

Computer Network

MCA Code 163

Lab Activity

Objective: To observe the exchange of messages between various protocols, capturing and analysing it.

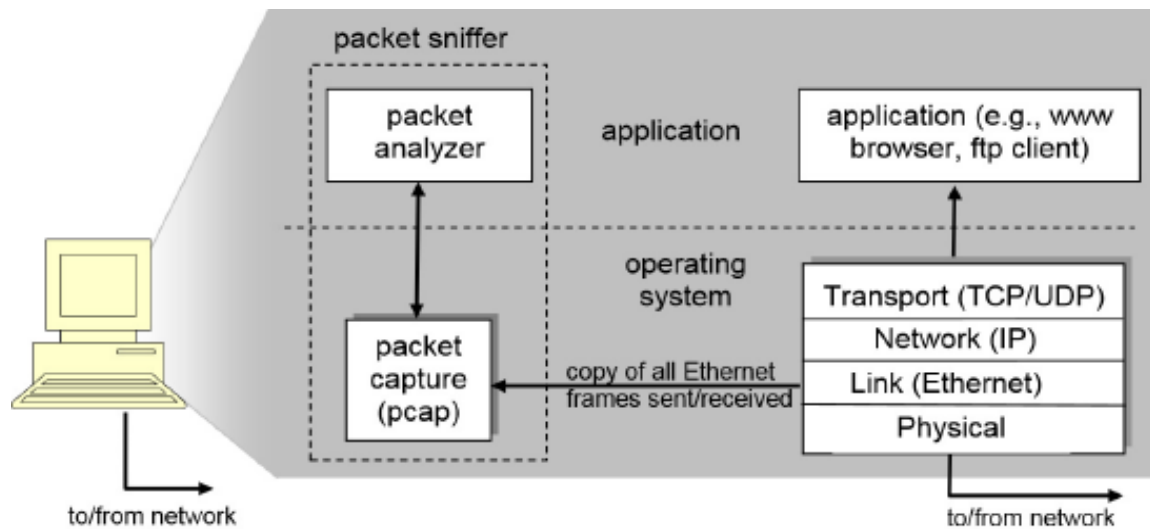
Tool Used: Wireshark

Introduction:

1. Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.
2. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable.
3. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.
4. Wireshark is used for
 - Network administrators use it to *troubleshoot network problems*
 - Network security engineers use it to *examine security problems*
 - QA engineers use it to *verify network applications*
 - Developers use it to *debug protocol implementations*
 - People use it to *learn network protocol* internals
5. Example of Packet Sniffing- The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**.

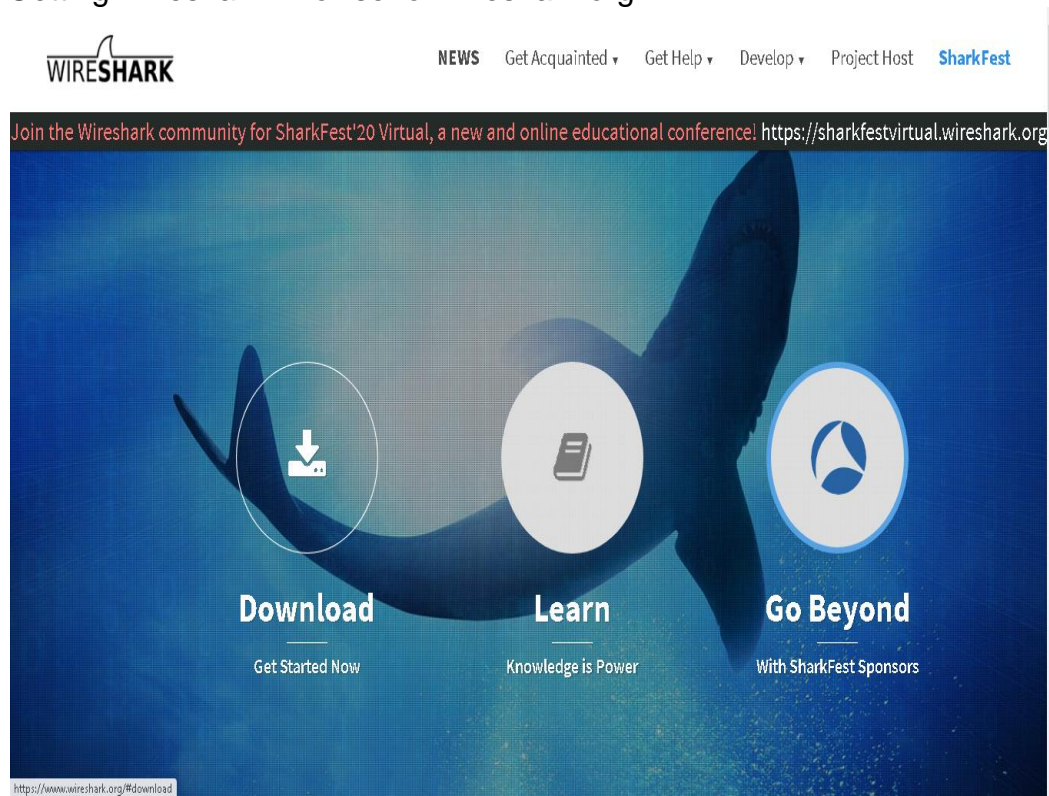
The packet sniffer consists of 2 parts:

- The **packet capture** library receives a copy of every link layer frame that is sent from or received by your computer.
- The **packet analyzer** which displays the contents of all fields within a protocol message.

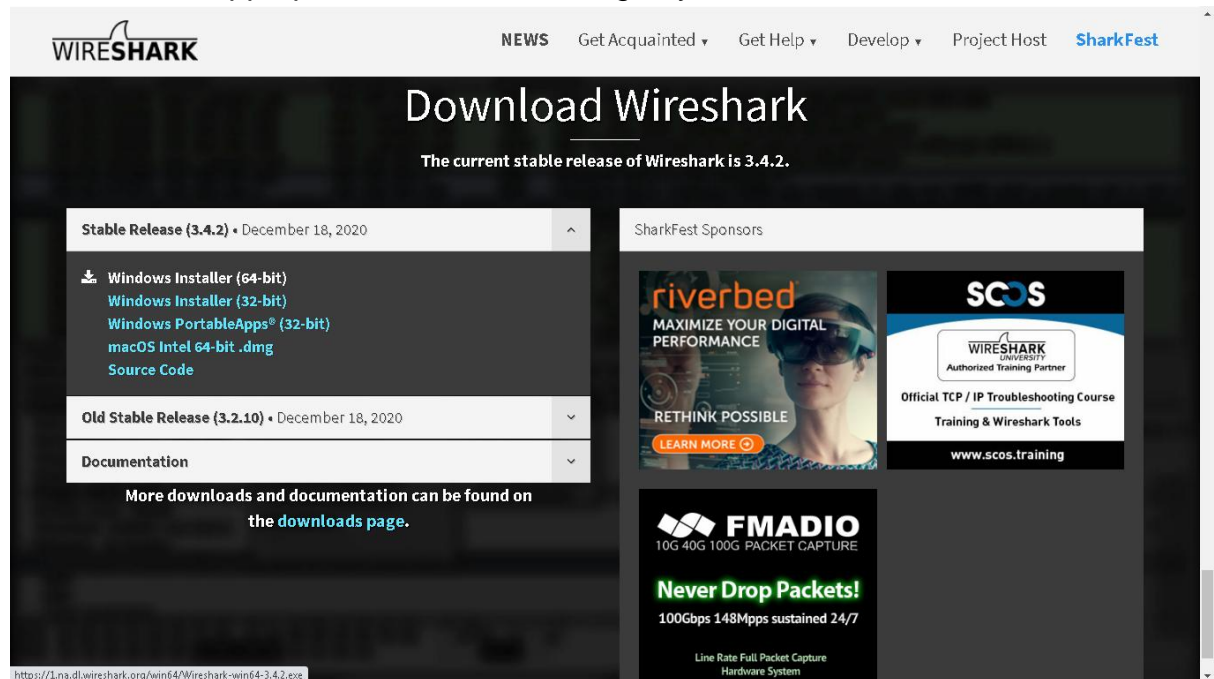


6. Steps to analyze Network Packets:

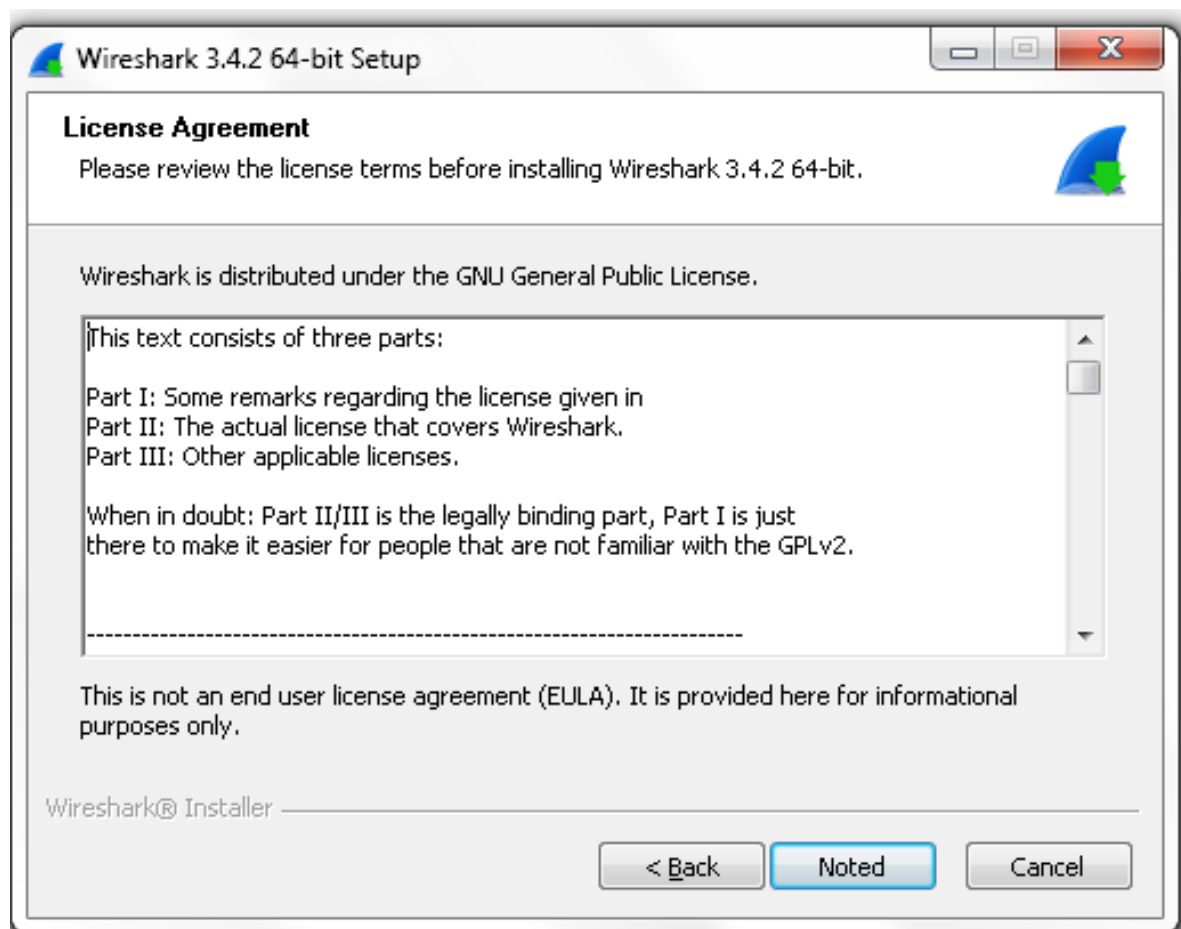
a. Getting Wireshark: Browse for wireshark.org

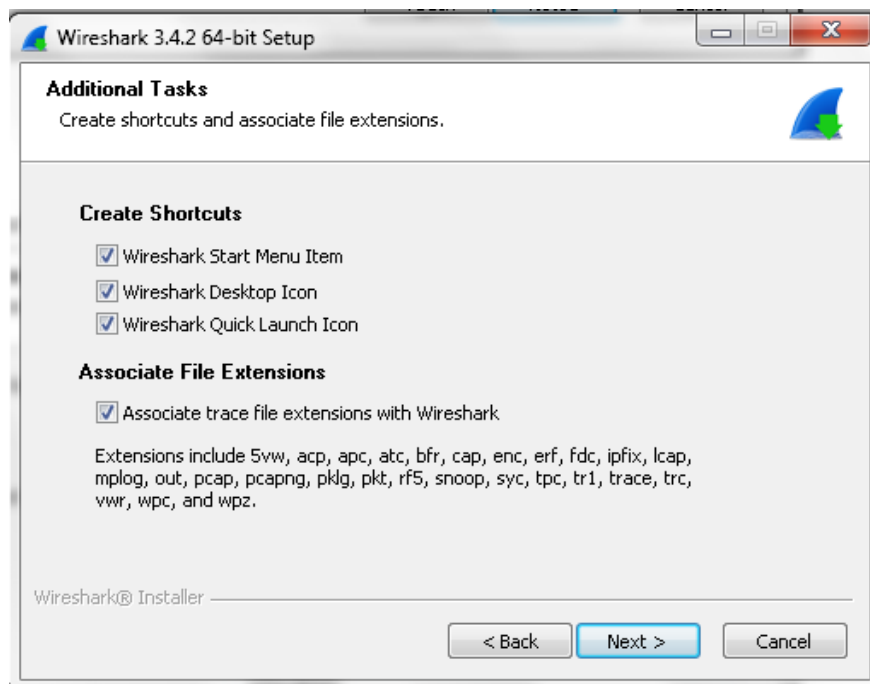
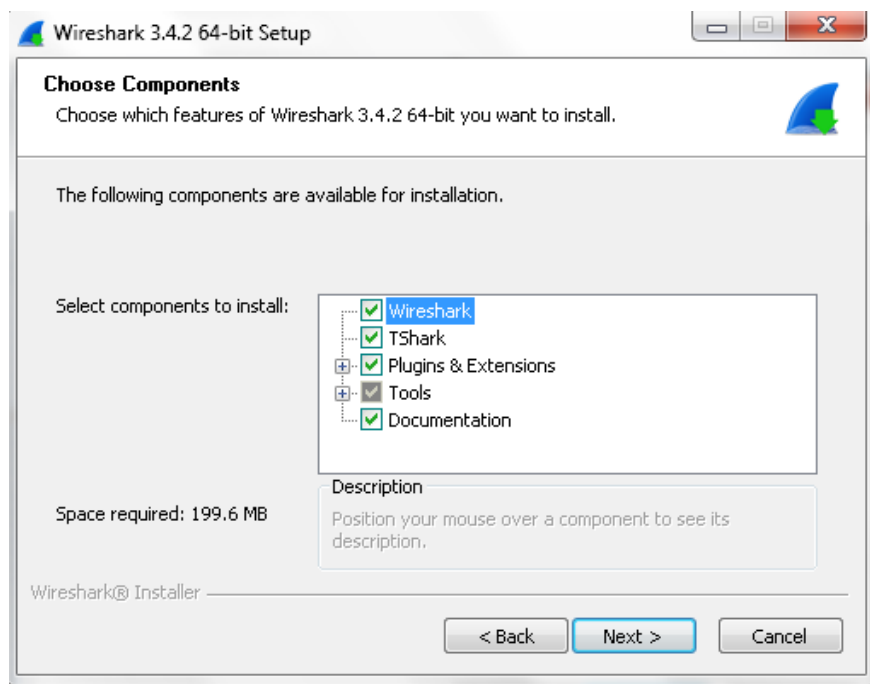


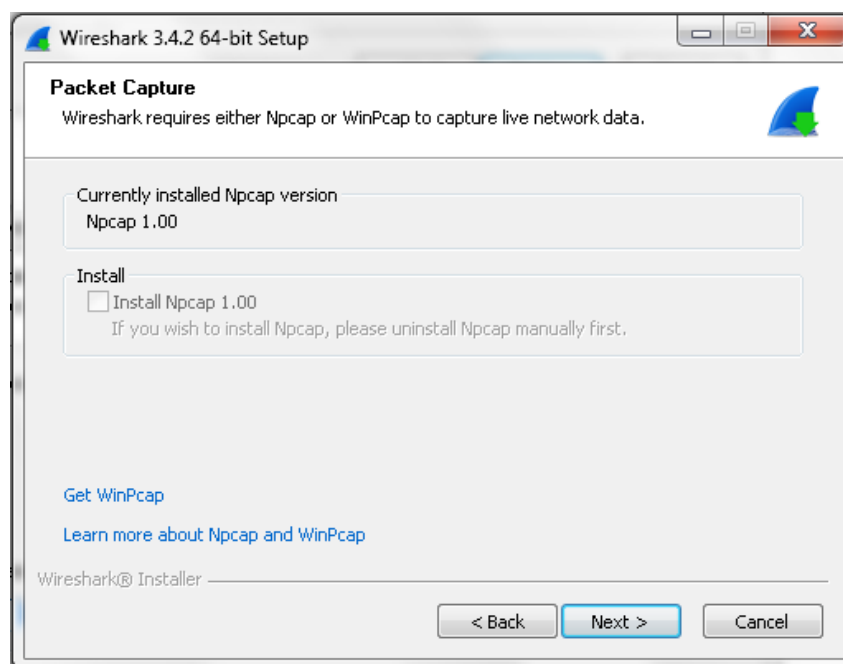
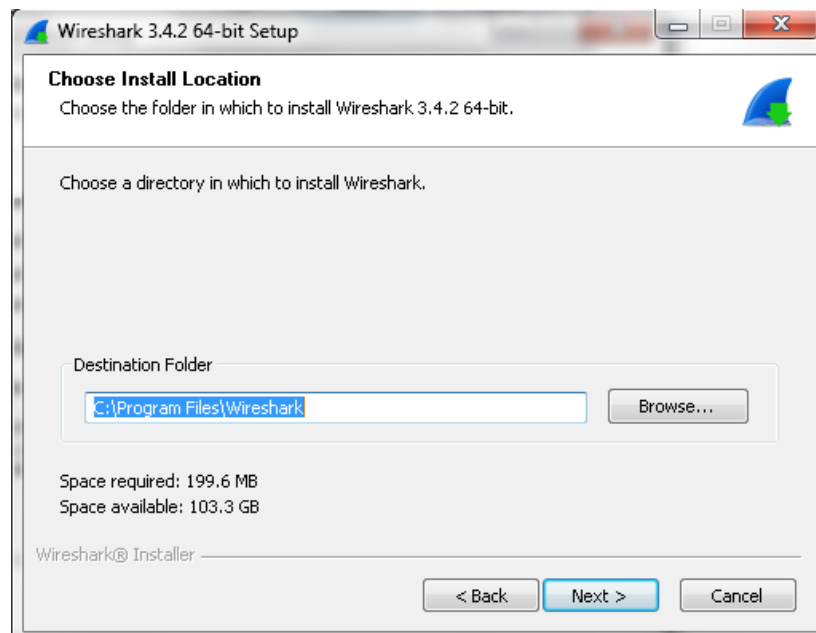
- b. Download the appropriate version according to your OS.

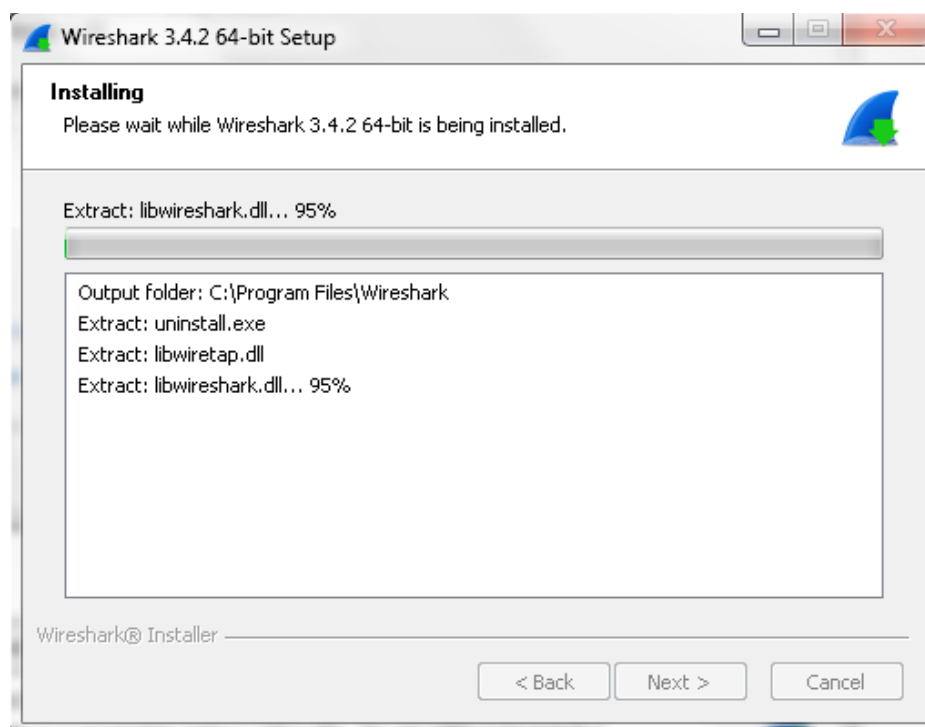
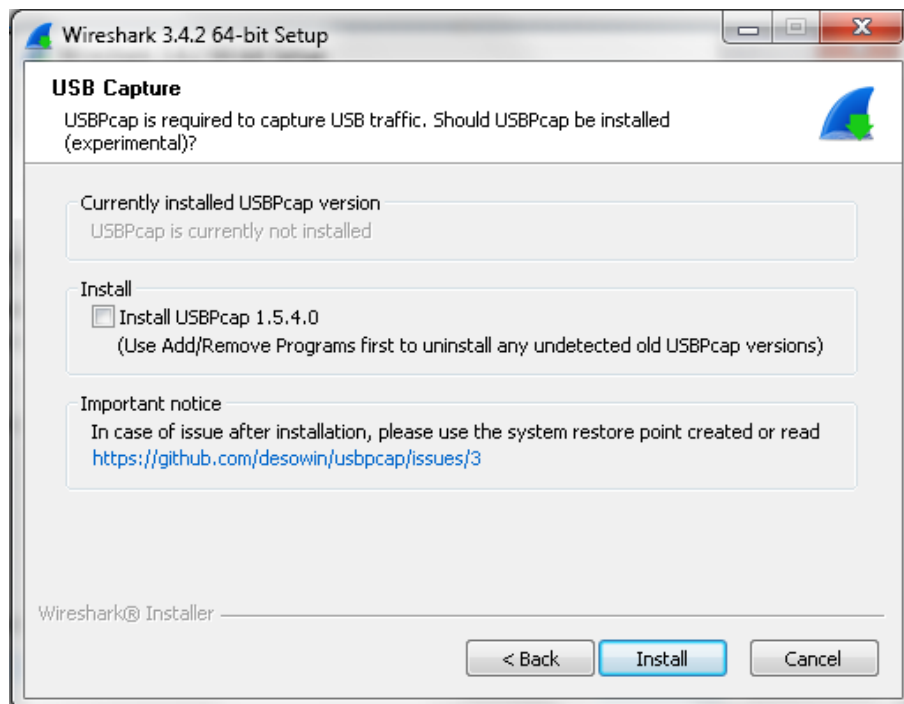


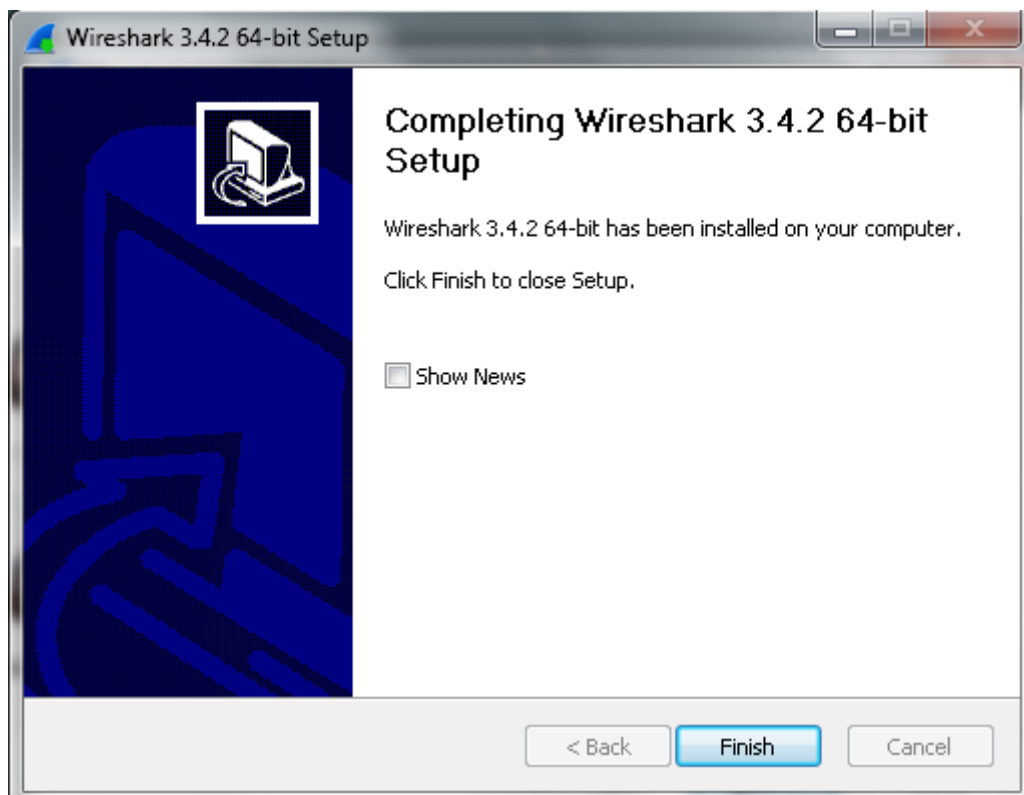
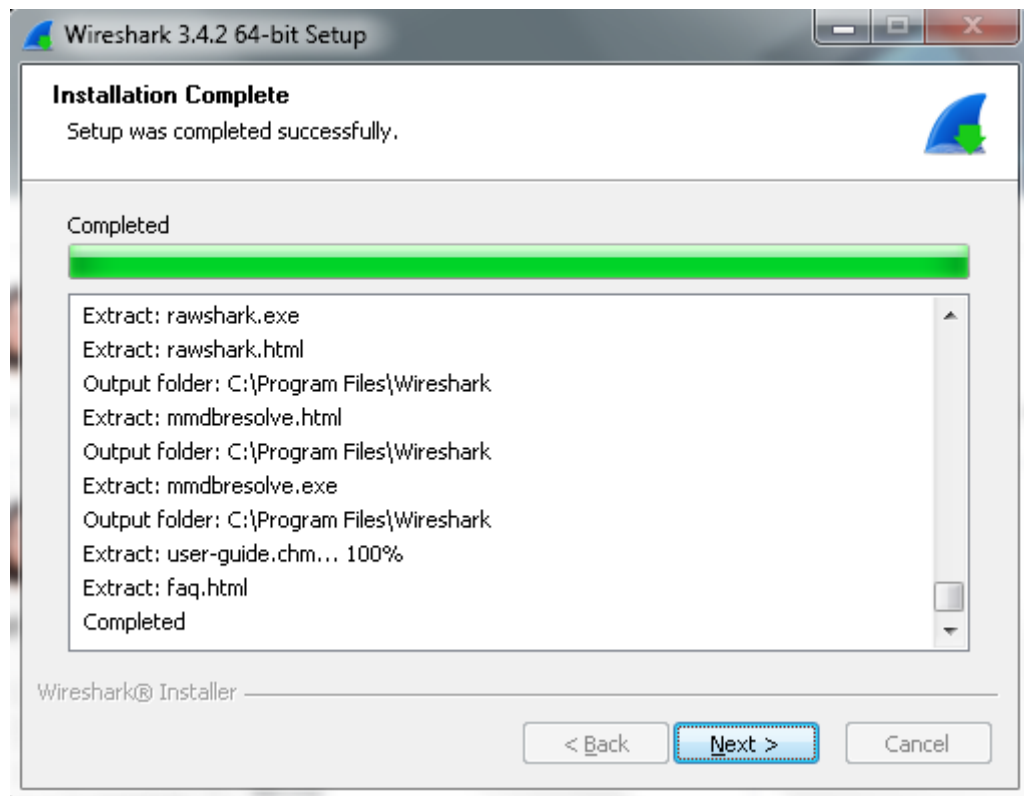
- c. Click on Noted







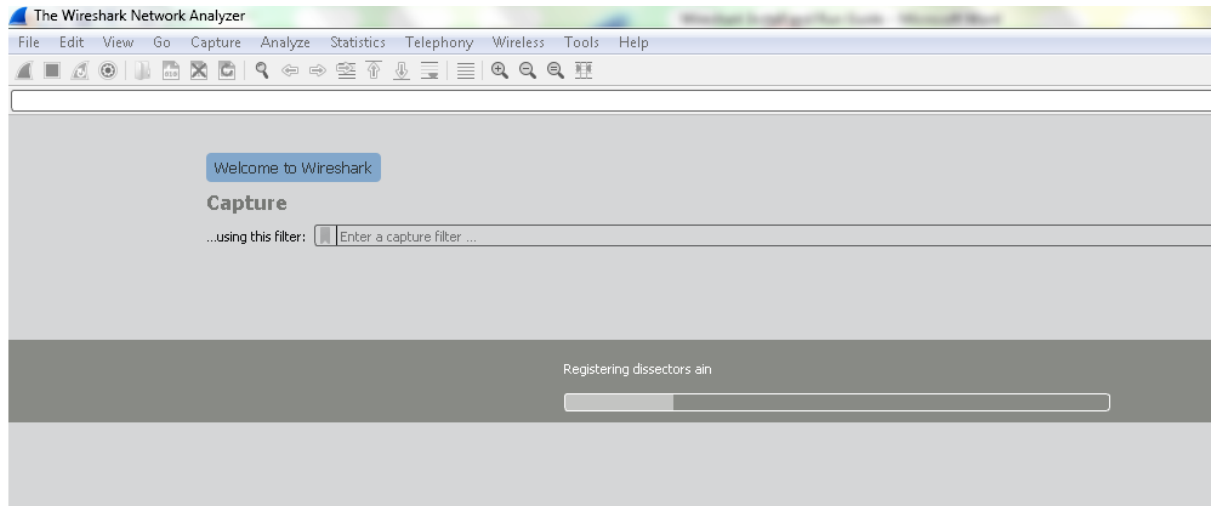




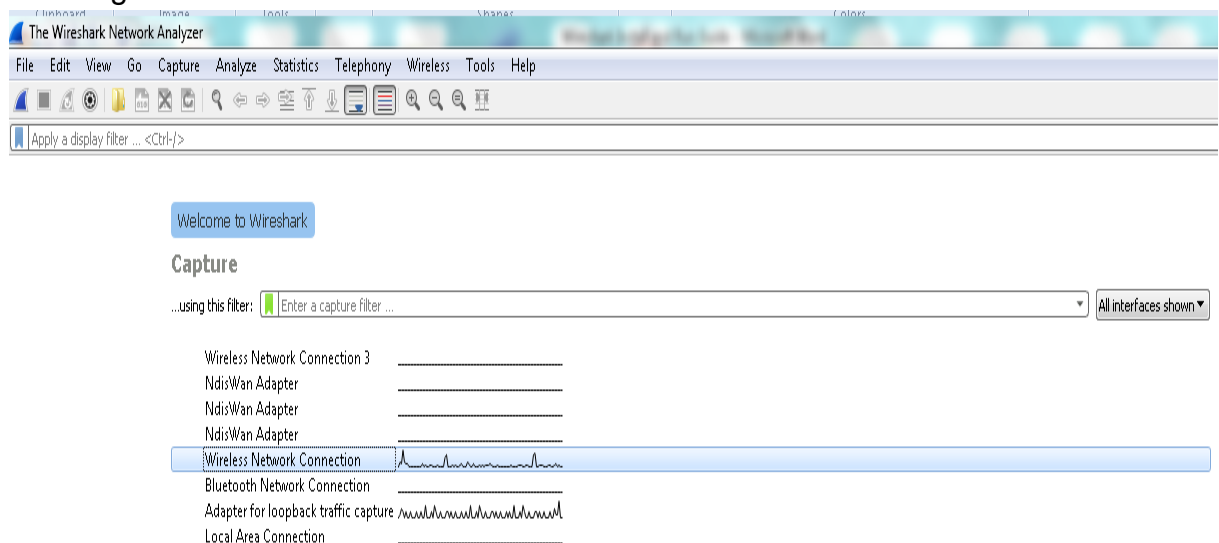
7. Testing Wireshark

a. Start your browser and select/ browse any homepage

b. Now start Wireshark software



c. Showing all interfaces connected to the network. Select wireless network connection.



- d. Automatic capturing of network filters on the selected interface

Running Wireshark (cont.)

command menus

display filter specification

listing of captured packets

details of selected packet header

packet content in hexadecimal and ASCII

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.46	128.121.50.122	TCP	1163 > http [SYN] Seq=0 Len=0 MSS=1460
2	0.127987	128.121.50.122	192.168.1.46	TCP	http > 1163 [SYN, ACK] Seq=0 Ack=1 win=57
3	0.128332	192.168.1.46	128.121.50.122	TCP	1163 > http [ACK] Seq=1 Ack=1 win=65535
4	0.153700	192.168.1.46	128.121.50.122	HTTP	GET /news/ HTTP/1.1
5	0.329641	128.121.50.122	192.168.1.46	TCP	[TCP segment of a reassembled PDU]
6	0.330326	128.121.50.122	192.168.1.46	HTTP	[TCP Previous segment lost] continuation
7	0.330457	192.168.1.46	128.121.50.122	TCP	1163 > http [ACK] Seq=657 Ack=1082 win=64
8	0.341042	128.121.50.122	192.168.1.46	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
9	0.341369	192.168.1.46	128.121.50.122	TCP	1163 > http [ACK] Seq=657 Ack=1082 win=64

Frame 4 (710 bytes on wire (568 bytes captured) on interface 0:00:00:00:00:00)

Ethernet II, Src: Netgear_61:8e:ed (00:09:5b:61:8e:ed), Dst: WestellT_9f:92:b9 (00:0f:db:9f:92:b9)

Internet Protocol, Src: 192.168.1.46 (192.168.1.46), Dst: 128.121.50.122 (128.121.50.122)

Transmission Control Protocol, Src Port: 1163 (1163), Dst Port: http (80), Seq: 1, Ack: 1, Len: 656

Hypertext Transfer Protocol

GET /news/ HTTP/1.1\r\n

Host: www.wireshark.org\r\n

User-Agent: Mozilla/5.0 (windows; u; windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n

Accept-Language: en-us,en;q=0.5\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

Referer: http://www.wireshark.org/faq.html\r\n

Cookie: __utma=87653150.62471437.1181007382.1181007382.1181169142.2; __utmz=87653150.1181007382.1.1.utm\r\n

0000 00 0f db 9f 92 b9 00 09 5b 61 8e ed 08 00 45 00 [a.m..E.

0010 02 b8 0f 25 40 00 80 06 74 51 c0 a8 01 2e 80 79 ...%B...TQ....Y

0020 32 7a 04 8b 00 50 ed bc 8e 1b 4e c6 f1 18 50 18 2z...P...N...P.

0030 ff ff 77 74 00 00 47 45 54 20 2f 6e 65 77 73 2f ..wt..GE T /news/

0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1..Host:

0050 20 77 77 77 2e 77 69 72 65 73 68 61 72 6b 2e 6f www.wireshark.o

0060 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 rg..User -Agent:

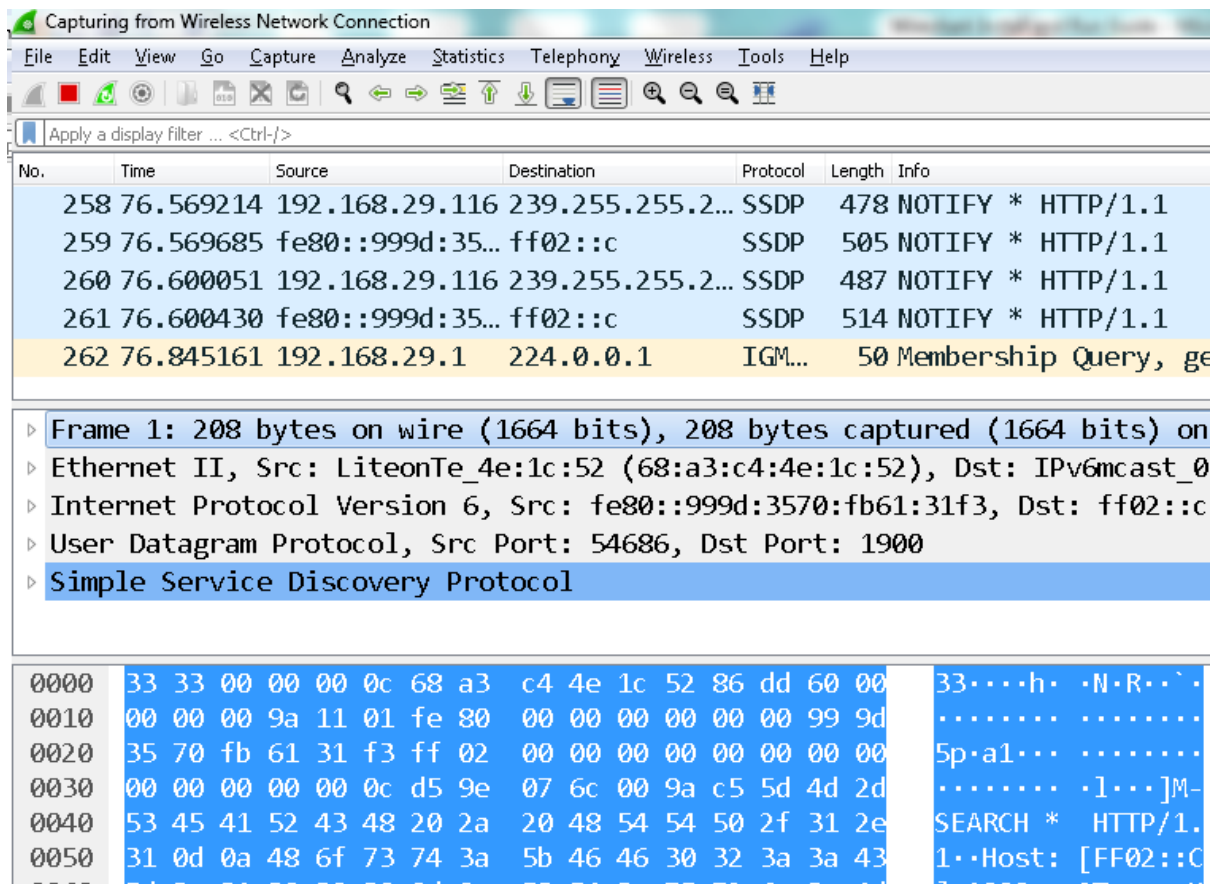
0070 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (win

0080 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 dows; u; windows

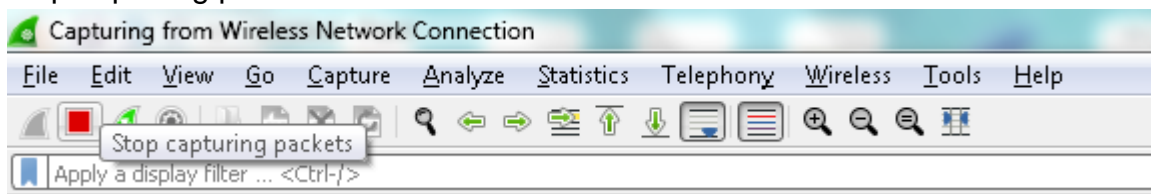
0090 20 4e 54 20 35 2e 31 3b 20 65 6e 2d 55 53 3b 20 NT 5.1; en-US;

00a0 72 76 3a 31 2e 38 2e 31 2e 34 29 20 47 65 63 6b rv:1.8.1 .4) Geck

00b0 6f 2f 32 30 30 37 30 35 31 35 20 46 69 72 65 66 o/200705 15 Firef



e. Stop capturing packets



f. Now, you can see multiple captured packets on the interface. In order to view the header content of a specific protocol, apply display filters.

g. Type "TCP" to apply display filter to see all segments of TCP protocol only

Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
10	3.070266	2405:201:4014...	2404:6800:400...	TCP	75	50827 → 443 [ACK] Seq=1 Ack=1 Win=16514 Len=1 [TCP segment of a reassembled...
11	3.076262	2404:6800:400...	2405:201:4014...	TCP	86	443 → 50827 [ACK] Seq=1 Ack=2 Win=279 Len=0 SLE=1 SRE=2
12	5.120255	192.168.29.116	13.224.22.71	TCP	55	50828 → 443 [ACK] Seq=1 Ack=1 Win=16572 Len=1 [TCP segment of a reassembled...
13	5.128116	13.224.22.71	192.168.29.116	TCP	66	443 → 50828 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
51	13.178555	2405:201:4014...	2404:6800:400...	TCP	75	50823 → 443 [ACK] Seq=1 Ack=1 Win=16414 Len=1 [TCP segment of a reassembled...
52	13.210061	2404:6800:400...	2405:201:4014...	TCP	86	443 → 50823 [ACK] Seq=1 Ack=2 Win=295 Len=0 SLE=1 SRE=2
62	21.188827	192.168.29.116	74.125.68.188	TCP	55	50497 → 5228 [ACK] Seq=1 Ack=1 Win=16423 Len=1
63	21.258283	74.125.68.188	192.168.29.116	TCP	66	5228 → 50497 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2

Frame 12: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{D2DAA985-85B9-48E5-8868-B379D992AF82}, interface 0

Ethernet II, Src: LiteonTe_4e:1c:52 (68:a3:c4:4e:1c:52), Dst: HonHaiPr_0b:86:15 (68:14:01:0b:86:15)

Internet Protocol Version 4, Src: 192.168.29.116, Dst: 13.224.22.71

Transmission Control Protocol, Src Port: 50828, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000 68 14 01 0b 86 15 68 a3 c4 4e 1c 52 08 00 45 00 h.....h..N.R..E..

0010 00 29 57 b5 40 00 40 06 e0 d6 c0 a8 1d 74 0d e0 ..)W.@. @.t..

0020 16 47 c6 8c 01 bb da cb 64 7e 16 8e 86 72 50 10 .G.....d....rP..

0030 40 bc c8 41 00 00 00 00 @...A....

- h. Select Any One TCP segment and look for the various level of addressing applicable for the segments captured i.e. at DLL, MAC layer, Network Layer and Transport layer.

Wireless Network Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
10	3.070266	2405:201:4014...	2404:6800:400...	TCP	75	50827 → 443 [ACK] Seq=1 Ack=1 Win=16514 Len=1 [TCP segment of a reassembled...

Frame 10: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{D2DAA985-85B9-48E5-8868-B379D992AF82}, interface 0

Ethernet II, Src: LiteonTe_4e:1c:52 (68:a3:c4:4e:1c:52), Dst: HonHaiPr_0b:86:15 (68:14:01:0b:86:15)

Internet Protocol Version 6, Src: 2405:201:4014:104c:55d8:ee1d:77db:681e, Dst: 2404:6800:4002:812::200e

Transmission Control Protocol, Src Port: 50827, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

0000 68 14 01 0b 86 15 68 a3 c4 4e 1c 52 86 dd 60 00 h.....h..N.R... ..

0010 00 00 00 15 06 40 24 05 02 01 40 14 10 4c 55 d8@\$. ..@..LU..

0020 ee 1d 77 db 68 1e 24 04 68 00 40 02 08 12 00 00 ..w.h.\$..h@.....

0030 00 00 00 00 20 0e c6 8b 01 bb 98 1f 81 4c 0b c2L... ..

0040 20 5d 50 10 40 82 d3 02 00 00 00 00 00 00 00 00]P.@.... ..

Frame (frame), 75 bytes

Packets: 588 · Displayed: 73 (12.4%) · Dropped: 0 (0.0%)

Profile: Default

15:38 22-01-2021

Lab Experiments based on Wireshark:

Carefully read the lab instructions and finish all tasks above.

1. Find 3 different protocols that appear in the protocol list.
2. Find the internet address of your computer and your server. Identify the internet address of any one homepage captured.
3. Find and capture the protocol hierarchy for a UDP/ SSDP segment.
4. Apply display filter to show all TCP segments on an interface. Also state what does black coloured TCP Segments indicate?
5. Identify the time difference between a set of DNS query and its DNS response. Show it with the help of an example.

Compiled by:

Dr. Vandana Sharma, Asst. Prof.