Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that the IP address of the website http://www.yummyrecipesforme.com/ cannot be reached successfully through the receiving DNS server. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message UDP port 53 unreachable. The port noted in the error message is used for receiving the IP address from the DNS server – which is the UDP port 53. The most likely issue is that the DNS provider server is down or under DOS / DDOS attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred was at 1:24 PM, 32.192571 seconds. The IT team became aware of the incident through the reports from our various clients who were complaining of inability to connect to their respective websites. The actions taken by the IT department to investigate the incident was first, running the tcpdump command on the reported websites that are not functioning. Checking our firewalls, antivirus, and virtual private network (VPN) to see if there could be any possible misconfigurations. Key findings of the IT department's investigation related to the port affected is that the DNS server when getting a request to the UDP port 53, is unable to successfully translate the human-readable domain name to an IP address. This is ha s shown a significant security flaw in the UDP server. Considering that, it would be ideal that our company transitions to using TCP protocol – which is more secure than the UDP protocol. A likely cause of the incident could be DOS / DDOS attack from malicious threat actors.