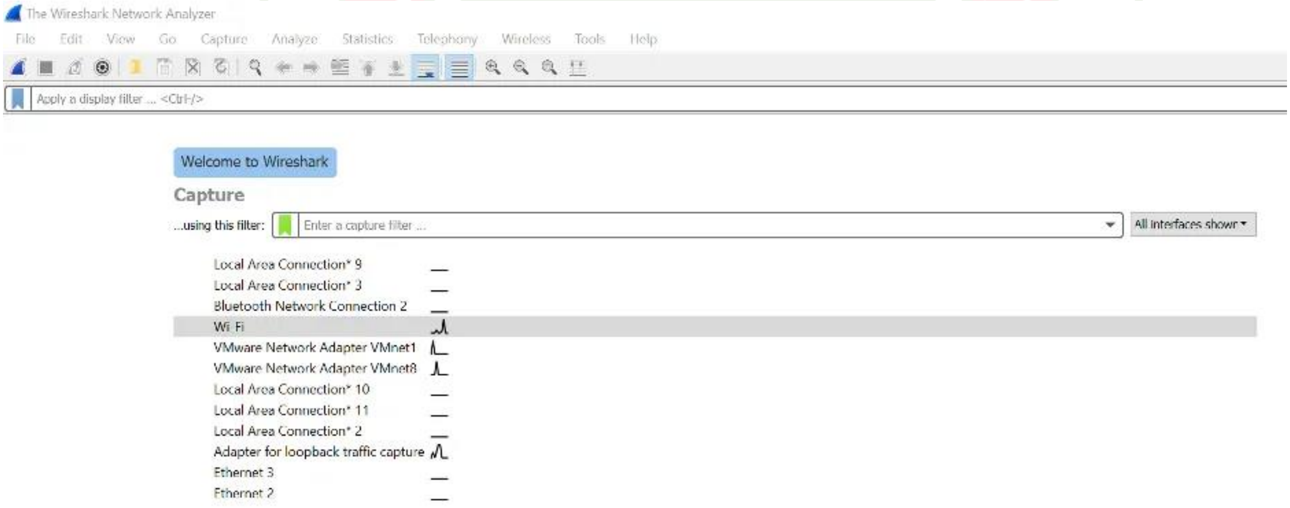
AIM: To demonstrate the use of Wireshark Packet Sniffer Software and capture the packets.

DESCRIPTION:

Originally known as Ethereal, Wireshark displays data from hundreds of different protocols on all major network types. Data packets can be viewed in real-time or analyzed offline. Wireshark supports dozens of capture/trace file formats, including CAP and ERF. Integrated decryption tools display the encrypted packets for several common protocols, including WEP and WPA/WPA2. Wireshark can be downloaded at no cost from the Wireshark Foundation website for both macOS and Windows. You'll see the latest stable release and the current developmental release. Unless you're an advanced user, download the stable version.

Installation setup:

During the Windows setup process, choose to install **WinPcap** or **Npcap** if prompted as these include libraries required for live data capture. You must be logged in to the device as an administrator to use Wireshark. In Windows 10, search for Wireshark and select **Run as administrator**. In macOS, right-click the app icon and select **Get Info**. In the **Sharing & Permissions** settings, give the admin **Read & Write** privileges.



Local Area Connection* 9
Local Area Connection* 3
Bluetooth Network Connection 2
Wi-Fi
VMware Network Adapter VMnet1
VMware Network Adapter VMnet8
Local Area Connection* 10
Local Area Connection* 11
Local Area Connection* 2
Adapter for loopback traffic capture
Ethernet 3
Ethernet 2

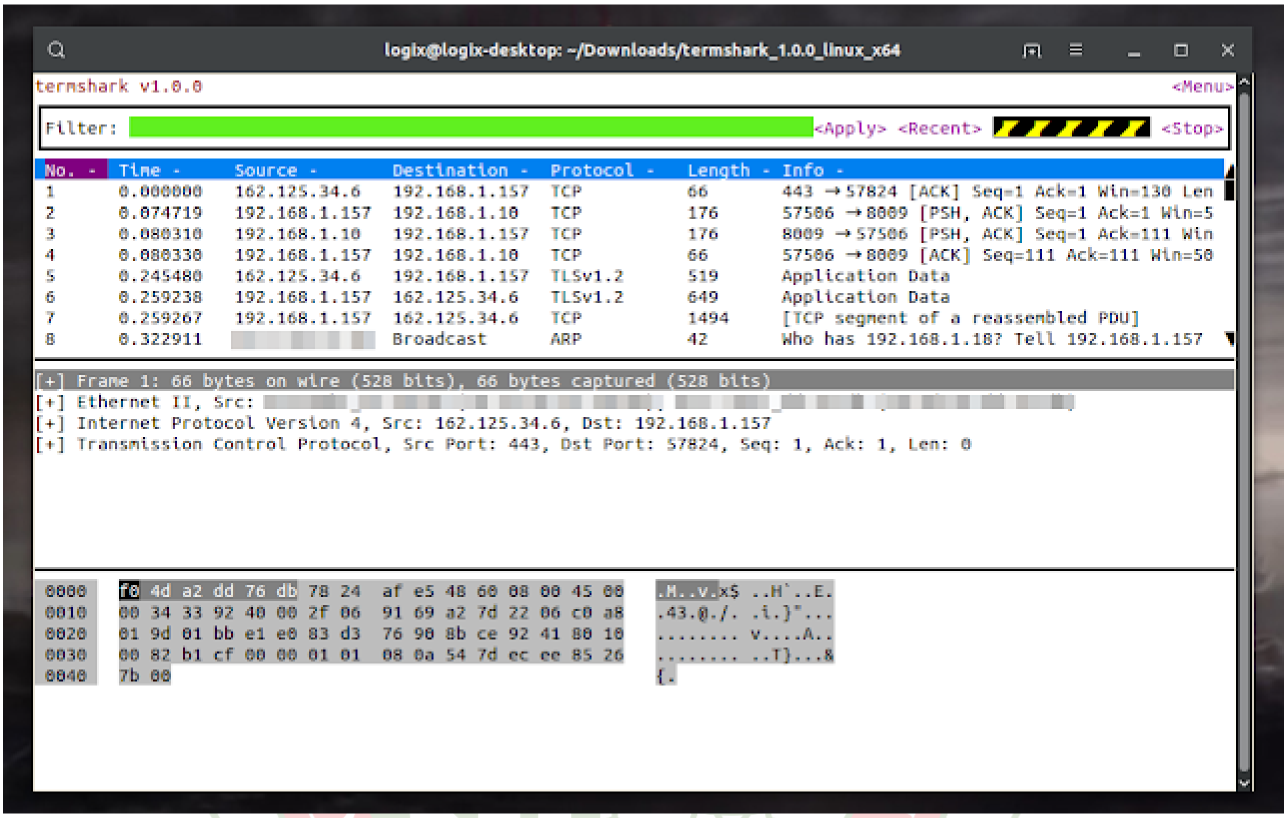
How to Capture Data Packets With Wireshark

When you launch Wireshark, a welcome screen lists the available network connections on your current device. Displayed to the right of each is an EKG-style line graph that represents live traffic on that network.

To begin capturing packets with Wireshark:

1. Select one or more of networks, go to the menu bar, then select **Capture**.
2. In the **Wireshark Capture Interfaces** window, select **Start**.
3. Select **File** > **Save As** or choose an **Export** option to record the capture.

4. To stop capturing, press **Ctrl+E**. Or, go to the Wireshark toolbar and select the red **Stop** button that's located next to the shark fin.



```
No. -  Time -     Source -        Destination -   Protocol -   Length -  Info -
1      0.000000   162.125.34.6    192.168.1.157   TCP          66        443 → 57824 [ACK] Seq=1 Ack=1 Win=130 Len
2      0.074719   192.168.1.157   192.168.1.10    TCP          176       57506 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=5
3      0.080310   192.168.1.10    192.168.1.157   TCP          176       8009 → 57506 [PSH, ACK] Seq=1 Ack=111 Win
4      0.080330   192.168.1.157   192.168.1.10    TCP          66        57506 → 8009 [ACK] Seq=111 Ack=111 Win=50
5      0.245480   162.125.34.6    192.168.1.157   TLSv1.2      519       Application Data
6      0.259238   192.168.1.157   162.125.34.6    TLSv1.2      649       Application Data
7      0.259267   192.168.1.157   162.125.34.6    TCP          1494      [TCP segment of a reassembled PDU]
8      0.322911   [redacted]      Broadcast       ARP          42        Who has 192.168.1.18? Tell 192.168.1.157

[+] Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
[+] Ethernet II, Src: [redacted]
[+] Internet Protocol Version 4, Src: 162.125.34.6, Dst: 192.168.1.157
[+] Transmission Control Protocol, Src Port: 443, Dst Port: 57824, Seq: 1, Ack: 1, Len: 0

0000   f0 4d a2 dd 76 db 78 24  af e5 48 60 08 00 45 00   .M..v.x$ ..H`..E.
0010   00 34 33 92 40 00 2f 06  91 69 a2 7d 22 06 c0 a8   .43.@./. .i.}"...
0020   01 9d 01 bb e1 e0 83 d3  76 90 8b ce 92 41 80 10   ........ v....A..
0030   00 82 b1 cf 00 00 01 01  08 0a 54 7d ec ee 85 26   ........ ..T}...&
0040   7b 00                                              {.
```

How to View and Analyze Packet Contents

The captured data interface contains three main sections:

- The packet list pane (the top section)
- The packet details pane (the middle section)
- The packet bytes pane (the bottom section)

Packet Details

- The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.