Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: **The network protocol analysis indicates that Port 53 is unreachable when attempting to access the website "www.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 used for: **domain name system (DNS)** The most likely issue is: **the web server**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: **13:24:36.098564** Explain how the IT team became aware of the incident: **Several customers of clients reported that they were not able to access the website in the middle of the day.** Explain the actions taken by the IT department to investigate the incident: 1. **Attempt to access the website** 2. **Load network protocol analyzer tool, tcpdump and attempt to load the website again.** 3. **Found out that ICMP packets sent containing the error message "udp port 53 unreachable."** 4. **Being handled by security engineers after reporting the issue.** Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): • **DNS Server** Note a likely cause of the incident: **Could be from DoS attack where threat actors attacked the network traffic.**