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 the DNS server is down or unreachable. As evident by the results of the network analysis, the ICMP echo reply returned the error message “udp port 53 unreachable,” Port 53 is commonly used for DNS protocol traffic. It is highly likely that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 1:23 p.m.. Customers called the organization to notify the IT team that they received the message “destination port unreachable” when they attempted to visit the website. The network security professionals within the organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.

DNS & ICMP traffic log

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```