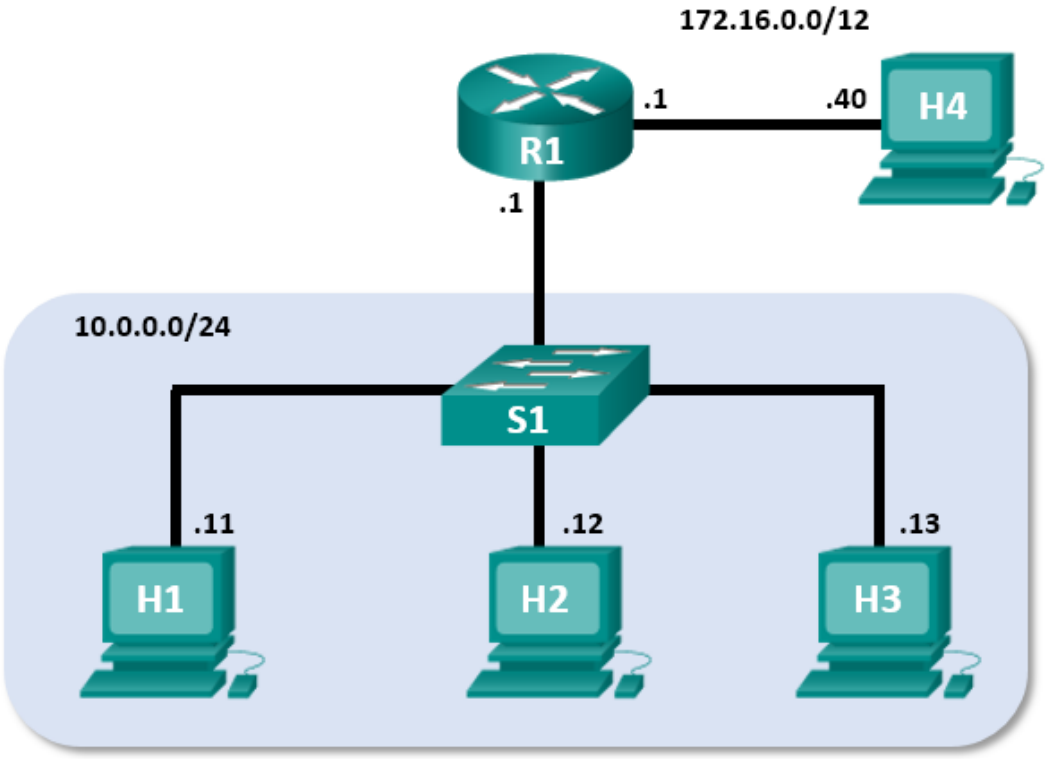
# Lab - Using Wireshark to Observe the TCP 3-Way Handshake

## Mininet Topology




## Objectives

**Part 1: Prepare the Hosts to Capture the Traffic**

**Part 2: Analyze the Packets using Wireshark**

**Part 3: View the Packets using tcpdump**

## Background / Scenario

In this lab, you will use Wireshark to capture and examine packets generated between the PC browser using the HyperText Transfer Protocol (HTTP) and a web server, such as www.google.com. When an application, such as HTTP or File Transfer Protocol (FTP) first starts on a host, TCP uses the three-way handshake to establish a reliable TCP session between the two hosts. For example, when a PC uses a web browser to surf the internet, a three-way handshake is initiated, and a session is established between the PC host and web server. A PC can have multiple, simultaneous, active TCP sessions with various web sites.

## Required Resources

- CyberOps Workstation virtual machine

## Instructions

## Part 1: Prepare the Hosts to Capture the Traffic

a. Start the CyberOps VM. Log in with username **analyst** and the password **cyberops**.

b. Start Mininet.

```
[analyst@secOps ~]$ sudo lab.support.files/scripts/cyberops_topo.py
```

c. Start host H1 and H4 in Mininet.

```
*** Starting CLI:
mininet> xterm H1
mininet> xterm H4
```

d. Start the web server on H4.

```
[root@secOps analyst]#
/home/analyst/lab.support.files/scripts/reg_server_start.sh
```

e. For security purposes, you are not able to run Firefox from the root user account. On host H1, use the switch user command to switch from the root user to the analyst user account:

```
[root@secOps analyst]# su analyst
```

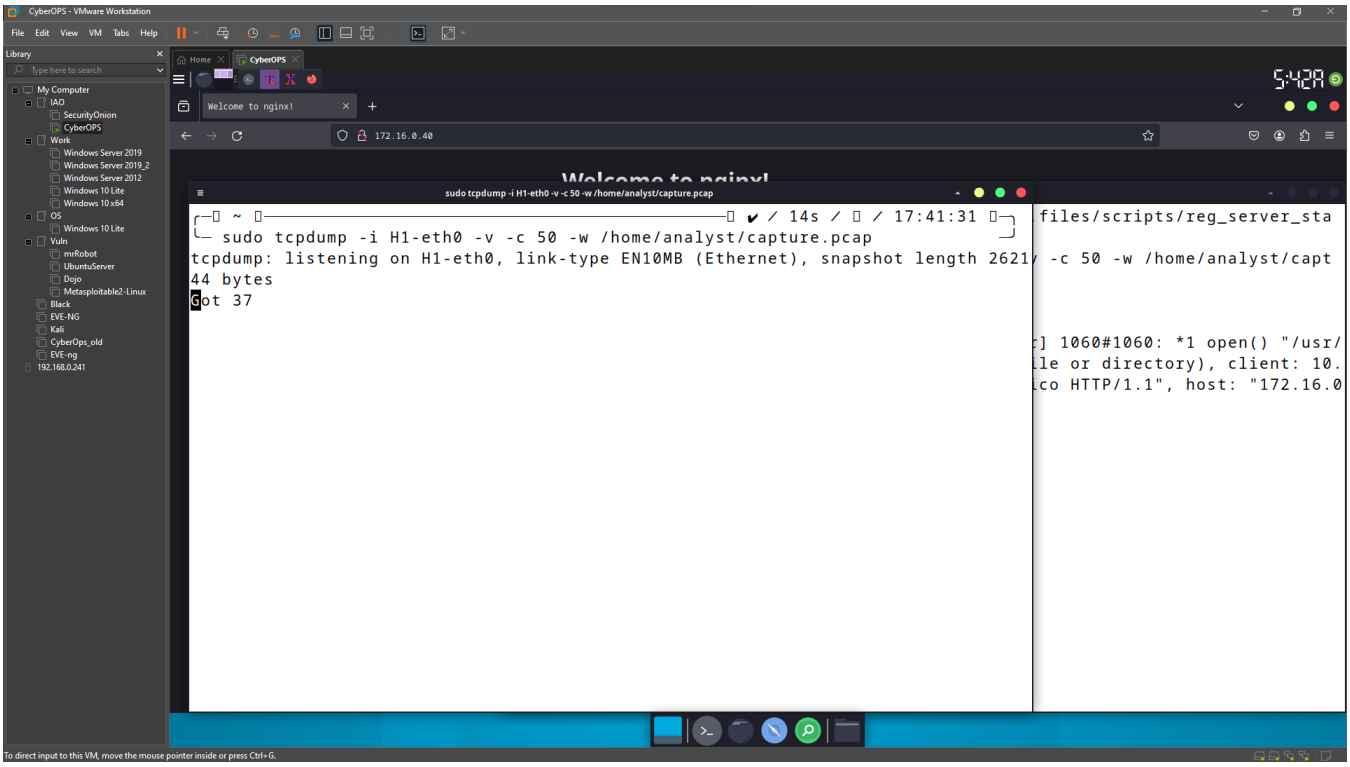
f. Start the web browser on H1. This will take a few moments.

```
[analyst@secOps ~]$ firefox &
```

g. After the Firefox window opens, start a tcpdump session in the terminal **Node: H1** and send the output to a file called **capture.pcap**. With the -v option, you can watch the progress. This capture will stop after capturing 50 packets, as it is configured with the option -c 50.

```
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w
/home/analyst/capture.pcap
```

h. After the tcpdump starts, quickly navigate to 172.16.0.40 in the Firefox web browser.




# Part 2: Analyze the Packets using Wireshark

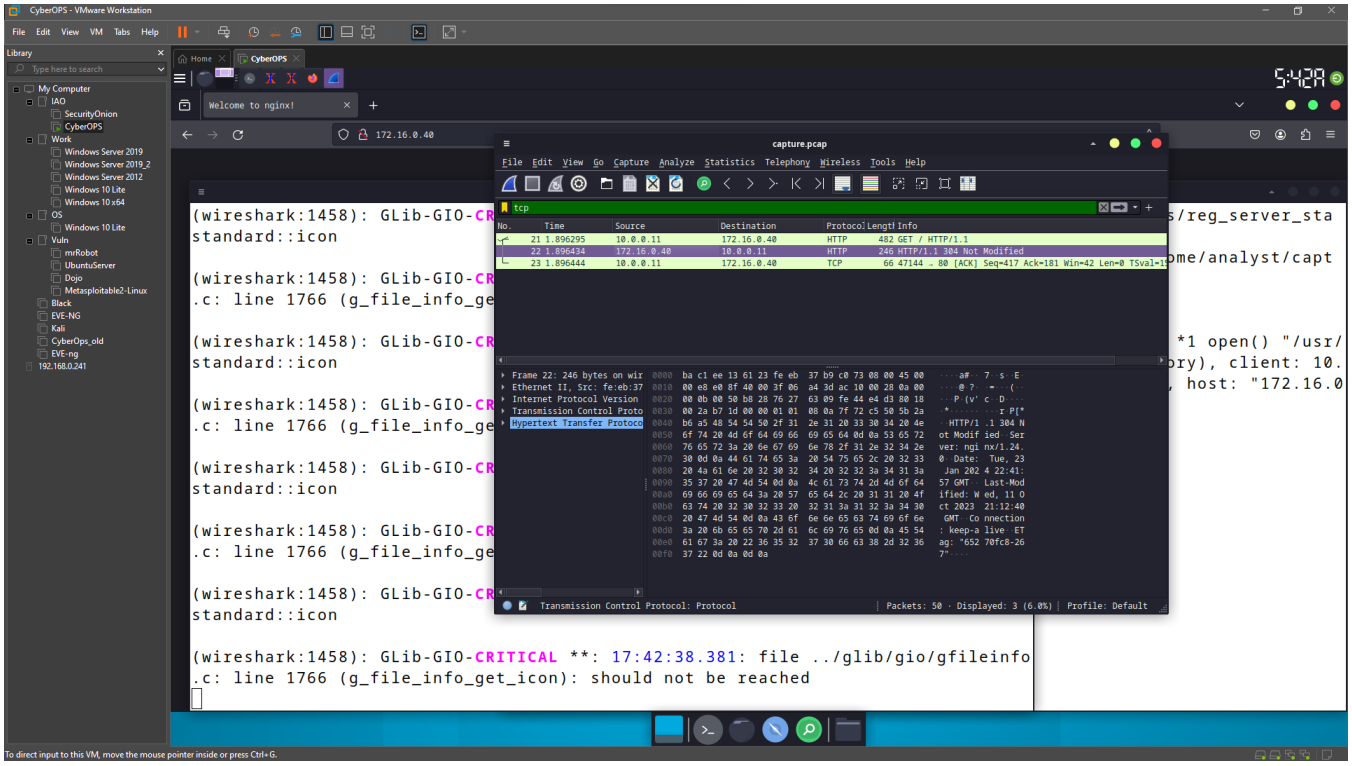
## Step 1: Apply a filter to the saved capture.

a. Press ENTER to see the prompt. Start Wireshark on **Node: H1**. Click **OK** when prompted by the warning regarding running Wireshark as superuser.

```
[analyst@secOps ~]$ wireshark &
```

b. In Wireshark, click **File** > **Open**. Select the saved pcap file located at /home/analyst/capture.pcap.

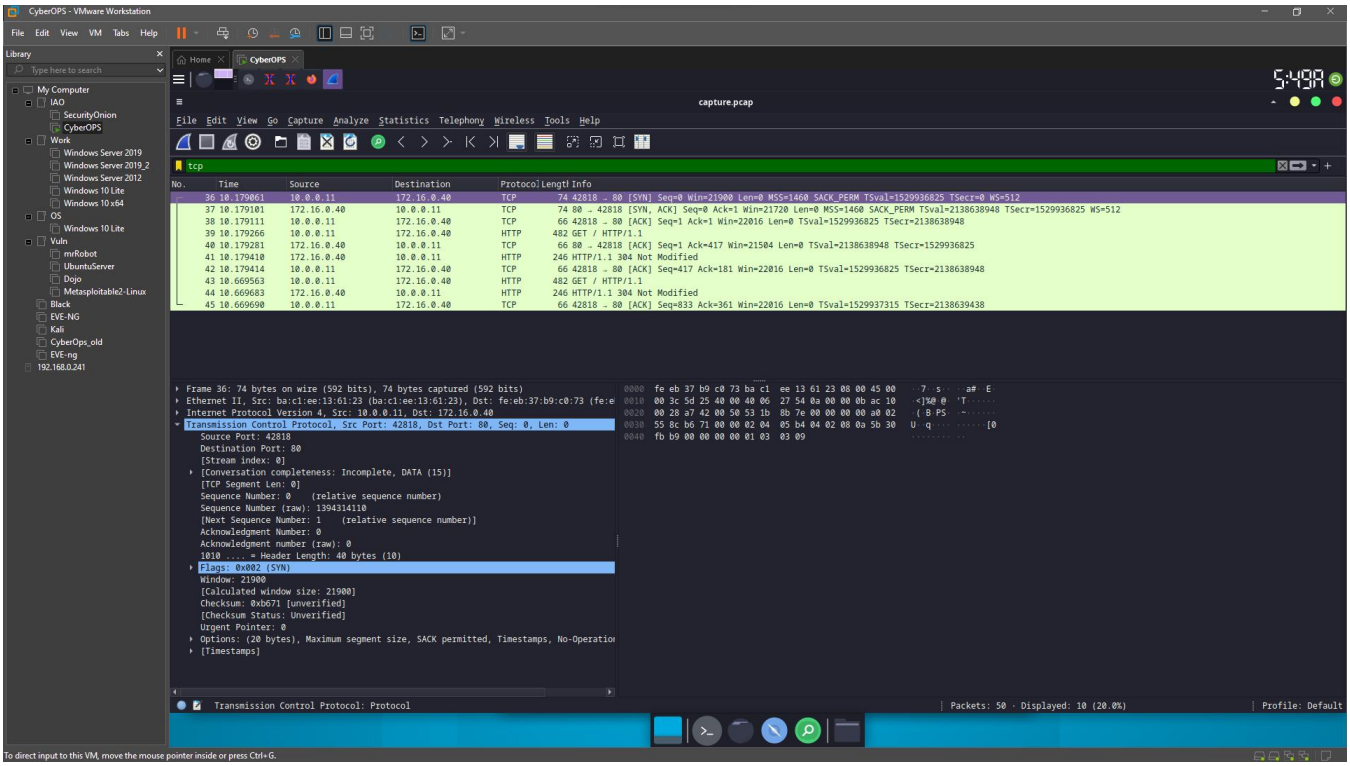
c. Apply a **tcp** filter to the capture. In this example, the first 3 frames are the interested traffic.




## Step 2: Examine the information within packets including IP addresses, TCP port numbers, and TCP control flags.

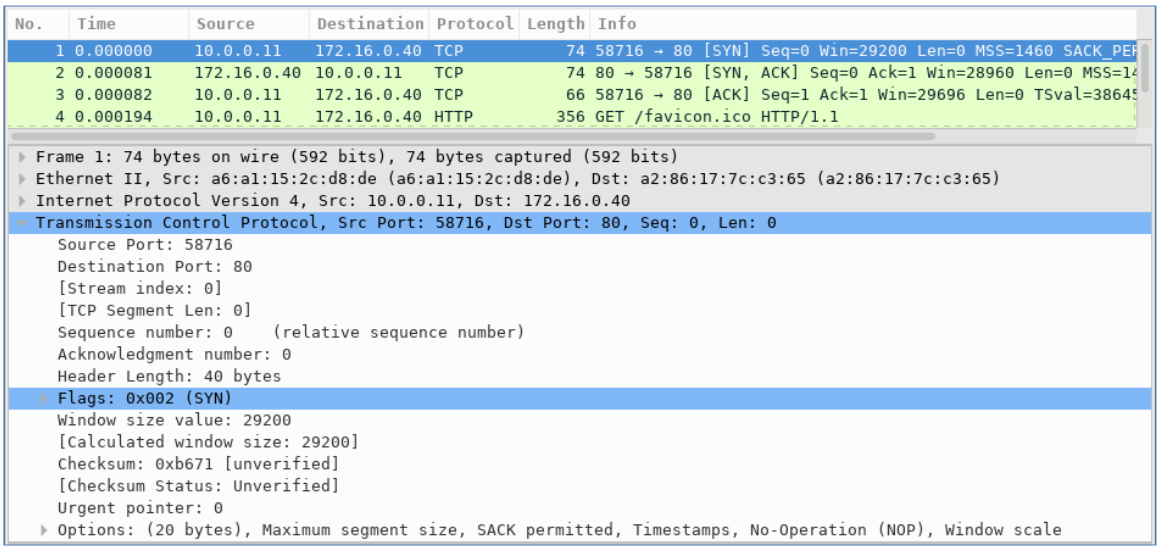
a. In this example, frame 1 is the start of the three-way handshake between the PC and the server on H4. In the packet list pane (top section of the main window), select the first packet, if necessary.

b. Click the **arrow** to the left of the Transmission Control Protocol in the packet details pane to expand it and examine the TCP information. Locate the source and destination port information.




c. Click the **arrow** to the left of the Flags. A value of 1 means that flag is set. Locate the flag that is set in this packet.

**Note**: You may have to adjust the top and middle windows sizes within Wireshark to display the necessary information.




Questions:

What is the TCP source port number?

42818

How would you classify the source port?

Dynamic or Private

What is the TCP destination port number?

80

How would you classify the destination port?

Well-known, registered (HTTP or web protocol)

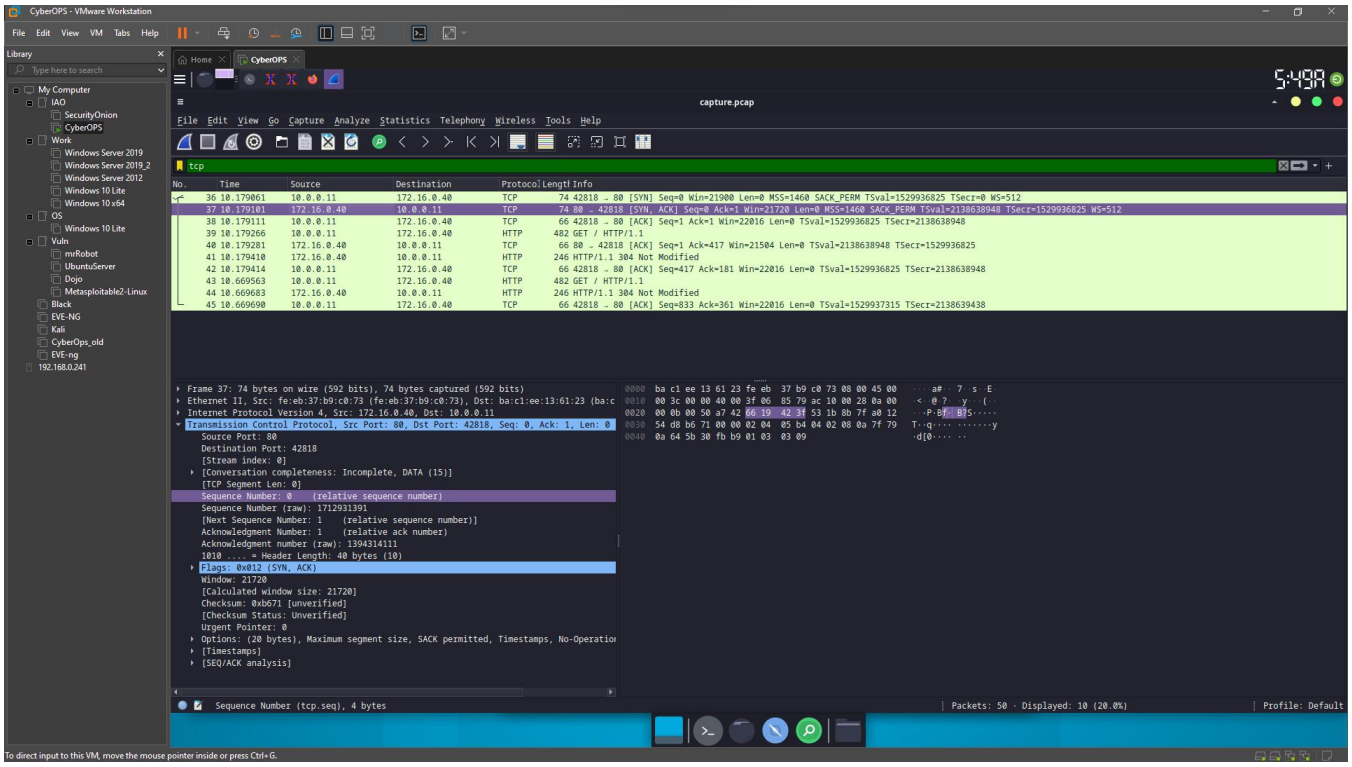
Which flag (or flags) is set?

SYN

What is the relative sequence number set to?

0

d. Select the next packet in the three-way handshake. In this example, this is frame 2. This is the web server replying to the initial request to start a session.




Questions:

What are the values of the source and destination ports?

Source Port is now 80, and Destination Port is now 42818

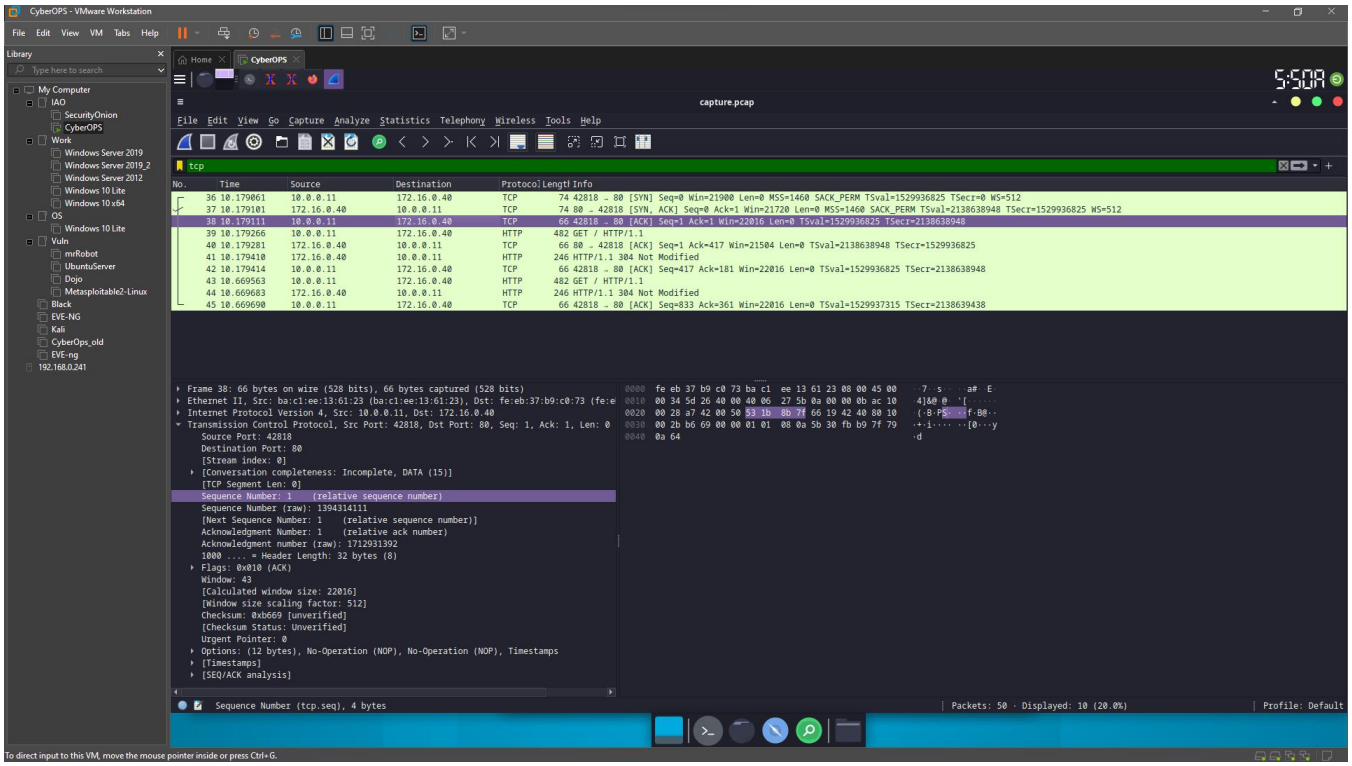
Which flags are set?

The Acknowledgment flag (ACK) and Syn flag (SYN)

What are the relative sequence and acknowledgment numbers set to?

The relative sequence number is 0, and the relative acknowledgment number is 1.

e. Finally, select the third packet in the three-way handshake.




Examine the third and final packet of the handshake.

Question:

Which flag (or flags) is set?

ACK

The relative sequence and acknowledgment numbers are set to 1 as a starting point. The TCP connection is established and communication between the source computer and the web server can begin.

## Part 3: View the packets using tcpdump

You can also view the pcap file and filter for the desired information.

a. Open a new terminal window, enter **man tcpdump**. **Note**: You may need to press ENTER to see the prompt.

Using the manual pages available with the Linux operating system, you read or search through the manual pages for options for selecting the desired information from the pcap file.

```
[analyst@secOps ~]$ man tcpdump
TCPDUMP(1)                  General Commands Manual                 TCPDUMP(1)


NAME
       tcpdump - dump traffic on a network


SYNOPSIS
       tcpdump [ -AbdDefhHIJKlLnNOpqStuUvxX# ] [ -B buffer_size ]
               [ -c count ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
```

```
                [ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ]
                [ --number ] [ -Q in|out|inout ]
                [ -r file ] [ -V file ] [ -s snaplen ] [ -T type ] [ -w file ]
                [ -W filecount ]
                [ -E spi@ipaddr algo:secret,...  ]
                [ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
                [ --time-stamp-precision=tstamp_precision ]
                [ --immediate-mode ] [ --version ]
                [ expression ]
<some output omitted>
```

To search through the man pages, you can use / (searching forward) or ? (searching backward) to find specific terms, and **n** to forward to the next match and **q** to quit. For example, search for the information on the switch -r, type **/-r**. Type **n** to move to the next match.

Question:

What does the switch **-r** do?

The option -r allows you to read packet from file that was saved using -w option with tcpdump or other tools that write pcap or pcap-ng files, such as Wireshark.

b. In the same terminal, open the capture file using the following command to view the first 3 TCP packets captured:

```
[analyst@secOps ~]$ tcpdump -r /home/analyst/capture.pcap tcp -c 3
reading from file capture.pcap, link-type EN10MB (Ethernet)
13:58:30.647462 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [S], seq 2432755549, win
29200, options [mss 1460,sackOK,TS val 3864513189 ecr 0,nop,wscale 9], length 0
13:58:30.647543 IP 172.16.0.40.http > 10.0.0.11.58716: Flags [S.], seq 1766419191, ack
2432755550, win 28960, options [mss 1460,sackOK,TS val 50557410 ecr
3864513189,nop,wscale 9], length 0
13:58:30.647544 IP 10.0.0.11.58716 > 172.16.0.40.http: Flags [.], ack 1, win 58,
options [nop,nop,TS val 3864513189 ecr 50557410], length 0
```

To view the 3-way handshake, you may need to increase the number of lines after the **-c** option.

c. Navigate to the terminal used to start Mininet. Terminate the Mininet by entering quit in the main CyberOps VM terminal window.

```
mininet> quit
*** Stopping 0 controllers

*** Stopping 2 terms
*** Stopping 5 links
.....
*** Stopping 1 switches
s1
*** Stopping 5 hosts
H1 H2 H3 H4 R1
*** Done
[analyst@secOps ~]$
```

d. After quitting Mininet, enter **sudo mn -c** to clean up the processes started by Mininet. Enter the password **cyberops** when prompted.

```
[analyst@secOps ~]$ sudo mn -c
[sudo] password for analyst:
```

## Reflection Questions

1. There are hundreds of filters available in Wireshark. A large network could have numerous filters and many different types of traffic. List three filters that might be useful to a network administrator.

   Filter by IP Address:

   Filter Expression: ip.addr == x.x.x.x

   Description: This filter allows a network administrator to focus on traffic to or from a specific IP address. It is valuable for isolating the communication of a particular host on the network, helping to identify potential issues or suspicious activity related to that specific IP address.

   Filter by Protocol:

   Filter Expression: tcp or udp

   Description: Filtering by protocol enables the administrator to isolate traffic based on the transport layer protocol. For example, tcp will show only TCP traffic, and udp will show only UDP traffic. This is useful for understanding the types of protocols in use and identifying potential protocol-specific issues.

   Filter by Port Number:

   Filter Expression: tcp.port == 80 or udp.port == 53

   Description: Network services are associated with specific port numbers. Filtering by port allows the administrator to focus on traffic related to a particular service. For instance, tcp.port == 80 filters for HTTP traffic, and udp.port == 53 filters for DNS traffic. This is helpful for diagnosing issues with specific services or applications.

2. What other ways could Wireshark be used in a production network?

   Wireshark can be used in a production network for:

   Troubleshooting: Identify and resolve network issues.

   Security Monitoring: Detect suspicious or malicious activity.

   Performance Monitoring: Analyze and optimize application performance.

   QoS Assessment: Evaluate Quality of Service policies.

   Protocol Analysis: Understand and optimize protocol behavior.

   Baseline Creation: Establish normal network behavior for anomaly detection.

   VoIP Troubleshooting: Diagnose issues in Voice over IP services.

   Capacity Planning: Plan for network upgrades based on traffic analysis.

*End of document*