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 network protocol analyzer has logged that the destination port is unreachable.**

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: **Due to the udp port 53 unreachable**

The port noted in the error message is used for: **This port is used for DNS (Domain Name System Service)**

The most likely issue is: **The DNS server responsible for resolving the domain name is not responding or is inaccessible**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred:
This incident occurred at 1:24 pm and 32.192571 seconds.

Explain how the IT team became aware of the incident:
The IT department became aware when many customers complained about an error code after attempting to access DNS.

Explain the actions taken by the IT department to investigate the incident:
The security specialist tried to access the website using a normal browser. The same error code was given “destination port unreachable”. After this was done a few attempts were made on the network analyzer tool, TCP dump, to Troubleshoot the issue.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
The TCP dump log shows repeated failed attempts to reach the DNS server at IP address 203.0.113.2 on port 53, indicating that the DNS service is not operational or

reachable. Note a likely cause of the incident: **The DNS server at 203.0.113.2 may be down, misconfigured, or experiencing a denial-of-service (DoS) attack.**