that the DNS server is either down or traffic to port 53 is being blocked by the firewall. The likely causes include a Denial of Service (DoS) attack or a DNS server misconfiguration.