Wireshark Lab:Lab #2

ITMO440/540

Spring 2019

Goal: To understand and analyze what happens on a network when you hold a Skype call.

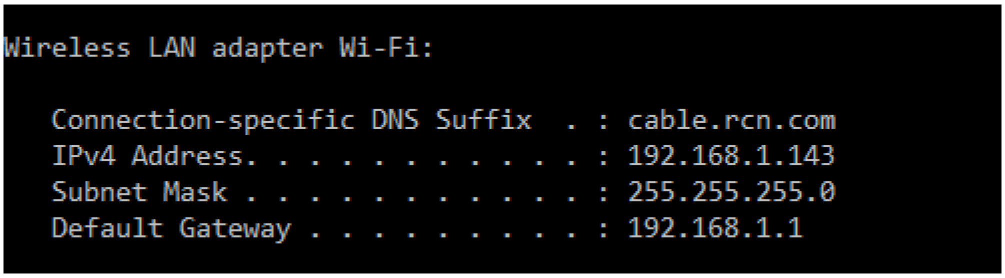
1. What is the IP Address of the computing device that you are using for this experiment? ____________________

2. What is the IP address of your default gateway? (See instructions below for how to find this information.) ______________________

INSTRUCTIONS for locating the IP Addresses of your computing device and of your default gateway router.

WINDOWS:

At the command line prompt, enter **ipconfig**. A list of your various network interface devices will appear. This might be wireless, Ethernet, and tunnel for example. Find the one or more of these that is not 'disconnected' and copy the IPv4 and/or IPv6 address associated with it. Also, note the IP address of the 'default network gateway.'



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : cable.rcn.com
   IPv4 Address. . . . . . . . . . . : 192.168.1.143
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

MAC:

If you are on a Mac OS, go to the Apple menus at the top of the screen. Select 'About this Mac." In the pop-up menu that appears, click on "more information." Click the "Network" line item in the left-hand frame. On the right, you will see the description of the active network interface(s). This description will include the IP address and the Router. The Router is your default network gateway.

PRE-TEST INSTRUCTIONS

Close all applications on the computer that you are using to run this test. This includes mail programs, browsers, and Skype.

TEST INSTRUCTIONS

1. Open Wireshark and start a capture on the network interface that you are using to connect to the Internet.

2. Open your browser.

3. Place a Skype call to someone using both voice and video. This could be a fellow student.

4. Talk for no more than 30 seconds. Then, stop your capture.

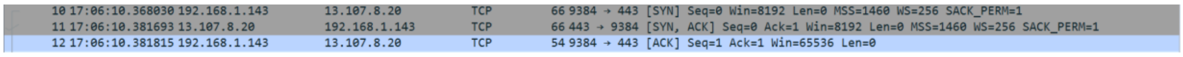
5. Save the file to your computer and name it <your last name>-<your first name>-PA-4-Skype-trace.

PART I

THREE WAY HANDSHAKE

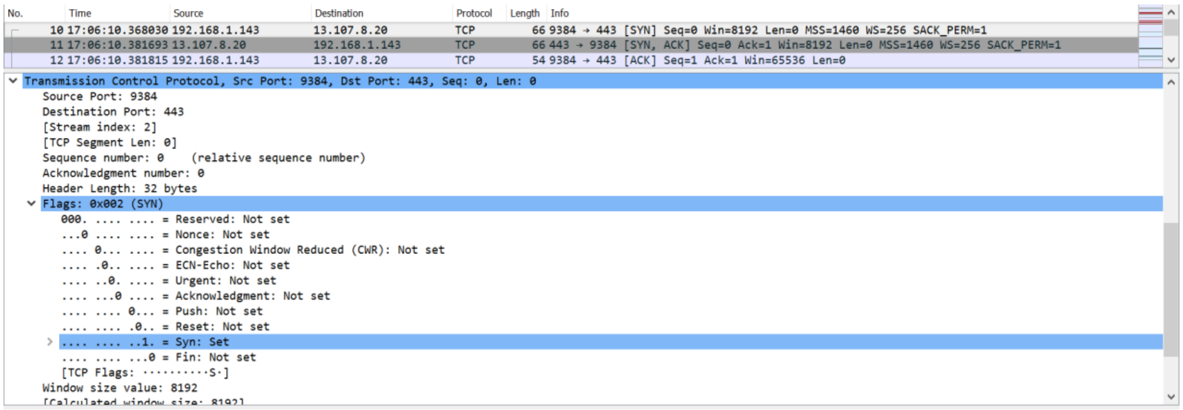
Provide the screenshot of the frames that indicate the three-way handshake that your system has made.

Three-way handshake is as shown below:



```
10 17:06:10.368030 192.168.1.143   13.107.8.20     TCP   66 9384 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11 17:06:10.381693 13.107.8.20     192.168.1.143   TCP   66 443 → 9384 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
12 17:06:10.381815 192.168.1.143   13.107.8.20     TCP   54 9384 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

Frame 10 indicates the first step of the handshake:

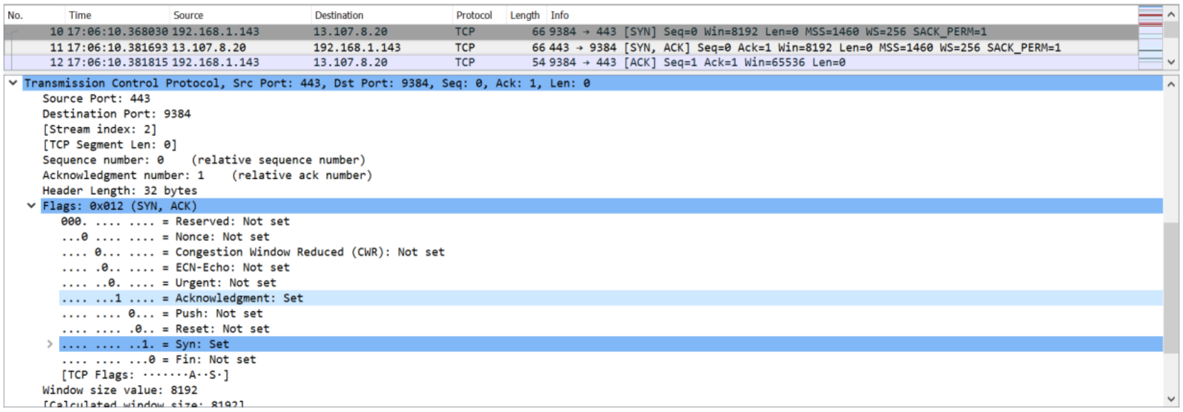


```
No.  Time               Source          Destination     Protocol  Length Info
  10 17:06:10.368030 192.168.1.143   13.107.8.20     TCP       66 9384 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  11 17:06:10.381693 13.107.8.20     192.168.1.143   TCP       66 443 → 9384 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  12 17:06:10.381815 192.168.1.143   13.107.8.20     TCP       54 9384 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0

Transmission Control Protocol, Src Port: 9384, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 9384
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 32 bytes
  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 size value: 8192
    [Calculated window size: 8192]
```

The TCP section of the **packet-header details window** shows that [SYN] bit is set to **1** which confirms that first step of the three-way handshake is successful.

Frame 11 indicates the second step of the handshake:

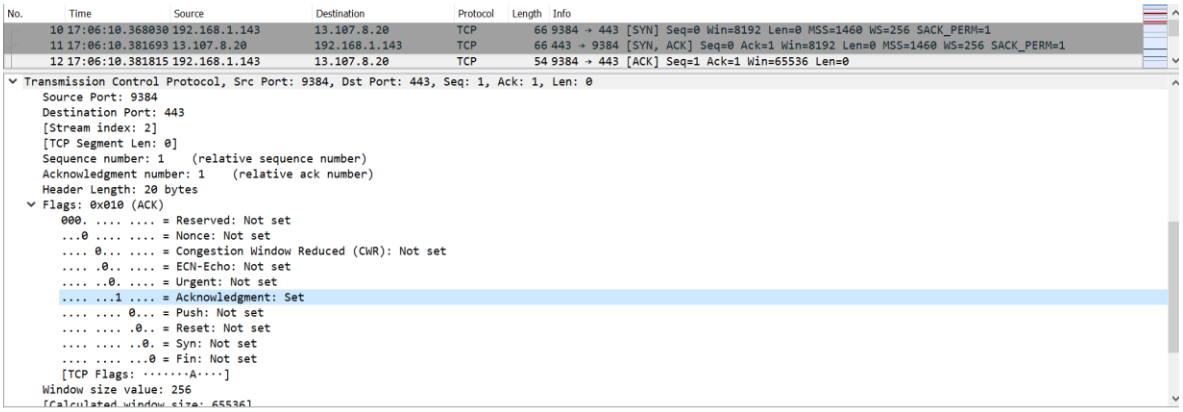


```
No.  Time               Source          Destination     Protocol  Length  Info
  10 17:06:10.368030 192.168.1.143   13.107.8.20     TCP         66 9384 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  11 17:06:10.381693 13.107.8.20     192.168.1.143   TCP         66 443 → 9384 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  12 17:06:10.381815 192.168.1.143   13.107.8.20     TCP         54 9384 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
Transmission Control Protocol, Src Port: 443, Dst Port: 9384, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 9384
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 32 bytes
  Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A··S·]
    Window size value: 8192
    [Calculated window size: 8192]
```

The TCP section of the **packet-header details window** shows that [SYN, ACK] bits is set to **1** which confirms that second step of the three-way handshake is successful.

Frame 12 indicates the third step of the handshake:



```
No.  Time               Source          Destination     Protocol  Length  Info
  10 17:06:10.368030 192.168.1.143   13.107.8.20     TCP         66 9384 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  11 17:06:10.381693 13.107.8.20     192.168.1.143   TCP         66 443 → 9384 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  12 17:06:10.381815 192.168.1.143   13.107.8.20     TCP         54 9384 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
Transmission Control Protocol, Src Port: 9384, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 9384
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header Length: 20 bytes
  Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A····]
    Window size value: 256
    [Calculated window size: 65536]
```

The TCP section of the **packet-header details window** shows that [ACK] bits is set to **1** which confirms that third step of the three-way handshake is successful.

Provide the screenshot of the frames (as shown above) that indicate the three-way handshake that your system has made.

NOTE: To obtain this three-way handshake you need to ensure that pre-test instructions must be Completed. If you were not able to reproduce three-way handshake, clear the cache, cookies, browsing history and try again.

PART II

DATA ANALYSIS

Open the .pcap file that you saved and perform the following steps

1. Filter the file to show only those frames whose source or destination IP address is the address of your computing device.

   Note: Use the following command in the filter section to complete step1.

   ip.addr == "your IP address"

   e.g. ip.addr == 192.168.1.147

2. List all the Protocol names that appear in the Protocol column of the display. (You only need to list a protocol one time, not every time you see it.) ________________________

Internet Protocol (IP)

In the "Statistics" menu for Wireshark, select the **"Conversations" report**. In the top menu bar of the "Conversations" report, select **IPv4**. Select the option "**Limit to display filter**."

3) What is the IP address of the computer that you exchanged the most bytes with? ____________

a) Use a command such as "dig" or "nslookup" (in command prompt) to try to discover the name of the computer that has that address. If you find the name, enter it here. _____________

NOTE 1: You may get a response that says there were '0' answers. You may see the response includes the string 'NXDOMAIN.' This means that there was no DNS entry found that corresponded to your query.

NOTE 2: You may get a response that is not very informative, such as ord08s08-in-f16.1e100.net. You can put this into a search window in your browser and that will bring you to several sites that can provide you with the name of the owner of the host and the geographic area in which the host is found. These many services use database lookups of different location databases and other databases to produce their results. They may not be accurate.

b) How many bytes did it send to you? ______________

c) How many bytes did you send to it? _______________

4) What is the IP address of the computer that you exchanged the next most bytes with? (The second highest number of bytes) _______________

a) Use a command such as "dig" or "nslookup" to try to discover the name of the computer that has that address. If you find the name, enter it here. _______________

b) How many bytes did it send to you? _______________

c) How many bytes did you send to it? _______________

User Datagram Protocol (UDP)

In the "Statistics" menu for Wireshark, select the **" Conversations" report**. In the top menu bar of the "Conversations" report, select **UDP**. Select the option "**Limit to display filter.**"

5) How many different UDP "conversations" did your computer have? ______________

6) List the different UDP ports that are identified in the Port B column of the display.

____

(The same port may appear many times. Only list it once.)

Transmission Control Protocol (TCP)

In the "Statistics" menu for Wireshark, select the **" Conversations" report**. In the top menu bar of the "Conversations" report, select **TCP**. Select the option "**Limit to display filter.**"

7) How many TCP conversations did your computer have?

8) List the different TCP ports that are identified in the Port B column of the display.

____

(The same port may appear many times. Only list it once.)