## Wireshark Lab 1.1. Recording  Network Traffic and creating A PCAP file (V1.1)

### OVERVIEW

What is a PCAP File?

**PCAP** files are data files created by using the Wireshark program, and they contain the packet data of a network. These files are mainly used in analyzing the network characteristics of certain data.
The files also contribute to successfully controlling the traffic of a certain network since they are being monitored by the program.

The data and the results of the network analysis are saved using the PCAP file extension, which is why they are called PCAP files.
These files are used to determine network status, allowing analyzers to attend to problems that may have occurred on the network and allow them to study data communications using Wireshark.

### OBJECTIVE:

**1- How to use the PCAP file.**
**2- How to examine a PCAP file.**
**3- How to find/extract information from a PCAP file.**

### REQUIREMENTS:

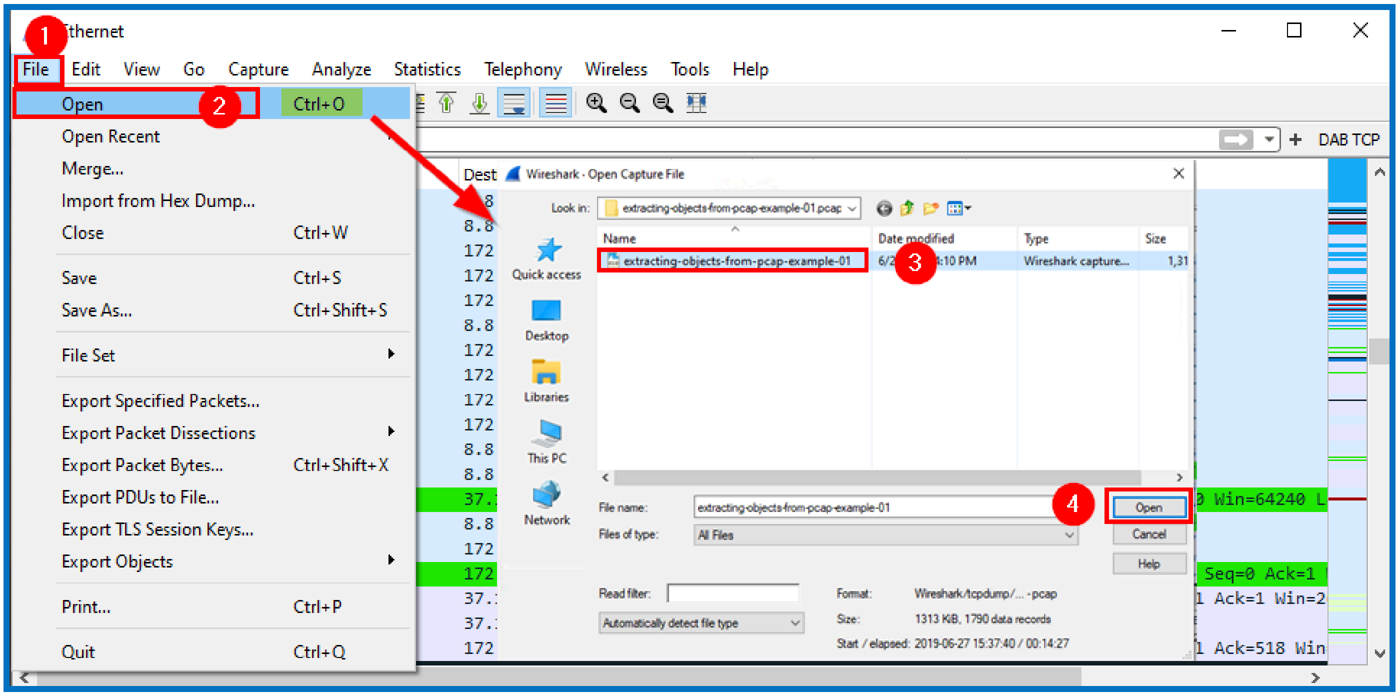
- □ Wireshark Application
- □ OS (Windows, macOS, or Linux)

### STEPS:

**Part 1 - Capture Traffic on Ethernet NIC /or WiFi Nic.**
**Part 2 - Add Coloring Rule for TCP packet.**
**Part 3 - adding Custom Columns (TCP Segment Len).**
**Part 4: Saving  captured Traffic.**

### Part 1- HOW TO OPEN A PCAP FILE?

Launch a PCAP file by double-clicking it. If your file associations are set up correctly, the application that is meant to open yourPCAP file will open it,  or use Wireshark software. Click on **file**, and then click **OPEN** or **(CTRL + O).**



Look in: extracting-objects-from-pcap-example-01.pcap

extracting-objects-from-pcap-example-01 | 6/2...:10 PM | Wireshark capture... | 1,31

File name: extracting-objects-from-pcap-example-01

Files of type: All Files

Read filter:

Automatically detect file type

Format: Wireshark/tcpdump/... - pcap

Size: 1313 KiB, 1790 data records

Start / elapsed: 2019-06-27 15:37:40 / 00:14:27

## Part 2 - Examining PCAP File:

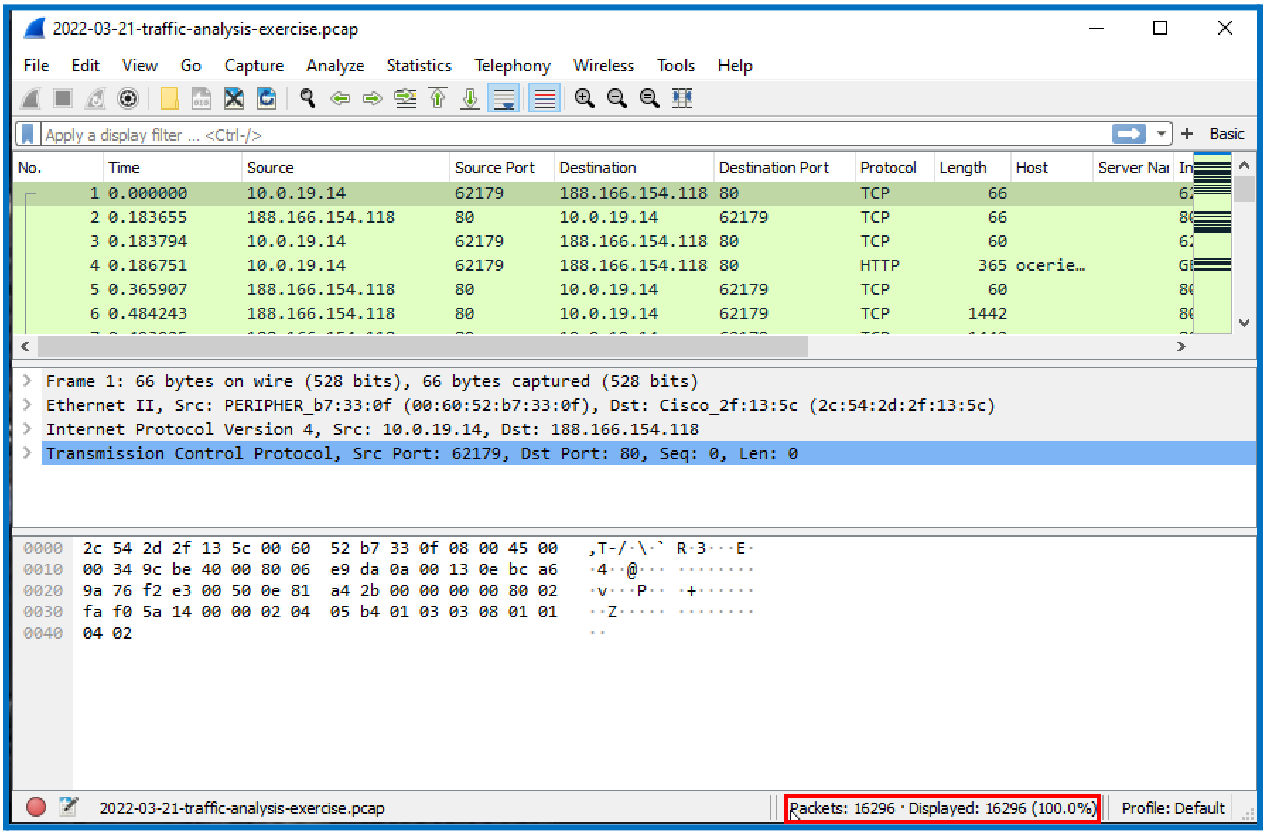
In this lab, we are going to examine **(2022-03-21 - TRAFFIC ANALYSIS EXERCISE - BURNINCANDLE)** PCAP file. To get started:

- ☑ ~~Download the PCAP for this lab using the link here **Password: infected**~~
    - ☐ **Extract the file after you download it, then open the PCAP file.**
- ☑ ~~Open the PCAP file in Wireshark.~~

How many packets were captured in this trace file?
16296

Check the bottom-right corner of the recorded packets to determine how many packets are there. The number of packets will appear as seen in the image below.

- Number of packets : **16296**



2022-03-21-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Basic

| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Host | Server Nai | In |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | 62 |
| 2 | 0.183655 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 66 | | | 80 |
| 3 | 0.183794 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62 |
| 4 | 0.186751 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | HTTP | 365 | ocerie… | | GE |
| 5 | 0.365907 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 60 | | | 80 |
| 6 | 0.484243 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 |
| 7 | 0.493025 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | |

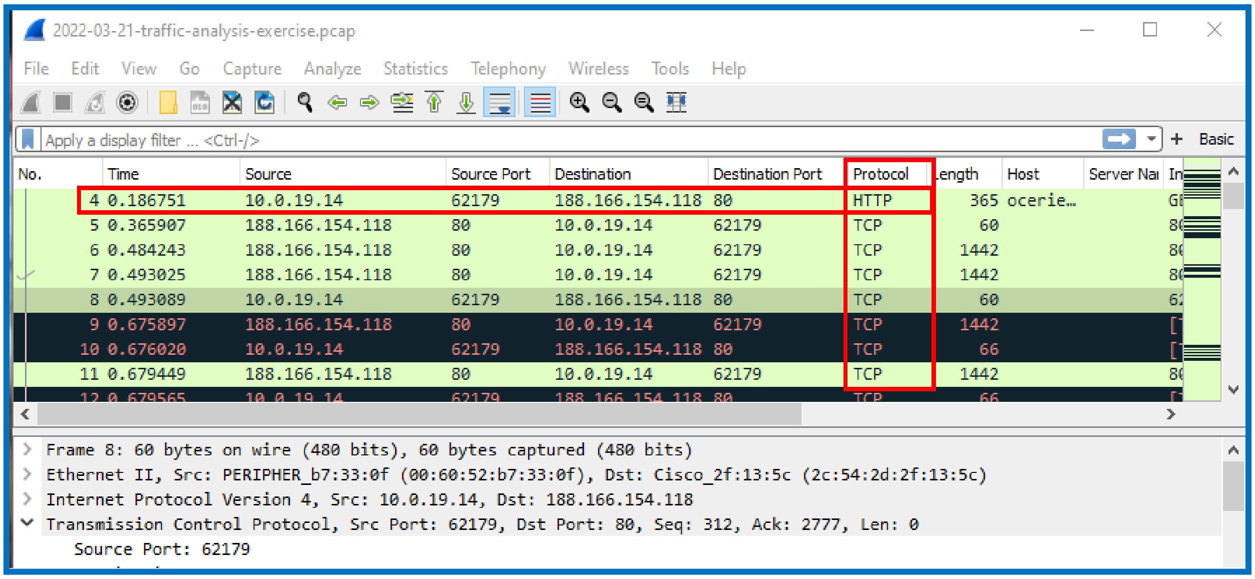
```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  2c 54 2d 2f 13 5c 00 60  52 b7 33 0f 08 00 45 00   ,T-/·\·` R·3···E·
0010  00 34 9c be 40 00 80 06  e9 da 0a 00 13 0e bc a6   ·4··@··· ········
0020  9a 76 f2 e3 00 50 0e 81  a4 2b 00 00 00 00 80 02   ·v···P·· ·+······
0030  fa f0 5a 14 00 00 02 04  05 b4 01 03 03 08 01 01   ··Z····· ········
0040  04 02                                              ··
```

2022-03-21-traffic-analysis-exercise.pcap | Packets: 16296 · Displayed: 16296 (100.0%) | Profile: Default

☑ ~~What protocol does packet number 4 contain?~~

The packet number 4 protocol is **HTTP** as shown in the picture below.



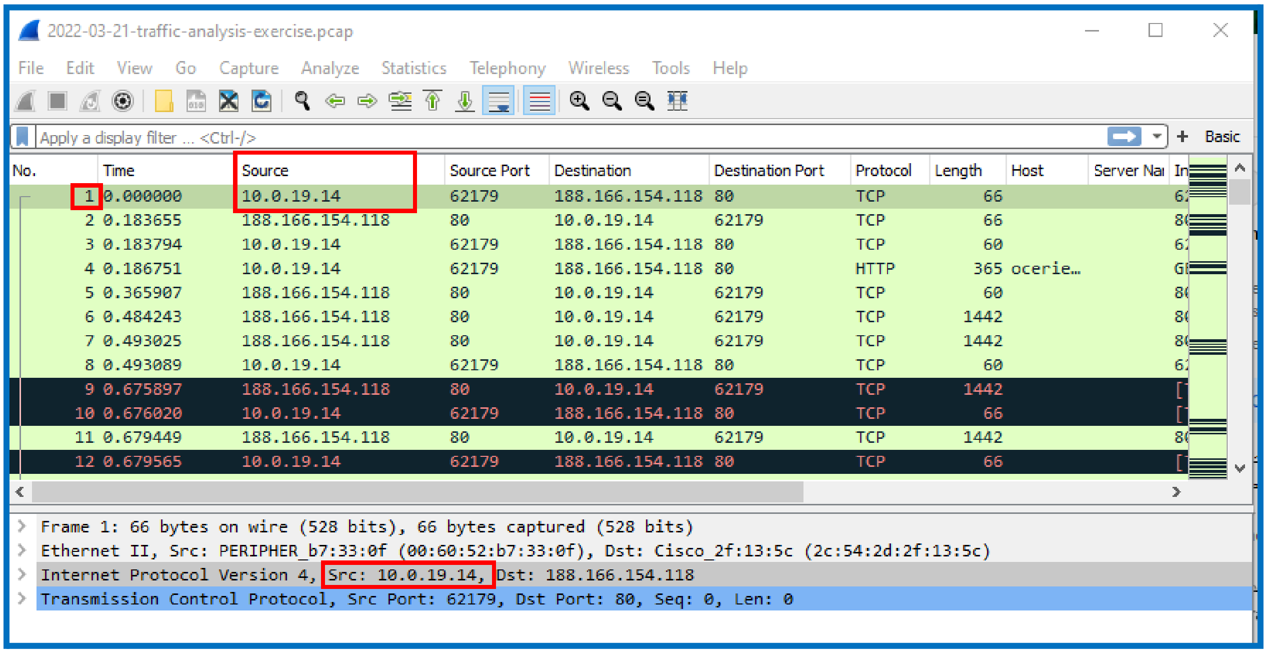
2022-03-21-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Basic

| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Host | Server Nai | In |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 0.186751 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | HTTP | 365 | ocerie… | | GE |
| 5 | 0.365907 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 60 | | | 80 |
| 6 | 0.484243 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 |
| 7 | 0.493025 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 |
| 8 | 0.493089 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62 |
| 9 | 0.675897 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | [ |
| 10 | 0.676020 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [ |
| 11 | 0.679449 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 |
| 12 | 0.679565 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [ |

```
Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 312, Ack: 2777, Len: 0
    Source Port: 62179
```

☑ ~~**Look at packet number 1. What is the source IP address in this packet?**~~
From the PCAP file, the source IP address for packet number one is : **10.0.19.14** as shown in the picture below.



2022-03-21-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Basic

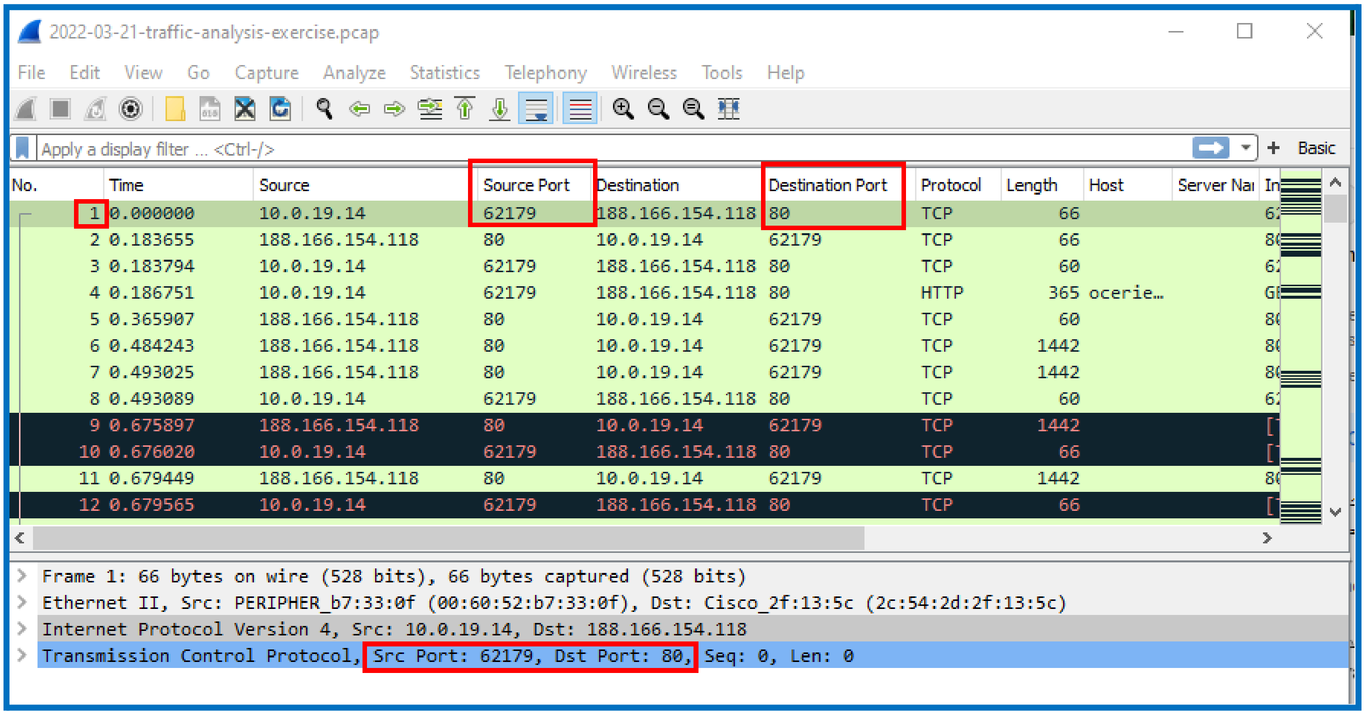
| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Host | Server Nai | In |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | 62 |
| 2 | 0.183655 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 66 | | | 8( |
| 3 | 0.183794 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62 |
| 4 | 0.186751 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | HTTP | 365 | ocerie… | | GE |
| 5 | 0.365907 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 60 | | | 8( |
| 6 | 0.484243 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 8( |
| 7 | 0.493025 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 8( |
| 8 | 0.493089 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62 |
| 9 | 0.675897 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | [ |
| 10 | 0.676020 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [ |
| 11 | 0.679449 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 8( |
| 12 | 0.679565 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [ |

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
> Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
> Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 0, Len: 0
```

☐ **What is the source and destination TCP port in this same packet?**

From the PCAP file:

- ❖ The source TCP port is: **62179.**
- ❖ The destination TCP port is: **80.**



2022-03-21-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Basic

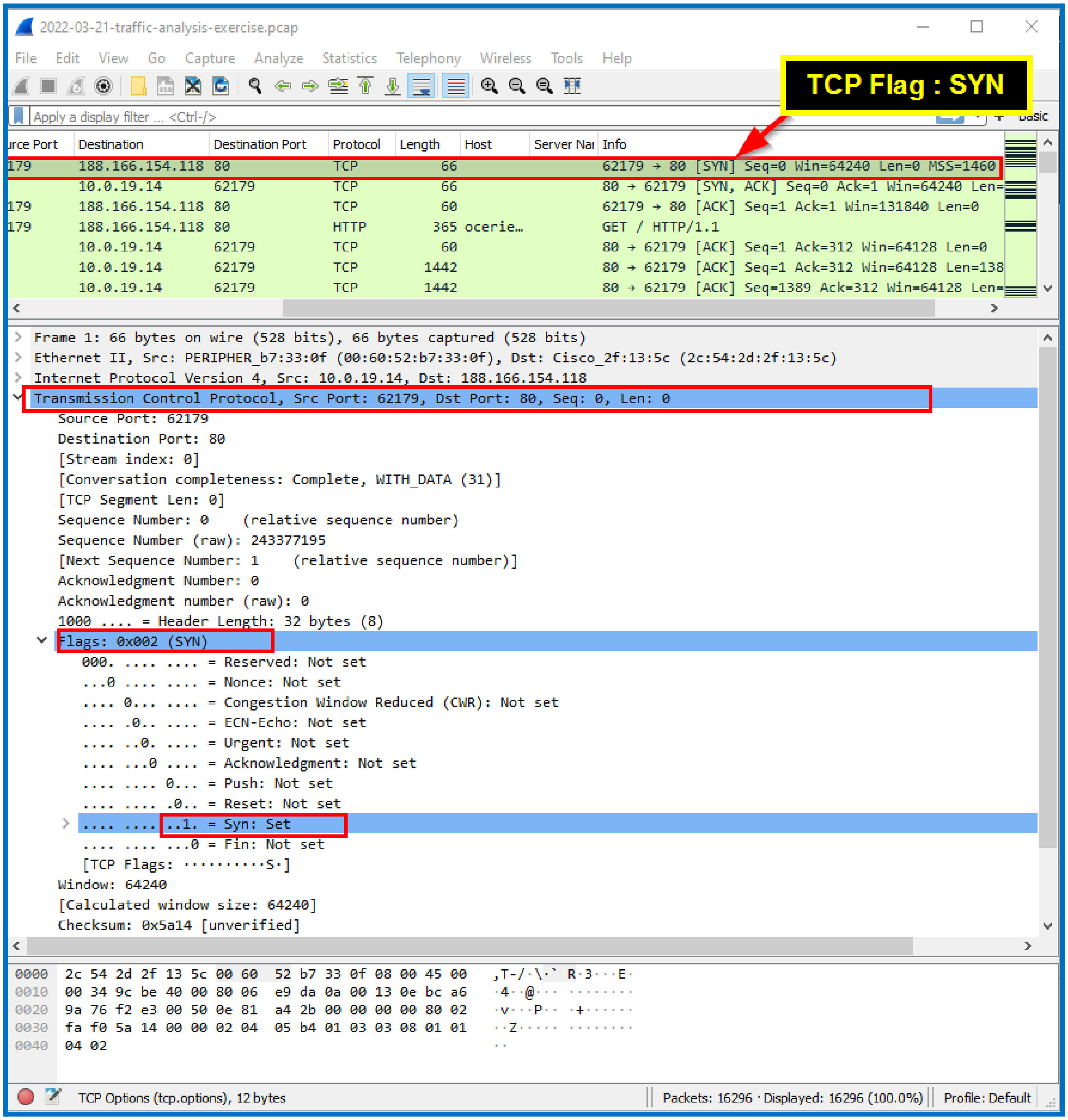
| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Host | Server Nai | In |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | 62 |
| 2 | 0.183655 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 66 | | | 8( |
| 3 | 0.183794 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62 |
| 4 | 0.186751 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | HTTP | 365 | ocerie… | | GE |
| 5 | 0.365907 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 60 | | | 8( |
| 6 | 0.484243 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 8( |
| 7 | 0.493025 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 8( |
| 8 | 0.493089 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62 |
| 9 | 0.675897 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | [ |
| 10 | 0.676020 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [ |
| 11 | 0.679449 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 8( |
| 12 | 0.679565 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [ |

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
> Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
> Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 0, Len: 0
```

☑ ~~**What TCP flag is set in packet number 1?**~~

From the PCAP, there are two ways to identify the TCP flag:

- The TCP flag is **SYN**, as shown in the first packet's **information column**.
- We can find the **TCP Flag** by expanding the **TCP section**, and then in the **flags section** as shown in the picture below.



2022-03-21-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Basic
TCP Flag : SYN

| urce Port | Destination | Destination Port | Protocol | Length | Host | Server Nai | Info |
|---|---|---|---|---|---|---|---|
| 179 | 188.166.154.118 | 80 | TCP | 66 | | | 62179 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 |
| | 10.0.19.14 | 62179 | TCP | 66 | | | 80 → 62179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len= |
| 179 | 188.166.154.118 | 80 | TCP | 60 | | | 62179 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0 |
| 179 | 188.166.154.118 | 80 | HTTP | 365 | ocerie… | | GET / HTTP/1.1 |
| | 10.0.19.14 | 62179 | TCP | 60 | | | 80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=0 |
| | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=138 |
| | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 → 62179 [ACK] Seq=1389 Ack=312 Win=64128 Len= |

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
> Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
v Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 62179
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 243377195
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x5a14 [unverified]
```

```
0000  2c 54 2d 2f 13 5c 00 60  52 b7 33 0f 08 00 45 00   ,T-/·\·` R·3···E·
0010  00 34 9c be 40 00 80 06  e9 da 0a 00 13 0e bc a6   ·4··@··· ········
0020  9a 76 f2 e3 00 50 0e 81  a4 2b 00 00 00 00 80 02   ·v···P·· ·+······
0030  fa f0 5a 14 00 00 02 04  05 b4 01 03 03 08 01 01   ··Z····· ········
0040  04 02                                              ··
```

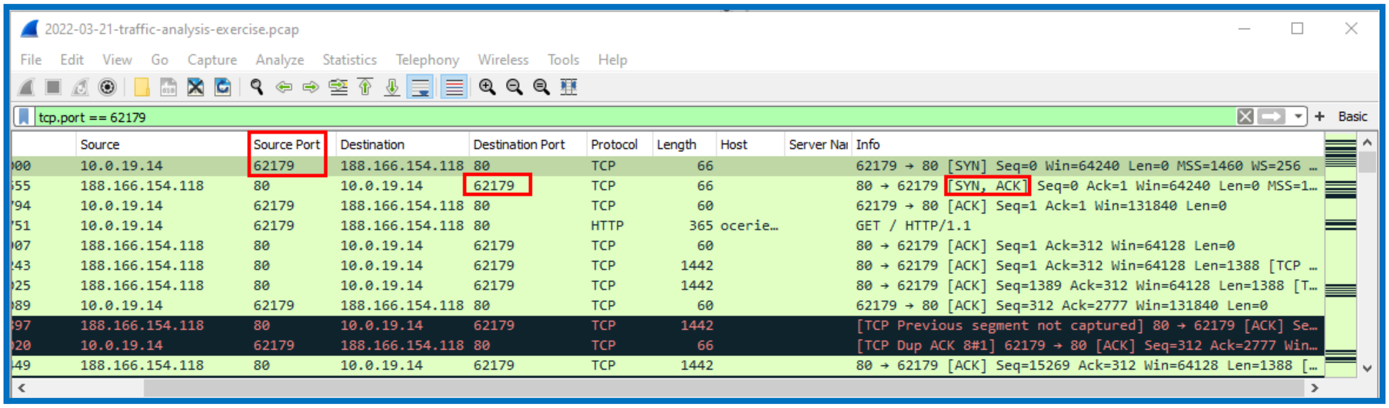
TCP Options (tcp.options), 12 bytes | Packets: 16296 · Displayed: 16296 (100.0%) | Profile: Default

- ☑ ~~What is the frame number of the next packet in this TCP conversation?~~

**The TCP 3-Way Handshake (SYN, SYN-ACK,ACK) - b**ecause the first packet is a **SYN** packet, the second packet will be a **SYN-ACK** packet.

There are many methods for locating all of the packets that are related to the first packet:

- ☑ ~~Use a filter (TCP.port == the first packet's port number).~~
- ☑ ~~Use scrolling, through the packets seeking a packet with the same port number.~~


2022-03-21-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Basic

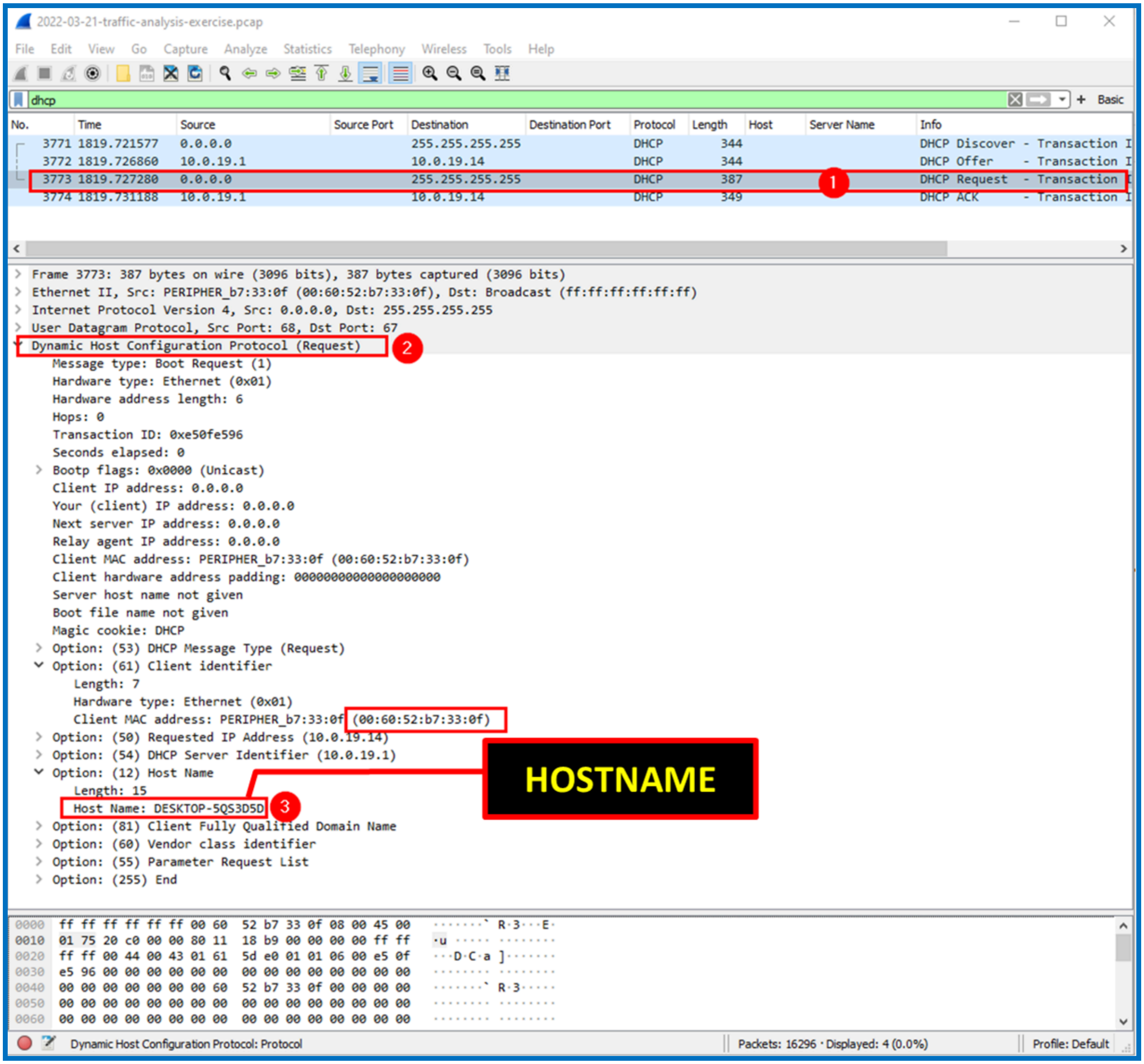
tcp.port == 62179

| | Source | Source Port | Destination | Destination Port | Protocol | Length | Host | Server Nai | Info |
|---|---|---|---|---|---|---|---|---|---|
| 00 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | 62179 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 … |
| 55 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 66 | | | 80 → 62179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1… |
| 94 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62179 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0 |
| 51 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | HTTP | 365 | ocerie… | | GET / HTTP/1.1 |
| 07 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 60 | | | 80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=0 |
| 43 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len=1388 [TCP … |
| 25 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 → 62179 [ACK] Seq=1389 Ack=312 Win=64128 Len=1388 [T… |
| 89 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 60 | | | 62179 → 80 [ACK] Seq=312 Ack=2777 Win=131840 Len=0 |
| 97 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | [TCP Previous segment not captured] 80 → 62179 [ACK] Se… |
| 20 | 10.0.19.14 | 62179 | 188.166.154.118 | 80 | TCP | 66 | | | [TCP Dup ACK 8#1] 62179 → 80 [ACK] Seq=312 Ack=2777 Win… |
| 49 | 188.166.154.118 | 80 | 10.0.19.14 | 62179 | TCP | 1442 | | | 80 → 62179 [ACK] Seq=15269 Ack=312 Win=64128 Len=1388 [… |

## Part 3 - Host Information from DHCP Traffic

To locate the host name in the PCAP file. Search for the DHCP DORA packets.

- ☑ ~~On the Filter tab, type DHCP.~~
- ☑ ~~Click the DHCP Request Packet.~~
- ☑ ~~Expand the TCP section, and then choose Option (12) Host Name~~
  - ☑ ~~Host Name = **DESKTOP-5QS3D5D**~~


2022-03-21-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
Basic
1
2
3
HOSTNAME

| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Host | Server Name | Info |
|---|---|---|---|---|---|---|---|---|---|---|
| 3771 | 1819.721577 | 0.0.0.0 | | 255.255.255.255 | | DHCP | 344 | | | DHCP Discover - Transaction I |
| 3772 | 1819.726860 | 10.0.19.1 | | 10.0.19.14 | | DHCP | 344 | | | DHCP Offer - Transaction I |
| 3773 | 1819.727280 | 0.0.0.0 | | 255.255.255.255 | | DHCP | 387 | | | DHCP Request - Transaction I |
| 3774 | 1819.731188 | 10.0.19.1 | | 10.0.19.14 | | DHCP | 349 | | | DHCP ACK - Transaction I |

```
> Frame 3773: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits)
> Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe50fe596
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: PERIPHER_b7:33:0f (00:60:52:b7:33:0f)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  v Option: (61) Client identifier
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: PERIPHER_b7:33:0f (00:60:52:b7:33:0f)
  > Option: (50) Requested IP Address (10.0.19.14)
  > Option: (54) DHCP Server Identifier (10.0.19.1)
  v Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-5QS3D5D
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

```
0000  ff ff ff ff ff ff 00 60  52 b7 33 0f 08 00 45 00   ·······` R·3···E·
0010  01 75 20 c0 00 00 80 11  18 b9 00 00 00 00 ff ff   ·u······ ········
0020  ff ff 00 44 00 43 01 61  5d e0 01 01 06 00 e5 0f   ···D·C·a ]·······
0030  e5 96 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 60  52 b7 33 0f 00 00 00 00   ·······` R·3·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Dynamic Host Configuration Protocol: Protocol | Packets: 16296 · Displayed: 4 (0.0%) | Profile: Default

This concludes this lab.

Please discuss the following questions with your instructor.

**LAB SUBMISSION REQUIREMENTS**

**Please submit a pdf with the following:**

1. **A screenshot of the snapshot taken once the lab is completed.**
2. **One to three screenshots demonstrating the configurations that you made during this lab.**
3. **Discussion questions with your answers.**

## DISCUSSION QUESTIONS:

1. *Can Wireshark modify packets?*

*While Wireshark is an excellent tool for capturing and analyzing network traffic, it does not have the functionality to modify packets.*

2. *What can you determine from the PCAP File?*

*By analyzing a PCAP file, you can determine a wide range of information about the network traffic and activities that took place during the capture. Here are some key insights you can gain from a PCAP file:*

*Network Traffic Analysis*

*Communication Patterns*

*Performance Metrics*

*Security Analysis*

*Application-Level Data*

*Network Troubleshooting*

3. *How do I get information from a PCAP File?*

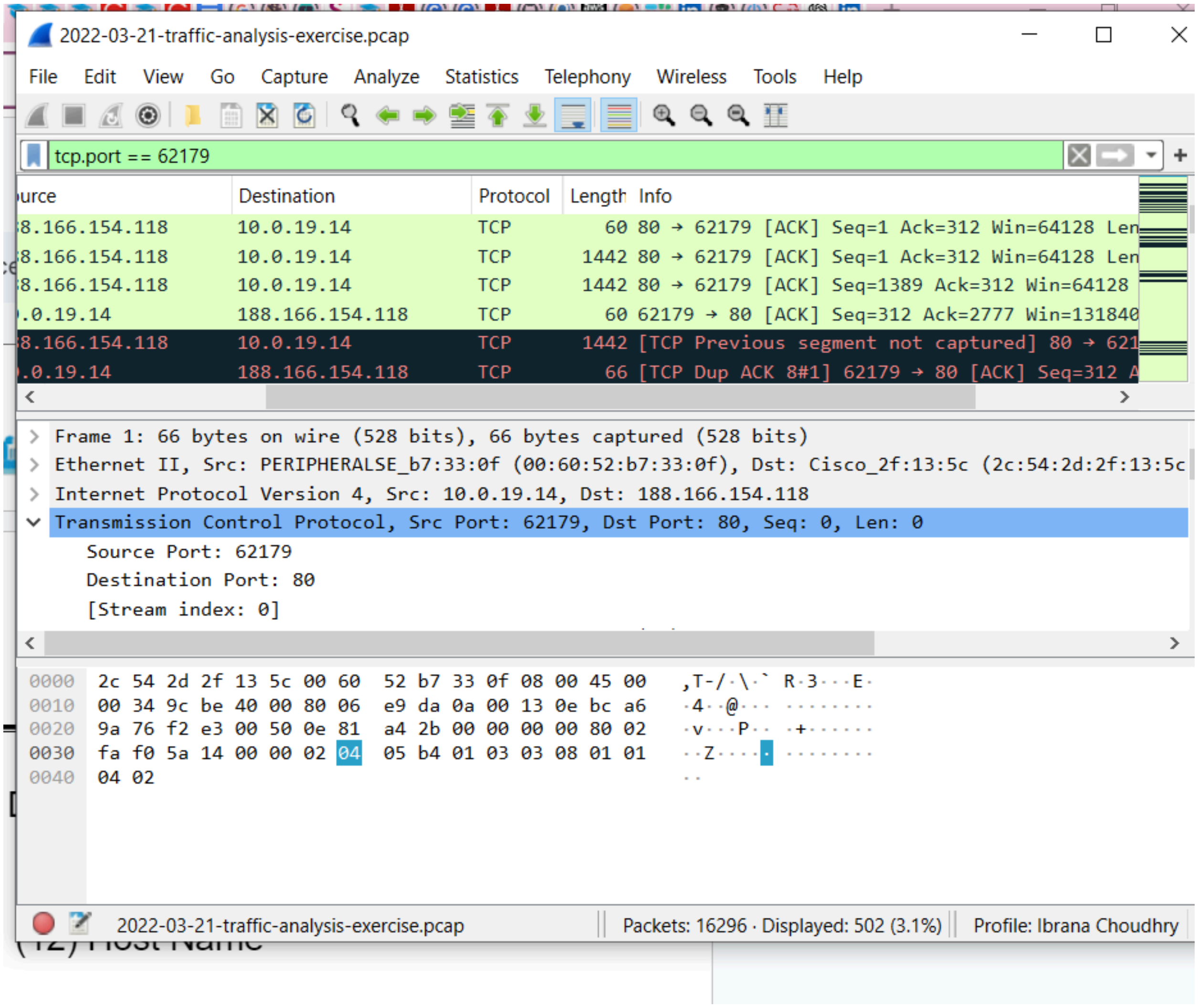
*Analyzing a PCAP file with Wireshark involves opening the file, applying filters to narrow down the data, examining specific packets and conversations, and using statistical tools to extract meaningful insights. With practice, you can efficiently diagnose network issues, monitor performance, and enhance security by leveraging the detailed information available in PCAP files.*

4. *How do I edit a PCAP File?*

*Editing a PCAP file involves altering the captured packet data. Wireshark itself does not support editing packets directly, but you can use other tools for this purpose.*

5. *What files can Wireshark read?*

*Wireshark can read an extensive range of capture file formats, which enables it to be used in a variety of environments and for multiple purposes. The most common formats include PCAP and PCAPNG, but Wireshark's versatility extends to numerous other formats as well.*



tcp.port == 62179

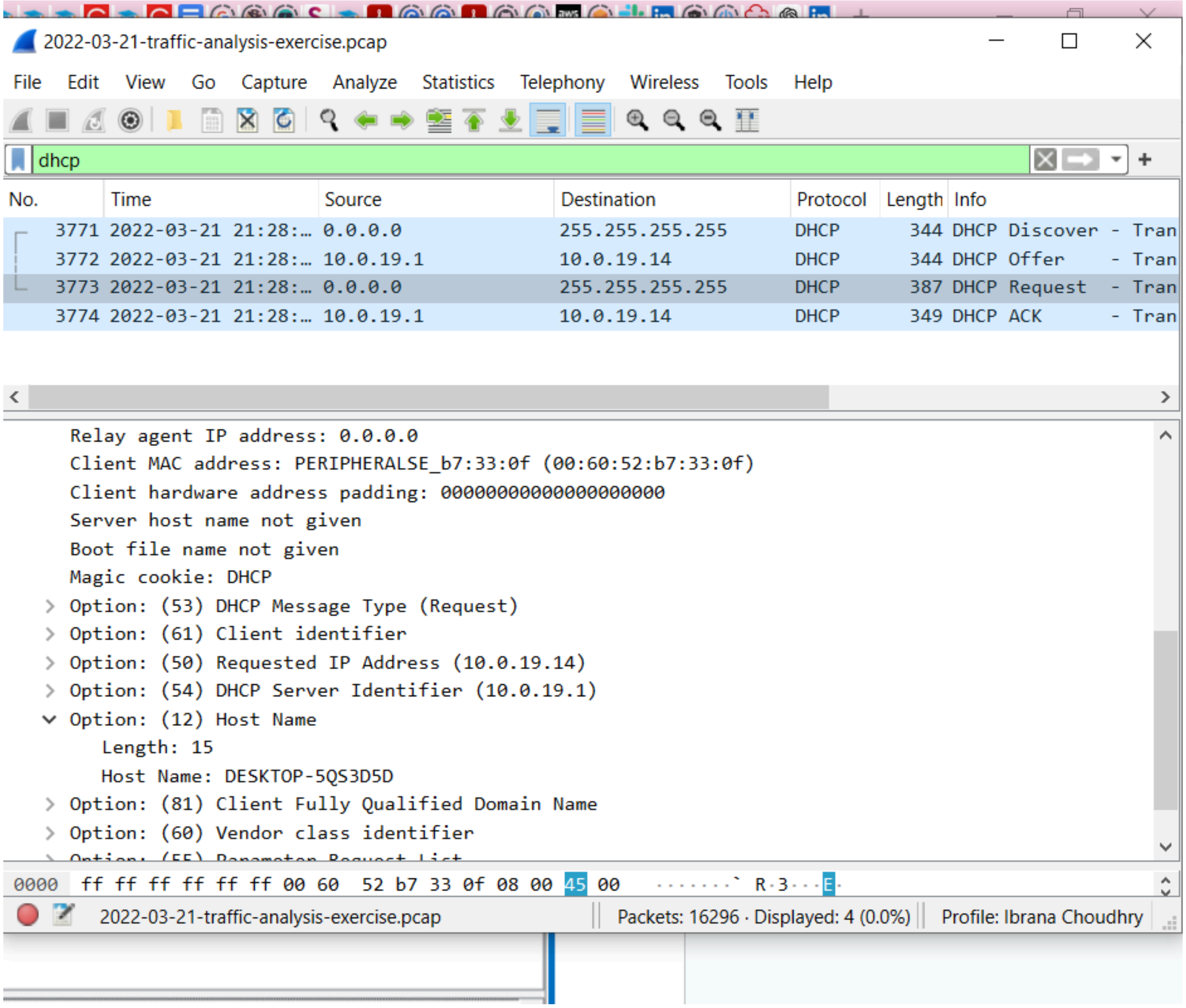
```
urce             Destination      Protocol  Length Info
8.166.154.118    10.0.19.14       TCP          60 80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len
8.166.154.118    10.0.19.14       TCP        1442 80 → 62179 [ACK] Seq=1 Ack=312 Win=64128 Len
8.166.154.118    10.0.19.14       TCP        1442 80 → 62179 [ACK] Seq=1389 Ack=312 Win=64128
.0.19.14         188.166.154.118  TCP          60 62179 → 80 [ACK] Seq=312 Ack=2777 Win=131840
8.166.154.118    10.0.19.14       TCP        1442 [TCP Previous segment not captured] 80 → 621
.0.19.14         188.166.154.118  TCP          66 [TCP Dup ACK 8#1] 62179 → 80 [ACK] Seq=312 A
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: PERIPHERALSE_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c
> Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
v Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 62179
     Destination Port: 80
     [Stream index: 0]
```

```
0000  2c 54 2d 2f 13 5c 00 60  52 b7 33 0f 08 00 45 00   ,T-/·\·` R·3···E·
0010  00 34 9c be 40 00 80 06  e9 da 0a 00 13 0e bc a6   ·4··@··· ········
0020  9a 76 f2 e3 00 50 0e 81  a4 2b 00 00 00 00 80 02   ·v···P·· ·+······
0030  fa f0 5a 14 00 00 02 04  05 b4 01 03 03 08 01 01   ··Z····· ········
0040  04 02                                              ··
```

2022-03-21-traffic-analysis-exercise.pcap | Packets: 16296 · Displayed: 502 (3.1%) | Profile: Ibrana Choudhry

(12) Host Name


2022-03-21-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

```
No.   Time                  Source       Destination       Protocol  Length Info
 3771 2022-03-21 21:28:…    0.0.0.0      255.255.255.255   DHCP         344 DHCP Discover  - Tran
 3772 2022-03-21 21:28:…    10.0.19.1    10.0.19.14        DHCP         344 DHCP Offer     - Tran
 3773 2022-03-21 21:28:…    0.0.0.0      255.255.255.255   DHCP         387 DHCP Request   - Tran
 3774 2022-03-21 21:28:…    10.0.19.1    10.0.19.14        DHCP         349 DHCP ACK       - Tran
```

```
    Relay agent IP address: 0.0.0.0
    Client MAC address: PERIPHERALSE_b7:33:0f (00:60:52:b7:33:0f)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (10.0.19.14)
  > Option: (54) DHCP Server Identifier (10.0.19.1)
  v Option: (12) Host Name
       Length: 15
       Host Name: DESKTOP-5QS3D5D
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
```

```
0000  ff ff ff ff ff ff 00 60  52 b7 33 0f 08 00 45 00   .......` R·3···E·
```

2022-03-21-traffic-analysis-exercise.pcap | Packets: 16296 · Displayed: 4 (0.0%) | Profile: Ibrana Choudhry