Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
When users attempted to access the website, they were unable to connect to the website. Based on the network analysis the ICMP was unreachable. The port noted in the error was port 53 which is used for DNS servers. The issue could be that a malicious attacker could be using ICMP Flood..

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident happened at 13:24 pm. The IT team became aware of the problem due to multiple customers calling in to report that the website www.yummyrecipes.com would not load and received an error code “ destination port unreachable”. The IT team used TCPdump to try and load the www.yummyrecipes.com again to get a better understanding of the error code. After the analysis IT determined that UDP protocol was used on port 53 which indicated that no service was listening on the receiving DNS port. Based on the findings from the IT team using the TCPdump we determined the malicious attack used ICMP Flood.