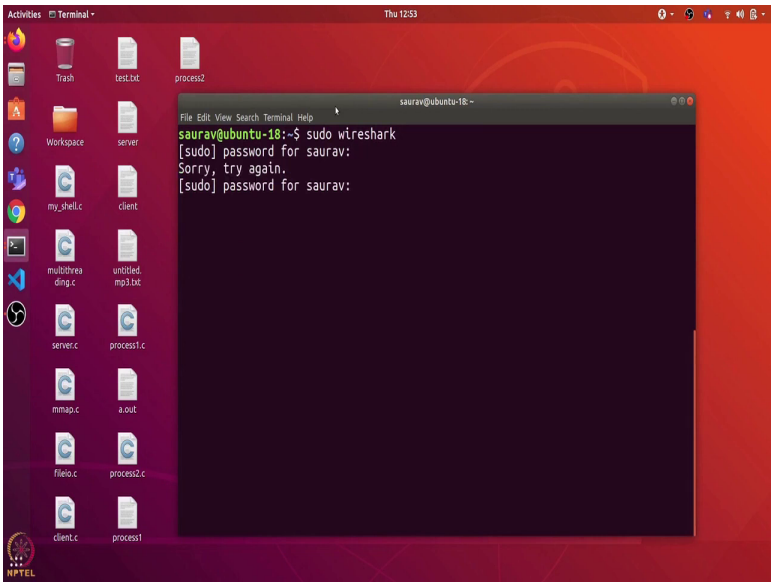
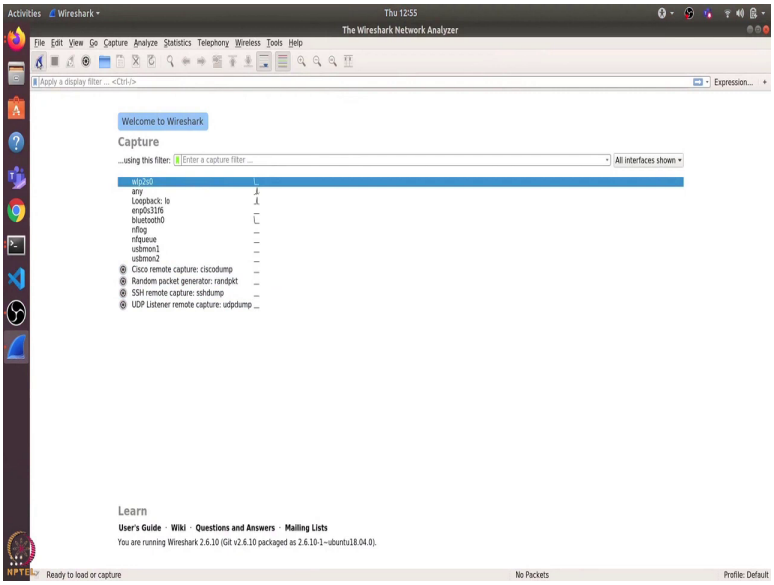
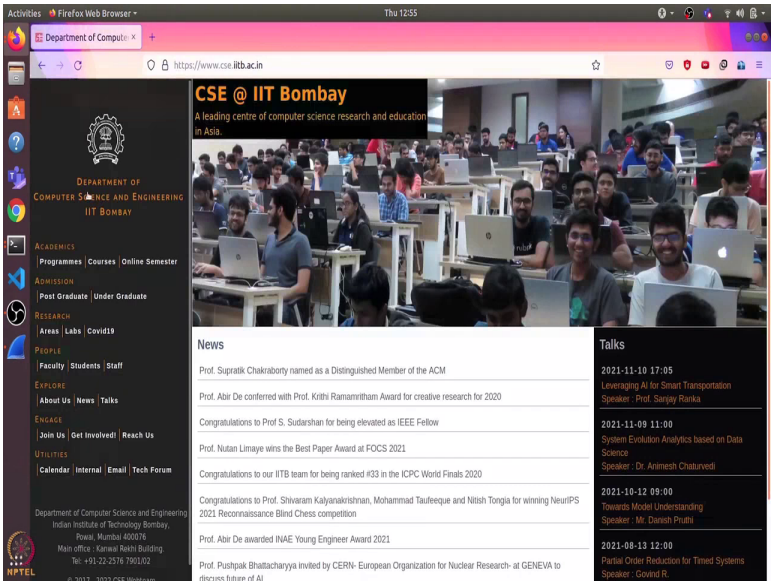
Design Engineering of Computer Systems
Professor. Mythili Vutukuru
Computer Science and Engineering
Indian Institute of Technology, Bombay
Lecture 37 (Week 5, Tutorial 2)
Learning Wireshark

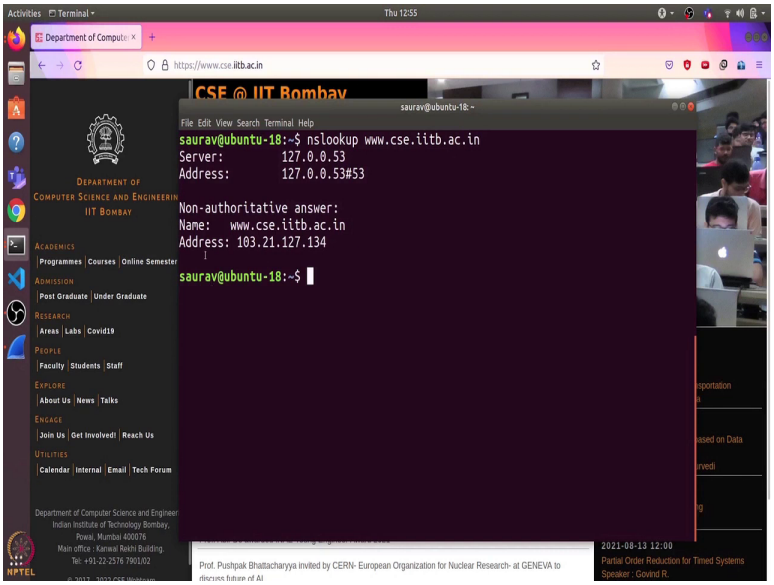
Hi, everyone. In this video, we will learn about Wireshark. Wireshark is a very useful utility which helps us to capture all the network packets which are passing through an interface cards on our computer.

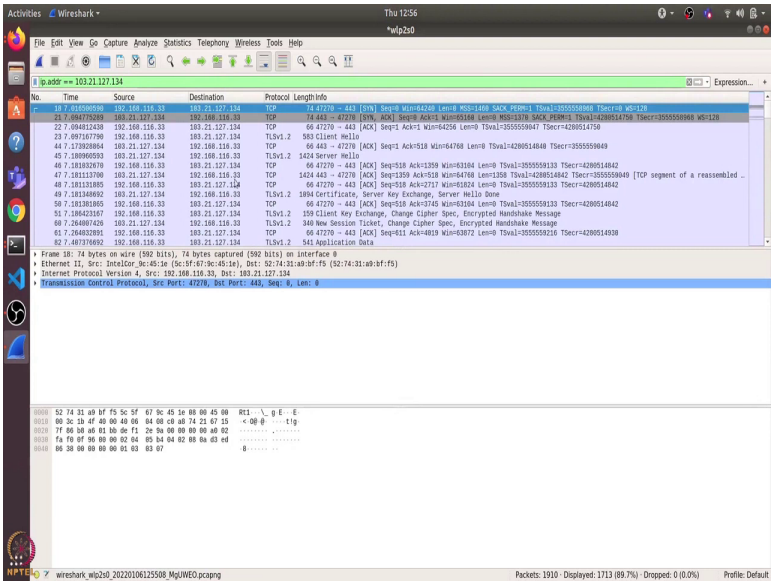
(Refer Slide Time: 00:29)

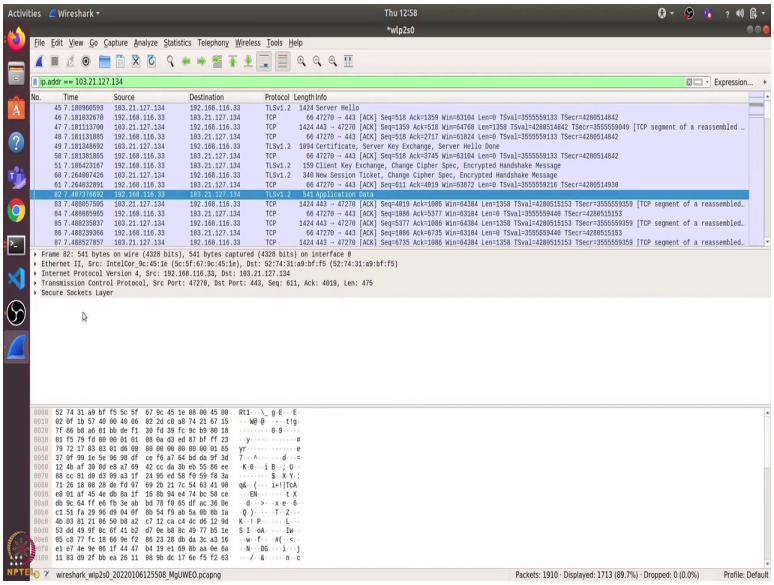


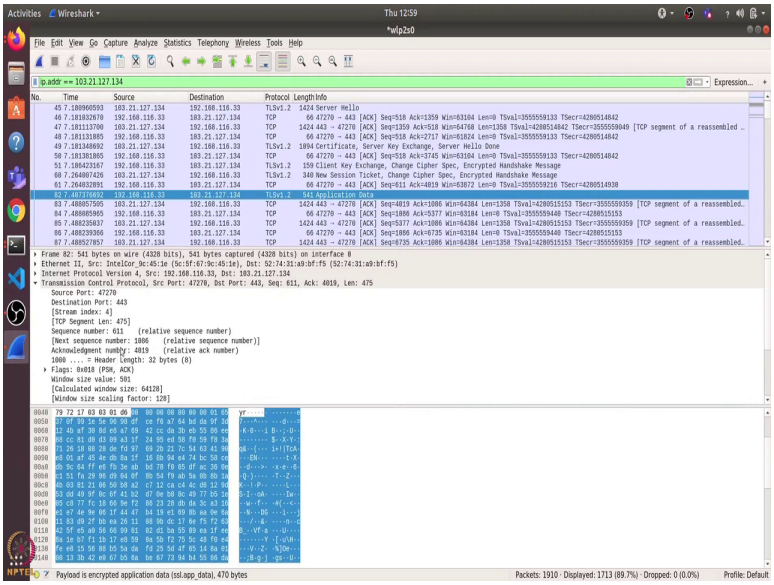



Activities
Firefox Web Browser
Thu 12:55
Department of Compute
https://www.cse.iitb.ac.in
CSE @ IIT Bombay
A leading centre of computer science research and education in Asia.
Department of Computer Science and Engineering IIT Bombay
Academics
Programmes | Courses | Online Semester
Admission
Post Graduate | Under Graduate
Research
Areas | Labs | Covid19
People
Faculty | Students | Staff
Explore
About Us | News | Talks
Engage
Join Us | Get Involved! | Reach Us
Utilities
Calendar | Internal | Email | Tech Forum
Department of Computer Science and Engineering
Indian Institute of Technology Bombay,
Powai, Mumbai 400076
Main office : Kanwal Rekhi Building.
Tel: +91-22-2576 7901/02
News
Prof. Supratik Chakraborty named as a Distinguished Member of the ACM
Prof. Abir De conferred with Prof. Krithi Ramamritham Award for creative research for 2020
Congratulations to Prof S. Sudarshan for being elevated as IEEE Fellow
Prof. Nutan Limaye wins the Best Paper Award at FOCS 2021
Congratulations to our IITB team for being ranked #33 in the ICPC World Finals 2020
Congratulations to Prof. Shivaram Kalyanakrishnan, Mohammad Taufeeque and Nitish Tongia for winning NeurIPS 2021 Reconnaissance Blind Chess competition
Prof. Abir De awarded INAE Young Engineer Award 2021
Prof. Pushpak Bhattacharyya invited by CERN- European Organization for Nuclear Research- at GENEVA to
Talks
2021-11-10 17:05
Leveraging AI for Smart Transportation
Speaker : Prof. Sanjay Ranka
2021-11-09 11:00
System Evolution Analytics based on Data Science
Speaker : Dr. Animesh Chaturvedi
2021-10-12 09:00
Towards Model Understanding
Speaker : Mr. Danish Pruthi
2021-08-13 12:00
Partial Order Reduction for Timed Systems
Speaker : Govind R.


Activities
Terminal
Thu 12:55
Department of Compute
https://www.cse.iitb.ac.in
saurav@ubuntu-18: ~
File Edit View Search Terminal Help
saurav@ubuntu-18:~$ nslookup www.cse.iitb.ac.in
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
Name: www.cse.iitb.ac.in
Address: 103.21.127.134
saurav@ubuntu-18:~$
Department of Computer Science and Engineering IIT Bombay
Academics
Programmes | Courses | Online Semester
Admission
Post Graduate | Under Graduate
Research
Areas | Labs | Covid19
People
Faculty | Students | Staff
Explore
About Us | News | Talks
Engage
Join Us | Get Involved! | Reach Us
Utilities
Calendar | Internal | Email | Tech Forum
Department of Computer Science and Engineer
Indian Institute of Technology Bombay,
Powai, Mumbai 400076
Main office : Kanwal Rekhi Building.
Tel: +91-22-2576 7901/02
Prof. Pushpak Bhattacharyya invited by CERN- European Organization for Nuclear Research- at GENEVA to
2021-08-13 12:00
Partial Order Reduction for Timed Systems
Speaker : Govind R.


Activities
Wireshark
Thu 12:56
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 103.21.127.134
Expression...
No. Time Source Destination Protocol Length Info
10 7.016590590 192.168.116.33 103.21.127.134 TCP 74 47270 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3555558060 TSecr=0 WS=128
11 7.094775298 103.21.127.134 192.168.116.33 TCP 74 443 → 47270 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1370 SACK_PERM=1 TSval=4208514750 TSecr=3555558060 WS=128
22 7.094912430 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3555559047 TSecr=4208514750
23 7.097167790 192.168.116.33 103.21.127.134 TLSv1.2 583 Client Hello
44 7.173928864 103.21.127.134 192.168.116.33 TCP 66 443 → 47270 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=4208514848 TSecr=3555559049
45 7.180960593 103.21.127.134 192.168.116.33 TLSv1.2 1424 Server Hello
46 7.181032670 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=518 Ack=1359 Win=63104 Len=0 TSval=3555559133 TSecr=4208514842
47 7.181113700 103.21.127.134 192.168.116.33 TCP 1424 443 → 47270 [ACK] Seq=1359 Ack=518 Win=64768 Len=1358 TSval=4208514842 TSecr=3555558949 [TCP segment of a reassembled …
48 7.181131885 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=518 Ack=2717 Win=61824 Len=0 TSval=3555559133 TSecr=4208514842
49 7.181348692 103.21.127.134 192.168.116.33 TLSv1.2 1094 Certificate, Server Key Exchange, Server Hello Done
50 7.181381865 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=518 Ack=3745 Win=63104 Len=0 TSval=3555559133 TSecr=4208514842
51 7.180422167 192.168.116.33 103.21.127.134 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60 7.264007426 103.21.127.134 192.168.116.33 TLSv1.2 340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
61 7.264032891 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=611 Ack=4019 Win=63872 Len=0 TSval=3555559216 TSecr=4208514930
82 7.467376692 192.168.116.33 103.21.127.134 TLSv1.2 541 Application Data
Frame 10: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: IntelCor_9c:45:1e (5c:5f:67:9c:45:1e), Dst: 52:74:31:a9:bf:f5 (52:74:31:a9:bf:f5)
Internet Protocol Version 4, Src: 192.168.116.33, Dst: 103.21.127.134
Transmission Control Protocol, Src Port: 47270, Dst Port: 443, Seq: 0, Len: 0
0000 52 74 31 a9 bf f5 5c 5f 67 9c 45 1e 08 00 45 00 Rt1···_ g·E···E·
0010 00 3c 1b 6f a0 00 40 06 84 08 c0 a8 74 21 67 15 ·<·o··@· ····t!g·
0020 7f 86 b8 a6 01 bb de f1 2e 9a 00 00 00 00 a0 02 ···· ···· ····
0030 fa f0 0f 96 00 00 02 04 05 b4 04 02 08 0a d3 ed ···· ···· ····
0040 86 38 00 00 00 00 01 03 03 07 ·8·· ····
wireshark_wlp2s0_20220106125508_MgUWEO.pcapng
Packets: 1910 · Displayed: 1713 (89.7%) · Dropped: 0 (0.0%)
Profile: Default


Activities
Wireshark
Thu 12:58
*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 103.21.127.134
Expression...
No. Time Source Destination Protocol Length Info
45 7.180960593 103.21.127.134 192.168.116.33 TLSv1.2 1424 Server Hello
46 7.181032670 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=518 Ack=1359 Win=63104 Len=0 TSval=3555559133 TSecr=4208514842
47 7.181113700 103.21.127.134 192.168.116.33 TCP 1424 443 → 47270 [ACK] Seq=1359 Ack=518 Win=64768 Len=1358 TSval=4208514842 TSecr=3555558949 [TCP segment of a reassembled …
48 7.181131885 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=518 Ack=2717 Win=61824 Len=0 TSval=3555559133 TSecr=4208514842
49 7.181348692 103.21.127.134 192.168.116.33 TLSv1.2 1094 Certificate, Server Key Exchange, Server Hello Done
50 7.181381865 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=518 Ack=3745 Win=63104 Len=0 TSval=3555559133 TSecr=4208514842
51 7.180422167 192.168.116.33 103.21.127.134 TLSv1.2 159 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
60 7.264007426 103.21.127.134 192.168.116.33 TLSv1.2 340 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
61 7.264032891 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=611 Ack=4019 Win=63872 Len=0 TSval=3555559216 TSecr=4208514930
82 7.467376692 192.168.116.33 103.21.127.134 TLSv1.2 541 Application Data
83 7.480857505 103.21.127.134 192.168.116.33 TCP 1424 443 → 47270 [ACK] Seq=4019 Ack=1006 Win=64384 Len=1358 TSval=4208515153 TSecr=3555559359 [TCP segment of a reassembled…
84 7.480885965 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=1006 Ack=5377 Win=63104 Len=0 TSval=3555559440 TSecr=4208515153
85 7.480235037 103.21.127.134 192.168.116.33 TCP 1424 443 → 47270 [ACK] Seq=5377 Ack=1006 Win=64384 Len=1358 TSval=4208515153 TSecr=3555559359 [TCP segment of a reassembled…
86 7.480239366 192.168.116.33 103.21.127.134 TCP 66 47270 → 443 [ACK] Seq=1006 Ack=6735 Win=63104 Len=0 TSval=3555559440 TSecr=4208515153
87 7.480527857 103.21.127.134 192.168.116.33 TCP 1424 443 → 47270 [ACK] Seq=6735 Ack=1006 Win=64384 Len=1358 TSval=4208515153 TSecr=3555559359 [TCP segment of a reassembled…
Frame 82: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface 0
Ethernet II, Src: IntelCor_9c:45:1e (5c:5f:67:9c:45:1e), Dst: 52:74:31:a9:bf:f5 (52:74:31:a9:bf:f5)
Internet Protocol Version 4, Src: 192.168.116.33, Dst: 103.21.127.134
Transmission Control Protocol, Src Port: 47270, Dst Port: 443, Seq: 611, Ack: 4019, Len: 475
Secure Sockets Layer
0000 52 74 31 a9 bf f5 5c 5f 67 9c 45 1e 08 00 45 00 Rt1···_ g·E···E·
0010 02 0f 1b 57 40 00 40 06 02 2d c0 a8 74 21 67 15 ···W@·@· ·-··t!g·
0020 7f 86 b8 a6 01 bb de f1 30 fd 39 fc 9c b9 80 18 ···· ···· 0·9·····
0030 01 f5 79 fd 00 00 01 01 08 0a d3 ed 87 bf ff 23 ··y· ···· ···· ···#
0040 79 72 17 63 03 01 d6 00 00 00 00 80 00 01 65 yr·c···· ···· ··e
0050 37 0f 99 1e 5e 96 90 df ce f6 a7 64 bd da 9f 3d 7···^··· ···d···=
0060 12 4b af 30 8d e8 a7 69 42 cc da 3b eb 55 86 ee ·K·0···i B··;·U··
0070 88 cc 81 d0 d3 09 a3 1f 24 95 ed 58 f9 59 f8 3a ···· ···· $··X·Y·:
0080 71 26 18 88 28 de fd 97 69 2b 21 7c 54 63 41 90 q&··(··· i+!|TcA·
0090 e8 01 af 45 4e db 8a 1f 16 8b 94 e4 74 bc 58 ce ···EN··· ···· t·X·
00a0 db 9c 64 ff e6 fb 3e ab bd 78 f0 65 df ac 36 0e ··d···>· ·x·e··6·
00b0 c1 51 fa 29 96 d9 04 0f 8b 54 f9 ab 5a 0b 8b 1a ·Q·)···· ·T··Z···
00c0 4b 03 81 21 06 50 b8 a2 c7 12 ca c4 4c d6 12 9d K··!·P·· ···· L···
00d0 53 dd 49 9f 0c 6f 41 b2 67 0e b8 8c 49 77 b5 1e S·I··oA· g··· Iw··
00e0 05 c0 77 fc 18 66 9e f2 86 23 20 db da 3c a3 16 ··w··f·· ·# ··<··
00f0 e1 e7 4e 9e 06 1f 44 47 b4 19 e1 09 8b aa 0e 6a ··N···DG ···· ···j
0100 11 83 d9 2f bb ea 26 11 08 9b dc 17 6e f5 f2 63 ···/··&· ···· n··c
wireshark_wlp2s0_20220106125508_MgUWEO.pcapng
Packets: 1910 · Displayed: 1713 (89.7%) · Dropped: 0 (0.0%)
Profile: Default



So, I will open a terminal and start wireshark. You can install wireshark using sudo app install wireshark. I have already installed it. So, I will directly open it using root privilege. So, let us enter the password. So, this is the wireshark interface. So, I will start the packet capturing using this button. So, let us try to open some website, let us say, cse.iitb.ac.in. And you can see that there are lots of packets which we can see in wireshark. So, they have various different IP addresses.

Let us first find what is the IP address of cse.iitb.ac.in. I will copy this IP address and I will stop this packet capturing and filter paste on the IP address. So, I will write ip.addr == this. So, now we can see tool packets were exchanged between my computer and the cse server. So, if we have a look at the first three packets we can identify that this is the three way handshake.

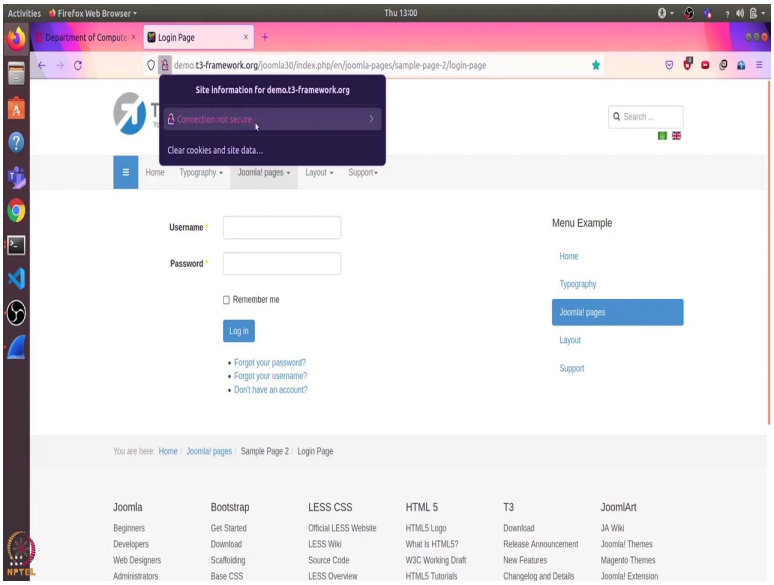
So, this is the IP address of my router and it sends to destination one TCP packet, the SYN packet and the server responds with an acknowledgement over the SYN packet and then my computer again sends the acknowledgement packet to complete the three way handshake. So, that is how the communication begins with the cse server and then it sends lots of other packets.

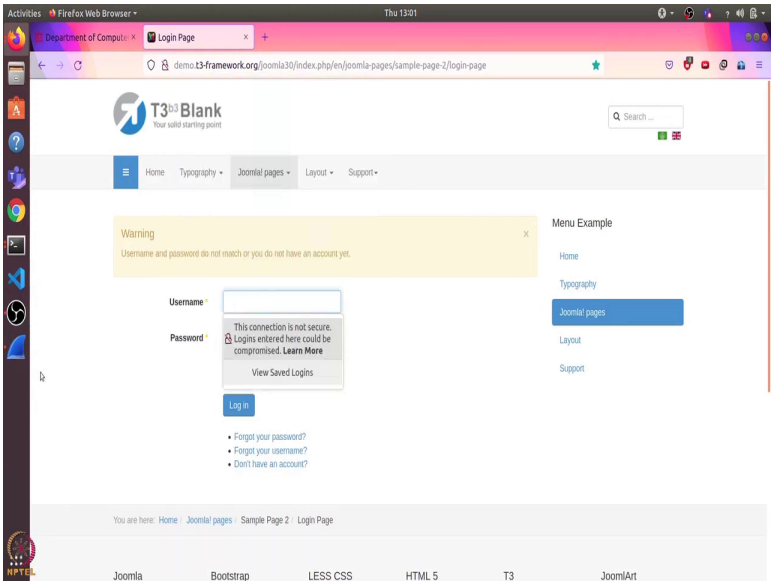
Let us first see what were other different fields. So, this is the time field which shows at what time relative to the beginning of packet capture, this transmission took place and it shows the source and destination, then which protocol was used. So, we can see there are two mainly, TCP and TLS. The TLS stands for transport layer security protocol, and then the length of the packet and then some information.

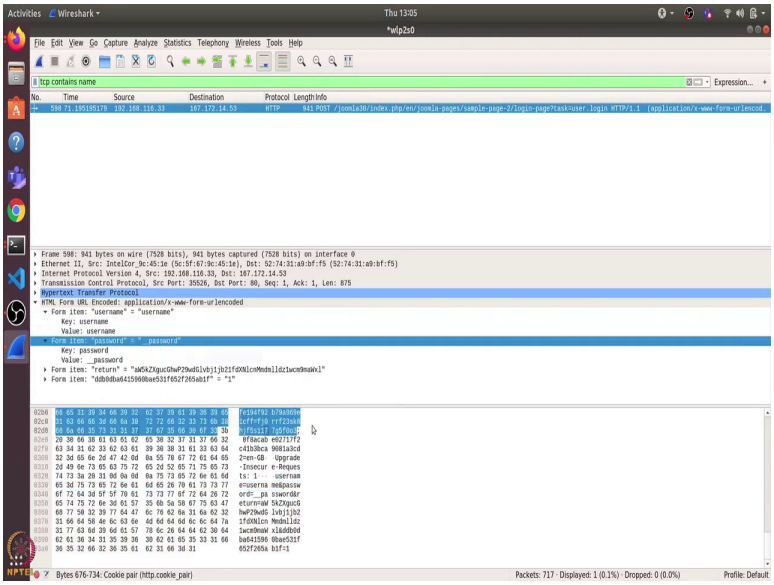
So, let us try to see some application data packet. So, this is one application data packet. And you can see that because it is a TLS packet, there is a secure sockets layer on top of the TCP layer. So, here we can go through various headers that are there in this packet. So, let us open this TCP header. So, here it shows us the source port, the destination port, the sequence number and the acknowledgement number and various other things such as checksum.

Similarly, we can go through other headers such as IP header, Ethernet header or the frame header. And here if you see the payload we cannot make any sense of it because this is encrypted application data. So, let us try to see if we can access some unsecure website and if we can make sense of the payload data.

(Refer Slide Time: 03:31)







So, what I will do here is I will open http website. Now, most of the website today use https, so the s stands for secure. So, they will encrypt the packet data before sending it over the network. But here I have copied one URL which is still using http. This is the website. And if I go to this log in page then here we can see that there is a red line on the lock and here it shows us that connection is not secure, because it is using http.

Let us start the capture and I will continue without saving and I will remove this filter also. And now if I enter some username and password, let us see, I enter username and password as __password and if I log in, I will just choose do not save. So, it says username and password do not match, but we do not care.

I will stop the capture. And now let us filter based on TCP packets which contains the word username. So, here it shows me this packet and you can see that we can clearly make sense of all this data because this is not encrypted. And if I click here then it shows me that the username is username and password is __password.

So, I can clearly see the password if I just snoop over the network traffic. So, that is one of the reason why it is suggested to use public wifi networks cautiously because someone might be snooping on the router and if we happen to visit some insecure website then the person can easily know ID password.

So, that was it for this video. Thanks and have a nice day.