

Wireshark interface showing a packet capture of an HTTP session. The top pane displays a list of packets, with packet 5444 selected. The middle pane shows the details of the selected packet, including the HTTP request and response. The bottom pane displays the raw packet data in hexadecimal and ASCII.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.38

No. Time Source Destination Protocol Length Info

5444 281.210835088 192.168.1.38 192.168.1.38 HTTP 2416 HTTP/1.1 200 OK [application/vnd.ms-cab-compressed]

5445 281.210835160 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=11501 Ack=384139 Win=65280 Len=0

5446 281.212649634 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729021_d763cecf7414f49efc1533b056a3736d4f67e29.cab HTTP/1.1

5447 281.242399192 192.168.1.38 20 50 68 235 TCP 60 1937 - 443 [RST] ACK Seq=1251 Ack=384139 Win=0 Len=0

5451 281.408318490 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=386813 Ack=11751 Win=32768 Len=2674 [TCP PDU reassembled in 5457]

5454 281.408318687 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=386813 Ack=11751 Win=32768 Len=2674 [TCP PDU reassembled in 5457]

5455 281.408318708 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=11751 Ack=389487 Win=65280 Len=0

5456 281.408777161 192.168.1.38 192.168.1.38 TCP 1391 80 - 1952 [ACK] Seq=389487 Ack=1251 Win=32768 Len=1337 [TCP PDU reassembled in 5457]

5457 281.41286647 192.168.1.38 192.168.1.38 HTTP 1077 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5458 281.41286729 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=11751 Ack=389487 Win=65280 Len=0

5459 281.414261927 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729029_89c2df389c9f10f170163240414854a43ca7e.cab HTTP/1.1

5460 281.608463936 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=381847 Ack=12001 Win=32768 Len=2674 [TCP PDU reassembled in 5465]

5461 281.608463287 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12001 Ack=384521 Win=65280 Len=0

5462 281.612712407 192.168.1.38 192.168.1.38 TCP 1391 80 - 1952 [ACK] Seq=384521 Ack=12001 Win=32768 Len=1337 [TCP PDU reassembled in 5465]

5463 281.612712528 192.168.1.38 192.168.1.38 TCP 60 [TCP ACKed unseq. segment] 1952 - 80 [ACK] Seq=12001 Ack=389532 Win=65280 Len=0

5464 281.612712544 192.168.1.38 192.168.1.38 TCP 1391 [TCP Spurious Retransmission] 80 - 1952 [ACK] Seq=387195 Ack=12001 Win=32768 Len=1337 [TCP PDU reassembled in 5465]

5465 281.612712549 192.168.1.38 192.168.1.38 HTTP 1083 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5466 281.615105525 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12001 Ack=389559 Win=65280 Len=0

5467 281.616744562 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729019_5729d7b65f1853f9d58eece6aca6b42d5fa40.cab HTTP/1.1

5468 281.812434981 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=389559 Ack=12251 Win=32768 Len=2674 [TCP PDU reassembled in 5472]

5469 281.812435217 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=402233 Ack=12251 Win=32768 Len=2674 [TCP PDU reassembled in 5472]

5470 281.812435238 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12251 Ack=404907 Win=65280 Len=0

5471 281.813994351 192.168.1.38 192.168.1.38 TCP 1391 80 - 1952 [ACK] Seq=404907 Ack=1251 Win=32768 Len=1337 [TCP PDU reassembled in 5472]

5472 281.820429216 192.168.1.38 192.168.1.38 HTTP 1079 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5473 281.820429486 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12251 Ack=407269 Win=65280 Len=0

5474 281.822921626 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729018_2946b65cbb724c5da696f0833ed41b02ab3d97.cab HTTP/1.1

5475 282.017408263 192.168.1.38 192.168.1.38 HTTP 1391 [TCP Previous segment not captured] Continuation

5476 282.017408263 192.168.1.38 192.168.1.38 TCP 60 [TCP Dup ACK 5473#1] 1952 - 80 [ACK] Seq=12001 Ack=407269 Win=65280 Len=0 SLE=408066 SRE=411280

5477 282.017408263 192.168.1.38 192.168.1.38 HTTP 1391 Continuation

5478 282.022343439 192.168.1.38 192.168.1.38 TCP 74 [TCP Dup ACK 5473#2] 1952 - 80 [ACK] Seq=12001 Ack=407269 Win=65280 Len=0 SLE=411261 SRE=411280

5479 282.022343522 192.168.1.38 192.168.1.38 HTTP 1391 [TCP Previous segment not captured] Continuation

5480 282.035110967 192.168.1.38 192.168.1.38 TCP 60 [TCP ACKed unseq. segment] 1952 - 80 [ACK] Seq=12001 Ack=411280 Win=65280 Len=0 SLE=412617 SRE=413954

5481 282.035111157 192.168.1.38 192.168.1.38 TCP 1391 [TCP Spurious Retransmission] 80 - 1952 [ACK] Seq=407269 Ack=12001 Win=32768 Len=1337

5482 282.282946446 192.168.1.38 192.168.1.38 TCP 60 [TCP ACKed unseq. segment] 1952 - 80 [ACK] Seq=12001 Ack=413954 Win=65280 Len=0

5483 282.282946493 192.168.1.38 192.168.1.38 TCP 1391 [TCP Spurious Retransmission] 80 - 1952 [ACK] Seq=411280 Ack=12001 Win=32768 Len=1337

Frame 5485: 1081 bytes on wire (8648 bits), 1081 bytes captured (8648 bits) on interface eth0, id 0
Ethernet II, Src: Intel-Ed:53:fa (68:7a:64:ed:53:fa), Dst: VortexInfoTe:8:d6:c0 (4c:ea:14:a8:d6:c0)
Internet Protocol Version 4, Src: 192.168.1.38, Dst: 192.168.1.38
Transmission Control Protocol, Src Port: 1952, Dst Port: 80, Seq: 12001, Ack: 399559, Len: 0

Wireshark interface showing a packet capture of an HTTP session. The top pane displays a list of packets, with packet 5444 selected. The middle pane shows the details of the selected packet, including the HTTP request and response. The bottom pane displays the raw packet data in hexadecimal and ASCII.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.38 and tcp

No. Time Source Destination Protocol Length Info

5444 281.210835088 192.168.1.38 192.168.1.38 HTTP 2416 HTTP/1.1 200 OK [application/vnd.ms-cab-compressed]

5445 281.210835160 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=11501 Ack=384139 Win=65280 Len=0

5446 281.212649634 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729021_d763cecf7414f49efc1533b056a3736d4f67e29.cab HTTP/1.1

5447 281.242399192 192.168.1.38 20 50 68 235 TCP 60 1937 - 443 [RST] ACK Seq=1251 Ack=384139 Win=0 Len=0

5451 281.408318490 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=386813 Ack=11751 Win=32768 Len=2674 [TCP PDU reassembled in 5457]

5454 281.408318687 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=386813 Ack=11751 Win=32768 Len=2674 [TCP PDU reassembled in 5457]

5455 281.408318708 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=11751 Ack=389487 Win=65280 Len=0

5456 281.408777161 192.168.1.38 192.168.1.38 TCP 1391 80 - 1952 [ACK] Seq=389487 Ack=1251 Win=32768 Len=1337 [TCP PDU reassembled in 5457]

5457 281.41286647 192.168.1.38 192.168.1.38 HTTP 1077 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5458 281.41286729 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=11751 Ack=389487 Win=65280 Len=0

5459 281.414261927 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729019_5729d7b65f1853f9d58eece6aca6b42d5fa40.cab HTTP/1.1

5460 281.608463936 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=381847 Ack=12001 Win=32768 Len=2674 [TCP PDU reassembled in 5465]

5461 281.608463287 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12001 Ack=384521 Win=65280 Len=0

5462 281.612712407 192.168.1.38 192.168.1.38 TCP 1391 80 - 1952 [ACK] Seq=384521 Ack=12001 Win=32768 Len=1337 [TCP PDU reassembled in 5465]

5463 281.612712528 192.168.1.38 192.168.1.38 TCP 60 [TCP ACKed unseq. segment] 1952 - 80 [ACK] Seq=12001 Ack=389532 Win=65280 Len=0

5464 281.612712544 192.168.1.38 192.168.1.38 TCP 1391 [TCP Spurious Retransmission] 80 - 1952 [ACK] Seq=387195 Ack=12001 Win=32768 Len=1337 [TCP PDU reassembled in 5465]

5465 281.612712549 192.168.1.38 192.168.1.38 HTTP 1083 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5466 281.615105525 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12001 Ack=389559 Win=65280 Len=0

5467 281.616744562 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729019_5729d7b65f1853f9d58eece6aca6b42d5fa40.cab HTTP/1.1

5468 281.812434981 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=389559 Ack=12251 Win=32768 Len=2674 [TCP PDU reassembled in 5472]

5469 281.812435217 192.168.1.38 192.168.1.38 TCP 2728 80 - 1952 [PSH, ACK] Seq=402233 Ack=12251 Win=32768 Len=2674 [TCP PDU reassembled in 5472]

5470 281.812435238 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12251 Ack=404907 Win=65280 Len=0

5471 281.813994351 192.168.1.38 192.168.1.38 TCP 1391 80 - 1952 [ACK] Seq=404907 Ack=1251 Win=32768 Len=1337 [TCP PDU reassembled in 5472]

5472 281.820429216 192.168.1.38 192.168.1.38 HTTP 1079 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5473 281.820429486 192.168.1.38 192.168.1.38 TCP 60 1952 - 80 [ACK] Seq=12251 Ack=407269 Win=65280 Len=0

5474 281.822921626 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729018_2946b65cbb724c5da696f0833ed41b02ab3d97.cab HTTP/1.1

5475 282.017408263 192.168.1.38 192.168.1.38 HTTP 1391 [TCP Previous segment not captured] Continuation

5476 282.017408263 192.168.1.38 192.168.1.38 TCP 60 [TCP Dup ACK 5473#1] 1952 - 80 [ACK] Seq=12001 Ack=407269 Win=65280 Len=0 SLE=408066 SRE=411280

5477 282.017408263 192.168.1.38 192.168.1.38 HTTP 1391 Continuation

5478 282.022343439 192.168.1.38 192.168.1.38 TCP 74 [TCP Dup ACK 5473#2] 1952 - 80 [ACK] Seq=12001 Ack=407269 Win=65280 Len=0 SLE=411261 SRE=411280

5479 282.022343522 192.168.1.38 192.168.1.38 HTTP 1391 [TCP Previous segment not captured] Continuation

5480 282.035110967 192.168.1.38 192.168.1.38 TCP 60 [TCP ACKed unseq. segment] 1952 - 80 [ACK] Seq=12001 Ack=411280 Win=65280 Len=0 SLE=412617 SRE=413954

5481 282.035111157 192.168.1.38 192.168.1.38 TCP 1391 [TCP Spurious Retransmission] 80 - 1952 [ACK] Seq=407269 Ack=12001 Win=32768 Len=1337

5482 282.282946446 192.168.1.38 192.168.1.38 TCP 60 [TCP ACKed unseq. segment] 1952 - 80 [ACK] Seq=12001 Ack=413954 Win=65280 Len=0

5483 282.282946493 192.168.1.38 192.168.1.38 TCP 1391 [TCP Spurious Retransmission] 80 - 1952 [ACK] Seq=411280 Ack=12001 Win=32768 Len=1337

Frame 5485: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: Intel-Ed:53:fa (68:7a:64:ed:53:fa), Dst: VortexInfoTe:8:d6:c0 (4c:ea:14:a8:d6:c0)
Internet Protocol Version 4, Src: 192.168.1.38, Dst: 192.168.1.38
Transmission Control Protocol, Src Port: 1952, Dst Port: 80, Seq: 12001, Ack: 399559, Len: 0

Wireshark interface showing a packet capture of an HTTP session. The top pane displays a list of packets, with packet 5396 selected. The middle pane shows the details of the selected packet, including the HTTP request and response. The bottom pane displays the raw packet data in hexadecimal and ASCII.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.38 and http

No. Time Source Destination Protocol Length Info

5396 281.002176841 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729028_979d2bf5de9b019a5a5713c5682c96081512f645.cab HTTP/1.1

5396 281.002176981 192.168.1.38 192.168.1.38 TCP 1075 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5396 281.002620690 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729027_4675d2a55f7f8a404616542f4d74bb50da2815.cab HTTP/1.1

5403 280.201640244 192.168.1.38 192.168.1.38 TCP 2416 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5405 280.207423295 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729026_a9834c1bed3ba31402a895ccf6ea26a352a21ba.cab HTTP/1.1

5412 280.402526690 192.168.1.38 192.168.1.38 HTTP 1079 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5414 280.404942060 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729025_9175c0da464c73c9e1c2128a1b394d22c5c44.cab HTTP/1.1

5419 280.607975462 192.168.1.38 192.168.1.38 HTTP 2416 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5421 280.608409444 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729024_FF3b08b76ec2b59ff67a63c48a098c1456f0609.cab HTTP/1.1

5427 280.808917090 192.168.1.38 192.168.1.38 HTTP 1079 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5429 280.809818411 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729023_4e45b7f890463f161797abacdc42ea35927b.cab HTTP/1.1

5435 281.009794782 192.168.1.38 192.168.1.38 HTTP 1083 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5437 281.010642080 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729022_3ba3f90a7e4c51a19ae42c7969d11386dc52346.cab HTTP/1.1

5444 281.210835088 192.168.1.38 192.168.1.38 HTTP 2416 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5446 281.212649634 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729021_d763cecf7414f49efc1533b056a3736d4f67e29.cab HTTP/1.1

5457 281.41286647 192.168.1.38 192.168.1.38 HTTP 1077 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5459 281.414261927 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729020_89c2df389c9f10f170163240414854a43ca7e.cab HTTP/1.1

5460 281.608463936 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729019_5729d7b65f1853f9d58eece6aca6b42d5fa40.cab HTTP/1.1

5472 281.820429216 192.168.1.38 192.168.1.38 HTTP 1079 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5474 281.822921626 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729018_2946b65cbb724c5da696f0833ed41b02ab3d97.cab HTTP/1.1

5476 282.017408263 192.168.1.38 192.168.1.38 HTTP 1391 [TCP Previous segment not captured] Continuation

5477 282.017408263 192.168.1.38 192.168.1.38 HTTP 1391 Continuation

5478 282.022343439 192.168.1.38 192.168.1.38 HTTP 1391 [TCP Previous segment not captured] Continuation

5484 282.471062530 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729017_F444a1523bbe8c1ff4710d56b29bc8d1871d7.cab HTTP/1.1

5490 282.688403512 192.168.1.38 192.168.1.38 HTTP 2416 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5492 282.688611897 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729016_42cc1f1680f42759d24211e542ead795050f.cab HTTP/1.1

5498 282.884639841 192.168.1.38 192.168.1.38 HTTP 1079 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5500 282.886681794 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729015_89569c3f8da9b4fc4b3ba4580d02214eb187b.cab HTTP/1.1

5508 283.086708709 192.168.1.38 192.168.1.38 HTTP 2416 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5508 283.088117450 192.168.1.38 192.168.1.38 HTTP 384 GET /c/msdownload/update/others/2025/08/43729014_105a36df50a9e062b0e0a0ade190ff2f790.cab HTTP/1.1

5514 283.287384445 192.168.1.38 192.168.1.38 HTTP 1228 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)

5608 284.203883154 192.168.1.38 192.168.1.38 HTTP 384 GET /files/transfer-service/files/ce0ebcfb-Secf-4f13-B2D0-d36f4894310/pieceshash HTTP/1.1

5618 284.256338104 192.168.1.38 192.168.1.38 HTTP 369 GET /files/transfer-service/files/ce0ebcfb-Secf-4f13-B2D0-d36f4894310/pieceshash HTTP/1.1

Frame 5495: 1081 bytes on wire (8648 bits), 1081 bytes captured (8648 bits) on interface eth0, id 0
Ethernet II, Src: VortexInfoTe:8:d6:c0 (4c:ea:14:a8:d6:c0), Dst: Intel-Ed:53:fa (68:7a:64:ed:53:fa)
Internet Protocol Version 4, Src: 192.168.1.38, Dst: 192.168.1.38
Transmission Control Protocol, Src Port: 80, Dst Port: 1952, Seq: 399532, Ack: 12001, Len: 1027
[4 Reassembled TCP Segments (7712 bytes): #5460(2674), #5462(2674), #5464(1337), #5465(1027)]
Hypertext Transfer Protocol
Media Type

Frame 1081 bytes Reassembled TCP (7712 bytes)

Frame 23352: 23352 bytes on wire (186816 bits), 23352 bytes captured (186816 bits) on interface eth0, id 0
Ethernet II, Src: Intel-Ed:53:fa (68:7a:64:ed:53:fa), Dst: VortexInfoTe:8:d6:c0 (4c:ea:14:a8:d6:c0)
Internet Protocol Version 4, Src: 192.168.1.38, Dst: 192.168.1.38
Transmission Control Protocol, Src Port: 1952, Dst Port: 80, Seq: 12001, Ack: 399559, Len: 0

Wireshark network traffic capture showing DNS queries and responses. The packet list on the left shows various DNS queries from 192.168.1.1 to 192.168.1.38. The packet details pane shows the structure of a DNS query, including the question, answer, and authority sections. The packet bytes pane shows the raw data of the DNS query.

Terminal window showing a ping command being executed on a Kali Linux machine. The command is `ping google.com -c 5`. The output shows the results of the ping command, including the IP address of google.com (172.217.174.78) and the time taken for each packet to reach the destination.

Wireshark network traffic capture showing a TCP connection between a Kali Linux machine and a target IP address (127.0.0.1). The packet list on the left shows the TCP connection establishment process, including the SYN, SYN-ACK, and ACK packets. The packet details pane shows the structure of the TCP segments, including the source and destination ports, sequence numbers, and window sizes. The packet bytes pane shows the raw data of the TCP segments.

