### **Cybersecurity Incident Report: Network Traffic Analysis**

#### **summary of the problem found in the DNS and ICMP traffic log:**

**The UDP protocol reveals that DNS queries from the computer to the DNS server are being sent, but no valid responses are received.**

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

**The port noted in the error message is used for:**  
 **DNS (Domain Name System) services, which resolve domain names to IP addresses.**

**The most likely issue is:**  
 **The DNS server is either down, misconfigured, or there is a firewall/network issue preventing communication. The request to resolve "yummyrecipesforme.com" could not reach an active DNS server, leading to failure in name resolution and website access.**

#### **analysis of the data and cause of the incident:**

* **Time incident occurred:**  
   **The incident occurred at 1:24:32 PM, 1:26:32 PM, and 1:28:32 PM, based on timestamps in the logs.**
* **How the IT team became aware of the incident:**  
   **The issue was discovered when users reported they could not access the website and received a "Destination Port Unreachable" error. A network analysis using tcpdump confirmed DNS failures.**
* **Actions taken by the IT department to investigate the incident:**
  + **The team analyzed packet logs to check for DNS request and response behavior.**
  + **They identified that UDP packets sent to the DNS server (203.0.113.2) on port 53 received ICMP errors indicating the port was unreachable.**
  + **Multiple attempts were logged with the same issue occurring repeatedly, confirming a consistent failure in DNS resolution.**
* **Key findings of the IT department's investigation:**
  + **The computer's IP address (192.51.100.15) sent DNS queries to the server (203.0.113.2).**
  + **The DNS server did not respond and instead sent ICMP "port unreachable" errors.**
  + **No valid DNS response was received, causing failure to resolve the domain name.**
* **A likely cause of the incident:**  
   **1. The DNS server (203.0.113.2) was either down or not listening on port 53.**  
   **2. A firewall or network misconfiguration blocked access to the DNS server.**  
   **3. The DNS service on the server may not have been started or configured correctly.**