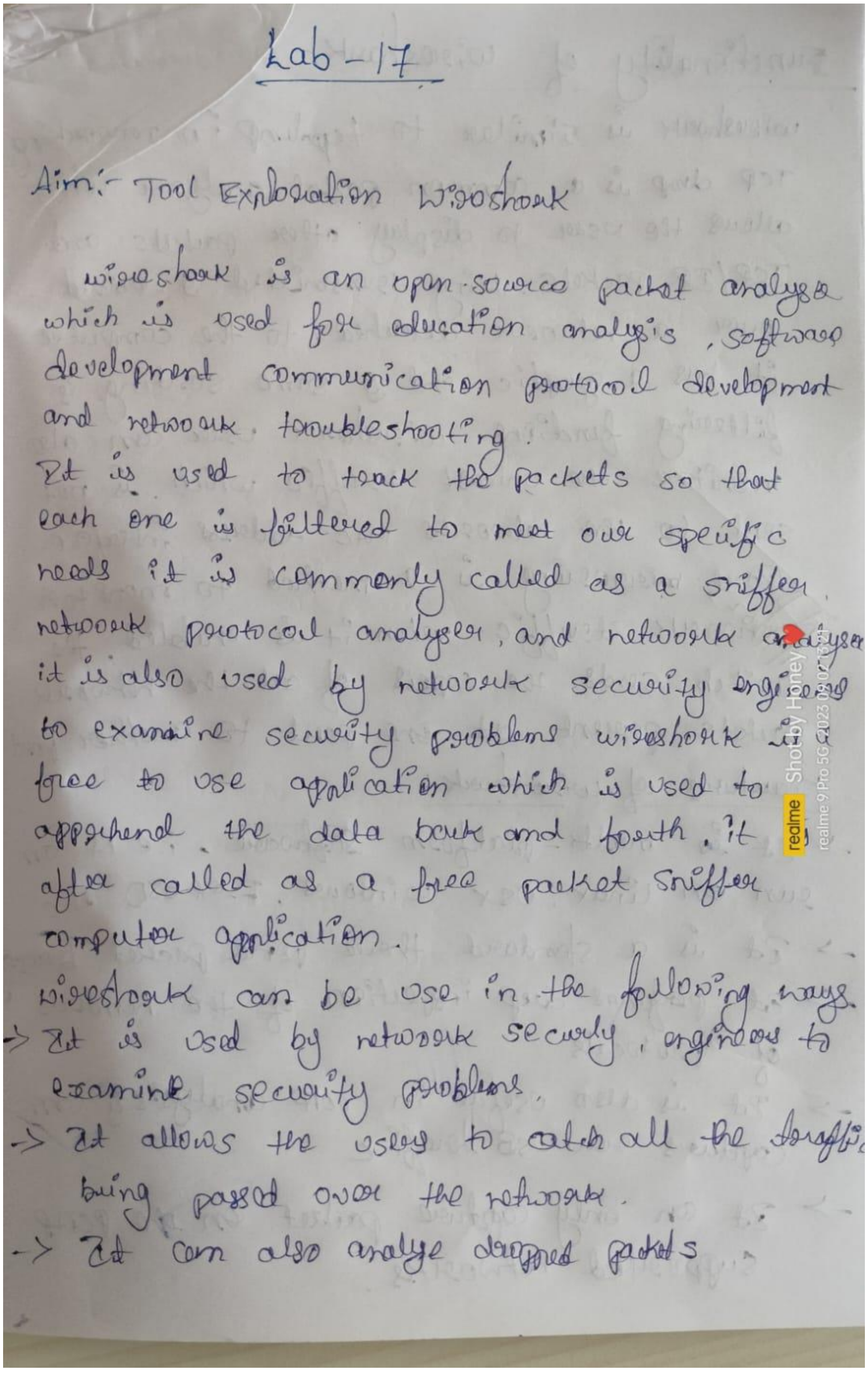
LAB 15

Tool Exploration -Wireshark.

OBSERVATION :



Lab - 17

Aim:- Tool Exploration Wireshark

wireshark is an open-source packet analyser which is used for education analysis, software development communication protocol development and network troubleshooting.

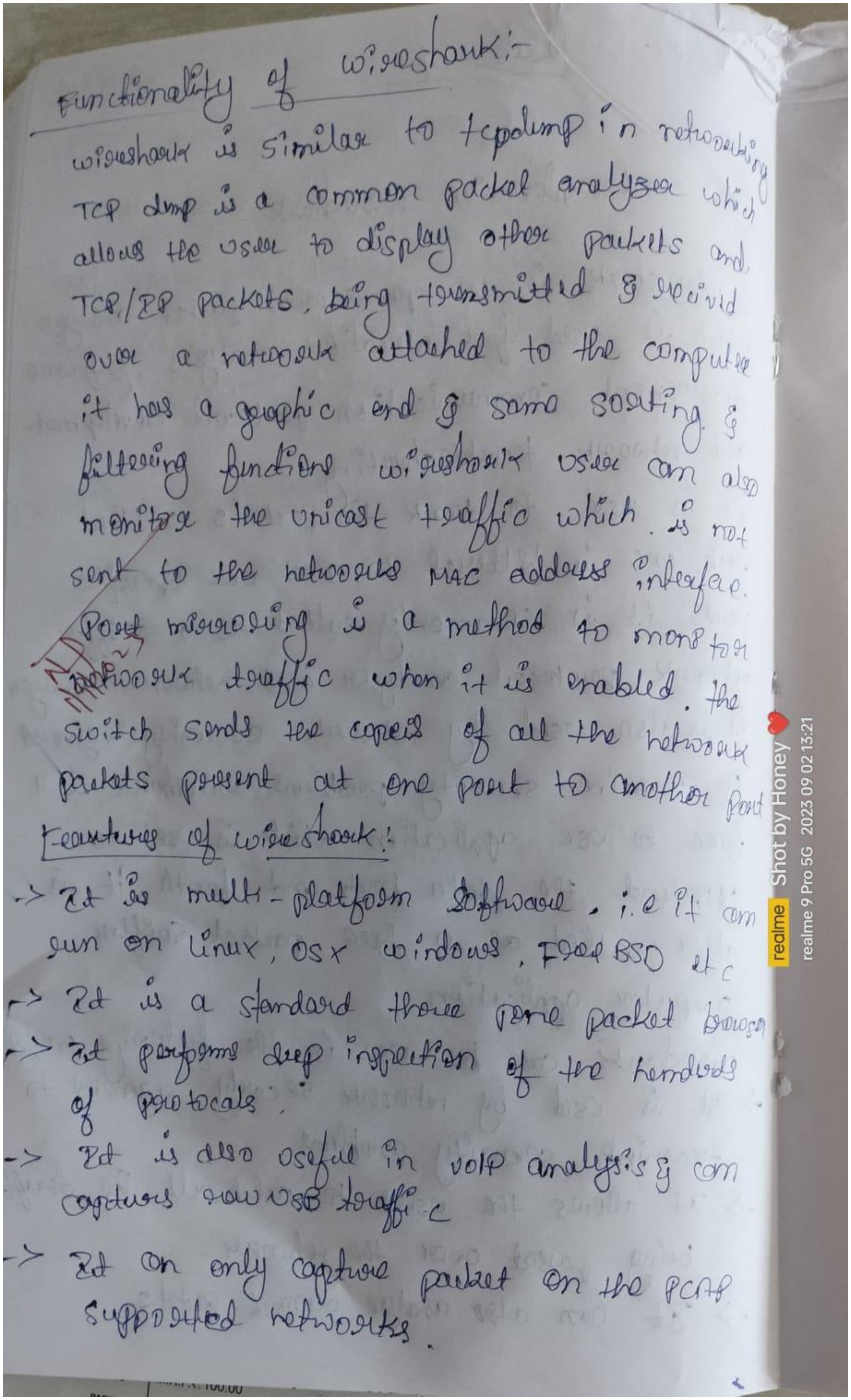
It is used to track the packets so that each one is filtered to meet our specific needs it is commonly called as a sniffer, network protocol analyser, and network analyser it is also used by network security engineers to examine security problems wireshark is a free to use application which is used to apprehend the data back and forth. it is often called as a free packet sniffer computer application.

wireshark can be use in the following ways.

-> It is used by network securly, engineers to examine security problems.

-> It allows the users to catch all the traffic being passed over the network.

-> It can also analye dropped packets



Functionality of wireshark:-

wireshark is similar to tcpdump in networking TCP dump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted & receivd over a network attached to the computer it has a graphic end & some sorting & filtering functions wireshark user can also monitor the unicast traffic which is not sent to the networks MAC address interface. Port mirroring is a method to monitor network traffic when it is enabled. the switch sends the copies of all the network packets present at one port to another port.

Features of wireshark:

-> It is multi-platform software. i.e it can run on Linux, OSX windows, Free BSD etc

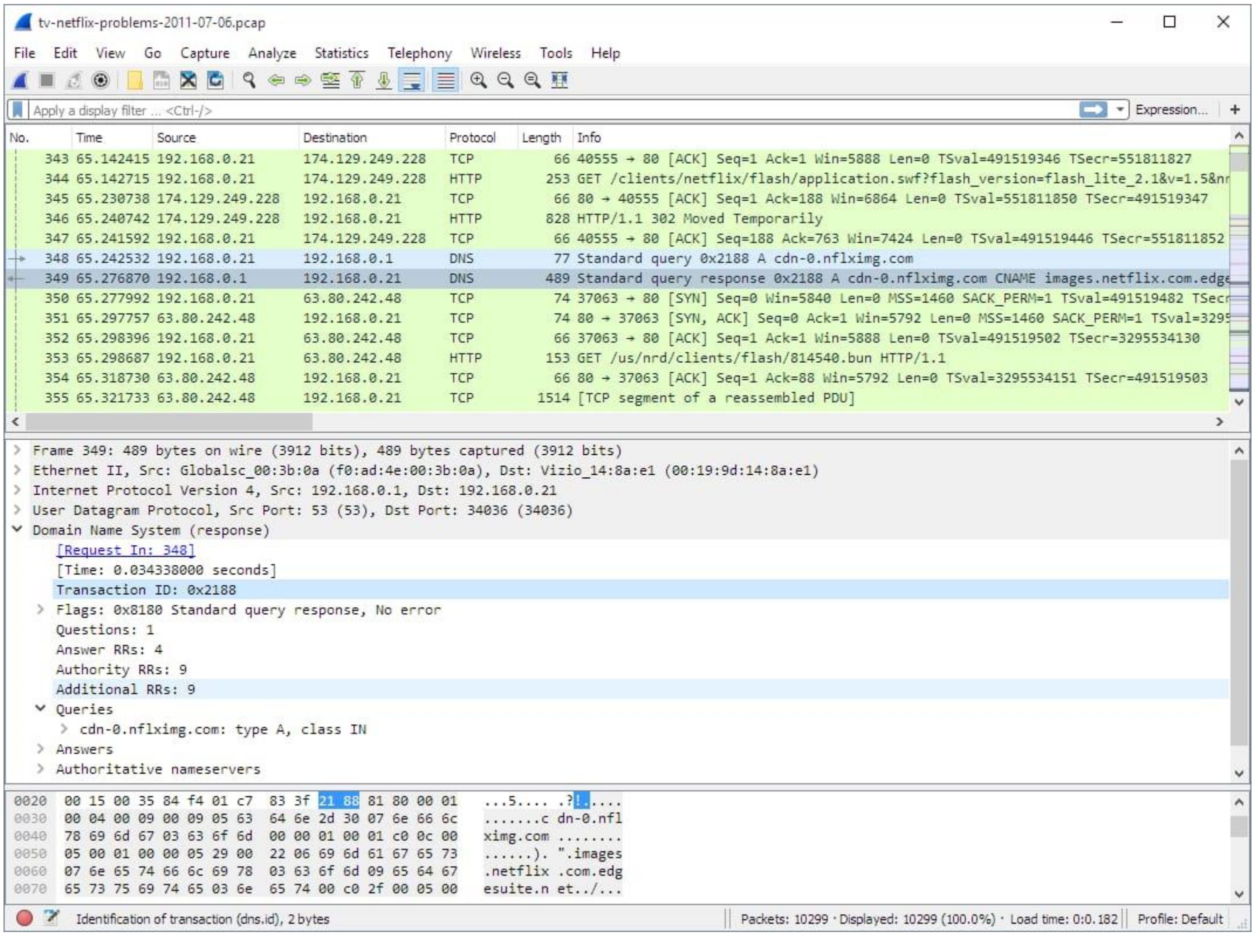
-> It is a standard three pane packet browser

-> It performs deep inspection of the hendreds of protocals.

-> It is also useful in voip analysis & can captures raw USB traffic

-> It can only capture packet on the PCAP supported networks.

OUTPUT :

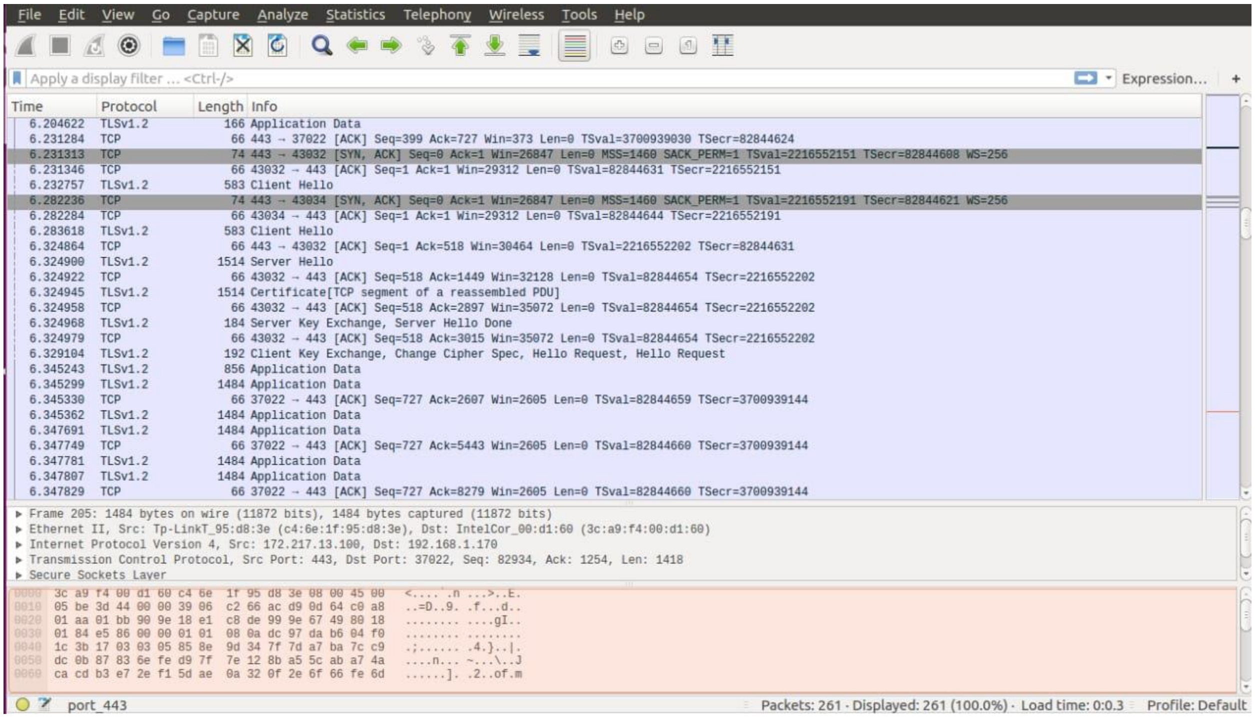

tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

```
Identification of transaction (dns.id), 2 bytes    Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182    Profile: Default
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
Time      Protocol Length Info
 6.204622 TLSv1.2    166 Application Data
 6.231284 TCP         66 443 → 37022 [ACK] Seq=399 Ack=727 Win=373 Len=0 TSval=3700939030 TSecr=82844624
 6.231313 TCP         74 443 → 43032 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2216552151 TSecr=82844608 WS=256
 6.231346 TCP         66 43032 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=82844631 TSecr=2216552151
 6.232757 TLSv1.2    583 Client Hello
 6.282236 TCP         74 443 → 43034 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2216552191 TSecr=82844621 WS=256
 6.282284 TCP         66 43034 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=82844644 TSecr=2216552191
 6.283618 TLSv1.2    583 Client Hello
 6.324864 TCP         66 443 → 43032 [ACK] Seq=1 Ack=518 Win=30464 Len=0 TSval=2216552202 TSecr=82844631
 6.324900 TLSv1.2   1514 Server Hello
 6.324922 TCP         66 43032 → 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=82844654 TSecr=2216552202
 6.324945 TLSv1.2   1514 Certificate[TCP segment of a reassembled PDU]
 6.324958 TCP         66 43032 → 443 [ACK] Seq=518 Ack=2897 Win=35072 Len=0 TSval=82844654 TSecr=2216552202
 6.324968 TLSv1.2    184 Server Key Exchange, Server Hello Done
 6.324979 TCP         66 43032 → 443 [ACK] Seq=518 Ack=3015 Win=35072 Len=0 TSval=82844654 TSecr=2216552202
 6.329104 TLSv1.2    192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
 6.345243 TLSv1.2    856 Application Data
 6.345299 TLSv1.2   1484 Application Data
 6.345330 TCP         66 37022 → 443 [ACK] Seq=727 Ack=2607 Win=2605 Len=0 TSval=82844659 TSecr=3700939144
 6.345362 TLSv1.2   1484 Application Data
 6.347691 TLSv1.2   1484 Application Data
 6.347749 TCP         66 37022 → 443 [ACK] Seq=727 Ack=5443 Win=2605 Len=0 TSval=82844660 TSecr=3700939144
 6.347781 TLSv1.2   1484 Application Data
 6.347807 TLSv1.2   1484 Application Data
 6.347829 TCP         66 37022 → 443 [ACK] Seq=727 Ack=8279 Win=2605 Len=0 TSval=82844660 TSecr=3700939144
```

```
▶ Frame 205: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits)
▶ Ethernet II, Src: Tp-LinkT_95:d8:3e (c4:6e:1f:95:d8:3e), Dst: IntelCor_00:d1:60 (3c:a9:f4:00:d1:60)
▶ Internet Protocol Version 4, Src: 172.217.13.100, Dst: 192.168.1.170
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 37022, Seq: 82934, Ack: 1254, Len: 1418
▶ Secure Sockets Layer
```

```
0000  3c a9 f4 00 d1 60 c4 6e  1f 95 d8 3e 08 00 45 00   <....`.n ...>..E.
0010  05 be 3d 44 00 00 39 06  c2 66 ac d9 0d 64 c0 a8   ..=D..9. .f...d..
0020  01 aa 01 bb 90 9e 18 e1  c8 de 99 9e 67 49 80 18   ........ ....gI..
0030  01 84 e5 86 00 00 01 01  08 0a dc 97 da b6 04 f0   ........ ........
0040  1c 3b 17 03 03 05 85 8e  9d 34 7f 7d a7 ba 7c c9   .;...... .4.}..|.
0050  dc 0b 87 83 6e fe d9 7f  7e 12 8b a5 5c ab a7 4a   ....n... ~...\..J
0060  ca cd b3 e7 2e f1 5d ae  0a 32 0f 2e 6f 66 fe 6d   ......]. .2..of.m
```

```
port_443    Packets: 261 · Displayed: 261 (100.0%) · Load time: 0:0.3    Profile: Default
```