Cybersecurity Incident Report: Network Traffic Analysis

Summary of the problem found in the DNS and ICMP traffic log:
The UDP protocol reveals that the DNS server hosting the company website "www.yummyrecipesforme.com" is down or unreachable over UDP port "53". This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message, "udp port 53 unreachable". The UDP protocol was used to request a domain name resolution using the address of the DNS server "203.0.113.2.domain" over port 53, but was undeliverable. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The most likely issue is that the DNS server is not responding.

Explanation of the analysis of the data and possible cause of the incident:
The incident was first recorded at 1:24 P.M., but occurred prior to the recorded time. The IT team became aware of the incident when customers reported being unable to access the company website www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load. The IT department then acted to investigate the incident. The cybersecurity analyst visited the company website and also received the error "destination port unreachable". Next, the analyst loaded the network analyzer tool, tcpdump, and reloaded the webpage. Packets were then received by the network analyzer which showed that when UDP packets were sent and received an ICMP response, returned to the host, the resulting logs contained an error message, "udp port 53 unreachable". The incident is now being handled by security engineers after the issue was reported to our direct supervisor, so customers can access our company website again. The next step is to identify whether the DNS server is down or traffic to port "53" is blocked by the firewall. The key findings were that port "53" was unreachable when attempting to send domain name resolution requests to the DNS server "203.0.113.2.domain" over the UDP protocol. The likely cause of the incident was a misconfiguration or a successful DoS attack on the DNS server.