

# IMMERSIVE LEARNING ENVIRONMENT

## LAB: THREE-WAY HANDSHAKE LAB

### INSTRUCTIONS



Client Machine



Remote Server

Three-way handshake is a method, which is used to establish a connection between local host/client and server. It is a three-step method in which both client and server exchange SYN and ACK packets before actual data communication begins.

#### **STEP 1: Establish a TCP session between client and remote server**

Open a web browser on your Linux virtual machine. Select the Firefox web browser icon from quick lunch bar on left side of your screen.

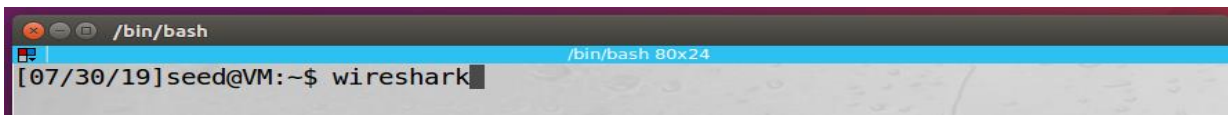
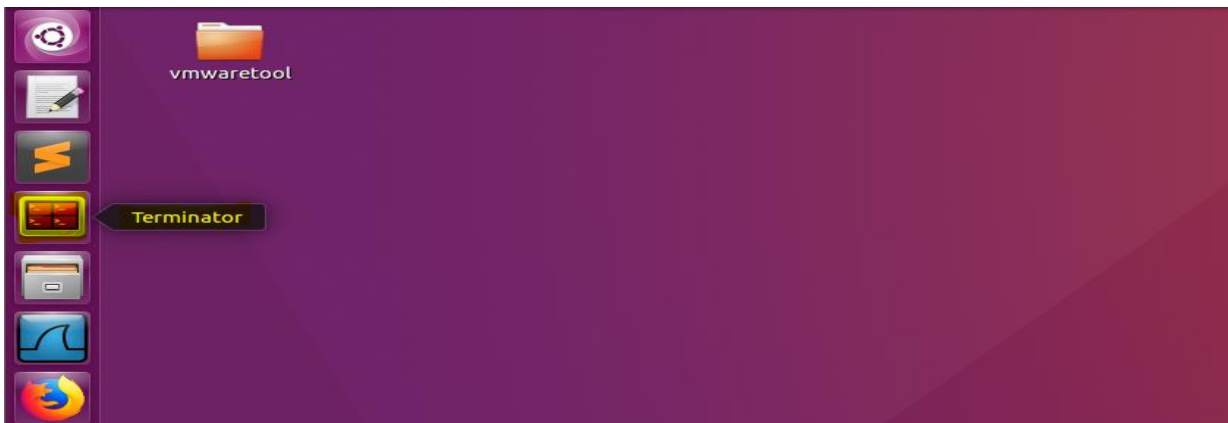
NOTE: Make sure your virtual machine is connected to an internet.



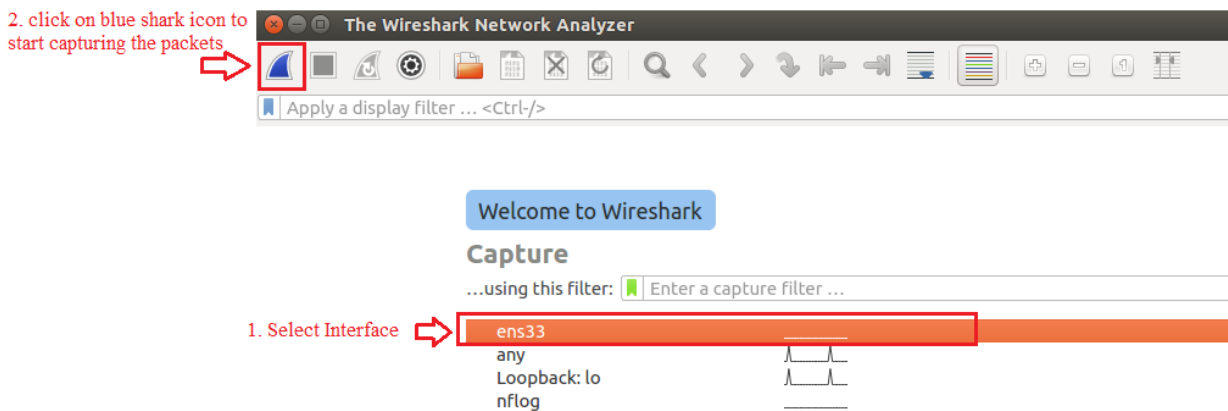
Now let's open Wireshark on our virtual machine from quick lunch bar or open terminal and type wireshark and hit enter on your terminal.



OR

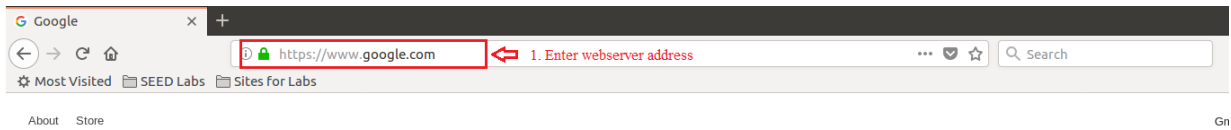


Select your virtual machine physical interface from Wireshark home screen. Most of the case it is usually first interface option on your Wireshark home screen.



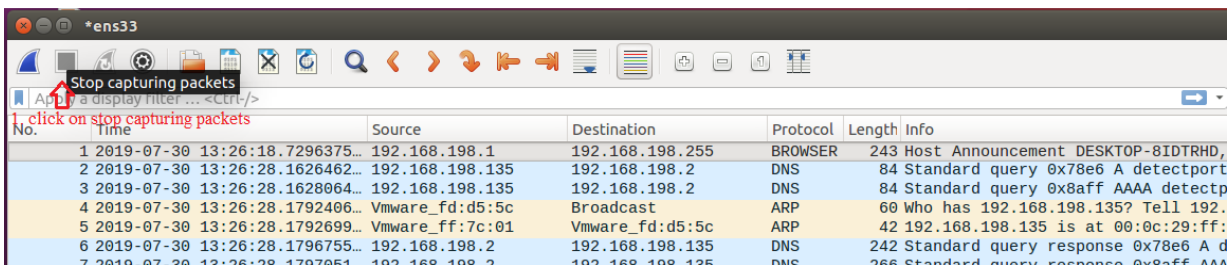
After selecting the interface from the Wireshark home screen click on blue shark icon on your Wireshark home screen.

Now let's enter web address on our Firefox web browser web address field and open the website.



## STEP 2: Analyze the captured packet on Wireshark

Once we have successfully opened the web address on our Firefox web browser. Let get back to our Wireshark active packet capture windows and stop capturing the packets.



Click on stop capturing packets icon on top of your Wireshark menu icon next to blue icon.

let's analyze the captured packets on Wireshark. You will notice a lot of packets.

Enter TCP on filter column below the menu icon and hit enter. The packets will be selected based on the filter option which makes easy to search capture packets. Lets focused on TCP protocol packets and observe the TCP packets follow. You will notice TCP SYN , SYN ACK and ACK packets stream with identical source and destination IP address associated with specific Destination port request. In our case it web request port 80. Find the detail on screenshot below.



1. Enter tcp

2. Observe the TCP packets

3. TCP Three-Way Handshake Packets

No.	Time	Source	Destination	Protoc	Length	Info
7053	2019-07-30 13:26:45.3253961	192.168.198.135	172.217.6.3	OCSP	495	Request
7063	2019-07-30 13:26:45.5045125	172.217.6.3	192.168.198.135	OCSP	755	Response
7199	2019-07-30 13:26:45.8190319	192.168.198.135	172.217.6.3	OCSP	495	Request
7212	2019-07-30 13:26:45.9969881	172.217.6.3	192.168.198.135	OCSP	755	Response
8	2019-07-30 13:26:28.1847797	192.168.198.135	149.165.180.17	TCP	74	37586 → 80 [SYN] Seq=721173754 Win=29200 Len=0 MSS=1460 SACK_PERM=0
9	2019-07-30 13:26:28.1936630	149.165.180.17	192.168.198.135	TCP	60	80 → 37586 [SYN, ACK] Seq=1650358064 Ack=721173755 Win=64240 Len=0
10	2019-07-30 13:26:28.1936546	192.168.198.135	149.165.180.17	TCP	54	37586 → 80 [ACK] Seq=721173755 Ack=1650358065 Win=29200 Len=0
12	2019-07-30 13:26:28.1942933	149.165.180.17	192.168.198.135	TCP	60	80 → 37586 [ACK] Seq=1650358065 Ack=721174049 Win=64240 Len=0
14	2019-07-30 13:26:28.2028198	192.168.198.135	149.165.180.17	TCP	54	37586 → 80 [ACK] Seq=721174049 Ack=1650358069 Win=36916 Len=0
19	2019-07-30 13:26:31.1932455	192.168.198.135	128.230.247.70	TCP	74	33306 → 80 [SYN] Seq=771871999 Win=29200 Len=0 MSS=1460 SACK_PERM=0
20	2019-07-30 13:26:31.2231481	128.230.247.70	192.168.198.135	TCP	60	80 → 33306 [SYN, ACK] Seq=1289766779 Ack=771872000 Win=64240 Len=0
21	2019-07-30 13:26:31.2232265	192.168.198.135	128.230.247.70	TCP	54	33306 → 80 [ACK] Seq=771872000 Ack=1289766780 Win=29200 Len=0
23	2019-07-30 13:26:31.7959602	128.230.247.70	192.168.198.135	TCP	60	80 → 33306 [ACK] Seq=1289766780 Ack=771872332 Win=64240 Len=0

Transmission Control Protocol, Src Port: 37586, Dst Port: 80, Seq: 721173754, Len: 0

Source Port: 37586  
 Destination Port: 80  
 [Stream index: 0]  
 [TCP Segment Len: 0]  
 Sequence number: 721173754  
 Acknowledgment number: 0  
 Header Length: 40 bytes  
 Flags: 0x002 (SYN)  
 Window size value: 29200

## WHAT TO SUBMIT

Submit your work with detailed screenshots.

