Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network analyzer reports that the udp is undeliverable to port 53 of the dns server which makes the client company website unreachable. The ICMP reply returned the error message " udp port 53 unreachable length 254". Port 53 is often used for DNS which is used for translating website domain names into IP addresses. The most likely issue could be a malicious attack known as a DDOS.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
: The incident occurred early in the afternoon after the IT team realized there were reports from clients not being able to access the "www.yummuyrecipesforme.com" website. The first actions of the IT team was to attempt to access the website themselves, after realizing they came across the same problem they try to troubleshoot the issue and load up their network protocol analyzer tool tcmdump and attempt to load the webpage again. That is when they receive the error message " UDP port53 unreachable". We are currently still working on a solution. Port 53 is used for DNS which helps users access websites.The probable cause of this incident is an incorrect IP address or subnet causing the DNS packets to be misrouted.