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 website is not reachable. 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: Resolving domain names. The most likely issue is: A (D)DOS attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 PM Explain how the IT team became aware of the incident: Several customers of a client reported that the website was not reachable. Explain the actions taken by the IT department to investigate the incident: Responded by initially trying to reach the website which gave us an error message. Used a packet analyzer(Tcpdump) to test the UDP protocol and were able to pinpoint what the issue is. Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): Port affected(Port 53) is responsible for resolving domain names. Note a likely cause of the incident: (D)DOS attack