Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The tcpdump reports that reaching the website “www.yummyrecipesforme.com” via UDP can't be reached as port 53 or the DNS is unreachable. There are various reasons why port 53 can’t be reached. The firewall might blocking port 53, improper configuration of router, network connectivity, the DNS is down, or a potential malicious attack

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred around 13:24 when several customers reported that they weren’t able to reach the company website. The IT team responded and analyzed what caused the error by sending UDP to the DNS. The log revealed that port 53 or DNS is unreachable causing the website company can’t be reach, This might be likely cause by the following issue: The firewall might blocking port 53, improper configuration of router, network connectivity, the DNS is down, or a potential malicious attack