Cybersecurity Incident Report:
Network Traffic Analysis

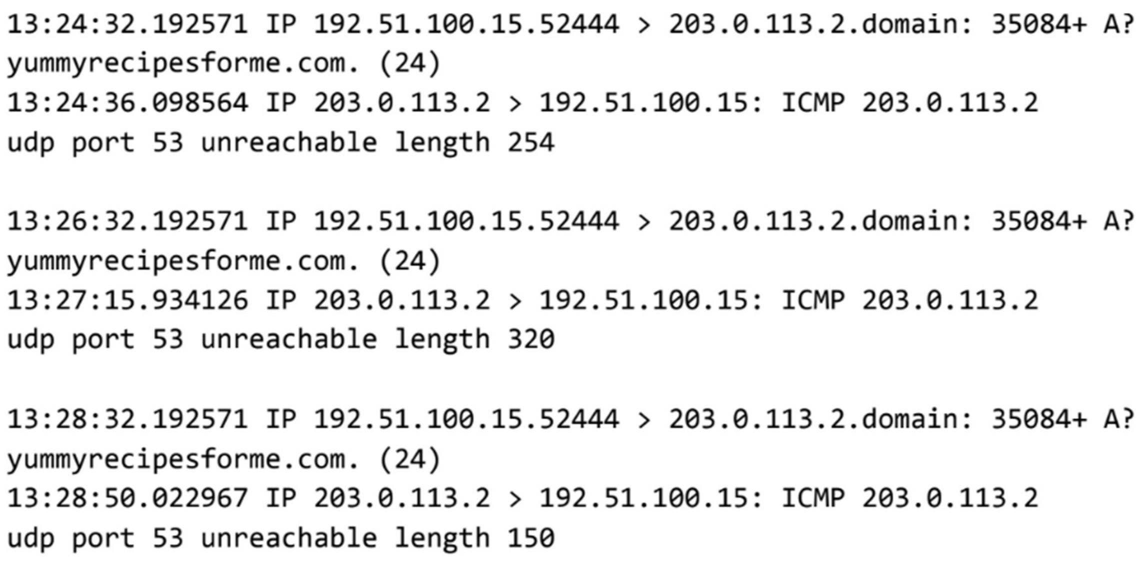
Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

As part of my continuing participation in the Google Cybersecurity Professional course, I was tasked to review the following practice scenario:

You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error "destination port unreachable" after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during this incident.

Tcpdump:



```
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 network log indicates UDP packets were undeliverable to port 53 (Domain Name Service). This is based on the the Internet Control Message Protocol (ICMP) reply which read as follows "udp port 53 unreachable length 150." It appears the DNS server for yummyrecipesforme.com is unreachable at the current time.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
In the early afternoon (1:24pm) Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The network security team responded and began running tests with a network protocol analyzer (tcpdump). The logs showed port 53 (DNS) was not reachable most likely due to ongoing DoS or DdoS attack.. The issue was then elevated to security engineers who are currently resolving the issue.