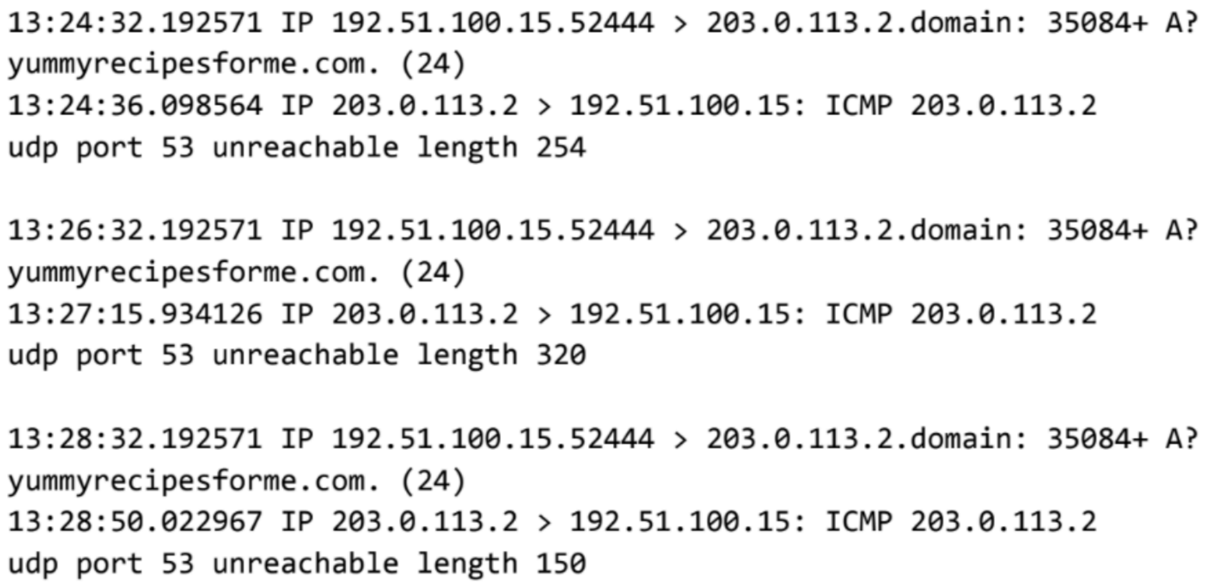
Cybersecurity Incident Report:
Network Traffic Analysis



```
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
```

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The request from the computer to the DNS server was unreachable. The browser sent a DNS query using UDP port 53 to resolve the domain www.yummyrecipesforme.com but the DNS server did not accept. This is based on the result of the error message: “udp port 53 unreachable length 150”. ICMP error was sent back by the DNS server’s IP address and is generated when a device is unable to deliver an incoming packet. This was shown in the first two lines of the error messages. The port used is DNS service. This is further noted with the query identification flag number 35084 and the “A?” symbol indicates flags performing the DNS protocol operations.. Port 53 is the standard port that handles DNS requests over UDP.
The most likely issue is the DNS server is not responding to the request.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident occurred at 13:24:32. Many customers reported not being able to access the client company website www.yummyrecipesforme.com and saw the error "destination port unreachable" The IT team visited the website and also received the error "destination port”. Troubleshooted the issue and loaded the network analyzer tool, tcpdump, and attempted to load the web page again. Analyzer showed that when the UDP packets were sent to the DNS server, the ICMP packets contained “udp port 53 unreachable". Some key findings were the DNS queries were sent over UDP from the user’s computer to, the DNS server at IP 203.0.113.2, DNS server responded with ICMP error packets, ICMP message stated “udp port 53 unreachable”, Multiple repeated attempts resulted in the same error. A likely cause is the DNS server was down or misconfigured preventing it from accepting DNS queries on UDP port 53 and stop the domain from resolving leading to website failure