[mycomputer@compute-0-1 ~]# tcpdump -tttt -r ex.pcap

reading from file enp0s3-26082018.pcap, link-type EN10MB (Ethernet)

2018-08-25 22:03:17.249648 IP compute-0-1.example.com.ssh > 169.144.0.1.39406: Flags [P.], seq 1426167803:1426167927, ack 3061962134, win 291, options

[nop,nop,TS val 81358717 ecr 20378789], length 124

2018-08-25 22:03:17.249840 IP 169.144.0.1.39406 > compute-0-1.example.com.ssh: Flags [.], ack 124, win 564, options [nop,nop,TS val 20378791 ecr 81358

717], length 0

2018-08-25 22:03:17.454559 IP controller0.example.com.amqp > compute-0-1.example.com.57836: Flags [.], ack 1079416895, win 1432, options [nop,nop,TS v

al 81352560 ecr 81353913], length 0

2018-08-25 22:03:17.454642 IP compute-0-1.example.com.57836 > controller0.example.com.amqp: Flags [.], ack 1, win 237, options [nop,nop,TS val 8135892

2 ecr 81317504], length 0

2018-08-25 22:03:17.646945 IP compute-0-1.example.com.57788 > controller0.example.com.amqp: Flags [.], seq 106760587:106762035, ack 688390730, win 237

, options [nop,nop,TS val 81359114 ecr 81350901], length 1448

2018-08-25 22:03:17.647043 IP compute-0-1.example.com.57788 > controller0.example.com.amqp: Flags [P.], seq 1448:1956, ack 1, win 237, options [nop,no

p,TS val 81359114 ecr 81350901], length 508

2018-08-25 22:03:17.647502 IP controller0.example.com.amqp > compute-0-1.example.com.57788: Flags [.], ack 1956, win 1432, options [nop,nop,TS val 813

52753 ecr 81359114], length 0

.........................................................................................................................

**Approach:**

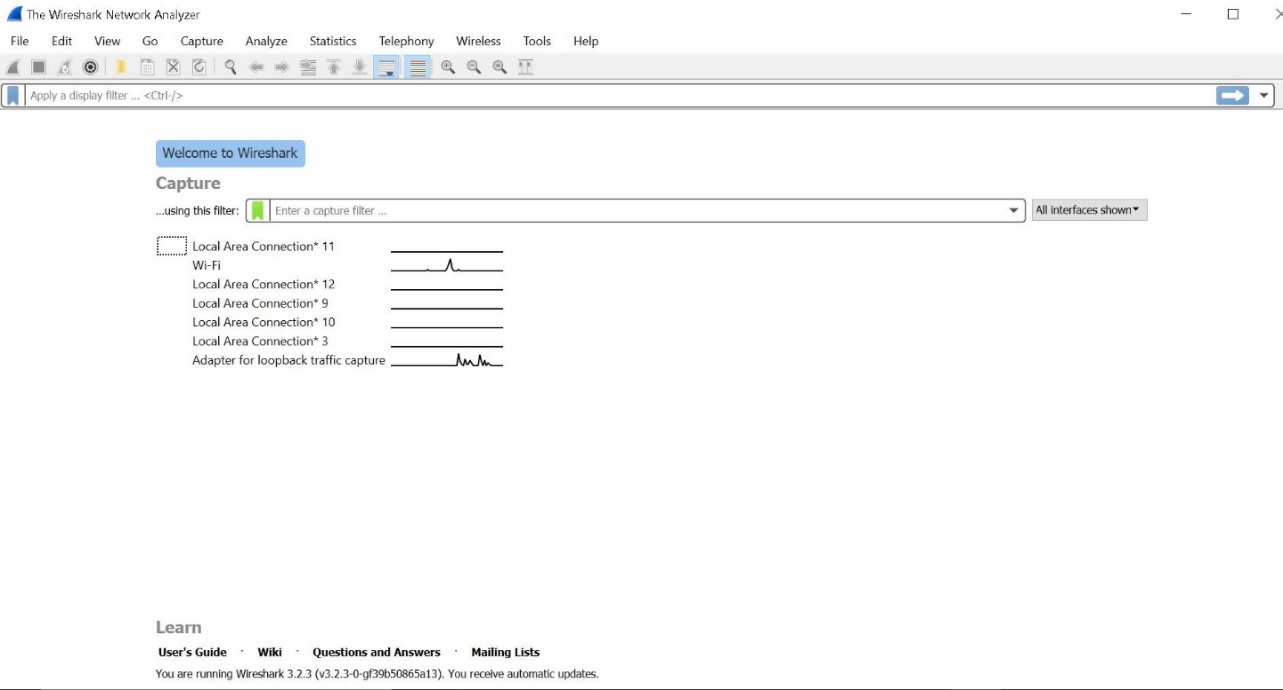
1. Capture packets from interface with GUI or TCPDUMP command as follows

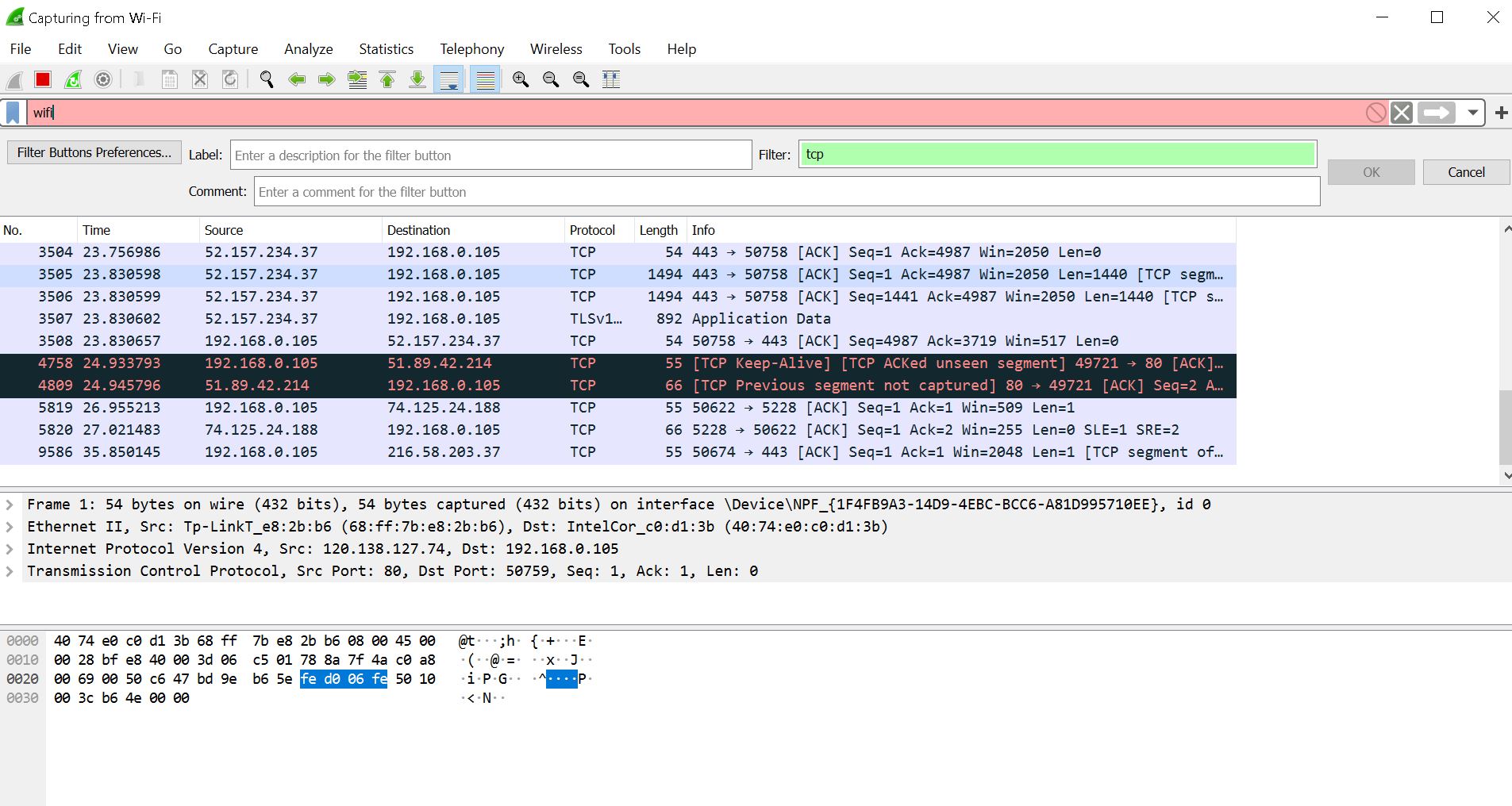
**tcpdump -i eth0 \_w ex.pcap**

**(Permission denied on machine for above command)**

1. Analyze o/p directly on comsol or on GUI of wireshark.

I have chosen to capture packets on GUI of (Wireshark) as follows:

Wireshark packets analysis as follows:



**Conclusion:**

From above experiment we learn to capture packets using Wireshark tool and get know exactly which packets are getting transferred in our system.

**Postlabs:**

1. What are the next hop router’s IP Address and MAC Address? How did you

get this information?

A: The router will use ARP to lookup the MAC Address of the default gateway.

Then the router will do the same to find its next hop. The router finds the IP

address of the next hop by a lookup of its routing table to find optimal path.

2. What are local DNS server’s hostname and IP Address? How did you get this

information?

A: DNS server hostname: UnKnown

DNS server IP Address: 192.168.29.1 / 2405:201:800:1507::c0a8:1d01

This information can be looked up using “ipconfig/all” command in a

terminal or command prompt and nslookup “IP Address” to find the

hostname of the DNS Server IP.