Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
UDP protocol reveals that : This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 unreachableThe port noted in the error message is used for the DNS service.The most likely issue is that when the udp is trying to get the domain resolved by the DNS it is getting the error that the DNS is unreachable.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred : 1:24 pm , 32.192571 seconds The IT team became aware of the incident when several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load. The Event is consistently being handled by security engineers after you and other analysts have reported the issue to your direct

supervisor.

The event was likely caused by someone doing a successful Denial of Service (DoS) attack .

In the process port 53 running DNS was affected and that is what caused the site to be unreachable.The next course of action is to identify if it is indeed a Dos attack or the port 53 was mistakenly blocked by the firewall.