Cybersecurity Incident Report: Network Traffic Analysis Example

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
Based on the results of the network analysis, the UDP protocol reveals that port 53 is unreachable when attempting to access the company website www.yummyrecipesforme.com while using an ICMP request packet. This port (53) is known for being related to the DNS service, and as such it may indicate a problem with either the server availability or the firewall configuration. There's a possibility of a malicious attack by a threat actor.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Today several customers contacted the company to report that they were not able to access the company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The logs show that the issues started at 1:24pm. To start the IT analysis, we visited the website and we also received the error “destination port unreachable.” Next, we loaded the network analyzer tool, tcpdump, and reloaded the webpage. This time, we received a lot of packets in your network analyzer. The analyzer shows that when we send UDP packets and receive an ICMP response returned to the host, the results contain the error message: “udp port 53 unreachable.” Due to this port being related to the DNS, it may either be a case of a badly configured firewall or the webpage server being unavailable. The cause of the incident may also be a result of the actions of a threat actor causing a DoS attack, but further investigation by the security engineers is required to reach a verdict.