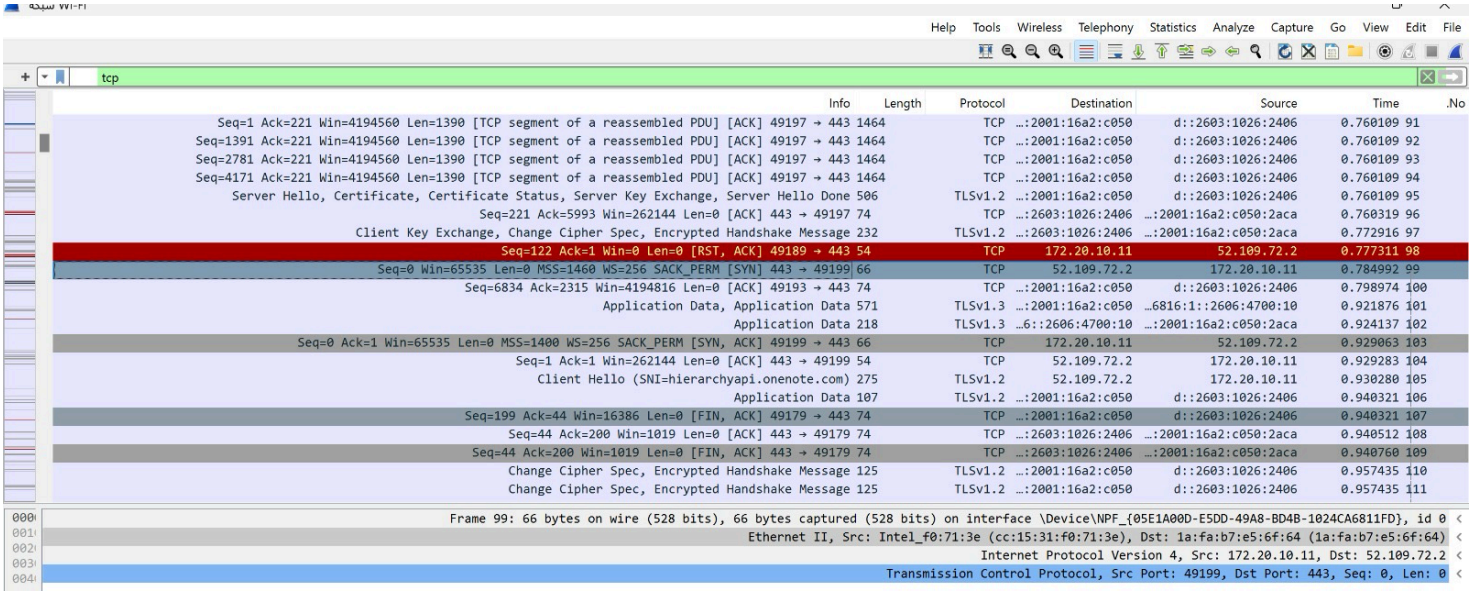
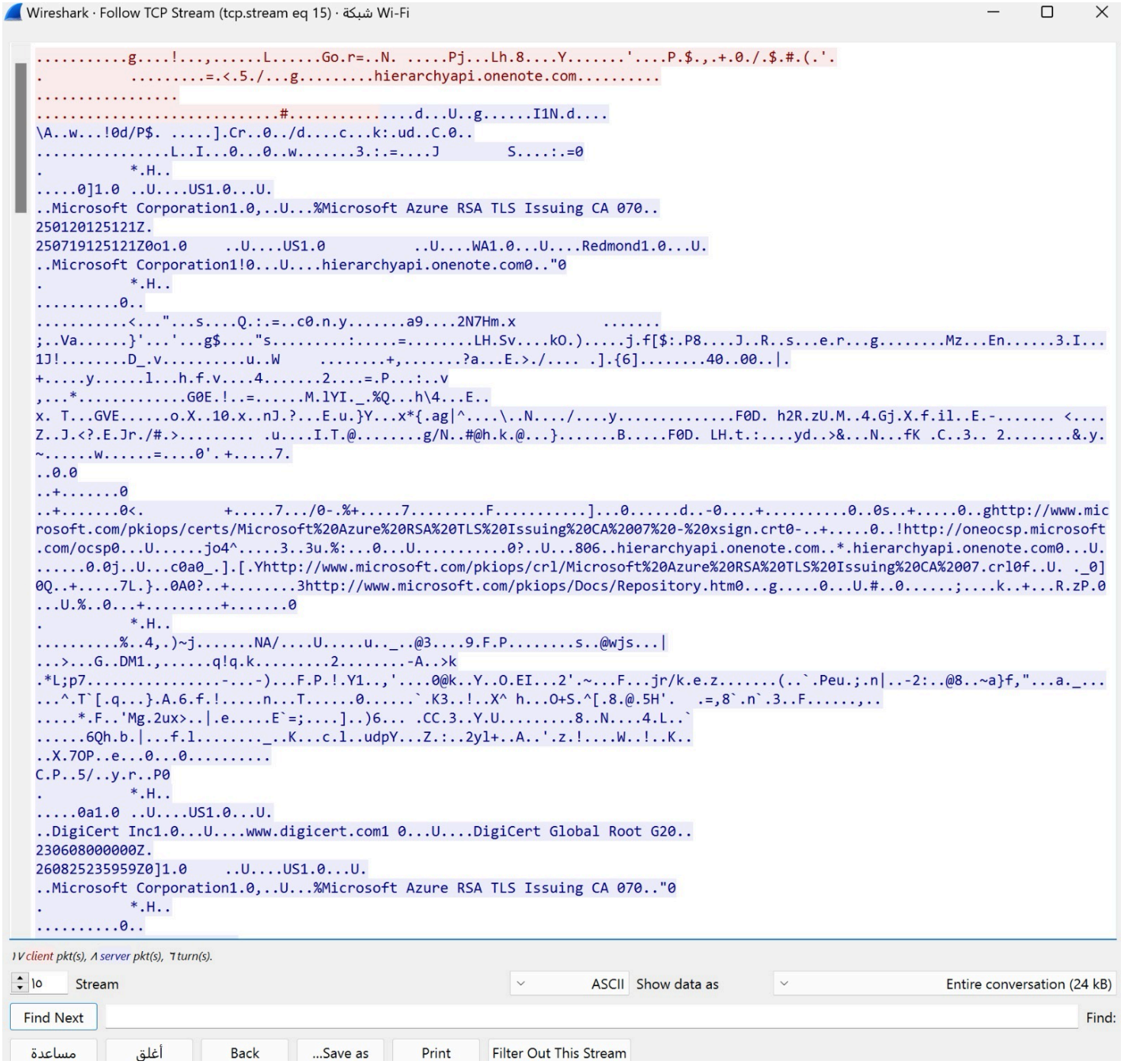
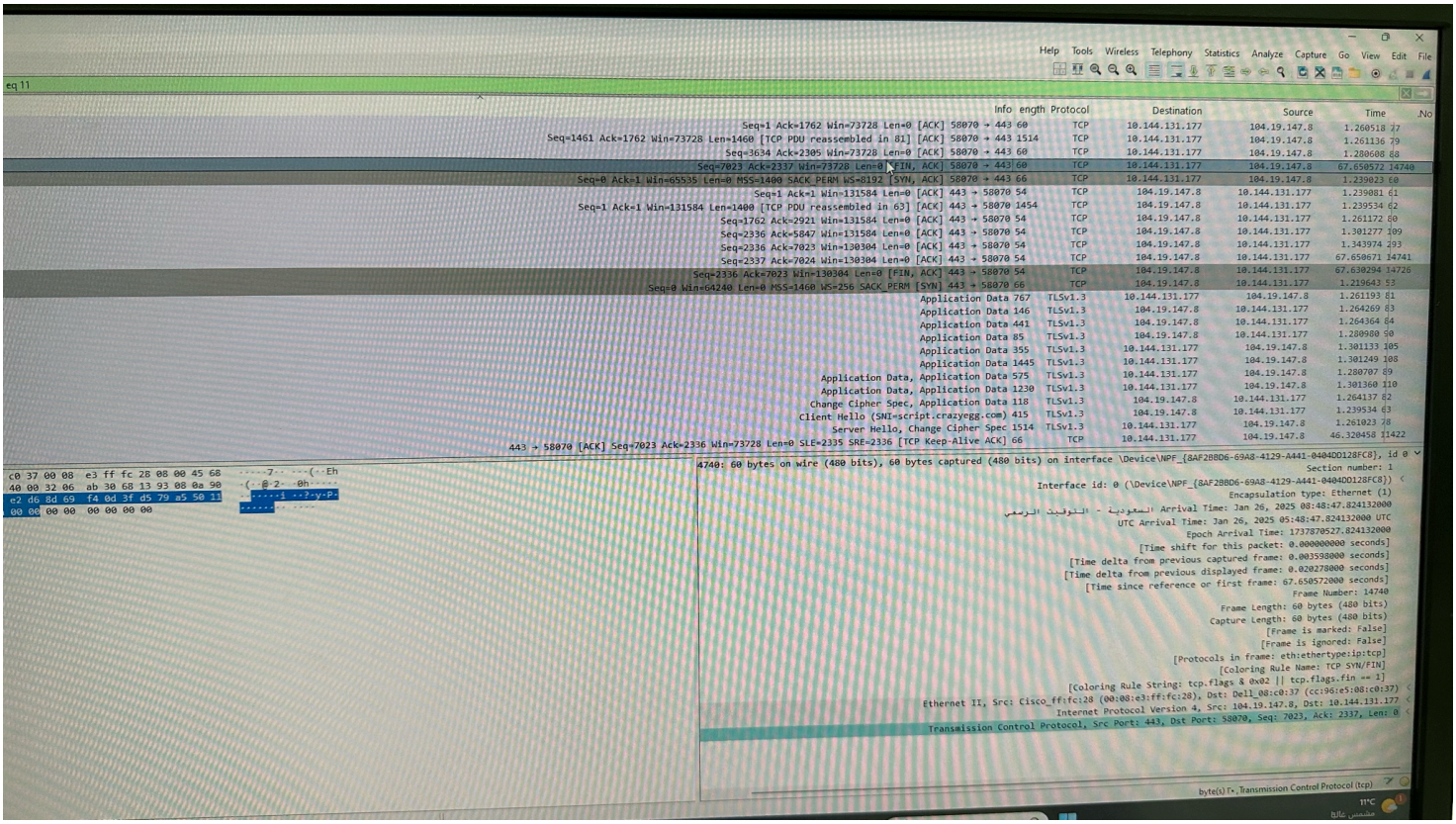

Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
tcp
Info Length Protocol Destination Source Time .No
Seq=1 Ack=221 Win=4194560 Len=1390 [TCP segment of a reassembled PDU] [ACK] 49197 → 443 1464 TCP …:2001:16a2:c050 d::2603:1026:2406 0.760109 91
Seq=1391 Ack=221 Win=4194560 Len=1390 [TCP segment of a reassembled PDU] [ACK] 49197 → 443 1464 TCP …:2001:16a2:c050 d::2603:1026:2406 0.760109 92
Seq=2781 Ack=221 Win=4194560 Len=1390 [TCP segment of a reassembled PDU] [ACK] 49197 → 443 1464 TCP …:2001:16a2:c050 d::2603:1026:2406 0.760109 93
Seq=4171 Ack=221 Win=4194560 Len=1390 [TCP segment of a reassembled PDU] [ACK] 49197 → 443 1464 TCP …:2001:16a2:c050 d::2603:1026:2406 0.760109 94
Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done 506 TLSv1.2 …:2001:16a2:c050 d::2603:1026:2406 0.760109 95
Seq=221 Ack=5993 Win=262144 Len=0 [ACK] 443 → 49197 74 TCP …:2603:1026:2406 …:2001:16a2:c050:2aca 0.760319 96
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 232 TLSv1.2 …:2603:1026:2406 …:2001:16a2:c050:2aca 0.772916 97
Seq=122 Ack=1 Win=0 Len=0 [RST, ACK] 49189 → 443 54 TCP 172.20.10.11 52.109.72.2 0.777311 98
Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 49199 66 TCP 52.109.72.2 172.20.10.11 0.784992 99
Seq=6834 Ack=2315 Win=4194816 Len=0 [ACK] 49193 → 443 74 TCP …:2001:16a2:c050 d::2603:1026:2406 0.798974 100
Application Data, Application Data 571 TLSv1.3 …:2001:16a2:c050 …6816:1::2606:4700:10 0.921876 101
Application Data 218 TLSv1.3 …6::2606:4700:10 …:2001:16a2:c050:2aca 0.924137 102
Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM [SYN, ACK] 49199 → 443 66 TCP 172.20.10.11 52.109.72.2 0.929063 103
Seq=1 Ack=1 Win=262144 Len=0 [ACK] 443 → 49199 54 TCP 52.109.72.2 172.20.10.11 0.929283 104
Client Hello (SNI=hierarchyapi.onenote.com) 275 TLSv1.2 52.109.72.2 172.20.10.11 0.930280 105
Application Data 107 TLSv1.2 …:2001:16a2:c050 d::2603:1026:2406 0.940321 106
Seq=199 Ack=44 Win=16386 Len=0 [FIN, ACK] 49179 → 443 74 TCP …:2001:16a2:c050 d::2603:1026:2406 0.940321 107
Seq=44 Ack=200 Win=1019 Len=0 [ACK] 443 → 49179 74 TCP …:2603:1026:2406 …:2001:16a2:c050:2aca 0.940512 108
Seq=44 Ack=200 Win=1019 Len=0 [FIN, ACK] 443 → 49179 74 TCP …:2603:1026:2406 …:2001:16a2:c050:2aca 0.940760 109
Change Cipher Spec, Encrypted Handshake Message 125 TLSv1.2 …:2001:16a2:c050 d::2603:1026:2406 0.957435 110
Change Cipher Spec, Encrypted Handshake Message 125 TLSv1.2 …:2001:16a2:c050 d::2603:1026:2406 0.957435 111
Frame 99: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{05E1A00D-E5DD-49A8-BD4B-1024CA6811FD}, id 0
Ethernet II, Src: Intel_f0:71:3e (cc:15:31:f0:71:3e), Dst: 1a:fa:b7:e5:6f:64 (1a:fa:b7:e5:6f:64)
Internet Protocol Version 4, Src: 172.20.10.11, Dst: 52.109.72.2
Transmission Control Protocol, Src Port: 49199, Dst Port: 443, Seq: 0, Len: 0

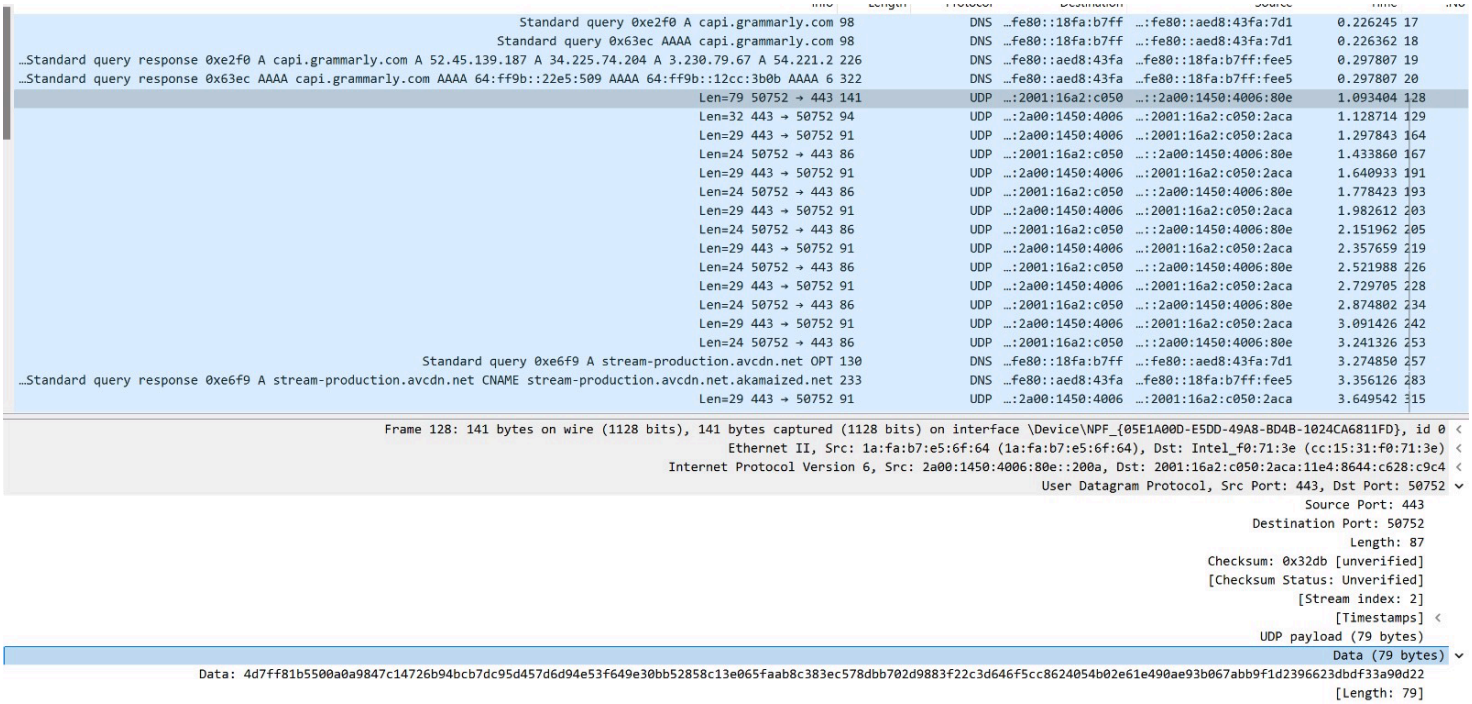

Wireshark · Follow TCP Stream (tcp.stream eq 15) · شبكة Wi-Fi
.....g....!...,.....L.....Go.r=..N. .....Pj...Lh.8....Y.....'....P.$.,.+.0./.$.#.(.'.
. .....=.<.5./...g.....hierarchyapi.onenote.com.....
.....
.....#.....d...U..g.....I1N.d....
\A..w...!0d/P$. .....].Cr..0../d....c...k:.ud..C.0..
.....L..I...0...0..w.....3.:.=....J S....:.=0
. *.H..
.....0]1.0 ..U....US1.0...U.
..Microsoft Corporation1.0,..U...%Microsoft Azure RSA TLS Issuing CA 070..
250120125121Z.
250719125121Z0o1.0 ..U....US1.0 ..U....WA1.0...U....Redmond1.0...U.
..Microsoft Corporation1!0...U....hierarchyapi.onenote.com0.."0
. *.H..
.....0..
.....<..."...s....Q.:.=..c0.n.y.....a9....2N7Hm.x .....
;..Va.....}'...'...g$...."s.....:.....=.....LH.Sv....kO.).....j.f[$:.P8....J..R..s...e.r...g.....Mz...En.....3.I...
1J!.....D_.v.....u..W .....+,.....?a...E.>./.... .].{6].....40..00..|.
+.....y.....l...h.f.v....4.....2....=.P...:..v
,...*.....G0E.!..=.....M.lYI._.%Q...h\4...E..
x. T...GVE.....o.X..10.x..nJ.?...E.u.}Y...x*{.ag|^....\..N..../....y.....F0D. h2R.zU.M..4.Gj.X.f.il..E.-..... <....
Z..J.<?.E.Jr./#.>..... .u....I.T.@.....g/N..#@h.k.@...}.....B.....F0D. LH.t.:....yd..>&...N...fK .C..3.. 2.....&.y.
~.....w.....=....0'.+.....7.
..0.0
..+.....0
..+.....0<. +.....7.../0-.%+.....7.....F.....]...0.....d..-0....+.....0..0s..+.....0..ghttp://www.mic
rosoft.com/pkiops/certs/Microsoft%20Azure%20RSA%20TLS%20Issuing%20CA%2007%20-%20xsign.crt0-..+.....0..!http://oneocsp.microsoft
.com/ocsp0...U.....jo4^.....3..3u.%:...0...U.....0?..U...806..hierarchyapi.onenote.com..*.hierarchyapi.onenote.com0...U.
.....0.0j..U...c0a0_.].[.Yhttp://www.microsoft.com/pkiops/crl/Microsoft%20Azure%20RSA%20TLS%20Issuing%20CA%2007.crl0f..U. ._0]
0Q..+.....7L.}..0A0?..+.....3http://www.microsoft.com/pkiops/Docs/Repository.htm0...g.....0...U.#..0.....;....k..+...R.zP.0
...U.%..0...+.....+.....0
. *.H..
.....%..4,.)~j.....NA/....U.....u.._..@3....9.F.P.....s..@wjs...|
...>...G..DM1.,.....q!q.k.....2.....-A..>k
.*L;p7.....-...-)...F.P.!.Y1..,'....0@k..Y..O.EI...2'.~...F...jr/k.e.z.....(..`.Peu.;.n|..-2:..@8..~a}f,"...a._...
...^.T`[.q...}.A.6.f.!.....n...T.....0.....`.K3..!..X^ h...O+S.^[.8.@.5H'. .=,8`.n`.3..F.....,..
.....*.F..'Mg.2ux>..|.e.....E`=;....]..)6... .CC.3..Y.U.....8..N....4.L..`
.....6Qh.b.|...f.l.....K...c.l..udpY...Z.:..2yl+..A..'.z.!....W..!..K..
..X.7OP..e...0...0.....
C.P..5/..y.r..P0
. *.H..
.....0a1.0 ..U....US1.0...U.
..DigiCert Inc1.0...U....www.digicert.com1 0...U....DigiCert Global Root G20..
230608000000Z.
260825235959Z0]1.0 ..U....US1.0...U.
..Microsoft Corporation1.0,..U...%Microsoft Azure RSA TLS Issuing CA 070.."0
. *.H..
.....0..
V client pkt(s), ^ server pkt(s), T turn(s).
Stream
ASCII
Show data as
Entire conversation (24 kB)
Find Next
Find:
مساعدة
أغلق
Back
...Save as
Print
Filter Out This Stream

tcp.stream eq 15

Info	Length	Protocol	Destination	Source	Time	.No
Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM [SYN] 443 → 49199 66		TCP	52.109.72.2	172.20.10.11	0.784992 99	
Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM [SYN, ACK] 49199 → 443 66		TCP	172.20.10.11	52.109.72.2	0.929063 103	
Seq=1 Ack=1 Win=262144 Len=0 [ACK] 443 → 49199 54		TCP	52.109.72.2	172.20.10.11	0.929283 104	
Client Hello (SNI=hierarchyapi.onenote.com) 275		TLSv1.2	52.109.72.2	172.20.10.11	0.930280 105	
Seq=1 Ack=222 Win=4194048 Len=1400 [TCP segment of a reassembled PDU] [ACK] 49199 → 443 1454		TCP	172.20.10.11	52.109.72.2	1.173774 130	
Seq=1401 Ack=222 Win=4194048 Len=1400 [TCP segment of a reassembled PDU] [ACK] 49199 → 443 1454		TCP	172.20.10.11	52.109.72.2	1.173774 131	
Seq=2801 Ack=222 Win=4194048 Len=1400 [TCP segment of a reassembled PDU] [ACK] 49199 → 443 1454		TCP	172.20.10.11	52.109.72.2	1.173774 132	
Seq=4201 Ack=222 Win=4194048 Len=1400 [TCP segment of a reassembled PDU] [ACK] 49199 → 443 1454		TCP	172.20.10.11	52.109.72.2	1.173774 133	
Seq=222 Ack=5601 Win=262144 Len=0 [ACK] 443 → 49199 54		TCP	52.109.72.2	172.20.10.11	1.173959 134	
Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done 447		TLSv1.2	172.20.10.11	52.109.72.2	1.176299 135	
Seq=222 Ack=5994 Win=261632 Len=0 [ACK] 443 → 49199 54		TCP	52.109.72.2	172.20.10.11	1.176396 136	
Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 212		TLSv1.2	52.109.72.2	172.20.10.11	1.186955 138	
Seq=380 Ack=5994 Win=261632 Len=1400 [TCP segment of a reassembled PDU] [ACK] 443 → 49199 1454		TCP	52.109.72.2	172.20.10.11	1.188087 139	
Application Data 447		TLSv1.2	52.109.72.2	172.20.10.11	1.188087 140	
Change Cipher Spec, Encrypted Handshake Message 105		TLSv1.2	172.20.10.11	52.109.72.2	1.433593 165	
Seq=2173 Ack=6045 Win=261632 Len=0 [ACK] 443 → 49199 54		TCP	52.109.72.2	172.20.10.11	1.433726 166	
Seq=6045 Ack=2173 Win=4194304 Len=0 [ACK] 49199 → 443 54		TCP	172.20.10.11	52.109.72.2	1.433860 168	
Application Data 838		TLSv1.2	172.20.10.11	52.109.72.2	1.440178 169	
Seq=2173 Ack=6829 Win=260864 Len=0 [ACK] 443 → 49199 54		TCP	52.109.72.2	172.20.10.11	1.440328 170	
Application Data 243		TLSv1.2	52.109.72.2	172.20.10.11	1.442363 171	
Seq=2362 Ack=6829 Win=260864 Len=1400 [TCP segment of a reassembled PDU] [ACK] 443 → 49199 1454		TCP	52.109.72.2	172.20.10.11	1.447149 172	

```
Frame 104: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{05E1A00D-E5DD-49A8-BD4B-1024CA6811FD}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{05E1A00D-E5DD-49A8-BD4B-1024CA6811FD})
    Encapsulation type: Ethernet (1)
    السعودية - التوقيت الرسمي Arrival Time: Jan 26, 2025 08:48:35.601020000
    UTC Arrival Time: Jan 26, 2025 05:48:35.601020000 UTC
    Epoch Arrival Time: 1737870515.601020000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000220000 seconds]
    [Time delta from previous displayed frame: 0.000220000 seconds]
    [Time since reference or first frame: 0.929283000 seconds]
    Frame Number: 104
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
Ethernet II, Src: Intel_f0:71:3e (cc:15:31:f0:71:3e), Dst: 1a:fa:b7:e5:6f:64 (1a:fa:b7:e5:6f:64)
Internet Protocol Version 4, Src: 172.20.10.11, Dst: 52.109.72.2
```




Standard query 0xe2f0 A capi.grammarly.com 98 DNS …fe80::18fa:b7ff …:fe80::aed8:43fa:7d1 0.226245 17
Standard query 0x63ec AAAA capi.grammarly.com 98 DNS …fe80::18fa:b7ff …:fe80::aed8:43fa:7d1 0.226362 18
…Standard query response 0xe2f0 A capi.grammarly.com A 52.45.139.187 A 34.225.74.204 A 3.230.79.67 A 54.221.2 226 DNS …fe80::aed8:43fa …fe80::18fa:b7ff:fee5 0.297807 19
…Standard query response 0x63ec AAAA capi.grammarly.com AAAA 64:ff9b::22e5:509 AAAA 64:ff9b::12cc:3b0b AAAA 6 322 DNS …fe80::aed8:43fa …fe80::18fa:b7ff:fee5 0.297807 20
Len=79 50752 → 443 141 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 1.093404 128
Len=32 443 → 50752 94 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 1.128714 129
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 1.297843 164
Len=24 50752 → 443 86 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 1.433860 167
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 1.640933 191
Len=24 50752 → 443 86 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 1.778423 193
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 1.982612 203
Len=24 50752 → 443 86 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 2.151962 205
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 2.357659 219
Len=24 50752 → 443 86 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 2.521988 226
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 2.729705 228
Len=24 50752 → 443 86 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 2.874802 234
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 3.091426 242
Len=24 50752 → 443 86 UDP …:2001:16a2:c050 …::2a00:1450:4006:80e 3.241326 253
Standard query 0xe6f9 A stream-production.avcdn.net OPT 130 DNS …fe80::18fa:b7ff …:fe80::aed8:43fa:7d1 3.274850 257
…Standard query response 0xe6f9 A stream-production.avcdn.net CNAME stream-production.avcdn.net.akamaized.net 233 DNS …fe80::aed8:43fa …fe80::18fa:b7ff:fee5 3.356126 283
Len=29 443 → 50752 91 UDP …:2a00:1450:4006 …:2001:16a2:c050:2aca 3.649542 315

Frame 128: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface \Device\NPF_{05E1A00D-E5DD-49A8-BD4B-1024CA6811FD}, id 0
Ethernet II, Src: 1a:fa:b7:e5:6f:64 (1a:fa:b7:e5:6f:64), Dst: Intel_f0:71:3e (cc:15:31:f0:71:3e)
Internet Protocol Version 6, Src: 2a00:1450:4006:80e::200a, Dst: 2001:16a2:c050:2aca:11e4:8644:c628:c9c4
User Datagram Protocol, Src Port: 443, Dst Port: 50752
Source Port: 443
Destination Port: 50752
Length: 87
Checksum: 0x32db [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
[Timestamps]
UDP payload (79 bytes)
Data (79 bytes)
Data: 4d7ff81b5500a0a9847c14726b94bcb7dc95d457d6d94e53f649e30bb52858c13e065faab8c383ec578dbb702d9883f22c3d646f5cc8624054b02e61e490ae93b067abb9f1d2396623dbdf33a90d22
[Length: 79]