

Use Wireshark sniffer to capture network traffic and analyze

The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into several panes.

Welcome to Wireshark

Capture

...using this filter: All interfaces shown

Adapter for loopback traffic capture

USBPcap1

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.101.112	192.168.101.50	DNS	84	Standard query 0x6802 A ipv6.msftconnecttest.com
2	0.001434	192.168.101.112	192.168.101.50	DNS	83	Standard query 0x83ac A www.msftconnecttest.com
3	0.001723	192.168.101.112	192.168.101.50	DNS	83	Standard query 0x5373 AAAA www.msftconnecttest.com
4	0.002595	192.168.101.112	192.168.101.50	DNS	84	Standard query 0x48df AAAA ipv6.msftconnecttest.com
5	0.009340	192.168.101.50	192.168.101.112	DNS	246	Standard query response 0x83ac A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msedge.net CNAME ncsi.4-c...
6	0.009340	192.168.101.50	192.168.101.112	DNS	230	Standard query response 0x5373 AAAA www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME v4ncsi.msedge.net CNAME ncsi...
7	0.009429	192.168.101.50	192.168.101.112	DNS	223	Standard query response 0x6802 A ipv6.msftconnecttest.com CNAME v6ncsi.msedge.net CNAME ncsi.6-c-0003.c-msedge.net CNAME 6-c-0003...
8	0.009429	192.168.101.50	192.168.101.112	DNS	194	Standard query response 0x48df AAAA ipv6.msftconnecttest.com CNAME v6ncsi.msedge.net CNAME ncsi.6-c-0003.c-msedge.net CNAME 6-c-0...
9	0.090396	192.168.101.112	13.107.4.52	TCP	66	49984 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10	0.090430	192.168.101.112	13.107.4.52	TCP	66	49985 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	0.090705	2401:4900:6287:95c4::2a01:111:2003::52	2401:4900:6287:95c4::2a01:111:2003::52	TCP	86	49987 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
12	0.090705	2401:4900:6287:95c4::2a01:111:2003::52	2401:4900:6287:95c4::2a01:111:2003::52	TCP	86	49986 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1

> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF_{AABE28C6-AA73-4100-9341-475B28D088C3}, id 0

> Ethernet II, Src: Chongqin_bd1a:fd (18:47:3d:bd:1a:fd), Dst: 2e:ca:21:f8:cd:d1 (2e:ca:21:f8:cd:d1)

> Internet Protocol Version 4, Src: 192.168.101.112, Dst: 192.168.101.50

> User Datagram Protocol, Src Port: 60282, Dst Port: 53

> Domain Name System (query)

0000 2e ca 21 f8 cd d1 18 47 3d bd 1a fd 08 00 45 00 G m E

0010 00 46 cf d0 00 00 80 11 1e e3 c0 a8 65 70 c0 a8 . F ep

0020 65 32 eb 7a 00 35 00 32 8a 6e 68 02 01 00 00 01 e2 z 5 2 . nh

0030 00 00 00 00 00 00 04 69 70 76 36 0f 6d 73 66 74 i pv6 msft

0040 63 6f 6e 6e 65 63 74 74 65 73 74 03 63 6f 6d 00 connect est com

0050 00 01 00 01

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
21	0.192117	192.168.101.112	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
22	0.192136	2401:4900:6287:95c4::	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
23	0.192136	2401:4900:6287:95c4::	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
24	0.192170	192.168.101.112	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
27	0.251014	2a01:111:2003::52	2401:4900:6287:95c4::	HTTP	613	HTTP/1.1 200 OK (text/plain)
29	0.251014	2a01:111:2003::52	2401:4900:6287:95c4::	HTTP	613	HTTP/1.1 200 OK (text/plain)
37	0.260968	13.107.4.52	192.168.101.112	HTTP	593	HTTP/1.1 200 OK (text/plain)
39	0.260968	13.107.4.52	192.168.101.112	HTTP	593	HTTP/1.1 200 OK (text/plain)
67	2.442400	2401:4900:6287:95c4::	2a01:111:2003::50	HTTP	276	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?425a33a750e43659 HTTP/1.1
72	2.564285	2a01:111:2003::50	2401:4900:6287:95c4::	HTTP	1257	HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
2304	77.634826	192.168.101.112	180.235.121.242	HTTP	531	GET /Login.aspx HTTP/1.1
2354	77.817599	180.235.121.242	192.168.101.112	HTTP	1078	HTTP/1.1 200 OK (text/html)

> Frame 29: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface \Device\NPF_{AABE28C6-AA73-4100-9341-475B28D088C3}, id 0

> Ethernet II, Src: 2e:ca:21:f8:cd:d1 (2e:ca:21:f8:cd:d1), Dst: Chongqin_bd:1a:fd (18:47:3d:bd:1a:fd)

> Internet Protocol Version 6, Src: 2a01:111:2003::52, Dst: 2401:4900:6287:95c4:::52

> Transmission Control Protocol, Src Port: 80, Dst Port: 49987, Seq: 1, Ack: 156, Len: 539

> Hypertext Transfer Protocol

> Line-based text data: text/plain (1 lines)

0000 18 47 3d bd 1a fd 2e ca 21 f8 cd d1 86 dd 60 0d [Google] |.....
0010 89 12 02 2f 06 33 2a 01 01 11 20 03 00 00 00 00 ---/3%
0020 00 00 00 00 52 24 01 49 00 62 87 95 c4 ac af ---RS I b....
0030 c9 52 92 ec bf ab 00 50 c3 43 c3 08 52 ec 87 84 R---P C R...
0040 ac d8 50 18 3f ff c1 ab 00 00 48 54 54 50 2f 31 P?---HTTP/1
0050 2e 31 20 32 30 30 20 4f 4b 0d 0a 43 61 63 68 65 .1 200 O K Cache
0060 2d 43 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 73 74 6f -Control : no-sto
0070 72 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 re-Cont ent-Leng
0080 74 68 3a 20 32 32 0d 0a 43 6f 6e 74 65 6e 74 2d th: 22- Content-
0090 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e Type: te xt/plain
00a0 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 0d ; charse t=utf-8
00b0 0a 4c 61 73 74 2d 4d 6f 64 09 66 69 65 64 3a 20 Last-Mo dified:
00c0 54 68 75 2c 20 30 38 20 53 65 70 20 32 30 32 32 Thu, 08 Sep 2022
00d0 20 30 30 3a 35 35 3a 30 37 20 47 4d 54 0d 0a 41 00:55:0 7 GMT A

wireshark_WinF27ULT1.pcapng Packets: 4305 · Displayed: 30 (0.7%) · Dropped: 0 (0.0%) Profile: Default