

Wireshark

What is Wireshark?

Wireshark is a network protocol analyzer. It provides us the tool for capturing, displaying, and analyzing messages that are exchanged in a network.

Installation

The Wireshark package can be downloaded from <http://www.wireshark.org/download.html>. Download the latest version. Note that in some computing environments, such as MS Windows, it is necessary to install a separate file capture utility (WinPcap for MS Windows). This utility is included to the latest version of the Wireshark installation package.

Installing Wireshark for macOS can be found here:

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

Using Wireshark

Wireshark manual and introductory videos can be found here: <http://www.wireshark.org/docs/>

When you run the Wireshark program, the Wireshark graphical user interface will be displayed. Creating a packet capture file is straightforward. Once the Wireshark application (and packet capture utility) is installed, you simply start Wireshark and select the “Capture” menu option. Be sure that the interface option is set to whichever interface your computer uses if more than one is listed.

When you finish capturing packets, the information about the captured traffic will be shown on your screen:

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the selected packet (No. 410), which is an Ethernet II frame containing an Internet Protocol (IP) datagram.

No.	Time	Source	Destination	Protocol	Info
402	3.967169	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
403	3.967234	192.168.1.47	89.108.65.213	TCP	3858 > http [ACK] Seq=0 Ack=18876 Win=17424 Len=0
404	3.975027	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
405	3.982385	217.112.41.95	192.168.1.47	HTTP	Continuation of non-HTTP traffic
406	3.989246	217.112.41.95	192.168.1.47	HTTP	Continuation of non-HTTP traffic
407	3.989819	192.168.1.47	217.112.41.95	TCP	3050 > http [ACK] Seq=0 Ack=49568 Win=17424 Len=0
408	3.997703	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
409	4.005072	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
410	4.012951	87.255.33.6	192.168.1.47	HTTP	Continuation of non-HTTP traffic
411	4.020472	87.255.33.6	192.168.1.47	HTTP	Continuation of non-HTTP traffic
412	4.020983	192.168.1.47	87.255.33.6	TCP	4042 > http [ACK] Seq=0 Ack=51724 Win=17424 Len=0
413	4.028344	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
414	4.035608	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
415	4.035669	192.168.1.47	89.108.65.213	TCP	3973 > http [ACK] Seq=0 Ack=6004 Win=17424 Len=0
416	4.042517	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
417	4.050073	87.255.33.6	192.168.1.47	HTTP	Continuation of non-HTTP traffic
418	4.057493	87.255.33.6	192.168.1.47	HTTP	Continuation of non-HTTP traffic
419	4.057562	192.168.1.47	87.255.33.6	TCP	4042 > http [ACK] Seq=0 Ack=56628 Win=17424 Len=0
420	4.067851	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
421	4.075957	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
422	4.076027	192.168.1.47	89.108.65.213	TCP	3906 > http [ACK] Seq=0 Ack=6940 Win=17424 Len=0
423	4.083368	217.112.41.95	192.168.1.47	HTTP	Continuation of non-HTTP traffic
424	4.090722	217.112.41.95	192.168.1.47	HTTP	Continuation of non-HTTP traffic
425	4.090784	192.168.1.47	217.112.41.95	TCP	3050 > http [ACK] Seq=0 Ack=52272 Win=17424 Len=0
426	4.098643	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
427	4.106007	89.108.65.213	192.168.1.47	HTTP	Continuation of non-HTTP traffic
428	4.106073	192.168.1.47	89.108.65.213	TCP	3906 > http [ACK] Seq=0 Ack=6940 Win=17424 Len=0

Frame 410 (54 bytes on wire (4 bytes captured))
 Ethernet II, Src: Mikro-St-07:ff:10 (00:11:09:07:ff:10), Dst: westellt_43:59:97 (00:0f:db:43:59:97)
 Destination: westellt_43:59:97 (00:0f:db:43:59:97)
 Source: Mikro-St-07:ff:10 (00:11:09:07:ff:10)
 Type: IP (0x0800)
 Internet Protocol, Src: 192.168.1.47 (192.168.1.47), Dst: 89.108.65.213 (89.108.65.213)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 Total length: 40
 Identification: 0xd693 (54931)
 Flags: 0x04 (Don't Fragment)
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (0x06)
 Header checksum: 0xc723 [correct]
 Source: 192.168.1.47 (192.168.1.47)
 Destination: 89.108.65.213 (89.108.65.213)
 Transmission Control Protocol, Src Port: 3863 (3863), Dst Port: http (80), Seq: 0, Ack: 11616, Len: 0
 Source port: 3863 (3863)
 Destination port: http (80)
 Sequence number: 0 (relative sequence number)
 Acknowledgment number: 11616 (relative ack number)
 0000 00 0f db 43 59 97 00 11 09 07 ff 10 08 00 40 00 ..C...E
 0010 00 28 09 93 40 00 80 06 c7 23 c8 a8 03 21 59 6c .L.R...A...
 0020 41 05 0f 17 00 50 68 71 98 7e 5d b5 60 c4 50 10 A...Ph...P.
 0030 44 10 3f db 00 00 D...D...

The upper part of the screen shows the information about all packets transmitted or received by your device. You can use filters to display only specified patterns. When a packet is highlighted in the upper pane of the main window, the lower panes will show you more detailed information about a given packet. It will show each protocol layer of the selected packet: the physical layer frame, the Ethernet frame and its headers, the Internet Protocol datagram and its headers, Transport layer protocol datagram and its headers, and the Hypertext Transfer Protocol (HTTP) message. For each protocol, you can expand the information even further. For example, if you expand the IP Layer, you can see each field in the IP header including version, the header length, etc. The lowest part of the main window shows each byte of the data contained in the packet.