Qassim University جامعة القصيم

Lab 1

CS471 – Web Technologies

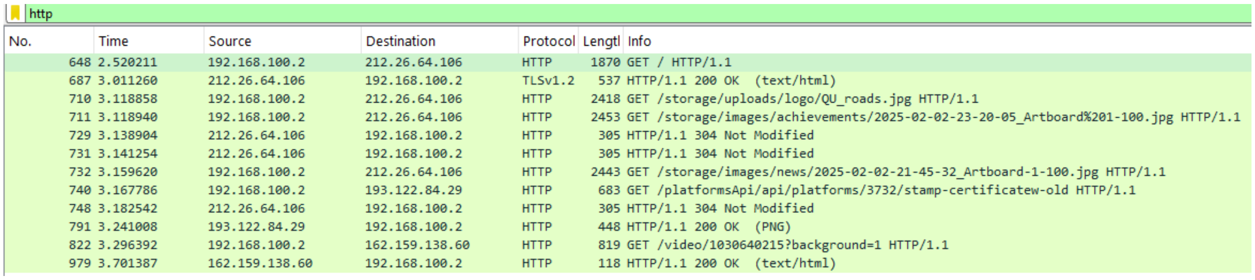
Muath Altresy 421107777

Dr. Musa Suliman Musa Al-Zakan

4/2/2025

Part 1: Filter HTTP packets and analyze them.

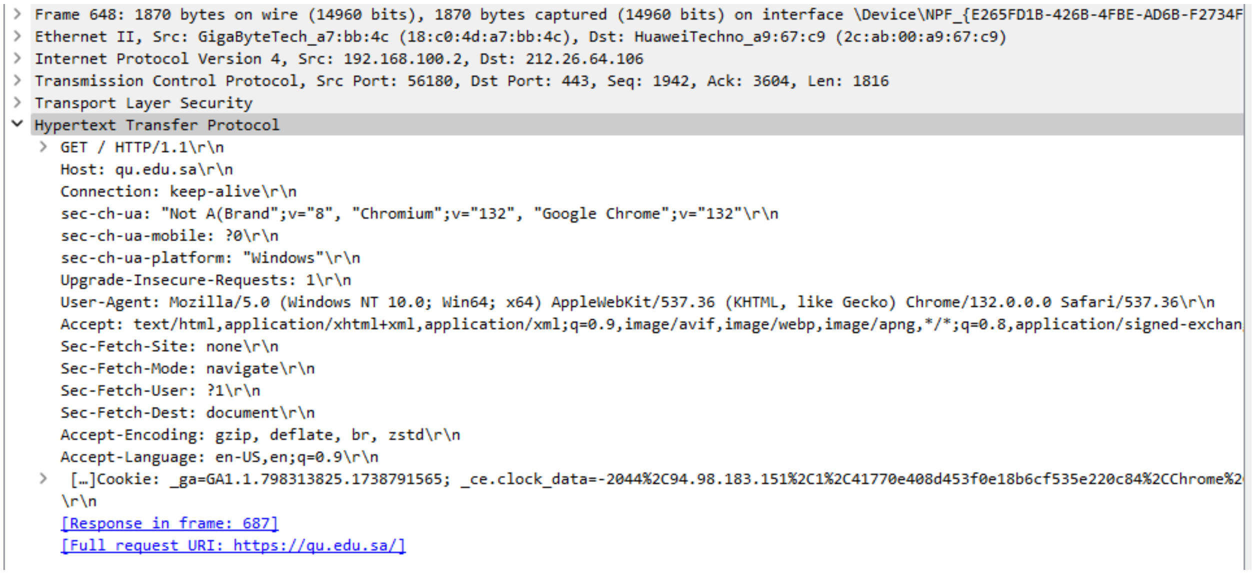
Step 1: In the filter bar type http and press Enter.



http

No.	Time	Source	Destination	Protocol	Lengtl	Info
648	2.520211	192.168.100.2	212.26.64.106	HTTP	1870	GET / HTTP/1.1
687	3.011260	212.26.64.106	192.168.100.2	TLSv1.2	537	HTTP/1.1 200 OK (text/html)
710	3.118858	192.168.100.2	212.26.64.106	HTTP	2418	GET /storage/uploads/logo/QU_roads.jpg HTTP/1.1
711	3.118940	192.168.100.2	212.26.64.106	HTTP	2453	GET /storage/images/achievements/2025-02-02-23-20-05_Artboard%201-100.jpg HTTP/1.1
729	3.138904	212.26.64.106	192.168.100.2	HTTP	305	HTTP/1.1 304 Not Modified
731	3.141254	212.26.64.106	192.168.100.2	HTTP	305	HTTP/1.1 304 Not Modified
732	3.159620	192.168.100.2	212.26.64.106	HTTP	2443	GET /storage/images/news/2025-02-02-21-45-32_Artboard-1-100.jpg HTTP/1.1
740	3.167786	192.168.100.2	193.122.84.29	HTTP	683	GET /platformsApi/api/platforms/3732/stamp-certificatew-old HTTP/1.1
748	3.182542	212.26.64.106	192.168.100.2	HTTP	305	HTTP/1.1 304 Not Modified
791	3.241008	193.122.84.29	192.168.100.2	HTTP	448	HTTP/1.1 200 OK (PNG)
822	3.296392	192.168.100.2	162.159.138.60	HTTP	819	GET /video/1030640215?background=1 HTTP/1.1
979	3.701387	162.159.138.60	192.168.100.2	HTTP	118	HTTP/1.1 200 OK (text/html)

Step 3: Observe the HTTP request and response messages.

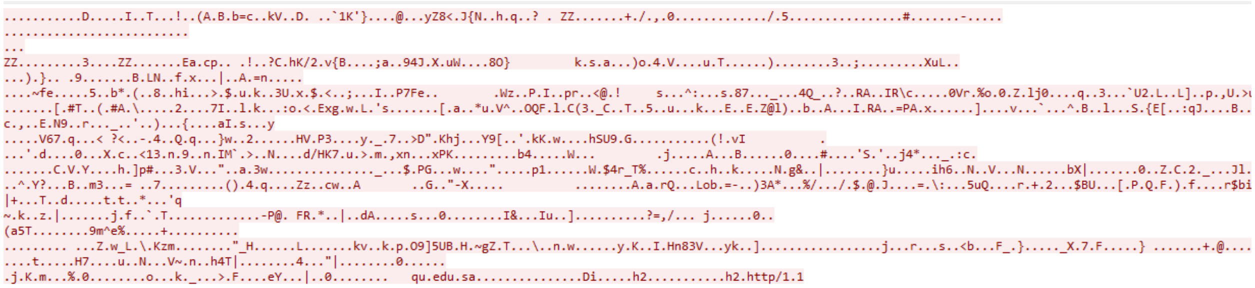


```
> Frame 648: 1870 bytes on wire (14960 bits), 1870 bytes captured (14960 bits) on interface \Device\NPF_{E265FD1B-426B-4FBE-AD6B-F2734F
> Ethernet II, Src: GigaByteTech_a7:bb:4c (18:c0:4d:a7:bb:4c), Dst: HuaweiTechno_a9:67:c9 (2c:ab:00:a9:67:c9)
> Internet Protocol Version 4, Src: 192.168.100.2, Dst: 212.26.64.106
> Transmission Control Protocol, Src Port: 56180, Dst Port: 443, Seq: 1942, Ack: 3604, Len: 1816
> Transport Layer Security
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: qu.edu.sa\r\n
    Connection: keep-alive\r\n
    sec-ch-ua: "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"\r\n
    sec-ch-ua-mobile: ?0\r\n
    sec-ch-ua-platform: "Windows"\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
    Sec-Fetch-Site: none\r\n
    Sec-Fetch-Mode: navigate\r\n
    Sec-Fetch-User: ?1\r\n
    Sec-Fetch-Dest: document\r\n
    Accept-Encoding: gzip, deflate, br, zstd\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  >  […]Cookie: _ga=GA1.1.798313825.1738791565; _ce.clock_data=-2044%2C94.98.183.151%2C1%2C41770e408d453f0e18b6cf535e220c84%2CChrome%2
    \r\n
    [Response in frame: 687]
    [Full request URI: https://qu.edu.sa/]
```

Part 2: Analyzing TCP/IP Traffic.

Task 1: Filter TCP packets

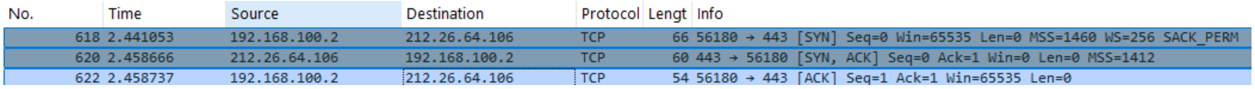
Step 4: shows the entire conversation between the client and server.



```
...........D.....I..T...!..(A.B.b=c..kV..D. ..`1K'}....@...yZ8<.J{N..h.q..? . ZZ.......+./.,.0............./.5................#.......-.....
.........................
...
ZZ.........3....ZZ.......Ea.cp.. .!..?C.hK/2.v{B....;a..94J.X.uW....8O}        k.s.a...)o.4.V....u.T......)........3..;.........XuL..
...).}.. .9.......B.LN..f.x...|..A.=n.....
....~fe.....5..b*.(..8..hi...>.$.u.k..3U.x.$.<..;...I..P7Fe..       .Wz..P.I..pr..<@.!     s...^:...s.87..._...4Q_..?..RA..IR\c.....0Vr.%o.0.Z.lj0....q..3...`U2.L..L]..p.,U.>u
.......[.#T..(.#A.\.....2....7I..l.k...:o.<.Exg.w.L.'s.......[.a..*u.V^..OQF.l.C(3._C..T..5..u...k...E..E.Z@l)..b..A...I.RA..=PA.x......]....v...`...^.B..l...S.{E[..:qJ....B..
c.,..E.N9..r..._..'..)...{....aI.s...y
.....V67.q...< ?<..-.4..Q.q...}w..2......HV.P3....y._.7..>D".Khj...Y9[..'.kK.w....hSU9.G...........(!.vI          .
...'.d....0...X.c..<13.n.9..n.IM`.>..N....d/HK7.u.>.m.,xn...xPK.........b4.....W...        .j.....A...B......0....#....'S.'..j4*..._.:c.
.......C.V.Y....h.]p#...3.V..."..a.3w..............._...$.PG...w...."......p1......W.$4r_T%......c..h..k.....N.g&..|........}u.....ih6..N..V...N......bX|.......0..Z.C.2._...Jl.
..^.Y?...B..m3...= ..7.........().4.q....Zz..cw..A       ..G.."-X.....          ........A.a.rQ...Lob.=-..)3A*...%/.../.$.@.J....=.\:...5uQ....r.+.2...$BU...[.P.Q.F.).f....r$bi
|+...T..d.....t.t..*...'q
~.k..z.|.......j.f..`.T.............-P@. FR.*..|..dA.....s...0........I&...Iu..]..........?=,/... j......0..
(a5T........9m^e%.....+.........
......... ...Z.w_L.\.Kzm........"_H......L.......kv..k.p.O9]5UB.H.~gZ.T...\..n.w......y.K..I.Hn83V...yk..]................j...r...s..<b...F_.}....._X.7.F.....} .......+.@....
....t.....H7....u..N...V~.n..h4T|........4..."|........0......
.j.K.m...%.0........o...k._...>.F....eY...|..0........   qu.edu.sa..............Di.....h2...........h2.http/1.1
```

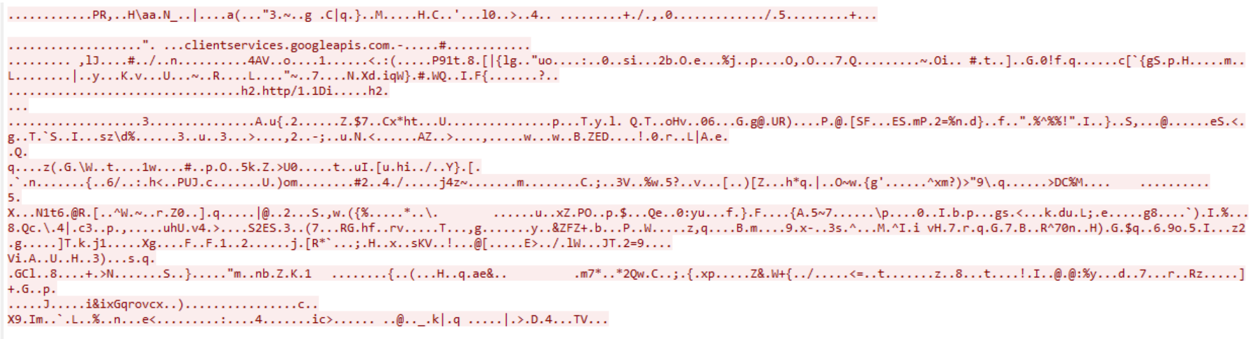
Task 2: Analyze TCP handshake and investigate Data Transfer and Termination

Step 2: Note the sequence and acknowledgment numbers.



```
No.        Time        Source          Destination     Protocol Lengt Info
       618 2.441053    192.168.100.2   212.26.64.106   TCP        66 56180 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
       620 2.458666    212.26.64.106   192.168.100.2   TCP        60 443 → 56180 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1412
       622 2.458737    192.168.100.2   212.26.64.106   TCP        54 56180 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
```

Step 3: Observe the data packets exchanged between the client and server.

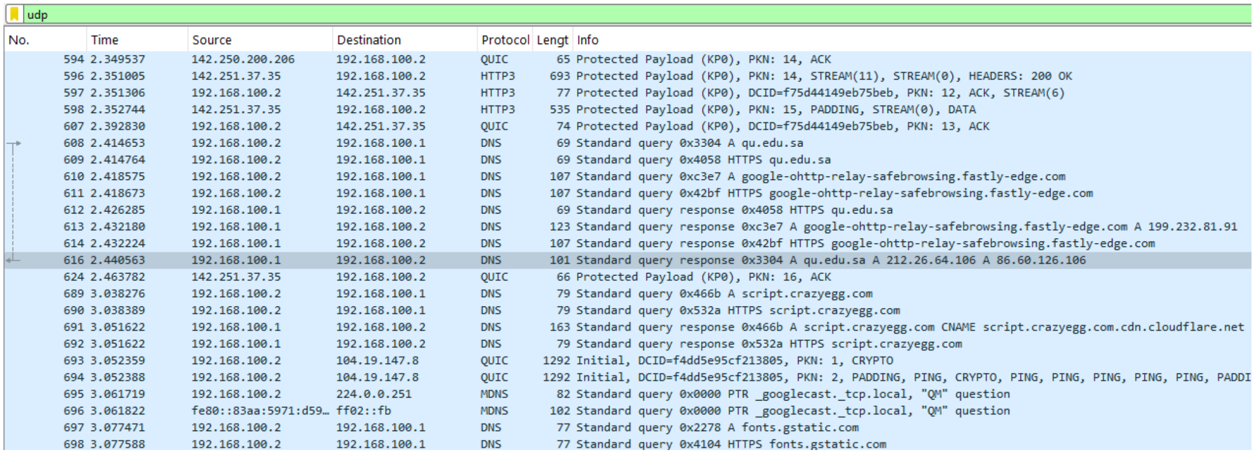


```
............PR,..H\aa.N_..|....a(..."3.~..g .C|q.}..M.....H.C..'...l0..>..4.. .........+./.,.0............./.5.........+...

...................". ...clientservices.googleapis.com.-.....#...........
......... ,lJ....#../..n..........4AV..o....1......<.:(.....P91t.8.[|{lg.."uo....:..0..si...2b.O.e...%j..p....O,.O...7.Q.........~.Oi.. #.t..]..G.0!f.q......c[`{gS.p.H.....m..
L........|..y...K.v...U...~..R....L...."~..7....N.Xd.iqW}.#.WQ..I.F{.......?..
...............................h2.http/1.1Di.....h2.
...
...................3...............A.u{.2......Z.$7..Cx*ht...U...............p...T.y.l. Q.T..oHv..06...G.g@.UR)....P.@.[SF...ES.mP.2=%n.d}..f..".%^%%!".I..}..S,...@......eS.<.
g..T.`S..I...sz\d%......3..u..3...>....,2..-;..u.N.<......AZ..>....,.....w...w..B.ZED....!.0.r..L|A.e.
.Q.
q....z(.G.\W..t....1w....#..p.O..5k.Z.>U0.....t..uI.[u.hi../..Y}.[.
.`.n.......{..6/..:.h<..PUJ.c.......U.)om........#2..4./.....j4z~.......m........C.;..3V..%w.5?..v...[..)[Z...h*q.|..O~w.{g'......^xm?)>"9\.q......>DC%M....   ..........
5.
X...N1t6.@R.[..^W.~..r.Z0..].q.....|@..2...S.,w.({%.....*..\.       ......u..xZ.PO..p.$...Qe..0:yu...f.}.F....{A.5~7......\p....0..I.b.p...gs.<...k.du.L;.e.....g8....`).I.%...
8.Qc.\.4|.c3..p.,.....uhU.v4.>....S2ES.3..(7...RG.hf..rv.....T...,g.......y..&ZFZ+.b...P..W.....z,q....B.m....9.x-..3s.^...M.^I.i vH.7.r.q.G.7.B..R^70n..H).G.$q..6.9o.5.I...z2
.g.....]T.k.j1.....Xg....F..F.1..2......j.[R*`...;.H..x..sKV..!...@[.....E>../.lW...JT.2=9....
Vi.A..U..H..3)...s.q.
.GCl..8....+.>N.......S..}....."m..nb.Z.K.1   ........{..(...H..q.ae&..         .m7*..*2Qw.C..;.{.xp.....Z&.W+{../.....<=..t.......z..8...t....!.I..@.@:%y...d..7...r..Rz.....]
+.G..p.
.....J.....i&ixGqrovcx..)................c..
X9.Im..`.L..%..n...e<.........:....4.......ic>...... ..@.._.k|.q .....|.>.D.4...TV...
```

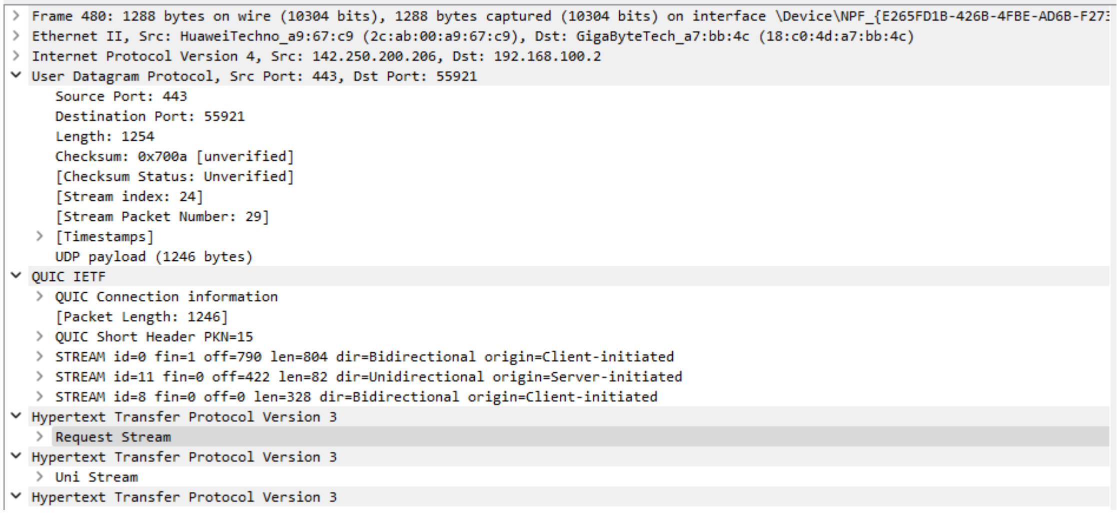
Part 3: Capturing and Analyzing UDP Traffic

Step 1: type UDP and press Enter



```
udp
No.      Time      Source               Destination     Protocol Lengt Info
     594 2.349537  142.250.200.206      192.168.100.2   QUIC       65 Protected Payload (KP0), PKN: 14, ACK
     596 2.351005  142.251.37.35        192.168.100.2   HTTP3     693 Protected Payload (KP0), PKN: 14, STREAM(11), STREAM(0), HEADERS: 200 OK
     597 2.351306  192.168.100.2        142.251.37.35   HTTP3      77 Protected Payload (KP0), DCID=f75d44149eb75beb, PKN: 12, ACK, STREAM(6)
     598 2.352744  142.251.37.35        192.168.100.2   HTTP3     535 Protected Payload (KP0), PKN: 15, PADDING, STREAM(0), DATA
     607 2.392830  192.168.100.2        142.251.37.35   QUIC       74 Protected Payload (KP0), DCID=f75d44149eb75beb, PKN: 13, ACK
     608 2.414653  192.168.100.2        192.168.100.1   DNS        69 Standard query 0x3304 A qu.edu.sa
     609 2.414764  192.168.100.2        192.168.100.1   DNS        69 Standard query 0x4058 HTTPS qu.edu.sa
     610 2.418575  192.168.100.2        192.168.100.1   DNS       107 Standard query 0xc3e7 A google-ohttp-relay-safebrowsing.fastly-edge.com
     611 2.418673  192.168.100.2        192.168.100.1   DNS       107 Standard query 0x42bf HTTPS google-ohttp-relay-safebrowsing.fastly-edge.com
     612 2.426285  192.168.100.1        192.168.100.2   DNS        69 Standard query response 0x4058 HTTPS qu.edu.sa
     613 2.432180  192.168.100.1        192.168.100.2   DNS       123 Standard query response 0xc3e7 A google-ohttp-relay-safebrowsing.fastly-edge.com A 199.232.81.91
     614 2.432224  192.168.100.1        192.168.100.2   DNS       107 Standard query response 0x42bf HTTPS google-ohttp-relay-safebrowsing.fastly-edge.com
     616 2.440563  192.168.100.1        192.168.100.2   DNS       101 Standard query response 0x3304 A qu.edu.sa A 212.26.64.106 A 86.60.126.106
     624 2.463782  142.251.37.35        192.168.100.2   QUIC       66 Protected Payload (KP0), PKN: 16, ACK
     689 3.038276  192.168.100.2        192.168.100.1   DNS        79 Standard query 0x466b A script.crazyegg.com
     690 3.038389  192.168.100.2        192.168.100.1   DNS        79 Standard query 0x532a HTTPS script.crazyegg.com
     691 3.051622  192.168.100.1        192.168.100.2   DNS       163 Standard query response 0x466b A script.crazyegg.com CNAME script.crazyegg.com.cdn.cloudflare.net
     692 3.051622  192.168.100.1        192.168.100.2   DNS        79 Standard query response 0x532a HTTPS script.crazyegg.com
     693 3.052359  192.168.100.2        104.19.147.8    QUIC     1292 Initial, DCID=f4dd5e95cf213805, PKN: 1, CRYPTO
     694 3.052388  192.168.100.2        104.19.147.8    QUIC     1292 Initial, DCID=f4dd5e95cf213805, PKN: 2, PADDING, PING, CRYPTO, PING, PING, PING, PING, PING, PADDI
     695 3.061719  192.168.100.2        224.0.0.251     MDNS       82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
     696 3.061822  fe80::83aa:5971:d59… ff02::fb        MDNS      102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
     697 3.077471  192.168.100.2        192.168.100.1   DNS        77 Standard query 0x2278 A fonts.gstatic.com
     698 3.077588  192.168.100.2        192.168.100.1   DNS        77 Standard query 0x4104 HTTPS fonts.gstatic.com
```

Step 3: Select any UDP packet to view its details.



```
> Frame 480: 1288 bytes on wire (10304 bits), 1288 bytes captured (10304 bits) on interface \Device\NPF_{E265FD1B-426B-4FBE-AD6B-F27:
> Ethernet II, Src: HuaweiTechno_a9:67:c9 (2c:ab:00:a9:67:c9), Dst: GigaByteTech_a7:bb:4c (18:c0:4d:a7:bb:4c)
> Internet Protocol Version 4, Src: 142.250.200.206, Dst: 192.168.100.2
v User Datagram Protocol, Src Port: 443, Dst Port: 55921
     Source Port: 443
     Destination Port: 55921
     Length: 1254
     Checksum: 0x700a [unverified]
     [Checksum Status: Unverified]
     [Stream index: 24]
     [Stream Packet Number: 29]
   > [Timestamps]
     UDP payload (1246 bytes)
v QUIC IETF
   > QUIC Connection information
     [Packet Length: 1246]
   > QUIC Short Header PKN=15
   > STREAM id=0 fin=1 off=790 len=804 dir=Bidirectional origin=Client-initiated
   > STREAM id=11 fin=0 off=422 len=82 dir=Unidirectional origin=Server-initiated
   > STREAM id=8 fin=0 off=0 len=328 dir=Bidirectional origin=Client-initiated
v Hypertext Transfer Protocol Version 3
   > Request Stream
v Hypertext Transfer Protocol Version 3
   > Uni Stream
v Hypertext Transfer Protocol Version 3
```

Part 4: Comparing TCP and UDP

TCP vs. UDP

	TCP or UDP	Reason
Reliability and Connection Establishment	**TCP**	TCP provide a three-way handshake before data transfer Ensuring a stable connection.
Data Integrity and Ordering	**TCP**	TCP Delivers data in order and retransmits lost packets to ensure accuracy.

Use Cases & Performance

	TCP	UDP
Use cases	- Web browsing (HTTP) - File transfers (FTP) - Emails (SMTP)	- Live video streaming (Twitch) - Online gaming
Performance	- Reliable - Connection-oriented - Slower	- Faster - Connectionless - Less reliable