Cybersecurity Incident Report: Network Traffic Analysis

```
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

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

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

The UDP protocol reveals that:
The network protocol analyzer logs indicate that the UDP packet was sent from the client to the DNS server requesting the IP address for the domain but the request was undeliverable.

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 length ...' This indicates that no service was available on port 53 of the DNS service to handle the request

The port noted in the error message is used for:
Port 53 is normally used DNS services

The most likely issue is:
The DNS server did not have a service listening on port 53, causing the UDP message requesting an IP address to fail

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

Time incident occurred:

The incident first occurred at 1:24 pm, with a few failed attempts recorded after that.

Explain how the IT team became aware of the incident:

The IT team was alerted by failed network communications, reported either through user complaints of inability to resolve the domain name or automated monitoring systems detecting DNS resolution errors.

Explain the actions taken by the IT department to investigate the incident:

- **Captured traffic using a network protocol analyzer**
- **Inspected the logs to trace the issue**
- **Identified the source and destination IPs and analyzed protocol level communication**
- **Confirmed the repeated ICMP unreachable error messages, indicating a failure on port 53**

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

- **Source IP: 192.51.100.15 (client)**
- **Destination IP: 203.0.113.2 (the DNS server)**
- **Affected Port: Port 53, which is reserved for DNS service**
- **Error Identified: No service was listening on port 53 of the DNS server which prevented domain resolution**

Note a likely cause of the incident:

The most probable cause is that the DNS server was not configured properly, or the DNS service was offline, resulting in no service listening on port 53 to handle the incoming UDP requests. Other possible causes include misconfiguration, software issues, or temporary service outages on the DNS server.