Cybersecurity Incident Report:
Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The `tcpdump` log reveals a **DNS name resolution failure** caused by an unreachable destination port.

- **The Incident:** At 13:24:32, the user's computer (IP `192.51.100.15`) attempted to perform a DNS query (A record) for the domain `yummyrecipesforme.com` using the **UDP** protocol on port **53**.
- **The Problem:** The destination server (`203.0.113.2`) could not process the request. Instead of a standard DNS response, it returned an error message via the **ICMP** protocol.
- **Root Cause:** The specific error was **"udp port 53 unreachable."** This indicates that while the packet reached the server, there was no DNS service actively running or "listening" on that specific port to handle the request.
- **Outcome:** The system attempted to resend the packet two more times, but all attempts failed for the same reason, ultimately preventing the user from accessing the website via its domain name.

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

Data Analysis: The logs show a failed communication attempt between the client and the DNS server. The client sent a **UDP** packet targeted at port **53** (the standard for DNS), identified by the **"A?"** flag, which represents a query for the IPv4 address of the domain `yummyrecipesforme.com`. The destination system responded immediately with an **ICMP** packet, which is the protocol used by the network to report delivery errors. The specific message "port unreachable" confirms that the network path is functional, but the requested service is unavailable at the destination.

Likely Causes:

1. **Inactive DNS Service:** The most probable cause is that the DNS server software at IP `203.0.113.2` is not running or has crashed, making it unable to listen for requests on port 53.
2. **Firewall Configuration:** A firewall on the destination server (or an intermediate security appliance) might be configured to explicitly reject connections on port 53 and send an ICMP "unreachable" response instead of silently dropping the packet.

affected, DNS server, etc.):

Note a likely cause of the incident: