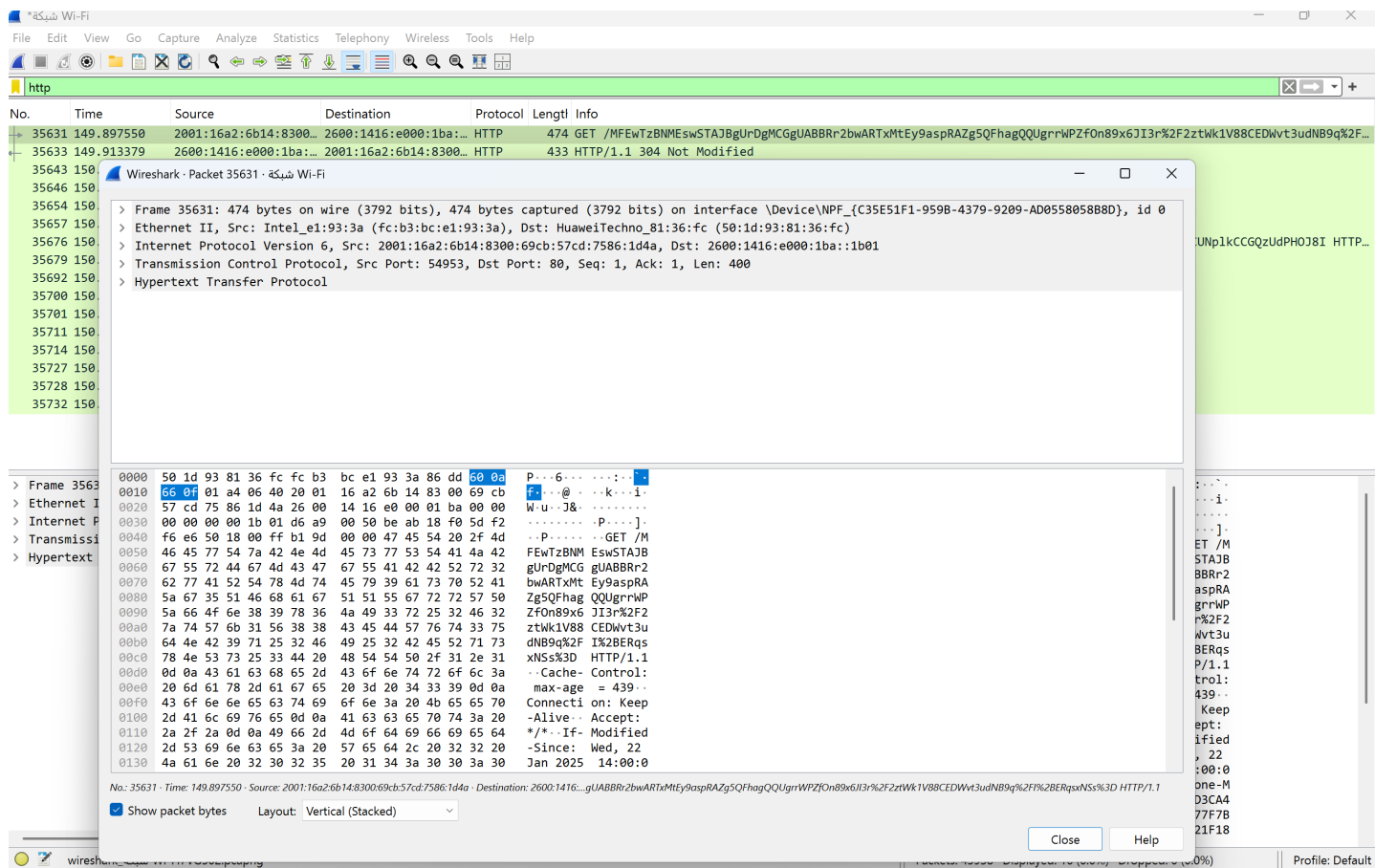
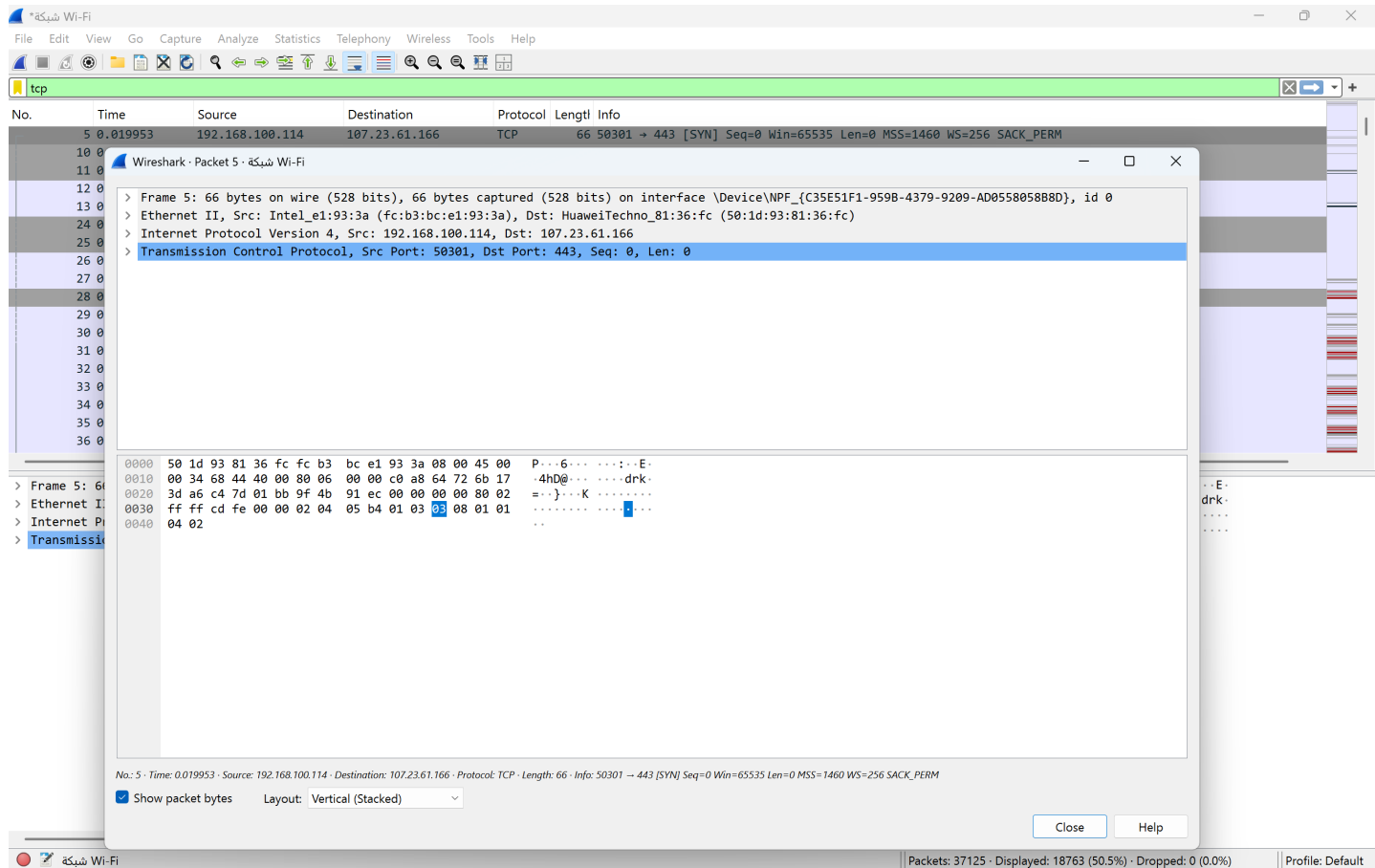


# Filter HTTP packets and analyze them



# Filter TCP packets



# Analyze TCP handshake and investigate Data Transfer and Termination

شبكة Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
456	10.584699	44.206.217.228	192.168.100.114	TCP	60	443 → 56374 [ACK] Seq=6028 Ack=315 Win=28160 Len=0
457	10.584920	44.206.217.228	192.168.100.114	TLSv1.2	258	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
458	10.601524	192.168.100.114	44.206.217.228	TLSv1.2	321	Application Data
459	10.785624	44.206.217.228	192.168.100.114	TLSv1.2	108	Application Data
460	10.795811	192.168.100.114	44.206.217.228	TLSv1.2	561	Application Data
461	10.985636	44.206.217.228	192.168.100.114	TLSv1.2	588	Application Data
462	11.029639	192.168.100.114	44.206.217.228	TCP	54	56374 → 443 [ACK] Seq=1089 Ack=6820 Win=64512 Len=0
463	12.089026	HikvisionDig_16:d9...	Broadcast	ARP	60	Who has 192.168.100.1? Tell 192.168.100.211
464	14.075328	192.168.100.114	2.16.70.4	TCP	54	56310 → 80 [FIN, ACK] Seq=1 Ack=1 Win=252 Len=0
465	14.140553	2.16.70.4	192.168.100.114	TCP	54	80 → 56310 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
466	14.140645	192.168.100.114	2.16.70.4	TCP	54	56310 → 80 [ACK] Seq=2 Ack=2 Win=252 Len=0
467	15.011805	fe80::8d5e:1eb4:9af...	fe80::1	DNS	103	Standard query 0xb543 A treatment.grammarly.com
468	15.011933	fe80::8d5e:1eb4:9af...	fe80::1	DNS	103	Standard query 0xd7d5 AAAA treatment.grammarly.com
469	15.033694	fe80::1	fe80::8d5e:1eb4:9af...	DNS	296	Standard query response 0xb543 A treatment.grammarly.com CNAME public-treatment.prod-experimentation.gr...
470	15.034733	fe80::1	fe80::8d5e:1eb4:9af...	DNS	252	Standard query response 0xd7d5 AAAA treatment.grammarly.com CNAME public-treatment.prod-experimentation...
471	15.036113	192.168.100.114	52.5.16.10	TCP	66	56376 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
472	15.036113	192.168.100.114	52.5.16.10	TCP	66	56375 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
473	15.300980	52.5.16.10	192.168.100.114	TCP	66	443 → 56375 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1412 SACK_PERM WS=256
474	15.301096	192.168.100.114	52.5.16.10	TCP	54	56375 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0

> Frame 474: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF...

> Ethernet II, Src: Intel\_e1:93:3a (fc:b3:bc:e1:93:3a), Dst: HuaweiTechno\_81:36:fc (50:1d:93:8...

> Internet Protocol Version 4, Src: 192.168.100.114, Dst: 52.5.16.10

> Transmission Control Protocol, Src Port: 56375, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 50 1d 93 81 36 fc fc b3 bc e1 93 3a 08 00 45 00 p...6...:..E..

0010 00 28 82 56 40 00 80 06 00 00 c0 a8 64 72 34 05 ..(V@...dr4..

0020 10 0a dc 37 01 bb a2 eb 7b 52 da e4 72 23 50 10 ...7...{R...r#P..

0030 00 ff 69 44 00 00 ..id..

wireshark شبكة Wi-FiUS2W02.pcapngPackets: 14221 · Dropped: 0 (0.0%)Profile: Default

شبكة Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 16

No.	Time	Source
472	15.036113	192.168.100.114
473	15.300980	52.5.16.10
474	15.301096	192.168.100.114
477	15.301823	192.168.100.114
479	15.501183	52.5.16.10
480	15.503046	52.5.16.10
481	15.503046	52.5.16.10
482	15.503046	52.5.16.10
483	15.503046	52.5.16.10
489	15.503385	192.168.100.114
492	15.515801	192.168.100.114
495	15.703234	52.5.16.10
496	15.703234	52.5.16.10
498	15.712013	192.168.100.114
499	15.903011	52.5.16.10
501	15.903484	192.168.100.114
508	16.067078	52.5.16.10
510	16.116037	192.168.100.114
533	17.084550	192.168.100.114

> Frame 472: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF...

> Ethernet II, Src: Intel\_e1:93:3a (fc:b3:bc:e1:93:3a), Dst: HuaweiTechno\_81:36:fc (50:1d:93:8...

> Internet Protocol Version 4, Src: 192.168.100.114, Dst: 52.5.16.10

> Transmission Control Protocol, Src Port: 56375, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

6 client pkts, 16 server pkts, 11 turns.

Entire conversation (17 kB)Show as ASCIINo delta timesStream 16

Find:Case sensitiveFind Next

Filter Out This StreamPrintSave as...BackCloseHelp

Wireshark · Follow TCP Stream (tcp.stream eq 16) · شبكة Wi-Fi

.....g...g.Q<M.I..Z\$.\\.....H...Ow.!.\$.>+.0./.\$.#.(.'.

.....=<.5./...]......treatment.grammarly.com.

.....#.....

.....C...\_.....'.....5d.....GV.

.....g...\\.....+.u.)...~.i.....=.....?./.....#.....0...0.....mv...R.>0

.....\*H...

.....0<1.0 ..U....US1.0

.....U.

.....Amazon1.0...U....Amazon RSA 2048 M020..

241026000000Z.

251123235959Z0"1 0...U....treatment.grammarly.com0.."0

.....\*H...

.....0...

.....D

(...&...I9.7..bi7...N...Sr..L.....ag.id.N.8v.3m.u.!.~...g~U.k3..I.qL.....kf....[];.....9g.....`e.(.Q...o.....A

0.&z\\.....W.{G[...=3.....\$".J..".G.cE.<.<r1..C.....P..sd n.b.....11[K.n.O.}(jYil....g..f#b.

.....?..'E.k.....v;q.....0.....0...U.#..0...1R.ZP..|tq.....z...0...U.....i.....g...m.ZH[.6.0"...U...0...t

reatment.grammarly.com0...U. ..0

0...g.....0...U.....0...U.%..0...+.....+.....0;;U...40200...,\*http://cr1.r2m02.amazontrust.com/r2m02.cr10u

...+.....10g0-...+.....0...!http://ocsp.r2m02.amazontrust.com06...+.....0...\*http://crt.r2m02.amazontrust.com/r2m02.cer0..

U.....0.0....

+...y.....p...l.j.v...N4.SrL.....?z...b...m0...&.....G0E.!!(<p.|.J|.I.44....+...P..8~.k.p@l@.\$...7.

}..G...N.j>z...A..w...1c@w..A..q...@.....2...7.P.....H0F.!!.....D...~4\_CqK.2..S.?..u....#r.!!../.J...\$u.D

Rm|Y...|...j".nv.(.w...j.q e...S...|".\\

.....~T..L

.....H0F.!!.....kJAK... ) .C.t)(?.....`

9.!.!..h.....W...6X...e..P...9...t70

.....\*H...

.....c.b.....L\n...E

>q.9.v.4.F...@.y...O.....\*c.....j.....N.:\\w.N.....q.x.....:cn.c1\$. ""6BG..... /Wa=\*..M ..\$./..B..a...A.{.....qo... ..

..%.."':...8...P...8...FpB[...].Fw...%\_n.....r.&Y:\*..K5...x..O+r.W ..P.c.j.....\_\$......X.O...\_EM&...!H...

.....b0...^0..F.....S.JK..N.;...-:i0

.....\*H...

.....091.0 ..U....US1.0

.....U.

.....Amazon1.0...U....Amazon Root CA 10..

220823222530Z.

300823222530Z0<1.0 ..U....US1.0

.....U.

.....Amazon1.0...U....Amazon RSA 2048 M020.."0

.....\*H...

.....0...

Wireshark interface showing a packet capture on a Wi-Fi network. The packet list on the left shows various TCP and TLSv1.2 packets. Packet 1115 is selected, showing details for a TCP FIN, ACK packet. The packet bytes pane on the right displays the raw data in hexadecimal and ASCII.

# Filter and analysis UDP Packets

Wireshark interface showing a packet capture on a Wi-Fi network. The packet list on the left shows various UDP packets. Packet 8 is selected, showing details for a UDP packet. The packet bytes pane on the right displays the raw data in hexadecimal and ASCII.