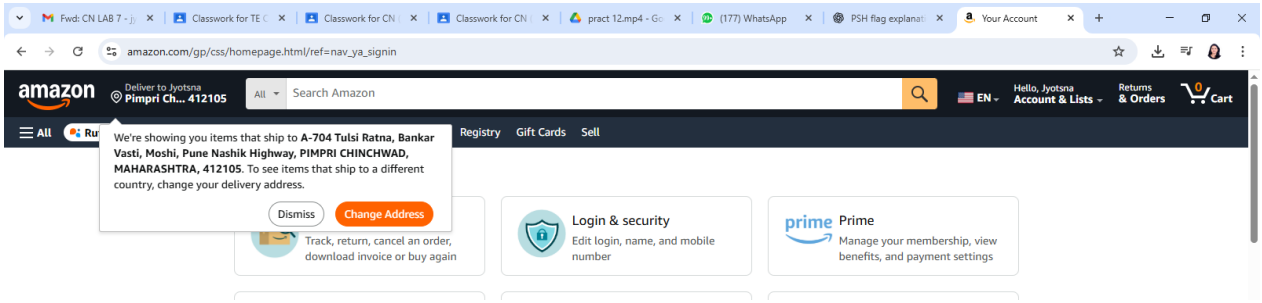
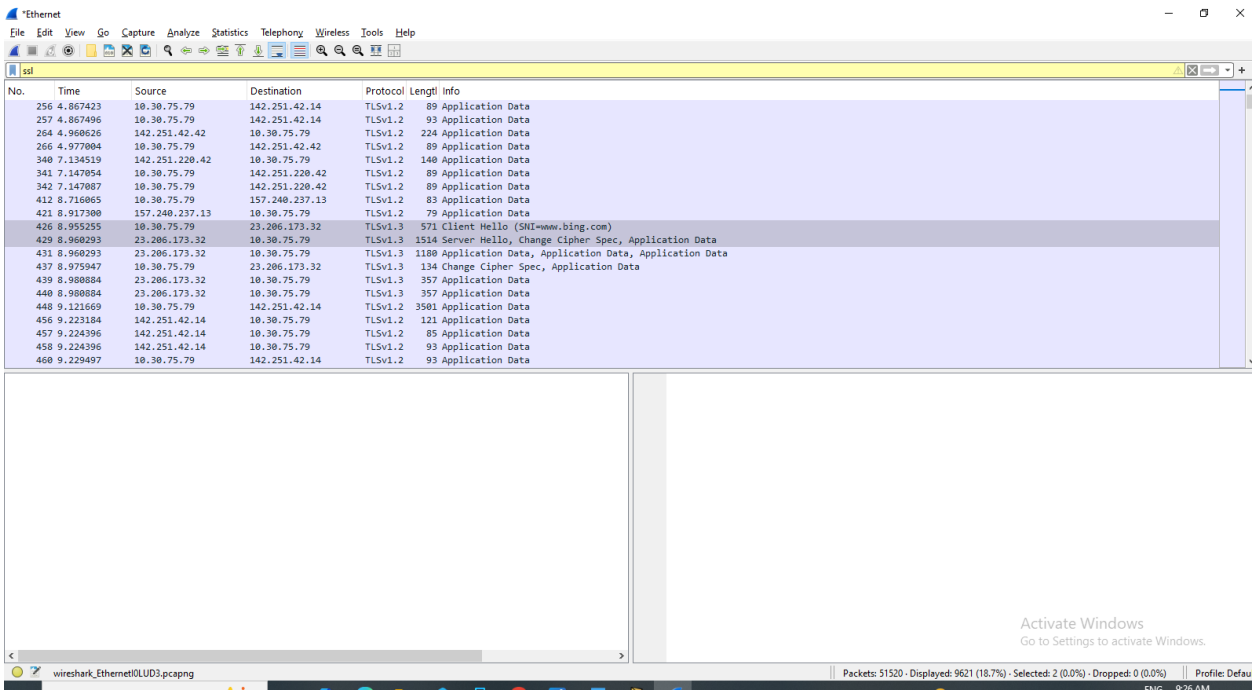
12. To study the SSL protocol by capturing the packets using Wireshark tool while visiting anySSL secured website (banking, e-commerce etc.).

1.Open Wireshark first

2.Open Amazone and login

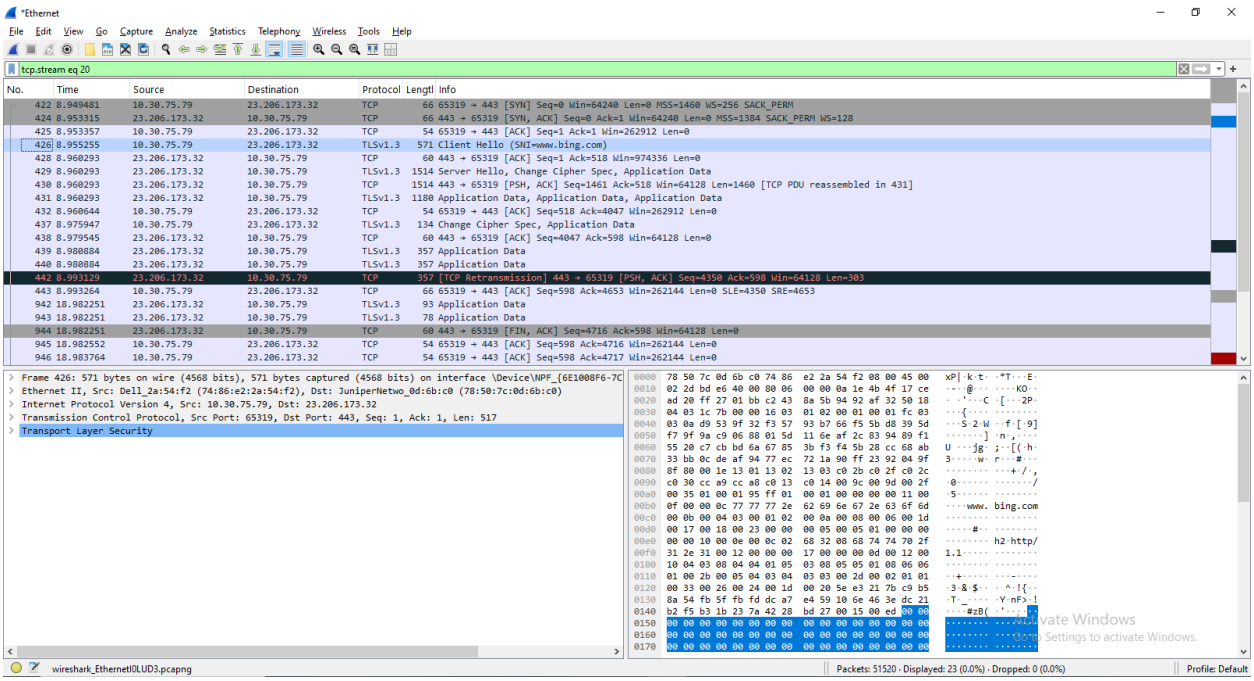


3.Stop packet capturing on wire shark

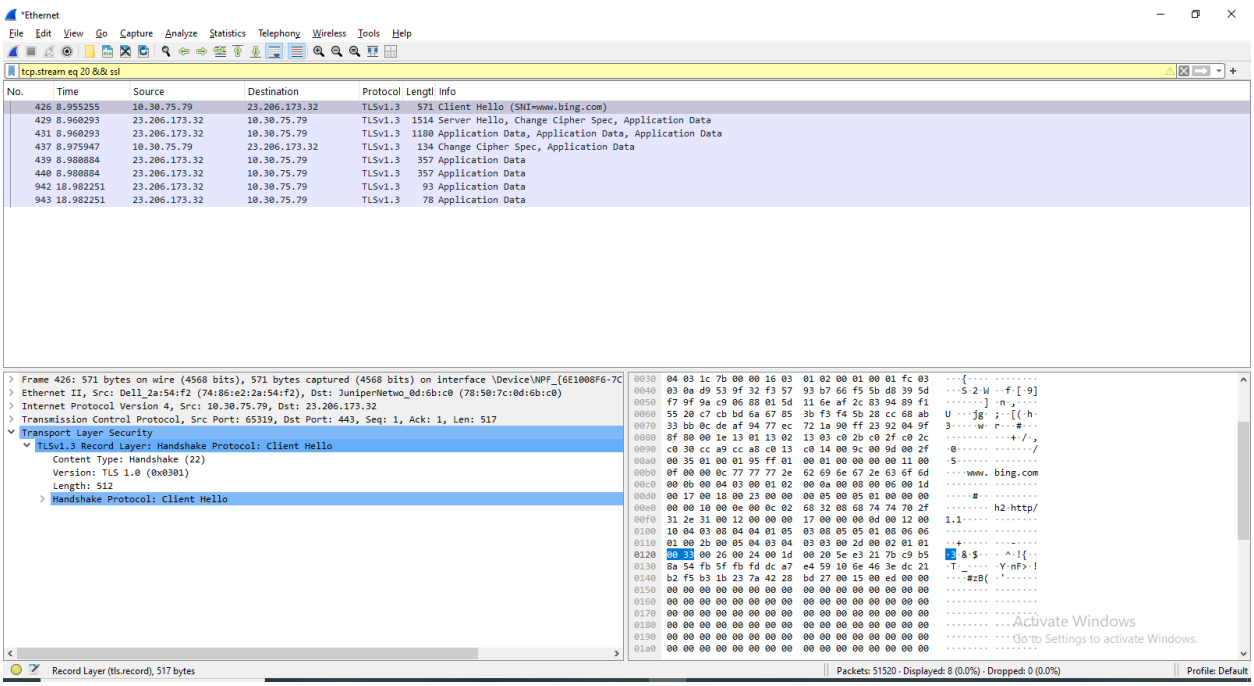


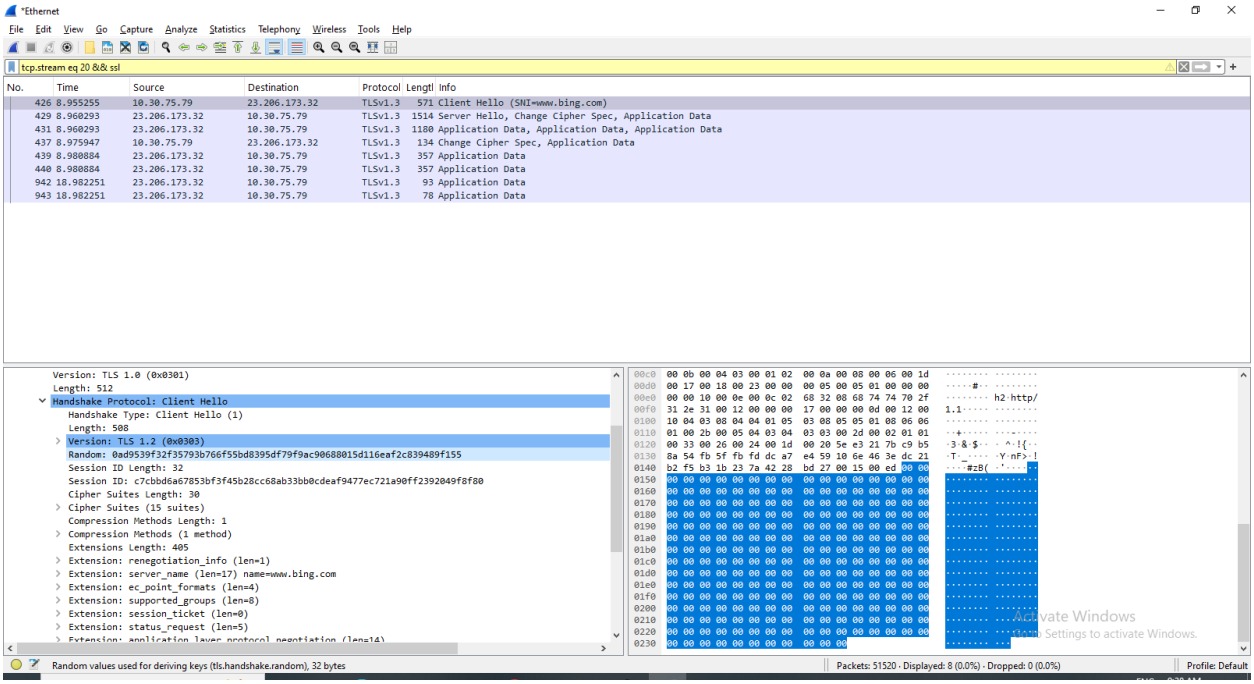
4.Right click Click on →> Client hello →follow → TLS Stream → you will get popup close that by doing this you will get one command on Wireshark as follow

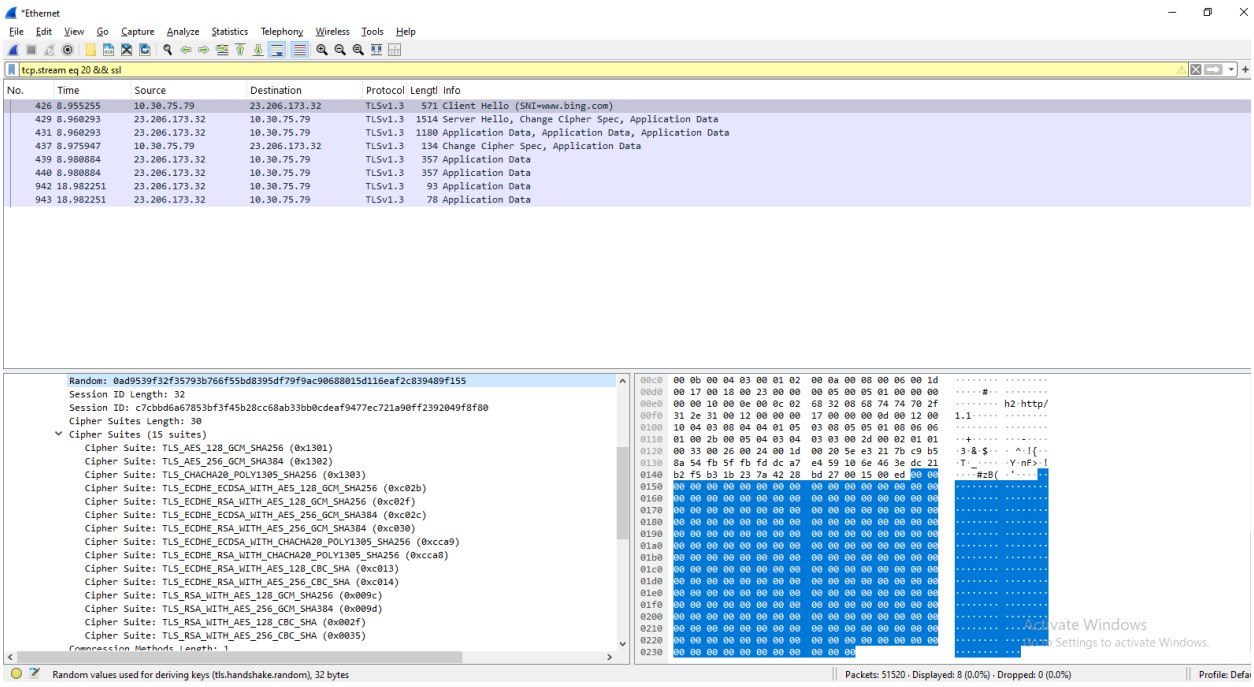
tcp.stream eq 20



5. tcp.stream eq 20 && ssl

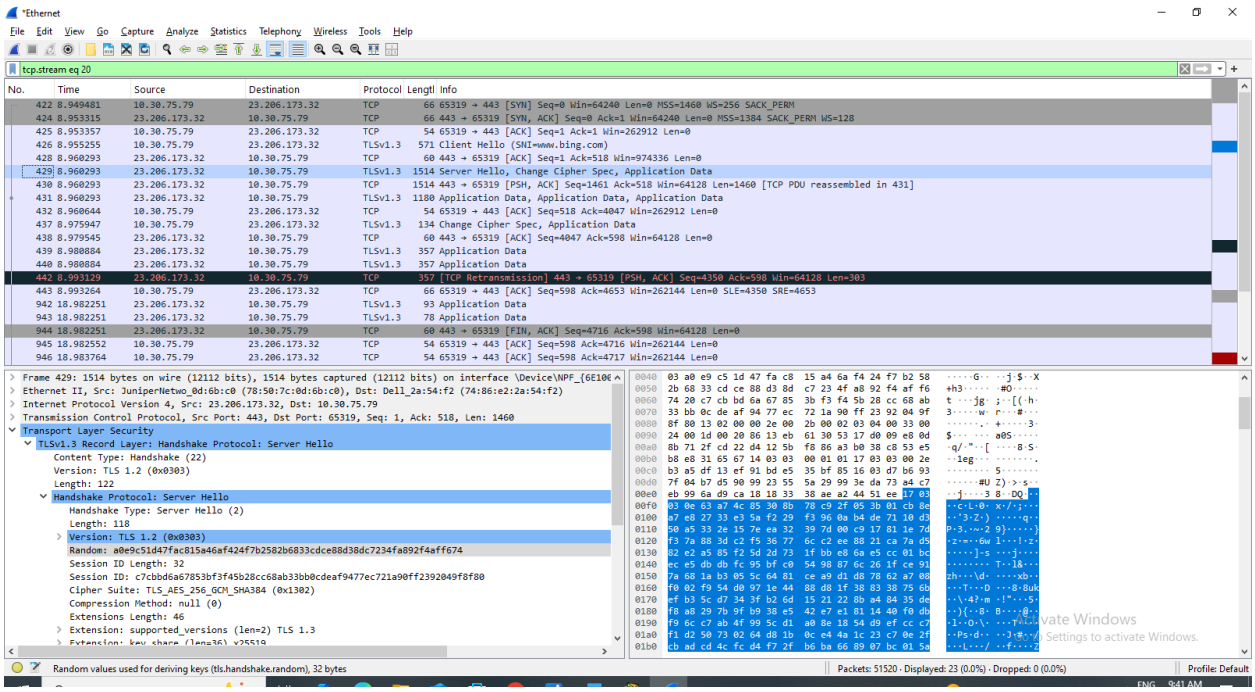






(Click on bottom Transport layer security thrn again click on arrow you will get all details)

7.If you do right click on server hello →follow → TLS Stream → you will get popup close that by doing this you will get one command on Wireshark as follow


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 20
No. Time Source Destination Protocol Length Info
422 8.949481 10.30.75.79 23.206.173.32 TCP 66 65319 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
424 8.953315 23.206.173.32 10.30.75.79 TCP 66 443 → 65319 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1384 SACK_PERM WS=128
425 8.953357 10.30.75.79 23.206.173.32 TCP 54 65319 → 443 [ACK] Seq=1 Ack=1 Win=262912 Len=0
426 8.955255 10.30.75.79 23.206.173.32 TLSv1.3 571 Client Hello (SNI=www.bing.com)
428 8.960293 23.206.173.32 10.30.75.79 TCP 60 443 → 65319 [ACK] Seq=1 Ack=518 Win=974336 Len=0
429 8.960293 23.206.173.32 10.30.75.79 TLSv1.3 1514 Server Hello, Change Cipher Spec, Application Data
430 8.960293 23.206.173.32 10.30.75.79 TCP 1514 443 → 65319 [PSH, ACK] Seq=1461 Ack=518 Win=64128 Len=1460 [TCP PDU reassembled in 431]
431 8.960293 23.206.173.32 10.30.75.79 TLSv1.3 1180 Application Data, Application Data, Application Data
432 8.960644 10.30.75.79 23.206.173.32 TCP 54 65319 → 443 [ACK] Seq=518 Ack=4047 Win=262912 Len=0
437 8.975947 10.30.75.79 23.206.173.32 TLSv1.3 134 Change Cipher Spec, Application Data
438 8.979545 23.206.173.32 10.30.75.79 TCP 60 443 → 65319 [ACK] Seq=4047 Ack=598 Win=64128 Len=0
439 8.980884 23.206.173.32 10.30.75.79 TLSv1.3 357 Application Data
440 8.980884 23.206.173.32 10.30.75.79 TLSv1.3 357 Application Data
442 8.993129 23.206.173.32 10.30.75.79 TCP 357 [TCP Retransmission] 443 → 65319 [PSH, ACK] Seq=4350 Ack=598 Win=64128 Len=303
443 8.993264 10.30.75.79 23.206.173.32 TCP 66 65319 → 443 [ACK] Seq=598 Ack=4653 Win=262144 Len=0 SLE=4350 SRE=4653
942 18.982251 23.206.173.32 10.30.75.79 TLSv1.3 93 Application Data
943 18.982251 23.206.173.32 10.30.75.79 TLSv1.3 78 Application Data
944 18.982251 23.206.173.32 10.30.75.79 TCP 60 443 → 65319 [FIN, ACK] Seq=4716 Ack=598 Win=64128 Len=0
945 18.982552 10.30.75.79 23.206.173.32 TCP 54 65319 → 443 [ACK] Seq=598 Ack=4716 Win=262144 Len=0
946 18.983764 10.30.75.79 23.206.173.32 TCP 54 65319 → 443 [ACK] Seq=598 Ack=4717 Win=262144 Len=0
Frame 429: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{6E10
Ethernet II, Src: JuniperNetwo_0d:6b:c0 (78:50:7c:0d:6b:c0), Dst: Dell_2a:54:f2 (74:86:e2:2a:54:f2)
Internet Protocol Version 4, Src: 23.206.173.32, Dst: 10.30.75.79
Transmission Control Protocol, Src Port: 443, Dst Port: 65319, Seq: 1, Ack: 518, Len: 1460
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 122
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 118
Version: TLS 1.2 (0x0303)
Random: a0e9c51d47fac815a46af424f7b2582b6833cdce88d38dc7234fa892f4aff674
Session ID Length: 32
Session ID: c7cbbd6a67853bf3f45b28cc68ab33bb0cdeaf9477ec721a90ff2392049f8f80
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Compression Method: null (0)
Extensions Length: 46
Extension: supported_versions (len=2) TLS 1.3
0040 03 a0 e9 c5 1d 47 fa c8 15 a4 6a f4 24 f7 b2 58
0050 2b 68 33 cd ce 88 d3 8d c7 23 4f a8 92 f4 af f6
0060 74 20 c7 cb bd 6a 67 85 3b f3 f4 5b 28 cc 68 ab
0070 33 bb 0c de af 94 77 ec 72 1a 90 ff 23 92 04 9f
0080 8f 80 13 02 00 00 2e 00 2b 00 02 03 04 00 33 00
0090 24 00 1d 00 20 86 13 eb 61 30 53 17 d0 09 e8 0d
00a0 8b 71 2f cd 22 d4 12 5b f8 86 a3 b0 38 c8 53 e5
00b0 b8 e8 31 65 67 14 03 03 00 01 01 17 03 03 00 2e
00c0 b3 a5 df 13 ef 91 bd e5 35 bf 85 16 03 d7 b6 93
00d0 7f 04 b7 d5 90 99 23 55 5a 29 99 3e da 73 a4 c7
00e0 eb 99 6a d9 ca 18 18 33 38 ae a2 44 51 ee 17 03
00f0 03 0e 63 a7 4c 85 30 8b 78 c9 2f 05 3b 01 cb 8e
0100 a7 e8 27 33 e3 5a f2 29 f3 96 0a b4 de 71 10 d3
0110 50 a5 33 2e 15 7e ea 32 39 7d 00 c9 17 81 1e 7d
0120 f3 7a 88 3d c2 f5 36 77 6c c2 ee 88 21 ca 7a d5
0130 02 e2 a5 85 f2 5d 2d 73 1f bb e8 6a e5 cc 01 bc
0140 ec e5 db db fc 95 bf c0 54 98 87 6c 26 1f ce 91
0150 7a 68 1a b3 05 5c 64 81 ce a9 d1 d8 78 62 a7 08
0160 f0 02 f9 54 d0 97 1e 44 88 d8 1f 38 83 38 75 6b
0170 ef b3 5c d7 34 3f b2 6d 15 21 22 8b a4 84 35 de
0180 f8 a8 29 7b 9f b9 38 e5 42 e7 e1 81 14 40 f0 db
0190 f9 6c c7 ab 4f 99 5c d1 a0 0e 18 54 d9 ef cc c7
01a0 f1 d2 50 73 02 64 d8 1b 0c e4 4a 1c 23 c7 0e 2f
01b0 cb ad cd 4c fc d4 f7 2f b6 ba 66 89 07 bc 01 5a
Random values used for deriving keys (tls.handshake.random), 32 bytes
Packets: 51520 · Displayed: 23 (0.0%) · Dropped: 0 (0.0%)
Profile: Default