Computer Network

MCA Code 163

Lab Activity

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

Tool Used: Wireshark

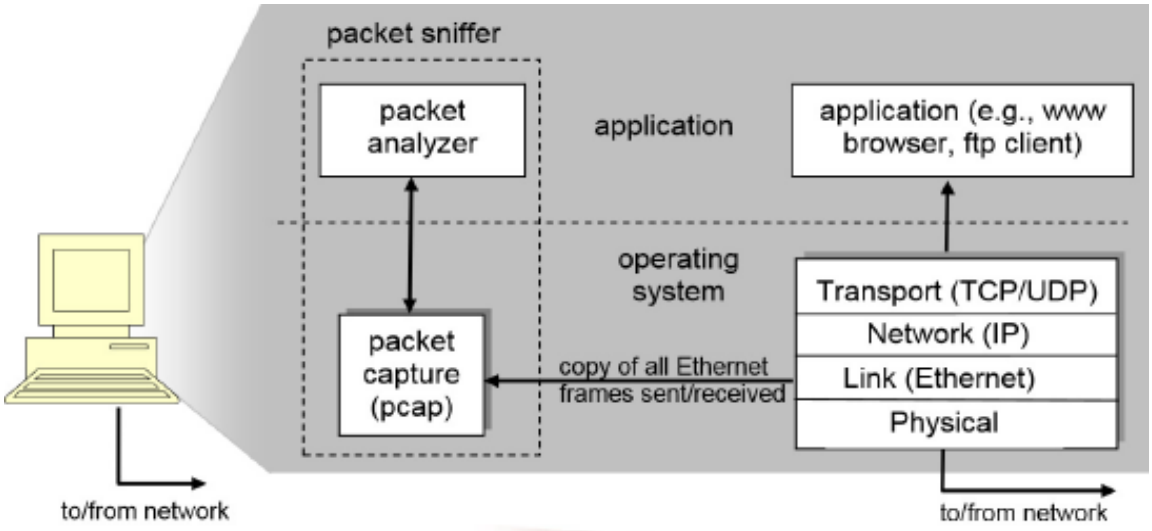
Introduction:

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

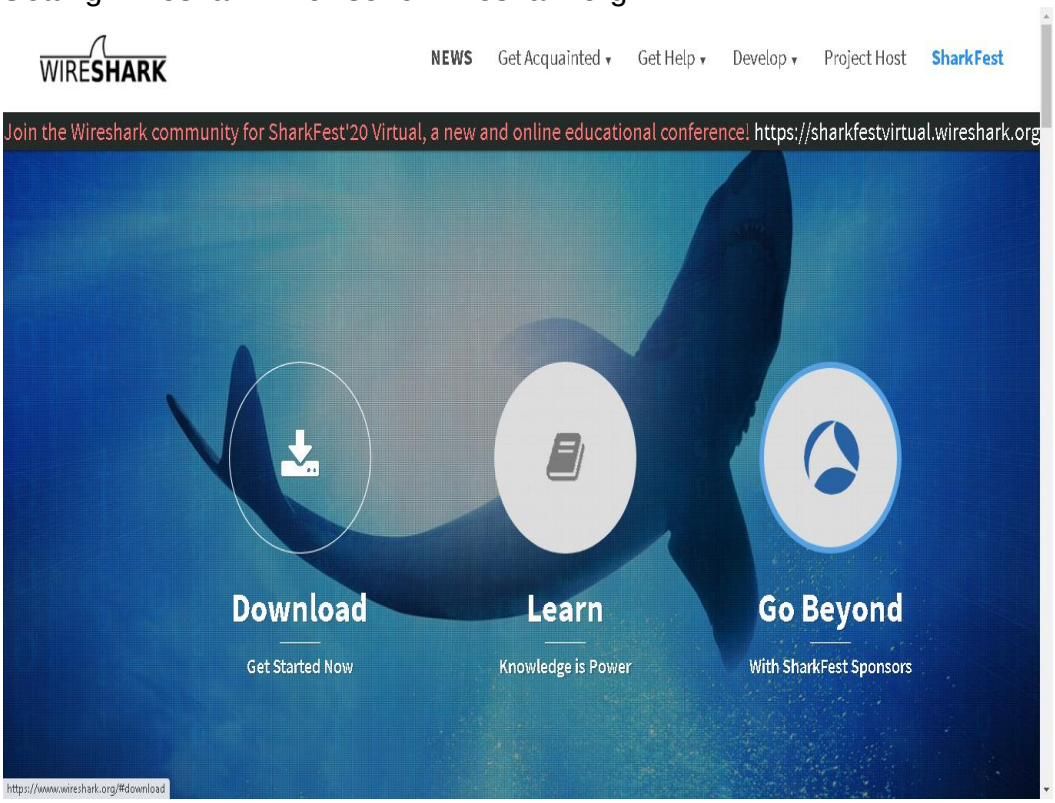
5. Example of Packet Sniffing- The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer.**

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.

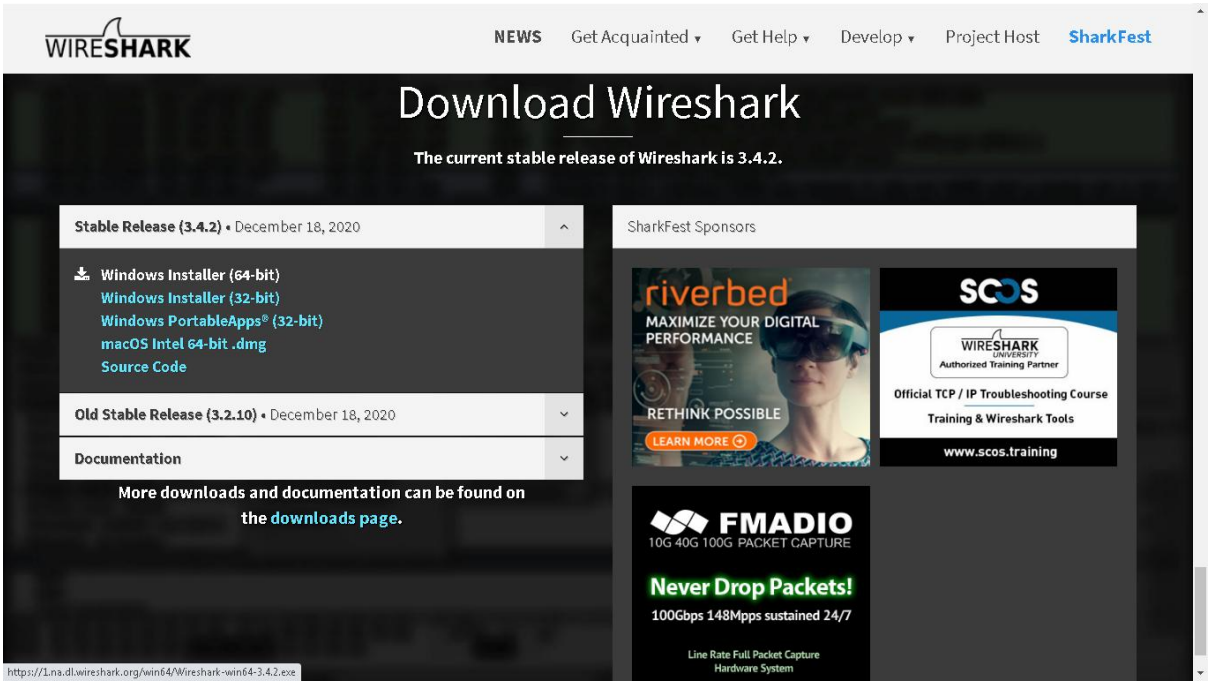


6. Steps to analyze Network Packets:

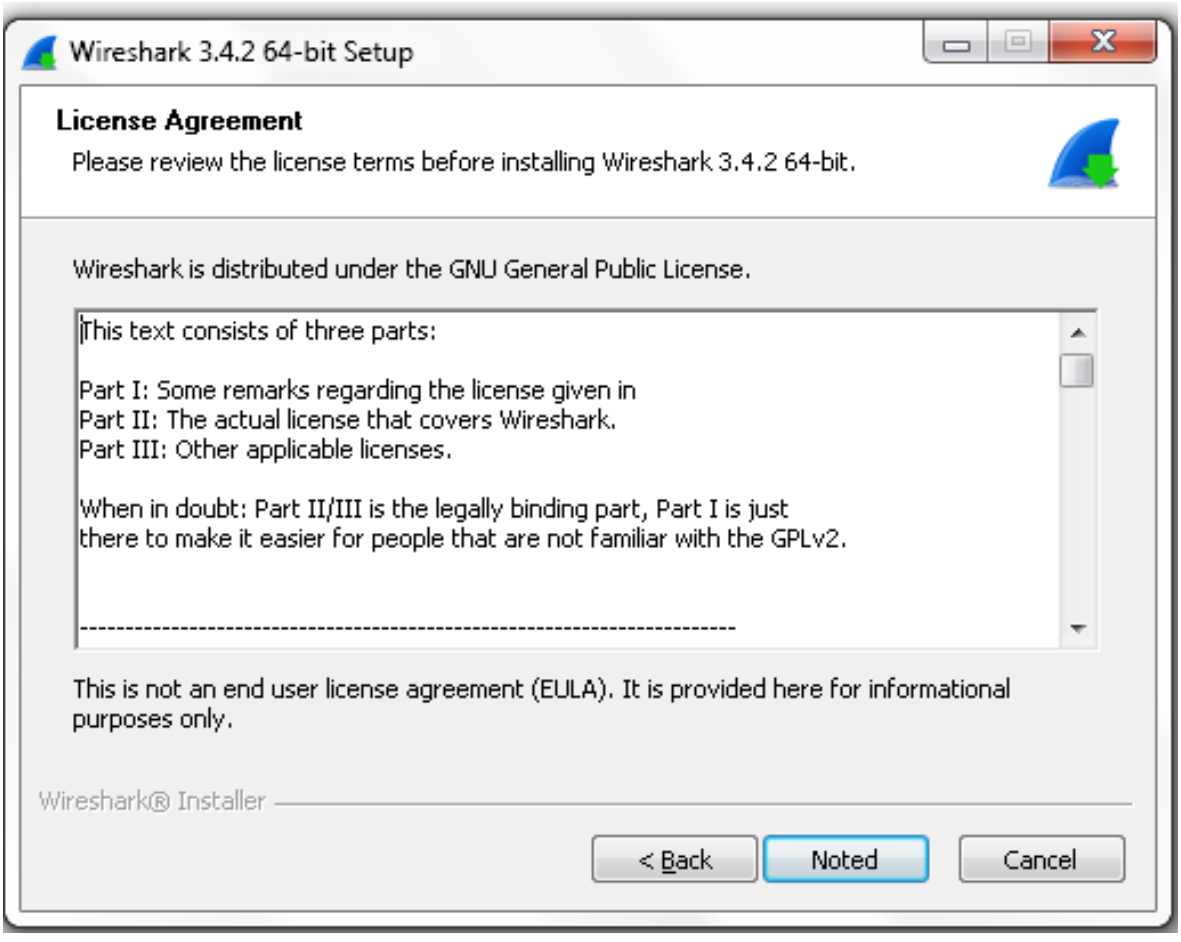
   a. Getting Wireshark: Browse for wireshark.org

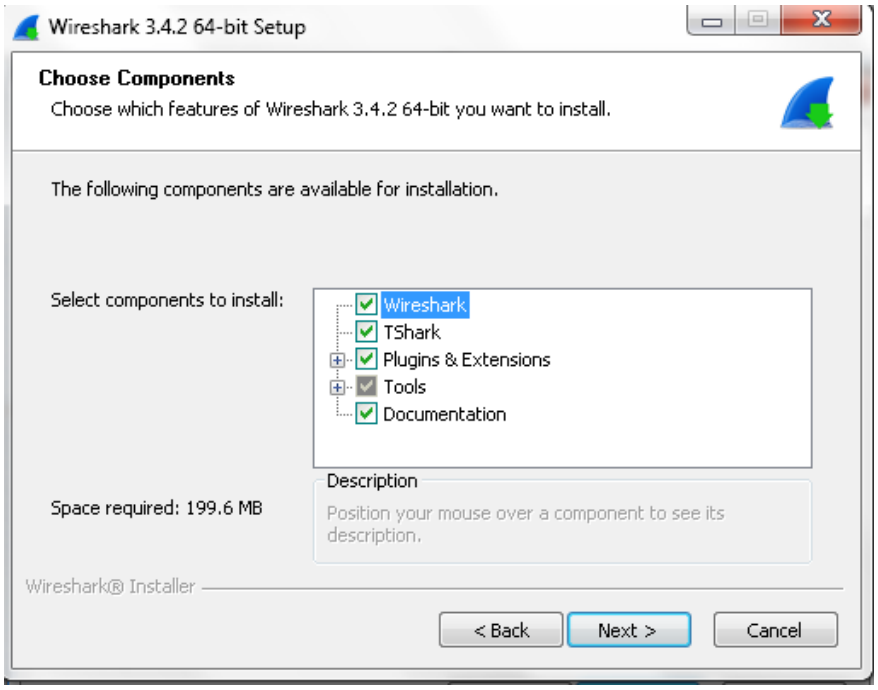


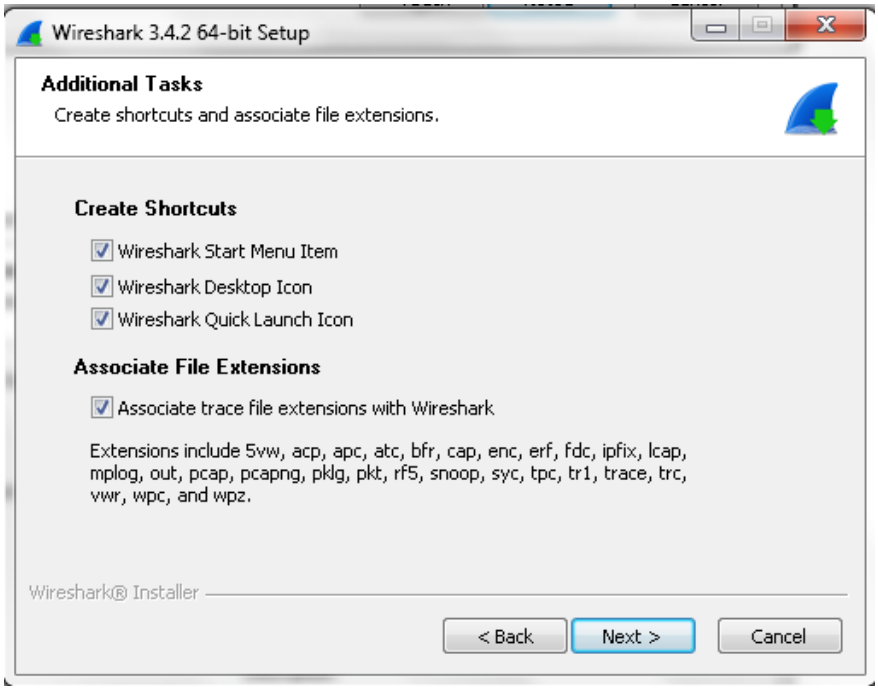
b. Download the appropriate version according to your OS.

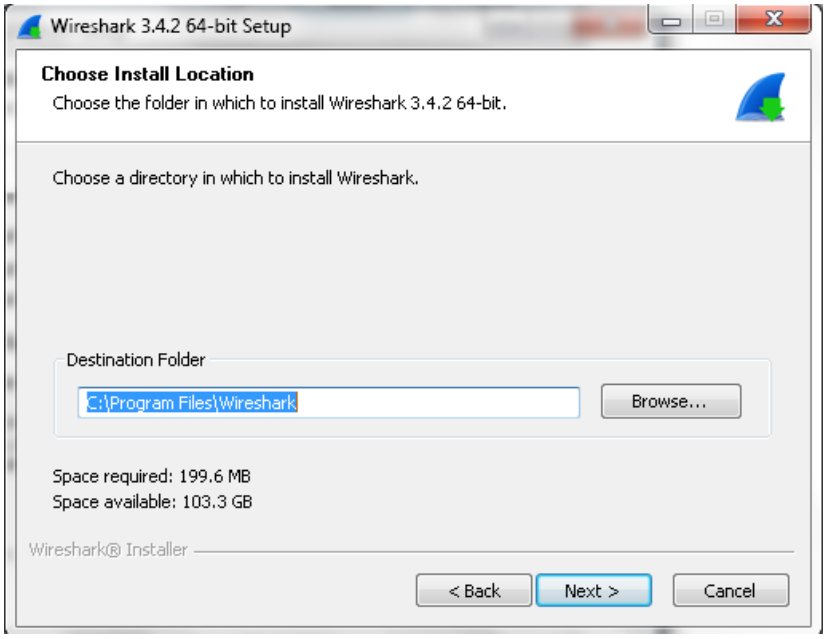


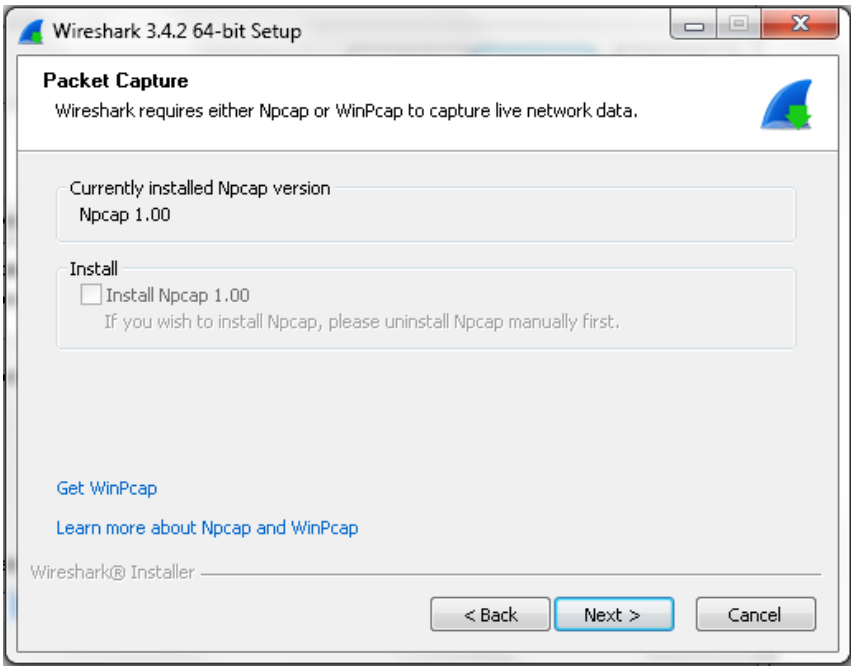
c. Click on Noted

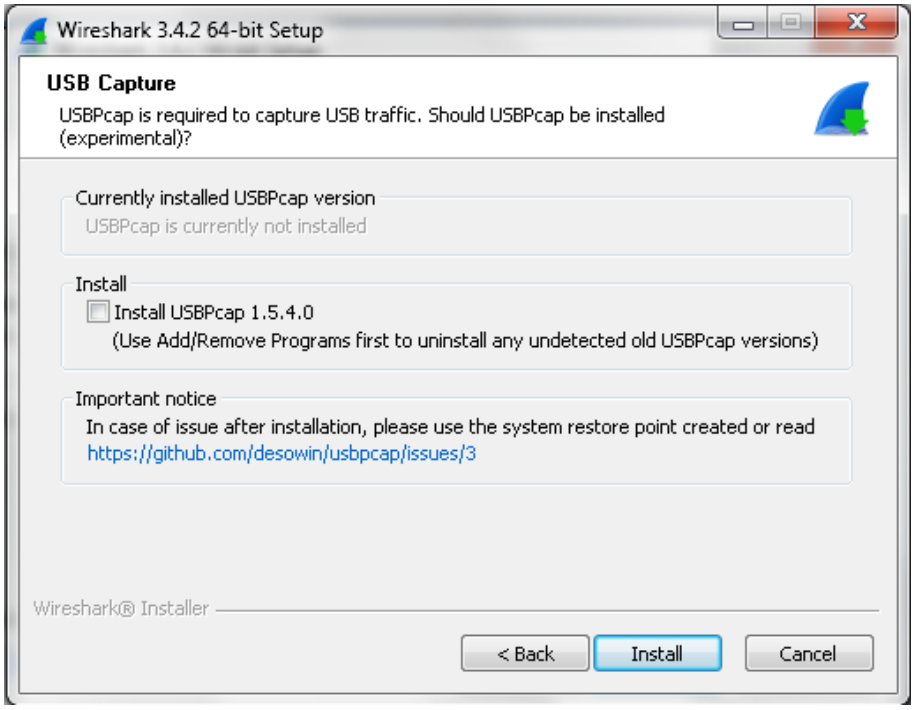


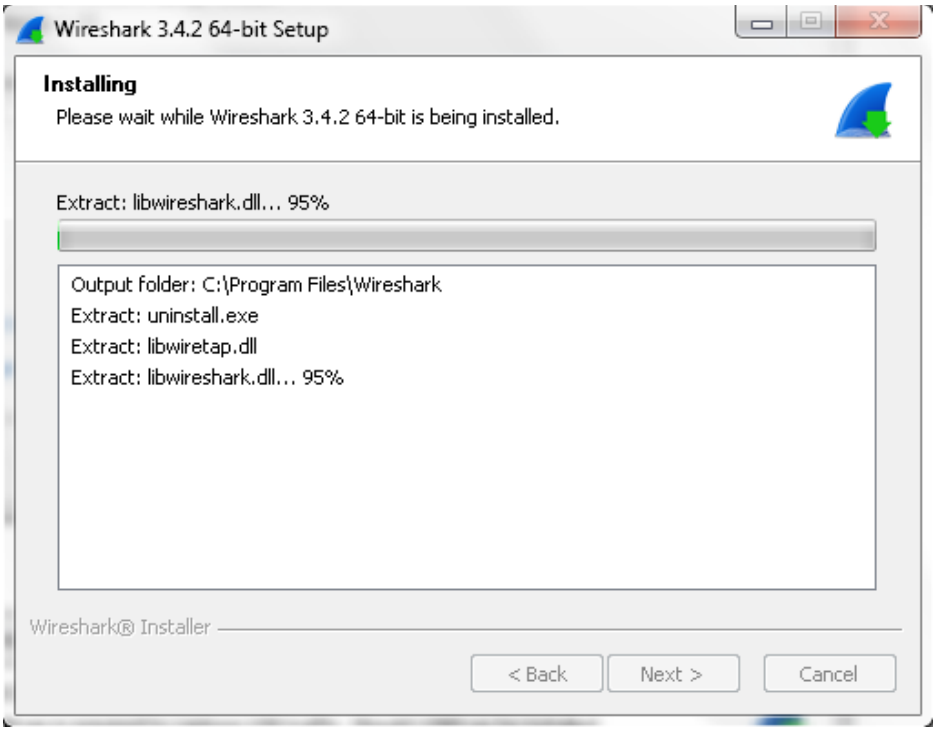

Wireshark 3.4.2 64-bit Setup
Choose Components
Choose which features of Wireshark 3.4.2 64-bit you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
Plugins & Extensions
Tools
Documentation
Description
Position your mouse over a component to see its description.
Space required: 199.6 MB
Wireshark® Installer
< Back
Next >
Cancel

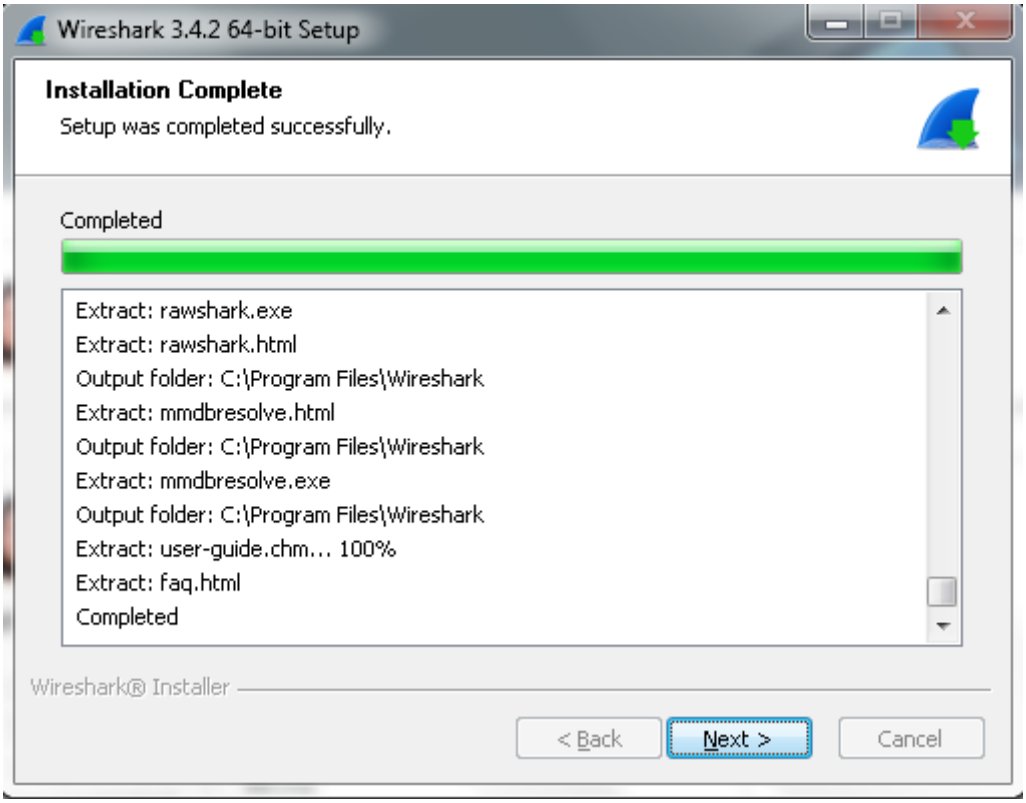

Wireshark 3.4.2 64-bit Setup
Additional Tasks
Create shortcuts and associate file extensions.
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Wireshark Quick Launch Icon
Associate File Extensions
Associate trace file extensions with Wireshark
Extensions include 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, lcap, mplog, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, and wpz.
Wireshark® Installer
< Back
Next >
Cancel

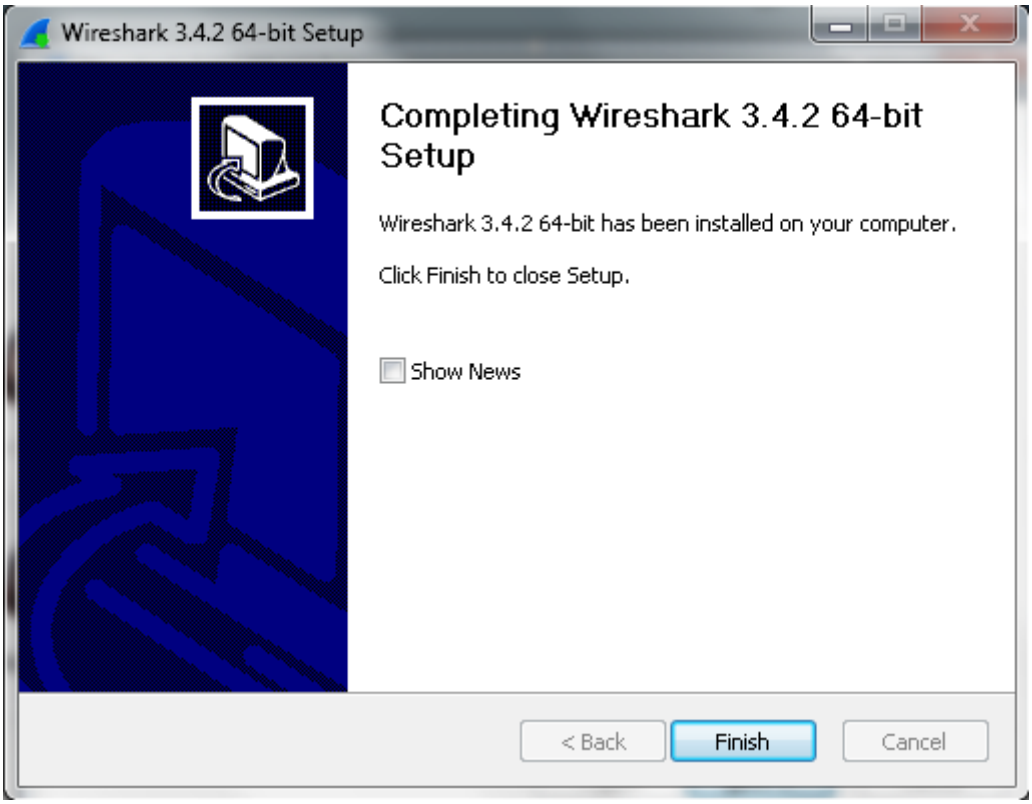

Wireshark 3.4.2 64-bit Setup
Choose Install Location
Choose the folder in which to install Wireshark 3.4.2 64-bit.
Choose a directory in which to install Wireshark.
Destination Folder
C:\Program Files\Wireshark
Browse...
Space required: 199.6 MB
Space available: 103.3 GB
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 3.4.2 64-bit Setup
Packet Capture
Wireshark requires either Npcap or WinPcap to capture live network data.
Currently installed Npcap version
Npcap 1.00
Install
Install Npcap 1.00
If you wish to install Npcap, please uninstall Npcap manually first.
Get WinPcap
Learn more about Npcap and WinPcap
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 3.4.2 64-bit Setup
USB Capture
USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?
Currently installed USBPcap version
USBPcap is currently not installed
Install
Install USBPcap 1.5.4.0
(Use Add/Remove Programs first to uninstall any undetected old USBPcap versions)
Important notice
In case of issue after installation, please use the system restore point created or read
https://github.com/desowin/usbpcap/issues/3
Wireshark® Installer
< Back
Install
Cancel


Wireshark 3.4.2 64-bit Setup
Installing
Please wait while Wireshark 3.4.2 64-bit is being installed.
Extract: libwireshark.dll... 95%
Output folder: C:\Program Files\Wireshark
Extract: uninstall.exe
Extract: libwiretap.dll
Extract: libwireshark.dll... 95%
Wireshark® Installer
< Back
Next >
Cancel

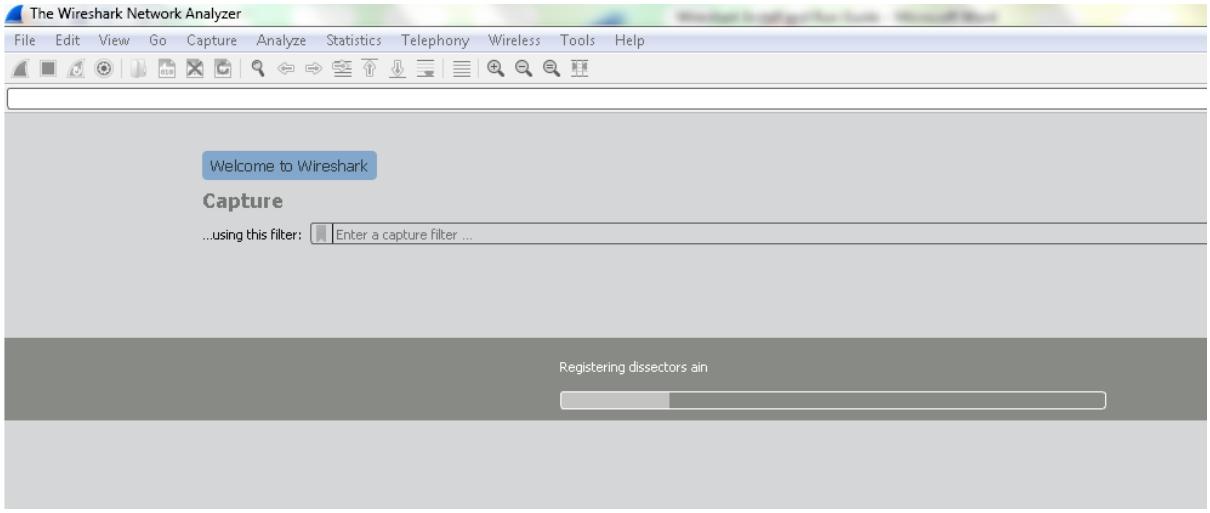

Wireshark 3.4.2 64-bit Setup
Installation Complete
Setup was completed successfully.
Completed
Extract: rawshark.exe
Extract: rawshark.html
Output folder: C:\Program Files\Wireshark
Extract: mmdbresolve.html
Output folder: C:\Program Files\Wireshark
Extract: mmdbresolve.exe
Output folder: C:\Program Files\Wireshark
Extract: user-guide.chm... 100%
Extract: faq.html
Completed
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 3.4.2 64-bit Setup
Completing Wireshark 3.4.2 64-bit Setup
Wireshark 3.4.2 64-bit has been installed on your computer.
Click Finish to close Setup.
Show News
< Back
Finish
Cancel

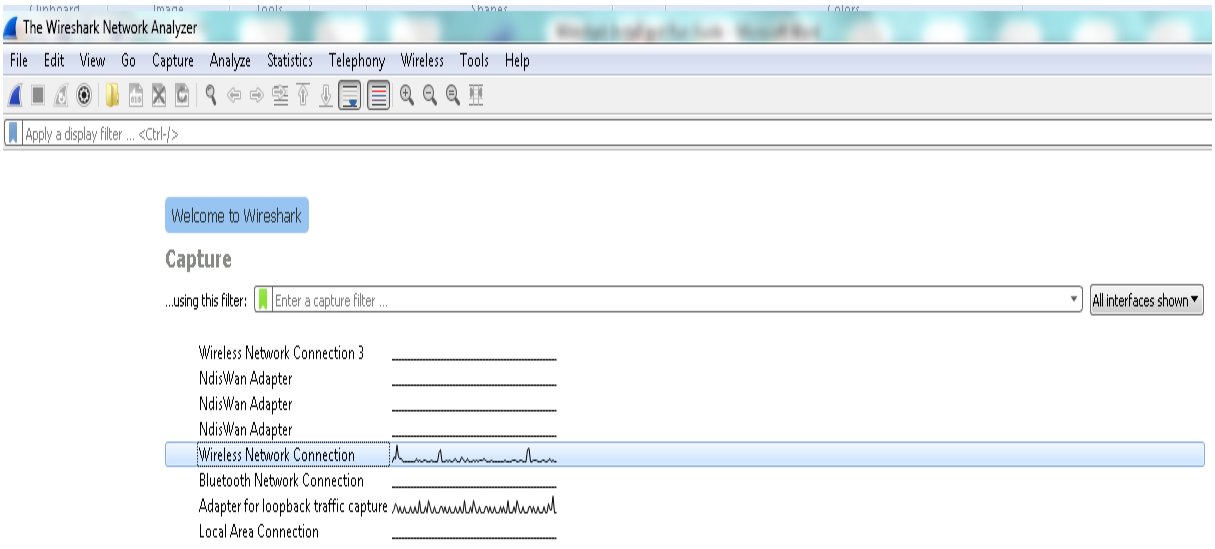
7. Testing Wireshark

a. Start your browser and select/ browse any homepage

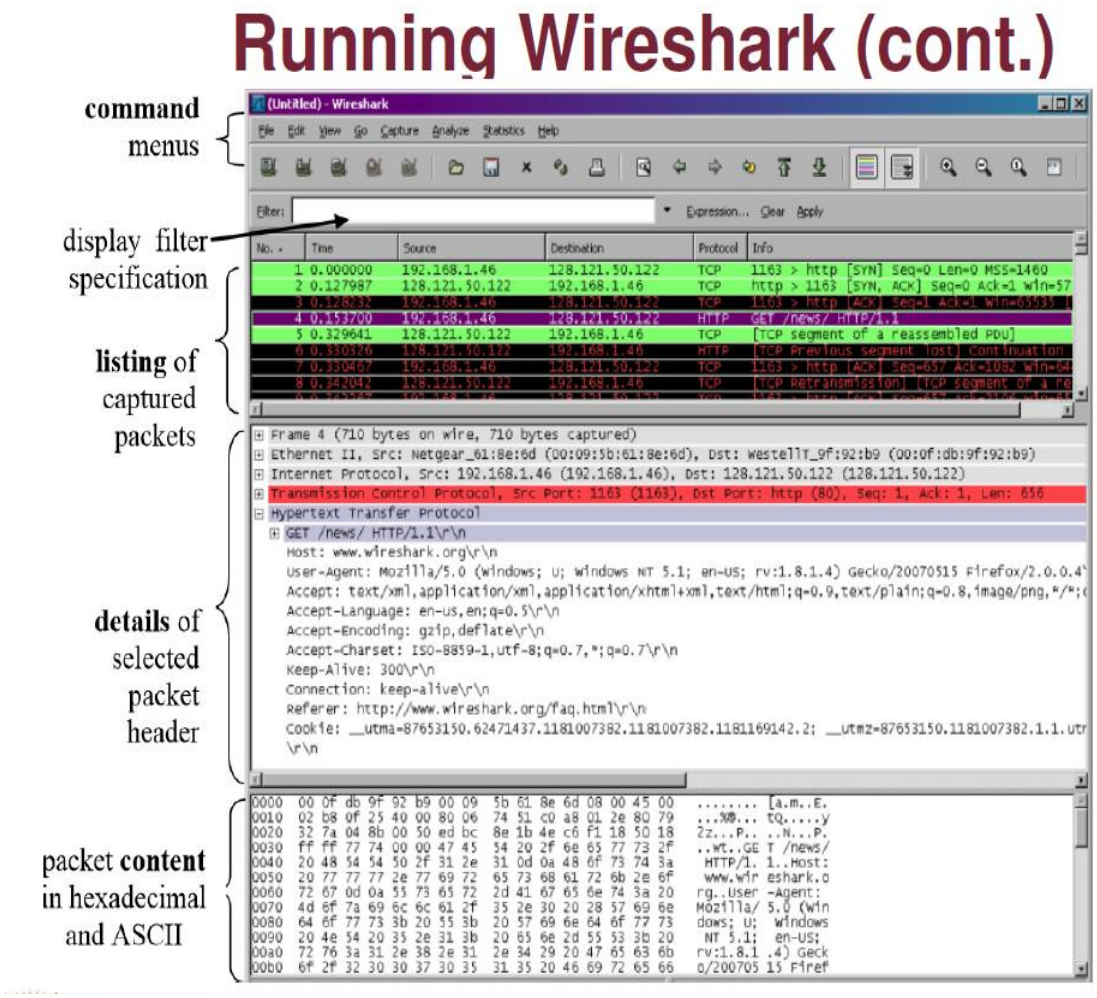
b. Now start Wireshark software

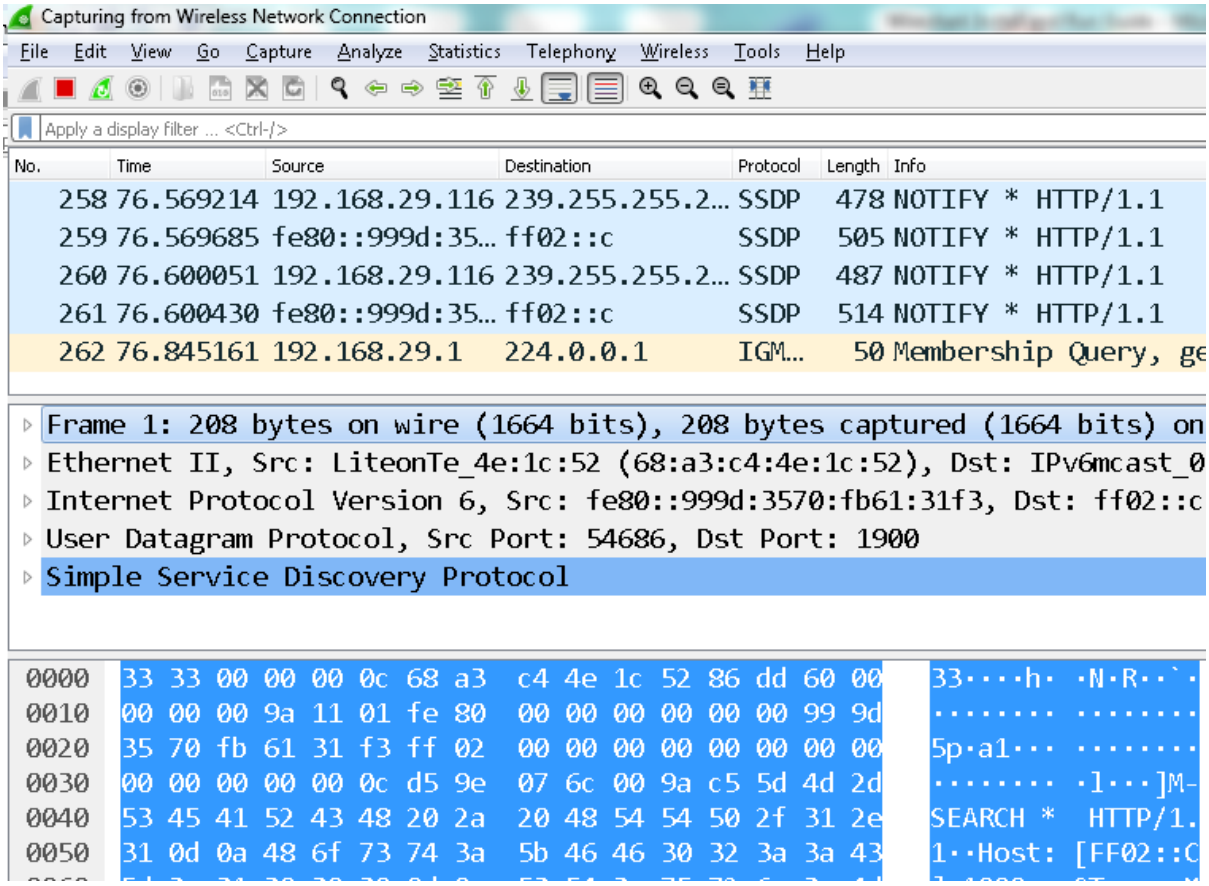


c. Showing all interfaces connected to the network. Select wireless network connection.

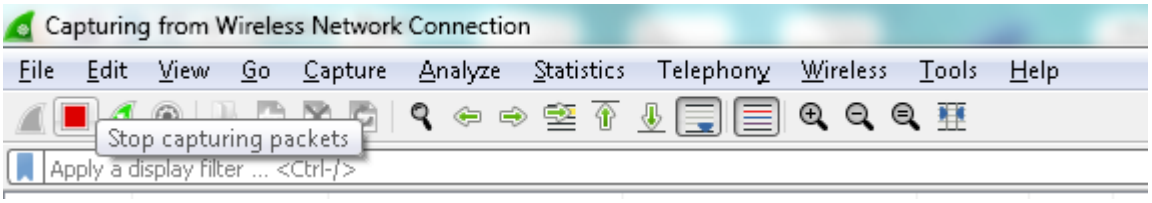


d. Automatic capturing of network filters on the selected interface



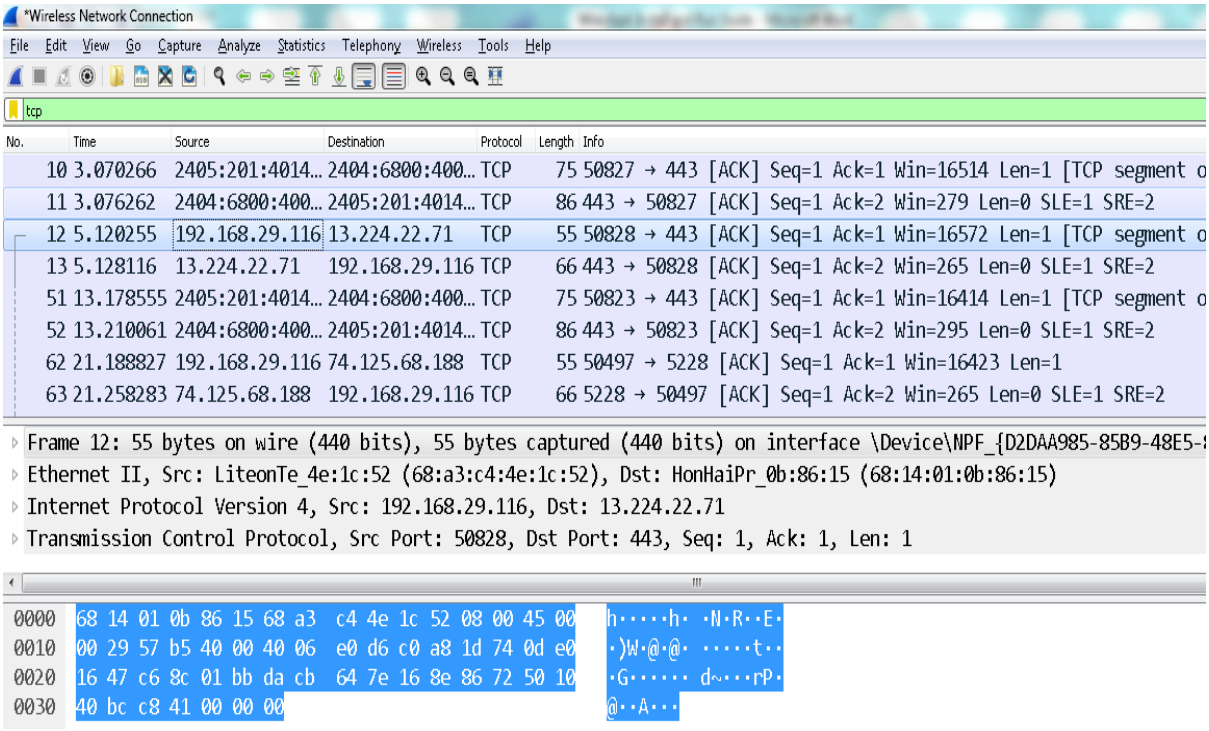


e. Stop capturing packets

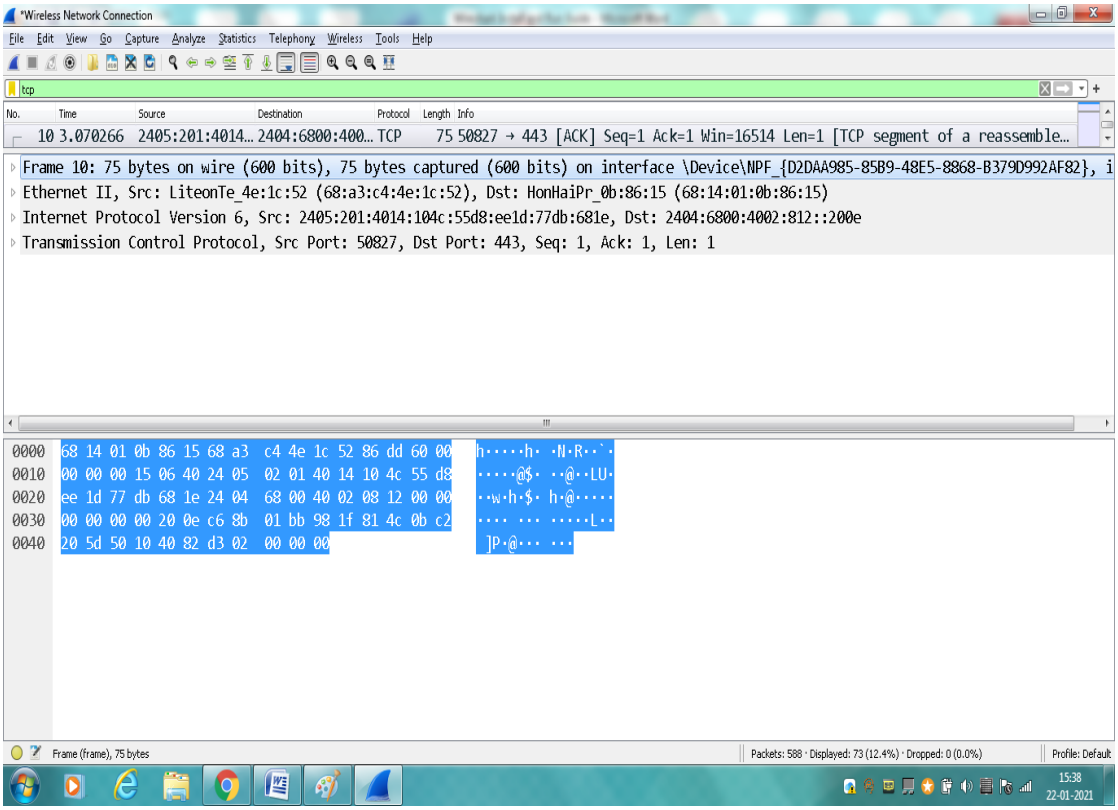


f. Now, you can see multiple captured packets on the interface. In order to view the header content of a specific protocol, apply display filters.

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



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.



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. Identity 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.