Atharva Yadav
Roll No. 127
Batch : S23
Network Lab

Assignment: TCPDUMP

Theory: 1. TCP (Transmission Control Protocol):

• TCP headers contain essential information for reliable, connection-oriented communication.

• Fields include source and destination ports, sequence and acknowledgment numbers, window size, and flags like SYN, ACK, and FIN.

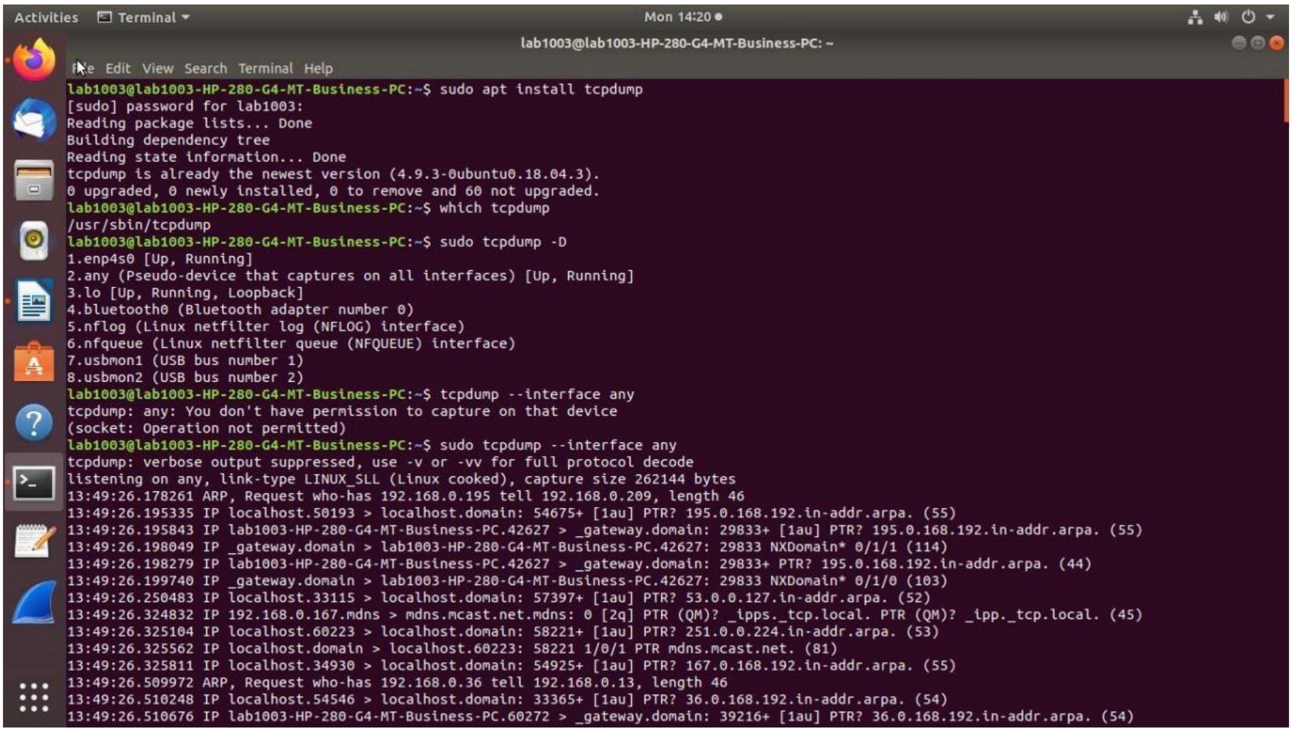
• Analysis of TCP headers helps in monitoring connection establishment, data transfer, and connection termination. 2. IP (Internet Protocol): • IP headers encapsulate data packets and facilitate routing across network devices.

• Fields include source and destination IP addresses, version, header length, protocol, and checksum.

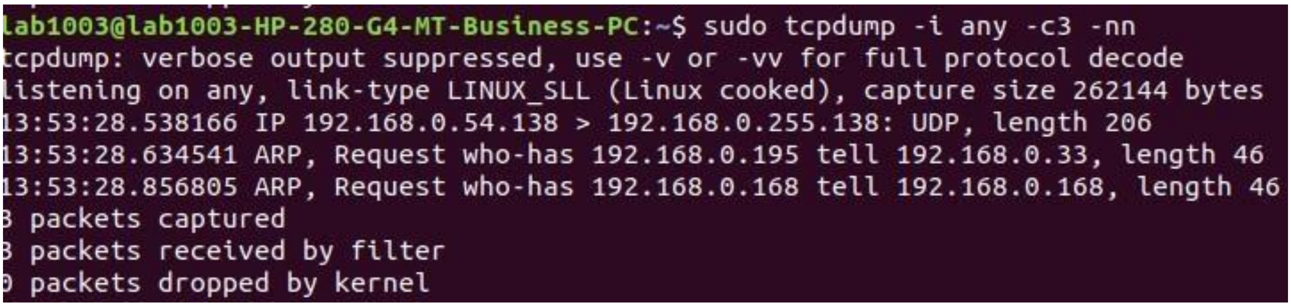
• Analysis of IP headers provides insights into packet routing, network addressing, and protocol version used for communication. 3. UDP (User Datagram Protocol):

• UDP headers support connectionless, unreliable communication, ideal for real□time applications.

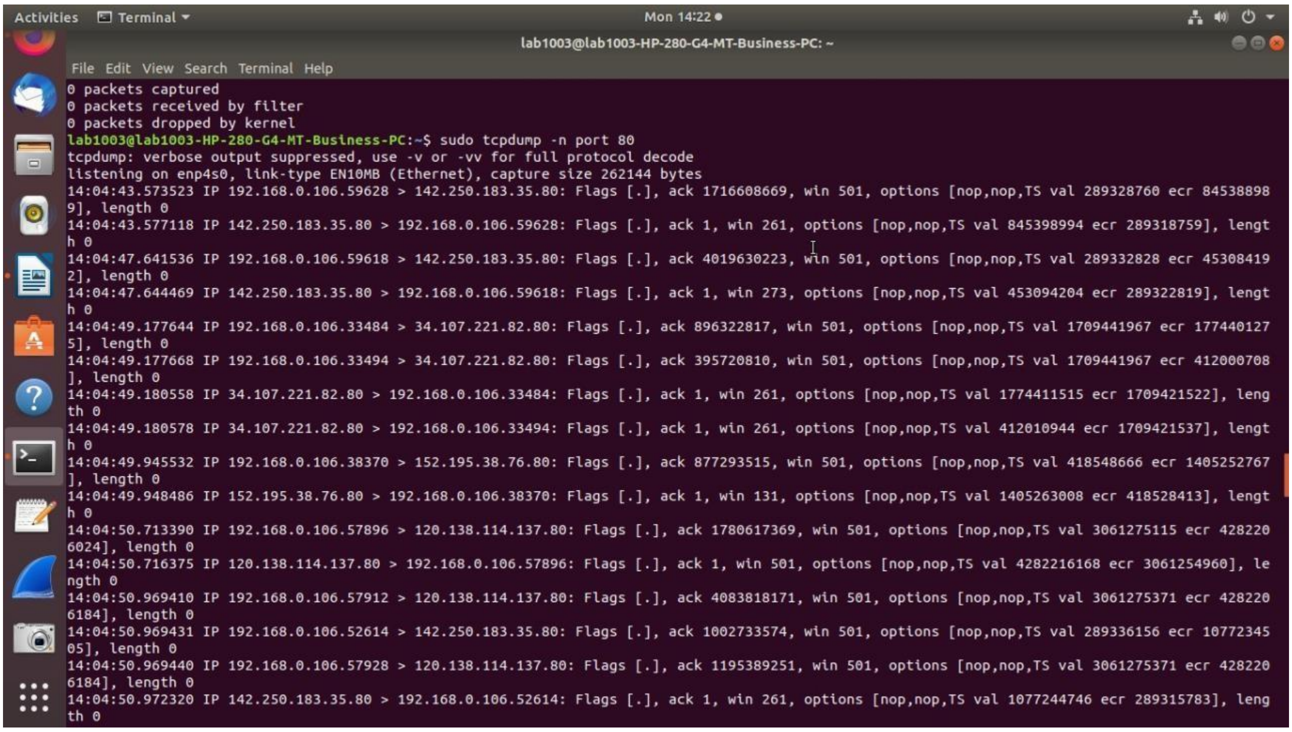
• Fields include source and destination ports, length, and checksum. • Analysis of UDP headers helps in understanding datagram transmission and reception without the overhead of connection establishment and acknowledgment.


Activities
Terminal
Mon 14:20
lab1003@lab1003-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

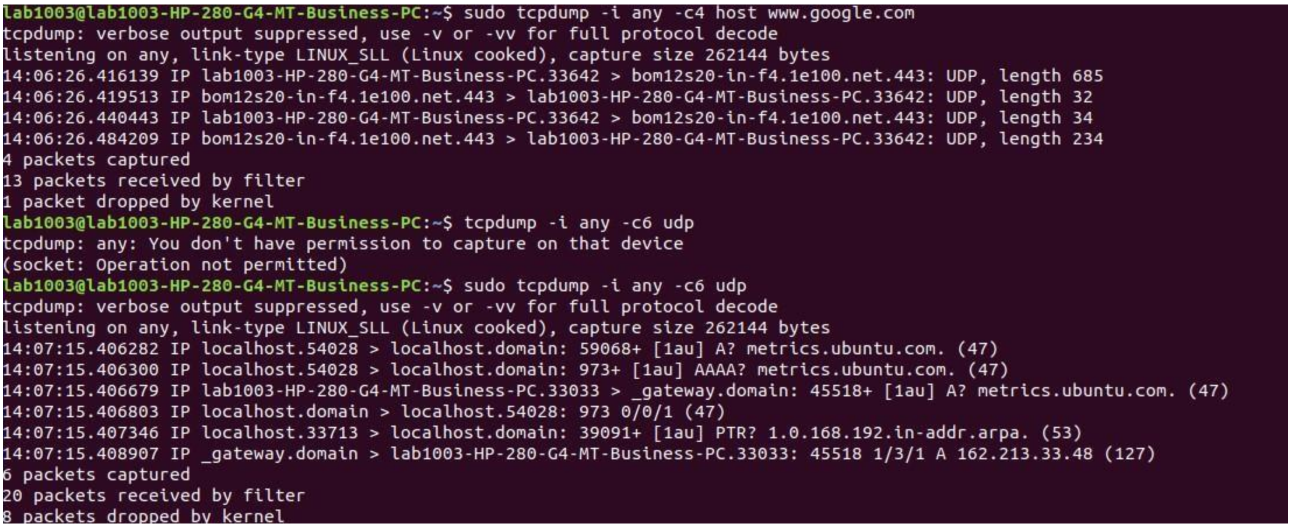
```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo apt install tcpdump
[sudo] password for lab1003:
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-0ubuntu0.18.04.3).
0 upgraded, 0 newly installed, 0 to remove and 60 not upgraded.
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ which tcpdump
/usr/sbin/tcpdump
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -D
1.enp4s0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
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-G4-MT-Business-PC:~$ tcpdump --interface any
tcpdump: any: You don't have permission to capture on that device
(socket: Operation not permitted)
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ 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
13:49:26.178261 ARP, Request who-has 192.168.0.195 tell 192.168.0.209, length 46
13:49:26.195335 IP localhost.50193 > localhost.domain: 54675+ [1au] PTR? 195.0.168.192.in-addr.arpa. (55)
13:49:26.195843 IP lab1003-HP-280-G4-MT-Business-PC.42627 > _gateway.domain: 29833+ [1au] PTR? 195.0.168.192.in-addr.arpa. (55)
13:49:26.198049 IP _gateway.domain > lab1003-HP-280-G4-MT-Business-PC.42627: 29833 NXDomain* 0/1/1 (114)
13:49:26.198279 IP lab1003-HP-280-G4-MT-Business-PC.42627 > _gateway.domain: 29833+ PTR? 195.0.168.192.in-addr.arpa. (44)
13:49:26.199740 IP _gateway.domain > lab1003-HP-280-G4-MT-Business-PC.42627: 29833 NXDomain* 0/1/0 (103)
13:49:26.250483 IP localhost.33115 > localhost.domain: 57397+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
13:49:26.324832 IP 192.168.0.167.mdns > mdns.mcast.net.mdns: 0 [2q] PTR (QM)? _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
13:49:26.325104 IP localhost.60223 > localhost.domain: 58221+ [1au] PTR? 251.0.0.224.in-addr.arpa. (53)
13:49:26.325562 IP localhost.domain > localhost.60223: 58221 1/0/1 PTR mdns.mcast.net. (81)
13:49:26.325811 IP localhost.34930 > localhost.domain: 54925+ [1au] PTR? 167.0.168.192.in-addr.arpa. (55)
13:49:26.509972 ARP, Request who-has 192.168.0.36 tell 192.168.0.13, length 46
13:49:26.510248 IP localhost.54546 > localhost.domain: 33365+ [1au] PTR? 36.0.168.192.in-addr.arpa. (54)
13:49:26.510676 IP lab1003-HP-280-G4-MT-Business-PC.60272 > _gateway.domain: 39216+ [1au] PTR? 36.0.168.192.in-addr.arpa. (54)
```



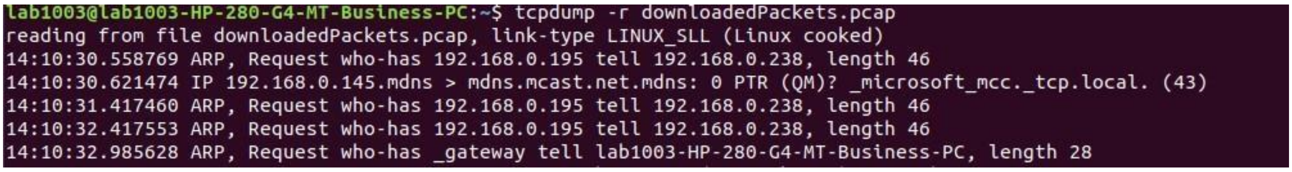
```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i any -c3 -nn
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
13:53:28.538166 IP 192.168.0.54.138 > 192.168.0.255.138: UDP, length 206
13:53:28.634541 ARP, Request who-has 192.168.0.195 tell 192.168.0.33, length 46
13:53:28.856805 ARP, Request who-has 192.168.0.168 tell 192.168.0.168, length 46
3 packets captured
3 packets received by filter
0 packets dropped by kernel
```


Activities
Terminal
Mon 14:22
lab1003@lab1003-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

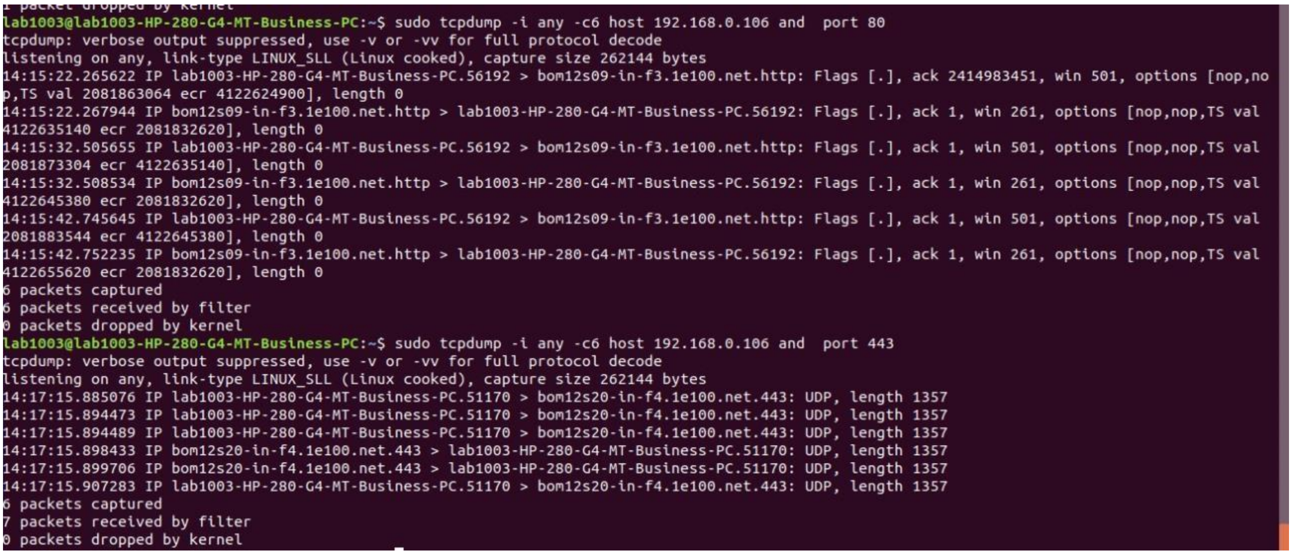
```
0 packets captured
0 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -n port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp4s0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:04:43.573523 IP 192.168.0.106.59628 > 142.250.183.35.80: Flags [.], ack 1716608669, win 501, options [nop,nop,TS val 289328760 ecr 84538898
9], length 0
14:04:43.577118 IP 142.250.183.35.80 > 192.168.0.106.59628: Flags [.], ack 1, win 261, options [nop,nop,TS val 845398994 ecr 289318759], lengt
h 0
14:04:47.641536 IP 192.168.0.106.59618 > 142.250.183.35.80: Flags [.], ack 4019630223, win 501, options [nop,nop,TS val 289332828 ecr 45308419
2], length 0
14:04:47.644469 IP 142.250.183.35.80 > 192.168.0.106.59618: Flags [.], ack 1, win 273, options [nop,nop,TS val 453094204 ecr 289322819], lengt
h 0
14:04:49.177644 IP 192.168.0.106.33484 > 34.107.221.82.80: Flags [.], ack 896322817, win 501, options [nop,nop,TS val 1709441967 ecr 177440127
5], length 0
14:04:49.177668 IP 192.168.0.106.33494 > 34.107.221.82.80: Flags [.], ack 395720810, win 501, options [nop,nop,TS val 1709441967 ecr 412000708
], length 0
14:04:49.180558 IP 34.107.221.82.80 > 192.168.0.106.33484: Flags [.], ack 1, win 261, options [nop,nop,TS val 1774411515 ecr 1709421522], leng
th 0
14:04:49.180578 IP 34.107.221.82.80 > 192.168.0.106.33494: Flags [.], ack 1, win 261, options [nop,nop,TS val 412010944 ecr 1709421537], lengt
h 0
14:04:49.945532 IP 192.168.0.106.38370 > 152.195.38.76.80: Flags [.], ack 877293515, win 501, options [nop,nop,TS val 418548666 ecr 1405252767
], length 0
14:04:49.948486 IP 152.195.38.76.80 > 192.168.0.106.38370: Flags [.], ack 1, win 131, options [nop,nop,TS val 1405263008 ecr 418528413], lengt
h 0
14:04:50.713390 IP 192.168.0.106.57896 > 120.138.114.137.80: Flags [.], ack 1780617369, win 501, options [nop,nop,TS val 3061275115 ecr 428220
6024], length 0
14:04:50.716375 IP 120.138.114.137.80 > 192.168.0.106.57896: Flags [.], ack 1, win 501, options [nop,nop,TS val 4282216168 ecr 3061254960], le
ngth 0
14:04:50.969410 IP 192.168.0.106.57912 > 120.138.114.137.80: Flags [.], ack 4083818171, win 501, options [nop,nop,TS val 3061275371 ecr 428220
6184], length 0
14:04:50.969431 IP 192.168.0.106.52614 > 142.250.183.35.80: Flags [.], ack 1002733574, win 501, options [nop,nop,TS val 289336156 ecr 10772345
05], length 0
14:04:50.969440 IP 192.168.0.106.57928 > 120.138.114.137.80: Flags [.], ack 1195389251, win 501, options [nop,nop,TS val 3061275371 ecr 428220
6184], length 0
14:04:50.972320 IP 142.250.183.35.80 > 192.168.0.106.52614: Flags [.], ack 1, win 261, options [nop,nop,TS val 1077244746 ecr 289315783], leng
th 0
```



```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i any -c4 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
14:06:26.416139 IP lab1003-HP-280-G4-MT-Business-PC.33642 > bom12s20-in-f4.1e100.net.443: UDP, length 685
14:06:26.419513 IP bom12s20-in-f4.1e100.net.443 > lab1003-HP-280-G4-MT-Business-PC.33642: UDP, length 32
14:06:26.440443 IP lab1003-HP-280-G4-MT-Business-PC.33642 > bom12s20-in-f4.1e100.net.443: UDP, length 34
14:06:26.484209 IP bom12s20-in-f4.1e100.net.443 > lab1003-HP-280-G4-MT-Business-PC.33642: UDP, length 234
4 packets captured
13 packets received by filter
1 packet dropped by kernel
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tcpdump -i any -c6 udp
tcpdump: any: You don't have permission to capture on that device
(socket: Operation not permitted)
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ 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
14:07:15.406282 IP localhost.54028 > localhost.domain: 59068+ [1au] A? metrics.ubuntu.com. (47)
14:07:15.406300 IP localhost.54028 > localhost.domain: 973+ [1au] AAAA? metrics.ubuntu.com. (47)
14:07:15.406679 IP lab1003-HP-280-G4-MT-Business-PC.33033 > _gateway.domain: 45518+ [1au] A? metrics.ubuntu.com. (47)
14:07:15.406803 IP localhost.domain > localhost.54028: 973 0/0/1 (47)
14:07:15.407346 IP localhost.33713 > localhost.domain: 39091+ [1au] PTR? 1.0.168.192.in-addr.arpa. (53)
14:07:15.408907 IP _gateway.domain > lab1003-HP-280-G4-MT-Business-PC.33033: 45518 1/3/1 A 162.213.33.48 (127)
6 packets captured
20 packets received by filter
8 packets dropped by kernel
```



```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tcpdump -r downloadedPackets.pcap
reading from file downloadedPackets.pcap, link-type LINUX_SLL (Linux cooked)
14:10:30.558769 ARP, Request who-has 192.168.0.195 tell 192.168.0.238, length 46
14:10:30.621474 IP 192.168.0.145.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? _microsoft_mcc._tcp.local. (43)
14:10:31.417460 ARP, Request who-has 192.168.0.195 tell 192.168.0.238, length 46
14:10:32.417553 ARP, Request who-has 192.168.0.195 tell 192.168.0.238, length 46
14:10:32.985628 ARP, Request who-has _gateway tell lab1003-HP-280-G4-MT-Business-PC, length 28
```



```
1 packet dropped by kernel
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i any -c6 host 192.168.0.106 and  port 80
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
14:15:22.265622 IP lab1003-HP-280-G4-MT-Business-PC.56192 > bom12s09-in-f3.1e100.net.http: Flags [.], ack 2414983451, win 501, options [nop,no
p,TS val 2081863064 ecr 4122624900], length 0
14:15:22.267944 IP bom12s09-in-f3.1e100.net.http > lab1003-HP-280-G4-MT-Business-PC.56192: Flags [.], ack 1, win 261, options [nop,nop,TS val
4122635140 ecr 2081832620], length 0
14:15:32.505655 IP lab1003-HP-280-G4-MT-Business-PC.56192 > bom12s09-in-f3.1e100.net.http: Flags [.], ack 1, win 501, options [nop,nop,TS val
2081873304 ecr 4122635140], length 0
14:15:32.508534 IP bom12s09-in-f3.1e100.net.http > lab1003-HP-280-G4-MT-Business-PC.56192: Flags [.], ack 1, win 261, options [nop,nop,TS val
4122645380 ecr 2081832620], length 0
14:15:42.745645 IP lab1003-HP-280-G4-MT-Business-PC.56192 > bom12s09-in-f3.1e100.net.http: Flags [.], ack 1, win 501, options [nop,nop,TS val
2081883544 ecr 4122645380], length 0
14:15:42.752235 IP bom12s09-in-f3.1e100.net.http > lab1003-HP-280-G4-MT-Business-PC.56192: Flags [.], ack 1, win 261, options [nop,nop,TS val
4122655620 ecr 2081832620], length 0
6 packets captured
6 packets received by filter
0 packets dropped by kernel
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ sudo tcpdump -i any -c6 host 192.168.0.106 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
14:17:15.885076 IP lab1003-HP-280-G4-MT-Business-PC.51170 > bom12s20-in-f4.1e100.net.443: UDP, length 1357
14:17:15.894473 IP lab1003-HP-280-G4-MT-Business-PC.51170 > bom12s20-in-f4.1e100.net.443: UDP, length 1357
14:17:15.894489 IP lab1003-HP-280-G4-MT-Business-PC.51170 > bom12s20-in-f4.1e100.net.443: UDP, length 1357
14:17:15.898433 IP bom12s20-in-f4.1e100.net.443 > lab1003-HP-280-G4-MT-Business-PC.51170: UDP, length 1357
14:17:15.899706 IP bom12s20-in-f4.1e100.net.443 > lab1003-HP-280-G4-MT-Business-PC.51170: UDP, length 1357
14:17:15.907283 IP lab1003-HP-280-G4-MT-Business-PC.51170 > bom12s20-in-f4.1e100.net.443: UDP, length 1357
6 packets captured
7 packets received by filter
0 packets dropped by kernel
```

Conclusions:

TCPDUMP enables detailed examination of packet headers, facilitating network troubleshooting, performance monitoring, and security analysis.

- By analyzing TCP headers, network administrators can diagnose connection issues, monitor traffic flow, and detect potential security threats.
- Examination of IP headers aids in understanding packet routing, identifying network congestion points, and ensuring proper addressing.
- Analysis of UDP headers helps in optimizing real-time applications,

diagnosing packet loss, and ensuring efficient data transmission. Overall, TCPDUMP provides valuable insights into network traffic behavior and protocol usage, empowering administrators to maintain and optimize network performance and security.