

Computer Networks Laboratory Week 1

Name : Tanishq Vyas
SRN : PES1201800125
Section : H
Semester : 5
Branch : CSE

TASK 1 : Linux Interface Configuration (ifconfig / IP command)

Interface Name	Ip Address	MAC Address
wlo1	192.168.43.249	ff:ff:ff:ff:ff:ff
lo	127.0.0.1	00:00:00:00:00:00

```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL: ~  
File Edit View Search Terminal Help  
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ifconfig  
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 17649 bytes 344747132 (344.7 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 17649 bytes 344747132 (344.7 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.43.249 netmask 255.255.255.0 broadcast 192.168.43.255  
    inet6 fe80::26ff:3f31:9d06:3737 prefixlen 64 scopeid 0x20<link>  
    inet6 2401:4900:16d9:3a87:e8b5:c671:2561:ab9c prefixlen 64 scopeid 0x0<global>  
    inet6 2401:4900:16d9:3a87:b44:9a52:b78c:1484 prefixlen 64 scopeid 0x0<global>  
    ether 24:ee:9a:e3:6b:10 txqueuelen 1000 (Ethernet)  
    RX packets 387458 bytes 476067770 (476.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 181367 bytes 92182401 (92.1 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ifconfig wlo1 10.0.8.4 netmask 255.255.255.  
0  
[sudo] password for tanishq:  
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ifconfig  
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 17661 bytes 344748104 (344.7 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 17661 bytes 344748104 (344.7 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.8.4 netmask 255.255.255.0 broadcast 10.0.8.255  
    inet6 fe80::26ff:3f31:9d06:3737 prefixlen 64 scopeid 0x20<link>  
    inet6 2401:4900:16d9:3a87:e8b5:c671:2561:ab9c prefixlen 64 scopeid 0x0<global>  
    inet6 2401:4900:16d9:3a87:b44:9a52:b78c:1484 prefixlen 64 scopeid 0x0<global>  
    ether 24:ee:9a:e3:6b:10 txqueuelen 1000 (Ethernet)  
    RX packets 387460 bytes 476068077 (476.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 181378 bytes 92184957 (92.1 MB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```

```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL: ~
File Edit View Search Terminal Help
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ifconfig wlo1 down
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ifconfig
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 17872 bytes 344868530 (344.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17872 bytes 344868530 (344.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo ifconfig wlo1 up
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ifconfig
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 17882 bytes 344869095 (344.8 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17882 bytes 344869095 (344.8 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.8.4 netmask 255.255.255.0 broadcast 10.0.8.255
    ether 24:ee:9a:e3:6b:10 txqueuelen 1000 (Ethernet)
    RX packets 387478 bytes 476070662 (476.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 181422 bytes 92191641 (92.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ip neigh
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```

TASK 2 : Ping PDU (Packet Data Units or Packets) Capture

Details	First Echo Request	First Echo Reply
Frame Number	3	4
Source IP address	10.0.8.4	10.0.8.4
Destination IP address	10.0.8.4	10.0.8.4
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	Version 4	Version 4
Time To Live (TTL) Value	64	64

```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL: ~  
File Edit View Search Terminal Help  
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ping -c 5 10.0.8.4  
PING 10.0.8.4 (10.0.8.4) 56(84) bytes of data:  
64 bytes from 10.0.8.4: icmp_seq=1 ttl=64 time=0.023 ms  
64 bytes from 10.0.8.4: icmp_seq=2 ttl=64 time=0.084 ms  
64 bytes from 10.0.8.4: icmp_seq=3 ttl=64 time=0.060 ms  
64 bytes from 10.0.8.4: icmp_seq=4 ttl=64 time=0.064 ms  
64 bytes from 10.0.8.4: icmp_seq=5 ttl=64 time=0.067 ms  
--- 10.0.8.4 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4075ms  
rtt min/avg/max/mdev = 0.023/0.059/0.084/0.021 ms  
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```


Wireshark - Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>/

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.4	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
2	0.00014184	127.0.0.1	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
3	4.94014523	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=1/256, ttl=64 (reply in 4)
4	4.940154050	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=2/512, ttl=64 (reply in 6)
5	5.943498103	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=2/512, ttl=64 (reply in 5)
6	5.943525122	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=3/768, ttl=64 (reply in 7)
7	6.967749183	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=4/1024, ttl=64 (reply in 10)
8	6.967765507	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=4/1024, ttl=64 (reply in 9)
9	7.991966695	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (request in 13)
10	7.991986142	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (request in 13)
11	8.002502848	10.0.0.4	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
12	8.002631859	127.0.0.1	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
13	9.016117841	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (reply in 14)
14	9.016137012	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (reply in 13)
15	24.00027067	10.0.0.4	224.0.0.251	MDNS	107	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
16	24.000316032	127.0.0.1	224.0.0.251	MDNS	107	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
17	17.173409800	127.0.0.1	127.0.0.1	TCP	76	2251 -> 4369 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=2262706077 TSecr=0 WS=256
18	17.173472666	127.0.0.1	127.0.0.1	TCP	76	4369 -> 2251 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=2262706077 TSecr=2262706077 WS=256
19	17.173474037	127.0.0.1	127.0.0.1	TCP	68	2251 -> 4369 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2262706077 TSecr=2213606444
20	17.173480919	127.0.0.1	127.0.0.1	EPMD	77	EPMD_PORT2_REQ rabbit
21	17.173480920	127.0.0.1	127.0.0.1	TCP	68	4369 -> 2251 [ACK] Seq=1 Ack=10 Win=65536 Len=0 TSval=2213606444 TSecr=2262706077
22	17.173493849	127.0.0.1	127.0.0.1	EPMD	88	EPMD_PORT2_RESP OK rabbit port=25672
23	17.173493849	127.0.0.1	127.0.0.1	TCP	68	2251 -> 4369 [ACK] Seq=10 Ack=21 Win=65536 Len=0 TSval=2262706077 TSecr=2213606444
24	17.173493849	127.0.0.1	127.0.0.1	TCP	68	4369 -> 2251 [FIN, ACK] Seq=21 Ack=10 Win=65536 Len=0 TSval=2213606444 TSecr=2262706077
25	17.1735067350	127.0.0.1	127.0.0.1	TCP	68	2251 -> 4369 [FIN, ACK] Seq=10 Ack=22 Win=65536 Len=0 TSval=2262706077 TSecr=2213606444
26	17.1735081742	127.0.0.1	127.0.0.1	TCP	68	4369 -> 2251 [ACK] Seq=22 Ack=11 Win=65536 Len=0 TSval=2213606444 TSecr=2262706077

Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0

- Linux cooked capture
- Internet Protocol Version 4, Src: 10.0.0.4, Dst: 224.0.0.251
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (query)

0000 00 04 00 01 00 06 24 ee 5a e3 0b 10 00 00 00 00\$..k:....
0010 45 00 00 44 ff ea 40 00 ff 11 a0 be 0a 00 00 04 E-D-@
any: <live capture in progress>

Packets: 26 - Displayed: 26 (100.0%) Profile: Default

Wireshark - Packet 3 - any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>/

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.4	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
2	0.00014184	127.0.0.1	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
3	4.94014523	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=1/256, ttl=64 (reply in 4)
4	4.940154050	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=2/512, ttl=64 (reply in 6)
5	5.943498103	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=2/512, ttl=64 (reply in 5)
6	5.943525122	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=3/768, ttl=64 (reply in 7)
7	6.967749183	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=4/1024, ttl=64 (reply in 10)
8	6.967765507	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=4/1024, ttl=64 (reply in 9)
9	7.991966695	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (request in 13)
10	7.991986142	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (request in 13)
11	8.002502848	10.0.0.4	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
12	8.002631859	127.0.0.1	224.0.0.251	MDNS	84	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
13	9.016117841	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (reply in 14)
14	9.016137012	10.0.0.4	10.0.0.4	ICMP	100	Echo (ping) request id=0x2851, seq=5/1280, ttl=64 (reply in 13)
15	24.00027067	10.0.0.4	224.0.0.251	MDNS	107	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
16	24.000316032	127.0.0.1	224.0.0.251	MDNS	107	Standard query 0x0000 PTR _pgkey-hkp._tcp.local, "QM" question
17	17.173409800	127.0.0.1	127.0.0.1	TCP	76	2251 -> 4369 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=2262706077 TSecr=0 WS=256
18	17.173472666	127.0.0.1	127.0.0.1	TCP	76	4369 -> 2251 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=2262706077 TSecr=2262706077 WS=256
19	17.173474037	127.0.0.1	127.0.0.1	TCP	68	2251 -> 4369 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2262706077 TSecr=2213606444
20	17.173480919	127.0.0.1	127.0.0.1	EPMD	77	EPMD_PORT2_REQ rabbit
21	17.173480920	127.0.0.1	127.0.0.1	TCP	68	4369 -> 2251 [ACK] Seq=1 Ack=10 Win=65536 Len=0 TSval=2213606444 TSecr=2262706077
22	17.173493849	127.0.0.1	127.0.0.1	EPMD	88	EPMD_PORT2_RESP OK rabbit port=25672
23	17.173493849	127.0.0.1	127.0.0.1	TCP	68	2251 -> 4369 [ACK] Seq=10 Ack=21 Win=65536 Len=0 TSval=2262706077 TSecr=2213606444
24	17.173493849	127.0.0.1	127.0.0.1	TCP	68	4369 -> 2251 [FIN, ACK] Seq=21 Ack=10 Win=65536 Len=0 TSval=2213606444 TSecr=2262706077
25	17.1735067350	127.0.0.1	127.0.0.1	TCP	68	2251 -> 4369 [FIN, ACK] Seq=10 Ack=22 Win=65536 Len=0 TSval=2262706077 TSecr=2213606444
26	17.1735081742	127.0.0.1	127.0.0.1	TCP	68	4369 -> 2251 [ACK] Seq=22 Ack=11 Win=65536 Len=0 TSval=2213606444 TSecr=2262706077

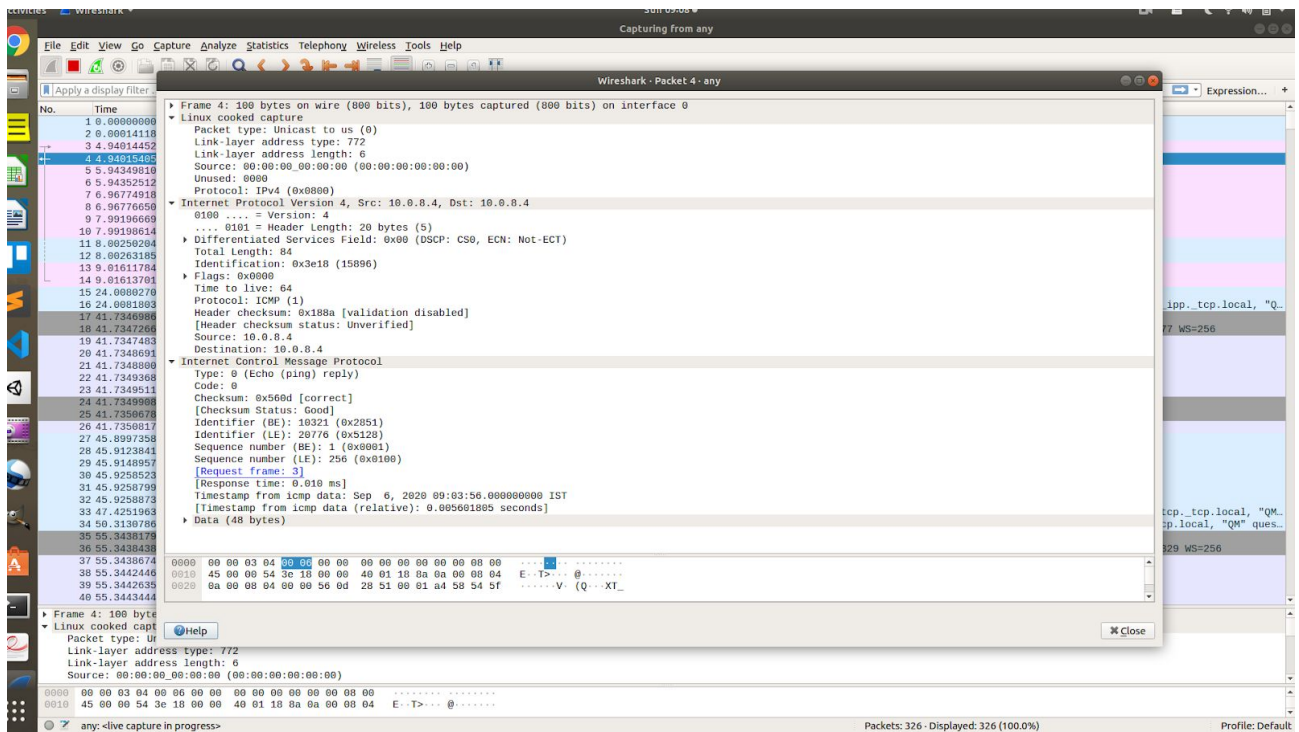
Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0

- Linux cooked capture
- Packet type: Unicast to us (0)
- Link-layer address type: 772
- Link-layer address length: 6
- Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Unused: 0000
- Protocol: IPv4 (0x0000)
- Internet Protocol Version 4, Src: 10.0.0.4, Dst: 10.0.0.4
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total length: 84
- Identification: 0x3e17 (15895)
- Flags: 0x4000, Don't fragment
- Time to live: 64
- Protocol: ICMP (1)
- Header checksum: 0xd88a [validation disabled]
- [Header checksum status: Unverified]
- Source: 10.0.0.4
- Destination: 10.0.0.4
- Internet Control Message Protocol
- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x4e0d [correct]
- [Checksum Status: Good]
- Identifier (BE): 10321 (0x2851)
- Identifier (LE): 20776 (0x5120)
- Sequence number (BE): 1 (0x0001)
- Sequence number (LE): 256 (0xd100)
- [Response frame: 4]
- Timestamp from icmp data: Sep 6, 2020 09:03:56.000000000 IST
- [Timestamp from icmp data (relative): 0.005592278 seconds]
- Data (48 bytes)

0000 00 00 03 04 00 00 00 00 00 00 00 00 00 00 00
0010 45 00 00 54 3e 17 40 00 00 00 00 00 00 00 00 E-T->@
0020 0a 00 08 04 00 00 4e 0d 28 51 00 01 a4 50 54 5fN(Q...XT..
0030 00 00 00 00 ca 15 00 00 00 00 00 10 11 12 13I*.....
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23P*.....
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 %&'()*+,-./0123

any: <live capture in progress>

Packets: 310 - Displayed: 310 (100.0%) Profile: Default



TASK 3 : HTTP PDU Capture

Details	First Echo Request	First Echo Reply
Frame Number	360	362
Source Port	5596	80
Destination Port	80	5596
Source IP address	192.168.43.249	15.207.162.112
Destination IP address	15.207.162.112	192.168.43.249
Source Ethernet Address	24:ee:9a:e3:6b:10	18:f0:e4:87:c1:81
Destination Ethernet Address	18:f0:e4:87:c1:81	24:ee:9a:e3:6b:10

HTTP Request		HTTP Response	
Get	GET / HTTP/1.1\r\n	Server	nginx/1.18.0\r\n
Host	www.freeclan.net\r\n	Content-Type	NA
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36\r\n	Date	Sun, 06 Sep 2020 03:48:54 GMT\r\n
Accept-Language	en-GB,en-US;q=0.9,en;q=0.8\r\n	Location	http://www.freeclan.net/
Accept-Encoding	gzip, deflate\r\n	Content-Length	NA
Connection	keep-alive\r\n	Connection	keep-alive\r\n

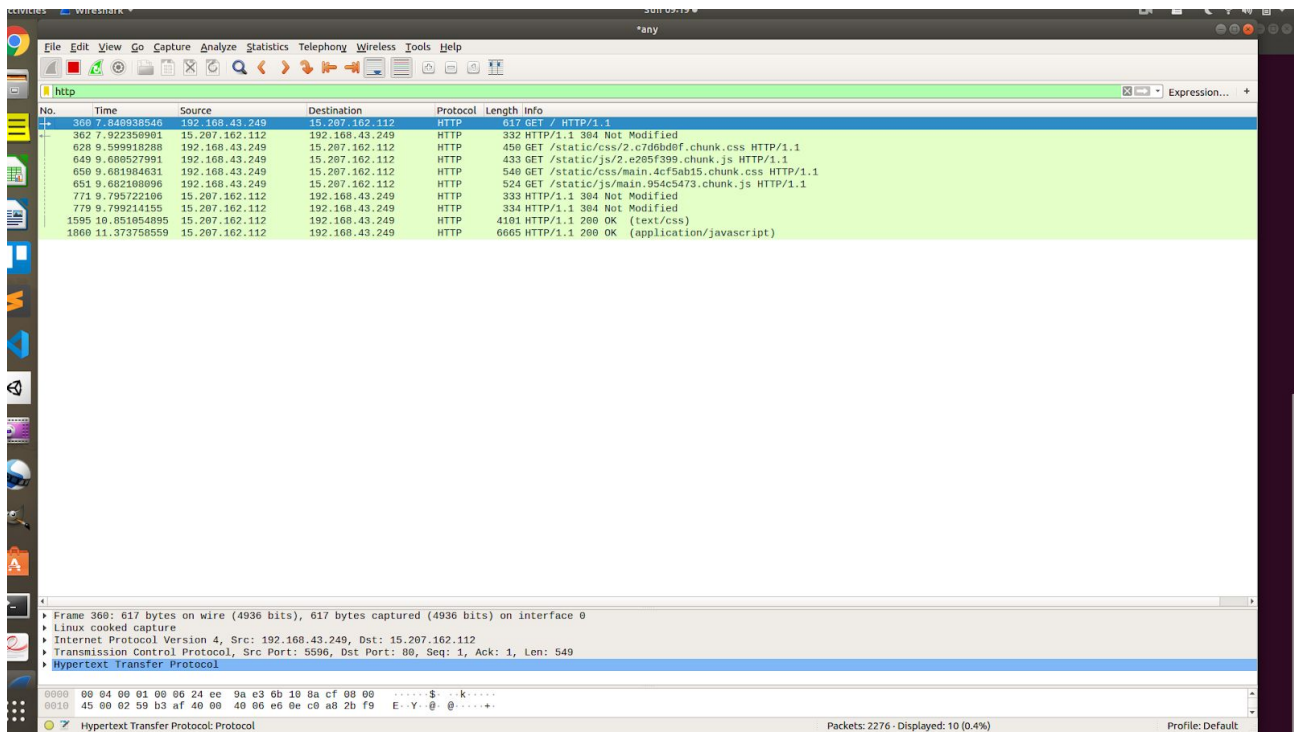


Fig : HTTP Filter for website

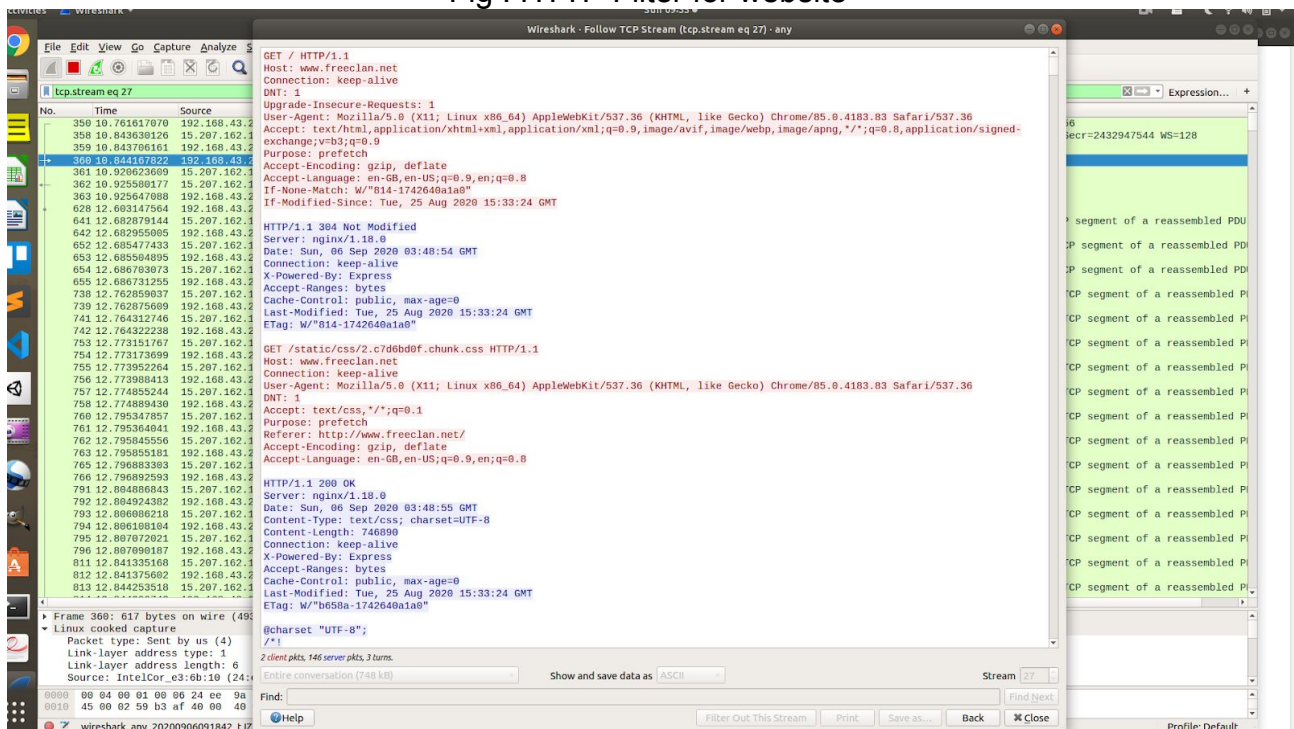


Fig : Follow TCP Stream

TASK 4 : Capturing packets with tcpdump

```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ ping -c 5 192.168.43.249
PING 192.168.43.249 (192.168.43.249) 56(84) bytes of data:
64 bytes from 192.168.43.249: icmp_seq=1 ttl=64 time=0.082 ms
64 bytes from 192.168.43.249: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 192.168.43.249: icmp_seq=3 ttl=64 time=0.091 ms
64 bytes from 192.168.43.249: icmp_seq=4 ttl=64 time=0.089 ms
64 bytes from 192.168.43.249: icmp_seq=5 ttl=64 time=0.080 ms

--- 192.168.43.249 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 408.0ms
rtt min/avg/max/ndev = 0.080/0.086/0.091/0.007 ms
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```

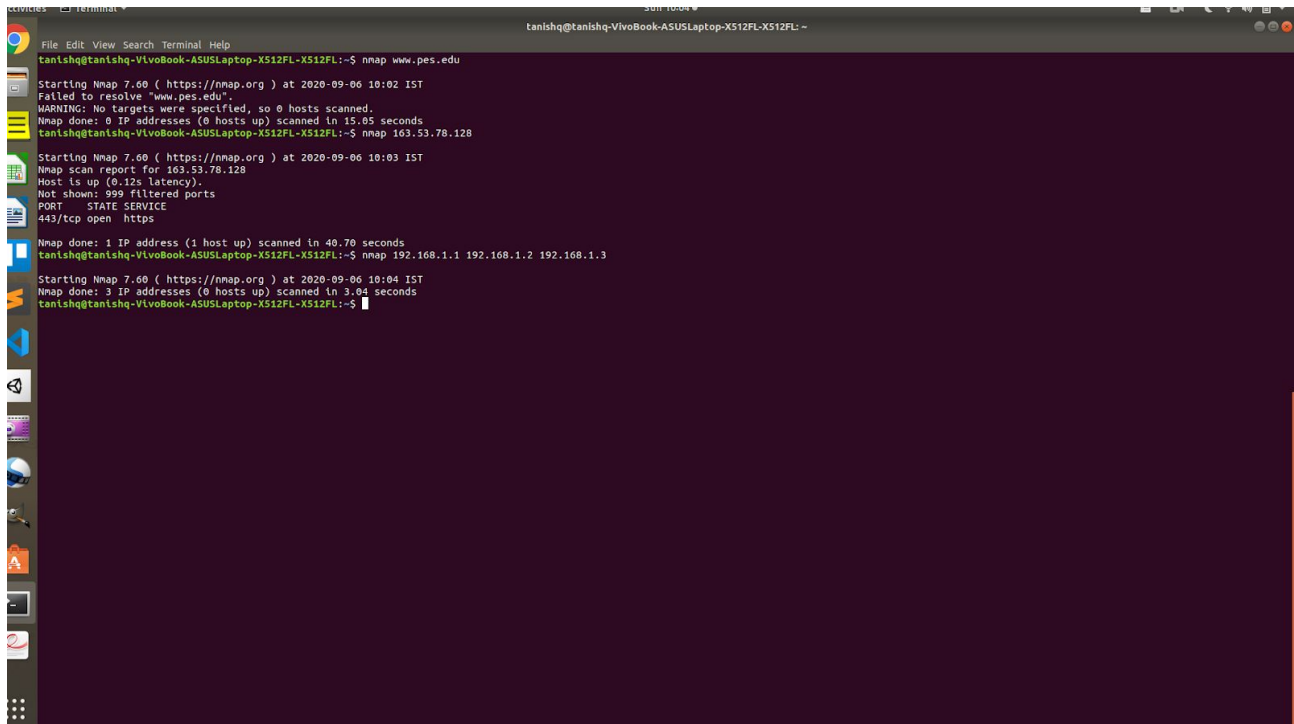
```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
09:38:11.821860 IP localhost.13065 > tanishq-VivoBook-ASUSLaptop-X512FL-X512FL.epmd: Flags [S], seq 6
8577644, win 65495, options [mss 65495,sackOK,TS val 2264726437 ecr 0,nop,wscale 8], length 0
09:38:13.821829 IP tanishq-VivoBook-ASUSLaptop-X512FL-X512FL.epmd > localhost.13065: Flags [S], seq
1504387896, ack 68577645, win 65483, options [mss 65495,sackOK,TS val 2215626804 ecr 2264726437,nop,
wscale 8], length 0
09:38:13.821849 IP localhost.13065 > tanishq-VivoBook-ASUSLaptop-X512FL-X512FL.epmd: Flags [R], ack 1
, win 256, options [nop,nop,TS val 2264726437 ecr 2215626804], length 0
09:38:13.821952 IP localhost.13065 > tanishq-VivoBook-ASUSLaptop-X512FL-X512FL.epmd: Flags [P], seq
1:40, ack 1, win 256, options [nop,nop,TS val 2264726437 ecr 2215626804], length 9
09:38:39.272997 IP localhost.33907 > localhost.33907: UDP, length 32
09:38:39.285043 IP localhost.33907 > localhost.33907: UDP, length 24
09:38:39.287480 IP localhost.33907 > localhost.33907: UDP, length 32
09:38:39.299851 IP localhost.33907 > localhost.33907: UDP, length 936
09:38:39.299881 IP localhost.33907 > localhost.33907: UDP, length 376
09:38:39.299891 IP localhost.33907 > localhost.33907: UDP, length 488
09:38:44.114339 IP localhost.ircs-u > localhost.9618: Flags [P], seq 3295165174:3295166798, ack 2281
918009, win 256, options [nop,nop,TS val 2230822372 ecr 2230822316], length 1624
09:38:44.114382 IP localhost.9618 > localhost.ircs-u: Flags [R], ack 1624, win 251, options [nop,nop,
TS val 2230822372 ecr 2230822372], length 0
09:38:46.579502 IP localhost.20735 > localhost.9618: Flags [P], seq 2201954737:2201958701, ack 27620
4653, win 256, options [nop,nop,TS val 2230824837 ecr 2230524589], length 3964
09:38:46.579531 IP localhost.9618 > localhost.20735: Flags [R], ack 3964, win 246, options [nop,nop,T
S val 2230824837 ecr 2230824837], length 0
09:38:47.121014 IP localhost.17857 > localhost.9618: Flags [P], seq 3391091790:3391095886, ack 85730
708, win 256, options [nop,nop,TS val 2230825379 ecr 2230525106], length 4096
09:38:47.121044 IP localhost.9618 > localhost.17857: Flags [R], ack 4096, win 246, options [nop,nop,T
S val 2230825379 ecr 2230825379], length 0
09:38:47.121145 IP localhost.17857 > localhost.9618: Flags [P], seq 4096:6123, ack 1, win 256, optio
ns [nop,nop,TS val 2230825379 ecr 2230825379], length 2027
09:38:47.121155 IP localhost.9618 > localhost.17857: Flags [R], ack 6123, win 242, options [nop,nop,T
S val 2230825379 ecr 2230825379], length 0
09:38:47.126063 IP localhost.33255 > localhost.9618: Flags [P], seq 147985604:147989700, ack 4056274
737, win 256, options [nop,nop,TS val 2230825384 ecr 2230526159], length 4096
09:38:47.126077 IP localhost.9618 > localhost.33255: Flags [R], ack 4096, win 246, options [nop,nop,T
S val 2230825384 ecr 2230825384], length 0
09:38:47.126124 IP localhost.33255 > localhost.9618: Flags [P], seq 4096:5103, ack 1, win 256, optio
ns [nop,nop,TS val 2230825384 ecr 2230825384], length 1007
09:38:47.126129 IP localhost.9618 > localhost.33255: Flags [R], ack 5103, win 244, options [nop,nop,T
S val 2230825384 ecr 2230825384], length 0
09:38:47.126738 IP localhost.33255 > localhost.9618: Flags [P], seq 5103:9199, ack 1, win 256, optio
ns [nop,nop,TS val 2230825385 ecr 2230825384], length 4096
09:38:47.126746 IP localhost.9618 > localhost.33255: Flags [R], ack 9199, win 246, options [nop,nop,T
S val 2230825385 ecr 2230825385], length 0
09:38:47.126790 IP localhost.33255 > localhost.9618: Flags [P], seq 9199:10168, ack 1, win 256, opti
ons [nop,nop,TS val 2230825385 ecr 2230825385], length 969
09:38:47.126818 IP localhost.9618 > localhost.33255: Flags [R], ack 10168, win 252, options [nop,nop,
TS val 2230825385 ecr 2230825385], length 0
09:38:47.127329 IP localhost.33255 > localhost.9618: Flags [P], seq 10168:14264, ack 1, win 256, opti
ons [nop,nop,TS val 2230825385 ecr 2230825385], length 4096
09:38:47.127335 IP localhost.9618 > localhost.33255: Flags [R], ack 14264, win 246, options [nop,nop,
TS val 2230825385 ecr 2230825385], length 0
09:38:47.127375 IP localhost.33255 > localhost.9618: Flags [P], seq 14264:15233, ack 1, win 256, opti
ons [nop,nop,TS val 2230825385 ecr 2230825385], length 969
```

Task 5: Perform Traceroute checks

```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (172.217.26.164), 30 hops max, 60 byte packets
 1 _gateway (192.168.43.1) 24.153 ms 24.301 ms 24.754 ms
 2 * * *
 3 10.40.19.125 (10.40.19.125) 151.990 ms 152.024 ms 152.024 ms
 4 * * *
 5 * * *
 6 * * *
 7 72.14.213.254 (72.14.213.254) 55.842 ms 40.169 ms 50.683 ms
 8 108.170.248.209 (108.170.248.209) 50.619 ms 74.125.37.81 (74.125.37.81) 50.643 ms 108.170.248.2
09 (108.170.248.209) 77.912 ms
 9 * 108.170.248.178 (108.170.248.178) 85.084 ms *
10 72.14.236.175 (72.14.236.175) 117.257 ms 209.85.251.243 (209.85.251.243) 70.551 ms *
11 172.253.72.136 (172.253.72.136) 82.711 ms * *
12 108.170.253.97 (108.170.253.97) 92.271 ms 108.170.253.113 (108.170.253.113) 94.162 ms 92.125 m
s
13 naa03s22-in-f4.1e100.net (172.217.26.164) 92.402 ms 95.718 ms 95.233 ms
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```

```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo traceroute www.google.com
traceroute to www.google.com (172.217.27.196), 30 hops max, 60 byte packets
 1 _gateway (192.168.43.1) 24.005 ms 24.273 ms 24.558 ms
 2 * * *
 3 10.40.19.125 (10.40.19.125) 95.927 ms 100.191 ms 100.146 ms
 4 10.50.73.185 (10.50.73.185) 95.817 ms 95.826 ms 95.811 ms
 5 dsl-tn-dynamic-145.222.22.125.airtelbroadband.in (125.22.222.145) 92.822 ms 92.795 ms 92.746 m
s
 6 182.79.239.147 (182.79.239.147) 125.506 ms 182.79.177.109 (182.79.177.109) 50.824 ms 182.79.239
.147 (182.79.239.147) 50.638 ms
 7 72.14.213.254 (72.14.213.254) 62.736 ms 62.651 ms 62.670 ms
 8 10.252.57.158 (10.252.57.158) 62.613 ms 10.252.57.126 (10.252.57.126) 62.668 ms 10.252.57.158 (
10.252.57.158) 62.826 ms
 9 209.85.252.52 (209.85.252.52) 63.016 ms 209.85.246.4 (209.85.246.4) 62.907 ms bon07s15-in-f4.1e
100.net (172.217.27.196) 62.945 ms
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (172.217.26.164), 30 hops max, 60 byte packets
 1 _gateway (192.168.43.1) 2.963 ms 2.955 ms 3.603 ms
 2 * * *
 3 10.40.19.125 (10.40.19.125) 75.890 ms 75.974 ms 76.356 ms
 4 10.50.73.185 (10.50.73.185) 77.213 ms 77.460 ms 77.225 ms
 5 dsl-tn-dynamic-145.222.22.125.airtelbroadband.in (125.22.222.145) 62.536 ms 76.515 ms 75.802 m
s
 6 182.79.142.154 (182.79.142.154) 77.654 ms 55.218 ms 56.211 ms
 7 72.14.213.254 (72.14.213.254) 55.810 ms 95.708 ms 95.749 ms
 8 108.170.248.177 (108.170.248.177) 95.714 ms 96.008 ms 96.218 ms
 9 108.170.248.179 (108.170.248.179) 93.401 ms 96.800 ms 97.351 ms
10 172.253.74.113 (172.253.74.113) 98.587 ms 98.250 ms 78.894 ms
11 172.253.72.136 (172.253.72.136) 78.108 ms 77.927 ms 77.124 ms
12 108.170.253.113 (108.170.253.113) 74.910 ms 74.773 ms 118.170 ms
13 74.125.253.65 (74.125.253.65) 118.450 ms 117.899 ms 117.473 ms
14 naa03s22-in-f4.1e100.net (172.217.26.164) 117.334 ms 115.421 ms 116.363 ms
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (172.217.27.196), 30 hops max, 60 byte packets
 1 192.168.43.1 2.818 ms 3.557 ms 3.746 ms
 2 * * *
 3 10.40.19.125 75.808 ms 75.830 ms 75.814 ms
 4 10.50.73.185 73.453 ms 73.529 ms 115.104 ms
 5 125.22.222.145 115.033 ms 115.022 ms 115.373 ms
 6 182.79.142.121 115.387 ms 116.119.44.123 112.653 ms 182.79.224.134 111.855 ms
 7 72.14.213.254 111.201 ms 46.495 ms 46.384 ms
 8 10.252.211.190 83.031 ms 10.252.109.158 82.965 ms 10.23.206.62 82.940 ms
 9 108.170.234.208 79.102 ms 108.170.248.177 86.108 ms 142.250.60.134 85.927 ms
10 216.239.56.35 86.305 ms 86.114 ms 216.239.56.115 85.836 ms
11 172.217.27.196 85.581 ms 108.170.248.193 85.531 ms 108.170.248.209 81.586 ms
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```

Task 6: Explore an entire network for information (Nmap)



```
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ nmap www.pes.edu
Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-06 10:02 IST
Failed to resolve "www.pes.edu".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 15.05 seconds
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ nmap 163.53.78.128
Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-06 10:03 IST
Nmap scan report for 163.53.78.128
Host is up (0.12s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 40.70 seconds
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.60 ( https://nmap.org ) at 2020-09-06 10:04 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.04 seconds
tanishq@tanishq-VivoBook-ASUSLaptop-X512FL-X512FL:~$
```

Answers :

1. Browser is running HTTP/1.1 and the Server is running HTTP/1.1 version. We see this in the request & response for a given communication between the client and server.

2. **last-modified: Tue, 25 Aug 2020 15:33:24 GMT**

This header helps us to know when the file was last modified.

3. In order to tell ping to send, let's say **N** packets then stop, we make use of **-c** argument.

Eg: To ask ping to stop after 4 packets we will use the command

ping -c 4 mywebsite.com

4. we can make use of **nmap** command in order to get the information for the same

```
$ nmap -O -v server.ip.address
```

This helps us to get the information for the OS and apps.