Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The logs given by the network protocol analyser displays the following error message: “udp port 53 unreachable.” Port 53 is the default port used for the Domain Name System (DNS) protocol. This error could have faulted from an incorrectly configured system on the network device such as a firewall. This fault could have been incurred purposefully by a malicious actor.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident was first noticed by customer’s of *Yummy Recipes For Me*. The customers alerted the client who then reported the issues to the IT team. A team member was assigned to investigate the issue, who replicated the reported issue while running a network analyser tool (tcpdump) to capture logs of the issue. The logs show that port 53 on the web server (the default and common port for DNS) was not responding. The exact cause of the issue and thus how to resolve it are still being looked into. The plan moving forward is to investigate the exact cause as to why the DNS port was shut down. It is likely that the firewall configuration on the web server was changed to block the port, and it is also possible that this was done intentionally by a bad faith actor. The network administrator was notified of the incident to investigate for any evidence that this was a purposeful attack.