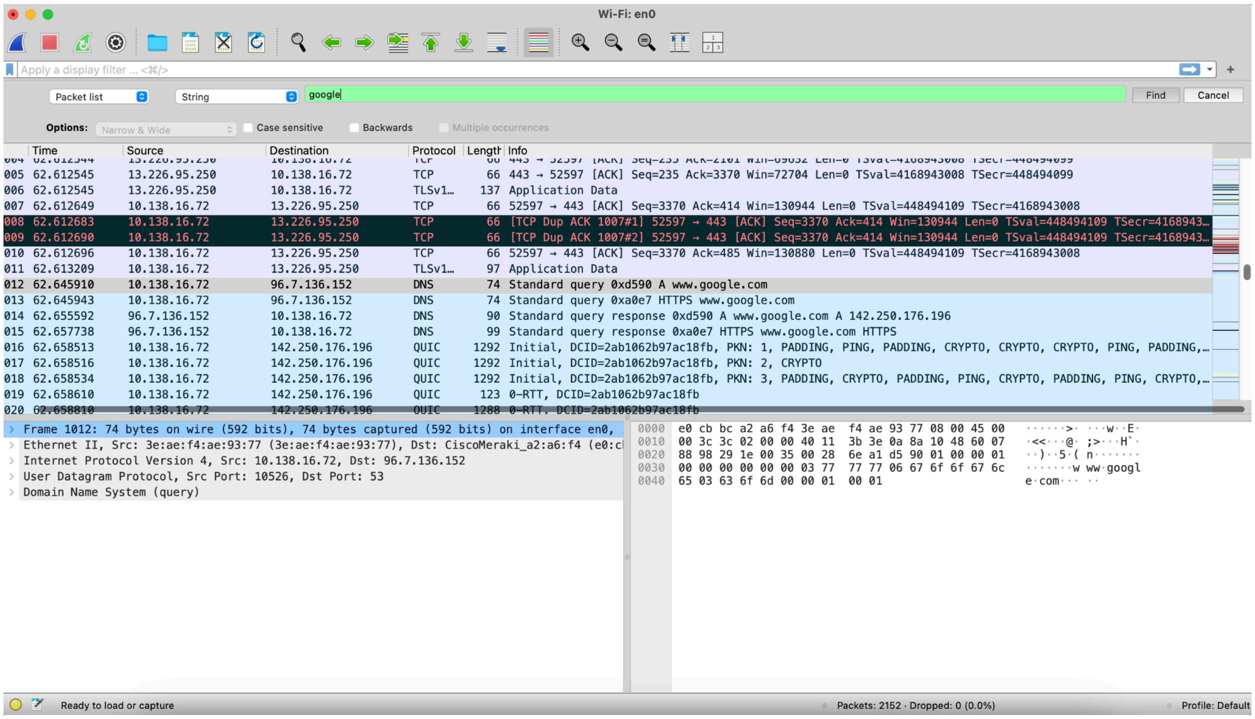
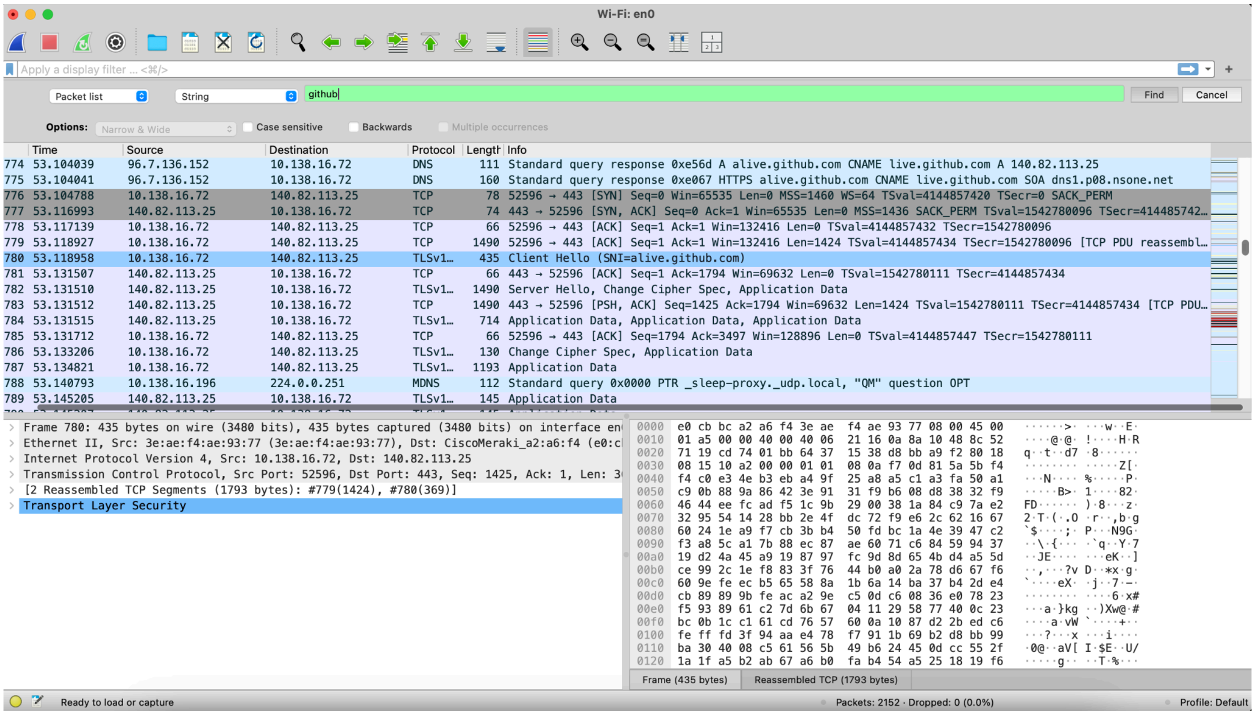


```
     Time        Source           Destination      Protocol Length Info
004  62.612544   13.226.95.250    10.138.16.72     TCP        66   443 → 52597 [ACK] Seq=235 Ack=2101 Win=69632 Len=0 TSval=4168943008 TSecr=448494099
005  62.612545   13.226.95.250    10.138.16.72     TCP        66   443 → 52597 [ACK] Seq=235 Ack=3370 Win=72704 Len=0 TSval=4168943008 TSecr=448494099
006  62.612545   13.226.95.250    10.138.16.72     TLSv1…    137   Application Data
007  62.612649   10.138.16.72     13.226.95.250    TCP        66   52597 → 443 [ACK] Seq=3370 Ack=414 Win=130944 Len=0 TSval=448494109 TSecr=4168943008
008  62.612683   10.138.16.72     13.226.95.250    TCP        66   [TCP Dup ACK 1007#1] 52597 → 443 [ACK] Seq=3370 Ack=414 Win=130944 Len=0 TSval=448494109 TSecr=4168943…
009  62.612690   10.138.16.72     13.226.95.250    TCP        66   [TCP Dup ACK 1007#2] 52597 → 443 [ACK] Seq=3370 Ack=414 Win=130944 Len=0 TSval=448494109 TSecr=4168943…
010  62.612696   10.138.16.72     13.226.95.250    TCP        66   52597 → 443 [ACK] Seq=3370 Ack=485 Win=130880 Len=0 TSval=448494109 TSecr=4168943008
011  62.613209   10.138.16.72     13.226.95.250    TLSv1…     97   Application Data
012  62.645910   10.138.16.72     96.7.136.152     DNS        74   Standard query 0xd590 A www.google.com
013  62.645943   10.138.16.72     96.7.136.152     DNS        74   Standard query 0xa0e7 HTTPS www.google.com
014  62.655592   96.7.136.152     10.138.16.72     DNS        90   Standard query response 0xd590 A www.google.com A 142.250.176.196
015  62.657738   96.7.136.152     10.138.16.72     DNS        99   Standard query response 0xa0e7 HTTPS www.google.com HTTPS
016  62.658513   10.138.16.72     142.250.176.196  QUIC     1292   Initial, DCID=2ab1062b97ac18fb, PKN: 1, PADDING, PING, PADDING, CRYPTO, CRYPTO, CRYPTO, PING, PADDING,…
017  62.658516   10.138.16.72     142.250.176.196  QUIC     1292   Initial, DCID=2ab1062b97ac18fb, PKN: 2, CRYPTO
018  62.658534   10.138.16.72     142.250.176.196  QUIC     1292   Initial, DCID=2ab1062b97ac18fb, PKN: 3, PADDING, CRYPTO, PADDING, PING, CRYPTO, PADDING, PING, CRYPTO,…
019  62.658610   10.138.16.72     142.250.176.196  QUIC      123   0-RTT, DCID=2ab1062b97ac18fb
020  62.658810   10.138.16.72     142.250.176.196  QUIC     1288   0-RTT, DCID=2ab1062b97ac18fb
```

```
> Frame 1012: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0,
> Ethernet II, Src: 3e:ae:f4:ae:93:77 (3e:ae:f4:ae:93:77), Dst: CiscoMeraki_a2:a6:f4 (e0:c
> Internet Protocol Version 4, Src: 10.138.16.72, Dst: 96.7.136.152
> User Datagram Protocol, Src Port: 10526, Dst Port: 53
> Domain Name System (query)
```

```
0000  e0 cb bc a2 a6 f4 3e ae  f4 ae 93 77 08 00 45 00   ······>· ··w··E·
0010  00 3c 3c 02 00 00 40 11  3b 3e 0a 8a 10 48 60 07   ·<<···@· ;>···H`·
0020  88 98 29 1e 00 35 00 28  6e a1 d5 90 01 00 00 01   ··)··5·( n·······
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······w ww·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com··· ··
```

Ready to load or capture   Packets: 2152 · Dropped: 0 (0.0%)   Profile: Default



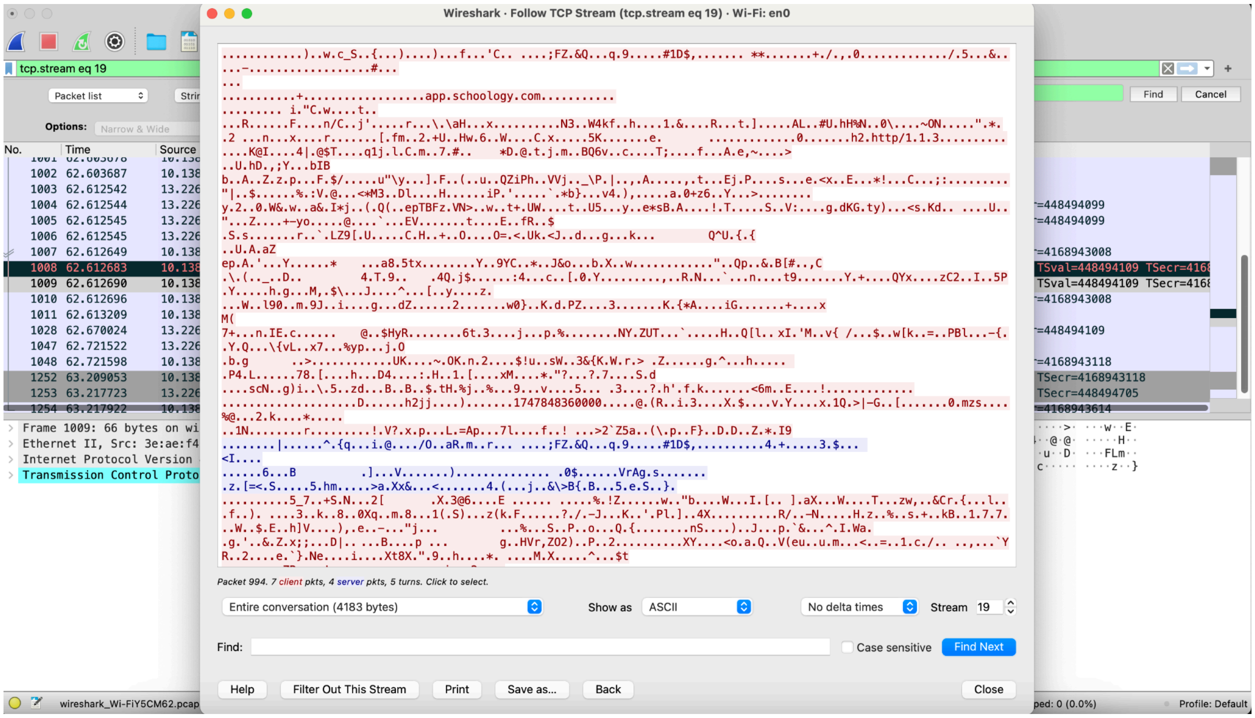
```
     Time        Source           Destination      Protocol Length Info
774  53.104039   96.7.136.152     10.138.16.72     DNS       111   Standard query response 0xe56d A alive.github.com CNAME live.github.com A 140.82.113.25
775  53.104041   96.7.136.152     10.138.16.72     DNS       160   Standard query response 0xe067 HTTPS alive.github.com CNAME live.github.com SOA dns1.p08.nsone.net
776  53.104788   10.138.16.72     140.82.113.25    TCP        78   52596 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4144857420 TSecr=0 SACK_PERM
777  53.116993   140.82.113.25    10.138.16.72     TCP        74   443 → 52596 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1436 SACK_PERM TSval=1542780096 TSecr=414485742…
778  53.117139   10.138.16.72     140.82.113.25    TCP        66   52596 → 443 [ACK] Seq=1 Ack=1 Win=132416 Len=0 TSval=4144857432 TSecr=1542780096
779  53.118927   10.138.16.72     140.82.113.25    TCP      1490   52596 → 443 [ACK] Seq=1 Ack=1 Win=132416 Len=1424 TSval=4144857434 TSecr=1542780096 [TCP PDU reassembl…
780  53.118958   10.138.16.72     140.82.113.25    TLSv1…    435   Client Hello (SNI=alive.github.com)
781  53.131507   140.82.113.25    10.138.16.72     TCP        66   443 → 52596 [ACK] Seq=1 Ack=1794 Win=69632 Len=0 TSval=1542780111 TSecr=4144857434
782  53.131510   140.82.113.25    10.138.16.72     TLSv1…   1490   Server Hello, Change Cipher Spec, Application Data
783  53.131512   140.82.113.25    10.138.16.72     TCP      1490   443 → 52596 [PSH, ACK] Seq=1425 Ack=1794 Win=69632 Len=1424 TSval=1542780111 TSecr=4144857434 [TCP PDU…
784  53.131515   140.82.113.25    10.138.16.72     TLSv1…    714   Application Data, Application Data, Application Data
785  53.131712   10.138.16.72     140.82.113.25    TCP        66   52596 → 443 [ACK] Seq=1794 Ack=3497 Win=128896 Len=0 TSval=4144857447 TSecr=1542780111
786  53.133206   10.138.16.72     140.82.113.25    TLSv1…    130   Change Cipher Spec, Application Data
787  53.134821   10.138.16.72     140.82.113.25    TLSv1…   1193   Application Data
788  53.140793   10.138.16.196    224.0.0.251      MDNS      112   Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question OPT
789  53.145205   140.82.113.25    10.138.16.72     TLSv1…    145   Application Data
```

```
> Frame 780: 435 bytes on wire (3480 bits), 435 bytes captured (3480 bits) on interface en
> Ethernet II, Src: 3e:ae:f4:ae:93:77 (3e:ae:f4:ae:93:77), Dst: CiscoMeraki_a2:a6:f4 (e0:c
> Internet Protocol Version 4, Src: 10.138.16.72, Dst: 140.82.113.25
> Transmission Control Protocol, Src Port: 52596, Dst Port: 443, Seq: 1425, Ack: 1, Len: 3
> [2 Reassembled TCP Segments (1793 bytes): #779(1424), #780(369)]
> Transport Layer Security
```

```
0000  e0 cb bc a2 a6 f4 3e ae  f4 ae 93 77 08 00 45 00   ······>· ··w··E·
0010  01 a5 00 00 40 00 40 06  21 16 0a 8a 10 48 8c 52   ····@·@· !····H·R
0020  71 19 cd 74 01 bb 64 37  15 38 d8 bb a9 f2 80 18   q··t··d7 ·8······
0030  08 15 10 a2 00 00 01 01  08 0a f7 0d 81 5a 5b f4   ········ ·····Z[·
0040  f4 c0 e3 4e b3 eb a4 9f  25 a8 a5 c1 a3 fa 50 a1   ···N···· %·····P·
0050  c9 0b 88 9a 86 42 3e 91  31 f9 b6 08 d8 38 32 f9   ·····B>· 1····82·
0060  46 44 ee fc ad f5 1c 9b  29 00 38 1a 84 c9 7a e2   FD······ )·8···z·
0070  32 95 54 14 28 bb 2e 4f  dc 72 f9 e6 2c 62 16 67   2·T·(·.O ·r··,b·g
0080  60 24 1e a9 f7 cb 3b b4  50 fd bc 1a 4e 39 47 c2   `$····;· P···N9G·
0090  f3 a8 5c a1 7b 88 ec 87  ae 60 71 c6 84 59 94 37   ··\·{··· ·`q··Y·7
00a0  19 d2 4a 45 a9 19 87 97  fc 9d 8d 65 4b d4 a5 5d   ··JE···· ···eK··]
00b0  ce 99 2c 1e f8 83 3f 76  44 b0 a0 2a 78 d6 67 f6   ··,···?v D··*x·g·
00c0  60 9e fe ec b5 65 58 8a  1b 6a 14 ba 37 b4 2d e4   `····eX· ·j··7·-·
00d0  cb 89 89 9b fe ac a2 9e  c5 0d c6 08 36 e0 78 23   ········ ····6·x#
00e0  f5 93 89 61 c2 7d 6b 67  04 11 29 58 77 40 0c 23   ···a·}kg ··)Xw@·#
00f0  bc 0b 1c c1 61 cd 76 57  60 0a 10 87 d2 2b ed c6   ····a·vW `····+··
0100  fe ff fd 3f 94 aa e4 78  f7 91 1b 69 b2 d8 bb 99   ···?···x ···i····
0110  ba 30 40 08 c5 61 56 5b  49 b6 24 45 0d cc 55 2f   ·0@··aV[ I·$E··U/
0120  1a 1f a5 b2 ab 67 a6 b0  fa b4 54 a5 25 18 19 f6   ·····g·· ··T·%···
```

Frame (435 bytes)   Reassembled TCP (1793 bytes)

Ready to load or capture   Packets: 2152 · Dropped: 0 (0.0%)   Profile: Default



Wireshark · Follow TCP Stream (tcp.stream eq 19) · Wi-Fi: en0

```
............)..w.c_S..{...)....)...f...'C.. ....;FZ.&Q...q.9.....#1D$,....... **.......+./.,.0............./.5...&..
...–..................#...
...
..........+.................app.schoology.com..........
......... i."C.w....t..
...R......F....n/C..j'.....r...\.\aH...x.........N3..W4kf..h....1.&....R...t.].....AL..#U.hH%N..0\....~ON.....".*.
.2 ...n...x....r.......[.fm..2.+U..Hw.6..W....C.x.....5K.......e.      .............0.......h2.http/1.1.3.........
....K@I....4|.@$T....q1j.l.C.m..7.#..    *D.@.t.j.m..BQ6v..c....T;....f...A.e,~....>
..U.hD.,;Y...bIB
b..A..Z.z.p...F.$/.....u"\y...].F..(..u..QZiPh..VVj.._\P.|..,.A.....,.t...Ej.P....s...e.<x..E...*!...C...;:........
"|..$......%.:V.@...<*M3..Dl....H......iP.'.....`.*b}...v4.),.....a.0+z6..Y...>.......
y.2..0.W&.w..a&.I*j..(.Q(..epTBFz.VN>..w..t+.UW....t..U5...y..e*sB.A....!.T.....S..V:....g.dKG.ty)...<s.Kd.. ....U..
"...Z....+–yo.....@....`...EV.......t....E..fR..$
.S.s.......r..`.LZ9[.U.....C.H..+..O....O=.<.Uk.<J..d...g...k...       Q^U.{.{
..U.A.aZ
ep.A.'...Y......*   ...a8.5tx........Y..9YC..*..J&o...b.X..w...........".Qp..&.B[#..,C
.\.(.._..D..        4.T.9..   .4Q.j$......:4...c..[.0.Y.........,..R.N...`...n....t9.......Y.+....QYx....zC2..I..5P
.Y.....h.g...M,.$\...J....^...[..y....z.
...W..l90..m.9J..i....g...dZ......2.......w0}..K.d.PZ....3.......K.{*A....iG.......+....x
M(
7+...n.IE.c......   @..$HyR........6t.3....j...p.%........NY.ZUT...`.....H..Q[l.. xI.'M..v{ /...$..w[k..=..PBl...–{.
.Y.Q...\{vL..x7...%yp...j.O
.b.g      ..>............UK....~.OK.n.2....$!u..sW..3&{K.W.r.> .Z......g.^...h.....
.P4.L......78.[....h...D4....:.H..1.[....xM....*."?...?.7....S.d
....scN..g)i..\.5..zd...B..B..$.tH.%j..%...9...v....5... .3....?.h'.f.k.......<6m..E....!............
....................D......h2jj....).......1747848360000.....@.(R..i.3....X.$....v.Y....x.1Q.>|–G..[.......0.mzs....
%@...2.k....*.....
..1N........r.........!.V?.x.p...L.=Ap...7l....f..! ...>2`Z5a..(\.p..F}..D.D..Z.*.I9
........|......^.{q...i.@..../O..aR.m..r... ....;FZ.&Q...q.9.....#1D$,..........4.+.....3.$...
<I....
......6...B         .]...V.......).............. .0$......VrAg.s.......
.z.[=<.S.....5.hm.....>a.Xx&...<.......4.(...j..&\>B{.B...5.e.S..}.
..........5_7..+S.N...2[       .X.3@6....E ...... .....%.!Z......w.."b....W...I.[.. ].aX...W....T...zw,..&Cr.{...l..
.f..). ....3..k..8..0Xq..m.8...1(.S)...z(k.F......?./.–J...K..'.Pl.]..4X..........R/..–N.....H.z..%..s.+..kB..1.7.7.
..W..$.E..h]V....),.e..–..."j...         ...%...S..P..o...Q.{........nS....)..J...p.`&...^.I.Wa.
.g.'..&.Z.x;;...D|.. ...B....p ...       g..HVr,ZO2)..P..2..........XY....<o.a.Q..V(eu..u.m...<..=..1.c./.. ..,...`Y
R..2....e.`}.Ne....i....Xt8X.".9..h....*. ....M.X.....^...$t
```

Packet 994. 7 client pkts, 4 server pkts, 5 turns. Click to select.

Entire conversation (4183 bytes) | Show as ASCII | No delta times | Stream 19

Find: □ Case sensitive | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

```
tcp.stream eq 19

No.   Time       Source
1002  62.603687  10.138                =448494099
1003  62.612542  13.226                =448494099
1004  62.612544  13.226
1005  62.612545  13.226                =4168943008
1006  62.612545  13.226
1007  62.612649  10.138
1008  62.612683  10.138                TSval=448494109 TSecr=4168
1009  62.612690  10.138                TSval=448494109 TSecr=4168
1010  62.612696  10.138                =4168943008
1011  62.613209  10.138
1028  62.670024  13.226                =448494109
1047  62.721522  13.226
1048  62.721598  10.138                =4168943118
1252  63.209053  10.138                TSecr=4168943118
1253  63.217723  13.226                TSecr=448494705
1254  63.217922  10.138                =4168943614

> Frame 1009: 66 bytes on wi
> Ethernet II, Src: 3e:ae:f4
> Internet Protocol Version
> Transmission Control Proto
```

Summary of Findings

- **Client IP:** 10.138.16.72
- **Server IP:** 13.226.95.250 (likely part of AWS CloudFront)
- **Destination Host (SNI):** app.schoology.com
- **Protocol Used:** TLS 1.3 over TCP port 443
- **Session Status:** Normal HTTPS session with complete handshake and termination
- **Potential Issue:** A couple of TCP duplicate ACKs suggest possible minor packet loss or reordering, but the session continued normally.

Step-by-Step Analysis

1. TLS Handshake (Packets 991–997)

- 991–993: TCP 3-way handshake:
  - SYN → SYN-ACK → ACK between client and server (port 443)
- 994–995: **Client Hello** including the SNI app.schoology.com (TLS handshake begins)
- 997: Server responds with **Server Hello**, completes the handshake with encryption setup (TLS 1.3)

2. TLS Encrypted Application Data Transfer (Packets 998–1011)

- After the handshake:
  - Multiple **Application Data** packets are exchanged.
  - Initial packets from client (999–1002): TLS-encrypted data likely includes HTTP request.
  - Server replies with Application Data (1003, 1006, 1047), likely encrypted HTTP response.
- **Note**: All content after handshake is encrypted, as expected in TLS 1.3.

3. TCP Anomalies (Packets 1008–1010)

- Two **TCP Duplicate ACKs** were observed:
  - Packets 1008, 1009 indicate the client sent repeated ACKs for packet 1007, implying possible **packet loss or reordering**.
  - This is **not an attack**—just a minor network hiccup; the stream continued normally.

4. Graceful Termination (Packets 1252–1254)

- **FIN-ACK exchange** completes the TCP session teardown:
  - Client initiates termination (1252)
  - Server acknowledges and sends its own FIN (1253)
  - Client sends final ACK (1254)

Conclusion

- **No evidence of attack or anomaly** — standard secure TLS session
- Proper session establishment, data exchange, and termination
- Minor TCP duplicate ACKs observed — typical in real-world networks, **no retransmission required**
- Destination server is likely **part of a CDN** serving app.schoology.com

Forensic Network Activity Timeline

Case: HTTPS Session to app.schoology.com
Client IP: 10.138.16.72
Server IP: 13.226.95.250
SNI (Target Host): app.schoology.com
Protocol: TLS 1.3 over TCP
Port: 443 (HTTPS)

#	Timestamp (s)	Source IP	Destination IP	Protocol	Description
991	62.587697	10.138.16.72	13.226.95.250	TCP	Client initiates connection with SYN to port 443
992	62.595061	13.226.95.250	10.138.16.72	TCP	Server responds with SYN-ACK
993	62.595163	10.138.16.72	13.226.95.250	TCP	Client sends ACK, completing TCP 3-way handshake
995	62.595492	10.138.16.72	13.226.95.250	TLS 1.3	Client Hello sent with SNI = app.schoology.com
997	62.603154	13.226.95.250	10.138.16.72	TLS 1.3	Server Hello, Change Cipher Spec, Application Data
999–1002	62.603478–62.603687	10.138.16.72	13.226.95.250	TLS 1.3	Client sends encrypted application data

1003, 1006	62.612542–62.612545	13.226.95.250	10.138.16.72	TLS 1.3	Server sends encrypted application data
1007	62.612649	10.138.16.72	13.226.95.250	TCP	Client sends ACK
1008–1009	62.612683–62.612690	10.138.16.72	13.226.95.250	TCP	Duplicate ACKs indicating potential packet reordering
1010–1011	62.612696–62.613209	10.138.16.72	13.226.95.250	TCP/TLS	Final ACK and encrypted data from client
1047–1048	62.721522–62.721598	13.226.95.250	10.138.16.72	TLS 1.3	Server sends additional application data; client ACKs
1252	63.209053	10.138.16.72	13.226.95.250	TCP	Client sends FIN-ACK, initiating connection teardown
1253	63.217723	13.226.95.250	10.138.16.72	TCP	Server responds with FIN-ACK
1254	63.217922	10.138.16.72	13.226.95.250	TCP	Client sends final ACK, session ends cleanly

Conclusion:

This timeline confirms a normal and complete HTTPS session initiated by the client to app.schoology.com, with a successful TLS 1.3 handshake, data exchange, and clean teardown. No signs of abnormal behavior or attack are present. The duplicate ACKs are minor and did not affect session integrity.