	Hope Foundation's **Finolex Academy of Management and Technology, Ratnagiri**
	Information Technology Department

Subject name: Cloud Service Design Lab			Subject Code: ITL603
Class	TE IT	Semester – VI (CBCGS)	Academic year: 2018-19
Name of Student	**Kazi Jawwad A Rahim**	**QUIZ Score : 06/10**	
Roll No	**27**	Assignment/Experiment No.	08

Title: To perform analysis of network traffic using wire shark and VM ware workstation

1.Course objectives applicable

COB3. To understand importance of cloud network security.

COB6.To understand the concept of network traffic.

2. Course outcomes applicable:

CO1 -To understand importance of cloud security

CO6-To understand the use of network traffic applications

3. Learning Objectives:

1. To analyze network traffic.
2. To understand the use of wire shark for network packet capturing

4. Practical applications of the assignment/experiment: In cloud environment

5. Prerequisites:

1. Prior knowledge of wire shark and VM ware workstation.
2. Internet Access

6. Hardware Requirements:

1. Internet Access with Browser

7. Software Requirements:

Browser like Chrome, Internet Explorer Edge

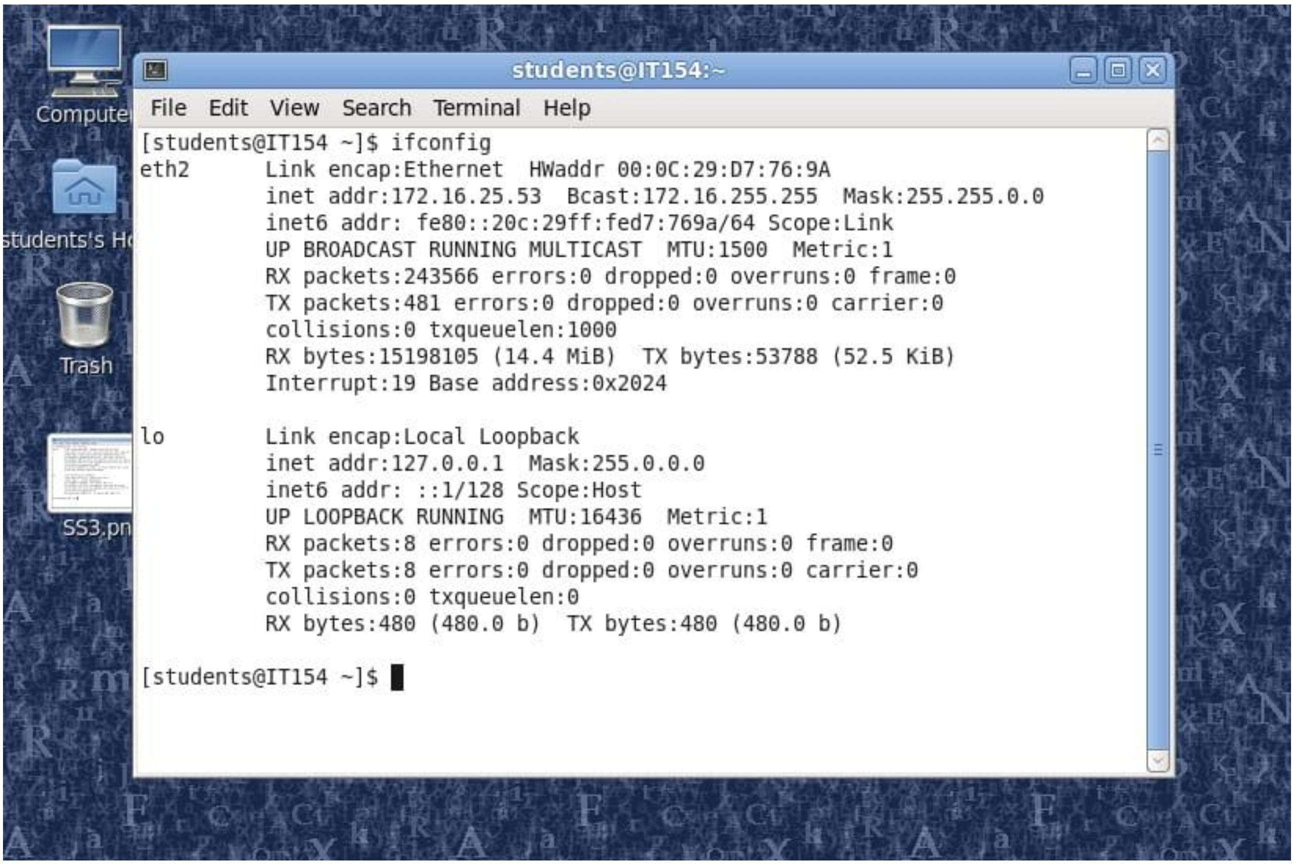
8. Quiz Questions (if any): (Online Exam will be taken separately batchwise, attach the certificate/ Marks obtained)

1. What is network traffic?
2. What is the use of wireshark?

9. Experiment/Assignment Evaluation:

Sr. No.	**Parameters**		**Marks obtained**	**Out of**
1	Technical Understanding (Assessment may be done based on Q & A **or** any other relevant method.) Teacher should mention the other method used -			6
2	Neatness/presentation			2
3	Punctuality			2
Date of performance (DOP)		**Total marks obtained**		**10**
Date of checking (DOC)		**Signature of teacher**		

OUTPUTS:

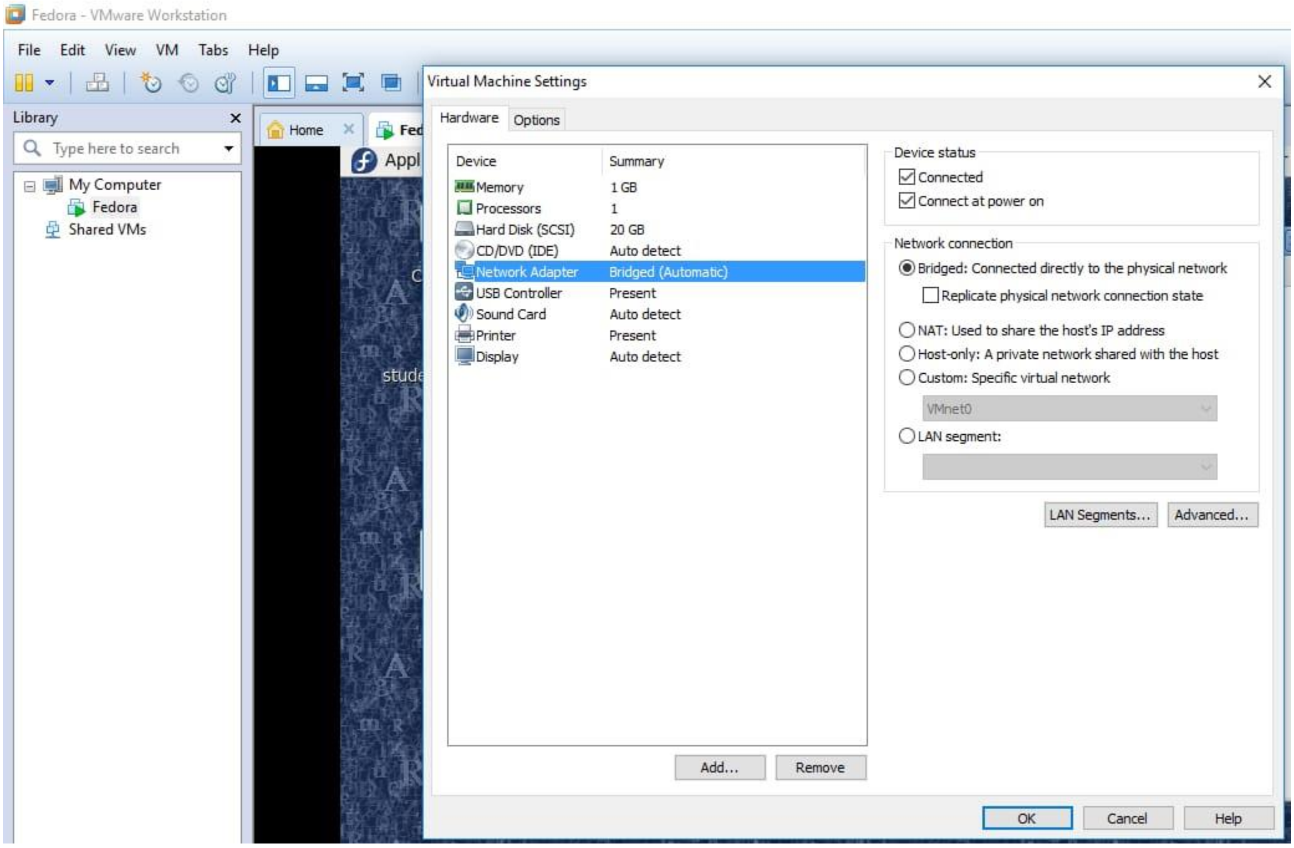


```
[students@IT154 ~]$ ifconfig
eth2      Link encap:Ethernet  HWaddr 00:0C:29:D7:76:9A
          inet addr:172.16.25.53  Bcast:172.16.255.255  Mask:255.255.0.0
          inet6 addr: fe80::20c:29ff:fed7:769a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:243566 errors:0 dropped:0 overruns:0 frame:0
          TX packets:481 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15198105 (14.4 MiB)  TX bytes:53788 (52.5 KiB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

[students@IT154 ~]$ 
```

Find the IP address



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

● Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

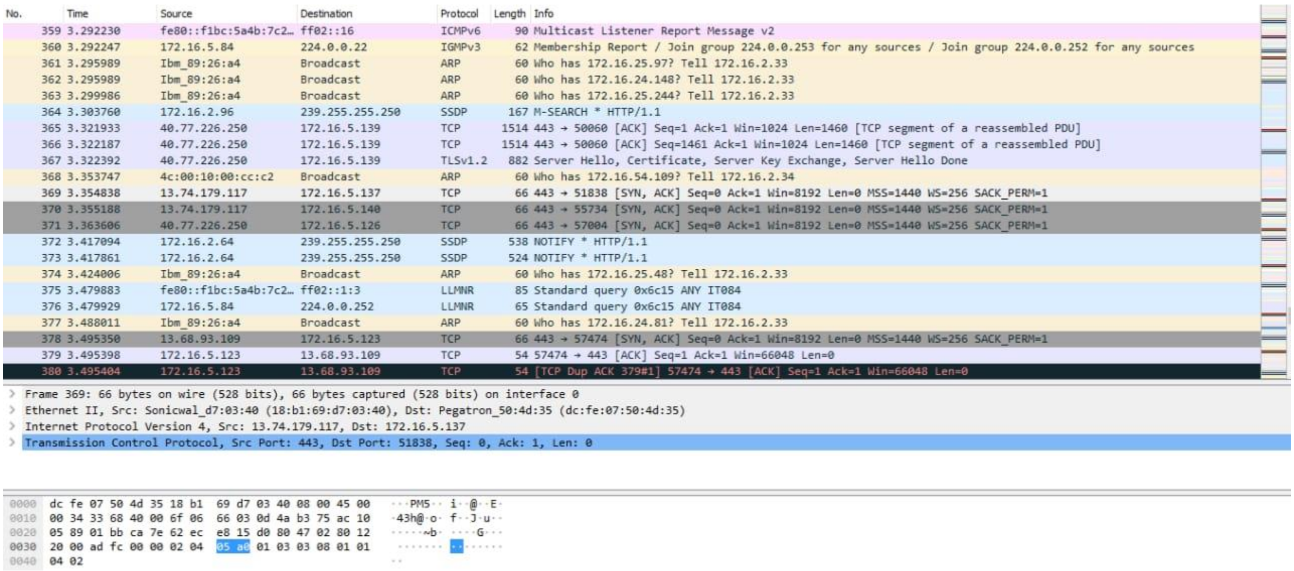
○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

○ LAN segment:

Check the network adapter



No.	Time	Source	Destination	Protocol	Length	Info
359	3.292230	fe80::f1bc:5a4b:7c2…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
360	3.292247	172.16.5.84	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.253 for any sources / Join group 224.0.0.252 for any sources
361	3.295989	Ibm_89:26:a4	Broadcast	ARP	60	Who has 172.16.25.97? Tell 172.16.2.33
362	3.295989	Ibm_89:26:a4	Broadcast	ARP	60	Who has 172.16.24.148? Tell 172.16.2.33
363	3.299986	Ibm_89:26:a4	Broadcast	ARP	60	Who has 172.16.25.244? Tell 172.16.2.33
364	3.303760	172.16.2.96	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
365	3.321933	40.77.226.250	172.16.5.139	TCP	1514	443 → 50060 [ACK] Seq=1 Ack=1 Win=1024 Len=1460 [TCP segment of a reassembled PDU]
366	3.322187	40.77.226.250	172.16.5.139	TCP	1514	443 → 50060 [ACK] Seq=1461 Ack=1 Win=1024 Len=1460 [TCP segment of a reassembled PDU]
367	3.322392	40.77.226.250	172.16.5.139	TLSv1.2	882	Server Hello, Certificate, Server Key Exchange, Server Hello Done
368	3.353747	4c:00:10:00:cc:c2	Broadcast	ARP	60	Who has 172.16.54.109? Tell 172.16.2.34
369	3.354838	13.74.179.117	172.16.5.137	TCP	66	443 → 51838 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
370	3.355188	13.74.179.117	172.16.5.140	TCP	66	443 → 55734 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
371	3.363606	40.77.226.250	172.16.5.126	TCP	66	443 → 57004 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
372	3.417094	172.16.2.64	239.255.255.250	SSDP	538	NOTIFY * HTTP/1.1
373	3.417861	172.16.2.64	239.255.255.250	SSDP	524	NOTIFY * HTTP/1.1
374	3.424006	Ibm_89:26:a4	Broadcast	ARP	60	Who has 172.16.25.48? Tell 172.16.2.33
375	3.479883	fe80::f1bc:5a4b:7c2…	ff02::1:3	LLMNR	85	Standard query 0x6c15 ANY IT084
376	3.479929	172.16.5.84	224.0.0.252	LLMNR	65	Standard query 0x6c15 ANY IT084
377	3.488011	Ibm_89:26:a4	Broadcast	ARP	60	Who has 172.16.24.81? Tell 172.16.2.33
378	3.495350	13.68.93.109	172.16.5.123	TCP	66	443 → 57474 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
379	3.495398	172.16.5.123	13.68.93.109	TCP	54	57474 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
380	3.495404	172.16.5.123	13.68.93.109	TCP	54	[TCP Dup ACK 379#1] 57474 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0

```
> Frame 369: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Sonicwal_d7:03:40 (18:b1:69:d7:03:40), Dst: Pegatron_50:4d:35 (dc:fe:07:50:4d:35)
> Internet Protocol Version 4, Src: 13.74.179.117, Dst: 172.16.5.137
> Transmission Control Protocol, Src Port: 443, Dst Port: 51838, Seq: 0, Ack: 1, Len: 0
```

```
0000  dc fe 07 50 4d 35 18 b1  69 d7 03 40 08 00 45 00   ···PM5·· i··@··E·
0010  00 34 33 68 40 00 6f 06  66 03 0d 4a b3 75 ac 10   ·43h@·o· f··J·u··
0020  05 89 01 bb ca 7e 62 ec  e8 15 d0 80 47 02 80 12   ·····~b· ····G···
0030  20 00 ad fc 00 00 02 04  05 a0 01 03 03 08 01 01    ········ ········
0040  04 02                                              ··
```

Run the Wireshark to capture packet traffic

11. Learning Outcomes Achieved

We have understood the use of wire shark for network packet capturing.

12. Conclusion:

1. **Applications of the studied technique in industry**
   a. Use of wire shark in cloud industry for traffic analysis.
2. **Engineering Relevance**
   a. Importance of cloud security
3. **Skills Developed**
   a. Understanding fundamentals of wire shark software.
   b. Understanding network traffic concept.

References :

[1] https://www.wireshark.org

[2] https://en.m.wikipedia.org/wiki/Wireshark