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 reveals that port 53 is unreachable when attempting to load the website www.exampleWebsite.com. Port 53 is commonly used for DNS services. This seems to indicate that the port is overloaded with packets, which is possibly a malicious attack. The evidence for this is the error message given in the ICMP echo reply: udp port 53 unreachable, which sent 3 packets back to the source IP after requesting a domain resolution using UDP.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident was first reported by several customers attempting to load the company website and subsequently contacting the company when they were unable to. When attempting to load the website, they were given the message “destination port unreachable.” At around 1:20 pm a cyber security analyst was tasked with analyzing the incident and discovering which network protocol was impacted. First the company website was visited and received the error “destination port unreachable” similar to the customers. Tests were run with tcpdump and the logs showed DNS port 53 was unreachable. The investigation for the cause of this non functioning port is still ongoing. At this point the best course of action is to determine whether the DNS server is down or if a firewall is misconfigured and blocking traffic to port 53. This port is likely receiving too many packets to be able to process legitimate DNS requests indicating a possible attack or an improperly functioning firewall.