Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
When using the UDP protocol there was an ICMP packet sent with tcpdump. There was a message received notifying a problem with port 53. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message, 'UDP packet was undeliverable to port 53'. The port noted in the error message is used for communication with the DNS server requesting the domain address, The most likely issue is that there has been an attack on port 53.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The message, '13:24:32.192571' refers to the time. This means the time is 1:24 p.m., 32.192571 seconds. By trying to open the website, the port was unreachable. An action taken by the IT department was sending an ICMP packet when opening the website and the TCP connection was analyzed by tcpdump. A key finding made by the department in the message was, 'A?', appearing in the error message, showing a flag when trying to request the domain name. The IP address of the domain is being reached so the server is responding. We suspect that there has been an attack on port 53 which does not allow the DNS server to send the domain name back to the computer.