

# SBA 162 - Analyze Traffic with Wireshark

Version 1.0, August 2023

## Before you Begin - How to Complete This Activity

Having a Google account is strongly recommended.

Once logged in to your Google account, you can use this document's File menu to make a copy of the file. The copy will reside in your personal Google Drive. Once you have a copy of the lab file, you can type answers to questions and paste screenshots directly into the lab file.

NOTE: Do not request edit access to the file.

If you do not have a Google account, use this document's File menu to download the lab file in a format compatible with your document editor. Open the file for editing using your editor of choice (Microsoft Word, LibreOffice, PDF editor, or other), type answers to questions, and paste screenshots directly into the file.

When you have completed the lab, save the file in .pdf format.

**NOTE:** You will also create a Wireshark .pcap file in this assessment.

**Upload the completed .pdf document and the Wireshark .pcap file to Canvas using the Submit button.**

Still confused? Refer to [The Lab Process guide](#).

## Introduction

Wireshark is a widely used open-source network protocol analyzer. It is primarily used for capturing and analyzing the traffic that flows across a computer network. Wireshark allows users to inspect the data packets exchanged between devices on a network, providing detailed information about the communication process.

During this module, you have explored different features of Wireshark. In this Skill-Based Assessment, you will demonstrate your skills in capturing and analyzing network traffic.

**Note:** As Wireshark constantly evolves, images, functions, and tool locations may differ slightly from what is displayed here.

## Objectives

- Capture network traffic with Wireshark.
- Create a profile.
- Customize the profile.
- Analyze ICMP traffic with Wireshark.
- Analyze DNS traffic with Wireshark.
- Analyze TCP headers with Wireshark.

- Analyze TLS with Wireshark.
- Analyze ARP traffic with Wireshark.

### Equipment

- A laptop or PC running Windows with Internet connectivity or A Windows Virtual Machine with Internet connectivity.
- Wireshark Protocol Analyzer installed on the laptop, PC, or virtual machine.

### Instructions

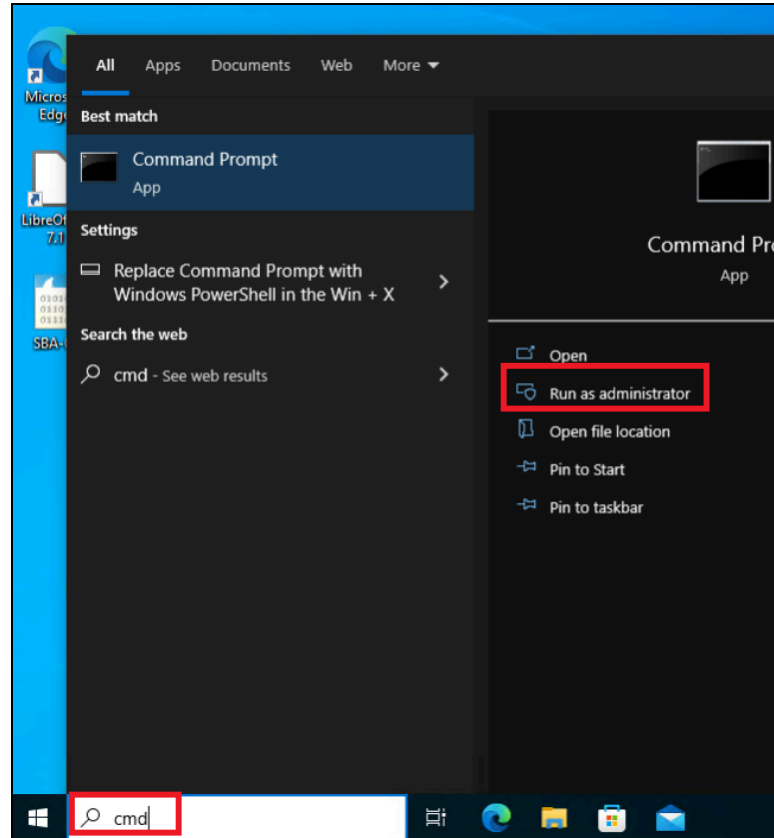
Answer the questions and provide screenshots.

### Capture network traffic with Wireshark.

Before you start capturing traffic with Wireshark, you will clear the DNS and ARP caches on the capturing device. This will help ensure that you capture the traffic necessary for this SBA.

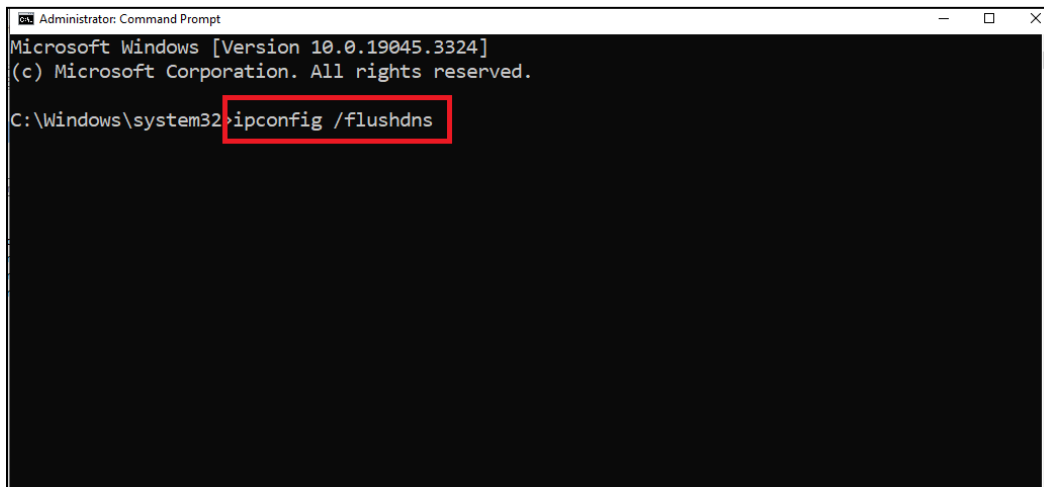
- a. On your **Windows** machine, launch the **Wireshark** program (Do not start the capture yet).
- b. On your **Windows** machine (the same one you will use to capture network traffic for this SBA), search for **cmd** and select **Run as administrator** from the **Command Prompt App** options.

C.



d.

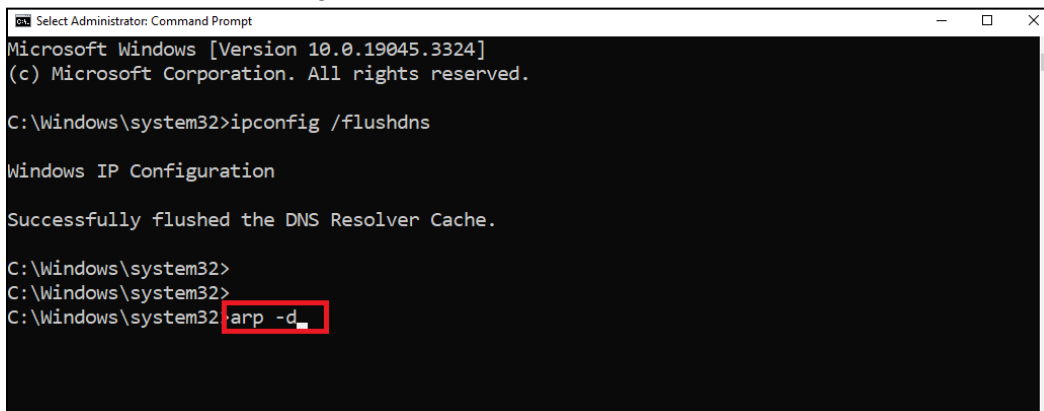
e. In the Command Prompt, type **ipconfig /flushdns** and press **Enter** key.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3324]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /flushdns
```

f. Once you are notified that **Windows IP Configuration successfully flushed the DNS resolver Cache**, type **arp -d** into the Command Prompt and press the **Enter** key.



```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.3324]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

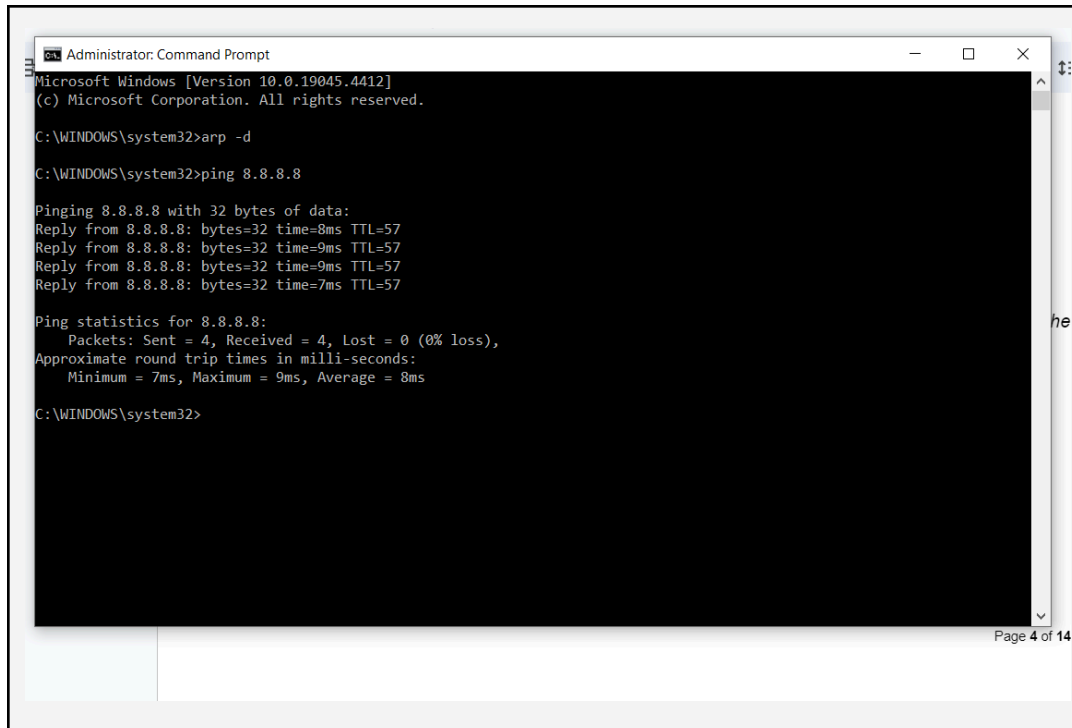
C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>arp -d
```

g. Back on the **Wireshark** program, what is the name of the interface you will be using to capture network traffic?

**Packet List**

h. Start the **network traffic capture** using **Wireshark**.

i. Back on the **Command Prompt**, ping the **8.8.8.8** IPv4 address. Take a screenshot of the ping results and paste the image into the box below.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=8ms TTL=57
Reply from 8.8.8.8: bytes=32 time=9ms TTL=57
Reply from 8.8.8.8: bytes=32 time=9ms TTL=57
Reply from 8.8.8.8: bytes=32 time=7ms TTL=57

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 9ms, Average = 8ms

C:\WINDOWS\system32>
```

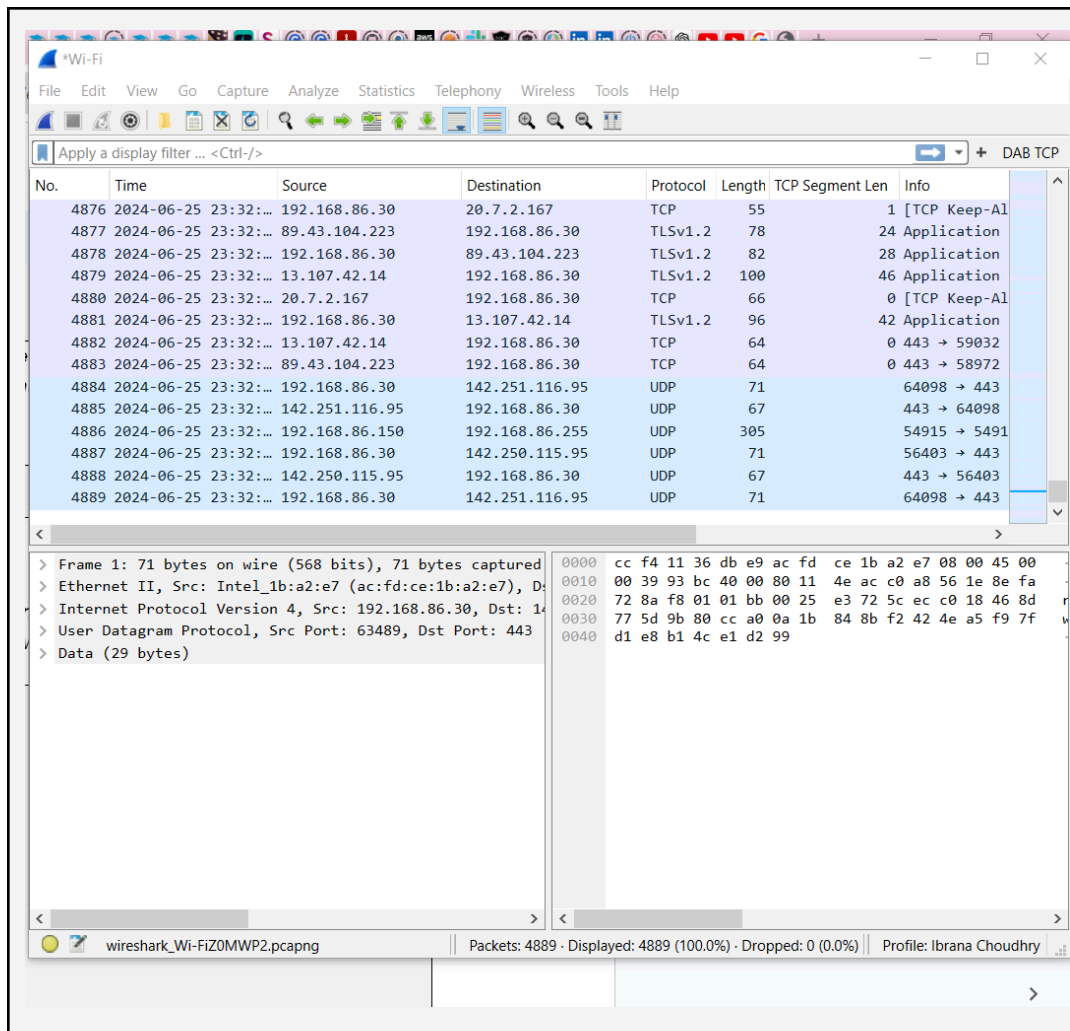
Page 4 of 14

- j. Launch a Web browser and navigate to **www.example.com**
- k. Let the capture run for one more minute.
- l. Stop the capture.
- m. How many frames did you capture?

4489

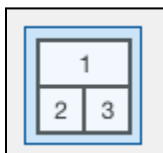
## Create a profile.

- a. Create a new Wireshark profile and name it with your name.
- b. Take a screenshot of the Wireshark window displaying your new profile and paste the image into the box below.



## Customize the profile.

- Using your new profile, zoom in to enlarge the display of the captured content.
- Resize the packet list to fit the contents.
- Ensure the display layout contains three panes, as shown in the image below.



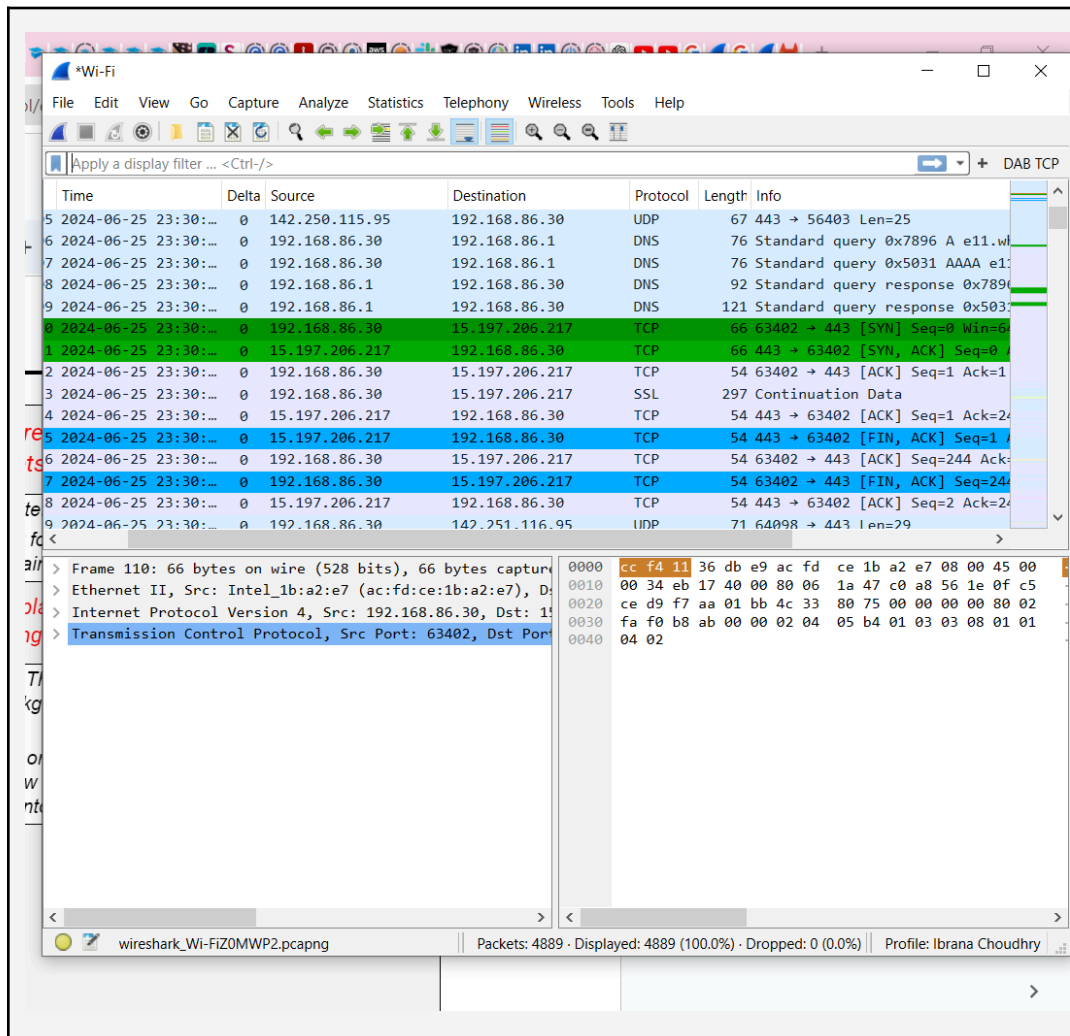
- Set pane number three to display bits.
- Add a new column named **Delta** and set it to **Delta time displayed**.
- Move the new column (Delta) to the right of the Time column.
- What information does the Delta column display?

*The delta time column in Wireshark displays the time between captured or displayed packets.*

- h. Set the No. column to alline its contents to the center.
- i. How would you change the display format of the Time column to display the time of day (note, do not change this, just explain how)?

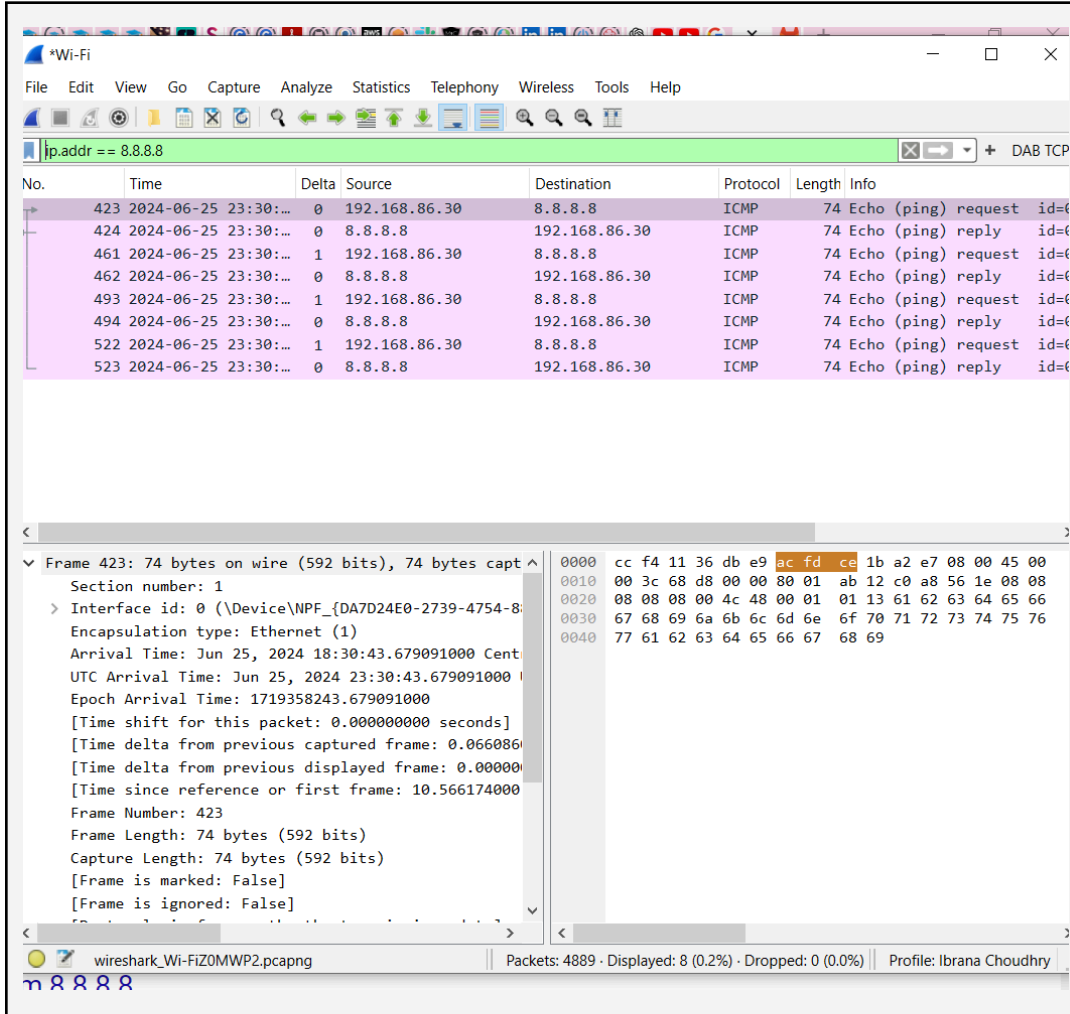
To change Wireshark's time display format, under the View menu, go to "Time Display Format," and change the value

- j. *Add a coloring rule for TCP SYN's. The rule should be the second rule after the existing Bad TCP and should color the background of the TCP SYN packets bright green. Use the filter `tcp.flags.syn == 1`*
- k. *Scroll through your packet capture or use a filter to find a TCP 3-way handshake. Take a screenshot of the Wireshark window displaying a TCP 3-way handshake using your coloring rule and paste the image into the box below.*



## Analyze ICMP traffic with Wireshark.

- Your packet capture should contain traffic generated by the ping 8.8.8.8 command issued by you earlier. Use a filter to display only the packets related to this exchange.
- Take a screenshot of the result and paste the image into the box below.



- How many packets did you find?

8

- What is the frame number of the first ping request?

423

- What is the frame number of the reply to the first ping request?

424

- What is the length of the first frame (request frame) in bytes?

74



- g. What is the Delta (time) between the first request and reply frames?

0

- h. Compare the Delta between the first request frame and the first reply frame with the first reply of the ping command in the screenshot you pasted into this file earlier. What can you conclude?

In the first screen shot it is 8ms whereas in the second one the delta is 0

- i. What is the MAC address of the sending device on the first ping request frame?

ac:fd:ce:1b:a2:e7

- j. What is the MAC address of the router used to forward the ping request to 8.8.8.8?

cc-f4-11-36-db-e9

- k. What hexadecimal value within the Ethernet II header identifies the IPV4 protocol?

0x0800

- l. What is the IPv4 address of the sending device?

192.168.86.30

- m. Within the Internet Protocol Version 4 section of the packet details (in pane 2), select the Source Address. This will highlight the bits representing the address in pane 3. Enter the 32 bits representing the IPv4 source address into the box below.

C0 a8 56 1e

- n. What is the decimal value within the Internet Control Message Protocol that signifies an Echo (ping) request?

8

- o. What is the decimal value within the Internet Control Message Protocol that signifies an Echo (ping) reply?

0

## Analyze DNS traffic with Wireshark.

- Your packet capture should contain DNS traffic generated by navigating to `www.example.com`. Note other DNS traffic may also have been captured.
- Apply a filter in Wireshark to display only the DNS traffic associated with resolving `www.example.com`.

- c. Type the filter you used into the box below.

*dns.qry.name == "www.example.com"*

- d. How many DNS packets are associated with resolving *www.example.com*?

*4*

- e. What type(s) of DNS records are queried in regard to *www.example.com*?

*A Record query*

- f. What version of the Internet Protocol is used to route the DNS packets?

*Internet Protocol version 4*

- g. What is the IP address of the DNS server?

*192.168.86.1*

- h. What transport layer protocol is used to send DNS queries?

*UDP*

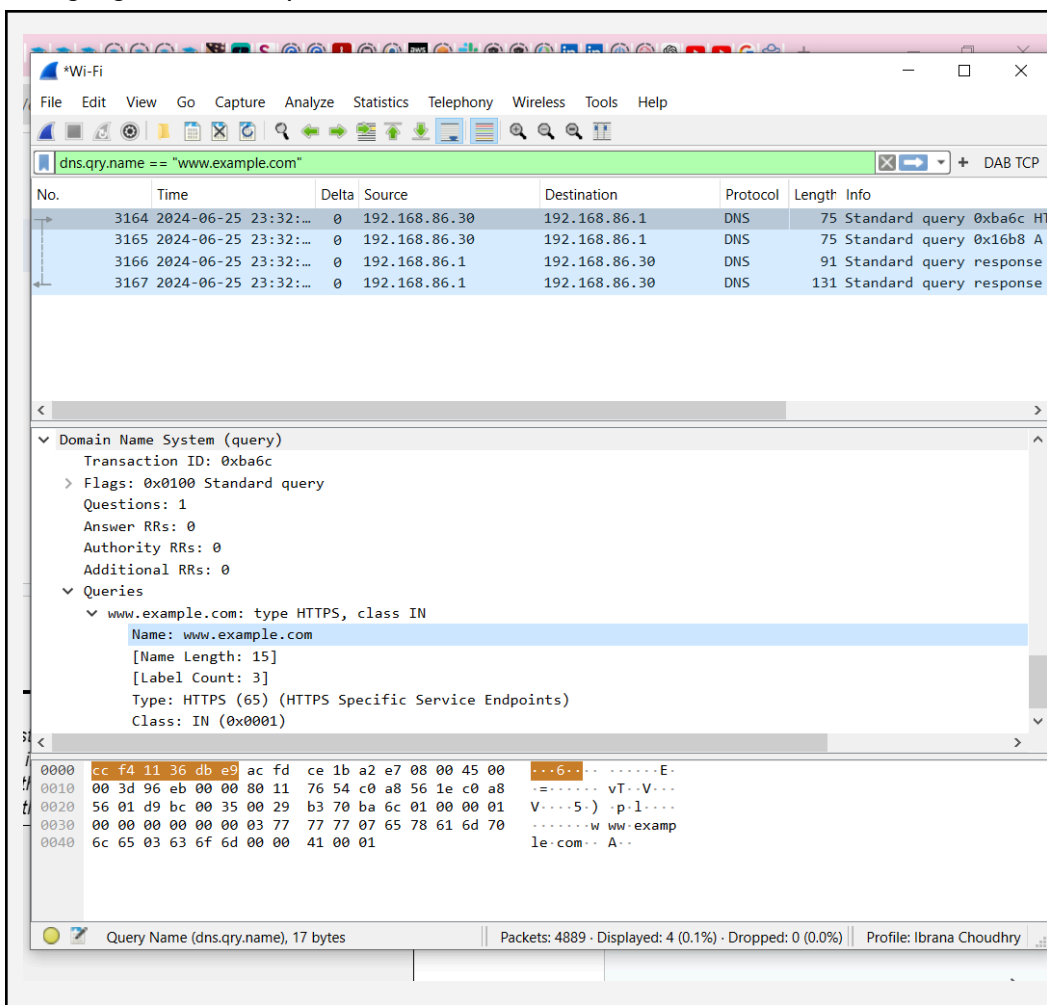
- i. What is the source port number(s) used to send the DNS queries resolving *www.example.com*?

*55740*

- j. What is the destination port number used to send DNS queries?

*53*

- k. Navigate into the Domain Name System query in the details section of the capture, locate the `www.example.com` name in the A record query, and highlight it. Take a screenshot of Wireshark displaying the result in all three panes, with the name displayed as highlighted bits on pane number three.



- l. What is the source port number(s) used to send the DNS response(s)?

53

- m. What IP address(es) are found in the Answers section of the DNS response to an A record query?

192.186.86.1 1 and 192.168.86.30

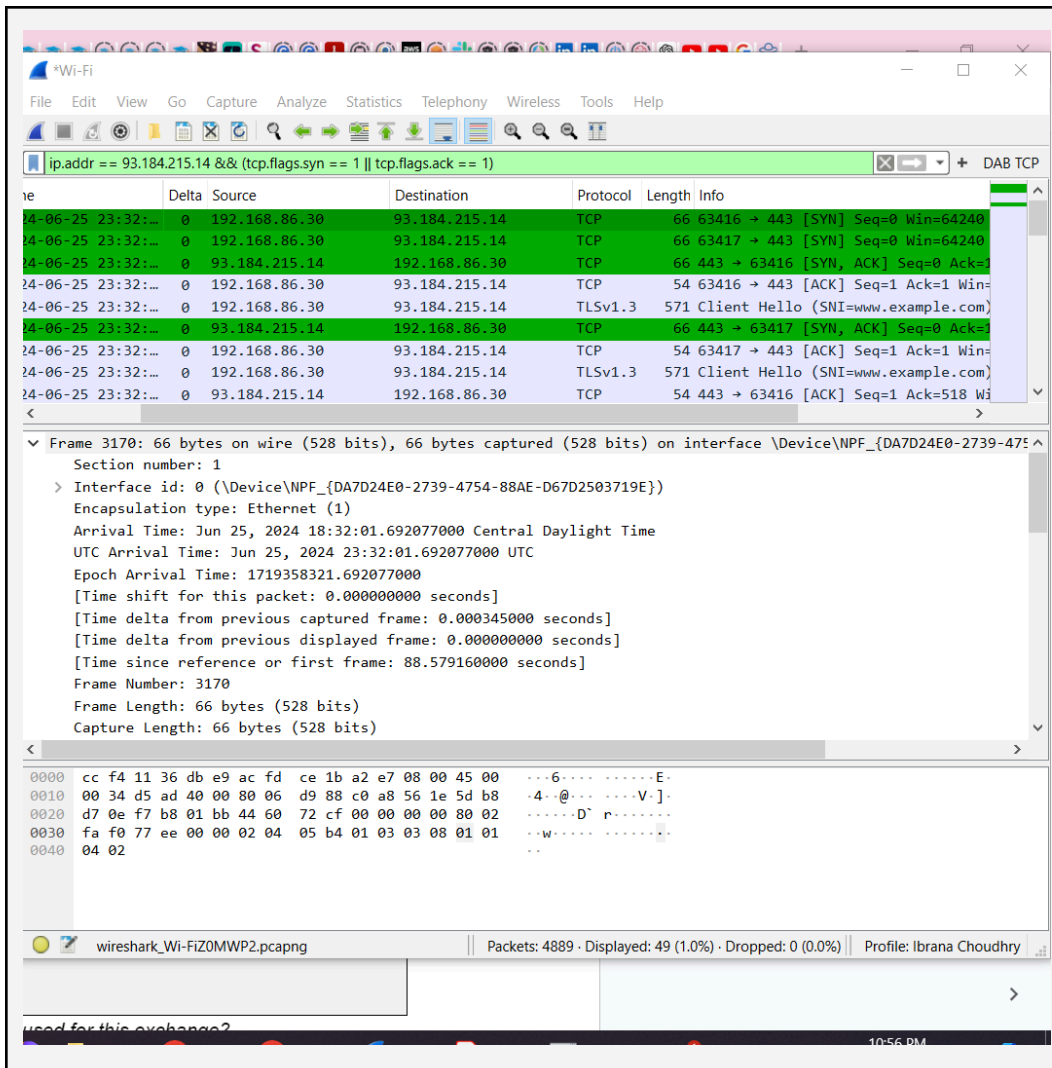
## Analyze TCP headers with Wireshark.

- Your packet capture should contain TCP traffic generated by navigating to the `www.example.com` Website.
- Use a filter to display the TCP 3-way handshake between the client and the server hosting `www.example.com`.

- c. Type the filter you used into the box below.

`ip.addr == 93.184.215.14 && (tcp.flags.syn == 1 || tcp.flags.ack == 1)`

- d. Take a screenshot of Wireshark displaying the TCP 3-way handshake between the client and the server hosting `www.example.com`. Paste the image into the box below.



- e. What is the Internet Protocol version used for this exchange?

`TCP`

- f. What is the port number used by the client for this exchange?

`63417`

- g. *What is the port number used by the server for this exchange?*

443

- h. *On the first packet of the TCP 3-way handshake, on the details pane, under the Transmission Control Protocol section, locate and highlight the flag indicating the Syn bit is set (this is the byte of data that indicates to the receiving device that this is a Syn request).*
- i. *Using the bits pane, enter the binary value of the flag indicating that this TCP packet is a Syn request into the box below.*

02

- j. *On the second packet of the TCP 3-way handshake, on the details pane, under the Transmission Control Protocol section, locate and highlight the flags indicating that both the Syn and Ack bits are set (this is the byte of data that indicates to the receiving device that this is a Syn/Ack TCP packet).*
- k. *Using the bits pane, enter the binary value of the flag indicating that this TCP packet is a Syn/Ack into the box below.*

80 12

## Analyze TLS with Wireshark.

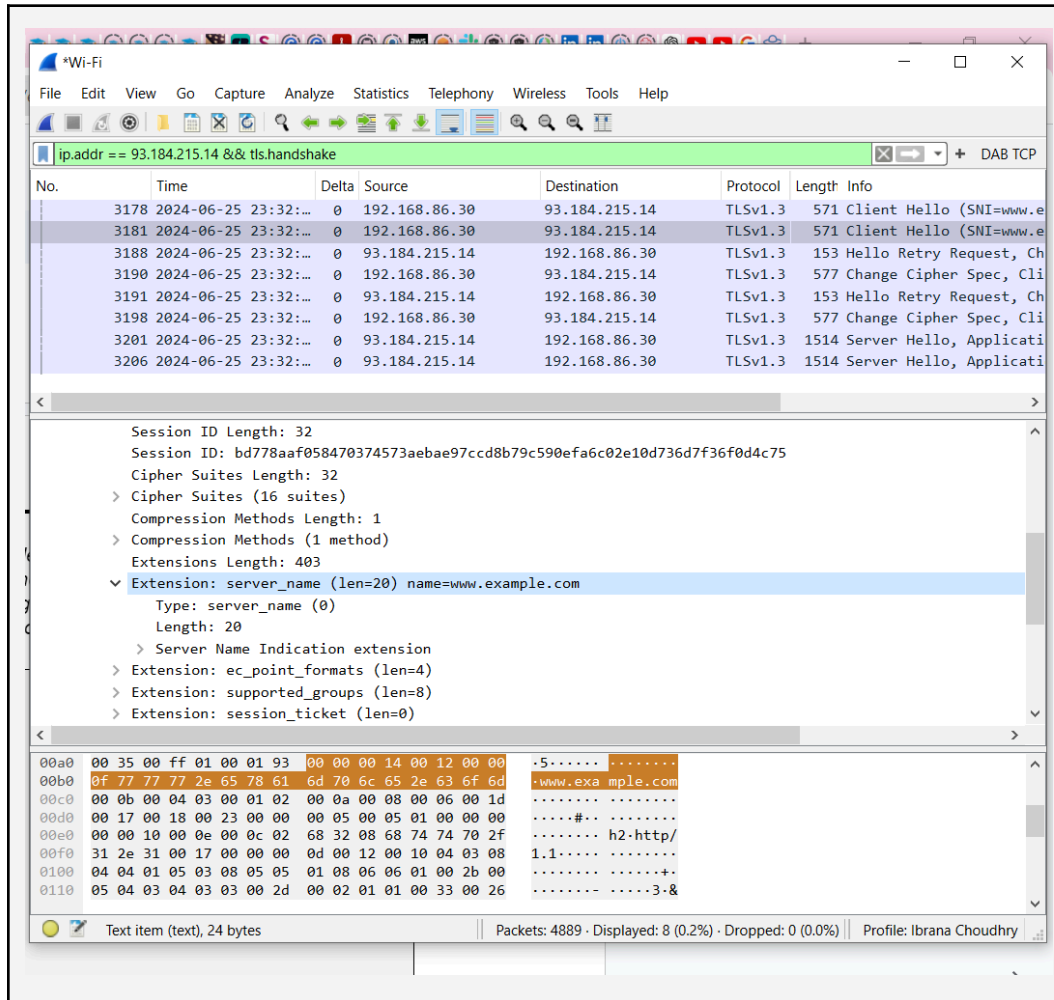
As most of the traffic on the Internet is encrypted, you will use Wireshark to examine a TLS handshake (or some of it).

Your packet capture should contain encrypted traffic generated by navigating to [www.example.com](http://www.example.com).

- a. *Use a filter to display the TLS handshake packets between the client and the server hosting [www.example.com](http://www.example.com).*
- b. *Type the filter you used into the box below.*

*ip.addr == 93.184.215.14 && tls.handshake*

- c. Select a Client Hello packet. In the details pane, locate the server name under the Extension: server\_name section of the Handshake Protocol within the Client Hello. Take a screenshot of Wireshark displaying the value `www.example.com` as the Server Name (this is one way to ensure you are looking at the correct handshake). Paste the image into the box below.



- d. How many Cipher Suites are supported by the client in this TLS session?

16

- e. List five (5) supported Cipher Suites. Include their name, hexadecimal identifier, and binary representation (16-bit binary string). Enter your answer into the table below.

Cipher Suite name	Hexadecimal identifier	16-bit binary representation
TLS_AES_256_GCM_SHA384	0x1302	0001 0011 0000 0010

<i>TLS_CHACHA20_POLY1305_SHA256</i>	<i>0x1303</i>	<i>0001 0011 0000 0011</i>
<i>TLS_AES_128_GCM_SHA256</i>	<i>0x1301</i>	<i>0001 0011 0000 0001</i>
<i>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</i>	<i>0xc02b</i>	<i>1100 0000 0010 1011</i>
<i>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</i>	<i>0xc02f</i>	<i>1100 0000 0010 1111</i>

- f. How many Signature Hash Algorithms are supported by the client in this TLS session?

8

## Analyze ARP traffic with Wireshark.

Your packet capture should contain ARP traffic generated by devices on the network.

- Search the capture file for an Address Resolution Protocol (ARP) request frame (destination address is broadcast) with a corresponding ARP reply (destination address is unicast). Use a filter in Wireshark to display only these two frames.
- Type the filter you used into the box below.

*arp.opcode==1 || arp.opcode==2*



Type: ARP (0x0806)

Protocol type: IPv4 (0x0800)

- Experiment 1 failed to find the effect of the number of trials on the effect of the number of trials on the effect of the number of trials.

4 full bytes + 4 bits

- ..... ( ) .....

00000000000000000000000000000000



- h. On the Address Resolution Protocol (request) frame, what is the hexadecimal value of the Target MAC address?

00:00:00:00:00:00

- a. On the Address Resolution Protocol (request) frame, what is the binary value of the destination MAC address?

1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111 1111