

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>F

Welcome to Wireshark

Open

C:\Users\Deil\Documents\wure1.pcapng (10259 KB)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Local Area Connection* 11

Local Area Connection* 8

Local Area Connection* 7

Wi-Fi

VMware Network Adapter VMnet8

VMware Network Adapter VMnet1

Local Area Connection* 14

Local Area Connection* 13

Adapter for loopback traffic capture

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.8 (v3.6.8-0-g92590cd51508). You receive automatic updates.

Ready to load or capture

No Packets

Profile: Default

2:35 PM 9/27/2022

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	192.168.114.227	20.198.119.84	TLSv1.2	155	Application Data
2	0.138251	20.198.119.84	192.168.114.227	TLSv1.2	225	Application Data
3	0.183148	192.168.114.227	20.198.119.84	TCP	54	49408 → 443 [ACK] Seq=102 Ack=172 Win=511 Len=0
4	0.508894	20.198.119.84	192.168.114.227	TCP	225	[TCP Spurious Retransmission] 443 → 49408 [PSH, ACK] Seq=1 Ack=102 Win=6982 Len=171
5	0.509244	192.168.114.227	20.198.119.84	TCP	66	[TCP Dup ACK 3#1] 49408 → 443 [ACK] Seq=107 Ack=172 Win=0 SLE=1 SRE=172
6	1.411318	192.168.114.227	168.119.147.171	TCP	55	49790 → 80 [ACK] Seq=1 Ack=1 Win=513 Len=1
7	1.589714	168.119.147.171	192.168.114.227	TCP	54	80 → 49790 [ACK] Seq=0 Ack=2 Win=501 Len=0
8	1.589746	192.168.114.227	168.119.147.171	TCP	54	[TCP Dup ACK 6#1] [TCP ACKed unseen segment] 49790 → 80 [ACK] Seq=2 Ack=1 Win=513 Len=0
9	3.411841	192.168.114.227	168.119.147.171	TCP	55	[TCP Keep-Alive] [TCP ACKed unseen segment] 49790 → 80 [ACK] Seq=1 Ack=1 Win=513 Len=1
10	3.651235	168.119.147.171	192.168.114.227	TCP	66	[TCP Previous segment not captured] 80 → 49790 [ACK] Seq=1 Ack=2 Win=501 SLE=1 SRE=2
11	4.377975	204.79.197.222	192.168.114.227	TCP	54	443 → 51067 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	4.551056	192.168.114.227	52.168.112.66	TCP	66	51112 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	4.889432	52.168.112.66	192.168.114.227	TCP	66	443 → 51112 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=256 SACK_PERM=1
14	4.889560	192.168.114.227	52.168.112.66	TCP	54	51112 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
15	4.914239	192.168.114.227	52.168.112.66	TLSv1.2	340	Client Hello
16	5.249889	52.168.112.66	192.168.114.227	TCP	1414	443 → 51112 [ACK] Seq=1 Ack=287 Win=524544 Len=1360 [TCP segment of a reassembled PDU]
17	5.249889	52.168.112.66	192.168.114.227	TCP	1414	443 → 51112 [ACK] Seq=1361 Ack=287 Win=524544 Len=1360 [TCP segment of a reassembled PDU]
18	5.249889	52.168.112.66	192.168.114.227	TCP	1414	443 → 51112 [ACK] Seq=2721 Ack=287 Win=524544 Len=1360 [TCP segment of a reassembled PDU]
19	5.249889	52.168.112.66	192.168.114.227	TCP	1414	443 → 51112 [ACK] Seq=4081 Ack=287 Win=524544 Len=1360 [TCP segment of a reassembled PDU]
20	5.249889	52.168.112.66	192.168.114.227	TLSv1.2	872	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
21	5.250114	192.168.114.227	52.168.112.66	TCP	54	51112 → 443 [ACK] Seq=287 Ack=6259 Win=262144 Len=0
22	5.258332	192.168.114.227	52.168.112.66	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23	5.537589	52.168.112.66	192.168.114.227	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
24	5.537749	192.168.114.227	52.168.112.66	TCP	54	51112 → 443 [ACK] Seq=445 Ack=6310 Win=261888 Len=0

> Frame 1: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface \Device\NPF_{09F3C37E-8117-4051-9E25-9AD76545C69F}, id 0

> Ethernet II, Src: Chongain_d7:75:27 (d4:1b:81:d7:75:27), Dst: f6:1f:c4:c9:85:0f (f6:1f:c4:c9:85:0f)

> Internet Protocol Version 4, Src: 192.168.114.227, Dst: 20.198.119.84

> Transmission Control Protocol, Src Port: 49408, Dst Port: 443, Seq: 1, Ack: 1, Len: 101

> Transport Layer Security

0000 f6 1f c4 c9 85 0f d4 1b 81 d7 75 27 08 00 45 00u'.E:

0010 00 bd 20 9e 40 00 00 06 1a 27 c0 a0 72 e3 14 c6@...".r..

0020 77 54 c1 00 01 bb 13 79 77 0d d1 04 6c 15 50 18 wT....y w...l.P:

0030 01 ff 72 03 00 00 17 03 03 00 60 00 00 00 00 00P.....

0040 00 00 16 6e 05 fc a7 ac e9 86 34 5c e2 70 83 71n....4\p.q

0050 62 0a 5f db 12 68 27 fc 3f f4 d7 d7 66 7b a9 c9 b....h'.?...f{..

0060 d7 ad b0 1b af bd b0 93 f5 a7 c1 1e 20 43 71 cbCq:

0070 7d f3 19 07 bb 8f f6 51 80 eb 90 01 6f 1b 3b acQ....o.;

Wi-Fi: <live capture in progress>

Packets: 60 · Displayed: 60 (100.0%)

Profile: Default

2:36 PM 9/27/2022

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2986	141.309515	2401:4900:6270:913a...	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
2993	141.328175	2401:4900:6270:913a...	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
2994	141.328516	192.168.11.227	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
2995	141.328559	192.168.11.227	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
3000	141.403859	2a01:111:2003::52	2401:4900:6270:913a...	HTTP	613	HTTP/1.1 200 OK (text/plain)
3002	141.403859	13.107.4.52	192.168.11.227	HTTP	593	HTTP/1.1 200 OK (text/plain)
3003	141.403859	13.107.4.52	192.168.11.227	HTTP	593	HTTP/1.1 200 OK (text/plain)
3004	141.403859	2a01:111:2003::52	2401:4900:6270:913a...	HTTP	613	HTTP/1.1 200 OK (text/plain)
3126	176.703269	2401:4900:6270:913a...	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
3127	176.703285	2401:4900:6270:913a...	2a01:111:2003::52	HTTP	229	GET /connecttest.txt HTTP/1.1
3130	176.747624	192.168.11.227	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
3135	176.759258	192.168.11.227	13.107.4.52	HTTP	208	GET /connecttest.txt HTTP/1.1
3136	176.762302	2a01:111:2003::52	2401:4900:6270:913a...	HTTP	613	HTTP/1.1 200 OK (text/plain)
3138	176.762302	2a01:111:2003::52	2401:4900:6270:913a...	HTTP	613	HTTP/1.1 200 OK (text/plain)
3141	176.799112	13.107.4.52	192.168.11.227	HTTP	593	HTTP/1.1 200 OK (text/plain)
3146	176.802882	13.107.4.52	192.168.11.227	HTTP	593	HTTP/1.1 200 OK (text/plain)
3233	183.966997	192.168.11.227	180.235.121.242	HTTP	1135	POST / HTTP/1.1 (application/x-www-form-urlencoded)
3276	184.969632	180.235.121.242	192.168.11.227	HTTP	1217	HTTP/1.1 302 Found (text/html)
3277	184.996602	192.168.11.227	180.235.121.242	HTTP	641	GET /StudentPortal/Landing.aspx HTTP/1.1
3375	196.346251	180.235.121.242	192.168.11.227	HTTP	1230	HTTP/1.1 200 OK (text/html)
3378	196.397634	192.168.11.227	180.235.121.242	HTTP	528	GET /assets/global/plugins/jquery-ui/jquery-ui.min.css HTTP/1.1
3380	196.397813	192.168.11.227	180.235.121.242	HTTP	532	GET /assets/global/plugins/uniform/css/uniform.default.css HTTP/1.1
3381	196.398169	192.168.11.227	180.235.121.242	HTTP	546	GET /assets/global/plugins/bootstrap-switch/css/bootstrap-switch.min.css HTTP/1.1

> Frame 3233: 1135 bytes on wire (9080 bits), 1135 bytes captured (9080 bits) on interface \Device\NPF_{05F3C37E-8117-4051-9E25-9AD76545C60F}, id 0

> Ethernet II, Src: Chongain_d7:75:27 (d4:1b:81:d7:75:27), Dst: 76:87:ee:b9:47:fd (76:87:ee:b9:47:fd)

> Internet Protocol Version 4, Src: 192.168.11.227, Dst: 180.235.121.242

> Transmission Control Protocol, Src Port: 51216, Dst Port: 80, Seq: 862, Ack: 5866, Len: 1081

> Hypertext Transfer Protocol

> HTML Form URL Encoded: application/x-www-form-urlencoded

03e0 67 66 43 53 68 44 54 71 74 76 35 30 77 49 58 30 gFCSHDtq tv50wIX0

03f0 34 33 63 39 37 59 44 58 56 55 55 72 6c 37 34 63 43c97YDX VUUr174c

0400 7a 70 25 32 42 32 56 6a 43 33 56 6d 42 79 44 49 zpK2B2Vj C3VmbYDI

0410 70 35 73 56 63 44 53 67 56 41 59 51 6e 0b 73 62 p5sVcD5g VAYQnksb

0420 4d 47 59 4e 58 51 61 72 5a 76 58 59 78 43 62 51 H6YMXQar ZuXYxcBQ

0430 25 33 44 26 74 78 74 75 73 65 72 6e 61 6d 65 3d %3D&txtu sername=

0440 31 39 32 30 31 31 30 37 37 26 74 78 74 70 61 73 19201107 7&txtpas

0450 73 77 6f 72 64 3d 63 68 69 6e 6e 61 31 37 31 38 sword=ch innal718

Bytes 1130-1134: Value (urlencoded-form.value)

Packets: 4546 - Displayed: 167 (3.7%) - Dropped: 0 (0.0%)

Profile: Default

2:40 PM 9/27/2022