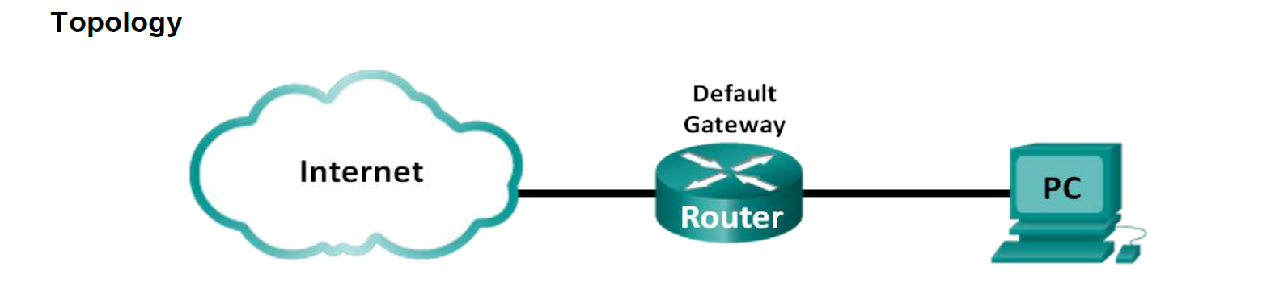
****

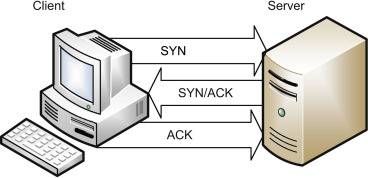
**Department of Information Science and Engineering**

DATA COMMUNICATION AND NETWORKING LAB-16IS5DCDCN

(2019-20)

1. Demo of TCP three way handshaking using wire shark.





Before the sending device and the receiving device start the exchange of data, both devices need to be synchronized. During the [TCP](http://www.omnisecu.com/tcpip/transmission-control-protocol-tcp.php) initialization process, the sending device and the receiving device exchange a few control packets for synchronization purposes. This exchange is known as Three-way handshake.

**TCP Three-way Handshake**

Step 1. Device A (Client) sends a [TCP segment](http://www.omnisecu.com/tcpip/tcp-header.php) with SYN = 0,

An Initial Sequence Number (ISN) is a random [Sequence Number](http://www.omnisecu.com/tcpip/tcp-header.php), allocated for the first packet in a new TCP connection.

The Active Open device (Device A) sends a segment with the[SYN flag](http://www.omnisecu.com/tcpip/tcp-header.php) set to 0 ,  [SYN](http://www.omnisecu.com/tcpip/tcp-header.php) is short for SYNchronize. [SYN flag](http://www.omnisecu.com/tcpip/tcp-header.php) announces an attempt to open a connection.

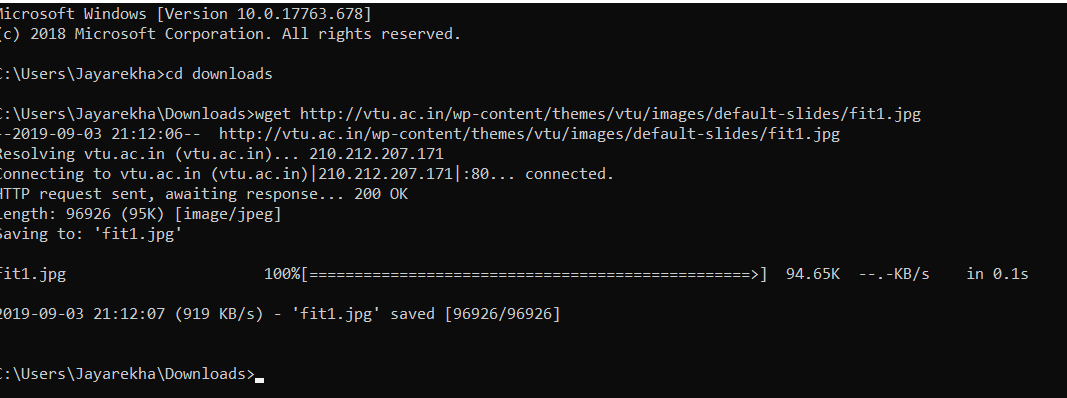
Step 2. Device B (Server) receives Device A's [TCP segment](http://www.omnisecu.com/tcpip/tcp-header.php) and returns a [TCP segment](http://www.omnisecu.com/tcpip/tcp-header.php) with SYN = 0, ACK = 1,

Step 3. Device A sends a [TCP segment](http://www.omnisecu.com/tcpip/tcp-header.php) to Device B that acknowledges receipt of Device B, With flags set as SYN = 01 ACK = 1, This handshaking technique is referred to as TCP Three-way handshake or SYN, SYN-ACK, ACK.

After the Three-way handshake, the connection is open and the participant computers start sending data using the agreed [sequence and acknowledge numbers](http://www.omnisecu.com/tcpip/tcp-header.php).

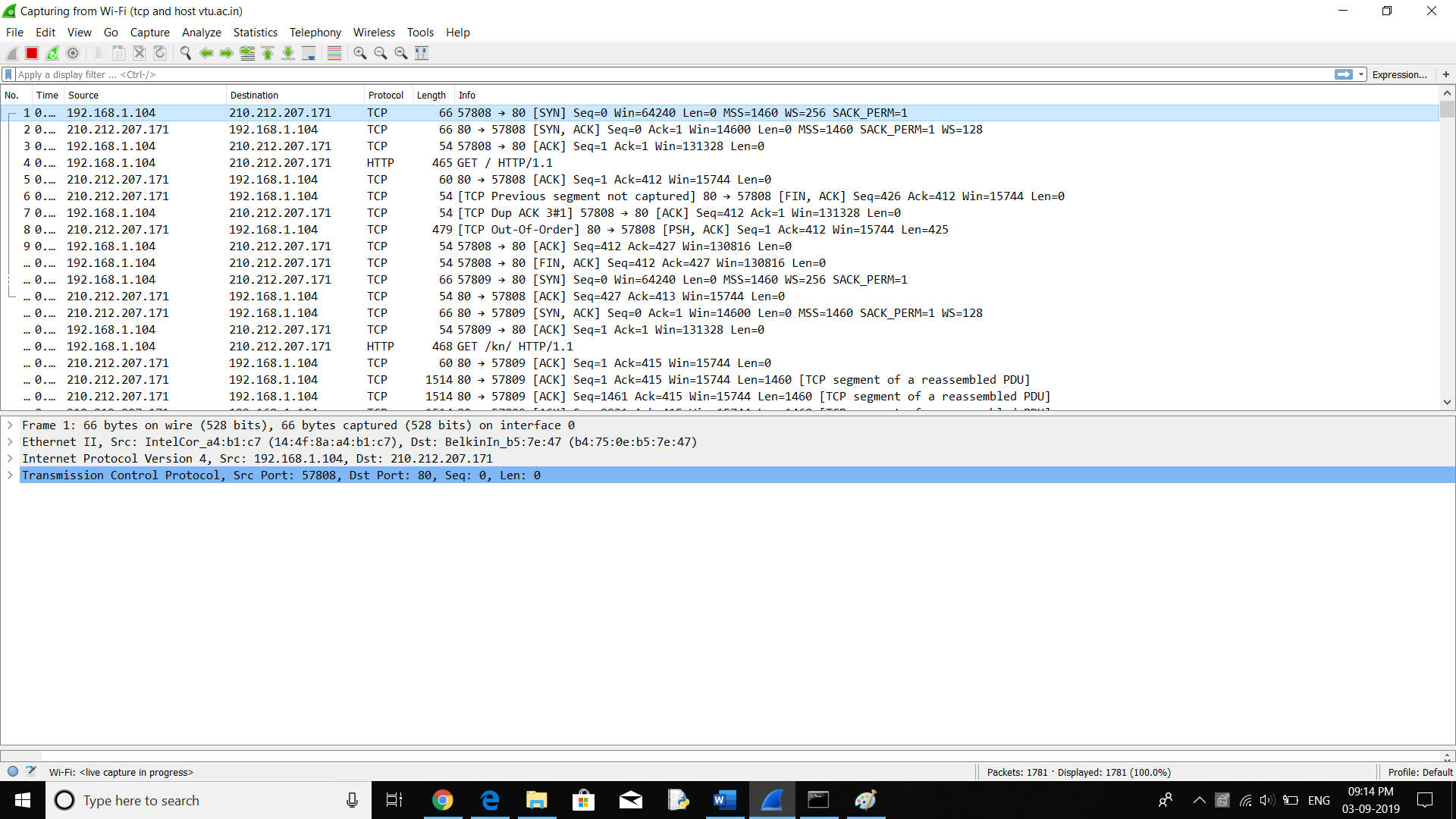
Before Starting the wireshark follow the steps

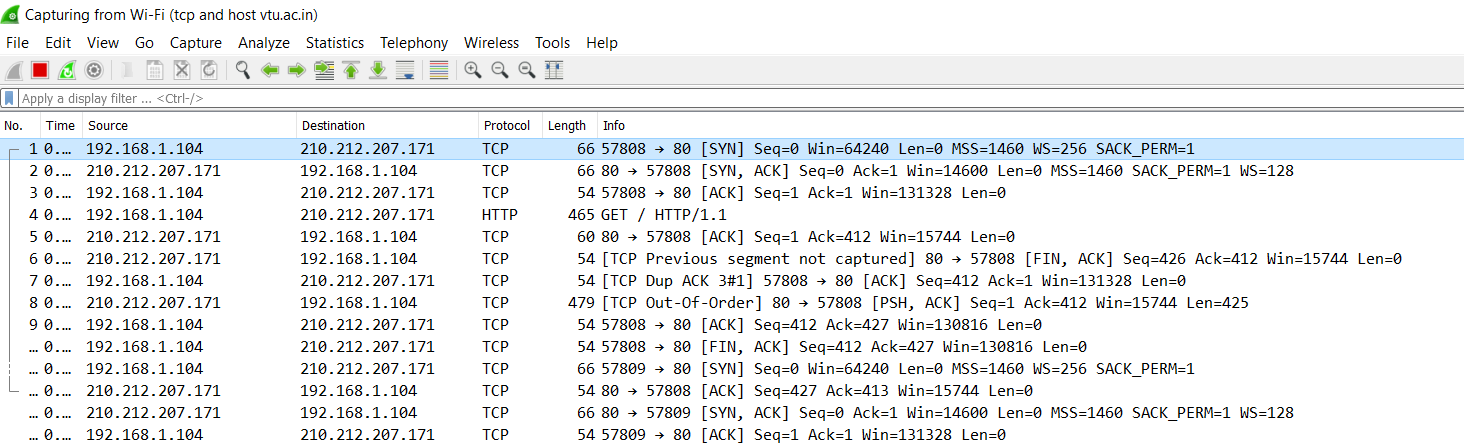
1. Download wget https://kevincurran.org/com320/labs/wget.exe
2. open vtu.ac.in , copy the link of any image to wget and download the image from the command prompt.



1. Launch Wireshark and start a capture with a filter of “tcp and host xx.xx.xx”, where xx.xx.xx is the name of the remote server from which you will fetch content for example it is vtu.ac.in

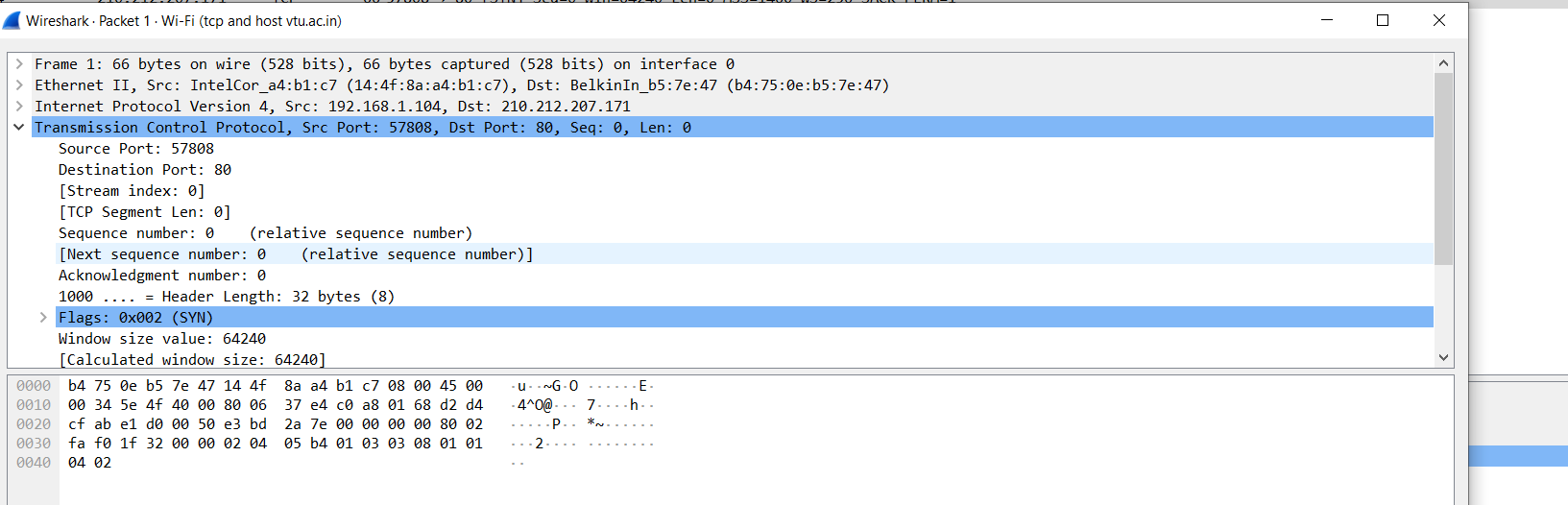
After the capture is started, repeat the wget command above. This time, the packets will also be recorded by Wireshark

1. 

4.

First three Statements are for the Three way handshaking.

The laptops port Number is 57808 and http server port number is 80.



Select a long packet anywhere in the middle of your trace whose protocol is listed as TCP. Expand the TCP protocol section in the middle panel (by using the “+” expander or icon). All packets except the initial HTTP GET and last packet of the HTTP response should be listed as TCP. Picking a long packet ensures that we are looking at a download packet from the server to your computer. Looking at the protocol layers, you should see an IP block before the TCP block. This is because the TCP segment is carried in an IP. We have shown the TCP block expanded in our figure.

You will see roughly the following fields:

• First comes the source port, then the destination port. This is the addressing that TCP adds beyond the IP address. The source port is likely to be 80 since the packet was sent by a web server and the standard web server port is 80.

• Then there is the sequence number field. It gives the position in the bytestream of the first payload byte.

• Next is the acknowledgement field. It tells the last received position in the reverse byte stream.

• The header length giving the length of the TCP header.

• The flags field has multiple flag bits to indicate the type of TCP segment. You can expand it and look at the possible flags.

• Next is a checksum, to detect transmission errors.

• There may be an Options field with various options. You can expand this field and explore if you would like, but we will look at the options in more detail later.

• Finally, there may be a TCP payload, carrying the bytes that are being transported.

Connection Tear Down

