Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Summary of the issue detected in the DNS and ICMP traffic log.
The UDP protocol reveals that: The client with IP `192.51.100.15` is attempting to send DNS queries to the server `203.0.113.2` using *UDP port 53*, which is the standard port for DNS services. **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"*, indicating that the destination server (`203.0.113.2`) is not accepting UDP packets directed to port 53. **The port indicated in the error message is used for:** *Domain Name System (DNS) resolution* via the *UDP protocol*, which is essential for translating names like `yummyrecipesforme.com` into IP addresses. **The most likely issue is:** The DNS server (`203.0.113.2`) is *not running a DNS service on UDP port 53* or is *being blocked by a firewall*, preventing DNS queries from being properly answered.

Part 2: Analysis of the DNS and ICMP traffic incident.
Time of the incident: *13:24:32* (first recorded attempt) *Note:* Similar failed attempts were observed at *13:26:32* and *13:28:32*.

Explanation of how the IT team became aware of the incident:

The IT team detected the incident through *network monitoring with* `tcpdump`, which showed multiple failed DNS resolution attempts followed by ICMP replies indicating that *UDP port 53 was unreachable*.

Explanation of the actions taken by the IT department to investigate the incident:

- Outgoing and incoming traffic logs for server `203.0.113.2` were reviewed.
- Multiple *ICMP Type 3 Code 3 (Port Unreachable)* responses were identified.
- It was validated that the client was generating *legitimate DNS requests*.
- A *port scan* was conducted on server `203.0.113.2` to confirm whether port *53* was open.
- The *local and network firewall configuration* on the server was verified.

Key findings of the IT department's investigation (i.e., details related to the affected port, the DNS server, etc.):

- Server `203.0.113.2` did *not have UDP port 53 open*, nor was a DNS service *listening on that port*.
- The *ICMP responses clearly indicated* that port 53 was *closed or blocked*.
- The requested domain `yummyrecipesforme.com` could not be resolved by the client due to the *lack of a valid server response*.

Possible cause of the incident:
Server `203.0.113.2` does *not have an operational DNS server on UDP port 53*, either because the service is *not installed/running*, or a *firewall is blocking* incoming traffic on that port. This *prevents clients from performing name resolution* through this server.