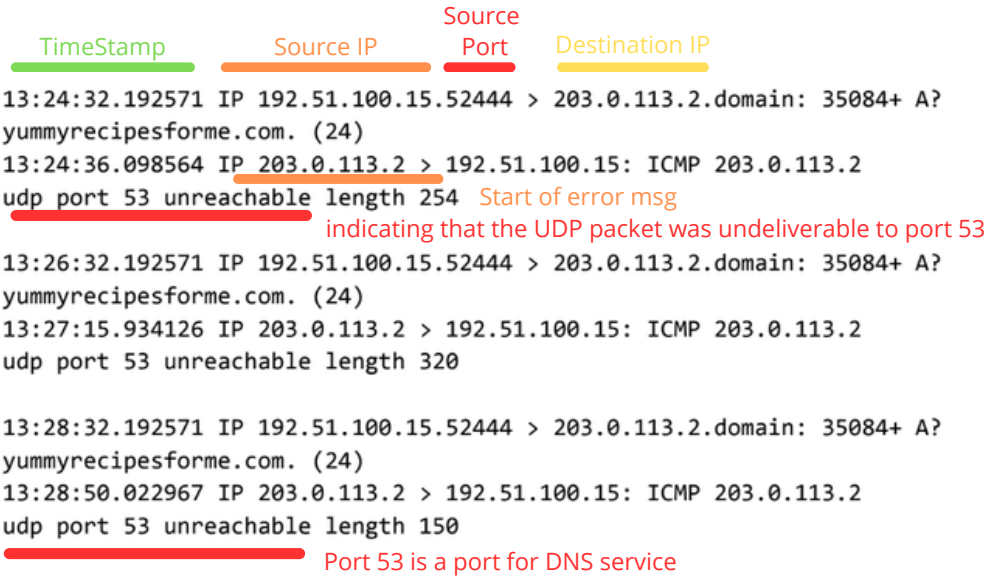
Review the scenario below. Then complete the step-by-step instructions.
You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.
You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again.
To load the webpage, your browser sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.”



In the tcpdump log, you find the following information:
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.

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.

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.

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.

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.

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.

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: DNS queries sent via UDP to port 53 are failing and not reaching a functioning DNS service.

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: UDP port 53 unreacheable

The port noted in the error message is used for: DNS(Domain name system)

The most likely issue is: No DNS service is listening on port 53 (or the service is bloqued/firewalled), causing DNS requests to fail and leadinf to the massege of unreachable error.

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

Time incident ocurred: 13:24:32

Explain how the IT team became aware of the incident: Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.

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

The IT department used TCPDUMP to capture and analyze netowork traffic.

Obserwing the UDP requests dor DNS resolution (port 53) triggering the response of the ICMP “unreachable”

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

The DNS server at IP 203.0.113.2 returned “udp port 53 unreachable” errors.

This indicates that the DNS server was not accepting or responding to requests on port 53, preventing successful name resolution.

Note a likelu cause of the incident:

The DNS service on 203.0.113.2 may have been offline or misconfigured.

A firewall or ACL(Access Control List) may have been blocking incoming DNS queries.

The DNS server process could have crashed, leaving port 53 closed.

Solution:

- Verify the DNS Service Status:
  - Log into the DNS server and check if the DNS service is running.
  - If the service is down, restart it using the appropriate command (e.g., systemctl restart named on Linux systems running BIND).
- Check DNS Server Configuration:
  - Confirm that the server is configured to listen on UDP port 53.
  - Review configuration files for any misconfigurations that might prevent the service from binding to the correct port.
- Review Firewall Settings:
  - Inspect firewall rules on both the DNS server and any intermediate firewalls.
  - Ensure that UDP traffic on port 53 is allowed. If necessary, update the rules to permit this traffic.