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 port 53 is unreachable.
 	
This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:
 	
`13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24)`
`13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable length 254`
 	
The port noted in the error message is used for: The DNS query to be translated to an actual IP address so that the user can access the website.
 	
The most likely issue is: A misconfiguration of the service.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred:The incident occurred at 01:24:36 PM **Explain how the IT team became aware of the incident**: Because several customers of clients reported that they were not able to access the client's website. Explain the actions taken by the IT department to investigate the incident: - First, troubleshoot the issue by loading the network analyzer tool, tcpdump, and attempt to load the webpage again. - Then review the information logs provided by the tcpdump. - Afterwards, identify which network protocol and service were impacted by this incident. - Finally, write a follow-up report. - **Note a likely cause of the incident**: Could be a misconfiguration or failure of the DNS server, since there was no external intervention like a DoS, ICMP flood, Ping of Death, etc. Not all errors or problems are going to be related to an attack, could also be an internal error, like in this case.