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: port 53 is unreachable, which is the DNS server to resolve Domain names. 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" with the flag set for "A?". This indicates that the Address Record is unreachable. The port noted in the error message is used for: **This port is used for resolving Domain names, which is important for customers to be able to reach the website. If the DNS is not able to attach an IP address to the website name, then the website will be unreachable.** The most likely issue is that the DNS server is down and no service was listening on the receiving DNS ports based on the information we received from the "tcpdumb" log, and the flags that the log is showing.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 p.m., 32.192571 seconds Explain how the IT team became aware of the incident: Several customers reported the error "destination port unreachable" when trying to reach the "www.yummyrecipesforme.com" website. Explain the actions taken by the IT department to investigate the incident: **Upon learning about this incident, we attempted to reach the website ourselves, but we also received the same error. Our next step was to troubleshoot by using a Netowrk Protocol Analyzer tool called "tcpdumb", which will give us a brief packet analysis of the network traffic to this website. After running this protocol, we came to the conclusion that the DNS server was having problems based on the information in the logs, and the errors and flags that were presented.**

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): **The key flag that we found was “A?”. This flag represents the A Record, which maps IP addresses to Domain Names. This flag told us that the DNS was unreachable on top of seeing “udp port 53 unreachable” from the ICMP error message.**

Note a likely cause of the incident: **Upon our investigation, we likely think that either port 53 could be blocked by the Firewall, or the DNS server for this website is down.**