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 UDP protocol reveals that port 53 is unreachable when attempting to access the website yummyrecipesforme.com. 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 port noted in the error message is port 53 used for DNS protocol traffic. The most likely issue is that the DNS server is not responding to the request that is being sent out by the client.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24pm.Several customers contacted our team and reported that they were experiencing trouble accessing the company website “www.yummyrecipesforme.com”. When they tried to access the website, they received the message “destination port unreachable”. To investigate this issue I attempted to visit the website. When doing so I also received the error message “destination port unreachable”. My next step was to utilize my network analyzer tool tcpdump and load the webpage again. The analyzer showed that when UDP packets were received, ICMP

returned to the host and contained the error message “udp port 53 unreachable”. The next step was to check to see if the DNS server was down or if port 53 was being blocked by a firewall. The DNS server could potentially be down due to a DoS attack or a firewall not allowing traffic.