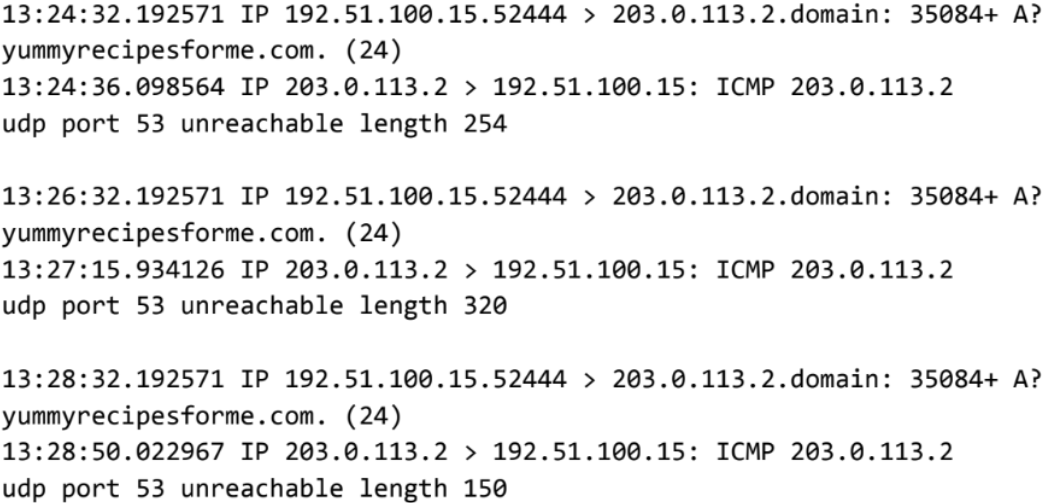
**Activity Analyze Network Layer Communication**

**Scenario**

You are a cybersecurity analyst and work at a company that specializes in providing IT consulting services. Several customers have contacted your business to report that they were unable to access the company's website *www.yummyrecipesforme.com* and saw the "destination port unreachable" error after waiting for the page to load.

You are tasked with analyzing the situation and determining which network protocol was affected during the incident. To begin with, you visit the website and also get the "destination port unreachable" error. Next, you load your network analysis tool, **tcpdump**, and load the web page again. This time, you get a lot of packets in your network analyzer. The parser shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: "*udp port 53 unreachable*".



In the DNS and ICMP log, you can find the following information:

1. In the first two lines of the log file, you see the initial outgoing request from your computer to the DNS server asking for the IP address of *yummyrecipesforme.com*. This request is sent in a UDP packet.
2. Below you will find timestamps that indicate when the event happened. In the log, this is the first sequence of numbers displayed. For example: 13:24:32.192571. This displays the time 1:24 PM, 32.192571 seconds.
3. The source and destination IP address is next. In the error log, this information is displayed as: 192.51.100.15.52444 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address. In this example, the source 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 of the DNS server: 203.0.113.2.domain
4. The second and third lines of the log show the response to your initial ICMP request packet. In this case, the ICMP line 203.0.113.2 is the beginning of the error message indicating that the ICMP packet could not be delivered to the DNS server port.
5. The following are the protocol and port number, which displays which protocol was used to handle communications and which port it was delivered to. In the error log, this appears as: UDP port 53 unreachable. This means that the UDP protocol was used to request a domain name resolution using the DNS server address on port 53. Port 53, which aligns with the .domain extension at 203.0.113.2.domain, is a well-known port for DNS service. The word "unreachable" in the message indicates that the message was not sent to the DNS server. Your browser was unable to obtain the yummyrecipesforme.com IP address needed to access the website because no service was listening on the receiving DNS port, as indicated by the ICMP error message "udp port 53 unreachable".
6. The remaining lines in the log indicate that the ICMP packets were sent two more times, but the same delivery error was received both times.

Now that you've captured data packets using a network analysis tool, it's your task to identify which network protocols and services were affected by this incident. Next, you'll need to write a follow-up report.

As an analyst, you can inspect network traffic and data to determine what is causing network-related issues during cybersecurity incidents. Later in this course, you will demonstrate how to manage and resolve incidents. For now, just look at the situation.

In the meantime, this incident is being handled by security engineers after you and other analysts reported the issue to your direct supervisor.

**Step 1: Access the template**

Use the sentence starters and instructions provided in the template to support your thinking and ensure that you include all relevant details about the incident.

"*Cybersecurity Incident Report*" File

**Step 2: Access Supporting Materials**

The following support materials will help you complete this activity. Keep them open as you move on to the next steps.

"*2 EXEMPLAR Cybersecurity Incident Report*" file

**What to include in your answer**

Be sure to cover the following items in your completed activity:

* Provide a summary of the problem found in the DNS and ICMP traffic log
* Explain your analysis of the data and provide a possible cause of the incident

**Example Evaluation**

Compare the copy with your completed activity. Proofread your work using each of the criteria in the issue. What did you do well? Where can you improve? Use your answers to these questions to guide you as you progress through the course.

**Note**: The sample offers a possible approach to investigate and analyze a potential security event. In your role as a security analyst, you and your team would make a better estimate about what happened and then investigate further to troubleshoot the issue and strengthen the overall security of your network.

Writing an effective cybersecurity analysis report can help troubleshoot network issues and vulnerabilities faster and more effectively. The more practice you have in analyzing network traffic for trends and suspicious activity, the more effective you and your team will be at managing and responding to the risks present in your network.

**Key findings**

As a security analyst, you don't always know exactly what's causing a network problem or a potential attack. But being able to analyze the IP packets involved will help you better guess what happened or potentially prevent an attack from breaking into the network. The network protocol and traffic logs will become the starting point for further investigating the issue and resolving the attack.