```
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
```

In the tcpdump log, you find the following information:

1. The first two lines of the log file show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.
2. The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server.
3. In front of each request and response, you find timestamps that indicate when the incident happened. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds.
4. After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this information is displayed as: 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address, which in this example is your computer's IP address. The IP address to the right of the greater than (>) symbol is the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computers IP address 192.51.100.15.
5. After the source and destination IP addresses, there can be a number of additional details like the protocol, port number of the source, and flags. In the first line of the error log, the query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to

an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message.

6. The error message, "udp port 53 unreachable" is mentioned in the last line. Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.
7. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.

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

The UDP protocol reveals that:

An outgoing request from the computer to the DNS server was made to resolve the domain name "yummyrecipesforme.com." However, this request did not reach the DNS server because of an issue indicated by the ICMP error message.

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"

The port noted in the error message is used for:

Domain system services (DNS)

The most likely issue is:

The DNS server “yummyrecipesforme.com” is down/does not exist on the specified port.

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

Time incident occurred:

1:24 p.m., 32.192571 seconds

Explain how the IT team became aware of the incident:

Error message given by the ICMP through the tcpdump.log

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

Reviewed the tcpdump.logs to pinpoint the error and then reproduced the error multiple times. Checked the configuration and status of the DNS server at 203.0.113.2. Concluded the port (53) was unreachable, suggesting the DNS service was not running or was blocked.

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

1. The source IP address was 192.51.100.15 (computer), and the destination IP address was 203.0.113.2 (DNS server).
2. The DNS server at 203.0.113.2 was not responding to requests on port 53.
3. ICMP error messages indicated that the port was unreachable, suggesting the DNS service was not running or was blocked.

Note a likely cause of the incident:

The DNS server at IP address 203.0.113.2 was not running the DNS service on port 53, this could be due to several reasons and will need further investigation