**WIRESHARK VS TCPDUMP**

|  |  |  |
| --- | --- | --- |
|  | Wireshark | TCPDump |
| CLI | YES | YES |
| GUI | YES | NO |
| LINUX / UNIX | YES | YES |
| Windows | YES | Requires WinPcap / Npcap Vstudio with Cmake |
| NIC live packet capture | YES |  |
| Save packet data capture | YES | Incoming and outgoing packets. |
| Export packet captures to file formats | YES | YES |
| Filter packets based on criteria | YES | YES |
| Colorize packet data | YES | NO |
| Open Source | YES | YES |
| Capture | ethernet, wireless, bluetooth, USB. | Ethernet, wifi |
| Save capture to file | YES | YES |
| Compress | YES (Gzip) |  |
| Convert file formats | YES |  |
| Merge capture files | YES |  |

**Limitations**

|  |  |
| --- | --- |
| Wireshark | TCPDump |
| Most file formats don't capture no: packets dropped. | Limited in its analysis capabilities |
| Cannot sniff packets at switch level | Snapshot length 262144 bytes. |
|  | 200 packets per second on a switch. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**System Requirements**

|  |  |
| --- | --- |
| Wireshark | TCPDump |
| Windows 10, 11 Server 2016, 2019, 2022 |  |
| Universal C Runtime |  |
| 64 bit Intel or ARM CPU |  |
| 500MB RAM |  |
| 500MB HD space |  |
| 1280×1024 display resolution |  |
| Ethernet or 802.11 |  |

MAC 11 or later is supported for wireshark

TCPDump for windows is fully functional however, there are license restritions.

Usage

For Wireshark typically Security professionals use wireshark to analyze packets generated from on system to another. Allows to determine suspicious activity occurring on a network filtering from saved packet capture files. It also used to monitor network performance

For TCPDump is typically used to capture network traffic the capture file is then saved and used for analysis within wireshark.

Filtering

With Wireshark packet filtering is performed by invoking commands in the address bar for example if you want to filter a source ip address you would type src.ip == xxx.xxx.xxx.xxx

With tcpdump filtering is performed by specifying the type of netwok interface or port which is then written to a pcap file by invoking the -w filename.pcap file within the tcpdump syntax.

Analysis

TCPDump does not provide the capability of performing an analysis it allows to store a packet capture to a file which is then later used withing wireshark. Wireshark allows you to perform detailed inspection.

Capture

Data packet captures with TCPDump is used to capture simple traffic via a text based command line whilst Wireshark is for capturing packets which are much more complex which can be either command line or GUI.

Sources

<https://www.techtarget.com/searchnetworking/answer/Wireshark-vs-tcpdump-Whats-the-difference>

<https://labcommand.com/contrast-and-compare-wireshark-vs-tcpdump/>