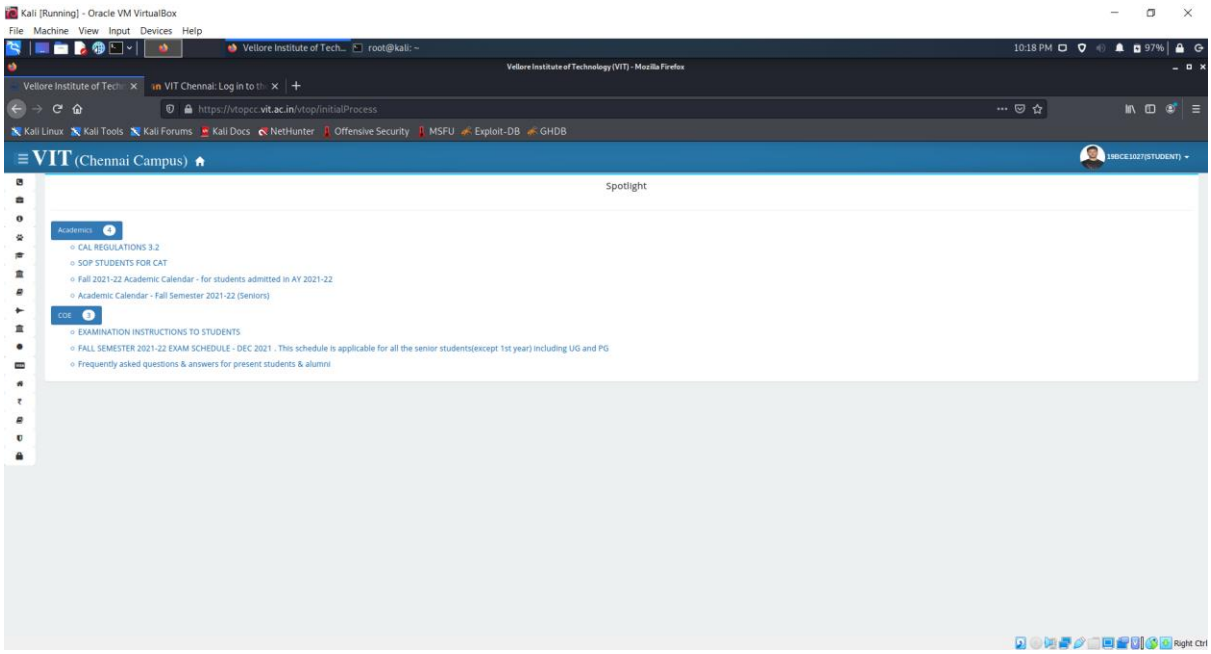
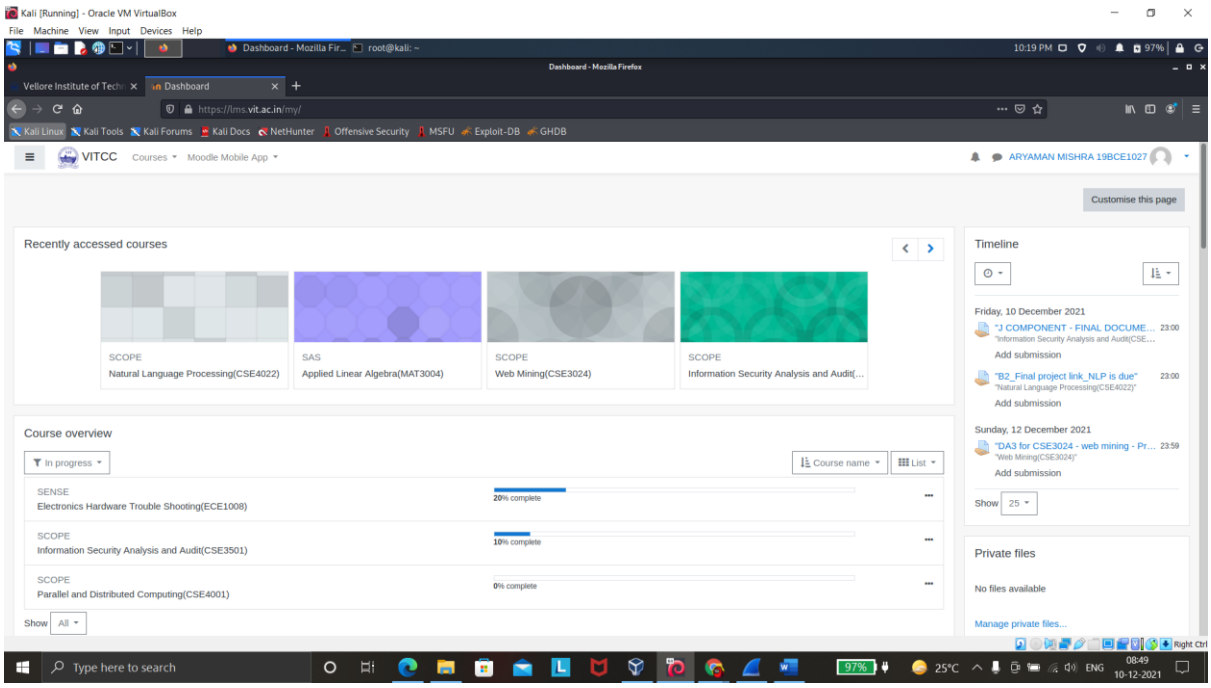
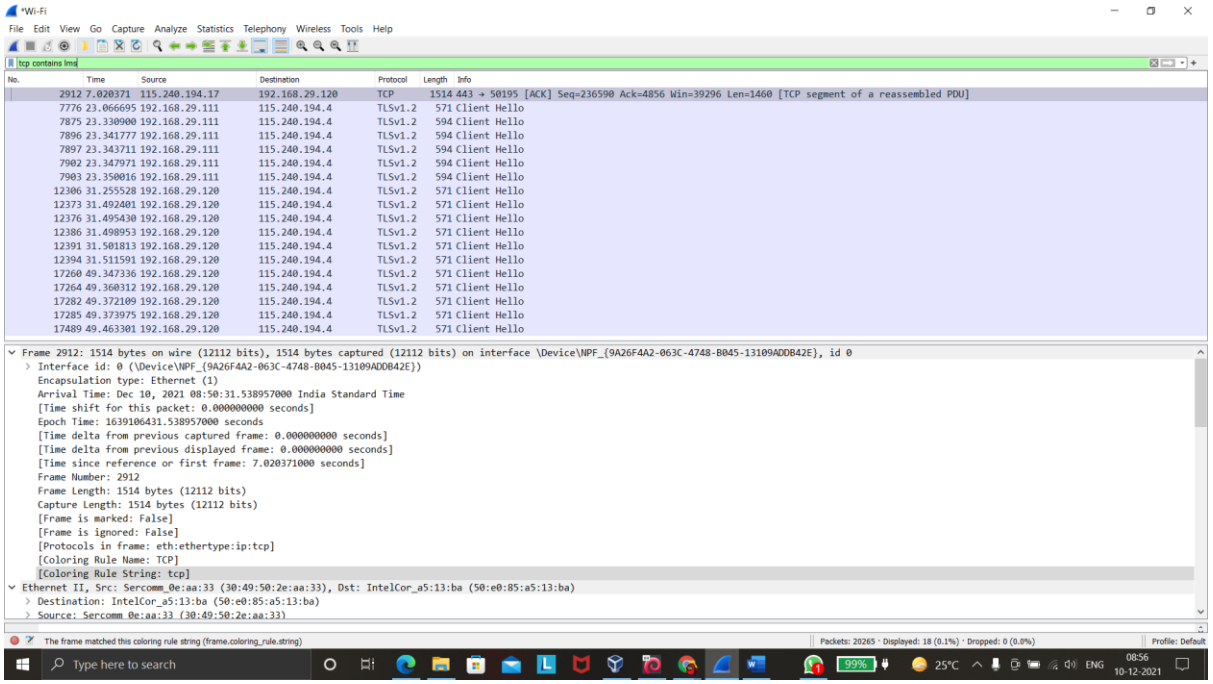
ARYAMAN MISHRA

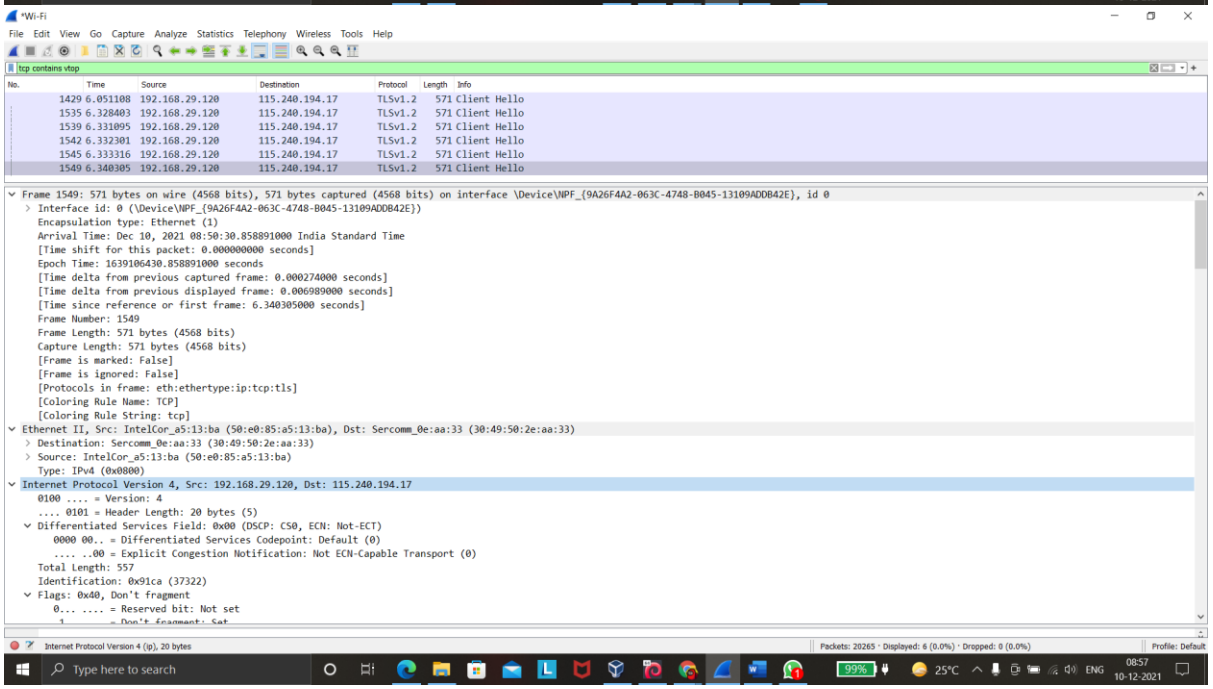
19BCE1027

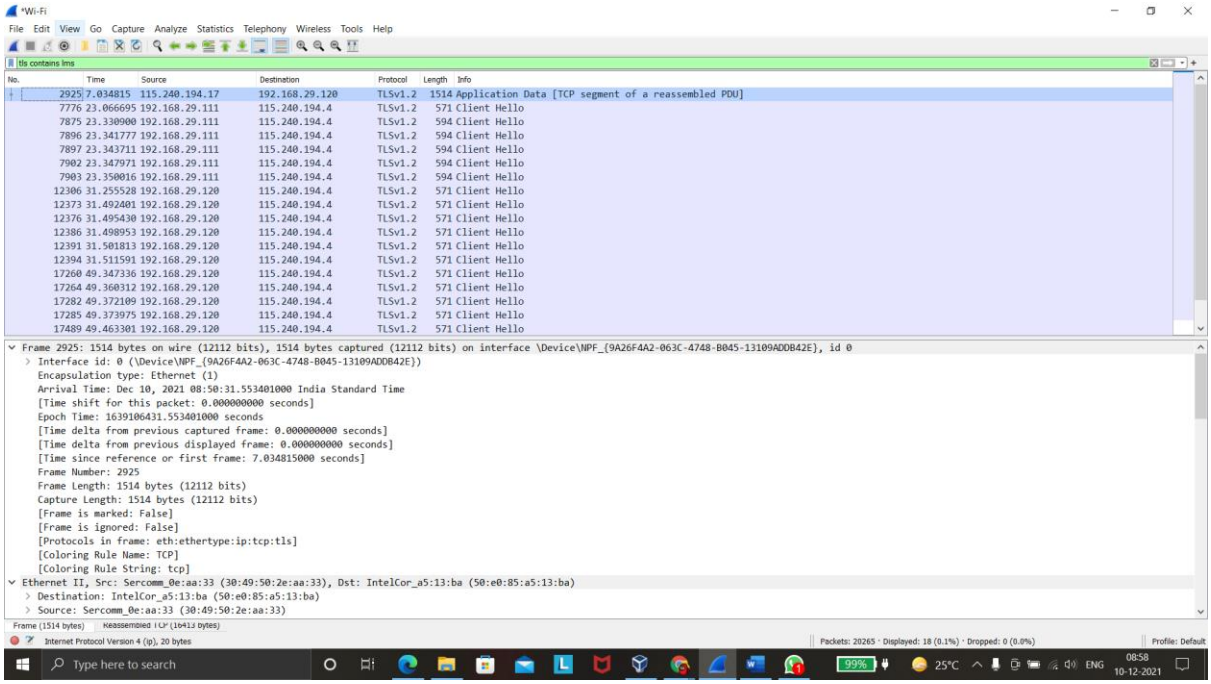
Enter into MOODLE and VTOP applications using the necessary login credentials and identify the user names and passwords of the two applications in the trace files of Wireshark. Display the screenshots that are showing the usernames and passwords in the trace and the respective ASCII codes as well.






*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp contains lms
No. Time Source Destination Protocol Length Info
2912 7.020371 115.240.194.17 192.168.29.120 TCP 1514 443 → 50195 [ACK] Seq=236590 Ack=4856 Win=39296 Len=1460 [TCP segment of a reassembled PDU]
7776 23.066695 192.168.29.111 115.240.194.4 TLSv1.2 571 Client Hello
7875 23.330900 192.168.29.111 115.240.194.4 TLSv1.2 594 Client Hello
7896 23.341777 192.168.29.111 115.240.194.4 TLSv1.2 594 Client Hello
7897 23.343711 192.168.29.111 115.240.194.4 TLSv1.2 594 Client Hello
7902 23.347971 192.168.29.111 115.240.194.4 TLSv1.2 594 Client Hello
7903 23.350016 192.168.29.111 115.240.194.4 TLSv1.2 594 Client Hello
12306 31.255528 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
12373 31.492401 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
12376 31.495430 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
12386 31.498953 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
12391 31.501813 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
12394 31.511591 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
17260 49.347336 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
17264 49.360312 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
17282 49.372109 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
17285 49.373975 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
17489 49.463301 192.168.29.120 115.240.194.4 TLSv1.2 571 Client Hello
Frame 2912: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E})
Encapsulation type: Ethernet (1)
Arrival Time: Dec 10, 2021 08:50:31.538957000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1639106431.538957000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 7.020371000 seconds]
Frame Number: 2912
Frame Length: 1514 bytes (12112 bits)
Capture Length: 1514 bytes (12112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Sercomm_0e:aa:33 (30:49:50:2e:aa:33), Dst: IntelCor_a5:13:ba (50:e0:85:a5:13:ba)
Destination: IntelCor_a5:13:ba (50:e0:85:a5:13:ba)
Source: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)
The frame matched this coloring rule string (frame.coloring_rule.string)
Packets: 20265 · Displayed: 18 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
99%
25°C
ENG
08:56
10-12-2021

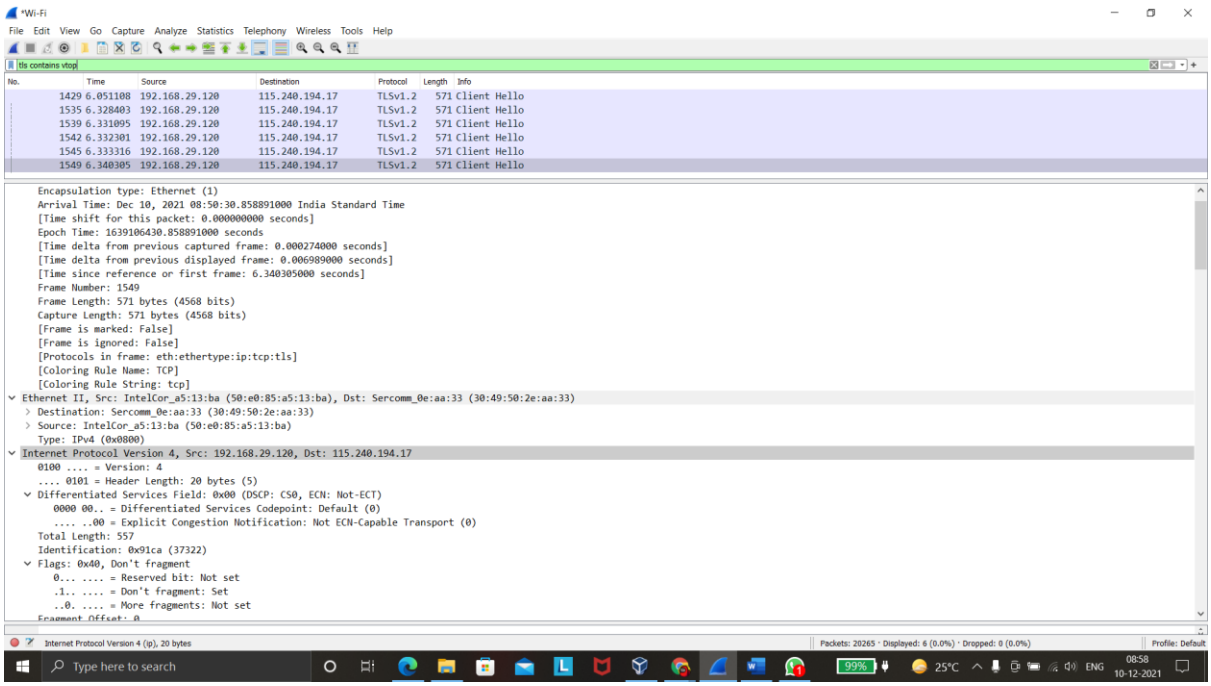

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp contains vtop
No. Time Source Destination Protocol Length Info
1429 6.051108 192.168.29.120 115.240.194.17 TLSv1.2 571 Client Hello
1535 6.328403 192.168.29.120 115.240.194.17 TLSv1.2 571 Client Hello
1539 6.331095 192.168.29.120 115.240.194.17 TLSv1.2 571 Client Hello
1542 6.332301 192.168.29.120 115.240.194.17 TLSv1.2 571 Client Hello
1545 6.333316 192.168.29.120 115.240.194.17 TLSv1.2 571 Client Hello
1549 6.340305 192.168.29.120 115.240.194.17 TLSv1.2 571 Client Hello
Frame 1549: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E}, id 0
Interface id: 0 (\Device\NPF_{9A26F4A2-063C-4748-B045-13109ADDB42E})
Encapsulation type: Ethernet (1)
Arrival Time: Dec 10, 2021 08:50:30.858891000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1639106430.858891000 seconds
[Time delta from previous captured frame: 0.000274000 seconds]
[Time delta from previous displayed frame: 0.006989000 seconds]
[Time since reference or first frame: 6.340305000 seconds]
Frame Number: 1549
Frame Length: 571 bytes (4568 bits)
Capture Length: 571 bytes (4568 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:tls]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: IntelCor_a5:13:ba (50:e0:85:a5:13:ba), Dst: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)
Destination: Sercomm_0e:aa:33 (30:49:50:2e:aa:33)
Source: IntelCor_a5:13:ba (50:e0:85:a5:13:ba)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.29.120, Dst: 115.240.194.17
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 557
Identification: 0x91ca (37322)
Flags: 0x40, Don't fragment
0... .... = Reserved bit: Not set
Internet Protocol Version 4 (ip), 20 bytes
Packets: 20265 · Displayed: 6 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
99%
25°C
ENG
08:57
10-12-2021



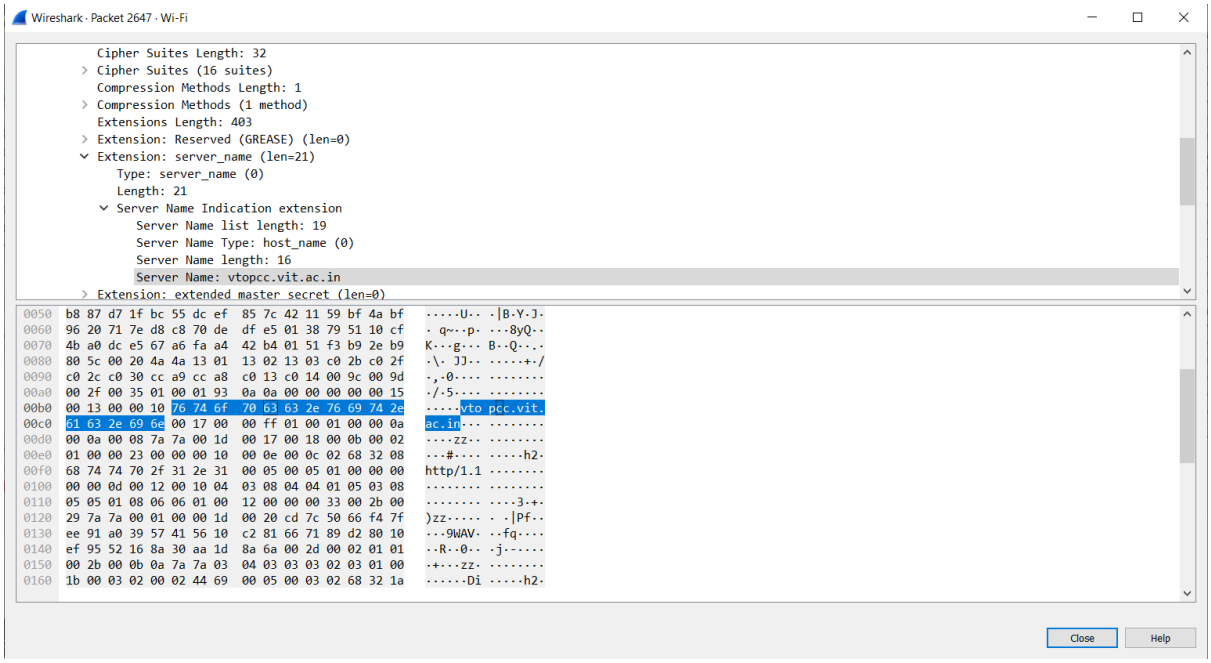
Open ***Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap*** in Wireshark. Use a basic web filter as described in this previous [tutorial about Wireshark filters](). Our basic filter for Wireshark 3.x is:

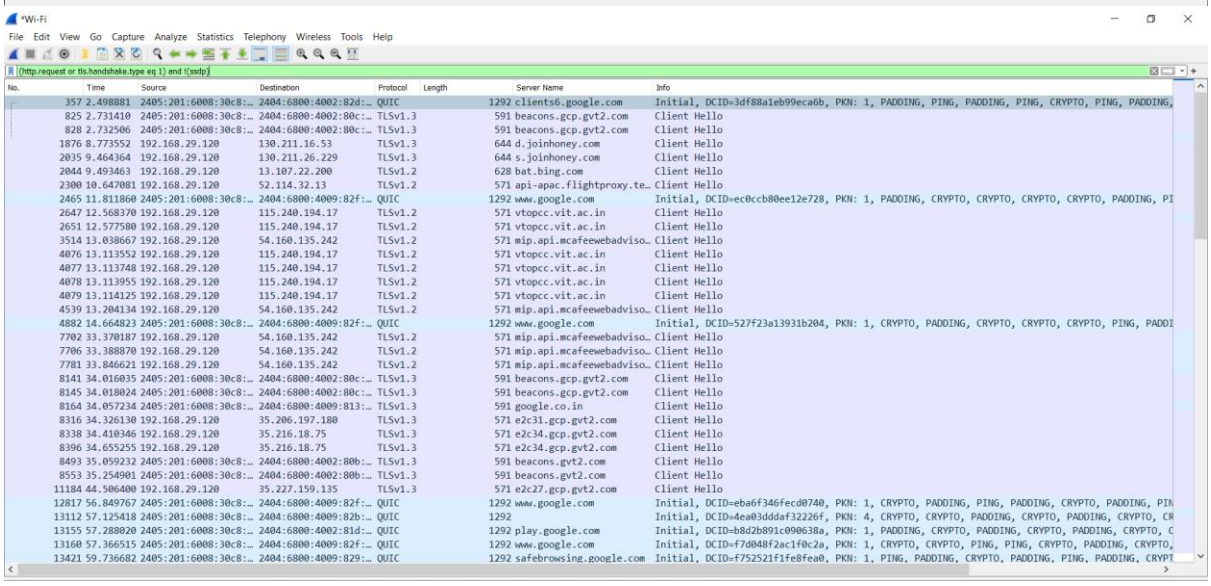
```
(http.request or tls.handshake.type eq 1) and !(ssdp)
```

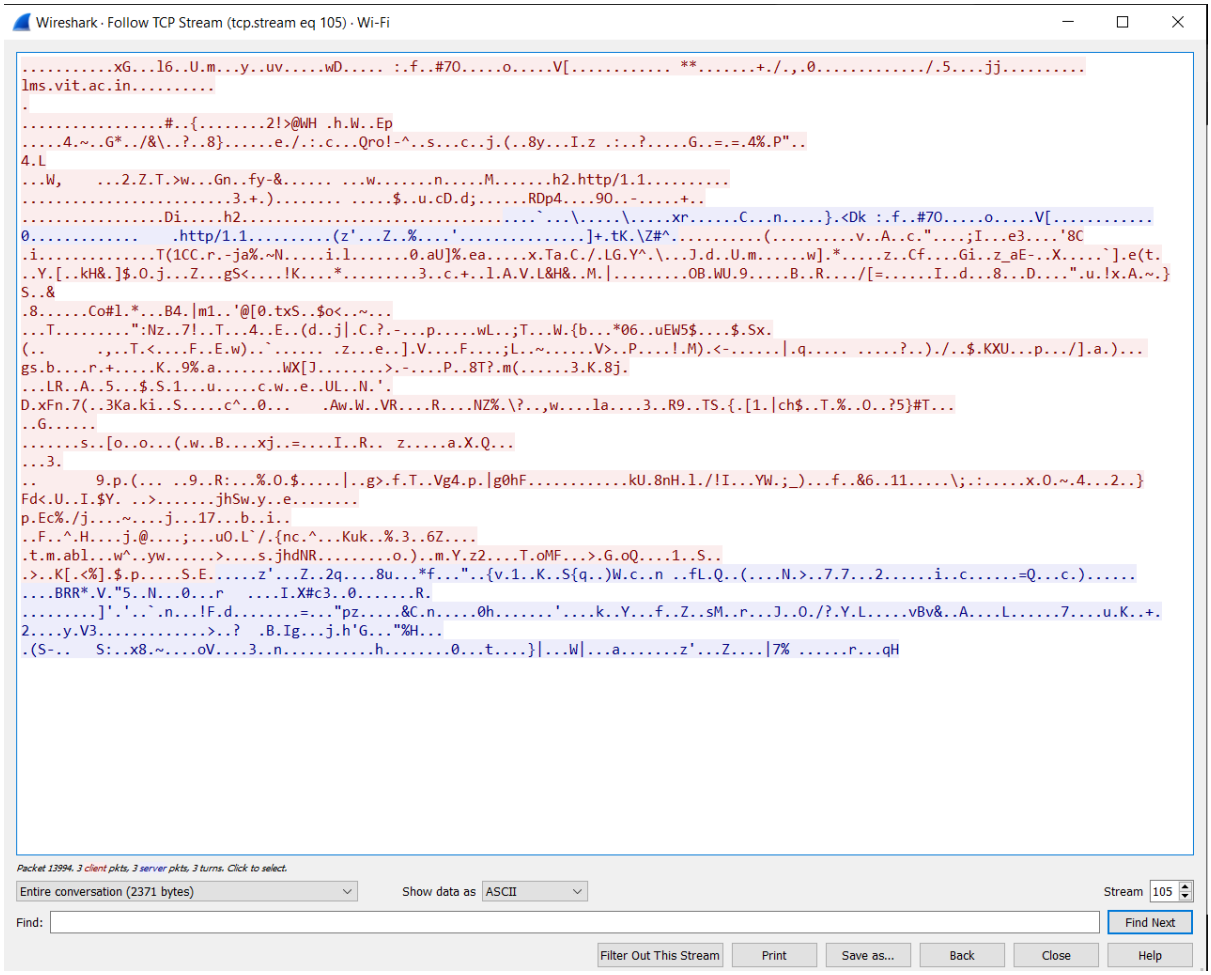
Open ***Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap*** in Wireshark. Then use the menu path ***Edit --> Preferences*** to bring up the Preferences Menu

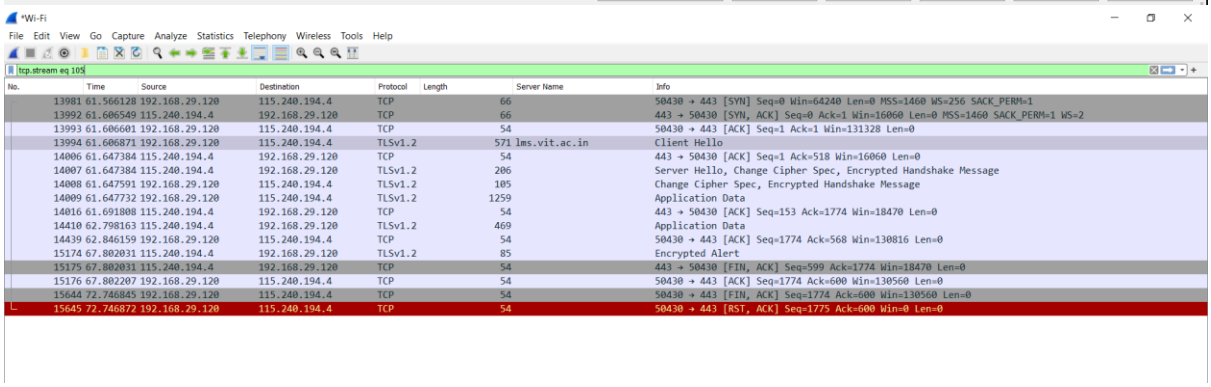


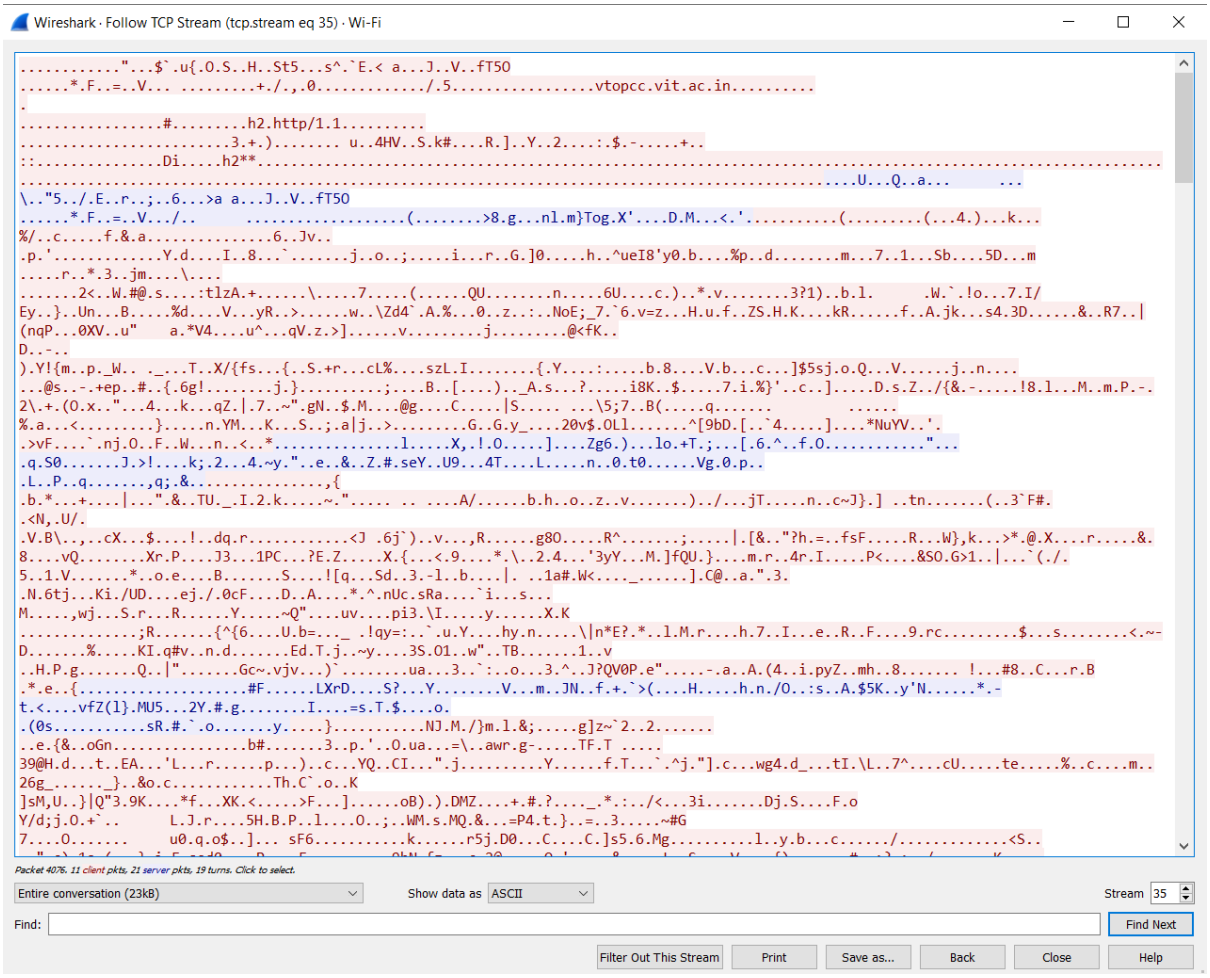
Once you have clicked “OK,” when using the basic filter, your Wireshark column display will list the decrypted HTTP requests under each of the HTTPS lines






Wireshark · Follow TCP Stream (tcp.stream eq 105) · Wi-Fi
lms.vit.ac.in
Packet 13994. 3 client pkts, 3 server pkts, 3 turns. Click to select.
Entire conversation (2371 bytes)
Show data as ASCII
Stream 105
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 105
No. Time Source Destination Protocol Length Server Name Info
13981 61.566128 192.168.29.120 115.240.194.4 TCP 66 50430 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13992 61.606549 115.240.194.4 192.168.29.120 TCP 66 443 → 50430 [SYN, ACK] Seq=0 Ack=1 Win=16060 Len=0 MSS=1460 SACK_PERM=1 WS=2
13993 61.606601 192.168.29.120 115.240.194.4 TCP 54 50430 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
13994 61.606871 192.168.29.120 115.240.194.4 TLSv1.2 571 lms.vit.ac.in Client Hello
14006 61.647384 115.240.194.4 192.168.29.120 TCP 54 443 → 50430 [ACK] Seq=1 Ack=518 Win=16060 Len=0
14007 61.647384 115.240.194.4 192.168.29.120 TLSv1.2 206 Server Hello, Change Cipher Spec, Encrypted Handshake Message
14008 61.647591 192.168.29.120 115.240.194.4 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
14009 61.647732 192.168.29.120 115.240.194.4 TLSv1.2 1259 Application Data
14016 61.691808 115.240.194.4 192.168.29.120 TCP 54 443 → 50430 [ACK] Seq=153 Ack=1774 Win=18470 Len=0
14410 62.798163 115.240.194.4 192.168.29.120 TLSv1.2 469 Application Data
14439 62.846159 192.168.29.120 115.240.194.4 TCP 54 50430 → 443 [ACK] Seq=1774 Ack=568 Win=130816 Len=0
15174 67.802031 115.240.194.4 192.168.29.120 TLSv1.2 85 Encrypted Alert
15175 67.802031 115.240.194.4 192.168.29.120 TCP 54 443 → 50430 [FIN, ACK] Seq=599 Ack=1774 Win=18470 Len=0
15176 67.802207 192.168.29.120 115.240.194.4 TCP 54 50430 → 443 [ACK] Seq=1774 Ack=600 Win=130560 Len=0
15644 72.746845 192.168.29.120 115.240.194.4 TCP 54 50430 → 443 [FIN, ACK] Seq=1774 Ack=600 Win=130560 Len=0
15645 72.746872 192.168.29.120 115.240.194.4 TCP 54 50430 → 443 [RST, ACK] Seq=1775 Ack=600 Win=0 Len=0



SHA Values for Passwords are

31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f

29!-!.

0d5ad14787be9df27b50dd7b99279b1b64c8bffd752e19a485d189467191bdca

Y|!B