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: DNS Server is down or unreachable. **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:** Logs indicate that port 53 is unreachable when attempting to access to site www.yummyrecipesforme.com. **The port noted in the error message is used for:** Port 53 is usually used by DNS protocol to translate iP protocol to domain name. **The most likely issue is:** It's possible to be a malicious attack to DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: Early in the afternoon. **Explain how the IT team became aware of the incident:** Several customers contacted the company to report that they were not able to access the company website. **Explain the actions taken by the IT department to investigate the incident:** The IT department star to attempt do access the website by they own and was not able to do it so well. They start running tests with the network protocol analyzer tool tcpdump. **Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):** The resulting logs revealed that port 53, which is used by DNS Server is not reachable. Next step is to identify the cause of the problem and understand how it occurs. **Note a likely cause of the incident:** DNS server might be down due do a DOS attack or a misconfiguration.