Name : Khushi Nitinkumar Patel
PRN : 2020BTECS00037
Batch : S3

1. Study different Internet Standards and write down note on each.

- An internet standard is a specification that has been approved by the Internet Engineering Task Force(IETF).
- Such a standard, helps to promote a consistent and universal use of the internet worldwide.
- In simple words ,these are technically matured standards which define protocols and formats of messages.

Organization of internet standards-

I.Internet Engineering Task Force (IETF)

The organization is open standard, with no membership and development of standards open to all. IETF formulates, publish and regulates internet standards related to TCP/IP. IETF document is freely available on internet.

II.Internet Society (ISOC)

The organization is found in 1992. It supports technical development of internet and conduct activities on standards, education , access and policies.

III. Internet Architecture Board (IAB)

IAB is one of the committee of IETF and an advisory body of ISOC. The main board of the organization consist of researchers and technology professionals for developing technical aspects. It manages the following task – Supervise architectural standards of different networks and IP, Review issues related to Internet Standards, Provide guidance to IETF and ISOC.

IV.Internet Research Task Force (IRTF)

IRTF is composed of a number of research groups whose overall objective is focused on the long-term development of the Internet. It is a parallel organization to IETF. The participants are individual contributors who have long-term memberships. The research groups work on Internet protocols, applications, technology and overall architecture.

V. World Wide Web Consortium (W3C)

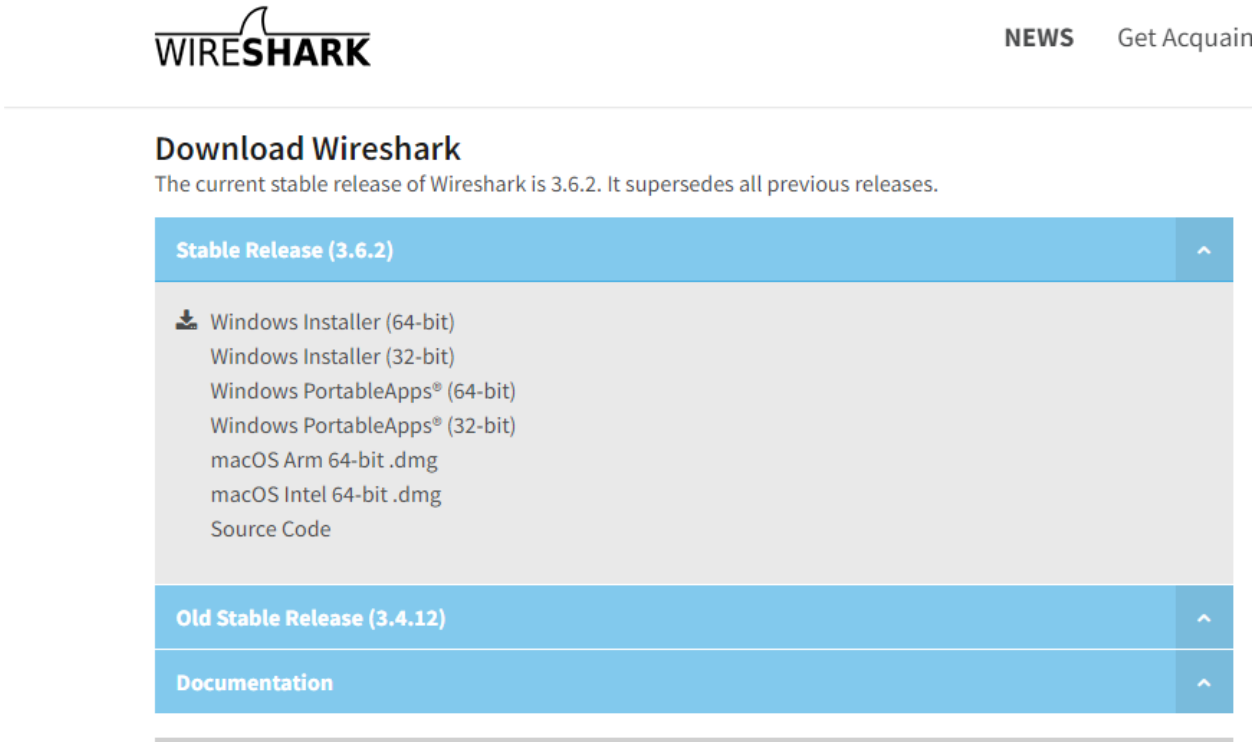
It is the foremost international standards organization for the world wide web (www). It is a community of a large number of member organizations, who work together to develop web standards and improve web services. Some of the popular standards developed by W3C are HTML, HTTP, XML, CSS, etc.

Internet Standard goals –

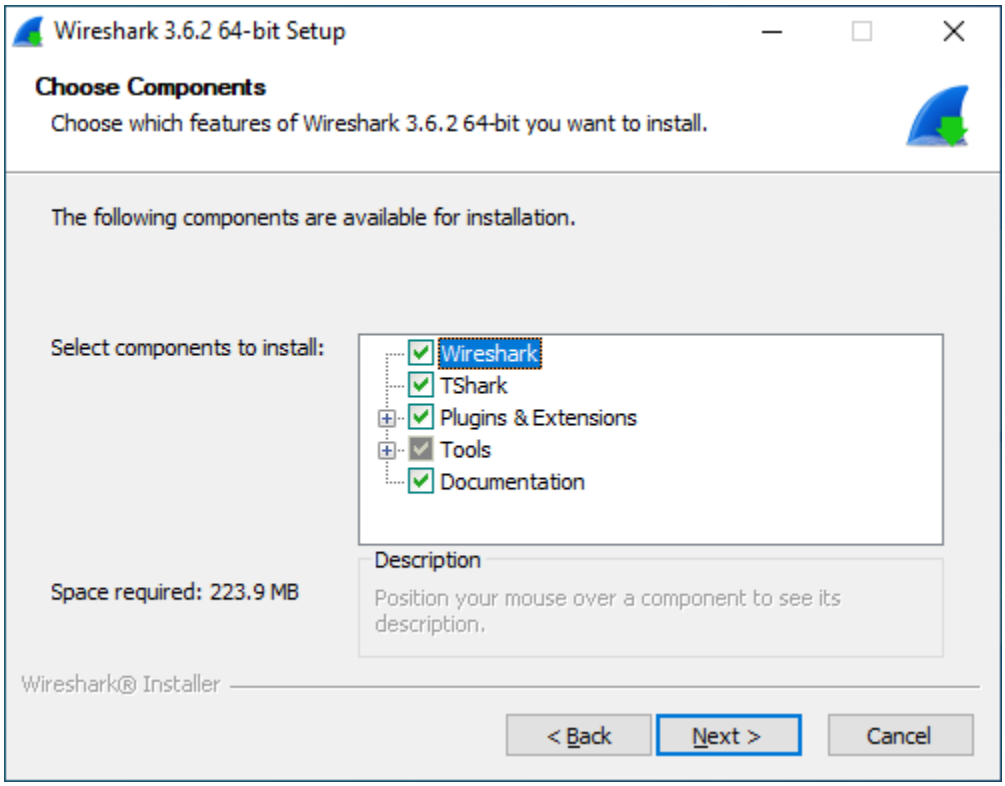
- High Quality
- Prior implementation and testing
- Open and fair
- Timeliness

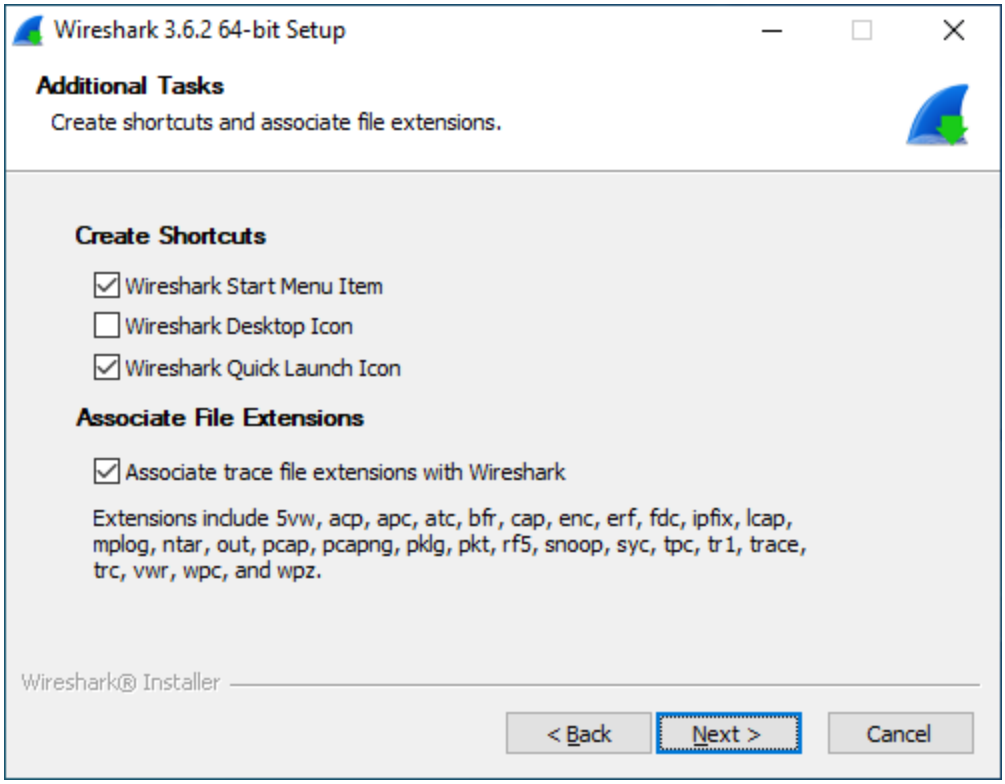
2. Study and install Wireshark: add screenshot of each step of installation with description. Write down information of Wireshark and use of its functionalities in networking study.

1. Go to the browser and search wireshark download and choose your respective operating system and click on download.

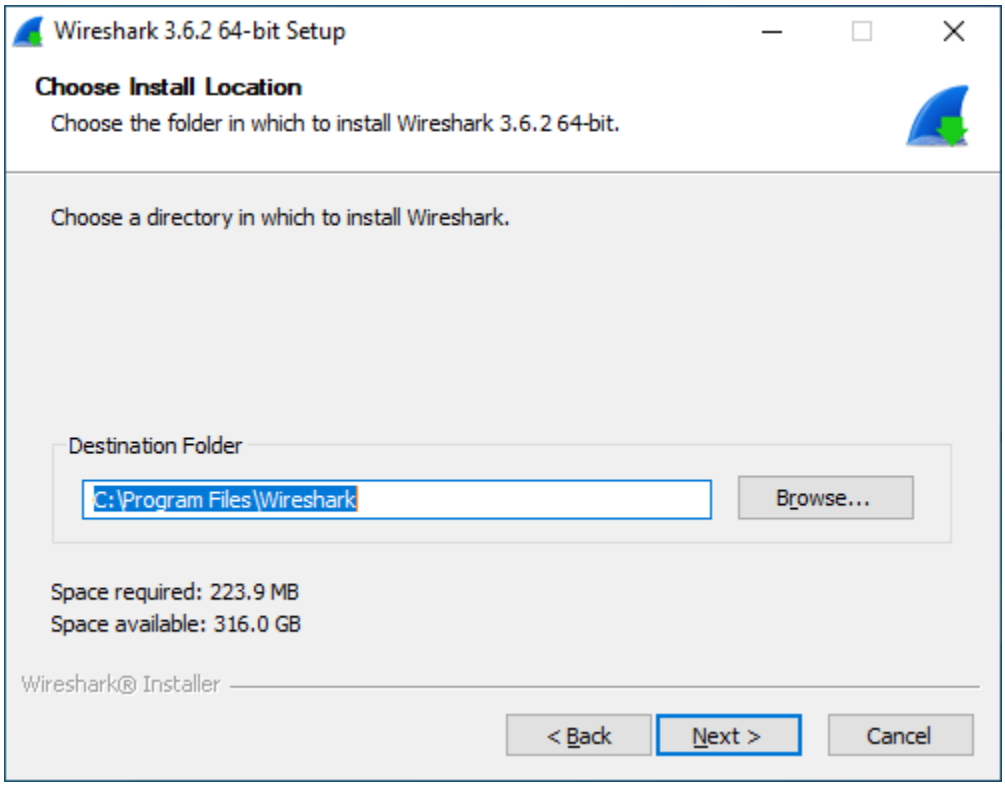


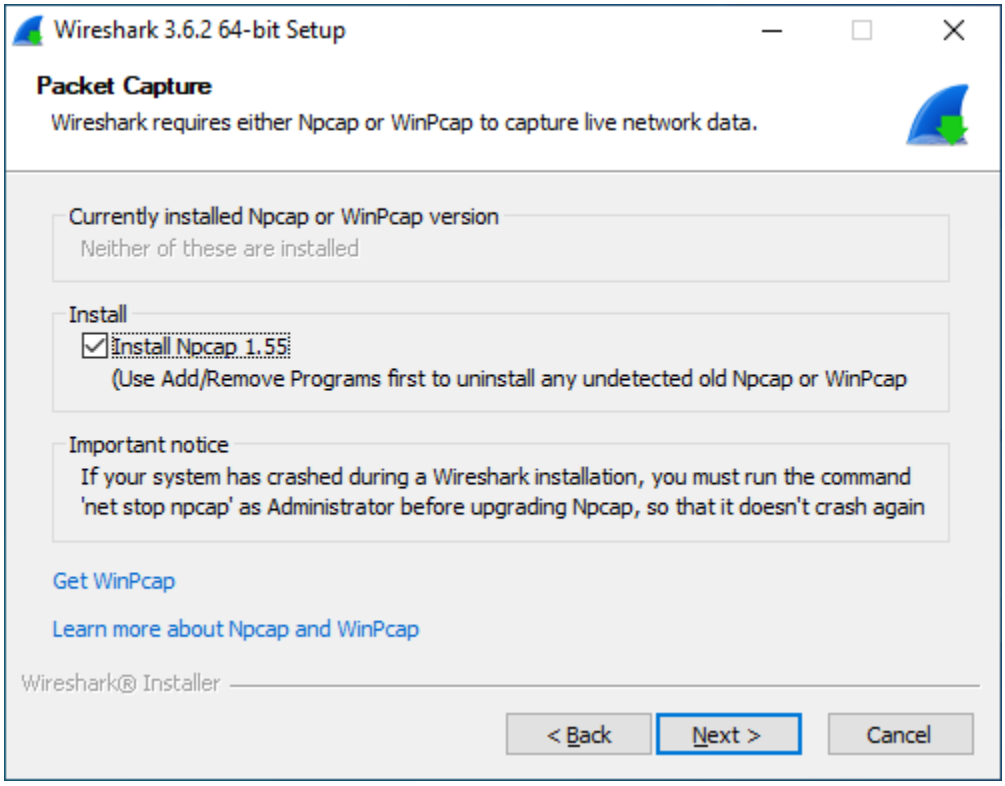
2.Next step is to install wire shark on your operating system.

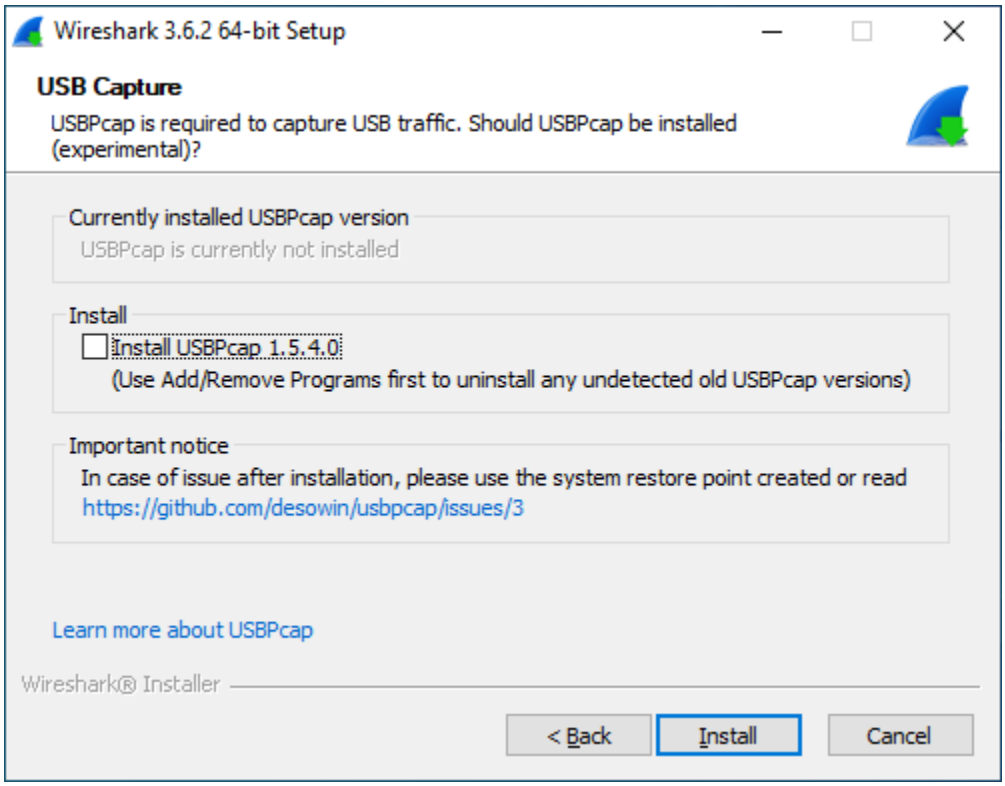




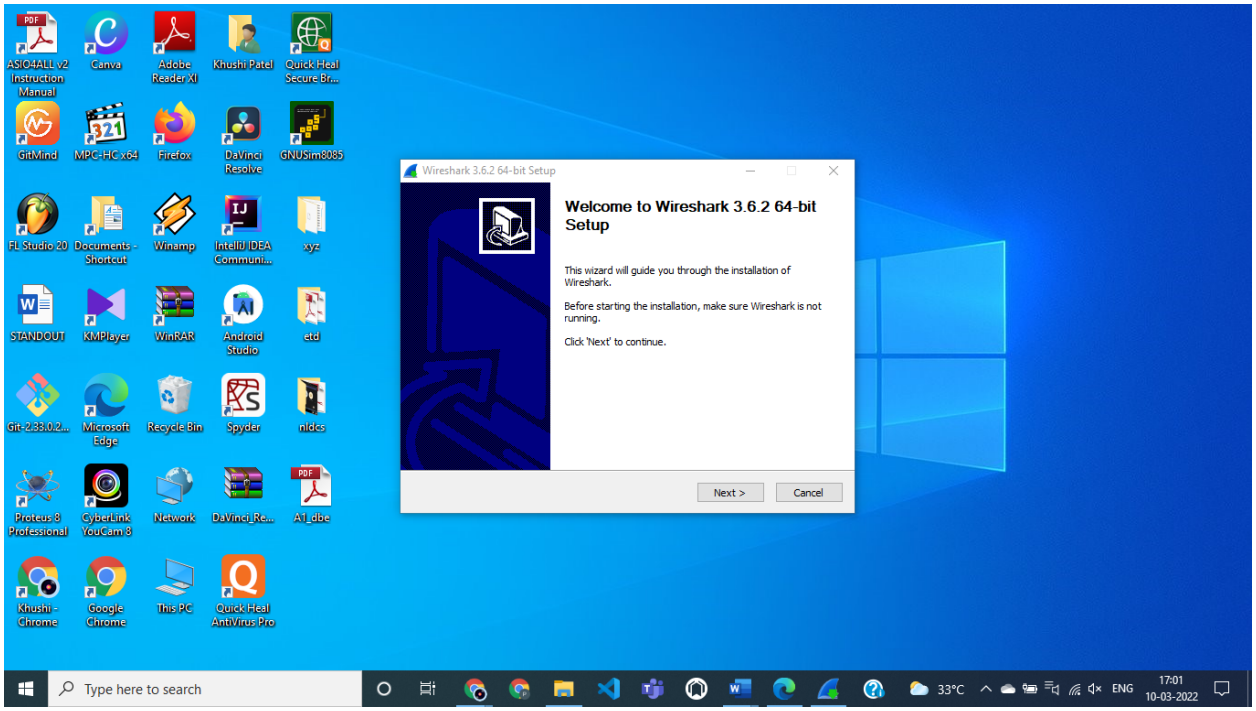
3.Choose the location where you would like to install wireshark.




Wireshark 3.6.2 64-bit Setup
Packet Capture
Wireshark requires either Npcap or WinPcap to capture live network data.
Currently installed Npcap or WinPcap version
Neither of these are installed
Install
Install Npcap 1.55
(Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap
Important notice
If your system has crashed during a Wireshark installation, you must run the command 'net stop npcap' as Administrator before upgrading Npcap, so that it doesn't crash again
Get WinPcap
Learn more about Npcap and WinPcap
Wireshark® Installer
< Back
Next >
Cancel


Wireshark 3.6.2 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
Learn more about USBPcap
Wireshark® Installer
< Back
Install
Cancel

4.Wireshark is successfully installed on your Operating system.



Wireshark

-Wireshark is an open source software that analyzes the network packets.

-Wireshark captures packets and lets you examine their content.

-It tries to find the local interface on your pc and if you want to analyze a packet, you need to select an interface.

-It can capture traffic from different network media types including Ethernet, Wireless LAN,Bluetooth, USB,etc.

-let’s choose the wi-fi interface to analyze the packets.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	119.201.83.206	192.168.220.96	TCP	54	6881 → 61575 [ACK] Seq=1 Ack=1 Win=4090 Len=0
2	0.054417	2600:1700:16a0:b100…	2401:4900:54f4:9522…	UDP	166	6881 → 6881 Len=104
3	0.054417	2600:1700:16a0:b100…	2401:4900:54f4:9522…	UDP	166	6881 → 6881 Len=104
4	0.055018	2401:4900:54f4:9522…	2600:1700:16a0:b100…	UDP	481	6881 → 6881 Len=419
5	0.055336	2401:4900:54f4:9522…	2600:1700:16a0:b100…	UDP	481	6881 → 6881 Len=419
6	0.073474	2001:448a:4023:2739…	2401:4900:54f4:9522…	UDP	82	64450 → 6881 Len=20
7	0.074015	2401:4900:54f4:9522…	2001:448a:4023:2739…	UDP	82	6881 → 64450 Len=20
8	0.263302	192.168.220.96	45.71.85.16	TCP	66	61521 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	0.263302	192.168.220.96	49.204.114.136	TCP	66	61529 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C64A5278-D1B9-4172-841F-FD251C390E6A}, id 0
> Ethernet II, Src: a2:ef:56:29:bb:87 (a2:ef:56:29:bb:87), Dst: AzureWav_49:a1:6d (48:e7:da:49:a1:6d)
> Internet Protocol Version 4, Src: 119.201.83.206, Dst: 192.168.220.96
> Transmission Control Protocol, Src Port: 6881, Dst Port: 61575, Seq: 1, Ack: 1, Len: 0

0000  48 e7 da 49 a1 6d a2 ef  56 29 bb 87 08 00 45 00   H··I·m·· V)····E·
0010  00 28 00 00 40 00 33 06  df 2f 77 c9 53 ce c0 a8   ·(··@·3· ·/w·S···
0020  dc 60 1a e1 f0 87 d1 93  0c 65 c5 2d 72 4e 50 10   ·`····· ·e··-rNP·
0030  0f fa 16 5c 00 00                                  ···\··
```

Wi-Fi: <live capture in progress> | Packets: 4335 · Displayed: 4335 (100.0%) | Profile: Default

Type here to search | 38°C | ENG | 08:20 17-03-2022

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
650	17.465501	192.168.220.96	139.47.37.194	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61596 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
651	17.465511	192.168.220.96	170.51.201.208	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61603 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
652	17.465560	192.168.220.96	114.125.88.65	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61597 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
653	17.465566	192.168.220.96	185.57.29.133	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61605 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
654	17.465587	192.168.220.96	186.176.250.57	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61611 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
655	17.465655	192.168.220.96	181.37.68.97	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61607 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
656	17.465691	192.168.220.96	186.232.206.23	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 61612 → 6881 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
657	17.482758	142.250.4.113	192.168.220.96	TCP	66	443 → 61253 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
658	17.636572	2401:4900:54f4:9522…	2404:6800:4003:c03:…	TCP	75	61252 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C64A5278-D1B9-4172-841F-FD251C390E6A}, id 0
> Ethernet II, Src: a2:ef:56:29:bb:87 (a2:ef:56:29:bb:87), Dst: AzureWav_49:a1:6d (48:e7:da:49:a1:6d)
> Internet Protocol Version 4, Src: 119.201.83.206, Dst: 192.168.220.96
> Transmission Control Protocol, Src Port: 6881, Dst Port: 61575, Seq: 1, Ack: 1, Len: 0

0000  48 e7 da 49 a1 6d a2 ef  56 29 bb 87 08 00 45 00   H··I·m·· V)····E·
0010  00 28 00 00 40 00 33 06  df 2f 77 c9 53 ce c0 a8   ·(··@·3· ·/w·S···
0020  dc 60 1a e1 f0 87 d1 93  0c 65 c5 2d 72 4e 50 10   ·`····· ·e··-rNP·
0030  0f fa 16 5c 00 00                                  ···\··
```

Wi-Fi: <live capture in progress> | Packets: 658 · Displayed: 658 (100.0%) | Profile: Default

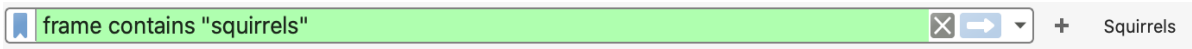
Type here to search | 38°C | ENG | 08:18 17-03-2022

Wireshark's main window

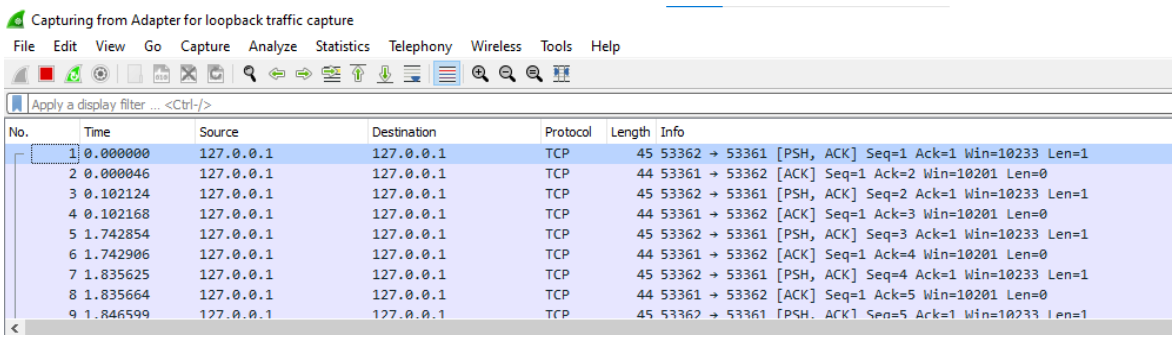
1. The menu is used to start actions.

2. The main toolbar provides quick access to frequently used items from the menu.

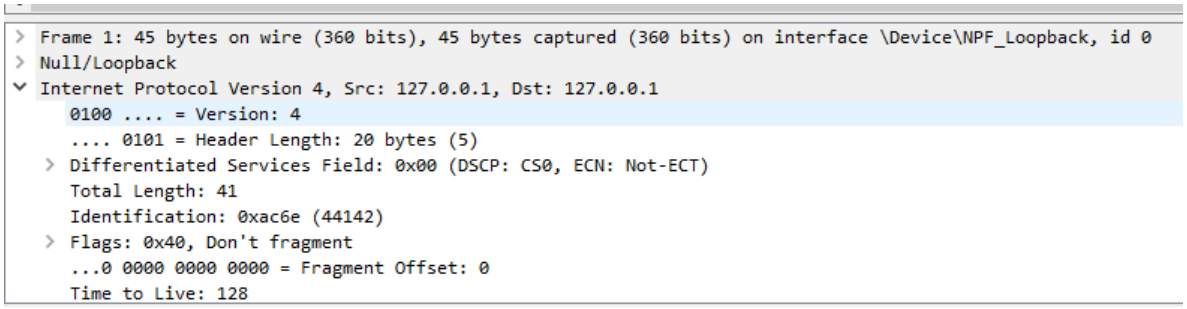
3. The filter toolbar allows users to set display filters to filter which packets are displayed.



4. The packet list pane displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.



5. The packet details pane displays the packet selected in the packet list pane in more detail.



6. The packet bytes pane displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.

```
0000  02 00 00 00 45 00 00 29  ac 6e 40 00 80 06 00 00   ····E··) ·n@·····
0010  7f 00 00 01 7f 00 00 01  d0 72 d0 71 50 8b ab c4   ····· ·r·qP···
0020  ab ef 9b 89 50 18 27 f9  a5 22 00 00 00            ····P·'· ·"···
```

Functionality of Wire Shark

i.Tcpdump is a packet analyzer which allows user to display other packets and TCP/IP packets, being transmitted and received over a network.Wire Shark is similar to Tcpdump.

ii.Wire Shark is also used to see traffic passing through a network.

iii. It can also see unicast traffic which is not sent to networks MAC address. Port mirroring method is used to analyse the network traffic.

Features of wireshark

i.Multi-platform software

ii.It has Standard three pane packet browser

iii. Performs inspection of many protocols

iv.It involves analysis and network traffic information, also live v. Captures raw USB traffic

vi. Useful in VoIP analysis