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 was used to contact the DNS server, which revealed issues contacting the DNS server. This is based on the results of the network analysis, which shows that the ICMP echo reply returned the error message “udp port 53 unreachable”. The port noted in the error message is used for DNS protocol traffic, this indicates it should be an issue with the DNS server not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred at 1:24 PM. The IT team was informed by several customers that they were unable to access the website yummyrecipesforme.com with the error message “destination port unreachable”. Our team has conducted packet sniffing tests using tcp dump and found that udp port 53 was unreachable. This could be due to the server being down, or the firewall could be blocking the connection. The DNS server could be down due to a successful DoS attack, or misconfiguration in the firewall.