**Cybersecurity Incident Report: Network Traffic Analysis**

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

The network protocol analyzer logs indicate that there was an issue when attempting to resolve the domain name [**www.yummyrecipesforme.com**](http://www.yummyrecipesforme.com). The DNS query sent via UDP to the DNS server at IP address **203.0.113.2** was unsuccessful. The log shows that the request resulted in an ICMP error message indicating "udp port 53 unreachable." This message suggests that the DNS service on the destination server was either not running, misconfigured, or that there was a network issue preventing the DNS request from reaching the correct port.

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

**Time incident occurred:**  
The incident was logged at **1:24 p.m., 32.192571 seconds** as indicated by the timestamps in the tcpdump log.

**How the IT team became aware of the incident:**  
The IT team was alerted to the issue after multiple customers reported being unable to access the website [**www.yummyrecipesforme.com**](http://www.yummyrecipesforme.com). Attempts to load the page resulted in a "destination port unreachable" error.

**Actions taken by the IT department:**  
The IT department began by replicating the issue and then used the network protocol analyzer tool, tcpdump, to capture and analyze the traffic. This confirmed that the DNS query was sent, but the DNS server did not respond correctly, leading to an ICMP error message being returned.

**Key findings of the investigation:**  
The investigation revealed that the DNS query, which was supposed to resolve the IP address of the domain name, failed because the destination port 53 on the DNS server was unreachable. This port is essential for DNS operations, and its unavailability meant that the domain name could not be resolved to an IP address, preventing the website from being accessed.

**Likely cause of the incident:**  
The most likely cause of the incident is that the DNS server at **203.0.113.2** was either down or misconfigured, preventing it from responding to queries on port 53. Another possible cause could be a firewall or network configuration issue blocking traffic to port 53.