Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The protocol used, which is UDP, is a connectionless protocol which is used when low reliability of data is required.

The network protocol analyser logs indicate that the ICMP returned an error indicating that the UDP packet was undeliverable to port 53 of the DNS server.

The UDP port 53 is used by DNS servers to resolve domain names to IP addresses. UDP is used due to its speed.

The most likely issue is:

DNS service at port 53 is down

The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the www.yummyrecipesforme.com.
UDP Port 53 is normally used for DNS service.

The word "unreachable" in the message indicates 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.

This may indicate a problem with the DNS service or the firewall configuration. It is possible that this is an indication of a malicious attack on the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident occurred in the afternoon at 1:24pm when several customers of our clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

The security engineers are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start with, the analyst attempts to visit the website and also receives the error “destination port unreachable.”

To troubleshoot the issue, we load the network analyzer tool, tcpdump, and attempt to load the webpage again.

To load the webpage, *the browser* sends a query to a *DNS server* via the *UDP protocol* to *retrieve the IP address* for the *website's domain name*; this is part of the DNS protocol.

The browser then uses *this IP address as the destination IP* for *sending an HTTPS request* to the *web server* to display the webpage

The analyzer shows that when *UDP packets* are sent to the *DNS server*, we receive *ICMP packets* containing the *error message*: ***"udp port 53 unreachable."*** **Port 53 is a port for DNS service.**

The protocol impacted this **DNS protocol.** The service impacted was **DNS service.**

Possible issues:

Web service listening at port 53 is down / DNS service is down which might be due to Firewall configuration / a malicious attack.