Wireshark

Wireshark is a free and open-source packet analyzer.

It is used for traffic monitor and network troubleshooting and analysis.

It captures network traffic on the local network and stores that data for offline analysis

Purposes

Network administrators use it to *troubleshoot network problems*

Network security engineers use it to *examine security problems*

QA engineers use it to *verify network applications*

Developers use it to *debug protocol implementations*

People use it to *learn network protocol* internals

Feature

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solarisand many others
- Captured network data can be browsed via a GUI
- The most powerful display filters in the industry
- Coloring rules can be applied to the packet list for quick, intuitive analysis

Wireshark Filters

Filters allow you to view the capture the way you need to see it so you can troubleshoot the issues

Wireshark Capture Filters

Capture filters limit the captured packets by the filter. Meaning if the packets don’t match the filter, Wireshark won’t save them.

Ex:

host IP-*address*: this filter limits the capture to traffic to and from the IP address

Wireshark Display Filters

Wireshark Display Filters change the view of the capture during analysis. After you have stopped the packet capture, you use display filters to narrow down the packets in the Packet List so you can troubleshoot your issue.

Ex:

ip.src==*IP-address* and ip.dst==*IP-address*

Wireshark Promiscuous Mode

By default, Wireshark only captures packets going to and from the computer where it runs.

By checking the box to run Wireshark in Promiscuous Mode in the Capture Settings, you can capture most of the traffic on the LAN.

What Wireshark is not

Here are some things Wireshark does not provide:

Wireshark isn’t an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things.


Wireshark Is A Safe Tool Used By:
Government agencies
Educational institutions
Corporations
Small businesses
Non-profits
VARONIS

More Info

https://www.wireshark.org/docs/wsug_html_chunked/index.html

https://www.wireshark.org/faq.html

Sniff Login details from Webpages

Http Protocol (GET AND POST)

Https Protocol

FTP

SSH

http.request.method==“GET“

http.request.method=="POST"

FTP

Downloads the Sample

https://wiki.wireshark.org/SampleCaptures