Cybersecurity Incident Report: Network Traffic Analysis

A summary of the problem found in the DNS and ICMP traffic log with reference to the tcpdump 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
```

The UDP protocol reveals that the UDP packet was undeliverable to port 53 of the DNS server. The DNS server is replying with the ICMP packets with the error message "udp port 53 unreachable". The port (53) noted in the error message is primarily used in DNS servers to resolve domain names via the UDP protocol. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS port on the DNS server.

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". 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server. There is also a + sign after the query id number which indicates flags from the UDP packet. After that, there is a “A?” which indicates a flag for the DNS request.

The most likely issue is that the DNS server on the target’s end is down or it has been misconfigured.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Based on the log file, the incident occurred at 1:24PM. The IT team became aware of this incident when multiple customers of clients reported that they were unable to access the client company's website and were getting the error message "destination port unreachable" when visiting the website: www.yummyrecipesforme.com Explain the actions taken by the IT department to investigate the incident: The IT department first simulated the incident and was able to replicate the issue. They then used the network analyzer tool, tcpdump to capture the packets sent and received from this request. They then analyzed the information in the packets. The key finding was that the UDP packet was undeliverable to port 53 of the DNS server, even after multiple attempts. There may have been a DOS attack on the DNS server for it to go down. Or there may be a misconfiguration on the firewall rules for their DNS server that is blocking these requests on port 53.