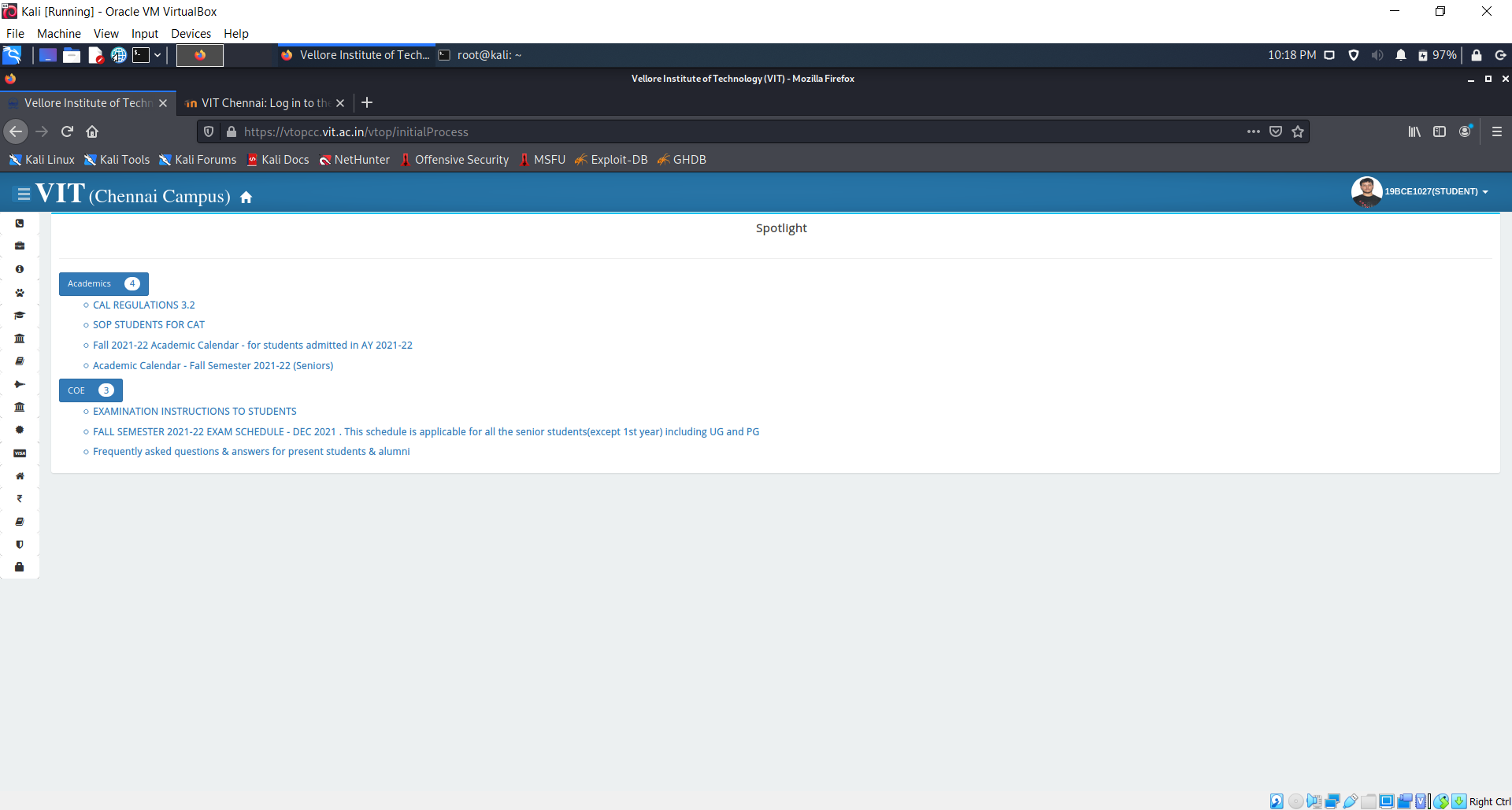
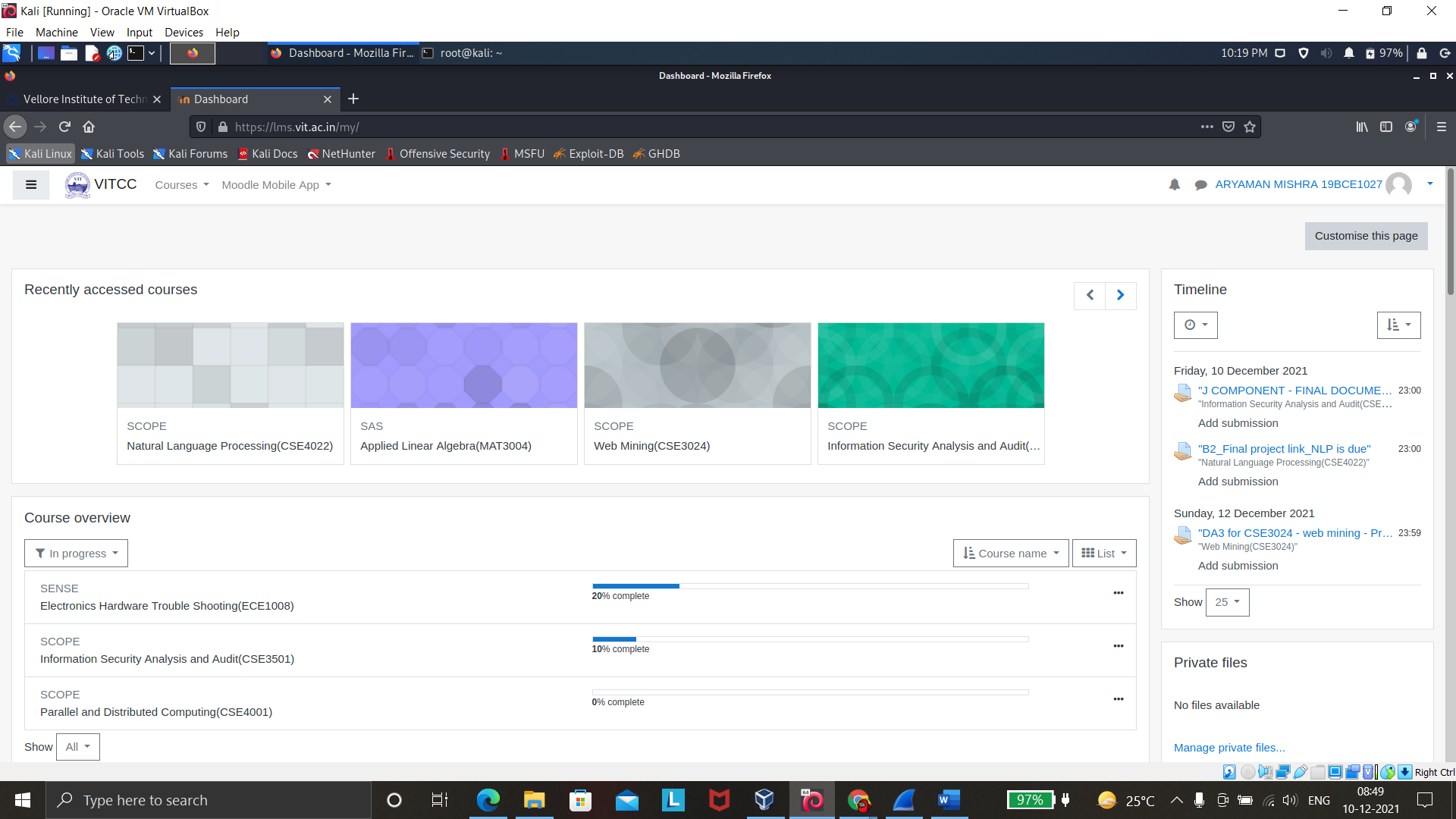
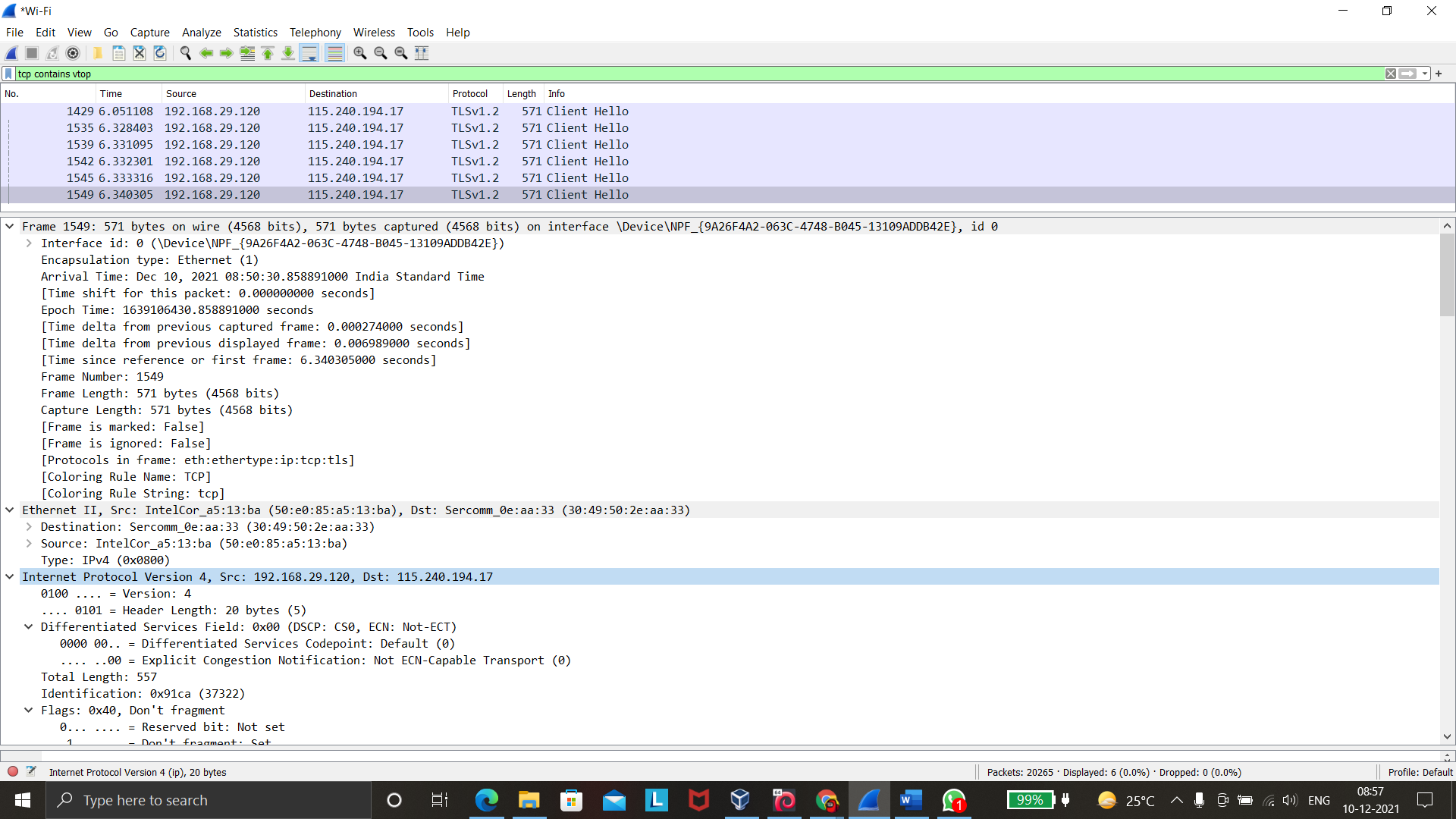
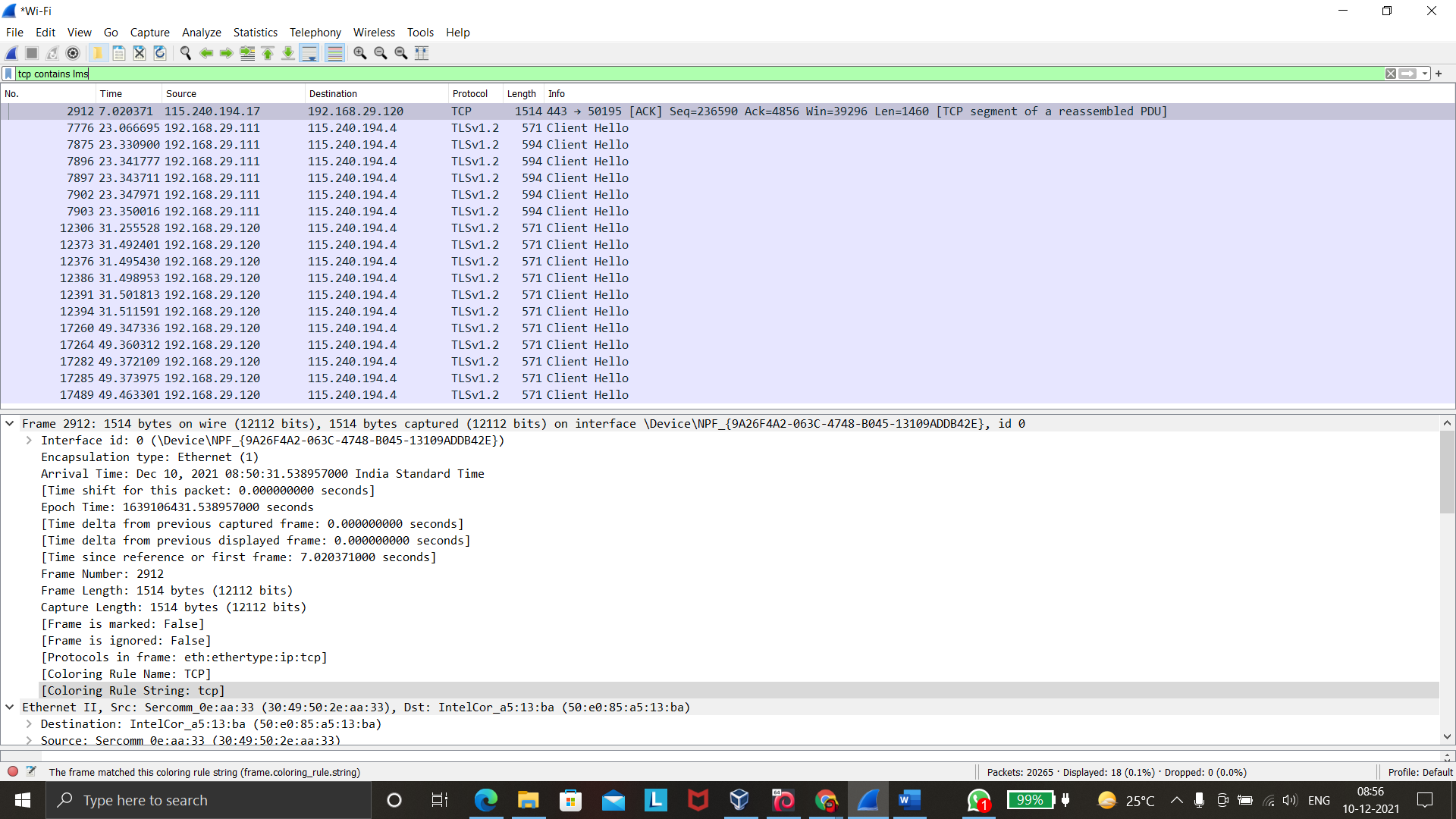
ARYAMAN MISHRA

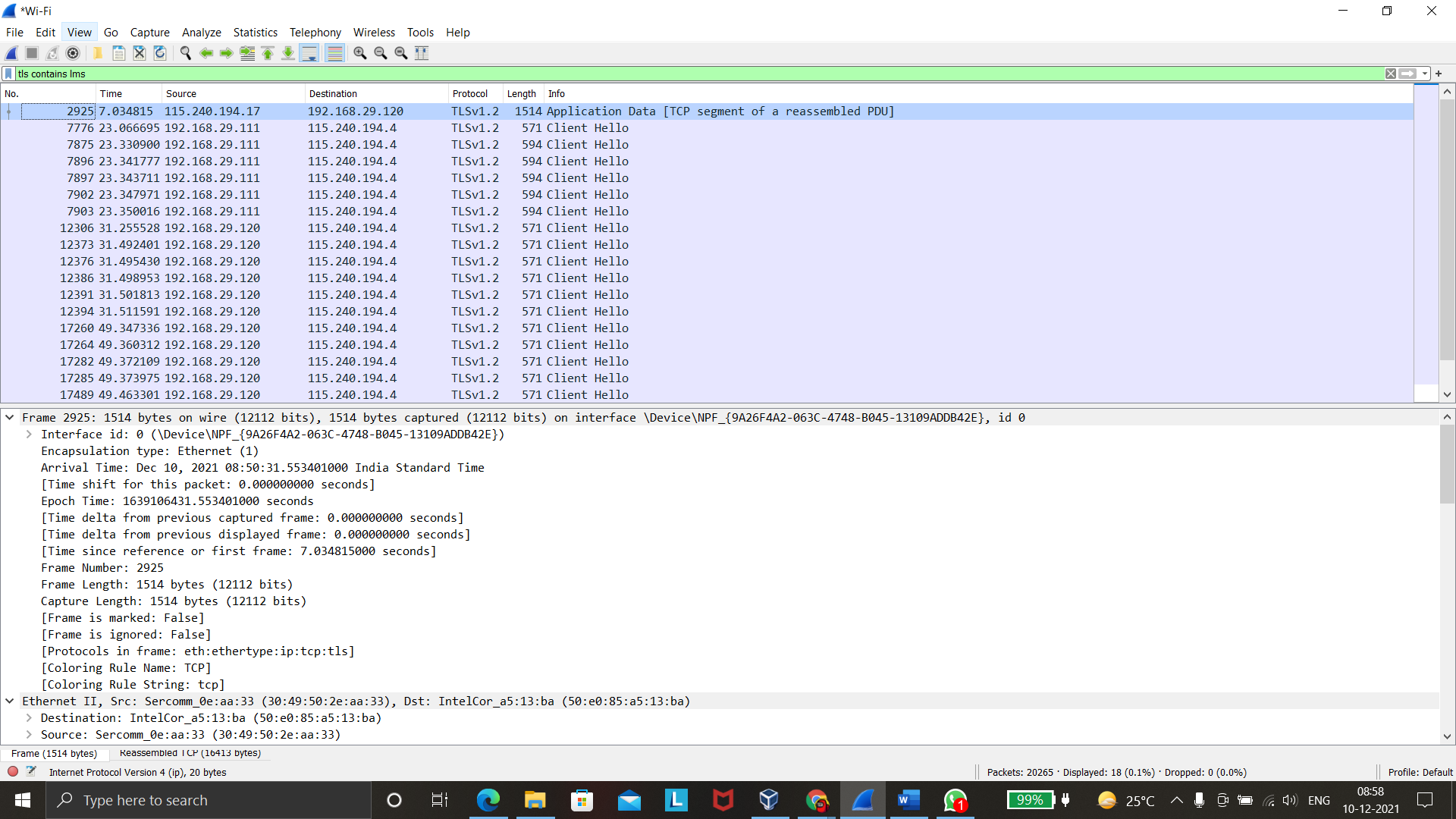
19BCE1027

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.





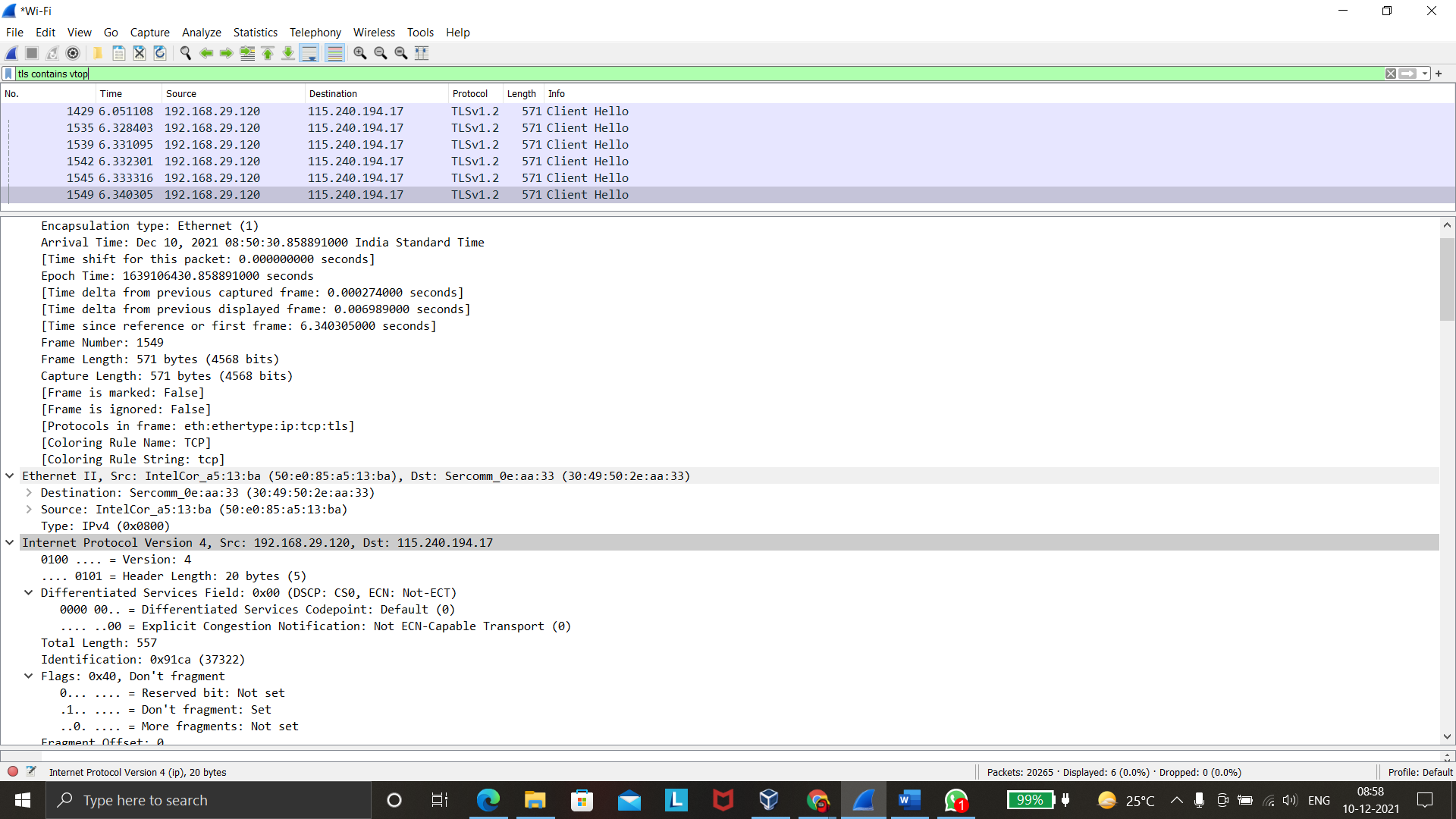


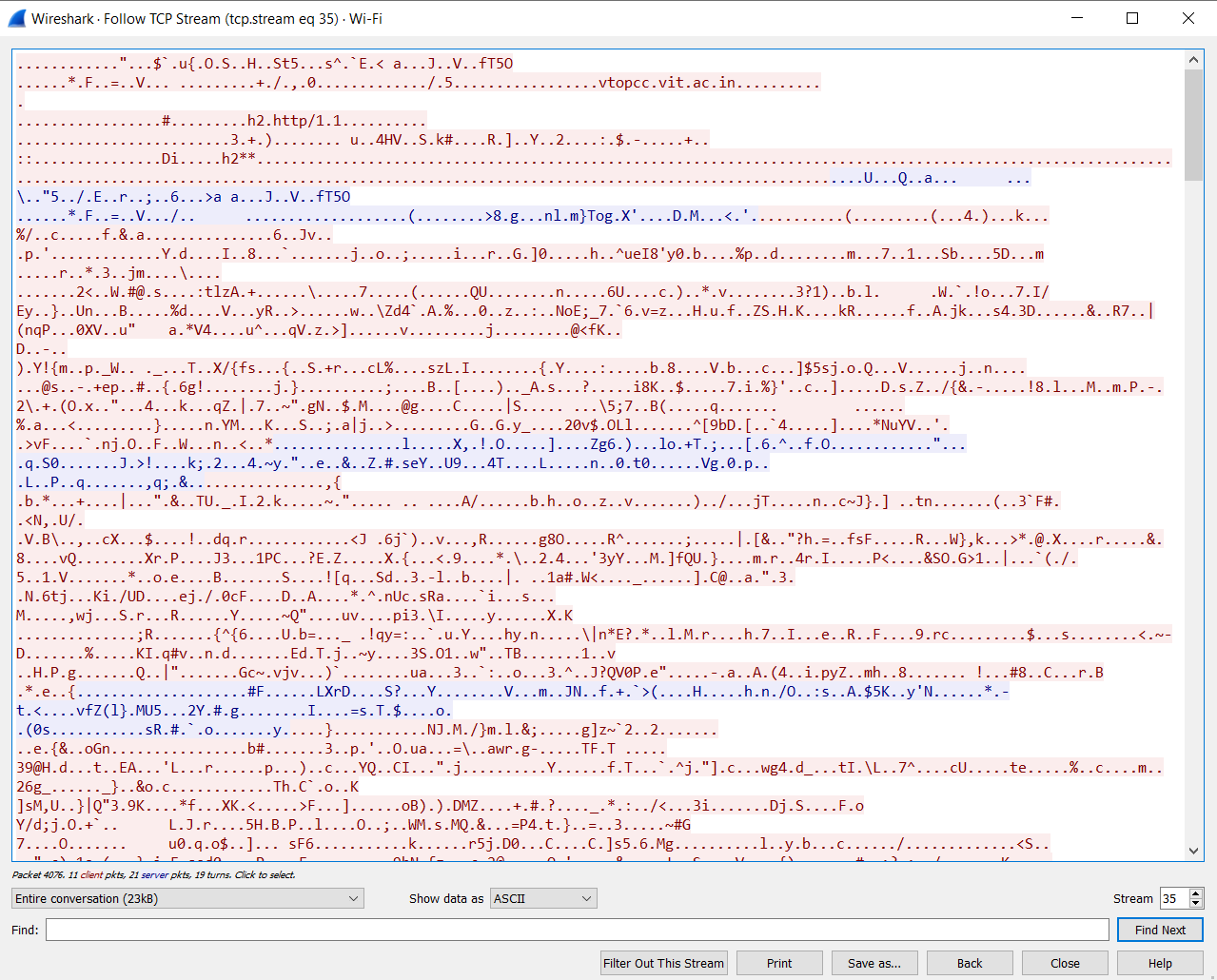
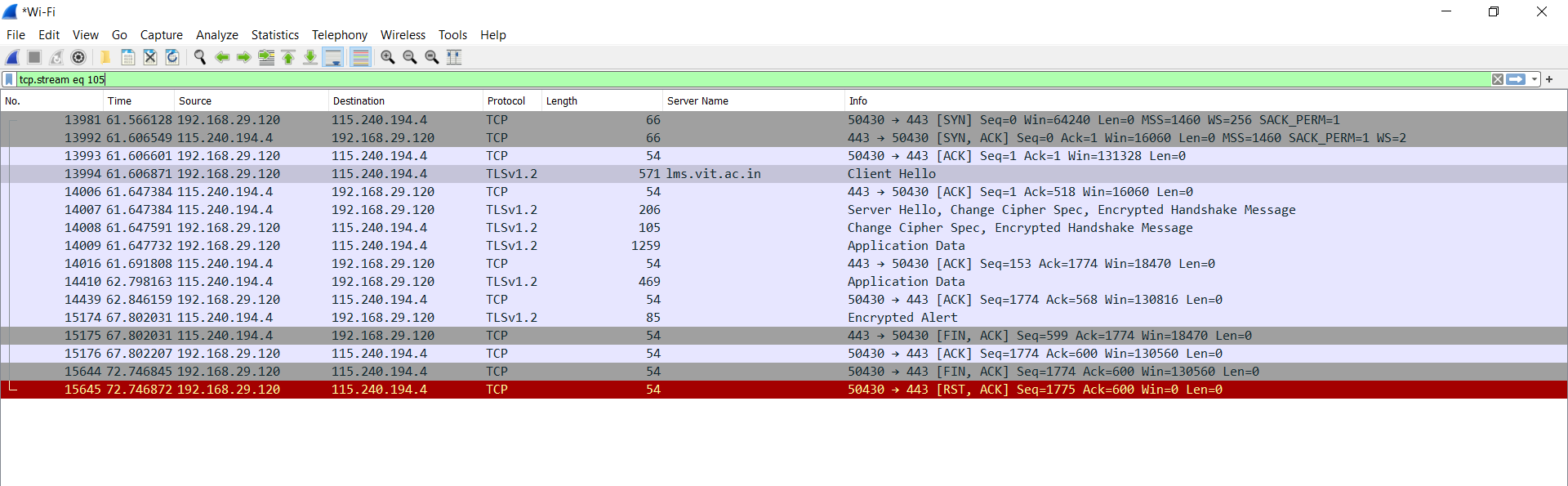
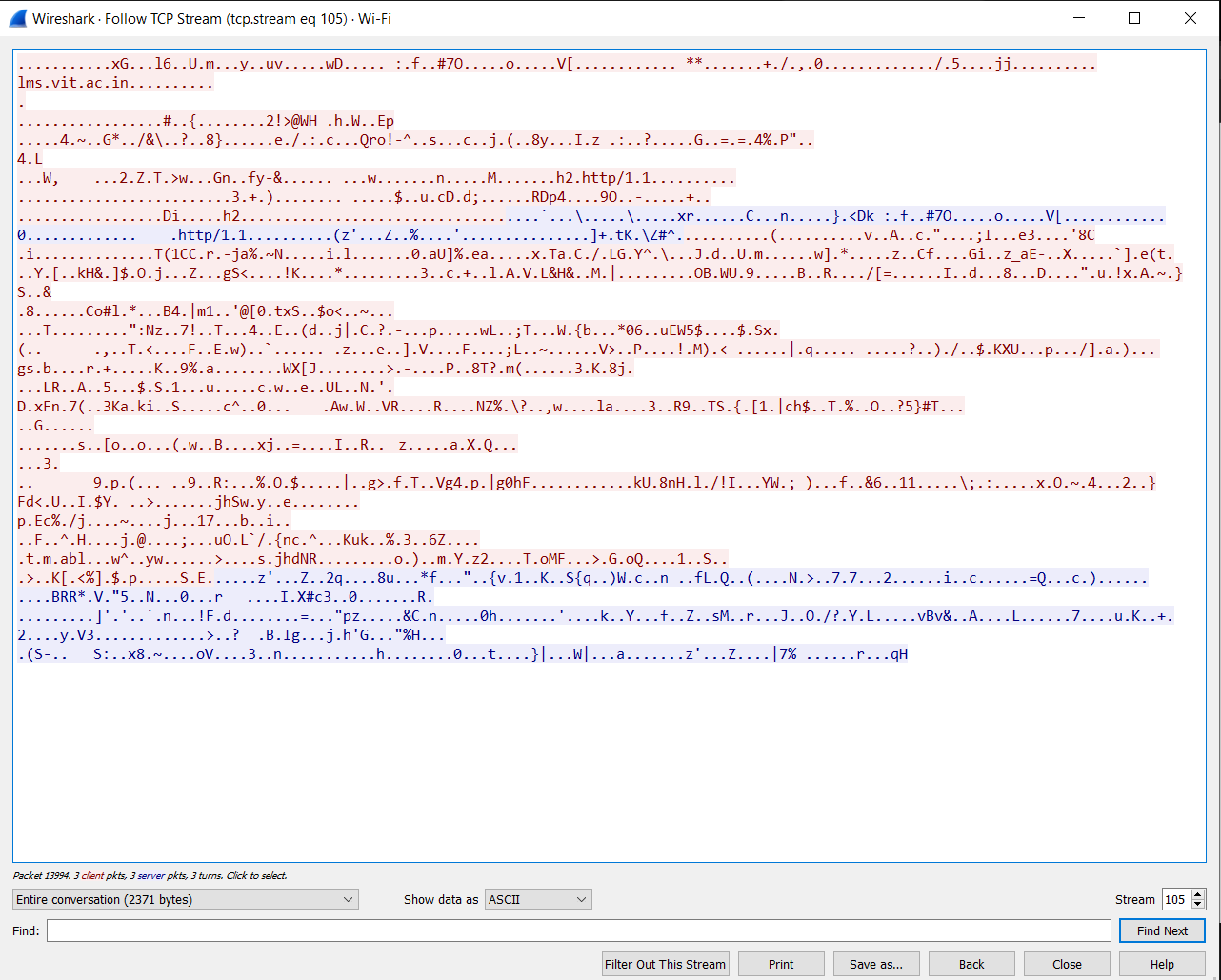
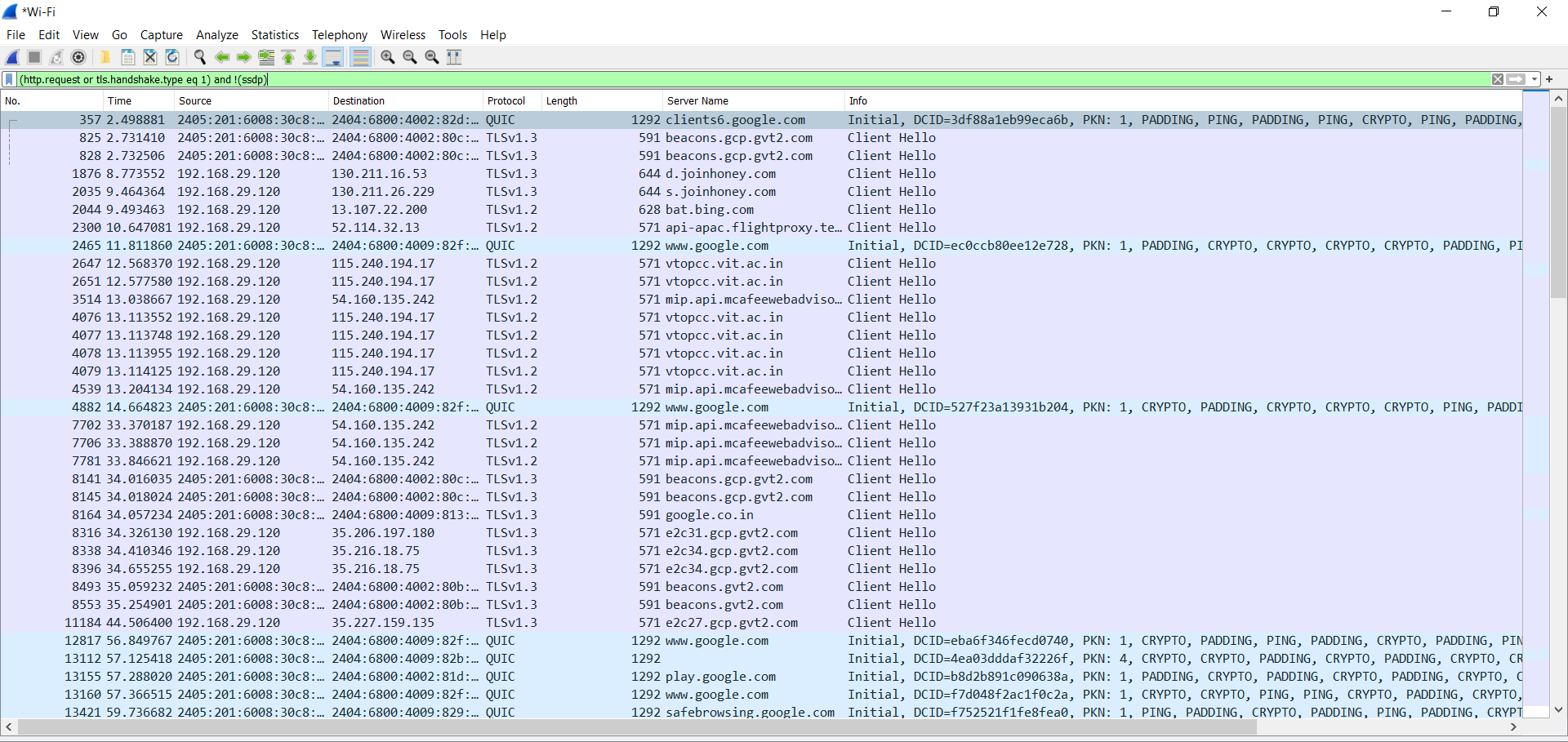
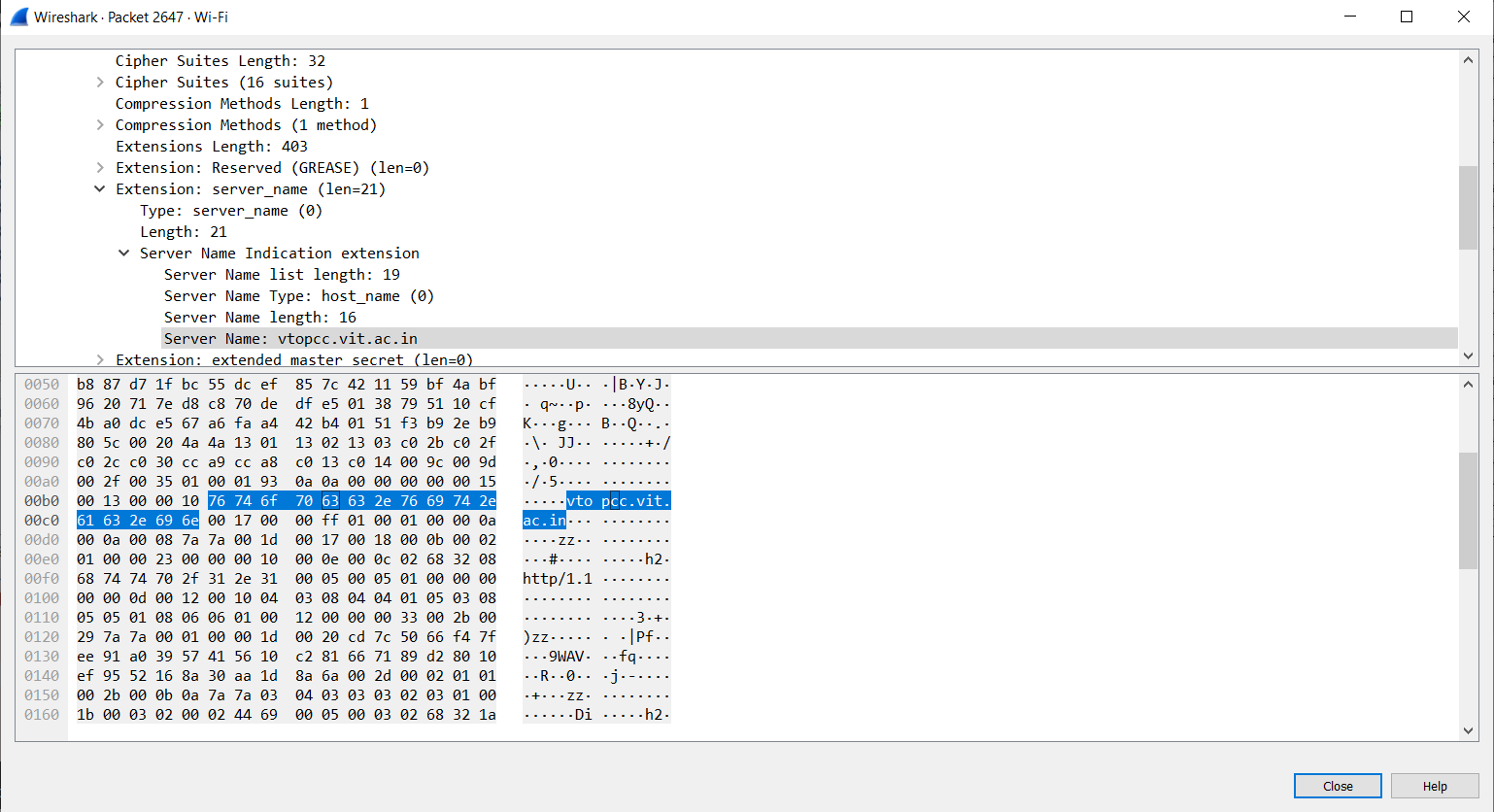


Open **Wireshark-tutorial-on-decrypting-HTTPS-SSL-TLS-traffic.pcap** in Wireshark. Use a basic web filter as described in this previous [tutorial about Wireshark filters](https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/). Our basic filter for Wireshark 3.x is:

(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

SHA Values for Passwords are

31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f

29!-!.

0d5ad14787be9df27b50dd7b99279b1b64c8bffd752e19a485d189467191bdca

Y|!B