WIRESHARK: A NETWORK PROTOCOL ANALYZER

WireShark is a free and open-source network protocol analyzer that captures and displays network traffic in real time. It is the most widely used packet sniffer globally and is compatible with Windows, Mac, Unix, and Linux systems.

Download and Install Wireshark…

Wireshark is available for free download on both Mac and Windows. Get it here. https://www.wireshark.org/download.html

- Open the application.

- Go to the 'Capture' section and choose your network interface:

Ethernet: en0
Wi-Fi: en1
Loopback: io0

- **Packet Capture:** Wireshark captures network packets, allowing users to inspect the raw data transmitted over the network. This includes data from protocols like TCP, UDP, HTTP, and more.
- **Real-time Monitoring:** Wireshark provides real-time monitoring of network traffic, enabling users to identify anomalies, diagnose network issues, and detect suspicious activity as it happens.
- **Protocol Analysis:** It can decode and analyze a wide range of network protocols, offering insights into how data is structured and exchanged between devices.
- **Deep Inspection:** Wireshark offers the ability to drill down into packets to view payload data, revealing the actual content of network communications, which is vital for troubleshooting and security investigations.
- **Filters and Search:** Users can apply filters and search functions to pinpoint specific packets, helping to focus on relevant network traffic and incidents.
- **Export and Reporting:** Wireshark allows for the export of captured data in various formats, making it easy to share findings and generate reports for further analysis.
- **One of the most useful display filters is:** ip.src==IP-address and ip.dst==IP-address

Wireshark commands

eq or ==	Equal	ip.dest == 192.168.1.1
ne or !=	Not equal	ip.dest != 192.168.1.1
gt or >	Greater than	frame.len > 10
it or <	less than	frame.len < 10
ge or >=	Greater than or equal	frame.len >= 10
le or <=	Less than or equal	frame.len <= 10

- https://www.youtube.com/watch?v=qTaOZrDnMzQ
- https://www.youtube.com/watch?v=lb1Dw0elw0Q

Use Wireshark when:

- a device not working on your network

- Phishing Investigation needed

- Need to improve and increase your bandwidth

- **Wireshark Capture Filters Include:**

  - host IP-address: This filter limits the captured traffic to and from the IP address
  - net 192.168.0.0/24: This filter captures all traffic on the subnet
  - dst host IP-address: Capture packets sent to the specified host
  - port 53: Capture traffic on port 53 only
  - port not 53 and not arp: Capture all traffic except DNS and ARP traffic