Practical 7 : Understand basic networking concept using Wireshark.

Software & Hardwere Requirements:
Wireshark

Knowledge requirements: basic knowledge of wireshark softwere…

Question:

Q-1. What are the features in Wireshark ?

Answer :
The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

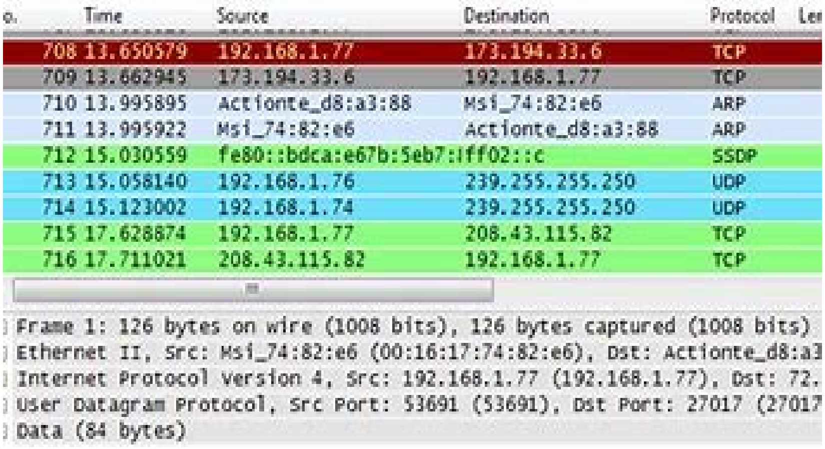
Theory:

Wireshark is a free application that allows you to capture and view the data traveling back and forth on your network, providing the ability to drill down and read the contents of each packet – filtered to meet your specific needs. It is commonly utilized to troubleshoot network problems as well as to develop and test software. This open- source protocol analyzer is widely accepted as the industry standard, winning its fair share of awards over the years.

Originally known as Ethereal, Wireshark features a user-friendly interface that can display data from hundreds of different protocols on all major network types. These data packets can be viewed in real-time or analyzed offline, with dozens of capture/trace file formats supported including CAP and ERF. Integrated decryption tools allow you to view encrypted packets for several popular protocols such as WEP and WPA/WPA2.

To begin capturing packets, first select one or more of these networks by clicking on your choice(s) and using the Shift or Ctrl keys if you'd like to record data from multiple networks simultaneously. Once a connection type is selected for capturing purposes, its background will be shaded in either blue or gray. Click on Capture from the main menu, located towards the top of the Wireshark interface. When the drop-down menu appears, select the Start option.
You can also initiate packet capturing via one of the following shortcuts.
Keyboard: Press Ctrl + E

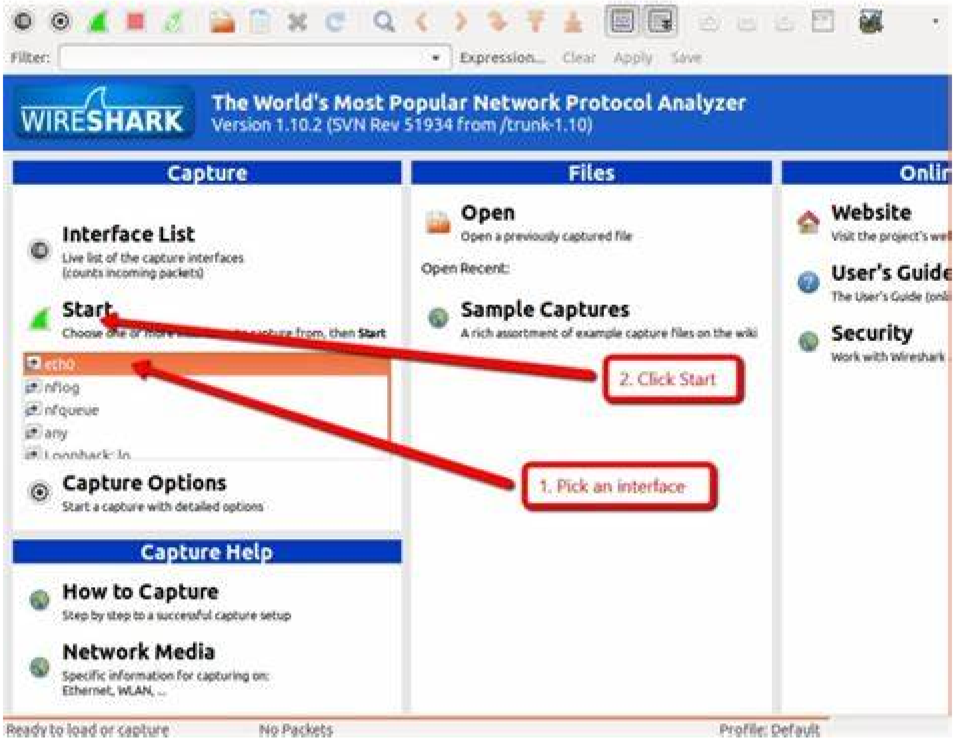
Mouse: To begin capturing packets from one particular network, simply double-click on its name
Toolbar: Click on the blue shark fin button, located on the far left-hand side of the Wireshark toolbar



```
o.   Time          Source                  Destination          Protocol  Le
708 13.650579   192.168.1.77            173.194.33.6            TCP
709 13.662945   173.194.33.6            192.168.1.77            TCP
710 13.995895   Actionte_d8:a3:88       Msi_74:82:e6            ARP
711 13.995922   Msi_74:82:e6            Actionte_d8:a3:88       ARP
712 15.030559   fe80::bdca:e67b:5eb7:ff02::c                    SSDP
713 15.058140   192.168.1.76            239.255.255.250         UDP
714 15.123002   192.168.1.74            239.255.255.250         UDP
715 17.628874   192.168.1.77            208.43.115.82           TCP
716 17.711021   208.43.115.82           192.168.1.77            TCP

Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits)
Ethernet II, Src: Msi_74:82:e6 (00:16:17:74:82:e6), Dst: Actionte_d8:a3
Internet Protocol Version 4, Src: 192.168.1.77 (192.168.1.77), Dst: 72.
User Datagram Protocol, Src Port: 53691 (53691), Dst Port: 27017 (27017
Data (84 bytes)
```

The live capture process will now begin, with packet details displayed in the Wireshark window as they are recorded. Perform one of the actions below to stop capturing.

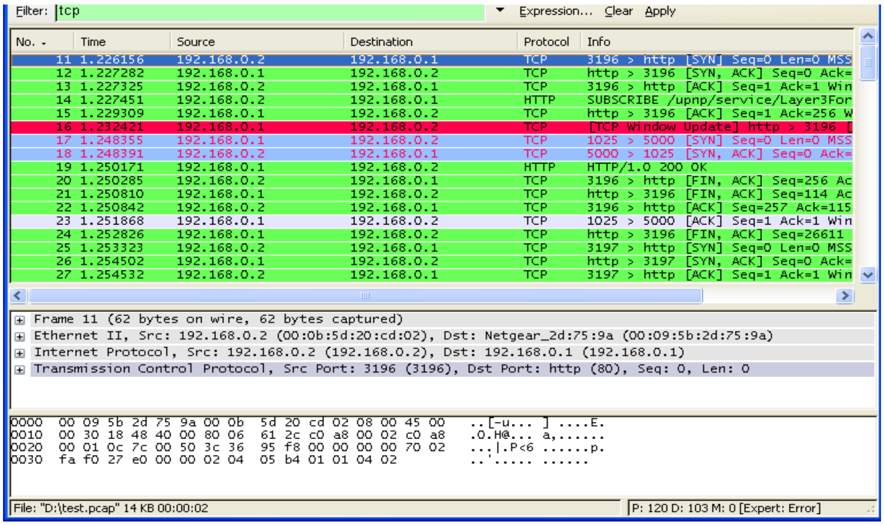
1) **Keyboard: Press Ctrl + E**
2) **Toolbar: Click on the red stop button, located next to the shark fin on the Wireshark toolbar**


Filter:
Expression...
Clear
Apply
Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.2 (SVN Rev 51934 from /trunk-1.10)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
echo
nflog
nfqueue
any
Loopback: lo
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (online)
Security
Work with Wireshark ...
2. Click Start
1. Pick an interface
Ready to load or capture
No Packets
Profile: Default

<u>Color Coding:</u>

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.



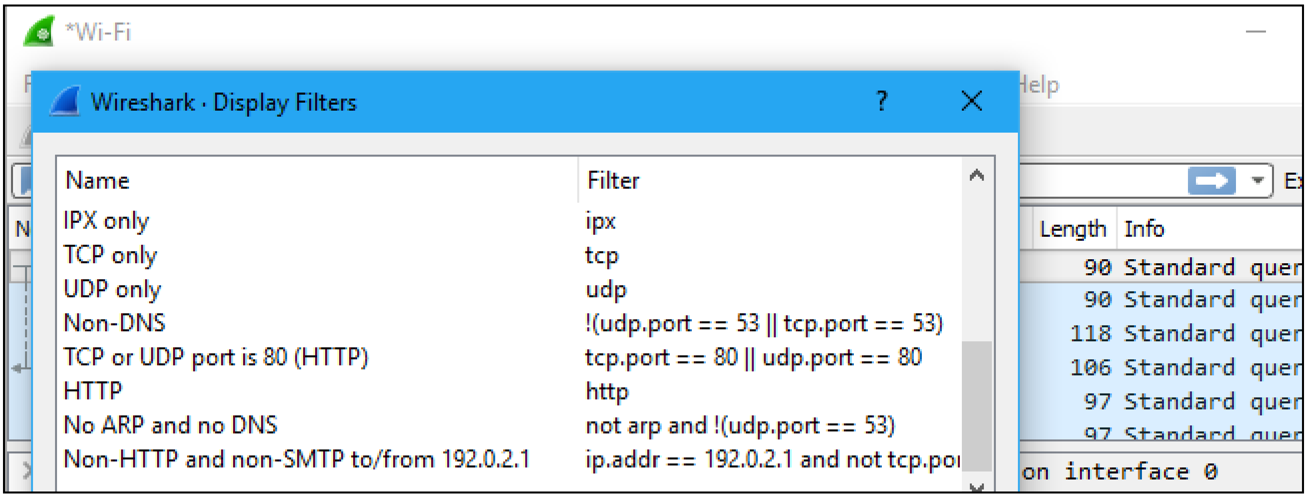
```
No. -  Time       Source        Destination   Protocol  Info
    11 1.226156   192.168.0.2   192.168.0.1   TCP       3196 > http [SYN] Seq=0 Len=0 MSS
    12 1.227282   192.168.0.1   192.168.0.2   TCP       http > 3196 [SYN, ACK] Seq=0 Ack=
    13 1.227325   192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=1 Ack=1 Win
    14 1.227451   192.168.0.2   192.168.0.1   HTTP      SUBSCRIBE /upnp/service/Layer3For
    15 1.229309   192.168.0.1   192.168.0.2   TCP       http > 3196 [ACK] Seq=1 Ack=256 W
    16 1.232421   192.168.0.1   192.168.0.2   TCP       [TCP Window Update] http > 3196 [
    17 1.248355   192.168.0.1   192.168.0.2   TCP       1025 > 5000 [SYN] Seq=0 Len=0 MSS
    18 1.248391   192.168.0.2   192.168.0.1   TCP       5000 > 1025 [SYN, ACK] Seq=0 Ack=
    19 1.250171   192.168.0.1   192.168.0.2   HTTP      HTTP/1.0 200 OK
    20 1.250285   192.168.0.2   192.168.0.1   TCP       3196 > http [FIN, ACK] Seq=256 Ac
    21 1.250810   192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=114 Ac
    22 1.250842   192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=257 Ack=115
    23 1.251868   192.168.0.1   192.168.0.2   TCP       1025 > 5000 [ACK] Seq=1 Ack=1 Win
    24 1.252826   192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=26611
    25 1.253323   192.168.0.2   192.168.0.1   TCP       3197 > http [SYN] Seq=0 Len=0 MSS
    26 1.254502   192.168.0.1   192.168.0.2   TCP       http > 3197 [SYN, ACK] Seq=0 Ack=
    27 1.254532   192.168.0.2   192.168.0.1   TCP       3197 > http [ACK] Seq=1 Ack=1 Win

⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0

0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......

File: "D:\test.pcap" 14 KB 00:00:02          P: 120 D: 103 M: 0 [Expert: Error]
```

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 number 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.



Name	Filter
IPX only	ipx
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.poı

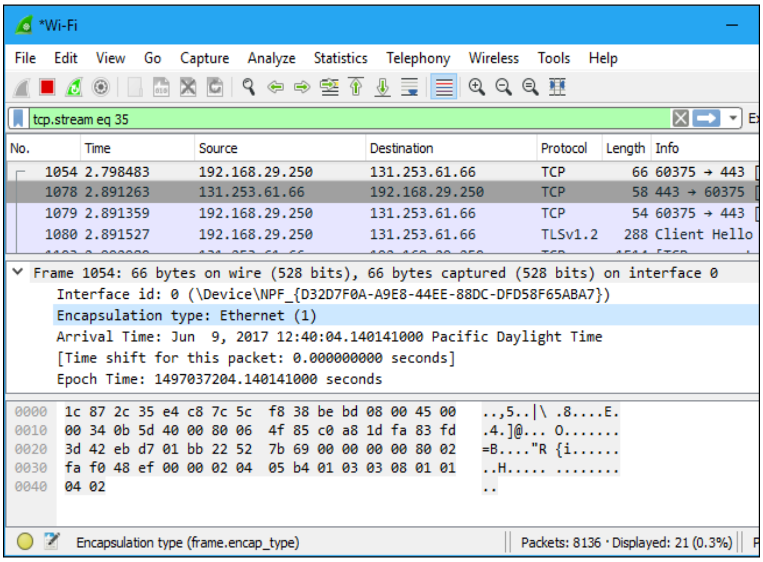
```
 90 Standard quer
 90 Standard quer
118 Standard quer
106 Standard quer
 97 Standard quer
 97 Standard quer
on interface 0
```

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.

Inspecting Packets:

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



tcp.stream eq 35

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

```
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
```

```
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                                              ..
```

Encapsulation type (frame.encap_type)   Packets: 8136 · Displayed: 21 (0.3%)

CONCLUSION:

We study and Understand basic networking concept using Wireshark.
And we perform this practical practically also…