

## SYCS CN

### PRACTICAL 9

#### AIM :

**Using Wireshark, network analyzer, set the filter for ICMP, TCP, HTTP, UDP, FTP and perform respective protocol transactions to show/prove that the network analyzer is working**

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.

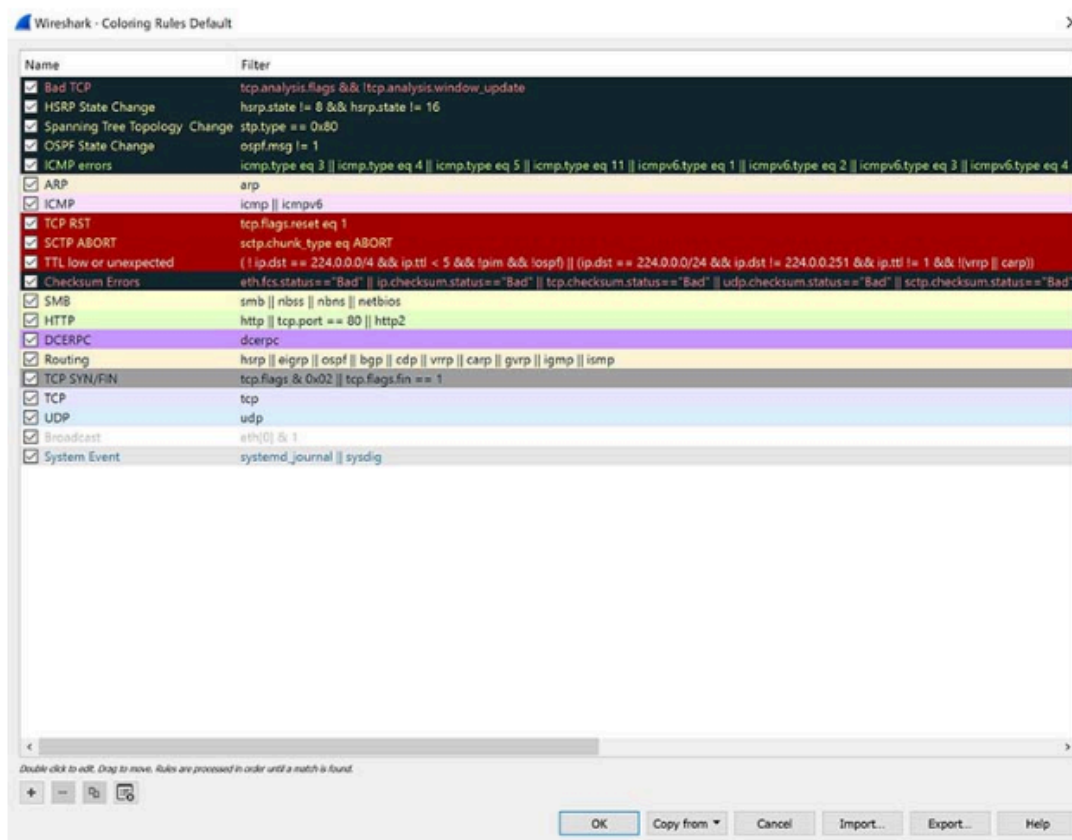
Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

Now that you have some packets, it's time to figure out what they mean. Wireshark tries to help you identify packet types by applying common-sense color coding. The table below describes the default colors given to major packet types.

Color in Wireshark	Packet Type
Light purple	TCP
Light blue	UDP
Black	Packets with errors
Light green	HTTP traffic
Light yellow	Windows-specific traffic, including Server Message Blocks (SMB) and NetBIOS
Dark yellow	Routing
Dark gray	TCP SYN, FIN and ACK traffic

The default coloring scheme is shown below in Figure 6.  
You can view this by going to **View >> Coloring Rules**.



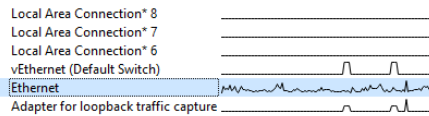


Welcome to Wireshark

## Capture

...using this filter:

All interfaces shown



[ Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
[ http]						
No.	Time	Source	Destination	Protocol	Length	Info
10256	186.341721	192.168.1.164	65.1.191.193	HTTP	423	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
10258	186.348286	65.1.191.193	192.168.1.164	HTTP	467	HTTP/1.1 200 OK (application/text)
10366	186.722939	192.168.1.164	65.1.191.193	HTTP	423	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
10376	186.730074	65.1.191.193	192.168.1.164	HTTP	467	HTTP/1.1 200 OK (application/text)
10579	187.365711	192.168.1.164	65.1.191.193	HTTP	403	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
10583	187.376970	65.1.191.193	192.168.1.164	HTTP	507	HTTP/1.1 200 OK (application/text)
12521	211.698649	192.168.1.164	65.1.191.193	HTTP	415	POST /URLCategorizerService/URLCategorize HTTP/1.1 (application/x-www-form-urlencoded)
12539	211.705669	65.1.191.193	192.168.1.164	HTTP	467	HTTP/1.1 200 OK (application/text)
14067	230.781191	192.168.1.164	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1

Frame 10256: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on interface \Device\NPF\_{9E87167D-EF4F-4EBC-A1C3-51BF9CFC43FD}, id 0  
Ethernet II, Src: Giga-Byt\_5b:2a:b4 (1c:1b:0d:5b:2a:b4), Dst: zte\_e9:f0:96 (10:10:81:e9:f0:96)  
Internet Protocol Version 4, Src: 192.168.1.164, Dst: 65.1.191.193  
Transmission Control Protocol, Src Port: 55945, Dst Port: 8080, Seq: 1, Ack: 1, Len: 369  
Hypertext Transfer Protocol  
HTML Form URL Encoded: application/x-www-form-urlencoded

[ icmpv6]						
No.	Time	Source	Destination	Protocol	Length	Info
1401	22.113439	fe80::e03b:95db:c3f... ff02::1:ff7d:653b	ff02::1:ff7d:653b	ICMPv6	86	Neighbor Solicitation for fe80::bc13:2f48:277d:653b from 1c:1b:0d:59:5a:b0
2606	38.592440	fe80::44ce:8f9d:b73... ff02::16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2631	39.077994	fe80::44ce:8f9d:b73... ff02::16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2863	43.218771	fe80::6ca2:b7e0:76a... ff02::1:ff58:80ac	ff02::1:ff58:80ac	ICMPv6	86	Neighbor Solicitation for fe80::7421:27f6:eb58:80ac from 00:24:1d:ef:e2:e0
3368	43.820463	fe80::2d9a:d36:3d99... ff02::1:ff58:80ac	ff02::1:ff58:80ac	ICMPv6	86	Neighbor Solicitation for fe80::7421:27f6:eb58:80ac from 00:21:5e:c2:6b:22
4373	62.000708	fe80::2d0a:c02b:e97... ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
4377	62.001220	fe80::2d0a:c02b:e97... ff02::16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
4379	62.001341	fe80::2d0a:c02b:e97... ff02::16	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
4407	62.229513	fe80::2d0a:c02b:e97... ff02::2	ff02::2	ICMPv6	62	Router Solicitation
4408	62.229518	::	ff02::1:ff74:f2cc	ICMPv6	78	Neighbor Solicitation for fe80::2d0a:c02b:e974:f2cc
4409	62.230531	fe80::2d0a:c02b:e97... ff02::16	ff02::16	ICMPv6	110	Multicast Listener Report Message v2

> Frame 1401: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF\_{9E87167D-EF4F-4EBC-A1C3-51BF9CFC43FD}, id 0  
> Ethernet II, Src: Giga-Byt\_59:5a:b0 (1c:1b:0d:59:5a:b0), Dst: IPv6mcast\_ff:7d:65:3b (33:33:ff:7d:65:3b)  
> Internet Protocol Version 6, Src: fe80::e03b:95db:c3fc:bfda, Dst: ff02::1:ff7d:653b  
> Internet Control Message Protocol v6

```
3000 33 33 ff 7d 65 3b 1c 1b 0d 59 5a b0 86 dd 00 00 33:}e;..-YZ...
3010 00 00 00 20 3a ff fe 80 00 00 00 00 00 e0 3b ...:.....;
3020 95 db c3 fc bf da ff 02 00 00 00 00 00 00 00 .....
3030 00 01 ff 7d 65 3b 87 00 20 bd 00 00 00 00 Fe 80 ...}e;...Fe 80
3040 00 00 00 00 00 00 bc 13 2f 48 27 7d 65 3b 01 01 ...../H'}e;..
3050 1c 1b 0d 59 5a b0 ...-YZ
```

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
238	3.376977	104.18.10.207	192.168.1.164	TCP	60	443 → 55751 [FIN, ACK] Seq=1 Ack=1 Win=63 Len=0
239	3.376977	104.18.10.207	192.168.1.164	TCP	93	[TCP Out-Of-Order] 443 → 55751 [PSH, ACK] Seq=4294967234 Ack=1 Win=63 Len=39
240	3.376977	104.18.10.207	192.168.1.164	TCP	78	[TCP Out-Of-Order] 443 → 55751 [PSH, ACK] Seq=4294967273 Ack=1 Win=63 Len=24
241	3.377091	192.168.1.164	104.18.10.207	TCP	54	55751 → 443 [ACK] Seq=1 Ack=4294967234 Win=1025 Len=0
242	3.377173	192.168.1.164	104.18.10.207	TCP	54	55751 → 443 [ACK] Seq=1 Ack=2 Win=1025 Len=0
243	3.377587	192.168.1.164	104.18.10.207	TCP	54	55751 → 443 [FIN, ACK] Seq=1 Ack=2 Win=1025 Len=0
256	3.445887	104.18.10.207	192.168.1.164	TCP	60	443 → 55751 [ACK] Seq=2 Ack=2 Win=63 Len=0
965	15.172665	192.168.1.164	74.125.130.188	TCP	55	[TCP segment of a reassembled PDU]
969	15.242638	74.125.130.188	192.168.1.164	TCP	66	5228 → 54015 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
1474	23.638719	192.168.1.6	192.168.1.5	TCP	66	56083 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1631	24.653000	192.168.1.6	192.168.1.5	TCP	66	[TCP Retransmission] [TCP Retransmission] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Frame 969: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{9E87167D-EFAF-4EBC-A1C3-518F9CFC43FD}, id 0

Ethernet II, Src: zte\_e9:f0:96 (10:10:81:e9:f0:96), Dst: Giga-Byt\_5b:2a:b4 (1c:1b:0d:5b:2a:b4)

Internet Protocol Version 4, Src: 74.125.130.188, Dst: 192.168.1.164

Transmission Control Protocol, Src Port: 5228, Dst Port: 54015, Seq: 1, Ack: 2, Len: 0

Source Port: 5228

Destination Port: 54015

[Stream index: 1]

[Conversation completeness: Incomplete (12)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1158115912

[Next Sequence Number: 1 (relative sequence number)]

0000 1c 1b 0d 5b 2a b4 10 10 81 e9 f0 96 08 00 45 80 ...[\*... ..E:

0010 00 34 af e0 00 00 68 06 12 de 4a 7d 82 bc c0 a8 ...4...h...}]...

0020 01 a4 14 6c d2 ff 45 07 72 48 77 84 19 ec 80 10 ...l...E...rHw....

0030 01 09 96 22 00 00 01 01 05 0a 77 84 19 eb 77 84 ...".... .w...w.

0040 19 ec ..