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: that is a problem with the DNS server when trying to retrieve the IP address for the domain name of the company website, yummyrecipesforme.com. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: ICMP followed by the destination ip of 203.0.113.2 (the company website) and then it states that udp port 53 is unreachable. There is also the identification number 35084 which indicates flags, followed by “A?” symbol indicating more flags. The port noted in the error message is used for: HTTPS request to the web server to display the webpage. The most likely issue is: Nobody can access the website because it’s not listening on port 53, which means that there is an issue with the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: The incident occured one morning when the website became unresponsive. The first time I did the log report was at 1:24 pm. Explain how the IT team became aware of the incident: The IT department became aware of the incident when the customers sent in a report stating that they were not able to access the company website, and saw the error message “destination port unreachable.” Explain the actions taken by the IT department to investigate the incident: The IT department and I used tcpdump to log the responses of the website when trying to retrieve the server ip address. When the website didn’t open up and gave us the error message that the port is unreachable, we knew that something had happened to the DNS server. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): In the afternoon at 1:24 pm, I attempted to load the website with my tcpdump and got an error. There are multiple flags when trying to reach the website, such as an ICMP statement saying that UDP port 53 is unreachable. After repeating this process multiple times, there is no difference. Note a likely cause of the incident: The IT team and I believe that the DNS server is down, whether it’s because a firewall is preventing port 53 to be reached or if there was a successful DoS attack is still up in the air.