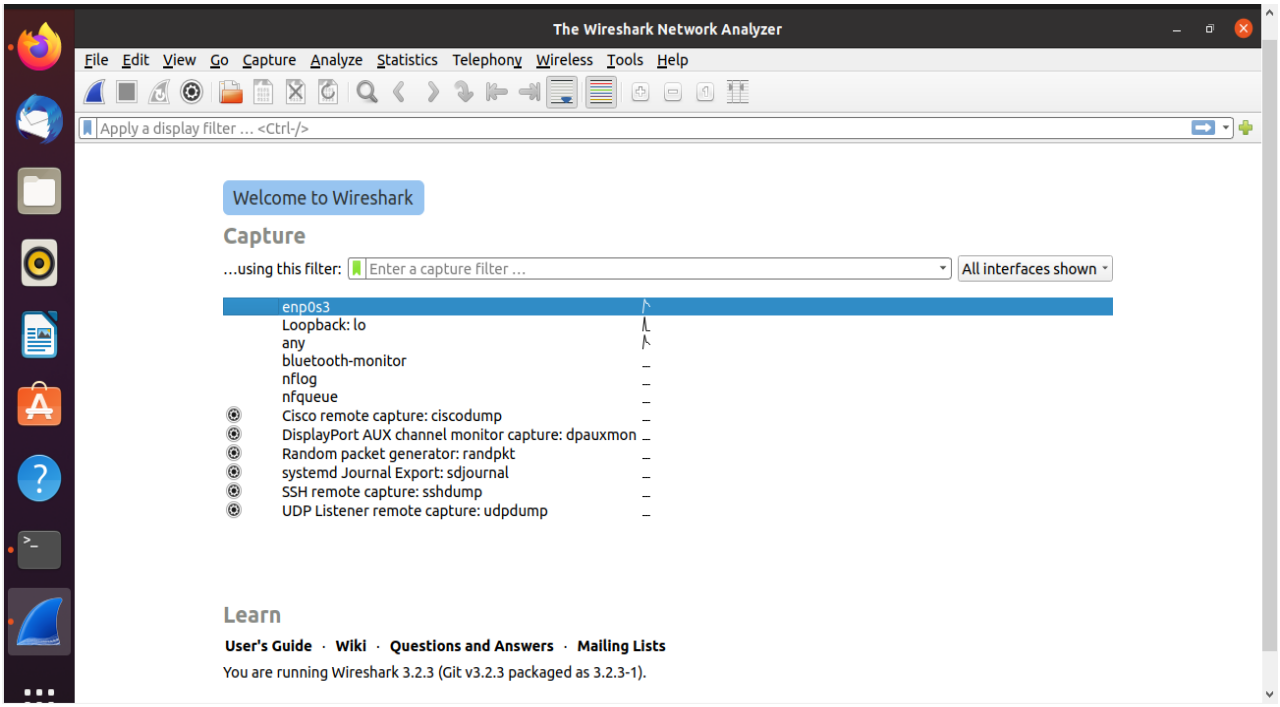
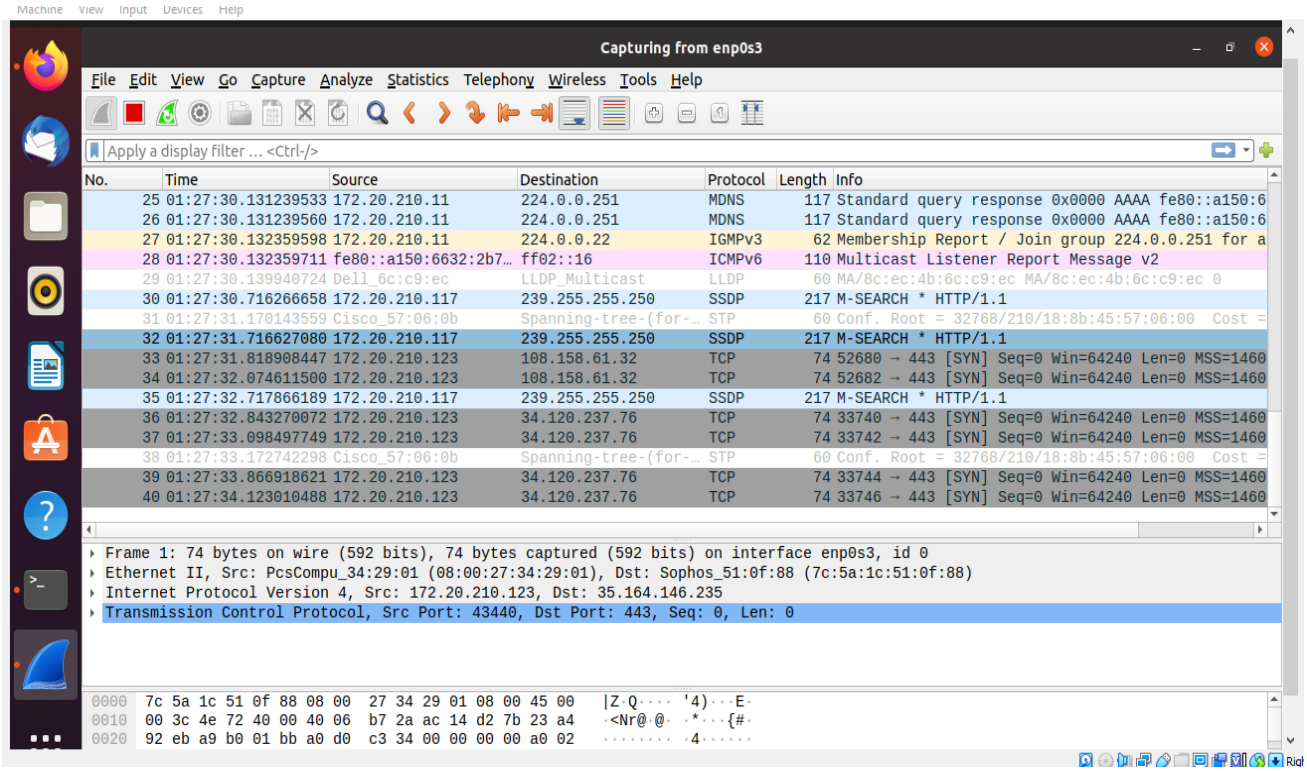
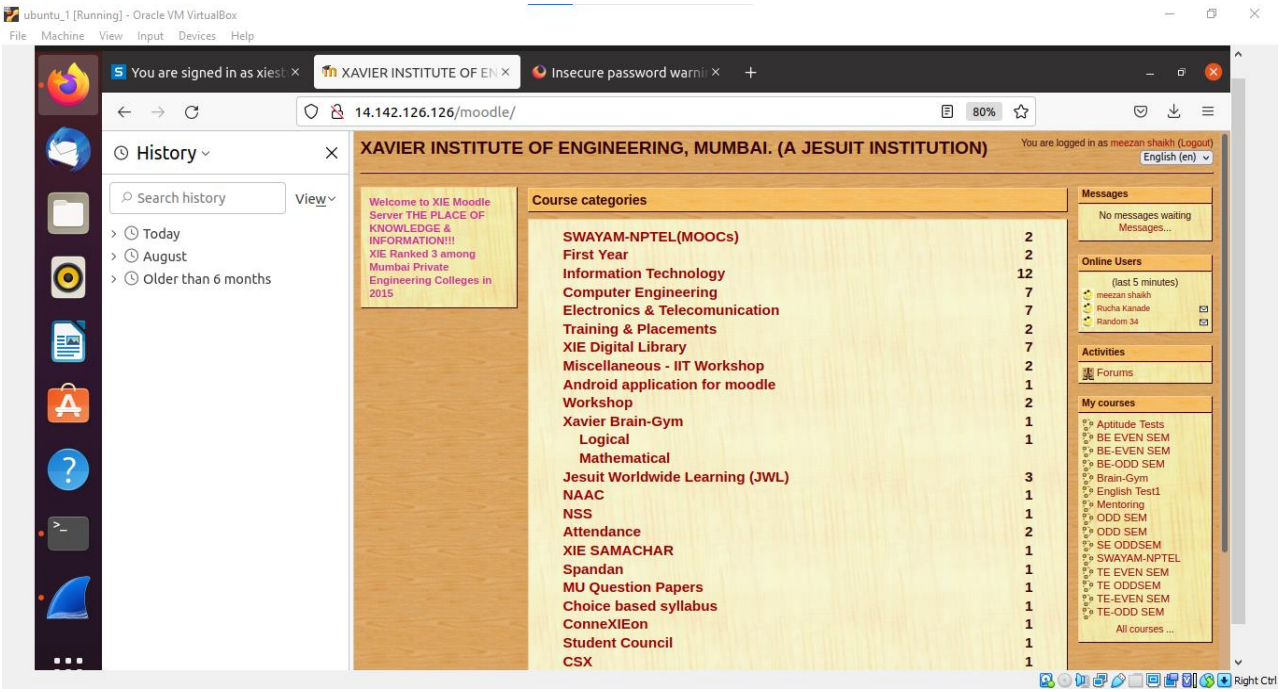
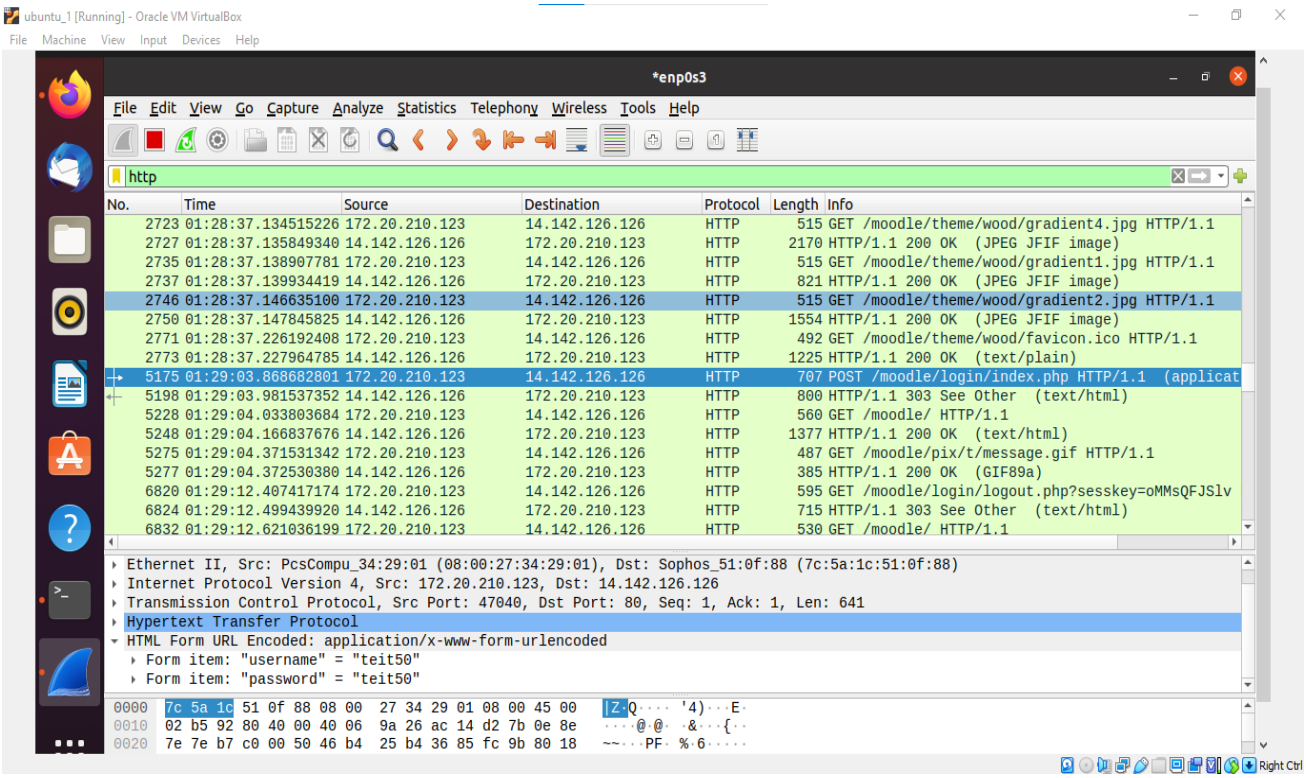
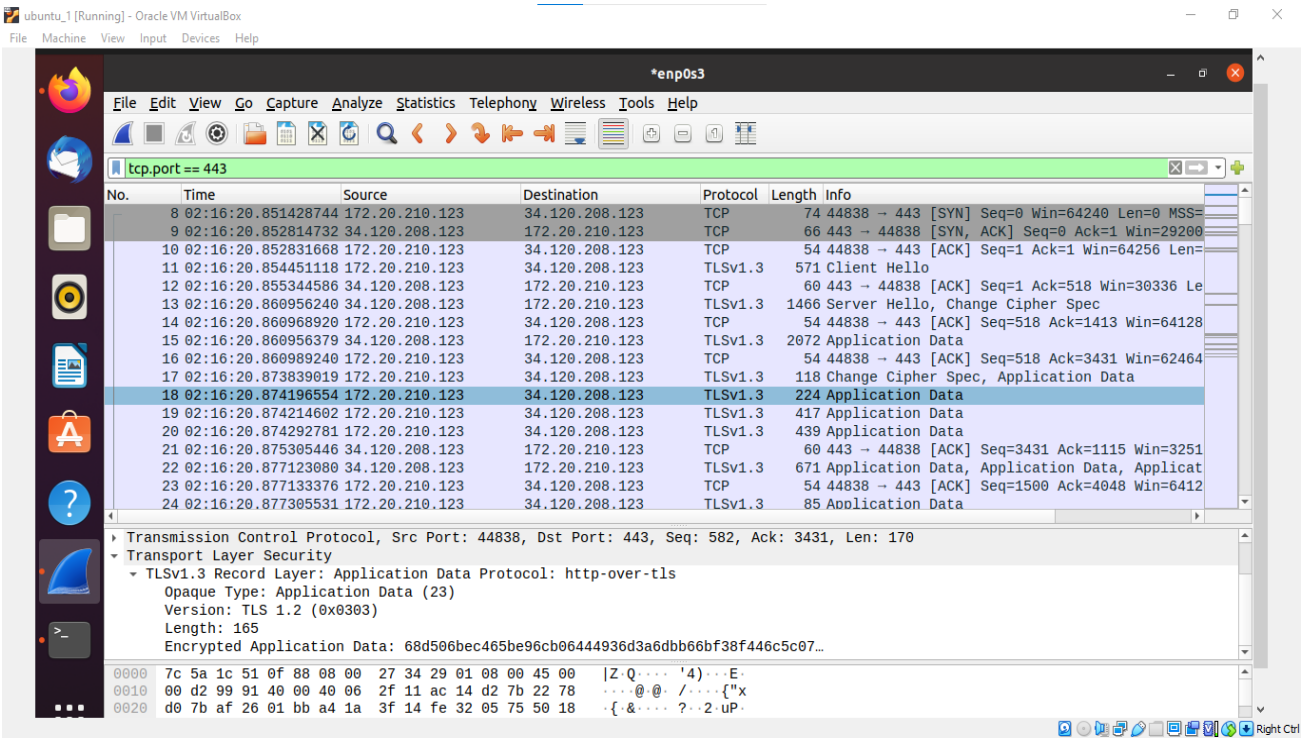
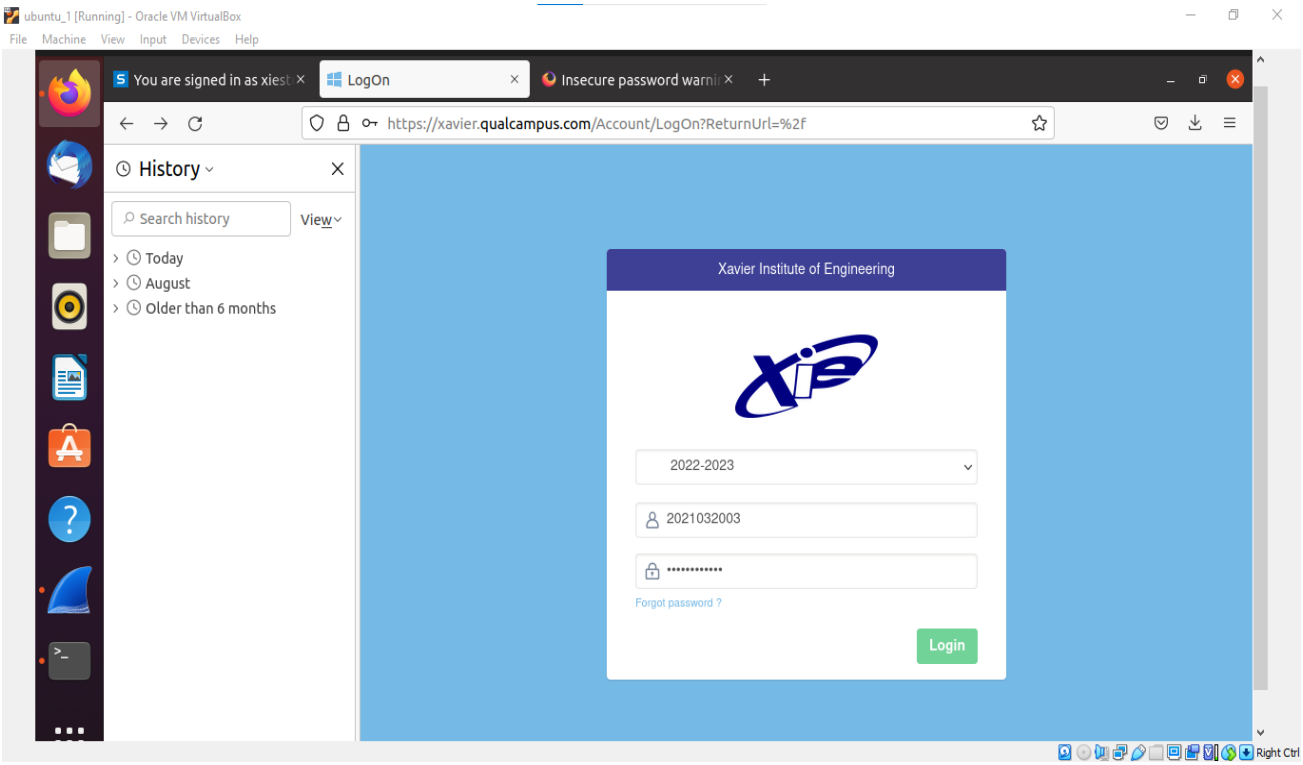

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
enp0s3
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

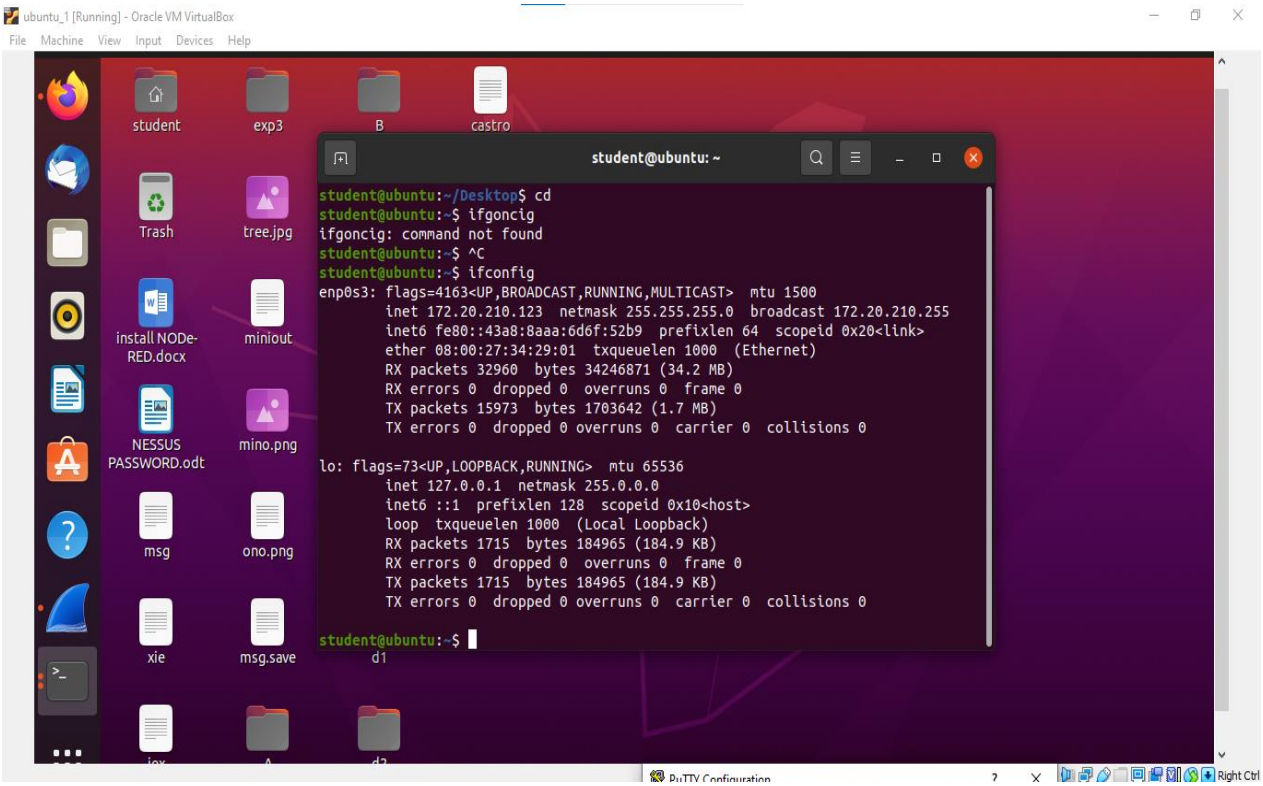

Machine View Input Devices Help
Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
25 01:27:30.131239533 172.20.210.11 224.0.0.251 MDNS 117 Standard query response 0x0000 AAAA fe80::a150:6
26 01:27:30.131239560 172.20.210.11 224.0.0.251 MDNS 117 Standard query response 0x0000 AAAA fe80::a150:6
27 01:27:30.132359598 172.20.210.11 224.0.0.22 IGMPv3 62 Membership Report / Join group 224.0.0.251 for a
28 01:27:30.132359711 fe80::a150:6632:2b7… ff02::16 ICMPv6 110 Multicast Listener Report Message v2
29 01:27:30.139940724 Dell_6c:c9:ec LLDP_Multicast LLDP 60 MA/8c:ec:4b:6c:c9:ec MA/8c:ec:4b:6c:c9:ec 0
30 01:27:30.716266658 172.20.210.117 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
31 01:27:31.170143559 Cisco_57:06:0b Spanning-tree-(for-… STP 60 Conf. Root = 32768/210/18:8b:45:57:06:00 Cost =
32 01:27:31.716627080 172.20.210.117 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
33 01:27:31.818908447 172.20.210.123 108.158.61.32 TCP 74 52680 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
34 01:27:32.074611500 172.20.210.123 108.158.61.32 TCP 74 52682 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
35 01:27:32.717866189 172.20.210.117 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
36 01:27:32.843270072 172.20.210.123 34.120.237.76 TCP 74 33740 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
37 01:27:33.098497749 172.20.210.123 34.120.237.76 TCP 74 33742 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
38 01:27:33.172742298 Cisco_57:06:0b Spanning-tree-(for-… STP 60 Conf. Root = 32768/210/18:8b:45:57:06:00 Cost =
39 01:27:33.866918621 172.20.210.123 34.120.237.76 TCP 74 33744 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
40 01:27:34.123010488 172.20.210.123 34.120.237.76 TCP 74 33746 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_34:29:01 (08:00:27:34:29:01), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
Internet Protocol Version 4, Src: 172.20.210.123, Dst: 35.164.146.235
Transmission Control Protocol, Src Port: 43440, Dst Port: 443, Seq: 0, Len: 0
0000 7c 5a 1c 51 0f 88 08 00 27 34 29 01 08 00 45 00 |Z·Q····· '4)···E·
0010 00 3c 4e 72 40 00 40 06 b7 2a ac 14 d2 7b 23 a4 ·<Nr@·@· ·*···{#·
0020 92 eb a9 b0 01 bb a0 d0 c3 34 00 00 00 00 a0 02 ·····4····

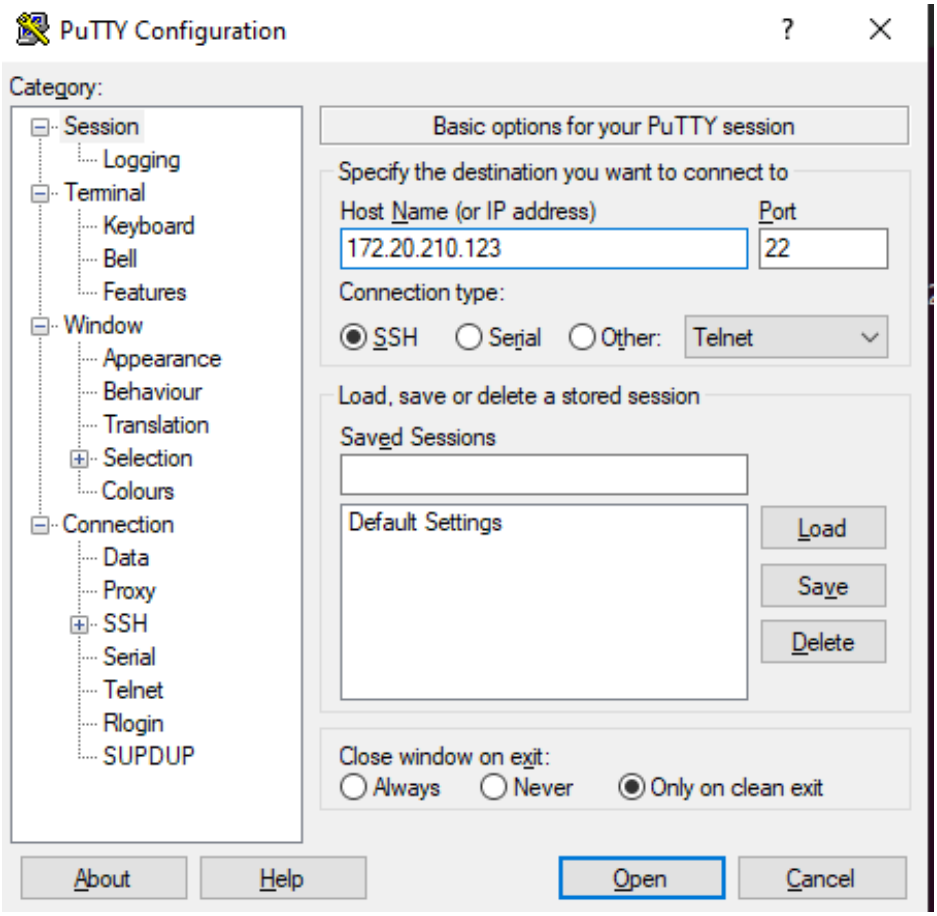

ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You are signed in as xiest
XAVIER INSTITUTE OF EN
Insecure password warni
14.142.126.126/moodle/
80%
History
Search history
View
Today
August
Older than 6 months
XAVIER INSTITUTE OF ENGINEERING, MUMBAI. (A JESUIT INSTITUTION)
You are logged in as meezan shaikh (Logout)
English (en)
Welcome to XIE Moodle Server THE PLACE OF KNOWLEDGE & INFORMATION!!! XIE Ranked 3 among Mumbai Private Engineering Colleges in 2015
Course categories
SWAYAM-NPTEL(MOOCs) 2
First Year 2
Information Technology 12
Computer Engineering 7
Electronics & Telecomunication 7
Training & Placements 2
XIE Digital Library 7
Miscellaneous - IIT Workshop 2
Android application for moodle 1
Workshop 2
Xavier Brain-Gym 1
Logical 1
Mathematical
Jesuit Worldwide Learning (JWL) 3
NAAC 1
NSS 1
Attendance 2
XIE SAMACHAR 1
Spandan 1
MU Question Papers 1
Choice based syllabus 1
ConneXIEon 1
Student Council 1
CSX 1
Messages
No messages waiting
Messages...
Online Users
(last 5 minutes)
meezan shaikh
Rucha Kanade
Random 34
Activities
Forums
My courses
Aptitude Tests
BE EVEN SEM
BE-EVEN SEM
BE-ODD SEM
Brain-Gym
English Test1
Mentoring
ODD SEM
ODD SEM
SE ODDSEM
SWAYAM-NPTEL
TE EVEN SEM
TE ODDSEM
TE-EVEN SEM
TE-ODD SEM
All courses ...
Right Ctrl

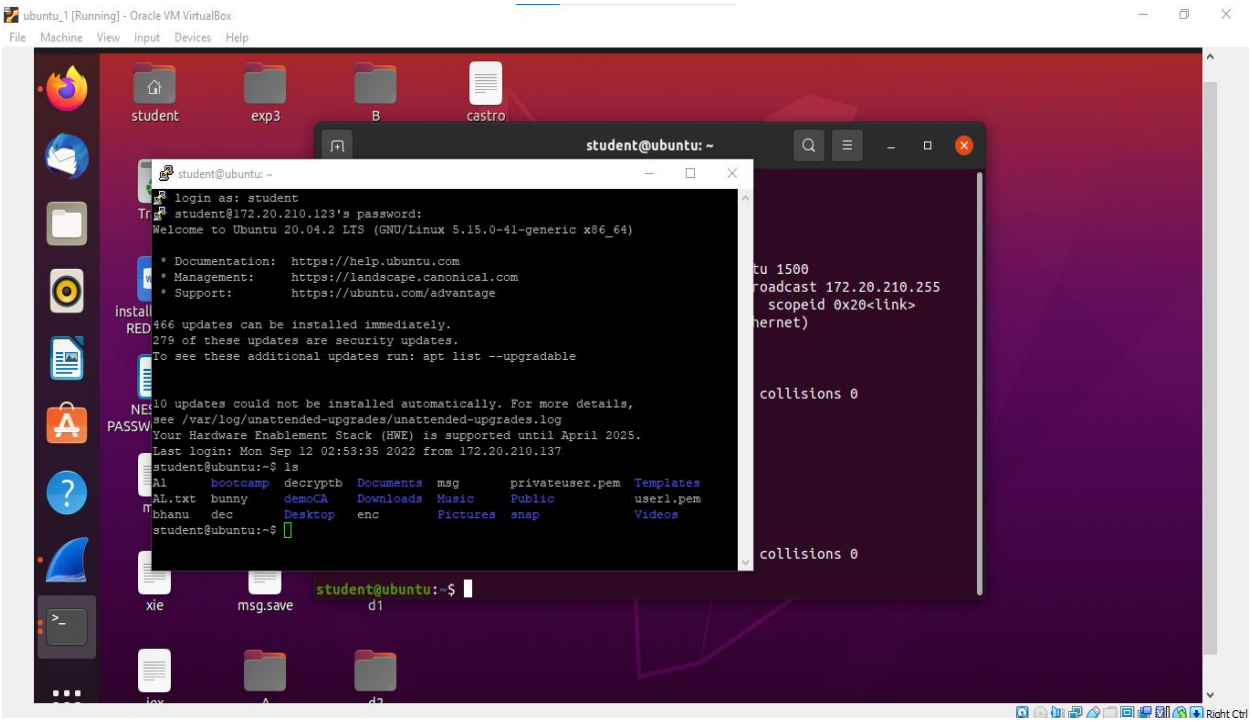

ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
2723 01:28:37.134515226 172.20.210.123 14.142.126.126 HTTP 515 GET /moodle/theme/wood/gradient4.jpg HTTP/1.1
2727 01:28:37.135849340 14.142.126.126 172.20.210.123 HTTP 2170 HTTP/1.1 200 OK (JPEG JFIF image)
2735 01:28:37.138907781 172.20.210.123 14.142.126.126 HTTP 515 GET /moodle/theme/wood/gradient1.jpg HTTP/1.1
2737 01:28:37.139934419 14.142.126.126 172.20.210.123 HTTP 821 HTTP/1.1 200 OK (JPEG JFIF image)
2746 01:28:37.146635100 172.20.210.123 14.142.126.126 HTTP 515 GET /moodle/theme/wood/gradient2.jpg HTTP/1.1
2750 01:28:37.147845825 14.142.126.126 172.20.210.123 HTTP 1554 HTTP/1.1 200 OK (JPEG JFIF image)
2771 01:28:37.226192408 172.20.210.123 14.142.126.126 HTTP 492 GET /moodle/theme/wood/favicon.ico HTTP/1.1
2773 01:28:37.227964785 14.142.126.126 172.20.210.123 HTTP 1225 HTTP/1.1 200 OK (text/plain)
5175 01:29:03.868682801 172.20.210.123 14.142.126.126 HTTP 707 POST /moodle/login/index.php HTTP/1.1 (applicat
5198 01:29:03.981537352 14.142.126.126 172.20.210.123 HTTP 800 HTTP/1.1 303 See Other (text/html)
5228 01:29:04.033803684 172.20.210.123 14.142.126.126 HTTP 560 GET /moodle/ HTTP/1.1
5248 01:29:04.166837676 14.142.126.126 172.20.210.123 HTTP 1377 HTTP/1.1 200 OK (text/html)
5275 01:29:04.371531342 172.20.210.123 14.142.126.126 HTTP 487 GET /moodle/pix/t/message.gif HTTP/1.1
5277 01:29:04.372530380 14.142.126.126 172.20.210.123 HTTP 385 HTTP/1.1 200 OK (GIF89a)
6820 01:29:12.407417174 172.20.210.123 14.142.126.126 HTTP 595 GET /moodle/login/logout.php?sesskey=oMMsQFJSlv
6824 01:29:12.499439920 14.142.126.126 172.20.210.123 HTTP 715 HTTP/1.1 303 See Other (text/html)
6832 01:29:12.621036199 172.20.210.123 14.142.126.126 HTTP 530 GET /moodle/ HTTP/1.1
Ethernet II, Src: PcsCompu_34:29:01 (08:00:27:34:29:01), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
Internet Protocol Version 4, Src: 172.20.210.123, Dst: 14.142.126.126
Transmission Control Protocol, Src Port: 47040, Dst Port: 80, Seq: 1, Ack: 1, Len: 641
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "username" = "teit50"
Form item: "password" = "teit50"
0000 7c 5a 1c 51 0f 88 08 00 27 34 29 01 08 00 45 00
0010 02 b5 92 80 40 00 40 06 9a 26 ac 14 d2 7b 0e 8e
0020 7e 7e b7 c0 00 50 46 b4 25 b4 36 85 fc 9b 80 18
Right Ctrl

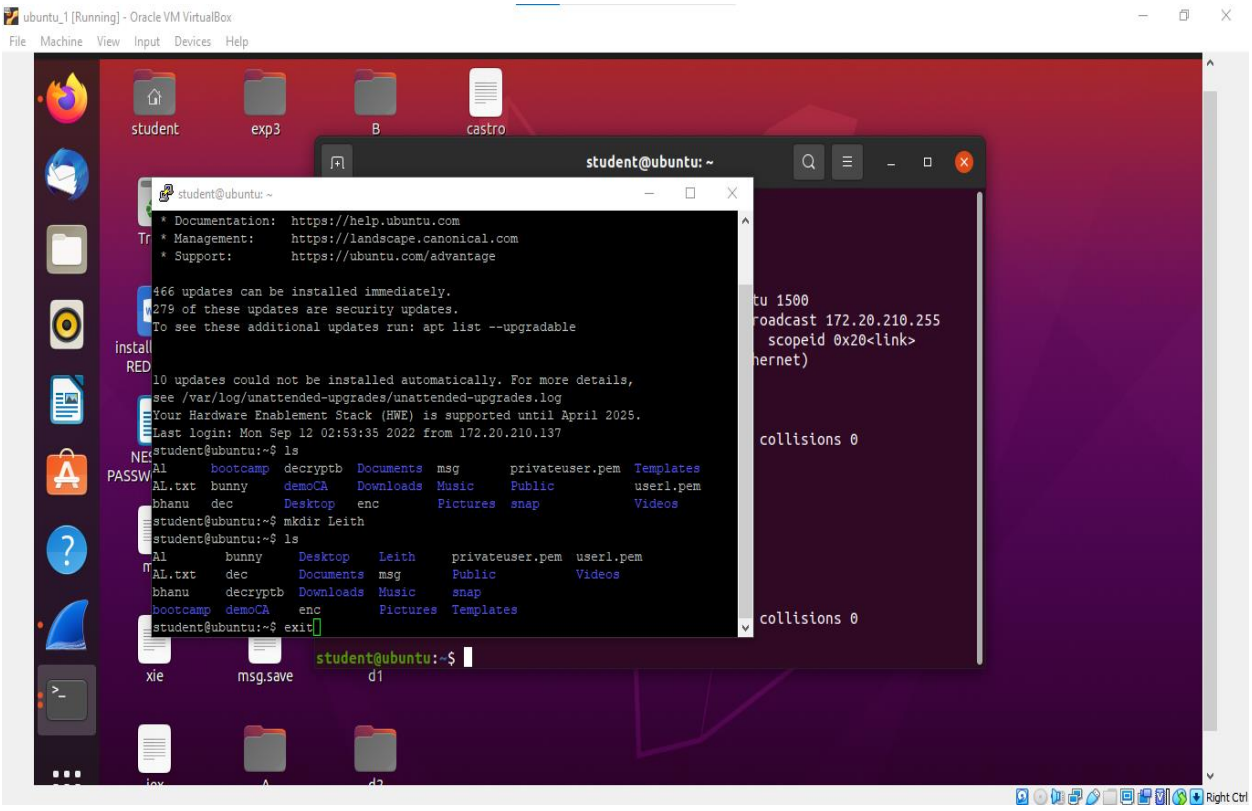

ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 443
No. Time Source Destination Protocol Length Info
8 02:16:20.851428744 172.20.210.123 34.120.208.123 TCP 74 44838 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=
9 02:16:20.852814732 34.120.208.123 172.20.210.123 TCP 66 443 → 44838 [SYN, ACK] Seq=0 Ack=1 Win=29200
10 02:16:20.852831668 172.20.210.123 34.120.208.123 TCP 54 44838 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=
11 02:16:20.854451118 172.20.210.123 34.120.208.123 TLSv1.3 571 Client Hello
12 02:16:20.855344586 34.120.208.123 172.20.210.123 TCP 60 443 → 44838 [ACK] Seq=1 Ack=518 Win=30336 Le
13 02:16:20.860956240 34.120.208.123 172.20.210.123 TLSv1.3 1466 Server Hello, Change Cipher Spec
14 02:16:20.860968920 172.20.210.123 34.120.208.123 TCP 54 44838 → 443 [ACK] Seq=518 Ack=1413 Win=64128
15 02:16:20.860956379 34.120.208.123 172.20.210.123 TLSv1.3 2072 Application Data
16 02:16:20.860989240 172.20.210.123 34.120.208.123 TCP 54 44838 → 443 [ACK] Seq=518 Ack=3431 Win=62464
17 02:16:20.873839019 172.20.210.123 34.120.208.123 TLSv1.3 118 Change Cipher Spec, Application Data
18 02:16:20.874196554 172.20.210.123 34.120.208.123 TLSv1.3 224 Application Data
19 02:16:20.874214602 172.20.210.123 34.120.208.123 TLSv1.3 417 Application Data
20 02:16:20.874292781 172.20.210.123 34.120.208.123 TLSv1.3 439 Application Data
21 02:16:20.875305446 34.120.208.123 172.20.210.123 TCP 60 443 → 44838 [ACK] Seq=3431 Ack=1115 Win=3251
22 02:16:20.877123080 34.120.208.123 172.20.210.123 TLSv1.3 671 Application Data, Application Data, Applicat
23 02:16:20.877133376 172.20.210.123 34.120.208.123 TCP 54 44838 → 443 [ACK] Seq=1500 Ack=4048 Win=6412
24 02:16:20.877305531 172.20.210.123 34.120.208.123 TLSv1.3 85 Application Data
Transmission Control Protocol, Src Port: 44838, Dst Port: 443, Seq: 582, Ack: 3431, Len: 170
Transport Layer Security
TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
Opaque Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 165
Encrypted Application Data: 68d506bec465be96cb06444936d3a6dbb66bf38f446c5c07…
0000 7c 5a 1c 51 0f 88 08 00 27 34 29 01 08 00 45 00 |Z·Q····· '4)···E·
0010 00 d2 99 91 40 00 40 06 2f 11 ac 14 d2 7b 22 78 ····@·@· /····{"x
0020 d0 7b af 26 01 bb a4 1a 3f 14 fe 32 05 75 50 18 ·{·&···· ?··2·uP·
Right Ctrl

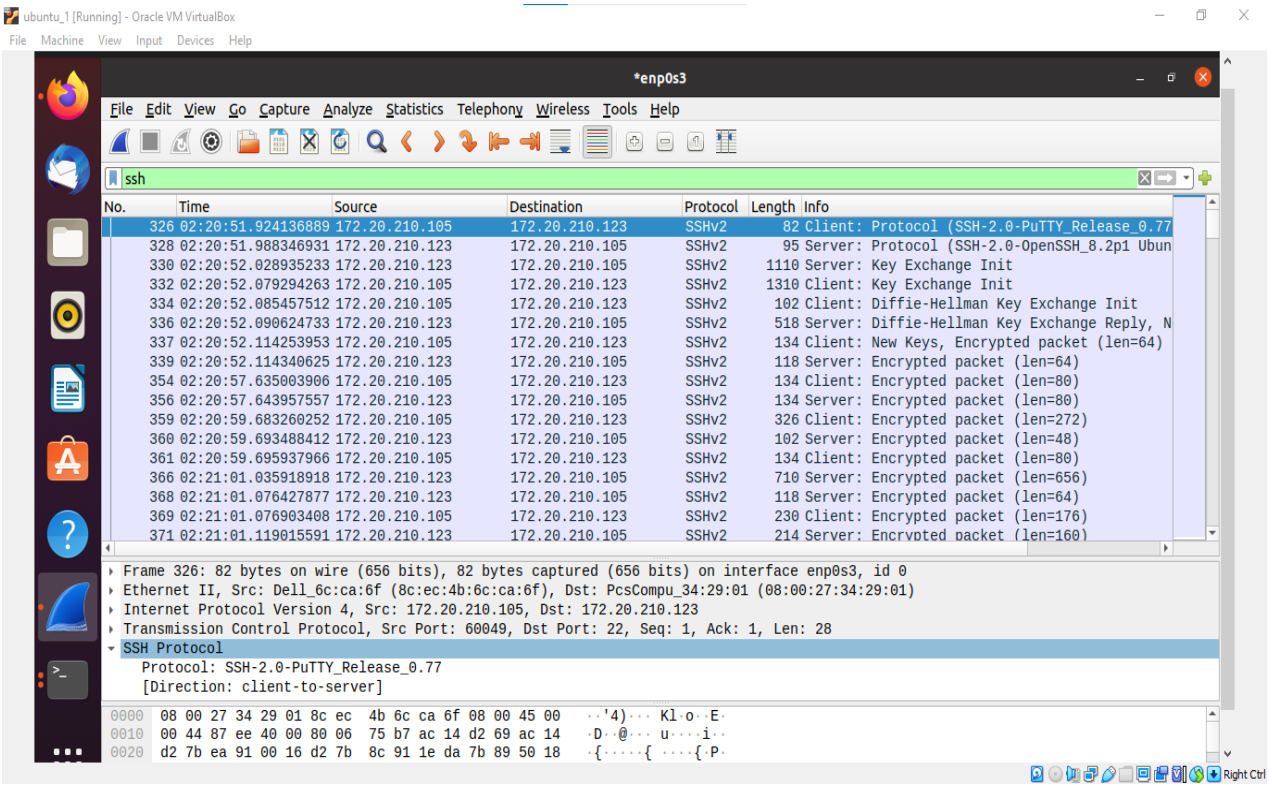

ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You are signed in as xiest
LogOn
Insecure password warnir
https://xavier.qualcampus.com/Account/LogOn?ReturnUrl=%2f
History
Search history
View
Today
August
Older than 6 months
Xavier Institute of Engineering
2022-2023
2021032003
Forgot password ?
Login
Right Ctrl


ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
student
exp3
B
castro
Trash
tree.jpg
install NODe-RED.docx
miniout
NESSUS PASSWORD.odt
mino.png
msg
ono.png
xie
msg.save
d1
student@ubuntu: ~
student@ubuntu:~/Desktop$ cd
student@ubuntu:~$ ifgoncig
ifgoncig: command not found
student@ubuntu:~$ ^C
student@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.20.210.123 netmask 255.255.255.0 broadcast 172.20.210.255
inet6 fe80::43a8:8aaa:6d6f:52b9 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:34:29:01 txqueuelen 1000 (Ethernet)
RX packets 32960 bytes 34246871 (34.2 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 15973 bytes 1703642 (1.7 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 1715 bytes 184965 (184.9 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1715 bytes 184965 (184.9 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
student@ubuntu:~$
PuTTY Configuration
Right Ctrl


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
SSH
Serial
Telnet
Rlogin
SUPDUP
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
172.20.210.123
22
Connection type:
SSH
Serial
Other:
Telnet
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Help
Open
Cancel


ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
student
exp3
B
castro
student@ubuntu: ~
login as: student
student@172.20.210.123's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.15.0-41-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
466 updates can be installed immediately.
279 of these updates are security updates.
To see these additional updates run: apt list --upgradable
10 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Sep 12 02:53:35 2022 from 172.20.210.137
student@ubuntu:~$ ls
Al bootcamp decryptb Documents msg privateuser.pem Templates
AL.txt bunny demoCA Downloads Music Public user1.pem
bhanu dec Desktop enc Pictures snap Videos
student@ubuntu:~$
xie
msg.save
d1
Right Ctrl


ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
student
exp3
B
castro
student@ubuntu: ~
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
466 updates can be installed immediately.
279 of these updates are security updates.
To see these additional updates run: apt list --upgradable
10 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Mon Sep 12 02:53:35 2022 from 172.20.210.137
student@ubuntu:~$ ls
Al bootcamp decryptb Documents msg privateuser.pem Templates
AL.txt bunny demoCA Downloads Music Public user1.pem
bhanu dec Desktop enc Pictures snap Videos
student@ubuntu:~$ mkdir Leith
student@ubuntu:~$ ls
Al bunny Desktop Leith privateuser.pem user1.pem
AL.txt dec Documents msg Public Videos
bhanu decryptb Downloads Music snap
bootcamp demoCA enc Pictures Templates
student@ubuntu:~$ exit
xie
msg.save
d1
Right Ctrl


ubuntu_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh
No. Time Source Destination Protocol Length Info
326 02:20:51.924136889 172.20.210.105 172.20.210.123 SSHv2 82 Client: Protocol (SSH-2.0-PuTTY_Release_0.77
328 02:20:51.988346931 172.20.210.123 172.20.210.105 SSHv2 95 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubun
330 02:20:52.028935233 172.20.210.123 172.20.210.105 SSHv2 1110 Server: Key Exchange Init
332 02:20:52.079294263 172.20.210.105 172.20.210.123 SSHv2 1310 Client: Key Exchange Init
334 02:20:52.085457512 172.20.210.105 172.20.210.123 SSHv2 102 Client: Diffie-Hellman Key Exchange Init
336 02:20:52.090624733 172.20.210.123 172.20.210.105 SSHv2 518 Server: Diffie-Hellman Key Exchange Reply, N
337 02:20:52.114253953 172.20.210.105 172.20.210.123 SSHv2 134 Client: New Keys, Encrypted packet (len=64)
339 02:20:52.114340625 172.20.210.123 172.20.210.105 SSHv2 118 Server: Encrypted packet (len=64)
354 02:20:57.635003906 172.20.210.105 172.20.210.123 SSHv2 134 Client: Encrypted packet (len=80)
356 02:20:57.643957557 172.20.210.123 172.20.210.105 SSHv2 134 Server: Encrypted packet (len=80)
359 02:20:59.683260252 172.20.210.105 172.20.210.123 SSHv2 326 Client: Encrypted packet (len=272)
360 02:20:59.693488412 172.20.210.123 172.20.210.105 SSHv2 102 Server: Encrypted packet (len=48)
361 02:20:59.695937966 172.20.210.105 172.20.210.123 SSHv2 134 Client: Encrypted packet (len=80)
366 02:21:01.035918918 172.20.210.123 172.20.210.105 SSHv2 710 Server: Encrypted packet (len=656)
368 02:21:01.076427877 172.20.210.123 172.20.210.105 SSHv2 118 Server: Encrypted packet (len=64)
369 02:21:01.076903408 172.20.210.105 172.20.210.123 SSHv2 230 Client: Encrypted packet (len=176)
371 02:21:01.119015591 172.20.210.123 172.20.210.105 SSHv2 214 Server: Encrypted packet (len=160)
Frame 326: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface enp0s3, id 0
Ethernet II, Src: Dell_6c:ca:6f (8c:ec:4b:6c:ca:6f), Dst: PcsCompu_34:29:01 (08:00:27:34:29:01)
Internet Protocol Version 4, Src: 172.20.210.105, Dst: 172.20.210.123
Transmission Control Protocol, Src Port: 60049, Dst Port: 22, Seq: 1, Ack: 1, Len: 28
SSH Protocol
Protocol: SSH-2.0-PuTTY_Release_0.77
[Direction: client-to-server]
0000 08 00 27 34 29 01 8c ec 4b 6c ca 6f 08 00 45 00
0010 00 44 87 ee 40 00 80 06 75 b7 ac 14 d2 69 ac 14
0020 d2 7b ea 91 00 16 d2 7b 8c 91 1e da 7b 89 50 18
Right Ctrl