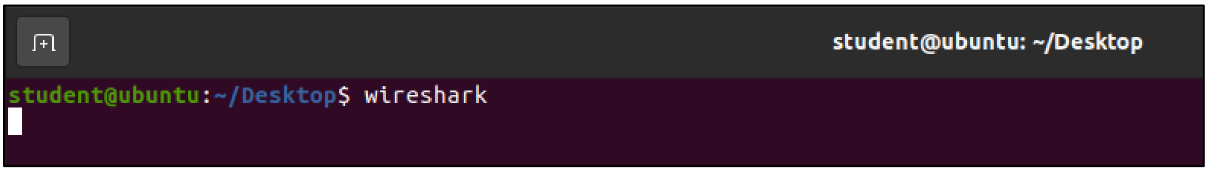
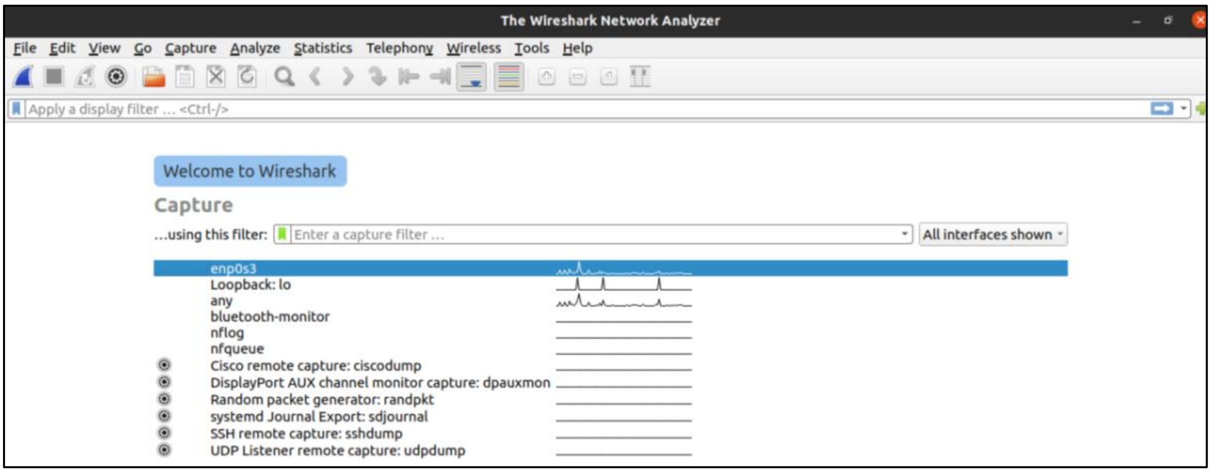
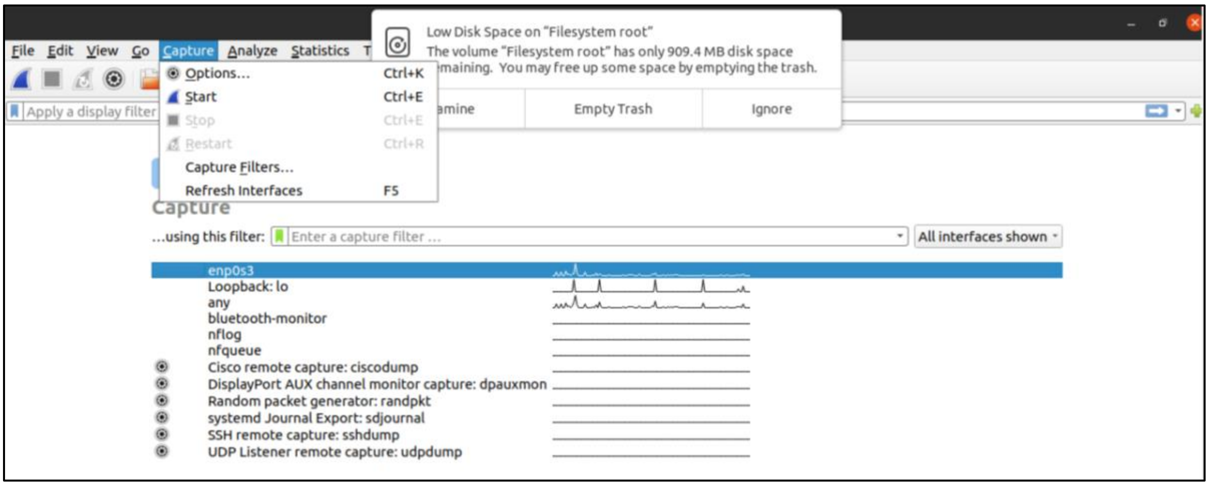
1a] Packet Sniffing Basics in non – primiscous mode:



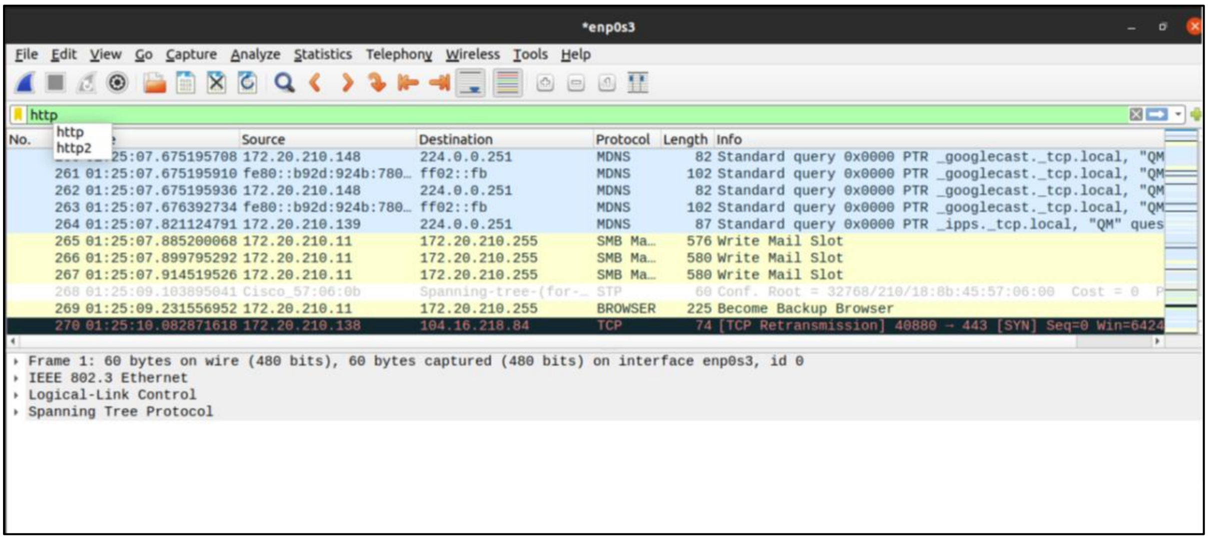
```
student@ubuntu:~/Desktop$ wireshark
```


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

Start capturing


File Edit View Go Capture Analyze Statistics T
Options… Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters…
Refresh Interfaces F5
Apply a display filter
amine
Empty Trash
Ignore
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

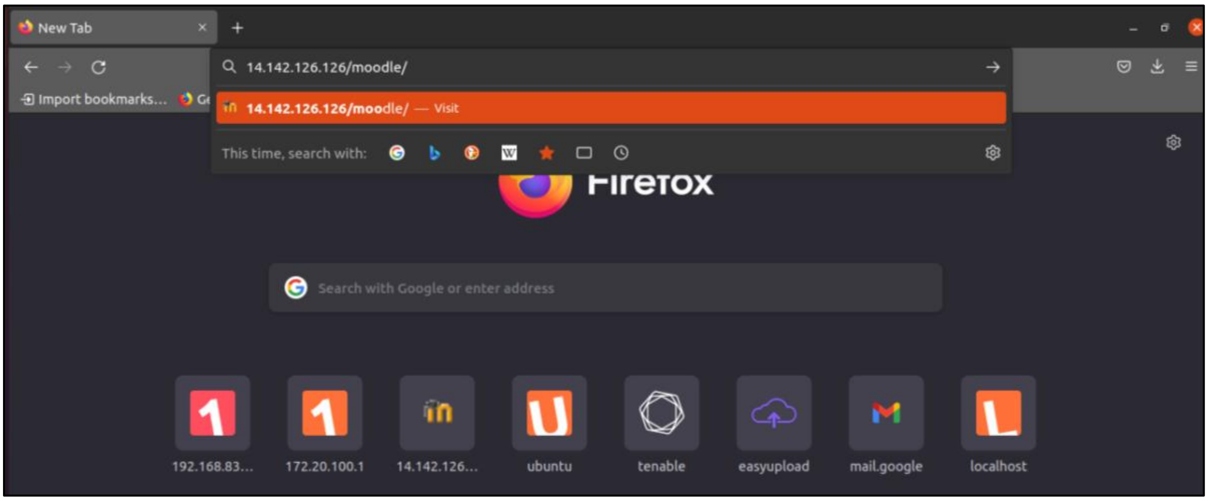
Low Disk Space on "Filesystem root"
The volume "Filesystem root" has only 909.4 MB disk space
maining. You may free up some space by emptying the trash.

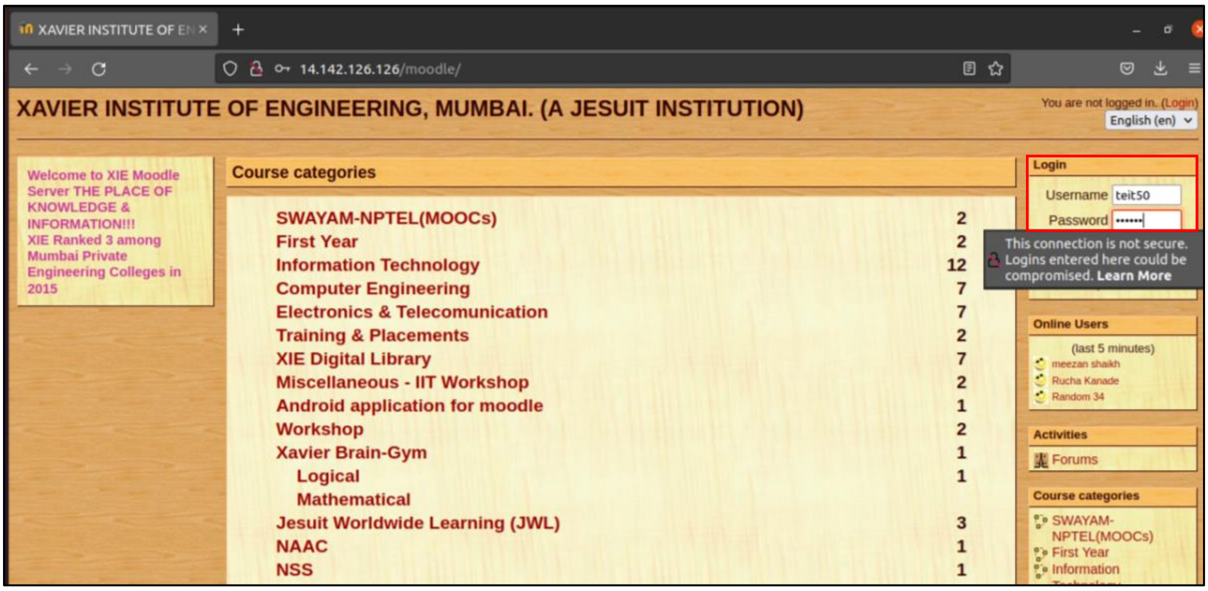

*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2

```
No.        e                  Source                 Destination           Protocol  Length Info
    ...:25:07.675195708 172.20.210.148         224.0.0.251           MDNS        82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM
    261 01:25:07.675195910 fe80::b92d:924b:780… ff02::fb              MDNS       102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM
    262 01:25:07.675195936 172.20.210.148         224.0.0.251           MDNS        82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM
    263 01:25:07.676392734 fe80::b92d:924b:780… ff02::fb              MDNS       102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM
    264 01:25:07.821124791 172.20.210.139         224.0.0.251           MDNS        87 Standard query 0x0000 PTR _ipps._tcp.local, "QM" ques
    265 01:25:07.885200068 172.20.210.11          172.20.210.255        SMB Ma…    576 Write Mail Slot
    266 01:25:07.899795292 172.20.210.11          172.20.210.255        SMB Ma…    580 Write Mail Slot
    267 01:25:07.914519526 172.20.210.11          172.20.210.255        SMB Ma…    580 Write Mail Slot
    268 01:25:09.103895041 Cisco_57:06:0b         Spanning-tree-(for-… STP          60 Conf. Root = 32768/210/18:8b:45:57:06:00  Cost = 0  P
    269 01:25:09.231556952 172.20.210.11          172.20.210.255        BROWSER    225 Become Backup Browser
    270 01:25:10.082871618 172.20.210.138         104.16.218.84         TCP         74 [TCP Retransmission] 40880 → 443 [SYN] Seq=0 Win=6424

› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp0s3, id 0
› IEEE 802.3 Ethernet
› Logical-Link Control
› Spanning Tree Protocol
```

1b] Packet Sniffing of SSH, HTTP and SSL packets

For HTTP: Go to Moddle IP Address and login using teit50 as username and password





XAVIER INSTITUTE OF ENGINEERING, MUMBAI. (A JESUIT INSTITUTION)

You are not logged in. (Login)

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

Login

Username teit50

Password ••••••

This connection is not secure. Logins entered here could be compromised. **Learn More**

Online Users

(last 5 minutes)

meezan shaikh

Rucha Kanade

Random 34

Activities

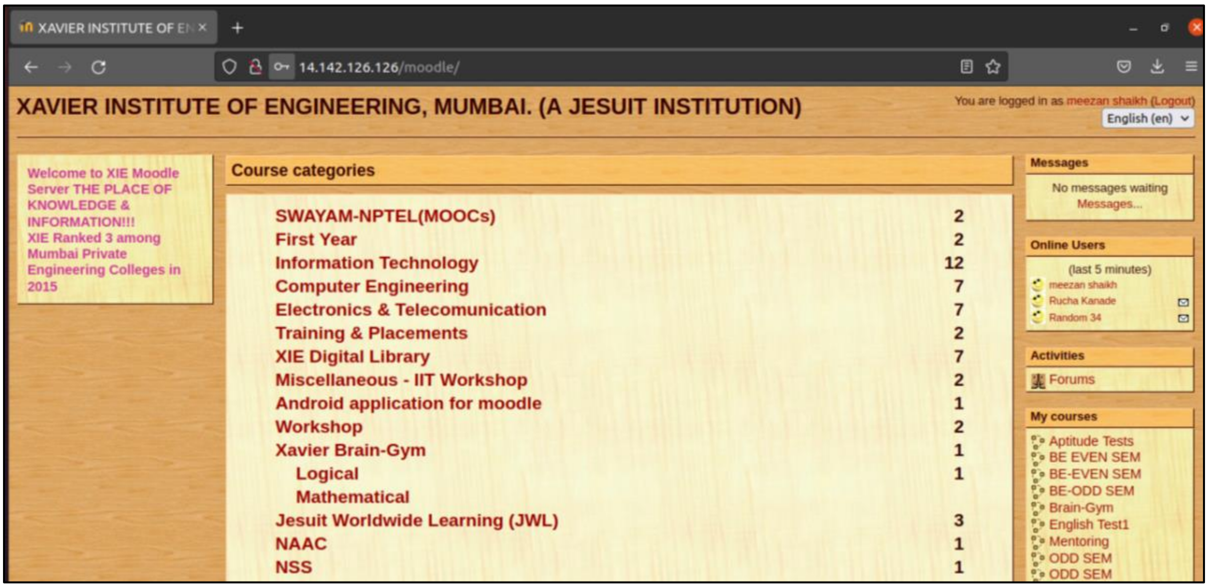
Forums

Course categories

SWAYAM-NPTEL(MOOCs)

First Year

Information



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

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

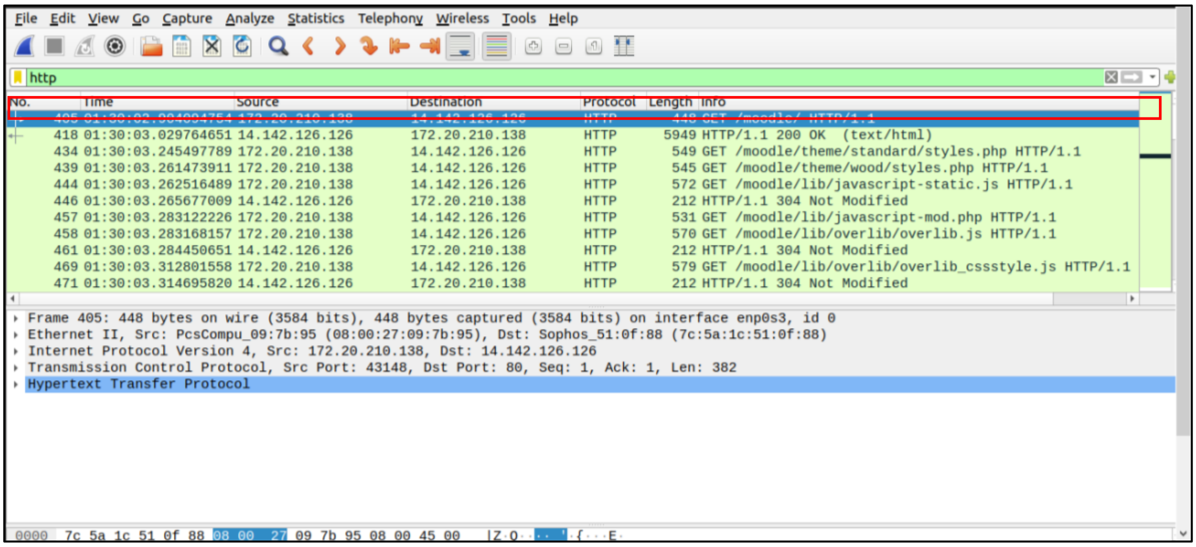
English Test1

Mentoring

ODD SEM

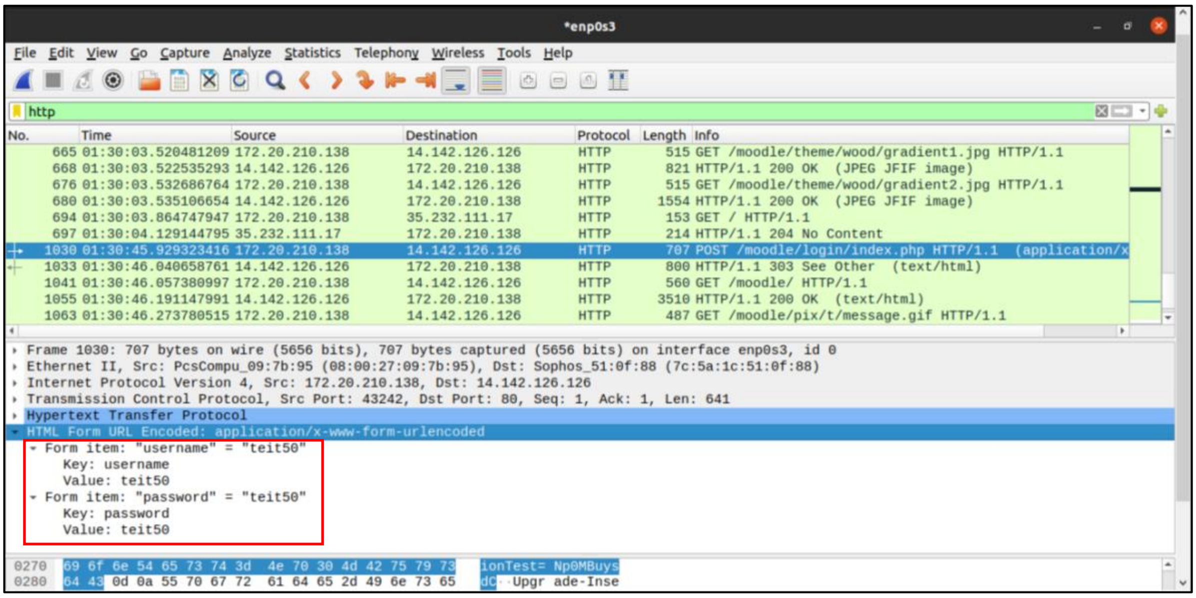
ODD SEM

Now stop capturing and select the http packet with POST method



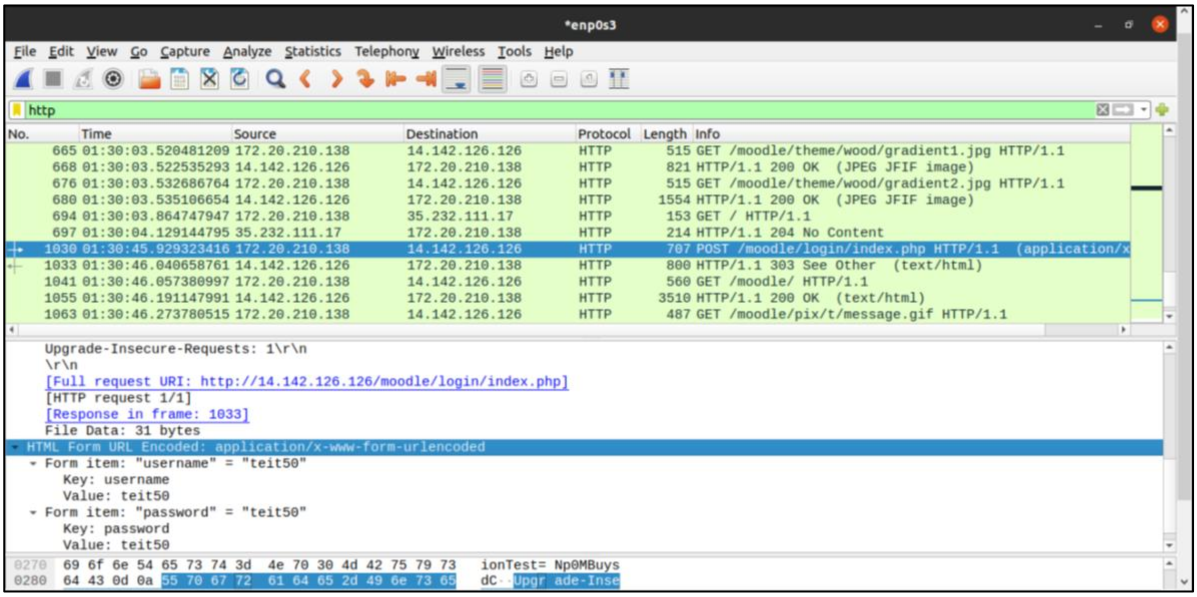
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time               Source          Destination     Protocol Length Info
  405 01:30:02.904094754 172.20.210.138  14.142.126.126  HTTP      448 GET /moodle/ HTTP/1.1
  418 01:30:03.029764651 14.142.126.126  172.20.210.138  HTTP     5949 HTTP/1.1 200 OK  (text/html)
  434 01:30:03.245497789 172.20.210.138  14.142.126.126  HTTP      549 GET /moodle/theme/standard/styles.php HTTP/1.1
  439 01:30:03.261473911 172.20.210.138  14.142.126.126  HTTP      545 GET /moodle/theme/wood/styles.php HTTP/1.1
  444 01:30:03.262516489 172.20.210.138  14.142.126.126  HTTP      572 GET /moodle/lib/javascript-static.js HTTP/1.1
  446 01:30:03.265677009 14.142.126.126  172.20.210.138  HTTP      212 HTTP/1.1 304 Not Modified
  457 01:30:03.283122226 172.20.210.138  14.142.126.126  HTTP      531 GET /moodle/lib/javascript-mod.php HTTP/1.1
  458 01:30:03.283168157 172.20.210.138  14.142.126.126  HTTP      570 GET /moodle/lib/overlib/overlib.js HTTP/1.1
  461 01:30:03.284450651 14.142.126.126  172.20.210.138  HTTP      212 HTTP/1.1 304 Not Modified
  469 01:30:03.312801558 172.20.210.138  14.142.126.126  HTTP      579 GET /moodle/lib/overlib/overlib_cssstyle.js HTTP/1.1
  471 01:30:03.314695820 14.142.126.126  172.20.210.138  HTTP      212 HTTP/1.1 304 Not Modified

› Frame 405: 448 bytes on wire (3584 bits), 448 bytes captured (3584 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_09:7b:95 (08:00:27:09:7b:95), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
› Internet Protocol Version 4, Src: 172.20.210.138, Dst: 14.142.126.126
› Transmission Control Protocol, Src Port: 43148, Dst Port: 80, Seq: 1, Ack: 1, Len: 382
› Hypertext Transfer Protocol

0000  7c 5a 1c 51 0f 88 08 00  27 09 7b 95 08 00 45 00   |Z·Q····'·{···E·
```



*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

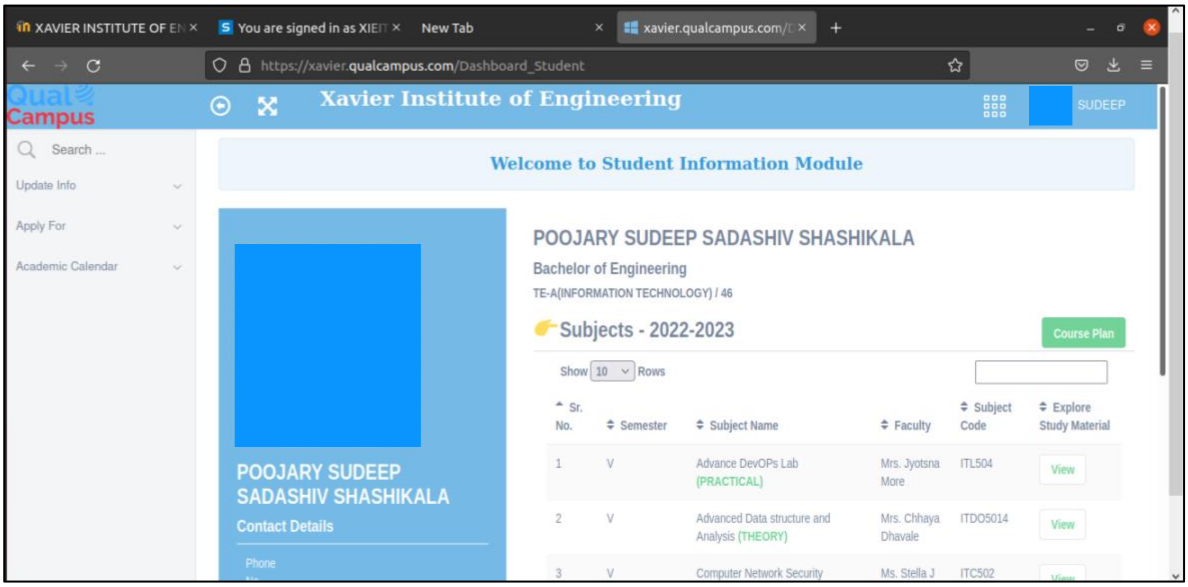
```
http
No.   Time               Source          Destination     Protocol Length Info
  665 01:30:03.520481209 172.20.210.138  14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient1.jpg HTTP/1.1
  668 01:30:03.522535293 14.142.126.126  172.20.210.138  HTTP      821 HTTP/1.1 200 OK  (JPEG JFIF image)
  676 01:30:03.532686764 172.20.210.138  14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient2.jpg HTTP/1.1
  680 01:30:03.535106654 14.142.126.126  172.20.210.138  HTTP     1554 HTTP/1.1 200 OK  (JPEG JFIF image)
  694 01:30:03.864747947 172.20.210.138  35.232.111.17   HTTP      153 GET / HTTP/1.1
  697 01:30:04.129144795 35.232.111.17   172.20.210.138  HTTP      214 HTTP/1.1 204 No Content
 1030 01:30:45.929323416 172.20.210.138  14.142.126.126  HTTP      707 POST /moodle/login/index.php HTTP/1.1  (application/x
 1033 01:30:46.040658761 14.142.126.126  172.20.210.138  HTTP      800 HTTP/1.1 303 See Other  (text/html)
 1041 01:30:46.057380997 172.20.210.138  14.142.126.126  HTTP      560 GET /moodle/ HTTP/1.1
 1055 01:30:46.191147991 14.142.126.126  172.20.210.138  HTTP     3510 HTTP/1.1 200 OK  (text/html)
 1063 01:30:46.273780515 172.20.210.138  14.142.126.126  HTTP      487 GET /moodle/pix/t/message.gif HTTP/1.1

› Frame 1030: 707 bytes on wire (5656 bits), 707 bytes captured (5656 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_09:7b:95 (08:00:27:09:7b:95), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
› Internet Protocol Version 4, Src: 172.20.210.138, Dst: 14.142.126.126
› Transmission Control Protocol, Src Port: 43242, 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"
      Key: username
      Value: teit50
  ▾ Form item: "password" = "teit50"
      Key: password
      Value: teit50

0270  69 6f 6e 54 65 73 74 3d  4e 70 30 4d 42 75 79 73   ionTest= NpOMBuys
0280  64 43 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   dC··Upgr ade-Inse
```



*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.   Time               Source          Destination     Protocol Length Info
  665 01:30:03.520481209 172.20.210.138  14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient1.jpg HTTP/1.1
  668 01:30:03.522535293 14.142.126.126  172.20.210.138  HTTP      821 HTTP/1.1 200 OK  (JPEG JFIF image)
  676 01:30:03.532686764 172.20.210.138  14.142.126.126  HTTP      515 GET /moodle/theme/wood/gradient2.jpg HTTP/1.1
  680 01:30:03.535106654 14.142.126.126  172.20.210.138  HTTP     1554 HTTP/1.1 200 OK  (JPEG JFIF image)
  694 01:30:03.864747947 172.20.210.138  35.232.111.17   HTTP      153 GET / HTTP/1.1
  697 01:30:04.129144795 35.232.111.17   172.20.210.138  HTTP      214 HTTP/1.1 204 No Content
 1030 01:30:45.929323416 172.20.210.138  14.142.126.126  HTTP      707 POST /moodle/login/index.php HTTP/1.1  (application/x
 1033 01:30:46.040658761 14.142.126.126  172.20.210.138  HTTP      800 HTTP/1.1 303 See Other  (text/html)
 1041 01:30:46.057380997 172.20.210.138  14.142.126.126  HTTP      560 GET /moodle/ HTTP/1.1
 1055 01:30:46.191147991 14.142.126.126  172.20.210.138  HTTP     3510 HTTP/1.1 200 OK  (text/html)
 1063 01:30:46.273780515 172.20.210.138  14.142.126.126  HTTP      487 GET /moodle/pix/t/message.gif HTTP/1.1

    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://14.142.126.126/moodle/login/index.php]
    [HTTP request 1/1]
    [Response in frame: 1033]
    File Data: 31 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "username" = "teit50"
      Key: username
      Value: teit50
  ▾ Form item: "password" = "teit50"
      Key: password
      Value: teit50

0270  69 6f 6e 54 65 73 74 3d  4e 70 30 4d 42 75 79 73   ionTest= NpOMBuys
0280  64 43 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   dC··Upgr ade-Inse
```

For HTTP/SSL: Login to ERP and start capturing in Wireshark again



Welcome to Student Information Module

POOJARY SUDEEP SADASHIV SHASHIKALA

Bachelor of Engineering

TE-A(INFORMATION TECHNOLOGY) / 46

Subjects - 2022-2023

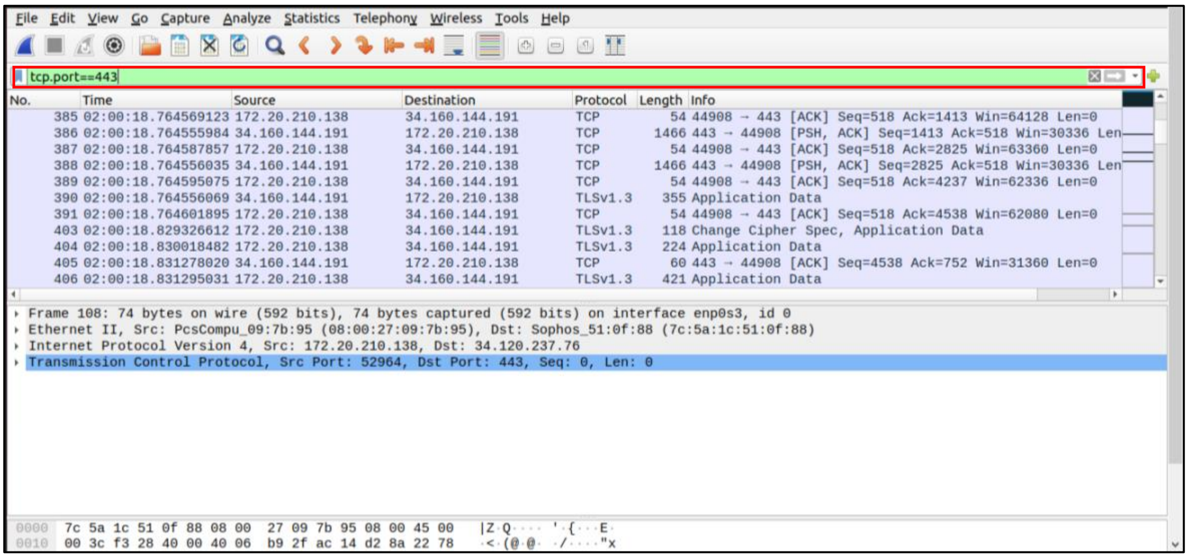
Show 10 Rows

Sr. No.	Semester	Subject Name	Faculty	Subject Code	Explore Study Material
1	V	Advance DevOPs Lab (PRACTICAL)	Mrs. Jyotsna More	ITL504	View
2	V	Advanced Data structure and Analysis (THEORY)	Mrs. Chhaya Dhavale	ITDO5014	View
3	V	Computer Network Security	Ms. Stella J	ITC502	View

POOJARY SUDEEP SADASHIV SHASHIKALA

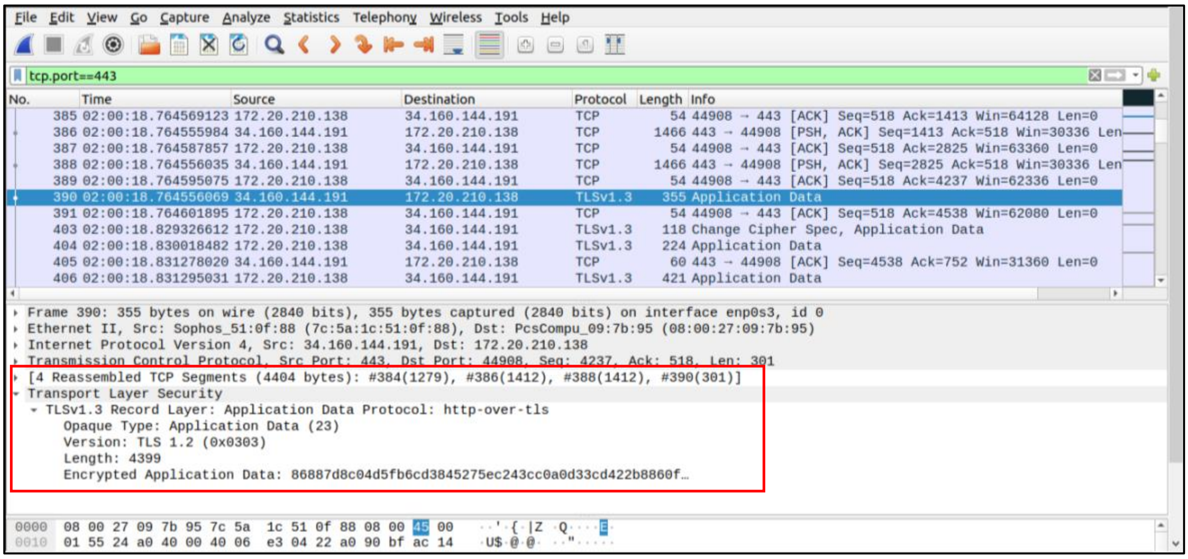
Contact Details

Stop capturing and filter using tcp.port==43


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==443

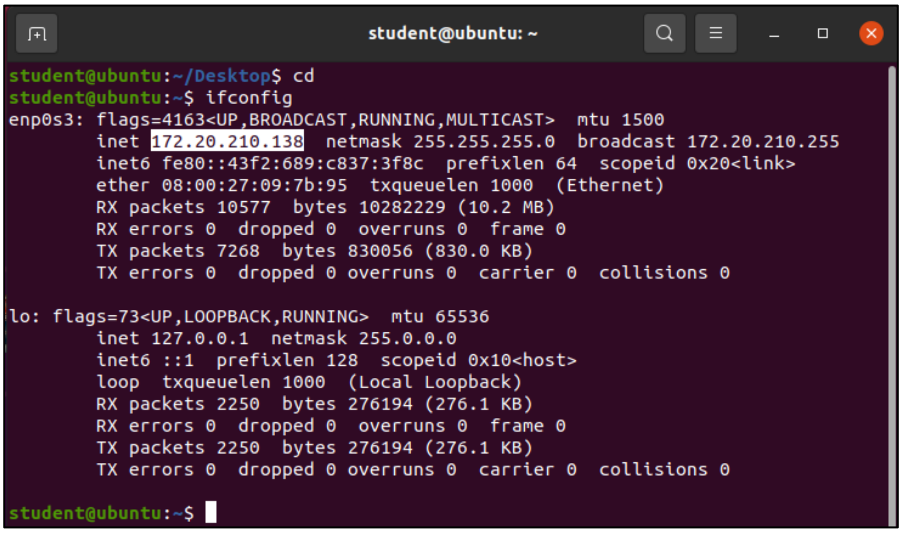
```
No.     Time               Source          Destination     Protocol  Length Info
    385 02:00:18.764569123 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=1413 Win=64128 Len=0
    386 02:00:18.764555984 34.160.144.191  172.20.210.138  TCP       1466 443 → 44908 [PSH, ACK] Seq=1413 Ack=518 Win=30336 Len
    387 02:00:18.764587857 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=2825 Win=63360 Len=0
    388 02:00:18.764556035 34.160.144.191  172.20.210.138  TCP       1466 443 → 44908 [PSH, ACK] Seq=2825 Ack=518 Win=30336 Len
    389 02:00:18.764595075 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=4237 Win=62336 Len=0
    390 02:00:18.764556069 34.160.144.191  172.20.210.138  TLSv1.3    355 Application Data
    391 02:00:18.764601895 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=4538 Win=62080 Len=0
    403 02:00:18.829326612 172.20.210.138  34.160.144.191  TLSv1.3    118 Change Cipher Spec, Application Data
    404 02:00:18.830018482 172.20.210.138  34.160.144.191  TLSv1.3    224 Application Data
    405 02:00:18.831278020 34.160.144.191  172.20.210.138  TCP         60 443 → 44908 [ACK] Seq=4538 Ack=752 Win=31360 Len=0
    406 02:00:18.831295031 172.20.210.138  34.160.144.191  TLSv1.3    421 Application Data

› Frame 108: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp0s3, id 0
› Ethernet II, Src: PcsCompu_09:7b:95 (08:00:27:09:7b:95), Dst: Sophos_51:0f:88 (7c:5a:1c:51:0f:88)
› Internet Protocol Version 4, Src: 172.20.210.138, Dst: 34.120.237.76
› Transmission Control Protocol, Src Port: 52964, Dst Port: 443, Seq: 0, Len: 0

0000  7c 5a 1c 51 0f 88 08 00  27 09 7b 95 08 00 45 00   |Z·Q···· '·{···E·
0010  00 3c f3 28 40 00 40 06  b9 2f ac 14 d2 8a 22 78   ·<·(@·@· ·/····"x
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

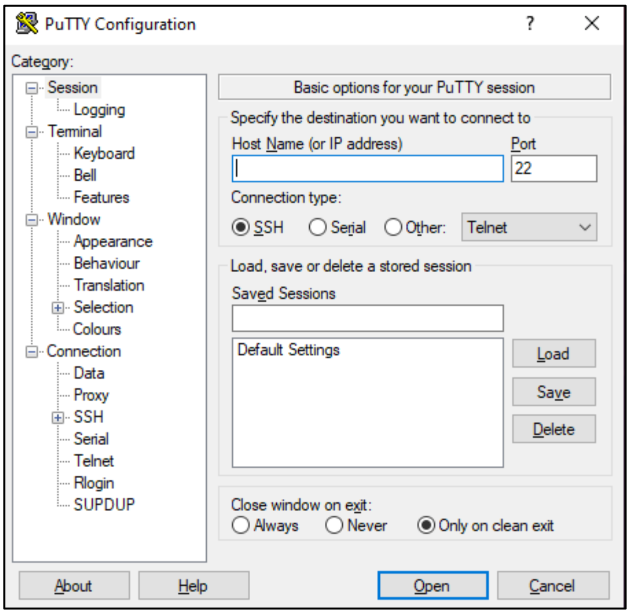
tcp.port==443

```
No.     Time               Source          Destination     Protocol  Length Info
    385 02:00:18.764569123 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=1413 Win=64128 Len=0
    386 02:00:18.764555984 34.160.144.191  172.20.210.138  TCP       1466 443 → 44908 [PSH, ACK] Seq=1413 Ack=518 Win=30336 Len
    387 02:00:18.764587857 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=2825 Win=63360 Len=0
    388 02:00:18.764556035 34.160.144.191  172.20.210.138  TCP       1466 443 → 44908 [PSH, ACK] Seq=2825 Ack=518 Win=30336 Len
    389 02:00:18.764595075 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=4237 Win=62336 Len=0
    390 02:00:18.764556069 34.160.144.191  172.20.210.138  TLSv1.3    355 Application Data
    391 02:00:18.764601895 172.20.210.138  34.160.144.191  TCP         54 44908 → 443 [ACK] Seq=518 Ack=4538 Win=62080 Len=0
    403 02:00:18.829326612 172.20.210.138  34.160.144.191  TLSv1.3    118 Change Cipher Spec, Application Data
    404 02:00:18.830018482 172.20.210.138  34.160.144.191  TLSv1.3    224 Application Data
    405 02:00:18.831278020 34.160.144.191  172.20.210.138  TCP         60 443 → 44908 [ACK] Seq=4538 Ack=752 Win=31360 Len=0
    406 02:00:18.831295031 172.20.210.138  34.160.144.191  TLSv1.3    421 Application Data

› Frame 390: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface enp0s3, id 0
› Ethernet II, Src: Sophos_51:0f:88 (7c:5a:1c:51:0f:88), Dst: PcsCompu_09:7b:95 (08:00:27:09:7b:95)
› Internet Protocol Version 4, Src: 34.160.144.191, Dst: 172.20.210.138
› Transmission Control Protocol, Src Port: 443, Dst Port: 44908, Seq: 4237, Ack: 518, Len: 301
› [4 Reassembled TCP Segments (4404 bytes): #384(1279), #386(1412), #388(1412), #390(301)]
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 4399
      Encrypted Application Data: 86887d8c04d5fb6cd3845275ec243cc0a0d33cd422b8860f…

0000  08 00 27 09 7b 95 7c 5a  1c 51 0f 88 08 00 45 00   ··'·{·|Z ·Q····E·
0010  01 55 24 a0 40 00 40 06  e3 04 22 a0 90 bf ac 14   ·U$·@·@· ··"·····
```

For SSH: Now, Packet Sniffing of SHH from Windows in Ubuntu



```
student@ubuntu:~/Desktop$ cd
student@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.210.138  netmask 255.255.255.0  broadcast 172.20.210.255
        inet6 fe80::43f2:689:c837:3f8c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:09:7b:95  txqueuelen 1000  (Ethernet)
        RX packets 10577  bytes 10282229 (10.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7268  bytes 830056 (830.0 KB)
        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 2250  bytes 276194 (276.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2250  bytes 276194 (276.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@ubuntu:~$ 
```



Specify the destination you want to connect to

Host Name (or IP address):

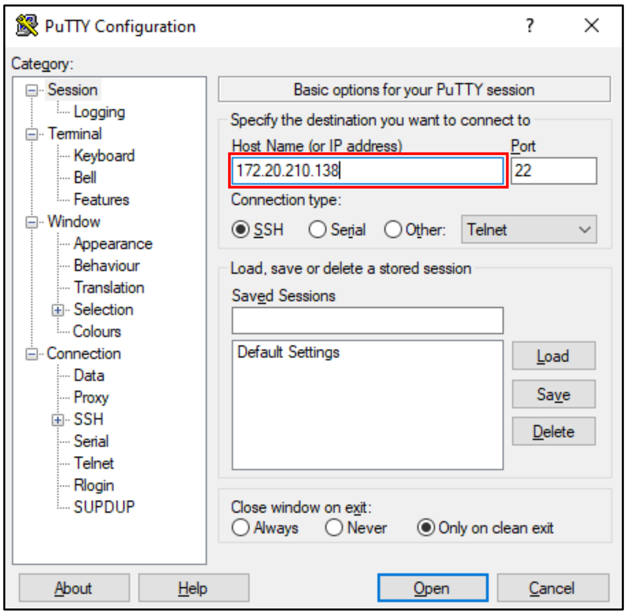
Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit



Specify the destination you want to connect to

Host Name (or IP address): 172.20.210.138

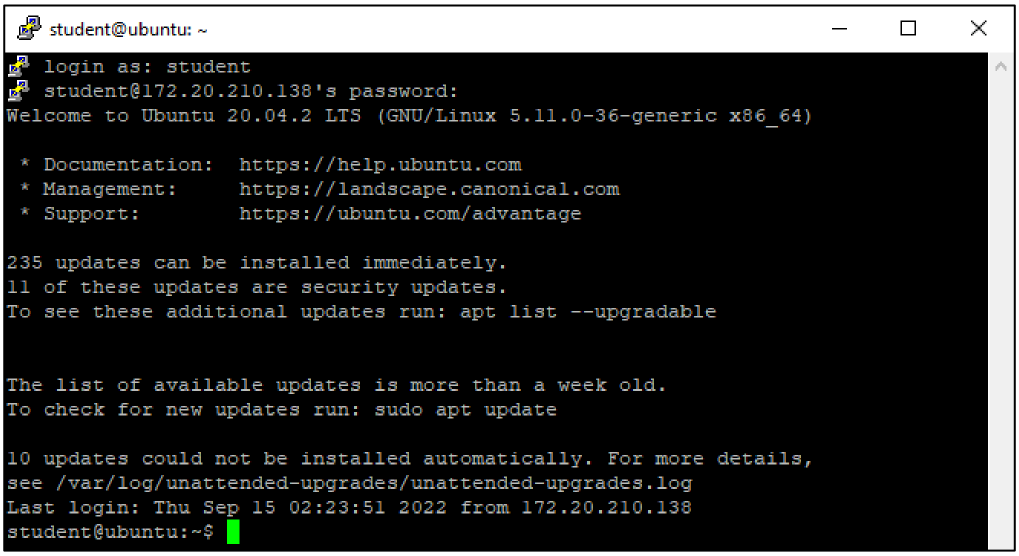
Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

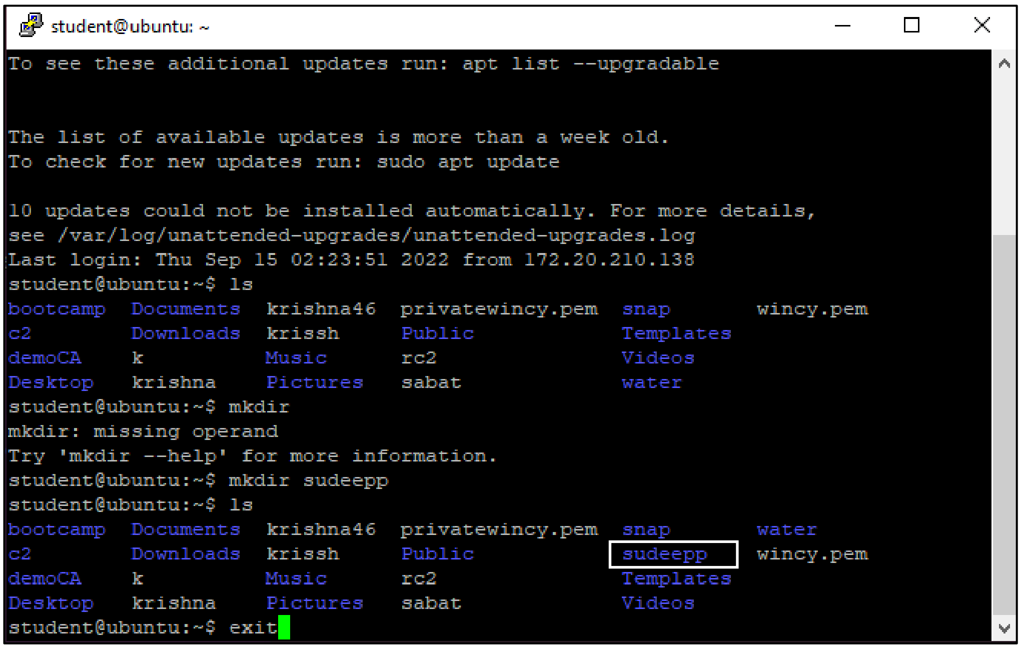
Load, save or delete a stored session

Saved Sessions: Default Settings

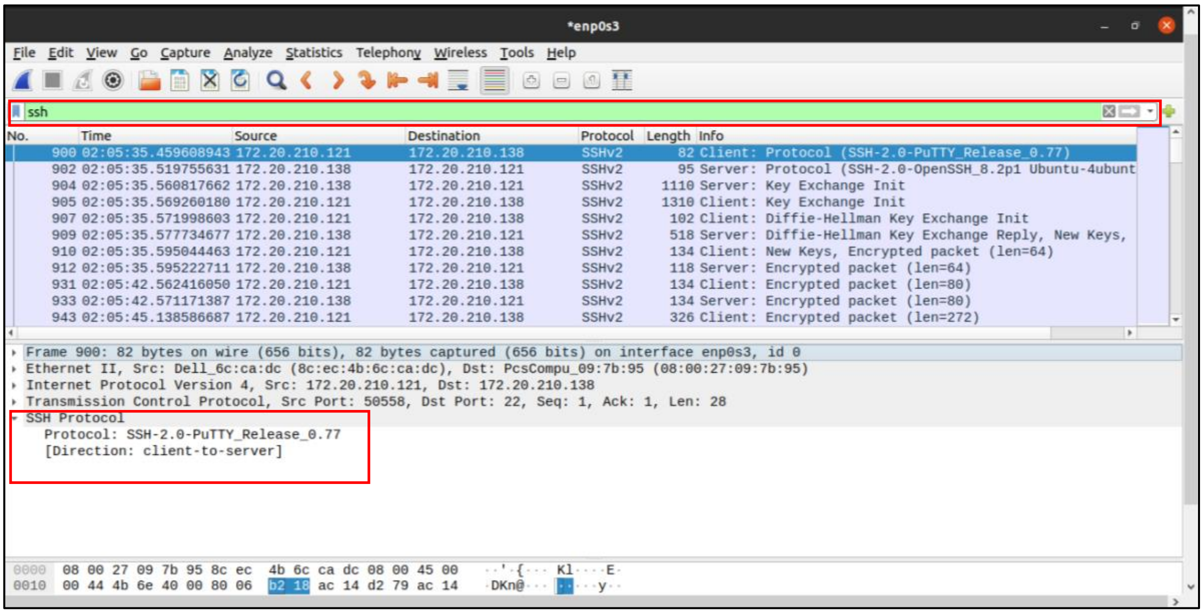
Close window on exit: ○ Always ○ Never ● Only on clean exit



```
login as: student
student@172.20.210.138's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.11.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

235 updates can be installed immediately.
11 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

10 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Thu Sep 15 02:23:51 2022 from 172.20.210.138
student@ubuntu:~$
```



```
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

10 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Thu Sep 15 02:23:51 2022 from 172.20.210.138
student@ubuntu:~$ ls
bootcamp  Documents  krishna46  privatewincy.pem  snap       wincy.pem
c2        Downloads  krissh     Public            Templates
demoCA    k          Music      rc2               Videos
Desktop   krishna    Pictures   sabat             water
student@ubuntu:~$ mkdir
mkdir: missing operand
Try 'mkdir --help' for more information.
student@ubuntu:~$ mkdir sudeepp
student@ubuntu:~$ ls
bootcamp  Documents  krishna46  privatewincy.pem  snap       water
c2        Downloads  krissh     Public            sudeepp    wincy.pem
demoCA    k          Music      rc2               Templates
Desktop   krishna    Pictures   sabat             Videos
student@ubuntu:~$ exit
```


*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ssh
```

```
No.  Time               Source          Destination     Protocol Length Info
 900 02:05:35.459608943 172.20.210.121  172.20.210.138  SSHv2       82 Client: Protocol (SSH-2.0-PuTTY_Release_0.77)
 902 02:05:35.519755631 172.20.210.138  172.20.210.121  SSHv2       95 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubunt
 904 02:05:35.560817662 172.20.210.138  172.20.210.121  SSHv2     1110 Server: Key Exchange Init
 905 02:05:35.569260180 172.20.210.121  172.20.210.138  SSHv2     1310 Client: Key Exchange Init
 907 02:05:35.571998603 172.20.210.121  172.20.210.138  SSHv2      102 Client: Diffie-Hellman Key Exchange Init
 909 02:05:35.577734677 172.20.210.138  172.20.210.121  SSHv2      518 Server: Diffie-Hellman Key Exchange Reply, New Keys,
 910 02:05:35.595044463 172.20.210.121  172.20.210.138  SSHv2      134 Client: New Keys, Encrypted packet (len=64)
 912 02:05:35.595222711 172.20.210.138  172.20.210.121  SSHv2      118 Server: Encrypted packet (len=64)
 931 02:05:42.562416050 172.20.210.121  172.20.210.138  SSHv2      134 Client: Encrypted packet (len=80)
 933 02:05:42.571171387 172.20.210.138  172.20.210.121  SSHv2      134 Server: Encrypted packet (len=80)
 943 02:05:45.138586687 172.20.210.121  172.20.210.138  SSHv2      326 Client: Encrypted packet (len=272)
```

```
▸ Frame 900: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: Dell_6c:ca:dc (8c:ec:4b:6c:ca:dc), Dst: PcsCompu_09:7b:95 (08:00:27:09:7b:95)
▸ Internet Protocol Version 4, Src: 172.20.210.121, Dst: 172.20.210.138
▸ Transmission Control Protocol, Src Port: 50558, 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 09 7b 95 8c ec  4b 6c ca dc 08 00 45 00   ··'·{··· Kl····E·
0010  00 44 4b 6e 40 00 80 06  b2 18 ac 14 d2 79 ac 14   ·DKn@··· ·····y··
```