Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer logs indicate that udp port 53 is unreachable when attempting to access the website, because udp message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port. The ICMPP echo reply returned error message is “UDP port 53 unreachable”. The port noted in the error message is used for packet was undeliverable to port 53 of the DNS server. The most likely issue is that no DNS service is listening on UDP port 53 on the DNS server maybe because the firewall block the website

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred is 1:24 p.m 32.192571 seconds. The IT team should be careful and became aware of the incident after reviewing network logs that showed repeated DNS request failures. IT department must take a look on network analyzer tool and reviewing the result, after that analyzed the time incident, icmpp response and make probability about the root problem. Note key for IT department’s is, udp request didn’t go through to the dns server because no service was listening on the receiving dns port, this message “UDP port 53 unreachable”. When i look on the internet likely cause of the incident is firewall was blocking UDP port 53, preventing the DNS server from receiving and processing DNS requests.