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 UDP port 53 was unreachable and the IP address for yummyrecipesforme.com was not obtainable. Thus no service was listening on the receiving DNS port. 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 our domain name service (DNS) and thus the browser was unable to obtain the IP address. The most likely issue is an attempted DoS attack by a maliocus threat actor.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occured early this afternoon at 1:24pm and 32.192571 seconds after several customers contacted the company to report their inability to access the company website. The network security team tried loading the website to find out the error message, then loaded our network analyser tool and tcpdump, then loaded the webpage again. They found that UDP port 53 was found to be unreachable using the DNS server address over this port. It was determined that this is due to the browser being unable to obtain the destination IP address for our company website yummyrecipesforme.com. They were also unable to access the website because no service was listening on the receiving DNS port. A likely cause of this incident is a malicious threat actor attempting to damage our reputation using a Denial of Service (DoS) attack to overload our servers and cause the website to crash.