

Ex No: 4a STUDY OF WIRESHARK TOOL FOR PACKET SNIFFING

Date : 10.8.2024

AIM:

To study packet sniffing concepts using Wireshark Tool.

DESCRIPTION:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

What we can do with Wireshark:

- Capture network traffic
- Decode packet protocols using dissectors
- Define filters – capture and display
- Watch smart statistics
- Analyze problems
- Interactively browse that traffic

Wireshark used for:

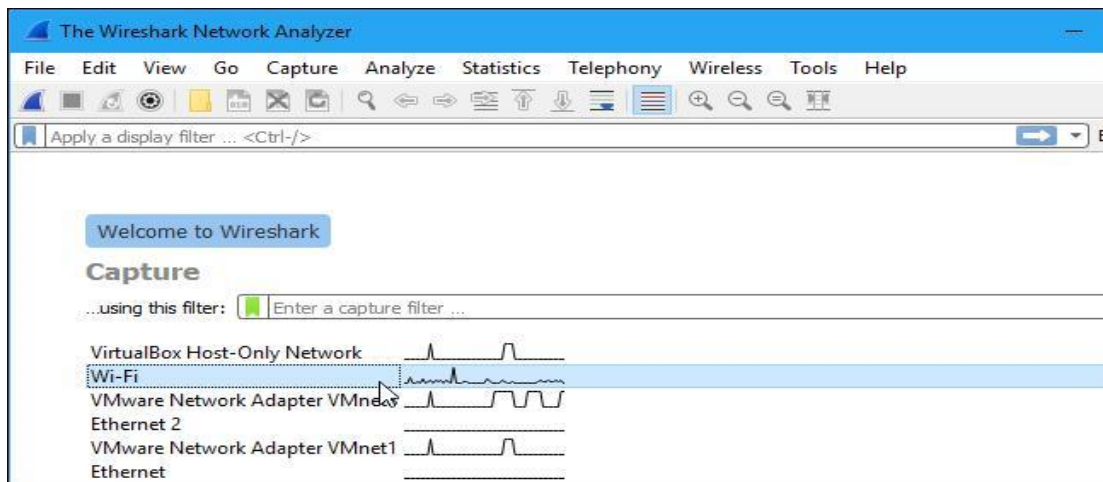
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

Getting Wireshark

Wireshark can be downloaded for Windows or macOS from [its official website](#). For Linux or another UNIX-like system, Wireshark will be found in its package repositories. For Ubuntu, Wireshark will be found in the Ubuntu Software Center.

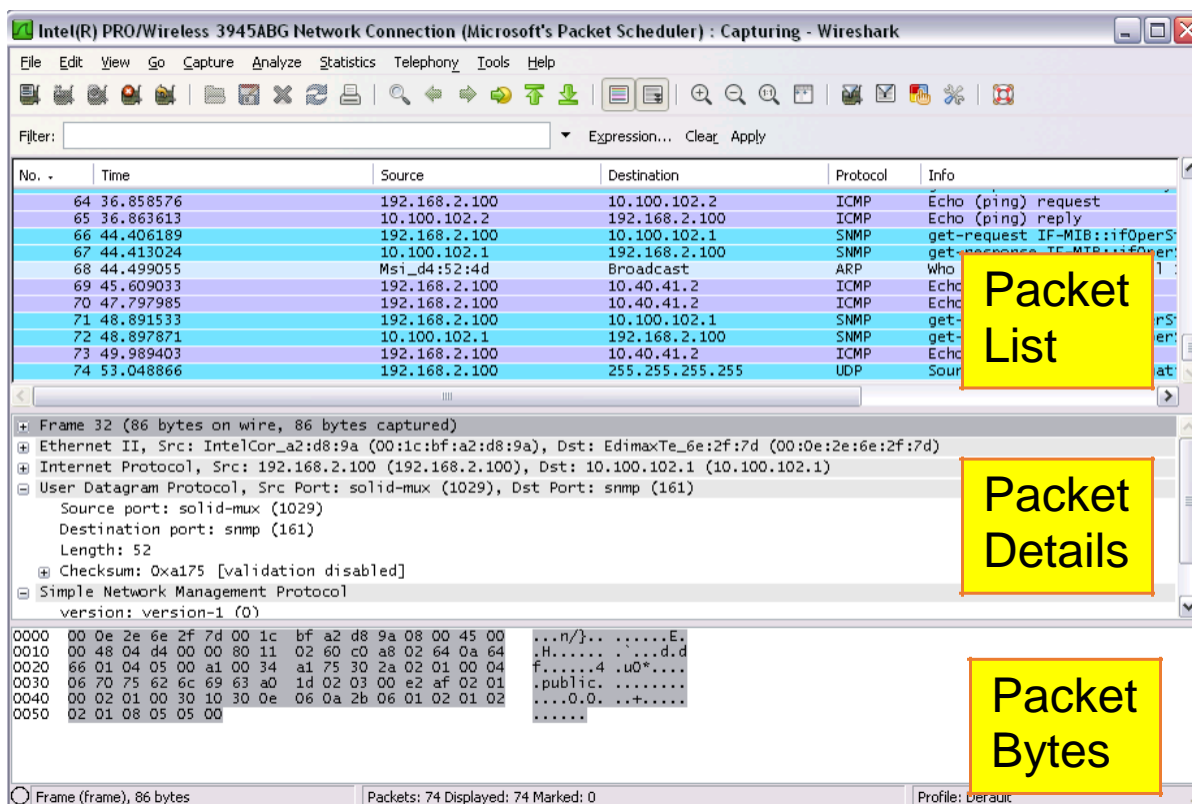
Capturing Packets

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.

The “Packet List” Pane

The packet list pane displays all the packets in the current capture file. The “Packet List” pane Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the “Packet Details” and “Packet Bytes” panes.

The “Packet Details” Pane

The packet details pane shows the current packet (selected in the “Packet List” pane) in a more detailed form. This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

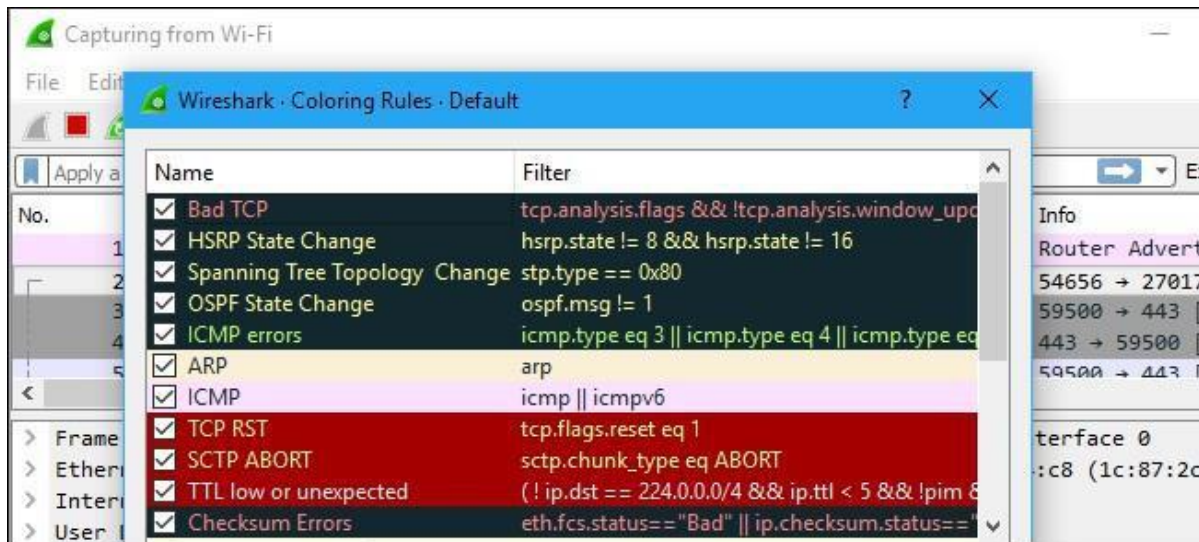
The “Packet Bytes” Pane

The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style.

Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

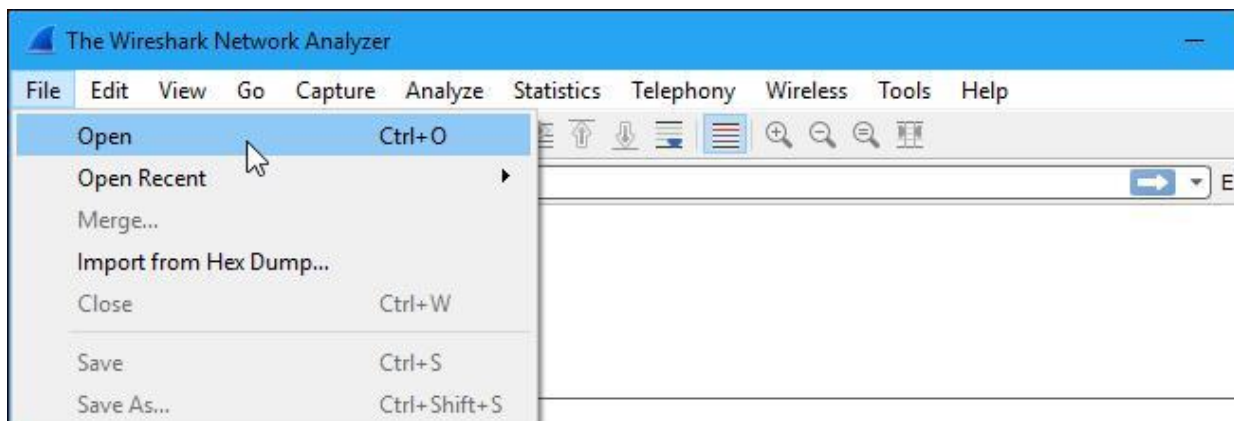
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a [page of sample capture files](#) that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.

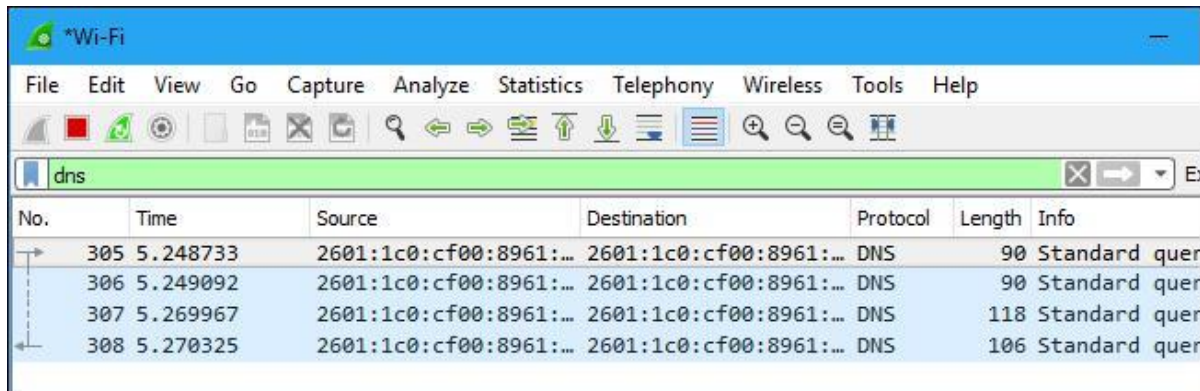


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the

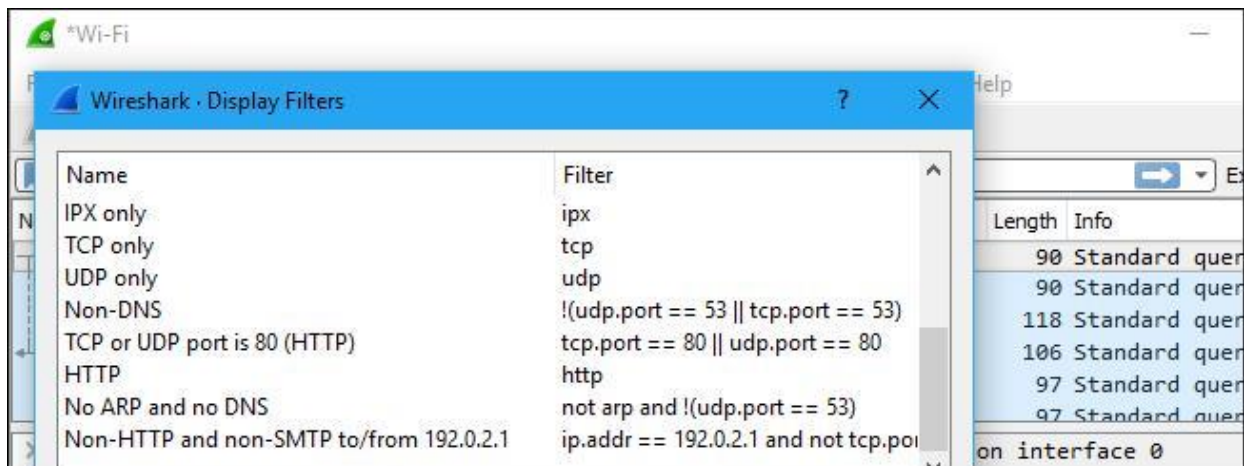
traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



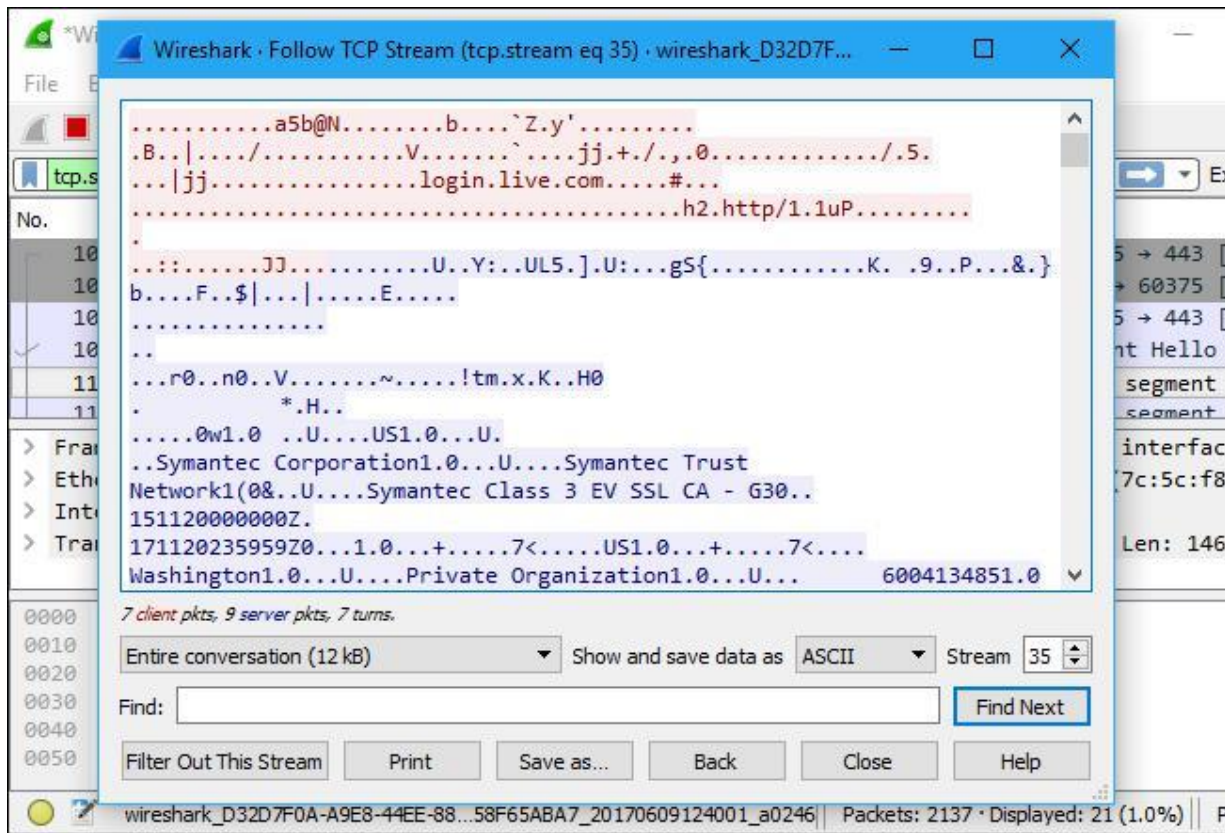
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the [Building display filter expressions](#) page in the official Wireshark documentation.

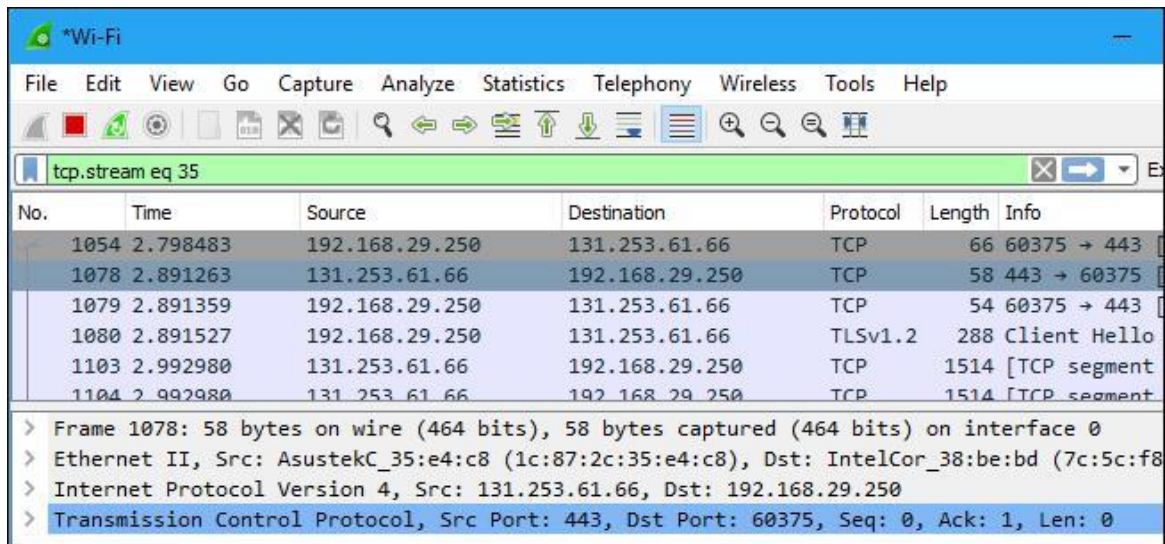


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.



Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.



Inspecting Packets

Click a packet to select it and you can dig down to view its details.

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The packet list pane shows a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

Packet 1054 is selected. The details pane shows the following information:

- Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
- Encapsulation type: Ethernet (1)
- Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1497037204.140141000 seconds

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00  ..,5..|\ .8....E.
0010  00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd  .4.].@... O.....
0020  3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02  =B...."R {i.....
0030  fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01  ..H.....
0040  04 02  ..
```

The status bar at the bottom indicates the encapsulation type (frame.encap_type) and the number of packets (8136) with 21 displayed (0.3%).

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

The image shows the Wireshark network protocol analyzer interface with the Graph Analysis pane open. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The packet list pane shows a table of captured packets:

Time	Source	Destination	Comment
0.000	192.168.2.100	10.40.41.2	Echo (ping) request
2.183	192.168.2.100	10.40.41.2	Echo (ping) request
3.430	25005	53	Standard query A ww
3.457	25005	53	Standard query resp
3.462	2895	53	Standard query A ww
3.624	3866	80	dzdaemon > http [SY
3.728	3866	80	http > dzdaemon [SY
3.728	3866	80	dzdaemon > http [AC
3.729	3866	80	GET / HTTP/1.1
3.769	3866	80	http > dzdaemon [AC
3.771	3866	80	HTTP/1.0 301 Moved
3.772	3866	80	GET /home/0,7340,L-
3.965	3866	80	[TCP Previous segme
3.965	3866	80	[TCP Dup ACK 12#1]
3.966	3866	80	[TCP segment of a r
3.966	3866	80	[TCP Dup ACK 12#2]
3.966	3866	80	[TCP segment of a r
3.968	3866	80	[TCP Dup ACK 12#3]
3.968	3866	80	[TCP segment of a r
3.968	2895	53	Standard query resp
3.990	3866	80	[TCP segment of a r

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00  ..,5..|\ .8....E.
0010  00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd  .4.].@... O.....
0020  3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02  =B...."R {i.....
0030  fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01  ..H.....
0040  04 02  ..
```

The status bar at the bottom indicates the encapsulation type (frame.encap_type) and the number of packets (8136) with 21 displayed (0.3%).

RESULT :

Thus the packet sniffing concepts using wireshark tool is studied.