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 ICMP packet was undeliverable to the DNS server port (53). Because the error message stated “unreachable,” this indicates that the message did not reach the DNS server. Consequently, the browser could not obtain the IP address for the website, resulting in an error. The DNS port did not have a service listening for requests.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The exact time of the incident is unclear, but we began receiving reports about the issue today. Several clients contacted our company via phone regarding an error with our website (www.yummyrecipesforme.com). When attempting to access the website, users encountered the error message “destination port unreachable” after waiting for the page to load. To address the issue, we first visited the site. Subsequently, we loaded our network analyzer tool, tcpdump, and tried accessing the webpage again to capture an ICMP response. We then examined the logs to investigate the timestamps, locations, and requests related to the site. Additionally, we utilized the UDP protocol to request a domain name. Our findings revealed that the message did not reach the DNS server, preventing the browser from obtaining the website's IP address, thereby causing the issue.