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 revealed that DNS queries for `www.yummyrecipesforme.com` were sent via the **UDP protocol** to port **53**, which is the standard port used for DNS resolution. Each query received an **ICMP response** from the DNS server stating "udp port 53 unreachable." This indicates that no service was listening or responding on port 53. Without DNS resolution, the website's domain name could not be translated into an IP address, preventing access to the site. The most likely issue is that the DNS service on the server was **down, misconfigured, or blocked by a firewall.**

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
• **Time incident first reported:** Customers initially reported being unable to access `www.yummyrecipesforme.com`, receiving "destination port unreachable" errors. • **Events and symptoms observed:** 1. Users could not load the website. 2. Browsers attempted DNS lookups, but all queries failed. 3. Tcpdump captured UDP DNS requests being sent out and ICMP error messages returning from the DNS server. • **Current status of the issue:** DNS resolution to the website domain is failing. ICMP error responses confirm that UDP port 53 is unavailable on the DNS server.

- **Findings from investigation:**
    1. UDP DNS queries left the client system correctly.
    2. DNS server at `203.0.113.2` responded with ICMP errors: “udp port 53 unreachable.”
    3. This blocked DNS lookups, which in turn blocked HTTPS connections to the web server.
- **Next steps in troubleshooting / resolving:**
    1. Verify whether the DNS service is running and listening on port 53.
    2. Check firewall or access control configurations that could be blocking UDP port 53.
    3. Restart or reconfigure the DNS server if necessary.
    4. Implement a temporary workaround by pointing clients to an alternate DNS resolver (e.g., Google DNS 8.8.8.8).
- **Suspected root cause:**
  The DNS server (`203.0.113.2`) was **not listening on or blocking UDP port 53**, preventing DNS resolution of the domain name and resulting in website inaccessibility.