# Cybersecurity Incident Report:
# Network Traffic Analysis

## Scenario

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 consultant services. Several customers contacted your company to report that they were not able to access the 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 visit the website and you also receive the error "destination port unreachable." Next, you load your network analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer. The analyzer 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 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 requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.
2. Next you 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 p.m., 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 for the DNS server: 233.18.9.101.domain
4. The second and third lines of the log show the response to your initial ICMP request packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the ICMP packet was undeliverable to the port of the DNS server.
5. Next 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 address of the DNS server over port 53. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs 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 ICMP packets were sent two more times, but the same delivery error was received both times.

Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.

As an analyst, you can inspect network traffic and network 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, you only need to analyze the situation.

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

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

According to the given information, the problem found in the DNS that server is unreachable which means message is not go through to the DNS server. The problem with ICMP is that browser unable to obtain the IP address for website instead it through an error message of “udp port 53 unreachable” which means service is not responding.

## Part 2: Explain your analysis of the data and provide one solution to implement

The incident began with a UDP request on port 53 from the user's machine to the DNS server (203.0.113.2). This request is a common action in the domain name to IP address mapping procedure. The requested UDP port 53 could not be reached, according to the ICMP error message that the DNS server (203.0.113.2) returned. This shows that port 53 was not being answered by the server's DNS service. The DNS server responded to subsequent efforts to contact it with the identical ICMP error messages reporting an unavailable UDP port 53.

The event was most likely brought on by a malfunction or interruption of the DNS service on the destination DNS server (203.0.113.2) on port 53. This may be the result of DNS server misconfiguration, DNS server failure, firewall or network filtering obstructing inbound DNS traffic, or DNS server service interruption.

According to the study, it is advised to investigate the DNS server (233.18.9.101) in order to identify the primary reason for the configuration problem or failure that is causing the "udp port 53 unreachable" error. To make sure it is correctly setup and functional, a complete review and troubleshooting of the DNS service on the server is required. This may entail examining the DNS server's configuration options, going over logs, and performing additional network analysis to find any potential firewall or network problems.