# Wireshark Lab: Lab #2

**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?
**10.0.0.99**
2.What is the IP address of your default gateway? (See instructions below for how to find this information.) **10.0.0.1**

## PART I

### THREE WAY HANDSHAKE

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

| | | | | | | |
|---|---|---|---|---|---|---|
| 6863 | 14:35:00.637901 | 10.0.0.99 | 99.84.170.123 | TCP | 54 | 50681 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 6861 | 14:35:00.637714 | 99.84.170.123 | 10.0.0.99 | TCP | 66 | 443 → 50681 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=256 |
| 6851 | 14:35:00.622408 | 10.0.0.99 | 99.84.170.123 | TCP | 66 | 50681 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |

**First step of the handshake:**

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 7882 | 14:35:03.816966 | 52.162.166.27 | 10.0.0.99 | TCP | 60 | 443 → 50558 [ACK] Seq=3821 Ack=13227 Win=1026 Len=0 |
| 7879 | 14:35:03.813566 | 10.0.0.99 | 52.162.166.27 | TCP | 1494 | 50557 → 443 [ACK] Seq=14238 Ack=3283 Win=253 Len=1440 [TCP segment of a reassembled PD |
| 7877 | 14:35:03.806388 | 10.0.0.99 | 52.114.158.102 | TCP | 66 | 50684 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 7874 | 14:35:03.800262 | 10.0.0.99 | 52.114.142.8 | TCP | 54 | 50650 → 443 [FIN, ACK] Seq=2097 Ack=5353 Win=65536 Len=0 |

```
Sequence number: 0    (relative sequence number)
[Next sequence number: 0    (relative sequence number)]
Acknowledgment number: 0
1000 .... = Header Length: 32 bytes (8)
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]
Checksum: 0xdbd6 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
[Timestamps]
```

The TCP section of the **packet-header details window** shows that [SYN] bit is set to **1**

## Second step of the handshake:

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 7934 | 14:35:04.489476 | 23.61.181.239 | 10.0.0.99 | TCP | 56 | 443 → 50685 [ACK] Seq=1 Ack=518 Win=30336 Len=0 |
| 7932 | 14:35:04.471117 | 10.0.0.99 | 23.61.181.239 | TCP | 54 | 50685 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 |
| 7931 | 14:35:04.470847 | 23.61.181.239 | 10.0.0.99 | TCP | 66 | 443 → 50685 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 |
| 7930 | 14:35:04.455401 | 10.0.0.99 | 23.61.181.239 | TCP | 66 | 50685 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 7929 | 14:35:04.454198 | 10.0.0.99 | 104.42.223.136 | TCP | 54 | 50573 → 443 [ACK] Seq=174 Ack=996 Win=258 Len=0 |

```
Sequence number: 0    (relative sequence number)
[Next sequence number: 0    (relative sequence number)]
Acknowledgment number: 1    (relative ack number)
1000 .... = Header Length: 32 bytes (8)
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: 29200
[Calculated window size: 29200]
Checksum: 0x2c80 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale
[SEQ/ACK analysis]
```

The TCP section of the **packet-header details window** shows that [SYN, ACK] bits is set to **1**

## Third step of the handshake:

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 7930 | 14:35:04.455401 | 10.0.0.99 | 23.61.181.239 | TCP | 66 | 50685 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 7929 | 14:35:04.454198 | 10.0.0.99 | 104.42.223.136 | TCP | 54 | 50573 → 443 [ACK] Seq=174 Ack=996 Win=258 Len=0 |
| 7924 | 14:35:04.427366 | 10.0.0.99 | 52.163.217.227 | TCP | 54 | 50567 → 443 [FIN, ACK] Seq=2 Ack=1 Win=258 Len=0 |
| 7922 | 14:35:04.191404 | 10.0.0.99 | 52.162.166.27 | TCP | 54 | 50556 → 443 [ACK] Seq=6023 Ack=1823 Win=258 Len=0 |

```
Sequence number: 174    (relative sequence number)
[Next sequence number: 174    (relative sequence number)]
Acknowledgment number: 996    (relative ack number)
0101 .... = Header Length: 20 bytes (5)
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: 258
[Calculated window size: 258]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x6a3d [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

The TCP section of the **packet-header details window** shows that [ACK] bits is set to **1.**

## 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 == **10.0.0.99**

ip.addr==10.0.0.99 Expression...

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 303 | 14:34:22.583045 | 10.0.0.99 | 13.107.3.128 | TCP | 55 | 50518 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU] |
| 306 | 14:34:22.590962 | 10.0.0.99 | 52.179.199.114 | TCP | 55 | 50566 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU] |
| 312 | 14:34:22.602575 | 13.107.3.128 | 10.0.0.99 | TCP | 66 | 443 → 50518 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2 |
| 350 | 14:34:22.628519 | 52.179.199.114 | 10.0.0.99 | TCP | 66 | 443 → 50566 [ACK] Seq=1 Ack=2 Win=1025 Len=0 SLE=1 SRE=2 |
| 419 | 14:34:22.863101 | 10.0.0.99 | 52.177.203.97 | TCP | 55 | 50578 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU] |
| 420 | 14:34:22.900099 | 52.177.203.97 | 10.0.0.99 | TCP | 66 | 443 → 50578 [ACK] Seq=1 Ack=2 Win=1022 Len=0 SLE=1 SRE=2 |
| 422 | 14:34:23.323168 | 10.0.0.99 | 13.68.117.223 | TCP | 55 | 50521 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU] |
| 423 | 14:34:23.360906 | 13.68.117.223 | 10.0.0.99 | TCP | 66 | 443 → 50521 [ACK] Seq=1 Ack=2 Win=1026 Len=0 SLE=1 SRE=2 |
| 424 | 14:34:23.834874 | 10.0.0.99 | 52.162.166.27 | TCP | 55 | 51882 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU] |
| 425 | 14:34:23.850304 | 52.162.166.27 | 10.0.0.99 | TCP | 66 | 443 → 51882 [ACK] Seq=1 Ack=2 Win=1026 Len=0 SLE=1 SRE=2 |
| 426 | 14:34:24.952983 | 10.0.0.99 | 40.83.21.197 | TLSv… | 110 | Application Data |
| 427 | 14:34:24.979820 | 40.83.21.197 | 10.0.0.99 | TLSv… | 99 | Application Data |
| 428 | 14:34:25.030605 | 10.0.0.99 | 40.83.21.197 | TCP | 54 | 50547 → 443 [ACK] Seq=57 Ack=46 Win=255 Len=0 |
| 429 | 14:34:25.358669 | 10.0.0.99 | 54.209.137.253 | TCP | 55 | 50455 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1 [TCP segment of a reassembled PDU] |
| 430 | 14:34:25.395685 | 54.209.137.253 | 10.0.0.99 | TCP | 66 | 443 → 50455 [ACK] Seq=1 Ack=2 Win=121 Len=0 SLE=1 SRE=2 |
| 433 | 14:34:25.684771 | 10.0.0.99 | 52.163.217.227 | TCP | 55 | 50567 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU] |
| 434 | 14:34:25.905490 | 52.163.217.227 | 10.0.0.99 | TCP | 66 | 443 → 50567 [ACK] Seq=1 Ack=2 Win=1026 Len=0 SLE=1 SRE=2 |
| 443 | 14:34:27.032850 | 10.0.0.99 | 104.46.97.118 | TCP | 55 | 50550 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a reassembled PDU] |
| 444 | 14:34:27.070964 | 104.46.97.118 | 10.0.0.99 | TCP | 66 | 443 → 50550 [ACK] Seq=1 Ack=2 Win=1025 Len=0 SLE=1 SRE=2 |
| 445 | 14:34:27.819773 | 13.107.4.52 | 10.0.0.99 | TCP | 56 | 80 → 50543 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 446 | 14:34:28.871632 | 10.0.0.99 | 52.162.166.27 | TCP | 55 | 50557 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU] |
| 447 | 14:34:28.886208 | 52.162.166.27 | 10.0.0.99 | TCP | 66 | 443 → 50557 [ACK] Seq=1 Ack=2 Win=1026 Len=0 SLE=1 SRE=2 |
| 452 | 14:34:32.675142 | 10.0.0.99 | 52.162.166.27 | TCP | 55 | 49860 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU] |
| 453 | 14:34:33.155770 | 10.0.0.99 | 52.162.166.27 | TLSv… | 1494 | Ignored Unknown Record |
| 454 | 14:34:33.155771 | 10.0.0.99 | 52.162.166.27 | TLSv… | 1170 | Ignored Unknown Record |
| 455 | 14:34:33.162434 | 10.0.0.99 | 52.114.158.102 | TCP | 54 | 50551 → 443 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0 |

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.)

**DNS, TCP, TLSv1.3, TLSv1.2, UDP, STUN, ARP, ICMPv6**

## Internet Protocol (IP)

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

**10.0.0.54**

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

**Default Server: cdns01.comcast.net**

**Address: 2001:558:feed::1**

```
C:\Users\javeria>nslookup 10.0.0.54
Server:  cdns01.comcast.net
Address:  2001:558:feed::1
```

b. How many bytes did it send to you?

**2256K**

c. How many bytes did you send to it?

**2079K**

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

**52.162.166.27**

a. Use a command such as “dig” or “nslookup” to try to discover the name of the computer that has that address.

**Default Server: cdns01.comcast.net**

**Address: 2001:558:feed::1**

**c.** How many bytes did it send to you?

**30K**

d. How many bytes did you send to it?

**109K**

## User Datagram Protocol (UDP)

5. How many different UDP “conversations” did your computer have?

**8 UDP conversations.**

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

**5353, 3330, 3478, 3725, 161, 1900, 53, 443.**

## Transmission Control Protocol (TCP)

7. How many TCP conversations did your computer have?

**3 TCP conversations**

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

**443, 80, 5228**