CS 342: Computer Networks Laboratory

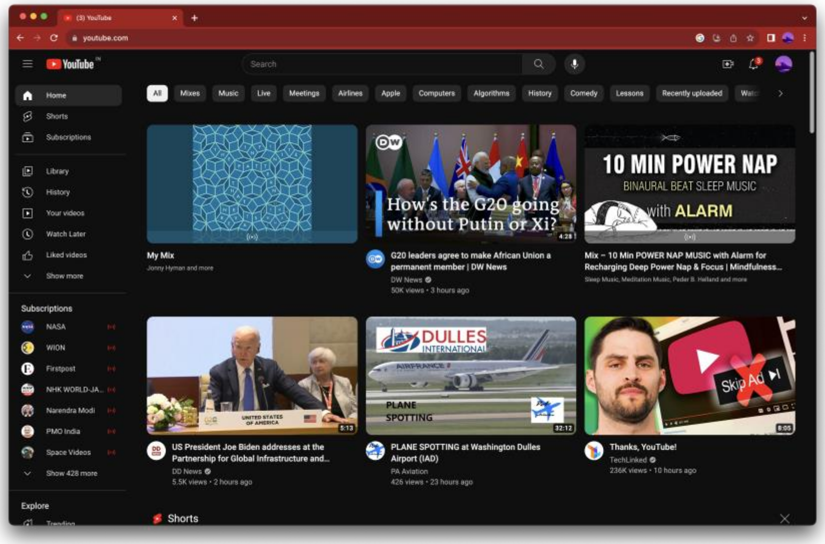
Packet Analysis Using Wireshark

M25

NAVEEN KUMAR A G	210123075
LAKSHYA KOHLI	210123077
ADVAITAA ARUN	210123078

Application: YouTube

The application under analysis is YouTube running on a Google chrome browser. Wireshark was used to capture incoming and outgoing packets.



# Question-1: The packets used the following protocols at different layers:

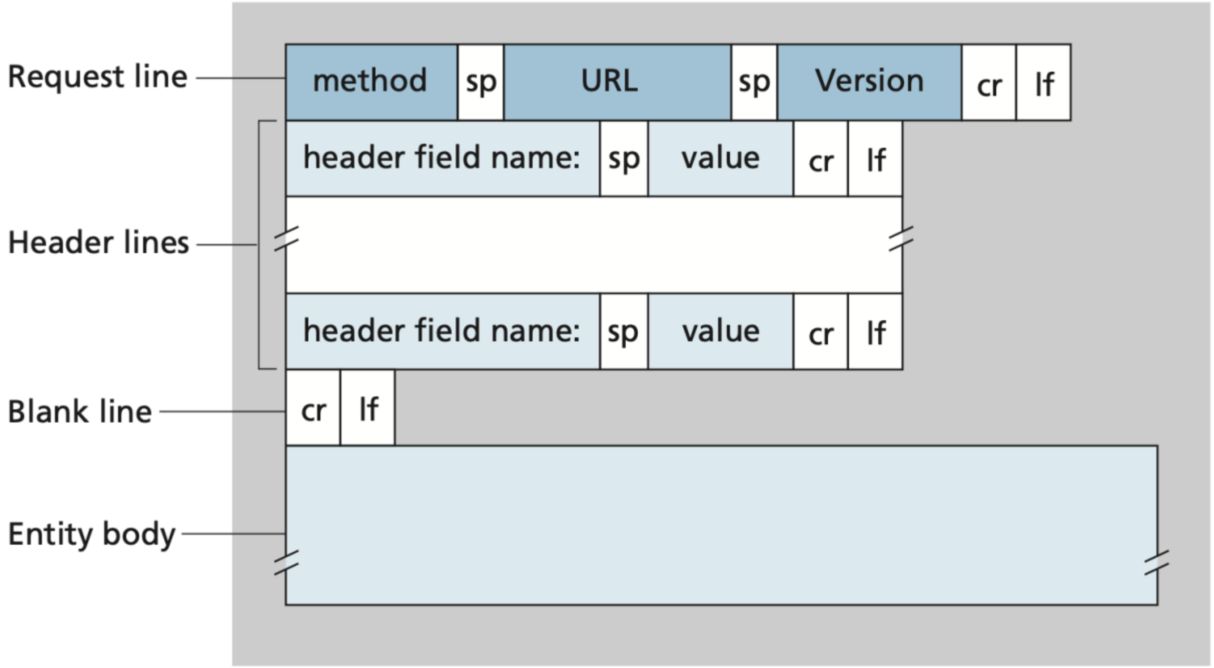
Application layer:	HTTPS (TLSv1.3), DNS,
Transport layer:	TCP, UDP (by DNS)
Network layer:	IPv4
Link layer:	Link Control Protocol
Physical layer:	Ethernet II

Note: Sites like YouTube use a secure version of HTTP called HTTPS which has data encryption using SSL/TLS. SSL is the original and now deprecated protocol created at Netscape in the mid 90s. TLS is the new protocol for secured encryption on the web maintained by IETF.

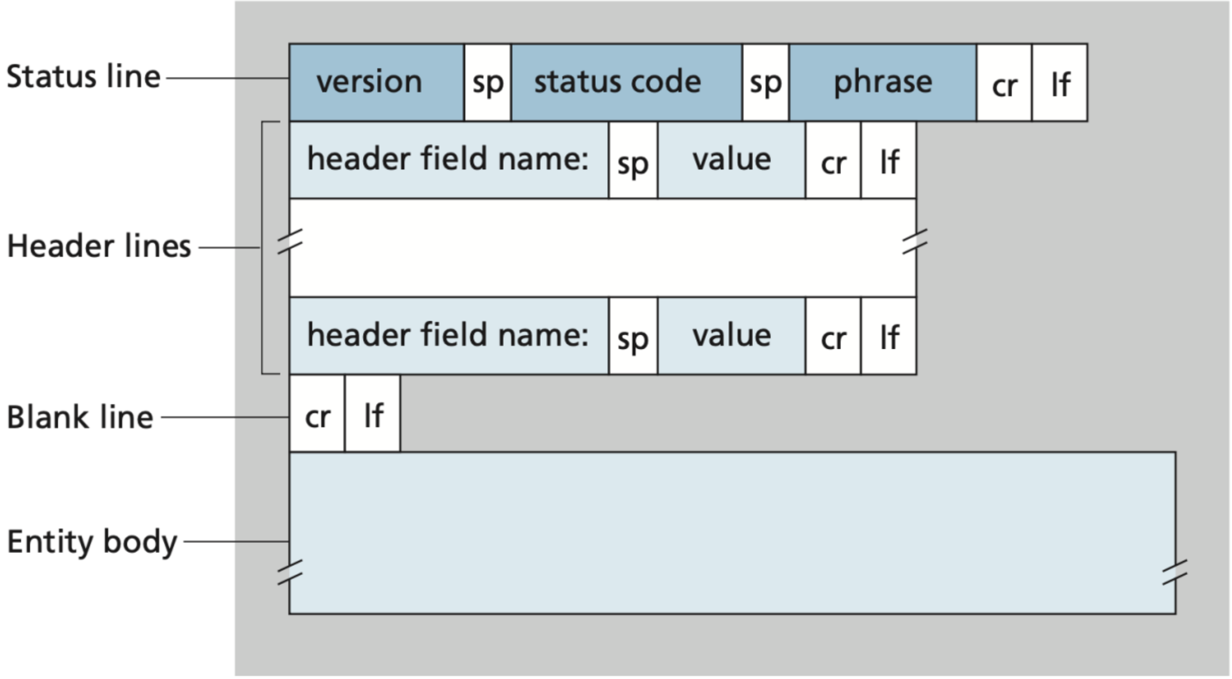
Packet formats:

HTTP(S):

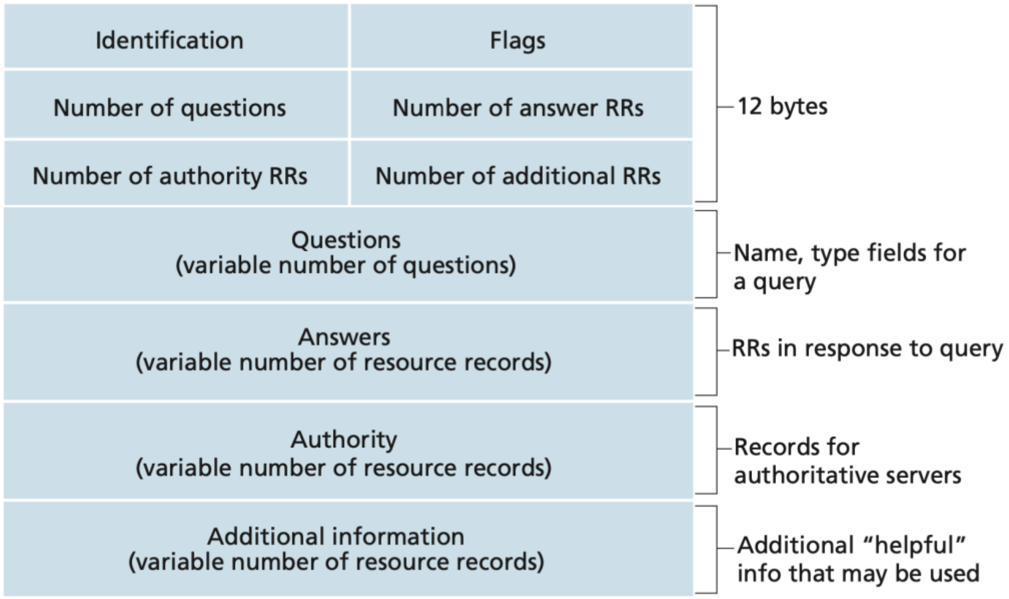
i) Request message:



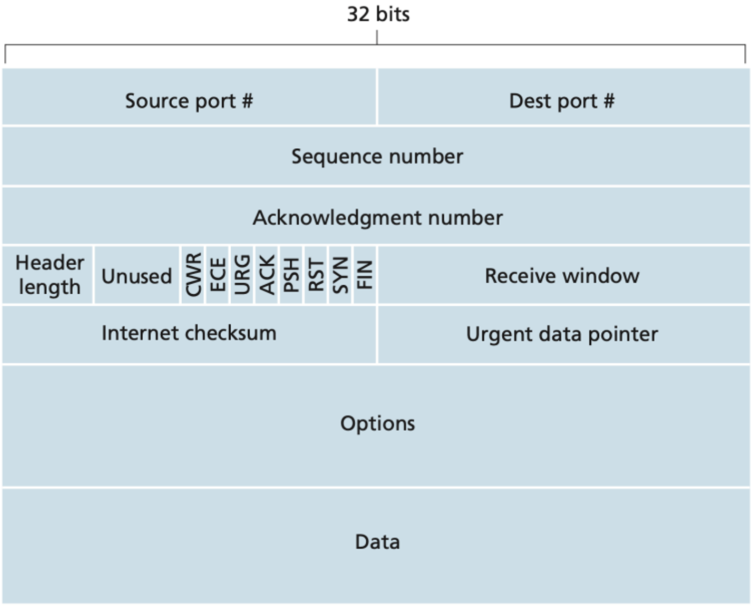
ii) Response message:



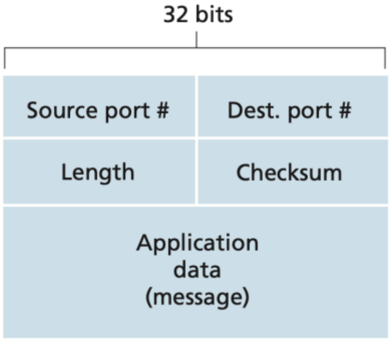
DNS:


Identification
Flags
Number of questions
Number of answer RRs
Number of authority RRs
Number of additional RRs
12 bytes
Questions
(variable number of questions)
Name, type fields for a query
Answers
(variable number of resource records)
RRs in response to query
Authority
(variable number of resource records)
Records for authoritative servers
Additional information
(variable number of resource records)
Additional "helpful" info that may be used

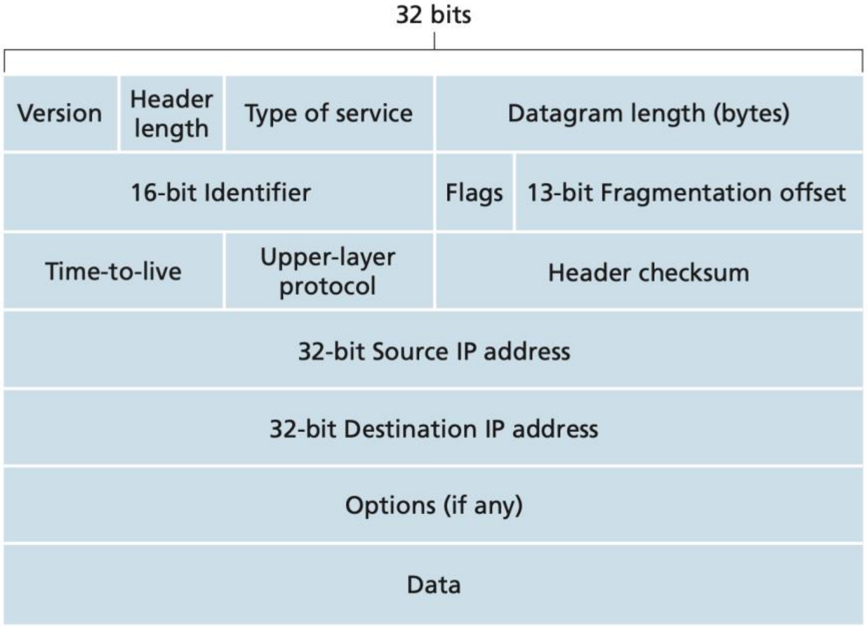
TCP:


32 bits
Source port #
Dest port #
Sequence number
Acknowledgment number
Header length
Unused
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Receive window
Internet checksum
Urgent data pointer
Options
Data

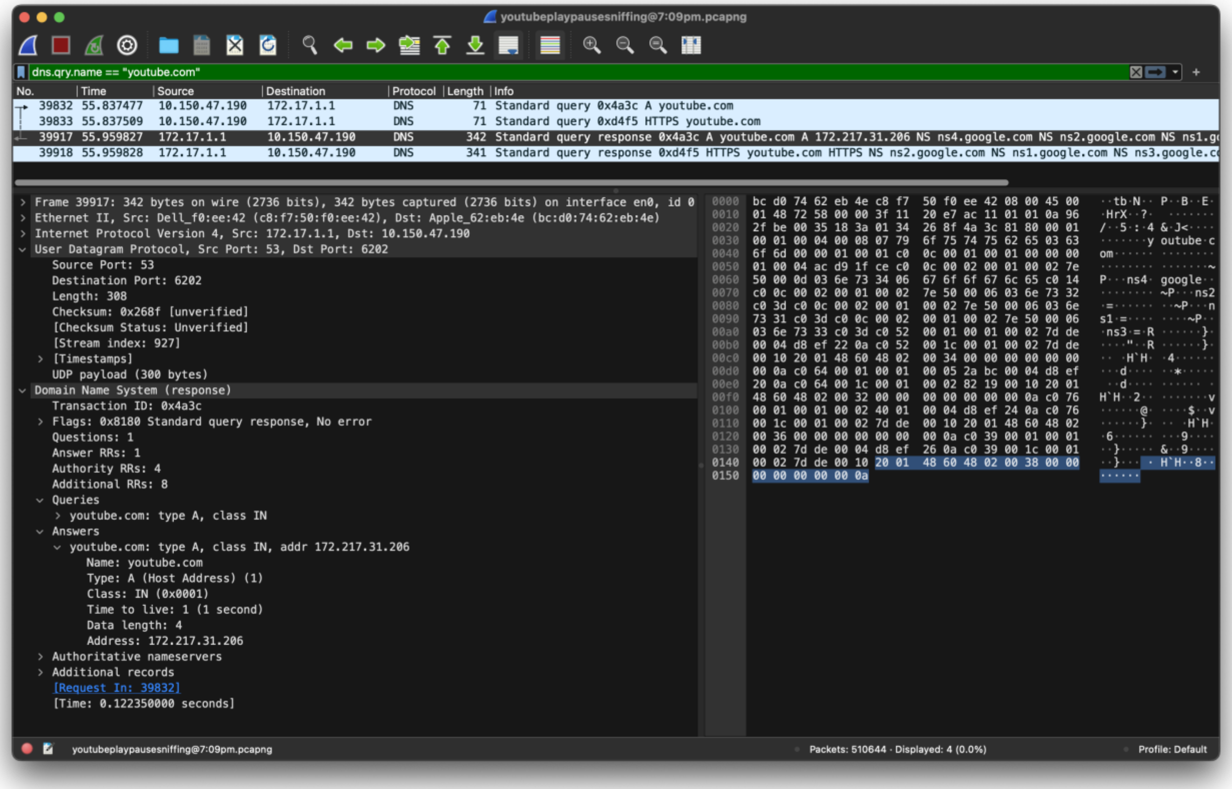
UDP:


32 bits
Source port #
Dest. port #
Length
Checksum
Application data (message)

IPv4:



# Question-2: Observed queries of protocols:



```
dns.qry.name == "youtube.com"

No.    Time       Source         Destination    Protocol Length Info
39832  55.837477  10.150.47.190  172.17.1.1     DNS      71     Standard query 0x4a3c A youtube.com
39833  55.837509  10.150.47.190  172.17.1.1     DNS      71     Standard query 0xd4f5 HTTPS youtube.com
39917  55.959827  172.17.1.1     10.150.47.190  DNS      342    Standard query response 0x4a3c A youtube.com A 172.217.31.206 NS ns4.google.com NS ns2.google.com NS ns1.g
39918  55.959828  172.17.1.1     10.150.47.190  DNS      341    Standard query response 0xd4f5 HTTPS youtube.com HTTPS NS ns2.google.com NS ns1.google.com NS ns3.google.c
```

```
> Frame 39917: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74:62:eb:4e)
> Internet Protocol Version 4, Src: 172.17.1.1, Dst: 10.150.47.190
v User Datagram Protocol, Src Port: 53, Dst Port: 6202
    Source Port: 53
    Destination Port: 6202
    Length: 308
    Checksum: 0x268f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 927]
  > [Timestamps]
    UDP payload (300 bytes)
v Domain Name System (response)
    Transaction ID: 0x4a3c
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  v Queries
    > youtube.com: type A, class IN
  v Answers
    v youtube.com: type A, class IN, addr 172.217.31.206
        Name: youtube.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1 (1 second)
        Data length: 4
        Address: 172.217.31.206
  > Authoritative nameservers
  > Additional records
    [Request In: 39832]
    [Time: 0.122350000 seconds]
```

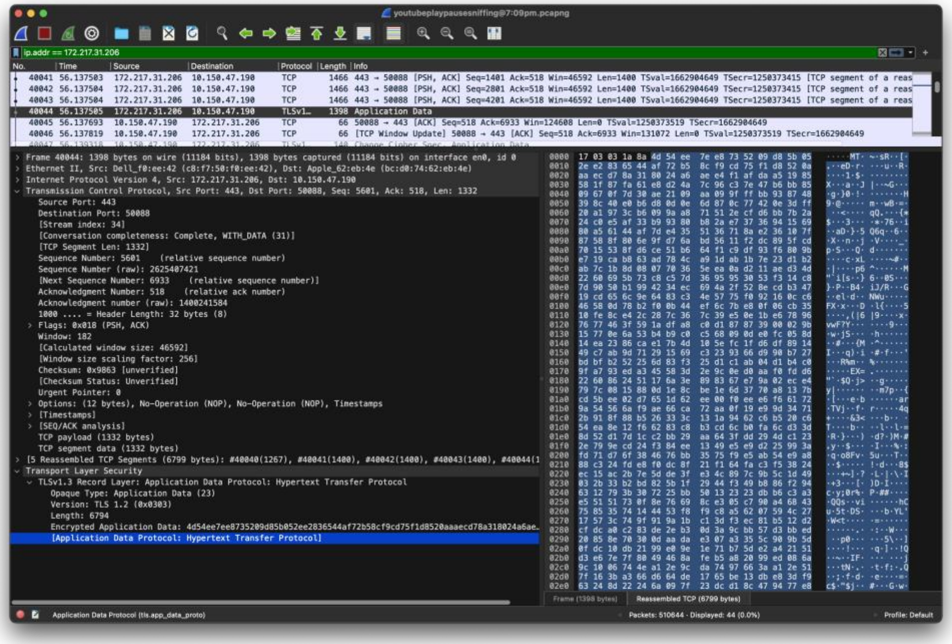
```
0000  bc d0 74 62 eb 4e c8 f7  50 f0 ee 42 08 00 45 00   ··tb·N··  P··B··E·
0010  01 48 72 58 00 00 3f 11  20 e7 ac 11 01 01 0a 96   ·HrX··?·   ·······
0020  2f be 00 35 18 3a 01 34  26 8f 4a 3c 81 80 00 01   /··5·:·4 &·J<····
0030  00 01 00 04 00 08 07 79  6f 75 74 75 62 65 03 63   ·······y outube·c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om······ ········
0050  01 00 04 ac d9 1f ce c0  0c 00 02 00 01 00 02 7e   ········ ·······~
0060  50 00 0d 03 6e 73 34 06  67 6f 6f 67 6c 65 c0 14   P···ns4· google··
0070  c0 0c 00 02 00 01 00 02  7e 50 00 06 03 6e 73 32   ········ ~P···ns2
0080  c0 3d c0 0c 00 02 00 01  00 02 7e 50 00 06 03 6e   ·=······ ··~P···n
0090  73 31 c0 3d c0 0c 00 02  00 01 00 02 7e 50 00 06   s1·=···· ····~P··
00a0  03 6e 73 33 c0 3d c0 52  00 01 00 01 00 02 7d de   ·ns3·=·R ······}·
00b0  00 04 d8 ef 22 0a c0 52  00 1c 00 01 00 02 7d de   ····"··R ······}·
00c0  00 10 20 01 48 60 48 02  00 34 00 00 00 00 00 00   ·· ·H`H· ·4······
00d0  00 0a c0 64 00 01 00 01  00 05 2a bc 00 04 d8 ef   ···d···· ··*·····
00e0  20 0a c0 64 00 1c 00 01  00 02 82 19 00 10 20 01    ··d···· ······ ·
00f0  48 60 48 02 00 32 00 00  00 00 00 00 00 0a c0 76   H`H··2·· ·······v
0100  00 01 00 01 00 02 40 01  00 04 d8 ef 24 0a c0 76   ······@· ····$··v
0110  00 1c 00 01 00 02 7d de  00 10 20 01 48 60 48 02   ······}· ·· ·H`H·
0120  00 36 00 00 00 00 00 00  00 0a c0 39 00 01 00 01   ·6······ ···9····
0130  00 02 7d de 00 04 d8 ef  26 0a c0 39 00 1c 00 01   ··}····· &··9····
0140  00 02 7d de 00 10 20 01  48 60 48 02 00 38 00 00   ··}··· · H`H··8··
0150  00 00 00 00 00 0a                                  ······
```

youtubeplaypausesniffing@7:09pm.pcapng   Packets: 510644 · Displayed: 4 (0.0%)   Profile: Default

Consider the following snapshot of the packet exchange between client and DNS server when the site "youtube.com" is searched on a new chrome browser window. From the brief description of the formats of the packets discussed earlier, the following can be deduced:

1) DNS:
   i) Identification: 0x4a3c (in hexadecimal) and Flags: 0x8180 (in hexadecimal): This means this message is a response to a query.
   ii) # Questions: 1, # Answer RRs (resource record): 1, # Authority RRs: 4, # Additional RRs: 8
   iii) Queries field has numerous queries set ascertained by the # Questions field.
   iv) Answers field has answers (i.e. domain name to IP resolution if type is A) to the corresponding queries.
   v) Authority field has records for authoritative servers while Additional information field has additional helpful information that may be used.
2) UDP:
   i) Source port: 53 and Destination port: 6202
   ii) Length: 308 bytes (header + application data) and Checksum: 0x268f (in hexadecimal)
   iii) Application data has message content from the upper layer which is 300 bytes long.
3) IPv4:
   i) Source: 172.17.1.1
   ii) Destination: 10.150.47.190
4) Ethernet II:
   i) Source: Dell_f0:ee:42 (c8:f7:50:f0:ee:42) and Destination: Apple_62:eb:4e (bc:d0:74:62:eb:4e)

Consider another snapshot which captures a random packet transferred from a server to the client while the YouTube video is being played.



ip.addr == 172.217.31.206

```
No.    Time       Source          Destination     Protocol Length Info
40041  56.137503  172.217.31.206  10.150.47.190   TCP      1466   443 → 50088 [PSH, ACK] Seq=1401 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reas
40042  56.137504  172.217.31.206  10.150.47.190   TCP      1466   443 → 50088 [PSH, ACK] Seq=2801 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reas
40043  56.137504  172.217.31.206  10.150.47.190   TCP      1466   443 → 50088 [PSH, ACK] Seq=4201 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reas
40044  56.137505  172.217.31.206  10.150.47.190   TLSv1…   1398   Application Data
40045  56.137693  10.150.47.190   172.217.31.206  TCP        66   50088 → 443 [ACK] Seq=518 Ack=6933 Win=124608 Len=0 TSval=1250373519 TSecr=1662904649
40046  56.137819  10.150.47.190   172.217.31.206  TCP        66   [TCP Window Update] 50088 → 443 [ACK] Seq=518 Ack=6933 Win=131072 Len=0 TSval=1250373519 TSecr=1662904649
40047  56.139318  10.150.47.190   172.217.31.206  TLSv1…    140   Change Cipher Spec, Application Data
```

```
> Frame 40044: 1398 bytes on wire (11184 bits), 1398 bytes captured (11184 bits) on interface en0, id 0
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74:62:eb:4e)
> Internet Protocol Version 4, Src: 172.217.31.206, Dst: 10.150.47.190
v Transmission Control Protocol, Src Port: 443, Dst Port: 50088, Seq: 5601, Ack: 518, Len: 1332
    Source Port: 443
    Destination Port: 50088
    [Stream index: 34]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1332]
    Sequence Number: 5601    (relative sequence number)
    Sequence Number (raw): 2625407421
    [Next Sequence Number: 6933    (relative sequence number)]
    Acknowledgment Number: 518    (relative ack number)
    Acknowledgment number (raw): 1400241584
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 182
    [Calculated window size: 46592]
    [Window size scaling factor: 256]
    Checksum: 0x9863 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (1332 bytes)
    TCP segment data (1332 bytes)
> [5 Reassembled TCP Segments (6799 bytes): #40040(1267), #40041(1400), #40042(1400), #40043(1400), #40044(1
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 6794
      Encrypted Application Data: 4d54ee7ee8735209d85b052ee2836544af72b58cf9cd75f1d8520aaaecd78a318024a6ae…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  17 03 03 1a 8a 4d 54 ee  7e e8 73 52 09 d8 5b 05   ·····MT· ~·sR··[·
0010  2e e2 83 65 44 af 72 b5  8c f9 cd 75 f1 d8 52 0a   .··eD·r· ···u··R·
0020  aa ec d7 8a 31 80 24 a6  ae e4 f1 af da a5 19 85   ····1·$· ········
0030  58 1f 87 fa 61 e8 d2 4a  7c 96 c3 7e 47 b6 bb 85   X···a··J |··~G···
0040  09 67 0f 7d 30 ae 21 09  aa 09 9f ff bb 93 87 48   ·g·}0·!· ·······H
0050  39 8c 40 e0 b6 d8 0d 0e  6d 87 0c 77 42 0e 3d ff   9·@····· m··wB·=·
0060  20 a1 97 3c b6 09 9a a8  71 51 2e cf d6 bb 7b 2a    ··<···· qQ.···{*
0070  24 c0 e5 af 33 b9 93 80  b8 2a e7 37 36 94 15 69   $···3··· ·*·76··i
0080  80 a5 61 44 af 7d e4 35  51 36 71 8a e2 36 10 7f   ··aD·}·5 Q6q··6··
0090  87 58 8f 80 6e 9f d7 6a  bd 56 11 f2 dc 89 5f cd   ·X··n··j ·V····_·
00a0  70 15 53 8f d6 ce 51 b6  64 f1 c9 df 93 f6 80 9b   p·S···Q· d·······
00b0  e7 19 ca b8 63 ad 78 4c  a9 1d ab 1b 7e 23 d1 b2   ····c·xL ····~#··
00c0  ab 7c 1b 8d 08 07 70 36  5e ea 0a d2 11 ae d3 4d   ·|····p6 ^······M
00d0  22 60 69 5b 73 c8 c5 7d  36 95 95 30 53 f3 14 c8   "`i[s··} 6··0S···
00e0  7d 90 50 b1 99 42 34 ec  69 4a 2f 52 8e cd b3 47   }·P··B4· iJ/R···G
00f0  19 cd 65 6c 9e 64 83 c3  4e 57 75 f0 92 16 0c c6   ··el·d·· NWu·····
0100  46 58 0d 78 b2 f0 0b 44  ef 6c 7b e8 0f 06 cb 35   FX·x···D ·l{····5
0110  10 fe 8c e4 2c 28 7c 36  7c 39 e5 0e 1b e6 78 96   ····,(|6 |9····x·
0120  76 77 46 3f 59 1a df a8  c0 d1 87 87 39 00 02 9b   vwF?Y··· ····9···
0130  15 77 0e 6a 53 b4 b9 c0  c5 68 09 0d e0 fc 05 8d   ·w·jS··· ·h······
0140  14 ea 23 86 ca e1 7b 4d  10 5e fc 1f d6 df 89 14   ··#···{M ·^······
0150  49 c7 ab 9d 71 29 15 69  c3 23 93 66 d9 90 b7 27   I···q)·i ·#·f···'
0160  bd bf b2 52 25 6d 83 f3  25 d1 c1 ab 04 d1 b4 c0   ···R%m·· %·······
0170  9f a7 93 ed a3 45 58 3d  2e 9c 0e d0 aa f0 fd d6   ·····EX= .·······
0180  22 60 86 24 51 17 6a 3e  89 83 67 e7 9a 02 ec e4   "`·$Q·j> ··g·····
0190  79 7c 08 15 88 0d 1e 8c  be 1e 6d 37 70 a8 13 7b   y|······ ··m7p··{
01a0  cd 5b ee 02 d7 65 1d 62  ee 00 f0 ee e6 f6 61 72   ·[···e·b ······ar
01b0  9a 54 56 6a f9 ae 66 ca  72 aa 0f 19 e9 9d 34 71   ·TVj··f· r·····4q
01c0  2b 91 8f 88 b5 26 33 3c  13 1a 94 62 c6 b5 20 c6   +····&3< ···b·· ·
01d0  54 ea 8e 12 f6 62 83 c8  b3 cd 6c b0 fa 6c d3 3d   T····b·· ··l··l·=
01e0  8d 52 d1 7d 1c c2 bb 29  aa 64 3f dd 29 4d c1 23   ·R·}···) ·d?·)M·#
01f0  2e 79 9e cd 24 f3 84 ee  13 49 e5 e9 d2 25 99 3a   .y··$··· ·I···%·:
0200  fd 71 d7 6f 38 46 76 bb  35 75 f9 e5 ab 54 e9 a8   ·q·o8Fv· 5u···T··
0210  88 c3 24 fd e8 f0 dc 8f  21 f1 64 fa c3 f5 38 24   ··$····· !·d···8$
0220  ec 15 ac 2b 7e 5d de 3f  e3 4c 89 7c 9b 5c 1d 49   ···+~]·? ·L·|·\·I
0230  03 2b 33 b2 bd 82 5b 1f  29 44 f3 49 b8 86 f2 94   ·+3···[· )D·I····
0240  63 12 79 3b 30 72 25 bb  50 13 23 23 db b6 c3 a3   c·y;0r%· P·##····
0250  e5 51 51 73 0f 8e 76 69  8c e3 05 c7 90 a4 68 43   ·QQs··vi ······hC
0260  75 85 35 74 14 44 53 f8  f9 c8 a5 62 07 59 4c 27   u·5t·DS· ···b·YL'
0270  17 57 3c 74 9f 91 9a 1b  c1 3d f3 ec 81 b5 12 d2   ·W<t···· ·=······
0280  cf dc a0 c2 83 de 2e b3  0d 3a 9c bb 57 d3 bb ed   ······.· ·:··W···
0290  20 85 8e 70 30 0d aa da  e3 07 a3 35 5c 90 9b 5d    ··p0··· ···5\··]
02a0  0f dc 10 db 21 99 e0 9e  1e 71 b7 5d e2 a4 21 51   ····!··· ·q·]··!Q
02b0  d3 e6 7e 7f 80 49 46 8a  fe b5 a8 20 99 ed 08 6a   ··~··IF· ··· ···j
02c0  9c 10 06 74 4e a1 2e 9c  da 74 97 66 3a a1 2e 51   ···tN·.· ·t·f:·.Q
02d0  7f 16 3b a3 66 d6 64 de  17 65 be 13 db e8 3d f9   ··;·f·d· ·e····=·
02e0  63 24 8d 22 24 6a 09 7f  23 dc d1 8c 47 94 77 e8   c$·"$j·· #···G·w·
```

Frame (1398 bytes)
Reassembled TCP (6799 bytes)
Application Data Protocol (tls.app_data_proto)
Packets: 510644 · Displayed: 44 (0.0%)
Profile: Default

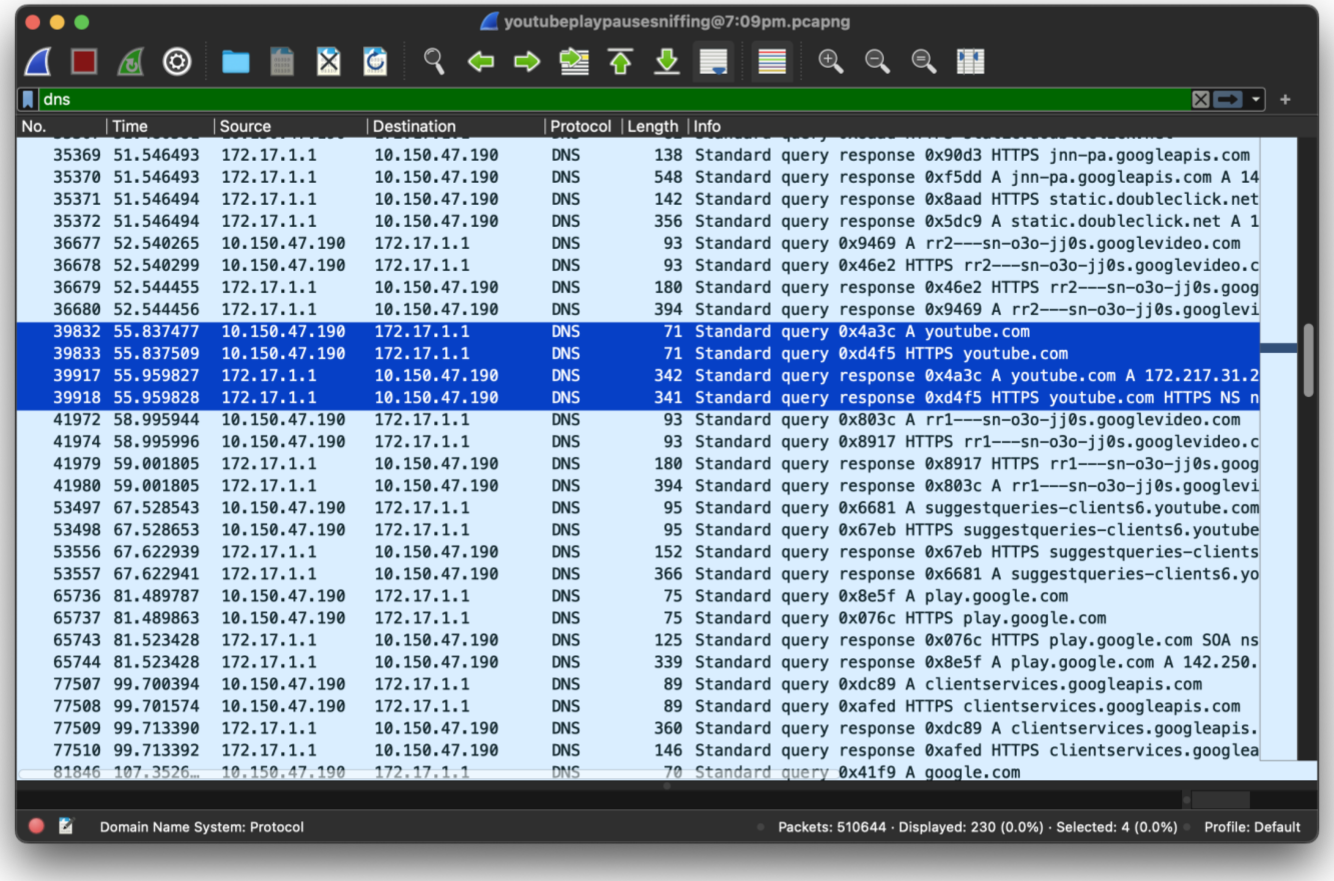
5) TCP:

    i) Source port: 443 and Destination port: 50088
    ii) Sequence number: 5601
    iii) Acknowledgment number: 518
    iv) Flags: 0x018 (convert to binary and divide between PSH and ACK)
    v) Receive window: 182 (used for flow control)
    vi) Internet checksum: 0x9863
    vii) Urgent data pointer: 0
    viii) Options: 12 bytes (used by receiver and sender to negotiate maximum segment size)
    ix) Data: 1332 bytes

6) TLSv1.3: (This is implemented on top of HTTP to make it more secure)

    i) Version: TLS 1.2
    ii) Length: 6794
    iii) Application data protocol: HTTP (Encrypted data on the right side of the screen.)

# Question-3: **DNS Name Resolution:**



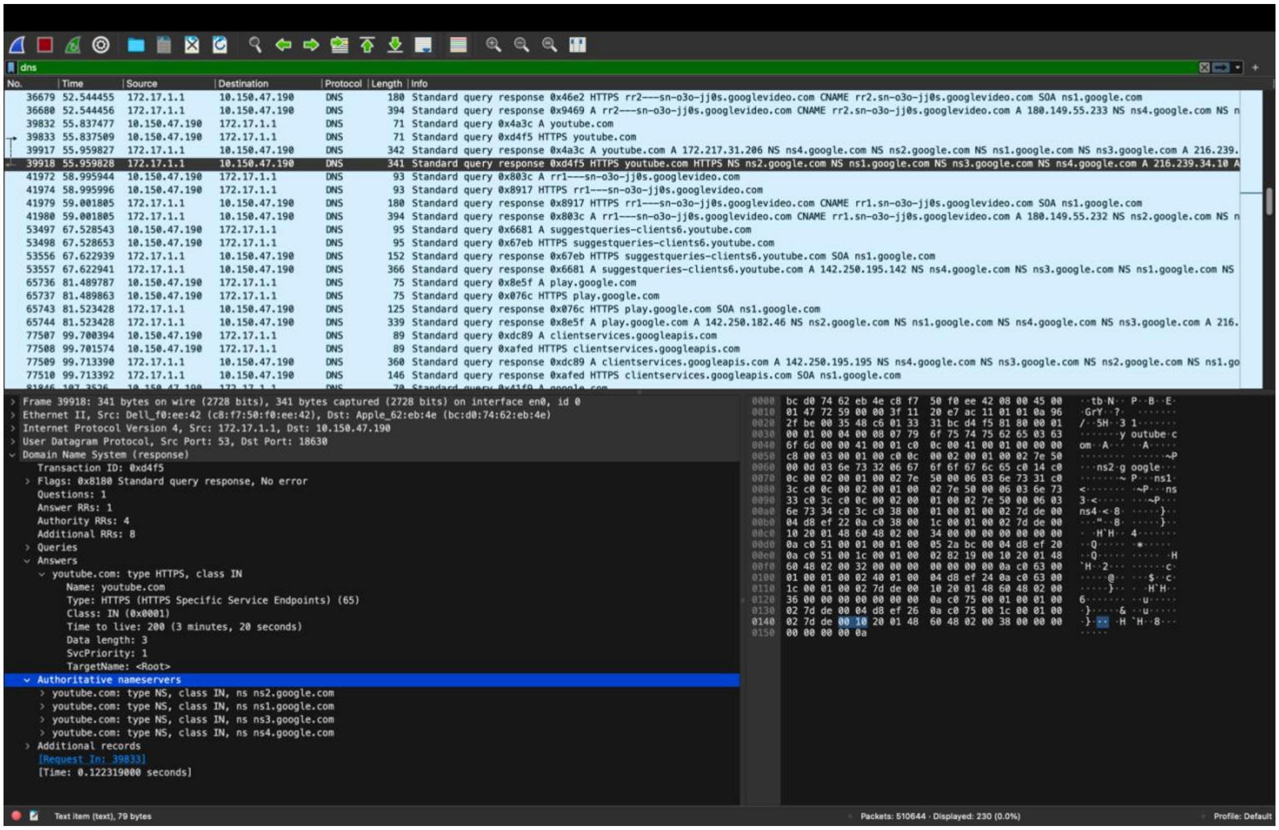
youtubeplaypausesniffing@7:09pm.pcapng

dns

```
No.    Time       Source         Destination    Protocol Length Info
 35369 51.546493  172.17.1.1     10.150.47.190  DNS       138 Standard query response 0x90d3 HTTPS jnn-pa.googleapis.com
 35370 51.546493  172.17.1.1     10.150.47.190  DNS       548 Standard query response 0xf5dd A jnn-pa.googleapis.com A 14
 35371 51.546494  172.17.1.1     10.150.47.190  DNS       142 Standard query response 0x8aad HTTPS static.doubleclick.net
 35372 51.546494  172.17.1.1     10.150.47.190  DNS       356 Standard query response 0x5dc9 A static.doubleclick.net A 1
 36677 52.540265  10.150.47.190  172.17.1.1     DNS        93 Standard query 0x9469 A rr2---sn-o3o-jj0s.googlevideo.com
 36678 52.540299  10.150.47.190  172.17.1.1     DNS        93 Standard query 0x46e2 HTTPS rr2---sn-o3o-jj0s.googlevideo.c
 36679 52.544455  172.17.1.1     10.150.47.190  DNS       180 Standard query response 0x46e2 HTTPS rr2---sn-o3o-jj0s.goog
 36680 52.544456  172.17.1.1     10.150.47.190  DNS       394 Standard query response 0x9469 A rr2---sn-o3o-jj0s.googlevi
 39832 55.837477  10.150.47.190  172.17.1.1     DNS        71 Standard query 0x4a3c A youtube.com
 39833 55.837509  10.150.47.190  172.17.1.1     DNS        71 Standard query 0xd4f5 HTTPS youtube.com
 39917 55.959827  172.17.1.1     10.150.47.190  DNS       342 Standard query response 0x4a3c A youtube.com A 172.217.31.2
 39918 55.959828  172.17.1.1     10.150.47.190  DNS       341 Standard query response 0xd4f5 HTTPS youtube.com HTTPS NS n
 41972 58.995944  10.150.47.190  172.17.1.1     DNS        93 Standard query 0x803c A rr1---sn-o3o-jj0s.googlevideo.com
 41974 58.995996  10.150.47.190  172.17.1.1     DNS        93 Standard query 0x8917 HTTPS rr1---sn-o3o-jj0s.googlevideo.c
 41979 59.001805  172.17.1.1     10.150.47.190  DNS       180 Standard query response 0x8917 HTTPS rr1---sn-o3o-jj0s.goog
 41980 59.001805  172.17.1.1     10.150.47.190  DNS       394 Standard query response 0x803c A rr1---sn-o3o-jj0s.googlevi
 53497 67.528543  10.150.47.190  172.17.1.1     DNS        95 Standard query 0x6681 A suggestqueries-clients6.youtube.com
 53498 67.528653  10.150.47.190  172.17.1.1     DNS        95 Standard query 0x67eb HTTPS suggestqueries-clients6.youtube
 53556 67.622939  172.17.1.1     10.150.47.190  DNS       152 Standard query response 0x67eb HTTPS suggestqueries-clients
 53557 67.622941  172.17.1.1     10.150.47.190  DNS       366 Standard query response 0x6681 A suggestqueries-clients6.yo
 65736 81.489787  10.150.47.190  172.17.1.1     DNS        75 Standard query 0x8e5f A play.google.com
 65737 81.489863  10.150.47.190  172.17.1.1     DNS        75 Standard query 0x076c HTTPS play.google.com
 65743 81.523428  172.17.1.1     10.150.47.190  DNS       125 Standard query response 0x076c HTTPS play.google.com SOA ns
 65744 81.523428  172.17.1.1     10.150.47.190  DNS       339 Standard query response 0x8e5f A play.google.com A 142.250.
 77507 99.700394  10.150.47.190  172.17.1.1     DNS        89 Standard query 0xdc89 A clientservices.googleapis.com
 77508 99.701574  10.150.47.190  172.17.1.1     DNS        89 Standard query 0xafed HTTPS clientservices.googleapis.com
 77509 99.713390  172.17.1.1     10.150.47.190  DNS       360 Standard query response 0xdc89 A clientservices.googleapis.
 77510 99.713392  172.17.1.1     10.150.47.190  DNS       146 Standard query response 0xafed HTTPS clientservices.googlea
 81846 107.3526…  10.150.47.190  172.17.1.1     DNS        70 Standard query 0x41f9 A google.com
```

Domain Name System: Protocol · Packets: 510644 · Displayed: 230 (0.0%) · Selected: 4 (0.0%) · Profile: Default

The highlighted packets represent the DNS queries and their corresponding replies for name resolution. The queries above are of type A (host name to IP Conversion) and NS (domain name to hostname of authoritative name server for this domain).



```
No.    Time       Source         Destination    Protocol Length Info
36679  52.544455  172.17.1.1     10.150.47.190  DNS      180 Standard query response 0x46e2 HTTPS rr2---sn-o3o-jj0s.googlevideo.com CNAME rr2.sn-o3o-jj0s.googlevideo.com SOA ns1.google.com
36680  52.544456  172.17.1.1     10.150.47.190  DNS      394 Standard query response 0x9469 A rr2---sn-o3o-jj0s.googlevideo.com CNAME rr2.sn-o3o-jj0s.googlevideo.com A 180.149.55.233 NS ns4.google.com NS n
39832  55.837477  10.150.47.190  172.17.1.1     DNS       71 Standard query 0x4a3c A youtube.com
39833  55.837509  10.150.47.190  172.17.1.1     DNS       71 Standard query 0xd4f5 HTTPS youtube.com
39917  55.959827  172.17.1.1     10.150.47.190  DNS      342 Standard query response 0x4a3c A youtube.com A 172.217.31.206 NS ns4.google.com NS ns2.google.com NS ns1.google.com NS ns3.google.com A 216.239.
39918  55.959828  172.17.1.1     10.150.47.190  DNS      341 Standard query response 0xd4f5 HTTPS youtube.com HTTPS NS ns2.google.com NS ns1.google.com NS ns3.google.com NS ns4.google.com A 216.239.34.10 A
41972  58.995944  10.150.47.190  172.17.1.1     DNS       93 Standard query 0x803c A rr1---sn-o3o-jj0s.googlevideo.com
41974  58.995996  10.150.47.190  172.17.1.1     DNS       93 Standard query 0x8917 HTTPS rr1---sn-o3o-jj0s.googlevideo.com
41979  59.001805  172.17.1.1     10.150.47.190  DNS      180 Standard query response 0x8917 HTTPS rr1---sn-o3o-jj0s.googlevideo.com CNAME rr1.sn-o3o-jj0s.googlevideo.com SOA ns1.google.com
41980  59.001805  172.17.1.1     10.150.47.190  DNS      394 Standard query response 0x803c A rr1---sn-o3o-jj0s.googlevideo.com CNAME rr1.sn-o3o-jj0s.googlevideo.com A 180.149.55.232 NS ns2.google.com NS n
53497  67.528543  10.150.47.190  172.17.1.1     DNS       95 Standard query 0x6681 A suggestqueries-clients6.youtube.com
53498  67.528653  10.150.47.190  172.17.1.1     DNS       95 Standard query 0x67eb HTTPS suggestqueries-clients6.youtube.com
53556  67.622939  172.17.1.1     10.150.47.190  DNS      152 Standard query response 0x67eb HTTPS suggestqueries-clients6.youtube.com SOA ns1.google.com
53557  67.622941  172.17.1.1     10.150.47.190  DNS      366 Standard query response 0x6681 A suggestqueries-clients6.youtube.com A 142.250.195.142 NS ns4.google.com NS ns3.google.com NS ns1.google.com NS
65736  81.489787  10.150.47.190  172.17.1.1     DNS       75 Standard query 0x8e5f A play.google.com
65737  81.489863  10.150.47.190  172.17.1.1     DNS       75 Standard query 0x076c HTTPS play.google.com
65743  81.523428  172.17.1.1     10.150.47.190  DNS      125 Standard query response 0x076c HTTPS play.google.com SOA ns1.google.com
65744  81.523428  172.17.1.1     10.150.47.190  DNS      339 Standard query response 0x8e5f A play.google.com A 142.250.182.46 NS ns2.google.com NS ns1.google.com NS ns4.google.com NS ns3.google.com A 216.
77507  99.700394  10.150.47.190  172.17.1.1     DNS       89 Standard query 0xdc89 A clientservices.googleapis.com
77508  99.701574  10.150.47.190  172.17.1.1     DNS       89 Standard query 0xafed HTTPS clientservices.googleapis.com
77509  99.713390  172.17.1.1     10.150.47.190  DNS      360 Standard query response 0xdc89 A clientservices.googleapis.com A 142.250.195.195 NS ns4.google.com NS ns3.google.com NS ns2.google.com NS ns1.go
77510  99.713392  172.17.1.1     10.150.47.190  DNS      146 Standard query response 0xafed HTTPS clientservices.googleapis.com SOA ns1.google.com
```

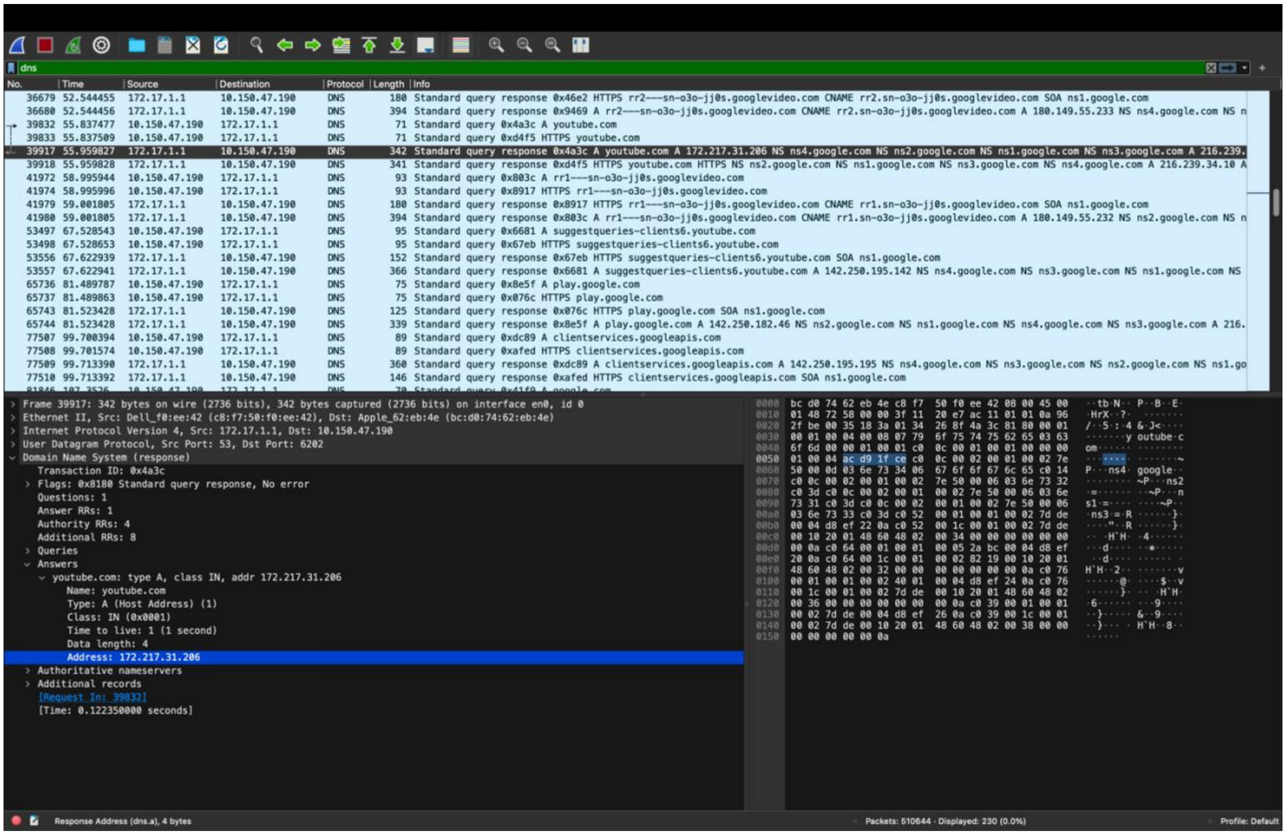
```
> Frame 39918: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface en0, id 0
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74:62:eb:4e)
> Internet Protocol Version 4, Src: 172.17.1.1, Dst: 10.150.47.190
> User Datagram Protocol, Src Port: 53, Dst Port: 18630
v Domain Name System (response)
    Transaction ID: 0xd4f5
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  > Queries
  v Answers
    v youtube.com: type HTTPS, class IN
        Name: youtube.com
        Type: HTTPS (HTTPS Specific Service Endpoints) (65)
        Class: IN (0x0001)
        Time to live: 200 (3 minutes, 20 seconds)
        Data length: 3
        SvcPriority: 1
        TargetName: <Root>
  v Authoritative nameservers
    > youtube.com: type NS, class IN, ns ns2.google.com
    > youtube.com: type NS, class IN, ns ns1.google.com
    > youtube.com: type NS, class IN, ns ns3.google.com
    > youtube.com: type NS, class IN, ns ns4.google.com
  > Additional records
    [Request In: 39833]
    [Time: 0.122319000 seconds]
```

```
0000  bc d0 74 62 eb 4e c8 f7  50 f0 ee 42 08 00 45 00   ··tb·N·· P··B··E·
0010  01 47 72 59 00 00 3f 11  20 e7 ac 11 01 01 0a 96   ·GrY··?·  ·······
0020  2f be 00 35 48 c6 01 33  31 bc d4 f5 81 80 00 01   /··5H··3 1·······
0030  00 01 00 04 00 08 07 79  6f 75 74 75 62 65 03 63   ·······y outube·c
0040  6f 6d 00 00 41 00 01 c0  0c 00 41 00 01 00 00 00   om··A··· ··A·····
0050  c8 00 03 00 01 00 c0 0c  00 02 00 01 00 02 7e 50   ········ ······~P
0060  00 0d 03 6e 73 32 06 67  6f 6f 67 6c 65 c0 14 c0   ···ns2·g oogle···
0070  0c 00 02 00 01 00 02 7e  50 00 06 03 6e 73 31 c0   ·······~ P···ns1·
0080  3c c0 0c 00 02 00 01 00  02 7e 50 00 06 03 6e 73   <······· ·~P···ns
0090  33 c0 3c c0 0c 00 02 00  01 00 02 7e 50 00 06 03   3·<····· ···~P···
00a0  6e 73 34 c0 3c c0 38 00  01 00 01 00 02 7d de 00   ns4·<·8· ·····}··
00b0  04 d8 ef 22 0a c0 38 00  1c 00 01 00 02 7d de 00   ···"··8· ·····}··
00c0  10 20 01 48 60 48 02 00  34 00 00 00 00 00 00 00   · ·H`H·· 4·······
00d0  0a c0 51 00 01 00 01 00  05 2a bc 00 04 d8 ef 20   ··Q····· ·*·····
00e0  0a c0 51 00 1c 00 01 00  02 82 19 00 10 20 01 48   ··Q····· ······ ·H
00f0  60 48 02 00 32 00 00 00  00 00 00 00 0a c0 63 00   `H··2··· ······c·
0100  01 00 01 00 02 40 01 00  04 d8 ef 24 0a c0 63 00   ·····@·· ···$··c·
0110  1c 00 01 00 02 7d de 00  10 20 01 48 60 48 02 00   ·····}·· · ·H`H··
0120  36 00 00 00 00 00 00 00  0a c0 75 00 01 00 01 00   6······· ··u·····
0130  02 7d de 00 04 d8 ef 26  0a c0 75 00 1c 00 01 00   ·}·····& ··u·····
0140  02 7d de 00 10 20 01 48  60 48 02 00 38 00 00 00   ·}··· ·H `H··8···
0150  00 00 00 00 0a                                      ·····
```

Text item (text), 79 bytes

Packets: 510644 · Displayed: 230 (0.0%)

Profile: Default



```
No.    Time       Source         Destination    Protocol Length Info
36679  52.544455  172.17.1.1     10.150.47.190  DNS      180 Standard query response 0x46e2 HTTPS rr2---sn-o3o-jj0s.googlevideo.com CNAME rr2.sn-o3o-jj0s.googlevideo.com SOA ns1.google.com
36680  52.544456  172.17.1.1     10.150.47.190  DNS      394 Standard query response 0x9469 A rr2---sn-o3o-jj0s.googlevideo.com CNAME rr2.sn-o3o-jj0s.googlevideo.com A 180.149.55.233 NS ns4.google.com NS n
39832  55.837477  10.150.47.190  172.17.1.1     DNS       71 Standard query 0x4a3c A youtube.com
39833  55.837509  10.150.47.190  172.17.1.1     DNS       71 Standard query 0xd4f5 HTTPS youtube.com
39917  55.959827  172.17.1.1     10.150.47.190  DNS      342 Standard query response 0x4a3c A youtube.com A 172.217.31.206 NS ns4.google.com NS ns2.google.com NS ns1.google.com NS ns3.google.com A 216.239.
39918  55.959828  172.17.1.1     10.150.47.190  DNS      341 Standard query response 0xd4f5 HTTPS youtube.com HTTPS NS ns2.google.com NS ns1.google.com NS ns3.google.com NS ns4.google.com A 216.239.34.10 A
41972  58.995944  10.150.47.190  172.17.1.1     DNS       93 Standard query 0x803c A rr1---sn-o3o-jj0s.googlevideo.com
41974  58.995996  10.150.47.190  172.17.1.1     DNS       93 Standard query 0x8917 HTTPS rr1---sn-o3o-jj0s.googlevideo.com
41979  59.001805  172.17.1.1     10.150.47.190  DNS      180 Standard query response 0x8917 HTTPS rr1---sn-o3o-jj0s.googlevideo.com CNAME rr1.sn-o3o-jj0s.googlevideo.com SOA ns1.google.com
41980  59.001805  172.17.1.1     10.150.47.190  DNS      394 Standard query response 0x803c A rr1---sn-o3o-jj0s.googlevideo.com CNAME rr1.sn-o3o-jj0s.googlevideo.com A 180.149.55.232 NS ns2.google.com NS n
53497  67.528543  10.150.47.190  172.17.1.1     DNS       95 Standard query 0x6681 A suggestqueries-clients6.youtube.com
53498  67.528653  10.150.47.190  172.17.1.1     DNS       95 Standard query 0x67eb HTTPS suggestqueries-clients6.youtube.com
53556  67.622939  172.17.1.1     10.150.47.190  DNS      152 Standard query response 0x67eb HTTPS suggestqueries-clients6.youtube.com SOA ns1.google.com
53557  67.622941  172.17.1.1     10.150.47.190  DNS      366 Standard query response 0x6681 A suggestqueries-clients6.youtube.com A 142.250.195.142 NS ns4.google.com NS ns3.google.com NS ns1.google.com NS
65736  81.489787  10.150.47.190  172.17.1.1     DNS       75 Standard query 0x8e5f A play.google.com
65737  81.489863  10.150.47.190  172.17.1.1     DNS       75 Standard query 0x076c HTTPS play.google.com
65743  81.523428  172.17.1.1     10.150.47.190  DNS      125 Standard query response 0x076c HTTPS play.google.com SOA ns1.google.com
65744  81.523428  172.17.1.1     10.150.47.190  DNS      339 Standard query response 0x8e5f A play.google.com A 142.250.182.46 NS ns2.google.com NS ns1.google.com NS ns4.google.com NS ns3.google.com A 216.
77507  99.700394  10.150.47.190  172.17.1.1     DNS       89 Standard query 0xdc89 A clientservices.googleapis.com
77508  99.701574  10.150.47.190  172.17.1.1     DNS       89 Standard query 0xafed HTTPS clientservices.googleapis.com
77509  99.713390  172.17.1.1     10.150.47.190  DNS      360 Standard query response 0xdc89 A clientservices.googleapis.com A 142.250.195.195 NS ns4.google.com NS ns3.google.com NS ns2.google.com NS ns1.go
77510  99.713392  172.17.1.1     10.150.47.190  DNS      146 Standard query response 0xafed HTTPS clientservices.googleapis.com SOA ns1.google.com
```

```
> Frame 39917: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface en0, id 0
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74:62:eb:4e)
> Internet Protocol Version 4, Src: 172.17.1.1, Dst: 10.150.47.190
> User Datagram Protocol, Src Port: 53, Dst Port: 6202
v Domain Name System (response)
    Transaction ID: 0x4a3c
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  > Queries
  v Answers
    v youtube.com: type A, class IN, addr 172.217.31.206
        Name: youtube.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1 (1 second)
        Data length: 4
        Address: 172.217.31.206
  > Authoritative nameservers
  > Additional records
    [Request In: 39832]
    [Time: 0.122350000 seconds]
```

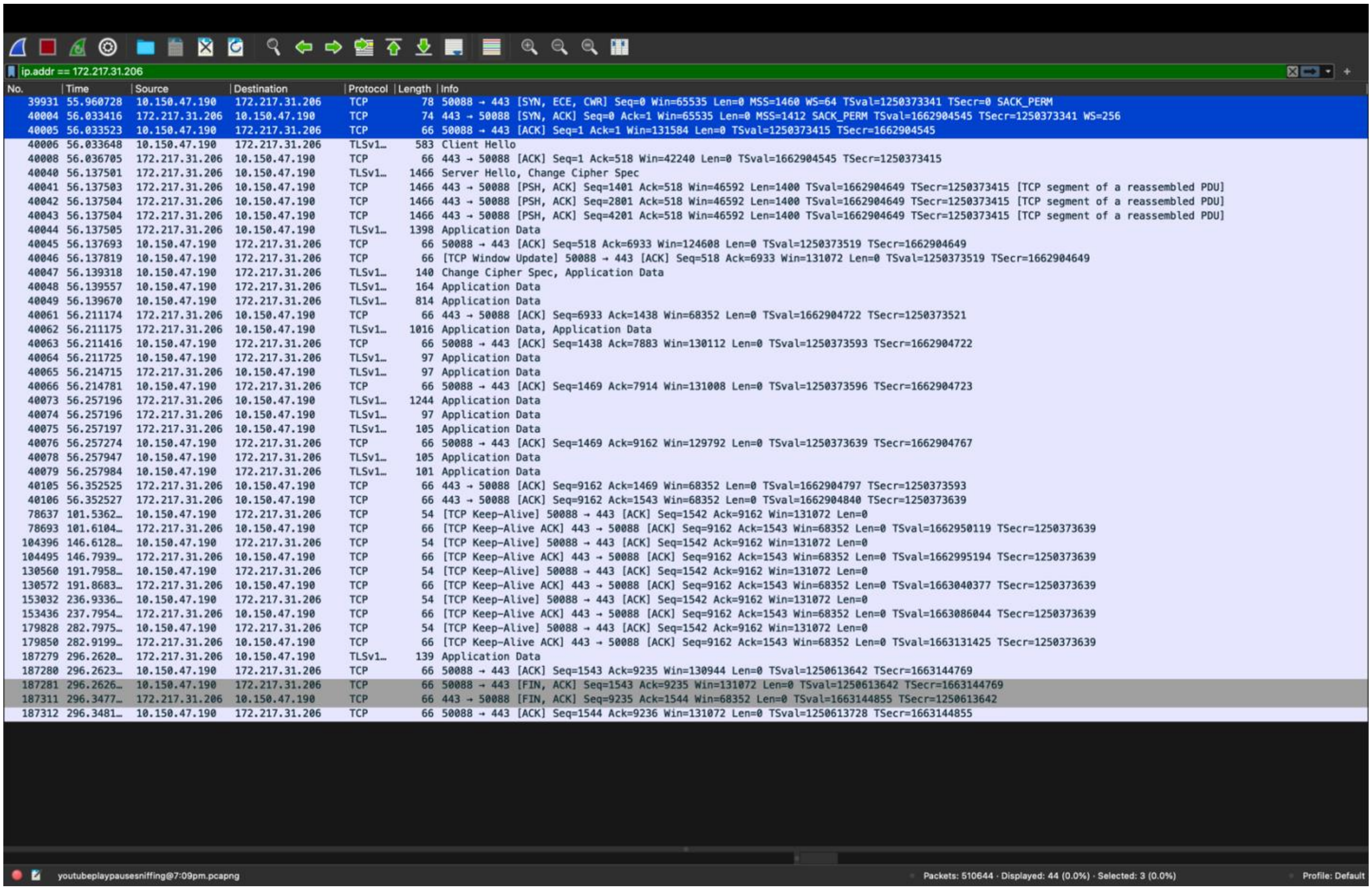
```
0000  bc d0 74 62 eb 4e c8 f7  50 f0 ee 42 08 00 45 00   ··tb·N·· P··B··E·
0010  01 48 72 58 00 00 3f 11  20 e7 ac 11 01 01 0a 96   ·HrX··?· ········
0020  2f be 00 35 18 3a 01 34  26 8f 4a 3c 81 80 00 01   /··5·:·4 &·J<····
0030  00 01 00 04 00 08 07 79  6f 75 74 75 62 65 03 63   ·······y outube·c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om······ ········
0050  01 00 04 ac d9 1f ce c0  0c 00 02 00 01 00 02 7e   ········ ·······~
0060  50 00 0d 03 6e 73 34 06  67 6f 6f 67 6c 65 c0 14   P···ns4· google··
0070  c0 0c 00 02 00 01 00 02  7e 50 00 06 03 6e 73 32   ········ ~P···ns2
0080  c0 3d c0 0c 00 02 00 01  00 02 7e 50 00 06 03 6e   ·=······ ··~P···n
0090  73 31 c0 3d c0 0c 00 02  00 01 00 02 7e 50 00 06   s1·=···· ····~P··
00a0  03 6e 73 33 c0 3d c0 52  00 01 00 01 00 02 7d de   ·ns3·=·R ······}·
00b0  00 04 d8 ef 22 0a c0 52  00 1c 00 01 00 02 7d de   ····"··R ······}·
00c0  00 10 20 01 48 60 48 02  00 34 00 00 00 00 00 00   ·· ·H`H· ·4······
00d0  00 0a c0 64 00 01 00 01  00 05 2a bc 00 04 d8 ef   ···d···· ··*·····
00e0  20 0a c0 64 00 1c 00 01  00 02 82 19 00 10 20 01    ··d···· ······ ·
00f0  48 60 48 02 00 32 00 00  00 00 00 00 00 0a c0 76   H`H··2·· ·······v
0100  00 01 00 01 00 02 40 01  00 04 d8 ef 24 0a c0 76   ······@· ····$··v
0110  00 1c 00 01 00 02 7d de  00 10 20 01 48 60 48 02   ······}· ·· ·H`H·
0120  00 36 00 00 00 00 00 00  00 0a c0 39 00 01 00 01   ·6······ ···9····
0130  00 02 7d de 00 04 d8 ef  26 0a c0 39 00 1c 00 01   ··}····· &··9····
0140  00 02 7d de 00 10 20 01  48 60 48 02 00 38 00 00   ··}··· · H`H··8··
0150  00 00 00 00 00 0a                                   ······
```

Response Address (dns.a), 4 bytes

Packets: 510644 · Displayed: 230 (0.0%)

Profile: Default

Handshaking protocol:



```
ip.addr == 172.217.31.206
No.     Time        Source          Destination     Protocol Length Info
  39931 55.960728   10.150.47.190   172.217.31.206  TCP        78 50088 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1250373341 TSecr=0 SACK_PERM
  40004 56.033416   172.217.31.206  10.150.47.190   TCP        74 443 → 50088 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1662904545 TSecr=1250373341 WS=256
  40005 56.033523   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1250373415 TSecr=1662904545
  40006 56.033648   10.150.47.190   172.217.31.206  TLSv1…    583 Client Hello
  40008 56.036705   172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=1 Ack=518 Win=42240 Len=0 TSval=1662904545 TSecr=1250373415
  40040 56.137501   172.217.31.206  10.150.47.190   TLSv1…   1466 Server Hello, Change Cipher Spec
  40041 56.137503   172.217.31.206  10.150.47.190   TCP      1466 443 → 50088 [PSH, ACK] Seq=1401 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reassembled PDU]
  40042 56.137504   172.217.31.206  10.150.47.190   TCP      1466 443 → 50088 [PSH, ACK] Seq=2801 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reassembled PDU]
  40043 56.137504   172.217.31.206  10.150.47.190   TCP      1466 443 → 50088 [PSH, ACK] Seq=4201 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reassembled PDU]
  40044 56.137505   172.217.31.206  10.150.47.190   TLSv1…   1398 Application Data
  40045 56.137693   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=518 Ack=6933 Win=124608 Len=0 TSval=1250373519 TSecr=1662904649
  40046 56.137819   10.150.47.190   172.217.31.206  TCP        66 [TCP Window Update] 50088 → 443 [ACK] Seq=518 Ack=6933 Win=131072 Len=0 TSval=1250373519 TSecr=1662904649
  40047 56.139318   10.150.47.190   172.217.31.206  TLSv1…    140 Change Cipher Spec, Application Data
  40048 56.139557   10.150.47.190   172.217.31.206  TLSv1…    164 Application Data
  40049 56.139670   10.150.47.190   172.217.31.206  TLSv1…    814 Application Data
  40061 56.211174   172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=6933 Ack=1438 Win=68352 Len=0 TSval=1662904722 TSecr=1250373521
  40062 56.211175   172.217.31.206  10.150.47.190   TLSv1…   1016 Application Data, Application Data
  40063 56.211416   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1438 Ack=7883 Win=130112 Len=0 TSval=1250373593 TSecr=1662904722
  40064 56.211725   10.150.47.190   172.217.31.206  TLSv1…     97 Application Data
  40065 56.214715   172.217.31.206  10.150.47.190   TLSv1…     97 Application Data
  40066 56.214781   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1469 Ack=7914 Win=131008 Len=0 TSval=1250373596 TSecr=1662904723
  40073 56.257196   172.217.31.206  10.150.47.190   TLSv1…   1244 Application Data
  40074 56.257196   172.217.31.206  10.150.47.190   TLSv1…     97 Application Data
  40075 56.257197   172.217.31.206  10.150.47.190   TLSv1…    105 Application Data
  40076 56.257274   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1469 Ack=9162 Win=129792 Len=0 TSval=1250373639 TSecr=1662904767
  40078 56.257947   10.150.47.190   172.217.31.206  TLSv1…    105 Application Data
  40079 56.257984   10.150.47.190   172.217.31.206  TLSv1…    101 Application Data
  40105 56.352525   172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=9162 Ack=1469 Win=68352 Len=0 TSval=1662904797 TSecr=1250373593
  40106 56.352527   172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1662904840 TSecr=1250373639
  78637 101.5362…   10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
  78693 101.6104…   172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1662950119 TSecr=1250373639
 104396 146.6128…   10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
 104495 146.7939…   172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1662995194 TSecr=1250373639
 130560 191.7958…   10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
 130572 191.8683…   172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1663040377 TSecr=1250373639
 153032 236.9336…   10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
 153436 237.7954…   172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1663086044 TSecr=1250373639
 179828 282.7975…   10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
 179850 282.9199…   172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1663131425 TSecr=1250373639
 187279 296.2620…   172.217.31.206  10.150.47.190   TLSv1…    139 Application Data
 187280 296.2623…   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1543 Ack=9235 Win=130944 Len=0 TSval=1250613642 TSecr=1663144769
 187281 296.2626…   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [FIN, ACK] Seq=1543 Ack=9235 Win=131072 Len=0 TSval=1250613642 TSecr=1663144769
 187311 296.3477…   172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [FIN, ACK] Seq=9235 Ack=1544 Win=68352 Len=0 TSval=1663144855 TSecr=1250613642
 187312 296.3481…   10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1544 Ack=9236 Win=131072 Len=0 TSval=1250613728 TSecr=1663144855

youtubeplaypausesniffing@7:09pm.pcapng          Packets: 510644 · Displayed: 44 (0.0%) · Selected: 3 (0.0%)          Profile: Default
```

The first four captured segment starting from no. 39931 are the 3 way TCP handshake data segments. The following are the 3 steps of handshaking to establish a TCP connection between client and server:

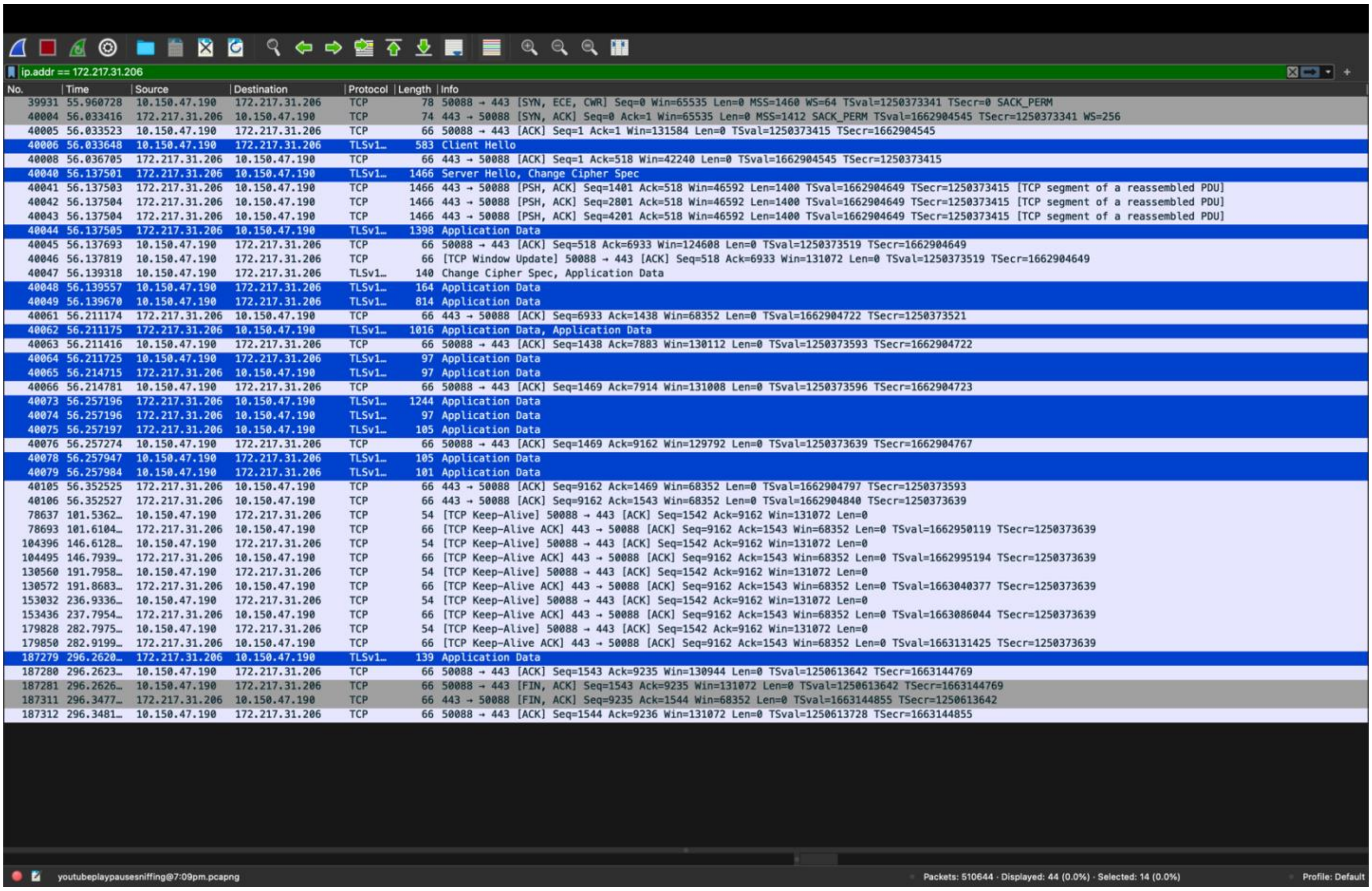
Step 1 (SYN): In the first step, the client wants to establish a connection with the server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with.

Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bit set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with.

Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the application data transfer.

Note: In the snapshot above, the first step of the TCP handshake has ECE (Echo) and CWR (Congestion window reduced) bits set in addition to SYN.

ECE is used to echo back the congestion indication(i.e signal the sender to reduce the transmission rate) and CWR is used to acknowledge that the congestion indication echoing was received.



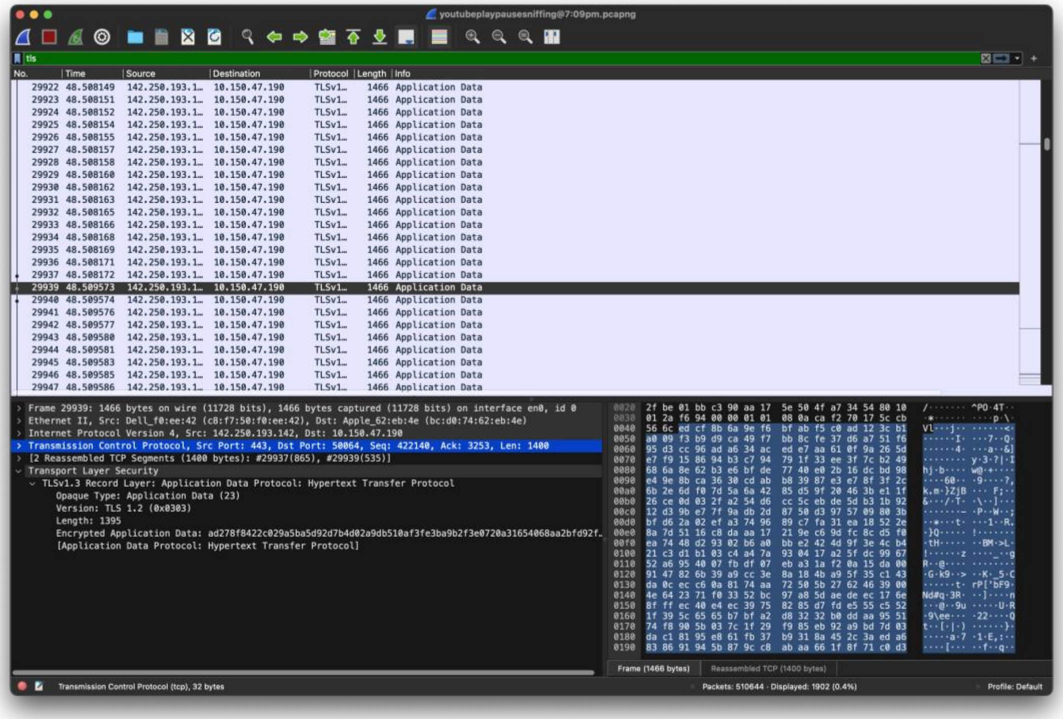
```
ip.addr == 172.217.31.206
No.     Time       Source          Destination     Protocol Length Info
 39931 55.960728  10.150.47.190   172.217.31.206  TCP        78 50088 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1250373341 TSecr=0 SACK_PERM
 40004 56.033416  172.217.31.206  10.150.47.190   TCP        74 443 → 50088 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM TSval=1662904545 TSecr=1250373341 WS=256
 40005 56.033523  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1250373415 TSecr=1662904545
 40006 56.033648  10.150.47.190   172.217.31.206  TLSv1…    583 Client Hello
 40008 56.036705  172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=1 Ack=518 Win=42240 Len=0 TSval=1662904545 TSecr=1250373415
 40040 56.137501  172.217.31.206  10.150.47.190   TLSv1…   1466 Server Hello, Change Cipher Spec
 40041 56.137503  172.217.31.206  10.150.47.190   TCP      1466 443 → 50088 [PSH, ACK] Seq=1401 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reassembled PDU]
 40042 56.137504  172.217.31.206  10.150.47.190   TCP      1466 443 → 50088 [PSH, ACK] Seq=2801 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reassembled PDU]
 40043 56.137504  172.217.31.206  10.150.47.190   TCP      1466 443 → 50088 [PSH, ACK] Seq=4201 Ack=518 Win=46592 Len=1400 TSval=1662904649 TSecr=1250373415 [TCP segment of a reassembled PDU]
 40044 56.137505  172.217.31.206  10.150.47.190   TLSv1…   1398 Application Data
 40045 56.137693  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=518 Ack=6933 Win=124608 Len=0 TSval=1250373519 TSecr=1662904649
 40046 56.137819  10.150.47.190   172.217.31.206  TCP        66 [TCP Window Update] 50088 → 443 [ACK] Seq=518 Ack=6933 Win=131072 Len=0 TSval=1250373519 TSecr=1662904649
 40047 56.139318  10.150.47.190   172.217.31.206  TLSv1…    140 Change Cipher Spec, Application Data
 40048 56.139557  10.150.47.190   172.217.31.206  TLSv1…    164 Application Data
 40049 56.139670  10.150.47.190   172.217.31.206  TLSv1…    814 Application Data
 40061 56.211174  172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=6933 Ack=1438 Win=68352 Len=0 TSval=1662904722 TSecr=1250373521
 40062 56.211175  172.217.31.206  10.150.47.190   TLSv1…   1016 Application Data, Application Data
 40063 56.211416  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1438 Ack=7883 Win=130112 Len=0 TSval=1250373593 TSecr=1662904722
 40064 56.211725  10.150.47.190   172.217.31.206  TLSv1…     97 Application Data
 40065 56.214715  172.217.31.206  10.150.47.190   TLSv1…     97 Application Data
 40066 56.214781  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1469 Ack=7914 Win=131008 Len=0 TSval=1250373596 TSecr=1662904723
 40073 56.257196  172.217.31.206  10.150.47.190   TLSv1…   1244 Application Data
 40074 56.257196  172.217.31.206  10.150.47.190   TLSv1…     97 Application Data
 40075 56.257197  172.217.31.206  10.150.47.190   TLSv1…    105 Application Data
 40076 56.257274  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1469 Ack=9162 Win=129792 Len=0 TSval=1250373639 TSecr=1662904767
 40078 56.257947  10.150.47.190   172.217.31.206  TLSv1…    105 Application Data
 40079 56.257984  10.150.47.190   172.217.31.206  TLSv1…    101 Application Data
 40105 56.352525  172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=9162 Ack=1469 Win=68352 Len=0 TSval=1662904797 TSecr=1250373593
 40106 56.352527  172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1662904840 TSecr=1250373639
 78637 101.5362…  10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
 78693 101.6104…  172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1662950119 TSecr=1250373639
104396 146.6128…  10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
104495 146.7939…  172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1662995194 TSecr=1250373639
130560 191.7958…  10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
130572 191.8683…  172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1663040377 TSecr=1250373639
153032 236.9336…  10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
153436 237.7954…  172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1663086044 TSecr=1250373639
179828 282.7975…  10.150.47.190   172.217.31.206  TCP        54 [TCP Keep-Alive] 50088 → 443 [ACK] Seq=1542 Ack=9162 Win=131072 Len=0
179850 282.9199…  172.217.31.206  10.150.47.190   TCP        66 [TCP Keep-Alive ACK] 443 → 50088 [ACK] Seq=9162 Ack=1543 Win=68352 Len=0 TSval=1663131425 TSecr=1250373639
187279 296.2620…  172.217.31.206  10.150.47.190   TLSv1…    139 Application Data
187280 296.2623…  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1543 Ack=9235 Win=130944 Len=0 TSval=1250613642 TSecr=1663144769
187281 296.2626…  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [FIN, ACK] Seq=1543 Ack=9235 Win=131072 Len=0 TSval=1250613642 TSecr=1663144769
187311 296.3477…  172.217.31.206  10.150.47.190   TCP        66 443 → 50088 [FIN, ACK] Seq=9235 Ack=1544 Win=68352 Len=0 TSval=1663144855 TSecr=1250613642
187312 296.3481…  10.150.47.190   172.217.31.206  TCP        66 50088 → 443 [ACK] Seq=1544 Ack=9236 Win=131072 Len=0 TSval=1250613728 TSecr=1663144855

youtubeplaypausesniffing@7:09pm.pcapng          Packets: 510644 · Displayed: 44 (0.0%) · Selected: 14 (0.0%)          Profile: Default
```

Right after the TCP handshake, TLS handshake occurs following which application data exchange occurs. These steps have been highlighted above.

Data Transmission during video playback:

A video was played on the YouTube tab which was open earlier.

Consider consecutive application data packets numbered 29940 and 29941 below.



youtubeplaypausesniffing@7:09pm.pcapng

tls

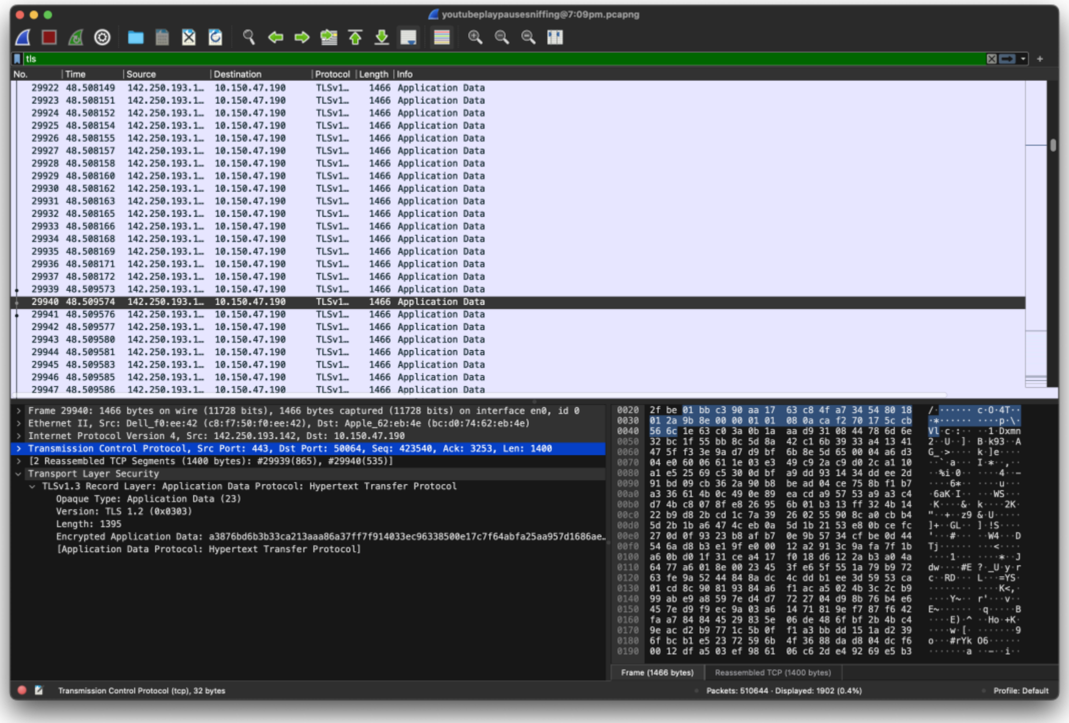
```
No.    Time       Source          Destination     Protocol  Length  Info
29922  48.508149  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29923  48.508151  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29924  48.508152  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29925  48.508154  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29926  48.508155  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29927  48.508157  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29928  48.508158  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29929  48.508160  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29930  48.508162  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29931  48.508163  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29932  48.508165  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29933  48.508166  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29934  48.508168  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29935  48.508169  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29936  48.508171  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29937  48.508172  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29939  48.509573  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29940  48.509574  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29941  48.509576  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29942  48.509577  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29943  48.509580  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29944  48.509581  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29945  48.509583  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29946  48.509585  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29947  48.509586  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
```

```
> Frame 29939: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface en0, id 0
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74:62:eb:4e)
> Internet Protocol Version 4, Src: 142.250.193.142, Dst: 10.150.47.190
> Transmission Control Protocol, Src Port: 443, Dst Port: 50064, Seq: 422140, Ack: 3253, Len: 1400
> [2 Reassembled TCP Segments (1400 bytes): #29937(865), #29939(535)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 1395
      Encrypted Application Data: ad278f8422c029a5ba5d92d7b4d02a9db510af3fe3ba9b2f3e0720a31654068aa2bfd92f…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0020  2f be 01 bb c3 90 aa 17  5e 50 4f a7 34 54 80 10   /·······  ^PO·4T··
0030  01 2a f6 94 00 00 01 01  08 0a ca f2 70 17 5c cb   ·*······  ····p·\·
0040  56 6c ed cf 8b 6a 9e f6  bf ab f5 c0 ad 12 3c b1   Vl···j··  ······<·
0050  a0 09 f3 b9 d9 ca 49 f7  bb 8c fe 37 d6 a7 51 f6   ······I·  ···7··Q·
0060  95 d3 cc 96 ad a6 34 ac  ed e7 aa 61 0f 9a 26 5d   ······4·  ···a··&]
0070  e7 f9 15 86 94 b3 c7 94  79 1f 33 ee 3f 7c b2 49   ········  y·3·?|·I
0080  68 6a 8e 62 b3 e6 bf de  77 40 e0 2b 16 dc bd 98   hj·b····  w@·+····
0090  e4 9e 8b ca 36 30 cd ab  b8 39 87 e3 e7 8f 3f 2c   ····60··  ·9····?,
00a0  6b 2e 6d f0 7d 5a 6a 42  85 d5 9f 20 46 3b e1 1f   k.m·}ZjB  ··· F;··
00b0  26 ce 0d 03 2f a2 54 d6  cc 5c eb de 5d b3 1b 92   &···/·T·  ·\··]···
00c0  12 d3 9b e7 7f 9a db 2d  87 50 d3 97 57 09 80 3b   ·······-  ·P··W··;
00d0  bf d6 2a 02 ef a3 74 96  89 c7 fa 31 ea 18 52 2e   ··*···t·  ···1··R.
00e0  8a 7d 51 16 c8 da aa 17  21 9e c6 9d fc 8c d5 f0   ·}Q·····  !·······
00f0  ea 74 48 d2 93 02 b6 a0  bb e2 42 4d 9f 3e 4c b4   ·tH·····  ··BM·>L·
0100  21 c3 d1 b1 03 c4 a4 7a  93 04 17 a2 5f dc 99 67   !······z  ····_··g
0110  52 a6 95 40 07 fb df 07  eb a3 1a f2 0a 15 da 00   R··@····  ········
0120  91 47 82 6b 39 a9 cc 3e  8a 18 4b a9 5f 35 c1 43   ·G·k9··>  ··K·_5·C
0130  da 0c ec c6 0a 81 74 aa  72 50 5b 27 62 46 39 00   ······t·  rP['bF9·
0140  4e 64 23 71 f0 33 52 bc  97 a8 5d ae de ec 17 6e   Nd#q·3R·  ··]····n
0150  8f ff ec 40 e4 ec 39 75  82 85 d7 fd e5 55 c5 52   ···@··9u  ·····U·R
0160  1f 39 5c 65 65 b7 bf a2  d8 32 32 b0 dd aa 95 51   ·9\ee···  ·22····Q
0170  74 f8 90 5b 03 7c 1f 29  f9 85 eb 92 a9 bd 7d 03   t··[·|·)  ······}·
0180  da c1 81 95 e8 61 fb 37  b9 31 8a 45 2c 3a ed a6   ·····a·7  ·1·E,:··
0190  83 86 91 94 5b 87 9c c8  ab aa 66 1f 8f 71 c0 d3   ····[···  ··f··q··
```

Frame (1466 bytes) | Reassembled TCP (1400 bytes)

Transmission Control Protocol (tcp), 32 bytes · Packets: 510644 · Displayed: 1902 (0.4%) · Profile: Default



youtubeplaypausesniffing@7:09pm.pcapng

tls

```
No.    Time       Source          Destination     Protocol  Length  Info
29922  48.508149  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29923  48.508151  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29924  48.508152  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29925  48.508154  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29926  48.508155  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29927  48.508157  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29928  48.508158  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29929  48.508160  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29930  48.508162  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29931  48.508163  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29932  48.508165  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29933  48.508166  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29934  48.508168  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29935  48.508169  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29936  48.508171  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29937  48.508172  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29939  48.509573  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29940  48.509574  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29941  48.509576  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29942  48.509577  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29943  48.509580  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29944  48.509581  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29945  48.509583  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29946  48.509585  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
29947  48.509586  142.250.193.1…  10.150.47.190   TLSv1…    1466    Application Data
```

```
> Frame 29940: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface en0, id 0
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74:62:eb:4e)
> Internet Protocol Version 4, Src: 142.250.193.142, Dst: 10.150.47.190
> Transmission Control Protocol, Src Port: 443, Dst Port: 50064, Seq: 423540, Ack: 3253, Len: 1400
> [2 Reassembled TCP Segments (1400 bytes): #29939(865), #29940(535)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 1395
      Encrypted Application Data: a3876bd6b3b33ca213aaa86a37ff7f914033ec96338500e17c7f64abfa25aa957d1686ae…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0020  2f be 01 bb c3 90 aa 17  63 c8 4f a7 34 54 80 18   /·······  c·O·4T··
0030  01 2a 9b 8e 00 00 01 01  08 0a ca f2 70 17 5c cb   ·*······  ····p·\·
0040  56 6c 1e 63 c0 3a 0b 1a  aa d9 31 08 44 78 6d 6e   Vl·c·:··  ··1·Dxmn
0050  32 bc 1f 55 bb 8c 5d 8a  42 c1 6b 39 33 a4 13 41   2··U··]·  B·k93··A
0060  47 5f f3 3e 9a d7 d9 bf  6b 8e 5d 65 00 04 a6 d3   G_·>····  k·]e····
0070  04 e0 60 06 61 1e 03 e3  49 c9 2a c9 d0 2c a1 10   ··`·a···  I·*··,··
0080  a1 e5 25 69 c5 30 0d bf  a9 dd 93 14 34 dd ee 2d   ··%i·0··  ····4··-
0090  91 bd 09 cb 36 2a 90 b8  be ad 04 ce 75 8b f1 b7   ····6*··  ····u···
00a0  a3 36 61 4b 0c 49 0e 89  ea cd a9 57 53 a9 a3 c4   ·6aK·I··  ···WS···
00b0  d7 4b c8 07 8f e8 26 95  6b 01 b3 13 ff 32 4b 14   ·K····&·  k····2K·
00c0  22 b9 d8 2b cd 1c 7a 39  26 02 55 90 8c a0 cb b4   "··+··z9  &·U·····
00d0  5d 2b 1b a6 47 4c eb 0a  5d 1b 21 53 e8 0b ce fc   ]+··GL··  ]·!S····
00e0  27 0d 0f 93 23 b8 af b7  0e 9b 57 34 cf be 0d 44   '···#···  ··W4···D
00f0  54 6a d8 b3 e1 9f e0 00  12 a2 91 3c 9a fa 7f 1b   Tj······  ···<····
0100  a6 0b d0 1f 31 ce a4 17  f0 18 d6 12 2a b3 a0 4a   ····1···  ····*··J
0110  64 77 a6 01 8e 00 23 45  3f e6 5f 55 1a 79 b9 72   dw····#E  ?·_U·y·r
0120  63 fe 9a 52 44 84 8a dc  4c dd b1 ee 3d 59 53 ca   c··RD···  L···=YS·
0130  01 cd 8c 90 81 93 84 a6  f1 ac a5 02 4b 3c 2c b9   ········  ····K<,·
0140  99 ab e9 a8 59 7e d4 d7  72 27 04 d9 8b 76 b4 e6   ····Y~··  r'···v··
0150  45 7e d9 f9 ec 9a 03 a6  14 71 81 9e f7 87 f6 42   E~······  ·q·····B
0160  fa a7 84 84 45 29 83 5e  06 de 48 6f bf 2b 4b c4   ····E)·^  ··Ho·+K·
0170  9e ac d2 b9 77 1c 5b 0f  f1 a3 bb dd 15 1a d2 39   ····w·[·  ·······9
0180  6f bc b1 e5 23 72 59 6b  4f 36 88 da d8 04 dc f6   o···#rYk  O6······
0190  00 12 df a5 03 ef 98 61  06 c6 2d e4 92 69 e5 b3   ·······a  ··-··i··
```

Frame (1466 bytes) | Reassembled TCP (1400 bytes)

Transmission Control Protocol (tcp), 32 bytes · Packets: 510644 · Displayed: 1902 (0.4%) · Profile: Default

As stated above, the sequence number in TCP segment keeps track of the number of bits sent. Here the TCP segment size is 1400. Therefore, it is observed that the sequence numbers increment by 1400 which is the segment size.

Observations are listed below for the following actions:

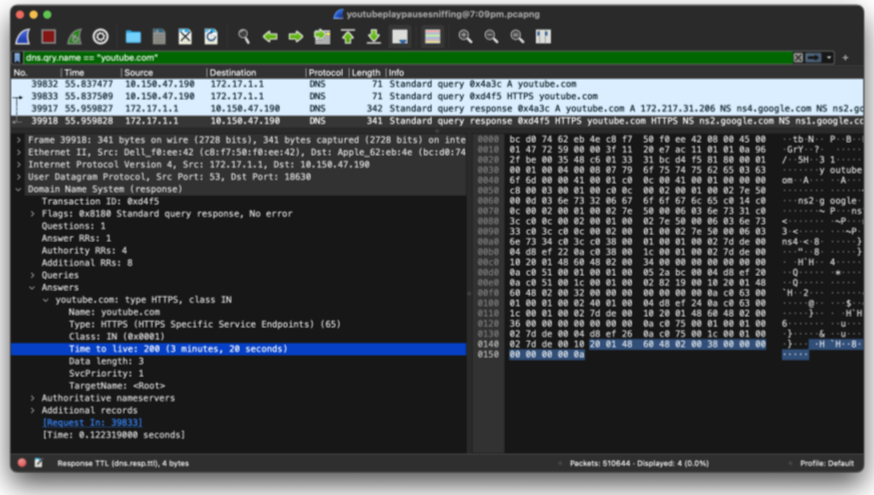
1) Video played without interruptions: The number of displayed packets filtered by TLS constantly rises as the video progresses without any interruptions.
2) Video is paused: The number of displayed packets increases for some time. This is because YouTube downloads the video few seconds in advance to prevent buffering. This is indicated by the white portion of the video progress bar. After this the displayed packets stop incrementing.
3) Switching to another point on the progress bar: The observations were similar to that of point 2.
4) Playing the video on loop: After the first viewing of the video, the displayed packets stopped incrementing as all packets have already been cached.

# Question-4: **Relevance of the protocols used above:**

1) HTTPS: This is a secure version of HTTP which is a pivotal protocol in the application layer. Security is of utmost importance for any application and since YouTube runs on ads, creatives and tracking elements, these objects are requested using an appropriate connection.
2) DNS: This is the main protocol in the application layer that converts the requested domain name to the IP address without which the video servers hosted by YouTube cannot be accessed.
3) UDP: This is the underlying transport protocol used by DNS. Since DNS is versatile, getting access to the video servers in quick time (faster as compared to TCP) is of importance to YouTube.
4) TCP: This protocol is used while streaming the video. It is used because of its reliability, in-order packet transmission and flow and congestion control.

# Question-5: **Caching mechanisms observed:**

DNS has a field named TTL (Time to live) which specifies the amount of time the resolution is valid.



youtubeplaypausesniffing@7:09pm.pcapng

dns.qry.name == "youtube.com"

```
No.     Time       Source         Destination    Protocol Length Info
  39832 55.837477  10.150.47.190  172.17.1.1     DNS        71 Standard query 0x4a3c A youtube.com
  39833 55.837509  10.150.47.190  172.17.1.1     DNS        71 Standard query 0xd4f5 HTTPS youtube.com
  39917 55.959827  172.17.1.1     10.150.47.190  DNS       342 Standard query response 0x4a3c A youtube.com A 172.217.31.206 NS ns4.google.com NS ns2.go
  39918 55.959828  172.17.1.1     10.150.47.190  DNS       341 Standard query response 0xd4f5 HTTPS youtube.com HTTPS NS ns2.google.com NS ns1.google.co
```

```
> Frame 39918: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on inte
> Ethernet II, Src: Dell_f0:ee:42 (c8:f7:50:f0:ee:42), Dst: Apple_62:eb:4e (bc:d0:74
> Internet Protocol Version 4, Src: 172.17.1.1, Dst: 10.150.47.190
> User Datagram Protocol, Src Port: 53, Dst Port: 18630
v Domain Name System (response)
    Transaction ID: 0xd4f5
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 4
    Additional RRs: 8
  > Queries
  v Answers
    v youtube.com: type HTTPS, class IN
        Name: youtube.com
        Type: HTTPS (HTTPS Specific Service Endpoints) (65)
        Class: IN (0x0001)
        Time to live: 200 (3 minutes, 20 seconds)
        Data length: 3
        SvcPriority: 1
        TargetName: <Root>
  > Authoritative nameservers
  > Additional records
    [Request In: 39833]
    [Time: 0.122319000 seconds]
```

```
0000  bc d0 74 62 eb 4e c8 f7  50 f0 ee 42 08 00 45 00
0010  01 47 72 59 00 00 3f 11  20 e7 ac 11 01 01 0a 96
0020  2f be 00 35 48 c6 01 33  31 bc d4 f5 81 80 00 01
0030  00 01 00 04 00 08 07 79  6f 75 74 75 62 65 03 63
0040  6f 6d 00 00 41 00 01 c0  0c 00 41 00 01 00 00 00
0050  c8 00 03 00 01 00 c0 0c  00 02 00 01 00 02 7e 50
0060  00 0d 03 6e 73 32 06 67  6f 6f 67 6c 65 c0 14 c0
0070  0c 00 02 00 01 00 02 7e  50 00 06 03 6e 73 31 c0
0080  3c c0 0c 00 02 00 01 00  02 7e 50 00 06 03 6e 73
0090  33 c0 3c c0 0c 00 02 00  01 00 02 7e 50 00 06 03
00a0  6e 73 34 c0 3c c0 38 00  01 00 01 00 02 7d de 00
00b0  04 d8 ef 22 0a c0 38 00  1c 00 01 00 02 7d de 00
00c0  10 20 01 48 60 48 02 00  34 00 00 00 00 00 00 00
00d0  0a c0 51 00 01 00 01 00  05 2a bc 00 04 d8 ef 20
00e0  0a c0 51 00 1c 00 01 00  02 82 19 00 10 20 01 48
00f0  60 48 02 00 32 00 00 00  00 00 00 00 0a c0 63 00
0100  01 00 01 00 02 40 01 00  04 d8 ef 24 0a c0 63 00
0110  1c 00 01 00 02 7d de 00  10 20 01 48 60 48 02 00
0120  36 00 00 00 00 00 00 00  0a c0 75 00 01 00 01 00
0130  02 7d de 00 04 d8 ef 26  0a c0 75 00 1c 00 01 00
0140  02 7d de 00 10 20 01 48  60 48 02 00 38 00 00 00
0150  00 00 00 00 0a
```

Response TTL (dns.resp.ttl), 4 bytes

Packets: 510644 · Displayed: 4 (0.0%)

Profile: Default

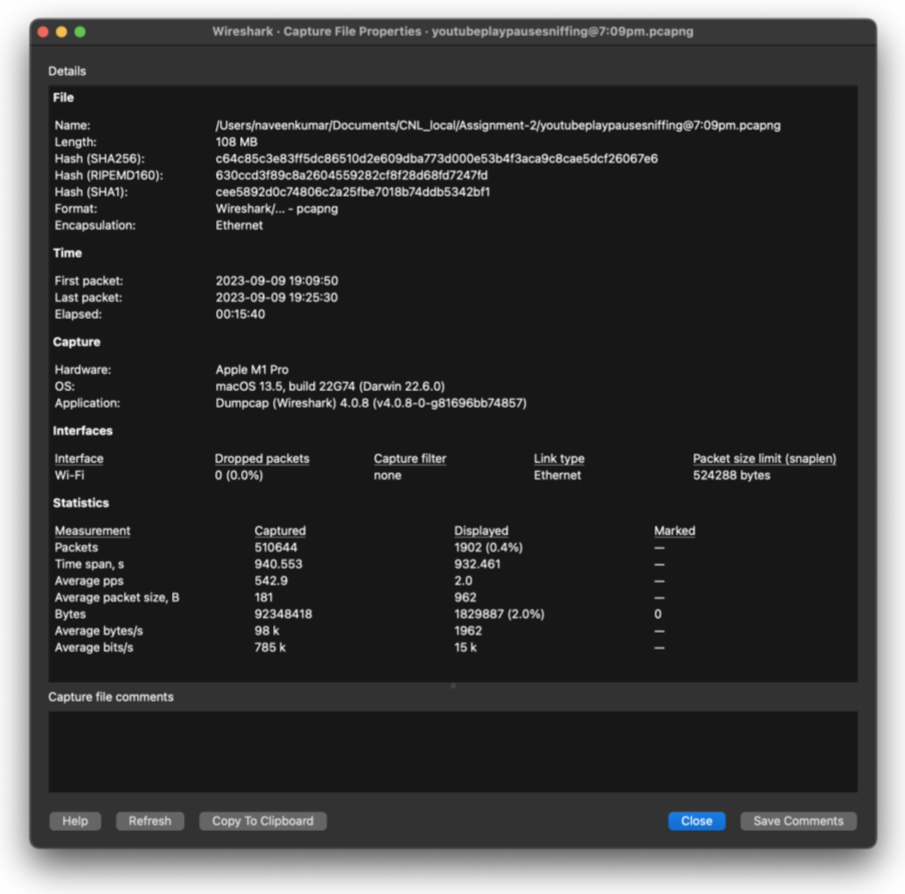
It was observed that if another request to youtube.com, then no DNS request was made if it was within 3 minutes and 20 seconds which is the TTL. Additionally, clearing the browser cache within the TTL resulted in repeated DNS request. This implies that there were caching mechanisms in the network.

Question-6:

Session 1:

Network: IITG CONNECT Time: 2023-09-09 19:09:50

Packet statistics:


Wireshark · Capture File Properties · youtubeplaypausesniffing@7:09pm.pcapng
Help
Refresh
Copy To Clipboard
Close
Save Comments

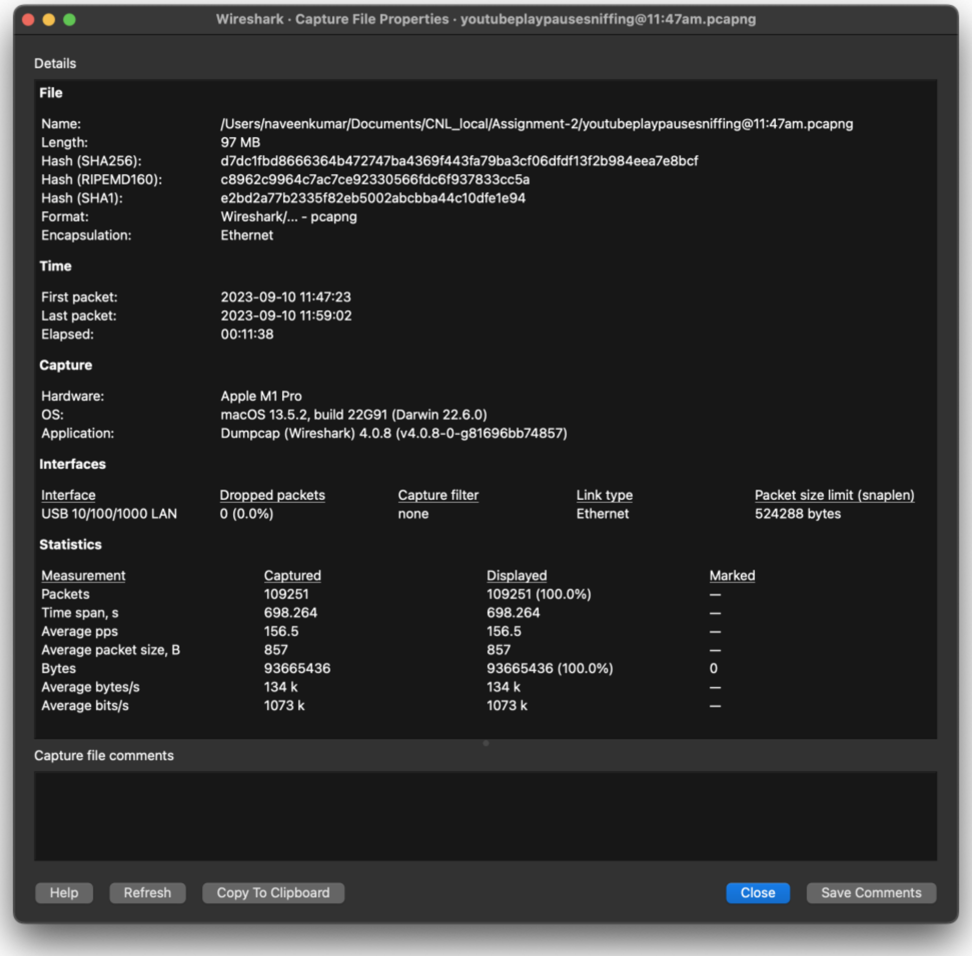
```
Details
File

Name:                  /Users/naveenkumar/Documents/CNL_local/Assignment-2/youtubeplaypausesniffing@7:09pm.pcapng
Length:                108 MB
Hash (SHA256):         c64c85c3e83ff5dc86510d2e609dba773d000e53b4f3aca9c8cae5dcf26067e6
Hash (RIPEMD160):      630ccd3f89c8a2604559282cf8f28d68fd7247fd
Hash (SHA1):           cee5892d0c74806c2a25fbe7018b74ddb5342bf1
Format:                Wireshark/... - pcapng
Encapsulation:         Ethernet

Time

First packet:          2023-09-09 19:09:50
Last packet:           2023-09-09 19:25:30
Elapsed:               00:15:40

Capture

Hardware:              Apple M1 Pro
OS:                    macOS 13.5, build 22G74 (Darwin 22.6.0)
Application:           Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

Interfaces

Interface              Dropped packets     Capture filter     Link type     Packet size limit (snaplen)
Wi-Fi                  0 (0.0%)            none               Ethernet      524288 bytes

Statistics

Measurement                 Captured        Displayed          Marked
Packets                     510644          1902 (0.4%)        —
Time span, s                940.553         932.461            —
Average pps                 542.9           2.0                —
Average packet size, B      181             962                —
Bytes                       92348418        1829887 (2.0%)     0
Average bytes/s             98 k            1962               —
Average bits/s              785 k           15 k               —

Capture file comments
```

Throughput	542.9 packets per second
RTT	122.350000ms
Packet Size	181 bytes
Number of packets lost	0
Number of UDP packets	139198
Number of TCP packets	4331
Number of responses w.r.t. one request	4.2171

Session 2:

Network: IITG LAN Hostel   Time: 2023-09-10 11:47:23

Packet statistics:



Wireshark · Capture File Properties · youtubeplaypausesniffing@11:47am.pcapng

Details

File

Name: /Users/naveenkumar/Documents/CNL_local/Assignment-2/youtubeplaypausesniffing@11:47am.pcapng
Length: 97 MB
Hash (SHA256): d7dc1fbd8666364b472747ba4369f443fa79ba3cf06dfdf13f2b984eea7e8bcf
Hash (RIPEMD160): c8962c9964c7ac7ce92330566fdc6f937833cc5a
Hash (SHA1): e2bd2a77b2335f82eb5002abcbba44c10dfe1e94
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2023-09-10 11:47:23
Last packet: 2023-09-10 11:59:02
Elapsed: 00:11:38

Capture

Hardware: Apple M1 Pro
OS: macOS 13.5.2, build 22G91 (Darwin 22.6.0)
Application: Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
USB 10/100/1000 LAN	0 (0.0%)	none	Ethernet	524288 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	109251	109251 (100.0%)	—
Time span, s	698.264	698.264	—
Average pps	156.5	156.5	—
Average packet size, B	857	857	—
Bytes	93665436	93665436 (100.0%)	0
Average bytes/s	134 k	134 k	—
Average bits/s	1073 k	1073 k	—

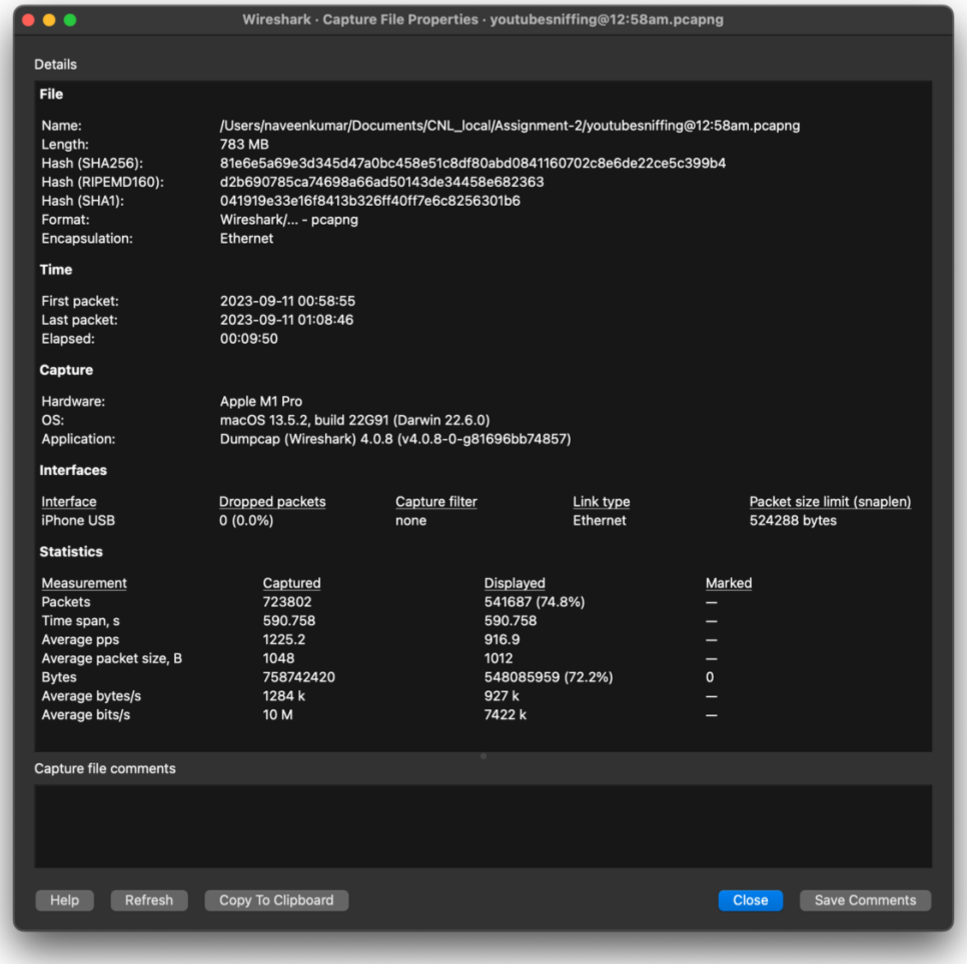
Capture file comments

Throughput	156.5 packets per second
RTT	0.591000ms
Packet Size	857 bytes
Number of packets lost	0
Number of UDP packets	83814
Number of TCP packets	13866
Number of responses w.r.t. one request	3.9854

Session 3:

Network: Mobile Hotspot   Time: 2023-09-11 00:58:55

Packet statistics:



Wireshark · Capture File Properties · youtubesniffing@12:58am.pcapng

Details

File

Name:	/Users/naveenkumar/Documents/CNL_local/Assignment-2/youtubesniffing@12:58am.pcapng
Length:	783 MB
Hash (SHA256):	81e6e5a69e3d345d47a0bc458e51c8df80abd0841160702c8e6de22ce5c399b4
Hash (RIPEMD160):	d2b690785ca74698a66ad50143de34458e682363
Hash (SHA1):	041919e33e16f8413b326ff40ff7e6c8256301b6
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2023-09-11 00:58:55
Last packet:	2023-09-11 01:08:46
Elapsed:	00:09:50

Capture

Hardware:	Apple M1 Pro
OS:	macOS 13.5.2, build 22G91 (Darwin 22.6.0)
Application:	Dumpcap (Wireshark) 4.0.8 (v4.0.8-0-g81696bb74857)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
iPhone USB	0 (0.0%)	none	Ethernet	524288 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	723802	541687 (74.8%)	—
Time span, s	590.758	590.758	—
Average pps	1225.2	916.9	—
Average packet size, B	1048	1012	—
Bytes	758742420	548085959 (72.2%)	0
Average bytes/s	1284 k	927 k	—
Average bits/s	10 M	7422 k	—

Capture file comments

Throughput	1225.2 packets per second
RTT	26.825000ms
Packet Size	1048 bytes
Number of packets lost	0
Number of UDP packets	181956
Number of TCP packets	541687
Number of responses w.r.t. one request	3.2472