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 DNS request could not be completed because the destination port could not be reached. **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. T**he port noted in the error message is used for:** DNS servers, which use UDP port 53. **The most likely issue is**: The DNS server is either down, misconfigured, or no service was listening on the receiving DNS port.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred: 1:24 p.m, 32.192571 seconds as indicated from the tcpdump log. **Explain how the IT team became aware of the incident:** The IT learned about several customers unable to access the www.yummyrecipesforme.com website. **Explain the actions taken by the IT department to investigate the incident:** They utilized tcpdump to try the website two more times but found the same error both times. **Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):** - UDP packets were sent to the DNS server to resolve the IP address for the website - The ICMP error message 'UDP port 53 was unreachable' indicates a DNS server issue - Multiple ICMP error messages were analyzed to confirm that no DNS server was listening on port 53 **Note a likely cause of the incident:** No DNS was listening on port 53, could be a DoS attack.