ASSIGNMENT NO.7

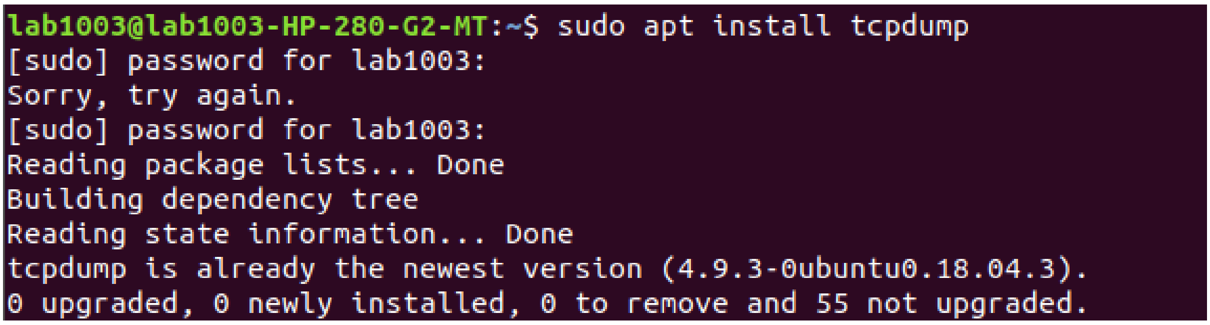
AIM:-

Analysis of packet headers -TCP ,IP,UDP using TCPDUMP

THEORY:-

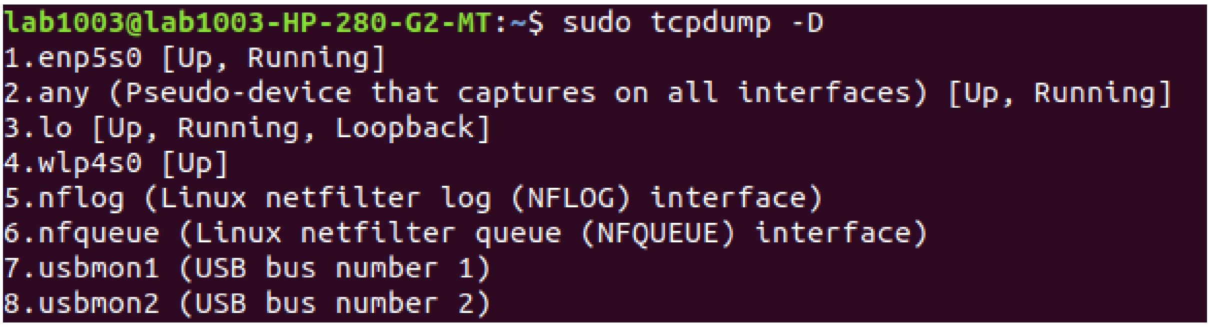
TCP dump is a packet analyser used to capture and analyse network traffic. It operates by intercepting and logging data packets traveling through a network interface. TCP dump can be used for various purposes, including network troubleshooting, security analysis, and protocol debugging. It captures packets in real-time and provides detailed information such as source and destination addresses, protocols, and payload data. TCP dump utilizes a command-line interface and offers various filters and options for capturing specific types of traffic. It is widely used by network administrators and security professionals to monitor and analyse network activity.

How to install “tcpdump”:

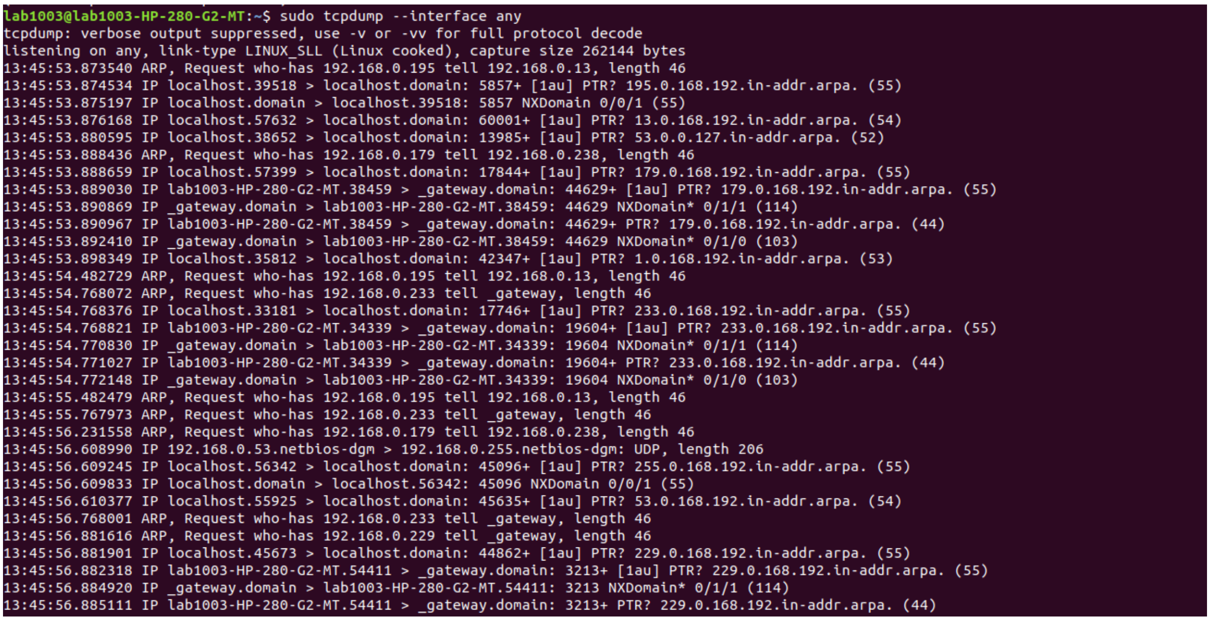


```
lab1003@lab1003-HP-280-G2-MT:~$ sudo apt install tcpdump
[sudo] password for lab1003:
Sorry, try again.
[sudo] password for lab1003:
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-0ubuntu0.18.04.3).
0 upgraded, 0 newly installed, 0 to remove and 55 not upgraded.
```

How to capture packets with tcpdump:

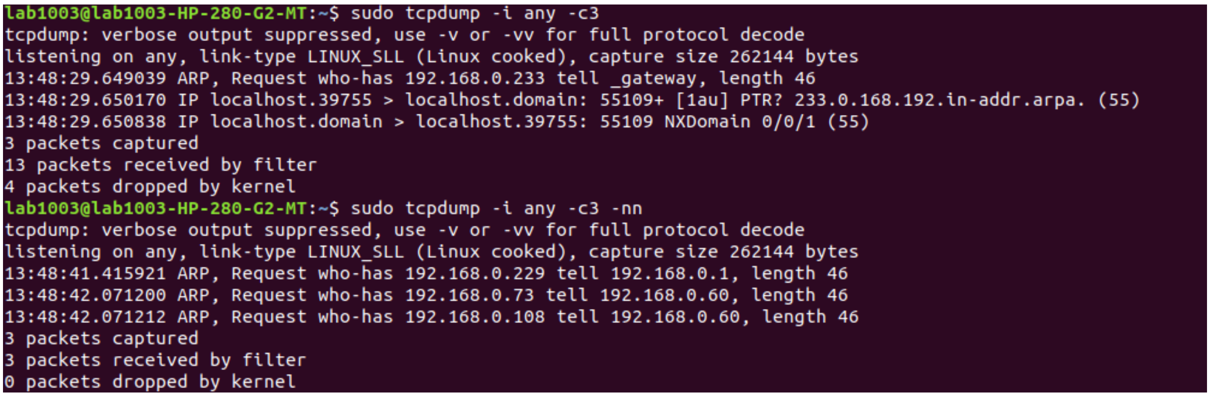


```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -D
1.enp5s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.wlp4s0 [Up]
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```



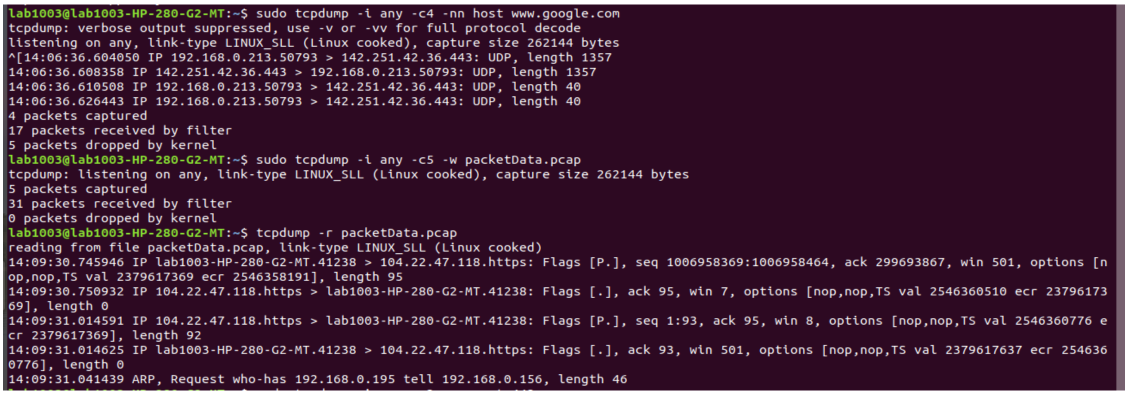
```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump --interface any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
13:45:53.873540 ARP, Request who-has 192.168.0.195 tell 192.168.0.13, length 46
13:45:53.874534 IP localhost.39518 > localhost.domain: 5857+ [1au] PTR? 195.0.168.192.in-addr.arpa. (55)
13:45:53.875197 IP localhost.domain > localhost.39518: 5857 NXDomain 0/0/1 (55)
13:45:53.876168 IP localhost.57632 > localhost.domain: 60001+ [1au] PTR? 13.0.168.192.in-addr.arpa. (54)
13:45:53.880595 IP localhost.38652 > localhost.domain: 13985+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
13:45:53.888436 ARP, Request who-has 192.168.0.179 tell 192.168.0.238, length 46
13:45:53.888659 IP localhost.57399 > localhost.domain: 17844+ [1au] PTR? 179.0.168.192.in-addr.arpa. (55)
13:45:53.889030 IP lab1003-HP-280-G2-MT.38459 > _gateway.domain: 44629+ [1au] PTR? 179.0.168.192.in-addr.arpa. (55)
13:45:53.890869 IP _gateway.domain > lab1003-HP-280-G2-MT.38459: 44629 NXDomain* 0/1/1 (114)
13:45:53.890967 IP lab1003-HP-280-G2-MT.38459 > _gateway.domain: 44629+ PTR? 179.0.168.192.in-addr.arpa. (44)
13:45:53.892410 IP _gateway.domain > lab1003-HP-280-G2-MT.38459: 44629 NXDomain* 0/1/0 (103)
13:45:53.898349 IP localhost.35812 > localhost.domain: 42347+ [1au] PTR? 1.0.168.192.in-addr.arpa. (53)
13:45:54.482729 ARP, Request who-has 192.168.0.195 tell 192.168.0.13, length 46
13:45:54.768072 ARP, Request who-has 192.168.0.233 tell _gateway, length 46
13:45:54.768376 IP localhost.33181 > localhost.domain: 17746+ [1au] PTR? 233.0.168.192.in-addr.arpa. (55)
13:45:54.768821 IP lab1003-HP-280-G2-MT.34339 > _gateway.domain: 19604+ [1au] PTR? 233.0.168.192.in-addr.arpa. (55)
13:45:54.770830 IP _gateway.domain > lab1003-HP-280-G2-MT.34339: 19604 NXDomain* 0/1/1 (114)
13:45:54.771027 IP lab1003-HP-280-G2-MT.34339 > _gateway.domain: 19604+ PTR? 233.0.168.192.in-addr.arpa. (44)
13:45:54.772148 IP _gateway.domain > lab1003-HP-280-G2-MT.34339: 19604 NXDomain* 0/1/0 (103)
13:45:55.482479 ARP, Request who-has 192.168.0.195 tell 192.168.0.13, length 46
13:45:55.767973 ARP, Request who-has 192.168.0.233 tell _gateway, length 46
13:45:56.231558 ARP, Request who-has 192.168.0.179 tell 192.168.0.238, length 46
13:45:56.608990 IP 192.168.0.53.netbios-dgm > 192.168.0.255.netbios-dgm: UDP, length 206
13:45:56.609245 IP localhost.56342 > localhost.domain: 45096+ [1au] PTR? 255.0.168.192.in-addr.arpa. (55)
13:45:56.609833 IP localhost.domain > localhost.56342: 45096 NXDomain 0/0/1 (55)
13:45:56.610377 IP localhost.55925 > localhost.domain: 45635+ [1au] PTR? 53.0.168.192.in-addr.arpa. (54)
13:45:56.768001 ARP, Request who-has 192.168.0.233 tell _gateway, length 46
13:45:56.881616 ARP, Request who-has 192.168.0.229 tell _gateway, length 46
13:45:56.881901 IP localhost.45673 > localhost.domain: 44862+ [1au] PTR? 229.0.168.192.in-addr.arpa. (55)
13:45:56.882318 IP lab1003-HP-280-G2-MT.54411 > _gateway.domain: 3213+ [1au] PTR? 229.0.168.192.in-addr.arpa. (55)
13:45:56.884920 IP _gateway.domain > lab1003-HP-280-G2-MT.54411: 3213 NXDomain* 0/1/1 (114)
13:45:56.885111 IP lab1003-HP-280-G2-MT.54411 > _gateway.domain: 3213+ PTR? 229.0.168.192.in-addr.arpa. (44)
```

To capture 3 packets:



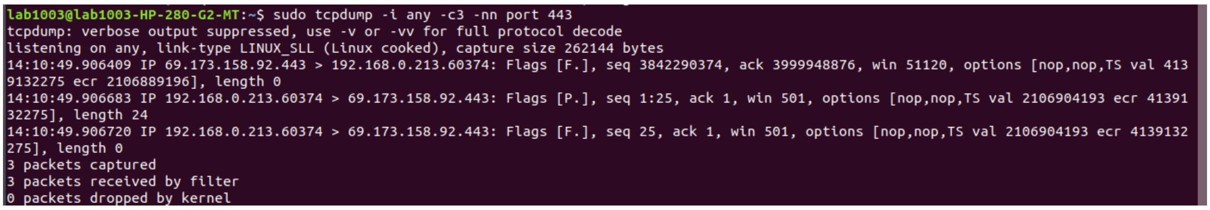
```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
13:48:29.649039 ARP, Request who-has 192.168.0.233 tell _gateway, length 46
13:48:29.650170 IP localhost.39755 > localhost.domain: 55109+ [1au] PTR? 233.0.168.192.in-addr.arpa. (55)
13:48:29.650838 IP localhost.domain > localhost.39755: 55109 NXDomain 0/0/1 (55)
3 packets captured
13 packets received by filter
4 packets dropped by kernel
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c3 -nn
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
13:48:41.415921 ARP, Request who-has 192.168.0.229 tell 192.168.0.1, length 46
13:48:42.071200 ARP, Request who-has 192.168.0.73 tell 192.168.0.60, length 46
13:48:42.071212 ARP, Request who-has 192.168.0.108 tell 192.168.0.60, length 46
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

How to store captured data:



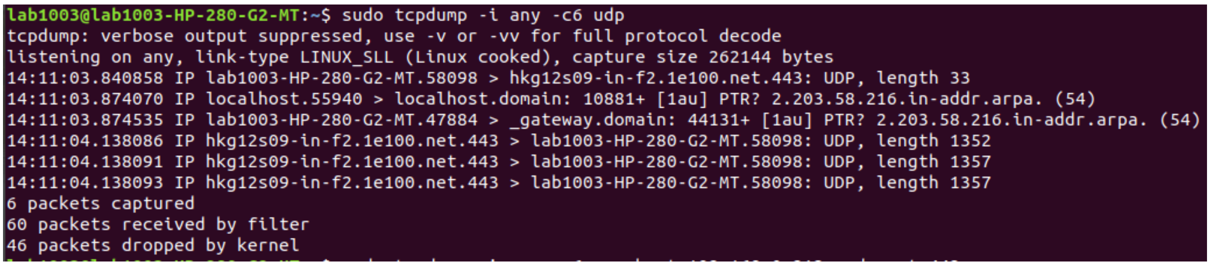
```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c4 -nn host www.google.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
^[14:06:36.604050 IP 192.168.0.213.50793 > 142.251.42.36.443: UDP, length 1357
14:06:36.608358 IP 142.251.42.36.443 > 192.168.0.213.50793: UDP, length 1357
14:06:36.610508 IP 192.168.0.213.50793 > 142.251.42.36.443: UDP, length 40
14:06:36.626443 IP 192.168.0.213.50793 > 142.251.42.36.443: UDP, length 40
4 packets captured
17 packets received by filter
5 packets dropped by kernel
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c5 -w packetData.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
5 packets captured
31 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-HP-280-G2-MT:~$ tcpdump -r packetData.pcap
reading from file packetData.pcap, link-type LINUX_SLL (Linux cooked)
14:09:30.745946 IP lab1003-HP-280-G2-MT.41238 > 104.22.47.118.https: Flags [P.], seq 1006958369:1006958464, ack 299693867, win 501, options [n
op,nop,TS val 2379617369 ecr 2546358191], length 95
14:09:30.750932 IP 104.22.47.118.https > lab1003-HP-280-G2-MT.41238: Flags [.], ack 95, win 7, options [nop,nop,TS val 2546360510 ecr 23796173
69], length 0
14:09:31.014591 IP 104.22.47.118.https > lab1003-HP-280-G2-MT.41238: Flags [P.], seq 1:93, ack 95, win 8, options [nop,nop,TS val 2546360776 e
cr 2379617369], length 92
14:09:31.014625 IP lab1003-HP-280-G2-MT.41238 > 104.22.47.118.https: Flags [.], ack 93, win 501, options [nop,nop,TS val 2379617637 ecr 254636
0776], length 0
14:09:31.041439 ARP, Request who-has 192.168.0.195 tell 192.168.0.156, length 46
```

How to capture a packet using port number with tcpdump command:



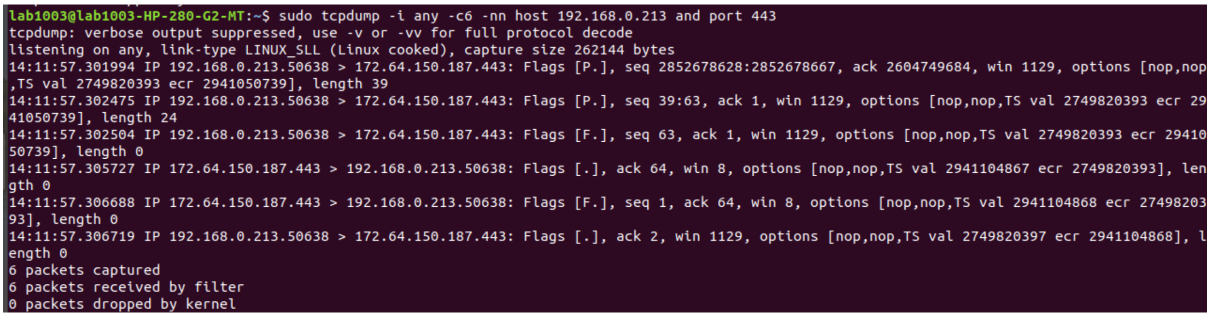
```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c3 -nn port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
14:10:49.906409 IP 69.173.158.92.443 > 192.168.0.213.60374: Flags [F.], seq 3842290374, ack 3999948876, win 51120, options [nop,nop,TS val 413
9132275 ecr 2106889196], length 0
14:10:49.906683 IP 192.168.0.213.60374 > 69.173.158.92.443: Flags [P.], seq 1:25, ack 1, win 501, options [nop,nop,TS val 2106904193 ecr 41391
32275], length 24
14:10:49.906720 IP 192.168.0.213.60374 > 69.173.158.92.443: Flags [F.], seq 25, ack 1, win 501, options [nop,nop,TS val 2106904193 ecr 4139132
275], length 0
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```

How to capture a packet using the protocol with tcpdump command:



```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c6 udp
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
14:11:03.840858 IP lab1003-HP-280-G2-MT.58098 > hkg12s09-in-f2.1e100.net.443: UDP, length 33
14:11:03.874070 IP localhost.55940 > localhost.domain: 10881+ [1au] PTR? 2.203.58.216.in-addr.arpa. (54)
14:11:03.874535 IP lab1003-HP-280-G2-MT.47884 > _gateway.domain: 44131+ [1au] PTR? 2.203.58.216.in-addr.arpa. (54)
14:11:04.138086 IP hkg12s09-in-f2.1e100.net.443 > lab1003-HP-280-G2-MT.58098: UDP, length 1352
14:11:04.138091 IP hkg12s09-in-f2.1e100.net.443 > lab1003-HP-280-G2-MT.58098: UDP, length 1357
14:11:04.138093 IP hkg12s09-in-f2.1e100.net.443 > lab1003-HP-280-G2-MT.58098: UDP, length 1357
6 packets captured
60 packets received by filter
46 packets dropped by kernel
```

How to combine filtering options using logical operators:



```
lab1003@lab1003-HP-280-G2-MT:~$ sudo tcpdump -i any -c6 -nn host 192.168.0.213 and port 443
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
14:11:57.301994 IP 192.168.0.213.50638 > 172.64.150.187.443: Flags [P.], seq 2852678628:2852678667, ack 2604749684, win 1129, options [nop,nop
,TS val 2749820393 ecr 2941050739], length 39
14:11:57.302475 IP 192.168.0.213.50638 > 172.64.150.187.443: Flags [P.], seq 39:63, ack 1, win 1129, options [nop,nop,TS val 2749820393 ecr 29
41050739], length 24
14:11:57.302504 IP 192.168.0.213.50638 > 172.64.150.187.443: Flags [F.], seq 63, ack 1, win 1129, options [nop,nop,TS val 2749820393 ecr 29410
50739], length 0
14:11:57.305727 IP 172.64.150.187.443 > 192.168.0.213.50638: Flags [.], ack 64, win 8, options [nop,nop,TS val 2941104867 ecr 2749820393], len
gth 0
14:11:57.306688 IP 172.64.150.187.443 > 192.168.0.213.50638: Flags [F.], seq 1, ack 64, win 8, options [nop,nop,TS val 2941104868 ecr 27498203
93], length 0
14:11:57.306719 IP 192.168.0.213.50638 > 172.64.150.187.443: Flags [.], ack 2, win 1129, options [nop,nop,TS val 2749820397 ecr 2941104868], l
ength 0
6 packets captured
6 packets received by filter
0 packets dropped by kernel
```

CONCLUSION:-

In conclusion, studying TCP dump offers a profound insight into the intricate dynamics of network traffic analysis. By delving into its functionalities,command structures, and filtering capabilities, one can unravel the complexities of data transmission across networks. Through real-time packet capture and detailed analysis, TCP dump serves as an indispensable tool for network administrators, security analysts, and researchers alike.

LO MAPPED:- LO5