1. Install Wireshark and WinPcap.

a) Double-click the **Wireshark-win64-2.0.1.exe** file to open the installer.

b) If necessary, Select **Yes** in the **User Account Control** message box.

c) In the **Wireshark 2.0.1 (64-bit) Setup** wizard, select **Next**.

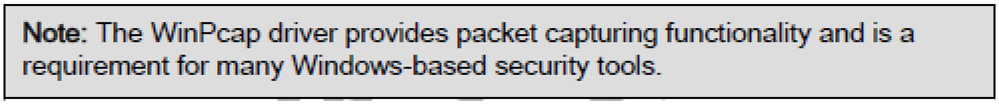
d) On the **License Agreement** page, select **I Agree**.

e) On the **Choose Components** page, accept the defaults by selecting **Next**.

f) On the **Select Additional Tasks** page, check the Wireshark Desktop Icon check box and select **Next**.

g) On the **Choose Install Location** page, accept the default location by selecting **Next**.

h) On the **Install WinPcap?** Page, verify that the **Install WinPcap 4.1.3** check box is checked and select **Next**.



Note: The WinPcap driver provides packet capturing functionality and is a requirement for many Windows-based security tools.

i) On the **Install USBPcap?** page, verify the check box is unchecked, then select **Install**.

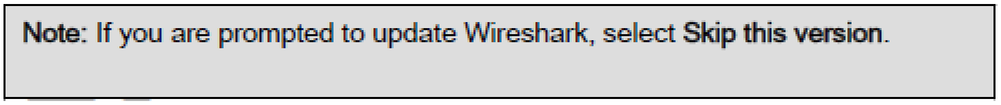
j) In the **WinPcap 4.1.3 Setup** wizard, select **Next**.

k) Agree to the license terms, then select **Install**.

l) Select **Finish** to close this installation wizard and return to Wireshark.

m) After Wireshark finishes installing, select **Next**.

n) Check the **Run Wireshark 2.0.1 (64-bit)** check box and select **Finish**.

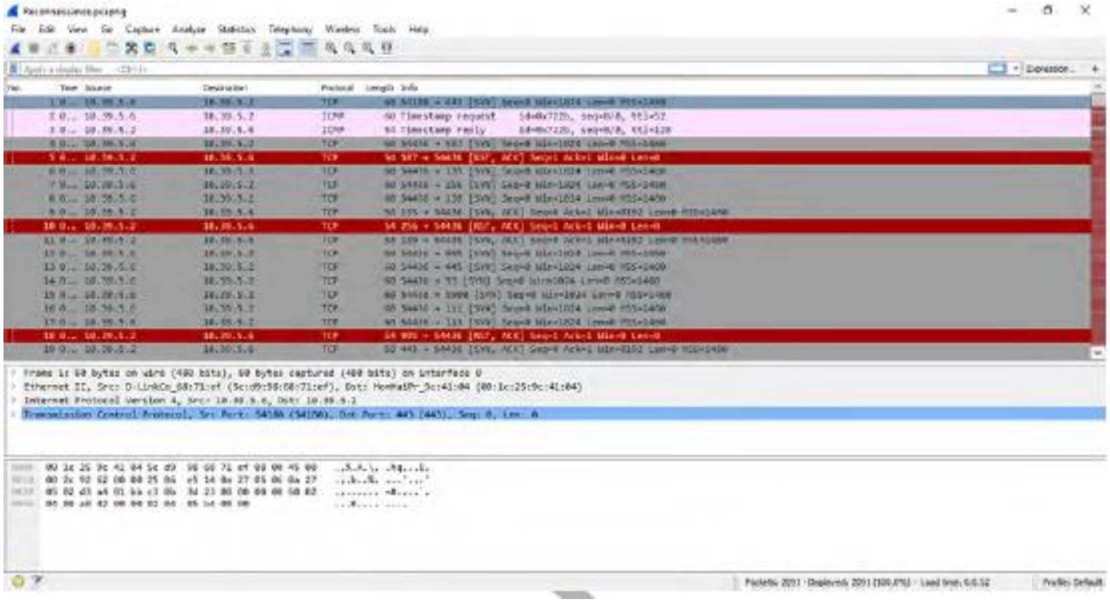


Note: If you are prompted to update Wireshark, select **Skip this version**.

2. Acquaint yourself with Wireshark's Interface.

a) In **The Wireshark Network Analyzer** window, select **File > Open** and navigate to the **Reconnaissance.pcapng** file. Double-click the **Reconnaissance.pcapng** file to open it in Wireshark.

b) If necessary, drag the middle pane down to see a display similar to the one shown here.



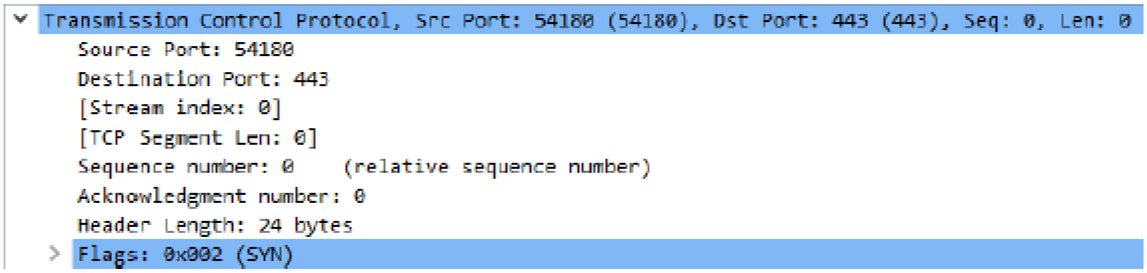
```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: D-LinkCo_68:71:ef (5c:d9:98:68:71:ef), Dst: HonHaiPr_9c:41:04 (00:1c:25:9c:41:04)
Internet Protocol Version 4, Src: 10.39.5.6, Dst: 10.39.5.2
Transmission Control Protocol, Src Port: 54180 (54180), Dst Port: 443 (443), Seq: 0, Len: 0
```

c) Observe the three Wireshark panes.

- The top pane contains a list of every packet captured in that session and some summary information about each one. The packet selected is the one you are looking at in the bottom two sections. (in this case, packet 1 is selected)
- The bottom pane displays a hexadecimal readout of the contents of the selected packet with 16bytes in each line. If you know your internet headers very well, you can discover the contents of the traffic from this area alone.
- Fortunately, the middle pane provides a field-by-field interpretation of everything that the bottom window displays.

d) In the top pane, select **packet 1**, if necessary.

4. In the middle pane, expand the **Transmission Control Protocol** section by selecting the right arrow. Note the source and destination port numbers and the flags field.



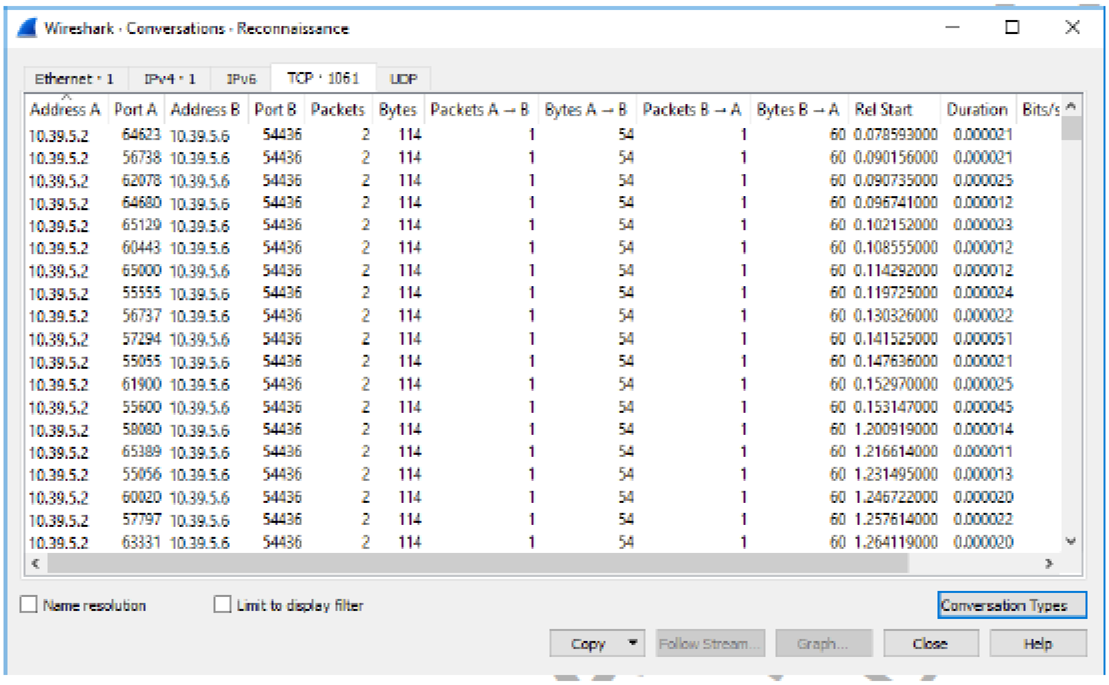
```
Transmission Control Protocol, Src Port: 54180 (54180), Dst Port: 443 (443), Seq: 0, Len: 0
    Source Port: 54180
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 24 bytes
  > Flags: 0x002 (SYN)
```

> **Note:** The port numbers and flags are also displayed in the **Info** column in the top pane. (The flags are indicated in brackets.)

5. Analyze the capture file to find the attack(s).

a) From the menu, select **Statistics > Conversations**.

b) If necessary, select **TCP** tab.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s
10.39.5.2	64623	10.39.5.6	54436	2	114	1	54	1	60	0.078593000	0.000021	
10.39.5.2	56738	10.39.5.6	54436	2	114	1	54	1	60	0.090156000	0.000021	
10.39.5.2	62078	10.39.5.6	54436	2	114	1	54	1	60	0.090735000	0.000025	
10.39.5.2	64680	10.39.5.6	54436	2	114	1	54	1	60	0.096741000	0.000012	
10.39.5.2	65129	10.39.5.6	54436	2	114	1	54	1	60	0.102152000	0.000023	
10.39.5.2	60443	10.39.5.6	54436	2	114	1	54	1	60	0.108555000	0.000012	
10.39.5.2	65000	10.39.5.6	54436	2	114	1	54	1	60	0.114292000	0.000012	
10.39.5.2	55555	10.39.5.6	54436	2	114	1	54	1	60	0.119725000	0.000024	
10.39.5.2	56737	10.39.5.6	54436	2	114	1	54	1	60	0.130326000	0.000022	
10.39.5.2	57294	10.39.5.6	54436	2	114	1	54	1	60	0.141525000	0.000051	
10.39.5.2	55055	10.39.5.6	54436	2	114	1	54	1	60	0.147636000	0.000021	
10.39.5.2	61900	10.39.5.6	54436	2	114	1	54	1	60	0.152970000	0.000025	
10.39.5.2	55600	10.39.5.6	54436	2	114	1	54	1	60	0.153147000	0.000045	
10.39.5.2	58080	10.39.5.6	54436	2	114	1	54	1	60	1.200919000	0.000014	
10.39.5.2	65389	10.39.5.6	54436	2	114	1	54	1	60	1.216614000	0.000011	
10.39.5.2	55056	10.39.5.6	54436	2	114	1	54	1	60	1.231495000	0.000013	
10.39.5.2	60020	10.39.5.6	54436	2	114	1	54	1	60	1.246722000	0.000020	
10.39.5.2	57797	10.39.5.6	54436	2	114	1	54	1	60	1.257614000	0.000022	
10.39.5.2	63331	10.39.5.6	54436	2	114	1	54	1	60	1.264119000	0.000020	

☐ Name resolution ☐ Limit to display filter

c) Select the **Packets** heading to sort the list by number of packets.

d) Scroll through the list of conversations. Note that there are many one-packet sessions and a few three-packet sessions.

e) Note the various destination port numbers (**Port B**).

f) Select the **Close** button to close the **Conversations** window.

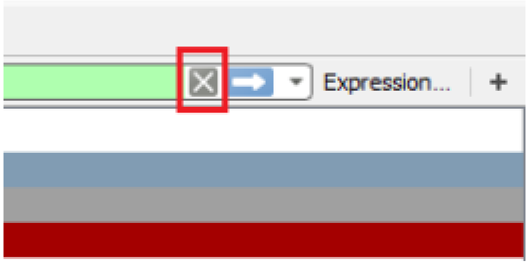
6. Follow the TCP stream for packet **1**.

a) Right-click **Packet 1** and select **Follow > TCP Stream** from the menu to look at just one session.

b) Close the **Follow TCP Stream** window. If there were data in the session, you would see it, but there isn't any in this case.

7. Clear the filter and examine packet **42**.

a) At the top-right of the window



b) Select packet **42**.

8. Close Wireshark application.