



Department of Computer Engineering

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

Name: Varun Viswanath

SAP ID: 60004210105

Experiment No: 11

Aim: Simulate Packet Capturing in Wireshark

Theory:

- Packet sniffers are a basic tool for observing the messages on a network. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine.
- At the right are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashedrectangle, is an addition to the usual software in your computer and consists of two parts. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer. As you know, messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In the figure, the assumed physical media is an Ethernet, and so all upper layer protocolsare eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.
- The existence of the packet capture box in this figure should give you cause to pause and think, particularly down two trains of thought. Firstly, it shows that any packet in



Department of Computer Engineering

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

a shared medium (Ethernet, Wi-Fi, etc) can be captured and examined without notification of the sender or receiver. You cannot rely on common link-layer protocols to protect your secrets or your privacy online. At a minimum, you should be using encryption protocols (generally buried in the application layer, though sometimes found elsewhere) to protect all network traffic you generate or receive. Secondly, you have the ability to act as the “bad guy” and capture the network traffic of other people, examine it and exploit what you find.

- The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must “understand” the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string “GET,” “POST,” or “HEAD”.
- We will be using the Wireshark packet sniffer, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer). Wireshark is a free network protocol analyzer that runs on Macintosh, Windows, and Linux/Unix computers. It's an ideal packet analyzer for our labs – it is stable, has a large user base and well-documented support that includes a userguide, man pages, and a detailed FAQ, rich functionality that includes the capability to analyze hundreds of protocols, and a well-designed user interface. It operates in computers using Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LANs, and ATM connections (if the OS on which it's running allows Wireshark to do so).



Department of Computer Engineering

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

Working:

Filters in Wireshark

1. Ip:

a. Src

No.	Source	Destination	Protocol	Length	Info
625 ip-src,rt	10.120.112.225	192.168.2.51	SMB2	212	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO
6254e 0x297900000000	192.168.2.51	10.120.112.225	SMB2	258	Ioctl Response FSCTL_DFS_GET_REFERRALS
19084 16.024327	192.168.2.108	10.120.112.225	SMB2	322	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
62541 829.588560	192.168.2.51	10.120.112.225	SMB2	322	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
62538 829.586367	192.168.2.51	10.120.112.225	SMB2	194	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO
19085 16.024386	192.168.2.108	10.120.112.225	SMB2	138	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
39958 182.789755	10.120.110.157	10.120.111.255	BROWSE	243	Local Master Announcement DESKTOP-L97LWNS, workstation, Server, SQL Server, NT Workstation, Potential Browser, Master Browser
16688 13.927223	10.120.112.144	10.120.111.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser
16770 14.877496	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser
29981 44.238148	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser
29991 44.341145	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser
60883 765.5904190	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser
38850 74.443121	10.120.113.250	10.120.113.255	BROWSE	243	Local Master Announcement HP-PC, workstation, Server, NT Workstation, Potential Browser, Master Browser
61482 792.439306	10.120.113.250	10.120.113.255	BROWSE	243	Local Master Announcement HP-PC, workstation, Server, NT Workstation, Potential Browser, Master Browser
64915 922.268249	10.120.101.249	10.120.111.255	BROWSE	243	Local Master Announcement NUM9922CPU0131, workstation, Server, NT Workstation, Potential Browser, Master Browser
45526 259.277817	10.120.98.198	10.120.111.255	BROWSE	243	Local Master Announcement NUM9922CPU0130, workstation, Server, NT Workstation, Potential Browser, Master Browser
48883 396.863973	10.120.110.124	10.120.111.255	BROWSE	243	Local Master Announcement SAIBA, workstation, Server, Print Queue Server, NT Workstation, Potential Browser, Master Browser
38863 89.508337	10.120.113.245	10.120.113.255	BROWSE	258	Local Master Announcement WIP0-1000, workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
62642 809.729413	10.120.113.245	10.120.113.255	BROWSE	258	Local Master Announcement WIP0-1000, workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
19101 16.116128	10.120.112.225	192.168.2.108	SMB2	170	Lock Request
19113 16.123975	10.120.112.225	192.168.2.108	SMB2	170	Lock Request
19107 16.128319	192.168.2.108	10.120.112.225	SMB2	126	Lock Response
19114 16.125882	192.168.2.108	10.120.112.225	SMB2	126	Lock Response
19106 16.126237	192.168.2.108	10.120.112.225	SMB2	138	Lock Response, Error: STATUS_PENDING
1 0.000000	10.120.113.25	239.255.255.250	SSDP	217	R-SEARCH * HTTP/1.1
489 0.417474	10.120.101.28	239.255.255.250	SSDP	217	R-SEARCH * HTTP/1.1

```
0000 01 00 5e 7f ff fa bc 00 1b 58 ba 60 00 00 45 00 . . . . . X - E
0010 00 cb 9b 6d 00 00 01 11 b2 29 0a 70 71 19 cf ff . . . . . m . . . . . x0
0020 ff fa cd fd 07 6c 00 b7 3f eb 4d 2d 53 45 41 52 . . . . . 1 . . . ? M-SEAR
0030 43 40 20 2a 20 48 54 54 50 2f 31 31 3d 0a 08 CH * HTT P/1.1 - H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 38 0d 0a 4d 41 4e 3a 20 .250:190 0 - MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a MOX 1 - ST: urn
0080 64 61 6c 2d 6d 75 6c 74 69 73 63 6f 72 65 65 6e dial-mul tiscreen
0090 6f 72 67 3a 70 72 63 65 6f 71 69 68 67 66 65 64 -organizer-disa
00a0 6c 3a 31 0d 0a 53 53 45 52 2d 41 47 45 44 54 3a 11 USE R-AGENT:
00b0 20 4d 69 63 72 6f 73 6f 66 74 20 45 44 67 65 2f Microsoft Edge/
00c0 31 31 32 2e 30 2e 31 37 32 32 2e 35 38 20 57 69 112.0 .17 22.58 /il
00d0 6e 64 6f 77 73 0d 0a 0d 0a ndows . . . . .
```

b. Dst

No.	Time	Source	Destination	Protocol	Length	Info
62537 829.504729	10.120.110.157	192.168.2.51	SMB2	212	Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO	
62542 829.588560	10.120.112.225	192.168.2.51	SMB2	258	Ioctl Response FSCTL_DFS_GET_REFERRALS	
19084 16.024327	192.168.2.108	10.120.112.225	SMB2	322	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO	
62541 829.588560	192.168.2.51	10.120.112.225	SMB2	322	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO	
62538 829.586367	192.168.2.51	10.120.112.225	SMB2	194	Ioctl Response FSCTL_VALIDATE_NEGOTIATE_INFO	
19085 16.024386	192.168.2.108	10.120.112.225	SMB2	138	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED	
39958 182.789755	10.120.110.157	10.120.111.255	BROWSE	243	Local Master Announcement DESKTOP-L97LWNS, workstation, Server, SQL Server, NT Workstation, Potential Browser, Master Browser	
16688 13.927223	10.120.112.144	10.120.111.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser	
16770 14.877496	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser	
29981 44.238148	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser	
29991 44.341145	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser	
60883 765.5904190	10.120.112.144	10.120.113.255	BROWSE	243	Local Master Announcement DESKTOP-R05B8MK, workstation, Server, NT Workstation, Potential Browser, Master Browser	
38850 74.443121	10.120.113.250	10.120.113.255	BROWSE	243	Local Master Announcement HP-PC, workstation, Server, NT Workstation, Potential Browser, Master Browser	
61482 792.439306	10.120.113.250	10.120.113.255	BROWSE	243	Local Master Announcement HP-PC, workstation, Server, NT Workstation, Potential Browser, Master Browser	
64915 922.268249	10.120.101.249	10.120.111.255	BROWSE	243	Local Master Announcement NUM9922CPU0131, workstation, Server, NT Workstation, Potential Browser, Master Browser	
45526 259.277817	10.120.98.198	10.120.111.255	BROWSE	243	Local Master Announcement NUM9922CPU0130, workstation, Server, NT Workstation, Potential Browser, Master Browser	
48883 396.863973	10.120.110.124	10.120.111.255	BROWSE	243	Local Master Announcement SAIBA, workstation, Server, Print Queue Server, NT Workstation, Potential Browser, Master Browser	
38863 89.508337	10.120.113.245	10.120.111.255	BROWSE	258	Local Master Announcement WIP0-1000, workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser	
62642 809.729413	10.120.113.245	10.120.113.255	BROWSE	258	Local Master Announcement WIP0-1000, workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser	
19101 16.116128	10.120.112.225	192.168.2.108	SMB2	170	Lock Request	
19113 16.123975	10.120.112.225	192.168.2.108	SMB2	170	Lock Request	
19107 16.128319	192.168.2.108	10.120.112.225	SMB2	126	Lock Response	
19114 16.125882	192.168.2.108	10.120.112.225	SMB2	126	Lock Response	
19106 16.126237	192.168.2.108	10.120.112.225	SMB2	138	Lock Response, Error: STATUS_PENDING	
1 0.000000	10.120.113.25	239.255.255.250	SSDP	217	R-SEARCH * HTTP/1.1	
489 0.417474	10.120.101.28	239.255.255.250	SSDP	217	R-SEARCH * HTTP/1.1	

```
0000 01 00 5e 7f ff fa bc 00 1b 58 ba 60 00 00 45 00 . . . . . X - E
0010 00 cb 9b 6d 00 00 01 11 b2 29 0a 70 71 19 cf ff . . . . . m . . . . . x0
0020 ff fa cd fd 07 6c 00 b7 3f eb 4d 2d 53 45 41 52 . . . . . 1 . . . ? M-SEAR
0030 43 40 20 2a 20 48 54 54 50 2f 31 31 3d 0a 08 CH * HTT P/1.1 - H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 38 0d 0a 4d 41 4e 3a 20 .250:190 0 - MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 72 65 72 22 0d "ssdp:discover"
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a MOX 1 - ST: urn
0080 64 61 6c 2d 6d 75 6c 74 69 73 63 6f 72 65 65 6e dial-mul tiscreen
0090 6f 72 67 3a 73 65 72 69 63 65 6a 64 61 -organizer-vicedia
00a0 6c 3a 31 0d 0a 53 53 45 52 2d 41 47 45 54 3a 20 .11 USE R-AGENT:
00b0 20 4d 69 63 72 6f 73 6f 66 74 20 45 44 67 65 2f Microsoft Edge/
00c0 31 31 32 2e 30 2e 31 37 32 32 2e 35 38 20 57 69 112.0 .17 22.58 /il
00d0 6e 64 6f 77 73 0d 0a 0d 0a ndows . . . . .
```



Course Code: DJ19CEL405

Course Name: Computer Networks Lab

c. Addr

No.	Time	Source	Destination	Protocol	Length	Info
50806	437.808555	10.128.113.227	10.128.113.255	BRONWSE	243	Host Announcement MUM15622CPU0005, Workstation, Server, NT Workstation, Potential Browser
50808	437.819995	10.128.113.227	10.128.113.255	BRONWSE	243	Host Announcement MUM15622CPU0005, Workstation, Server, NT Workstation, Potential Browser
41059	133.228153	10.128.113.218	10.128.113.255	BRONWSE	243	Host Announcement MUM15622CPU0007, Workstation, Server, NT Workstation
47792	365.688349	10.128.110.124	10.128.111.255	BRONWSE	243	Host Announcement SAIBA, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser
37804	70.999595	20.196.146.32	10.128.112.225	TLSv1.2	1087	Ignored Unknown Record
19003	1.619016	10.128.112.225	192.168.2.108	SHB2	238	Ioctl Request FSCTL_GET_REFERRALS, File: \192.168.2.108\SVKM-Software
19002	1.618859	10.128.112.225	192.168.2.108	SHB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
19004	16.024327	192.168.2.108	10.128.112.225	SHB2	332	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
19005	16.024385	192.168.2.108	10.128.112.225	SHB2	130	Ioctl Response, Error: STATUS_F5_DRIVER_REQUIRED
39590	102.709755	10.128.111.157	10.128.111.255	BRONWSE	243	Local Master Announcement DESKTOP-197LWNS, Workstation, Server, SQL Server, NT Workstation, Potential Browser, Master Browser
16688	13.527223	10.128.112.144	10.128.113.255	BRONWSE	243	Local Master Announcement DESKTOP-RDSBRWK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
16770	14.837406	10.128.112.144	10.128.113.255	BRONWSE	243	Local Master Announcement DESKTOP-RDSBRWK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
29981	44.238148	10.128.112.144	10.128.113.255	BRONWSE	243	Local Master Announcement DESKTOP-RDSBRWK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
29991	44.341145	10.128.112.144	10.128.113.255	BRONWSE	243	Local Master Announcement DESKTOP-RDSBRWK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
60883	365.7610496	10.128.112.144	10.128.113.255	BRONWSE	243	Local Master Announcement DESKTOP-RDSBRWK, Workstation, Server, NT Workstation, Potential Browser, Master Browser
38050	74.443121	10.128.113.250	10.128.113.255	BRONWSE	243	Local Master Announcement HP-PC, Workstation, Server, NT Workstation, Potential Browser, Master Browser
45526	259.277817	10.128.98.19	10.128.111.255	BRONWSE	243	Local Master Announcement MUM0922CP0U710, Workstation, Server, NT Workstation, Potential Browser, Master Browser
48883	398.863973	10.128.110.124	10.128.111.255	BRONWSE	243	Local Master Announcement SAIBA, Workstation, Server, Print Queue Server, NT Workstation, Potential Browser, Master Browser
38963	89.590337	10.128.113.245	10.128.113.255	BRONWSE	258	Local Master Announcement WIDP-1000, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser
19101	16.116128	10.128.112.225	192.168.2.108	SHB2	178	Lock Request
19113	16.123975	10.128.112.225	192.168.2.108	SHB2	178	Lock Request
19107	16.120319	10.128.112.225	10.128.112.225	SHB2	126	Lock Response
19114	16.125862	10.128.112.225	10.128.112.225	SHB2	126	Lock Response
19106	16.120237	10.128.112.225	10.128.112.225	SHB2	130	Lock Response, Error: STATUS_PENDING
1 0.000000	10.128.113.25	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
488.8147474	10.128.181.28	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1	
> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 'DeviceWPF-[414FC362-8DF7-4B81-AA2E-58BF2D80C14a'						
> Ethernet II, Src: IntelCor_58:b1:b0 (0c:09:1b:58:b1:b0), Dst: IPv4mcast_7f:ff:ff (01:00:5e:7f:ff:ff)						
> Internet Protocol Version 4, Src: 10.128.113.25, Dst: 239.255.255.250						
> User Datagram Protocol, Src Port: 52733, Dst Port: 1900						
> Simple Service Discovery Protocol						
0000	01 00 9d 7f ff fa bc 09	1b 58 ba 60 08 45 00	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	...----- X----- E-----	
0010	00 cb 9b 6d 00 00 01 11	b2 29 00 78 71 19 ef ff	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	...----- x(q-----	
0020	00 ff fa cd fd 07 06 00 67	3f eb 4d 22 53 45 1f 00	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	...----- 1----- 7-----	
0030	43 48 28 2a 20 48 54 54	50 2b 31 2e 01 00 08 04	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	CH ----- P/1.1----- H-----	
0040	4f 53 54 3a 20 32 33 39	2b 32 35 32 35 32 35 35	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	OSt----- 239.255.255.250----- 0:MAN-----	
0050	2e 32 35 30 3a 21 39 30	30 00 00 00 00 00 00 00	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	.250:190----- 0:MAN-----	
0060	22 73 63 74 60 70 3a 64	69 73 67 65 76 72 22 0d	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	sd----- pdi----- score-----	
0070	08 4d 24 64 75 6c 60 72	53 61 62 63 64 65 66 67	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	PM----- 1----- u----- w-----	
0080	64 65 66 67 68 69 6a 6b	60 73 74 75 72 73 65 66	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	----- 0:MAN----- 0:MAN----- 0:MAN----- 0:MAN-----	
0090	62 67 63 73 65 72	76 69 63 65 3a 64 69 61	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	----- 0:MAN----- 0:MAN----- 0:MAN----- 0:MAN-----	
00a0	63 3a 01 04 05 55 45 52	24 41 47 45 46 54 53	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	1:1----- USE R:AGENT-----	
00b0	20 4d 69 63 72 6f 73 6f	66 74 20 45 64 67 65 2f	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	Hicresr f Edge/-----	
00c0	31 31 32 2a 30 2e 31 37	32 32 2e 33 38 20 57 69	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	11.0.17.22.58 94-----	
00d0	6e 64 6f 77 73 00 00 00	00 00 00 00 00 00 00 00	5e 00 00 00 00 00 00 00	ff ff ff ff ff ff ff ff	ndows-----	

2. Tcp:

a. Tcp



Class: S V B Tech

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

b. Port

c. Ack



Department of Computer Engineering

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

d. Payload

3. Arp:



Department of Computer Engineering
Class: S.Y. B.Tech. Semester: IV

Class: S V B Tech

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

4. Udp:

The screenshot shows a Wi-Fi network monitor interface with various tabs like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and a search bar. The main pane displays a list of network traffic entries. A detailed view of a selected entry (No. 1) is shown on the right, including fields for Time, Source, Destination, Protocol, Length, Info, and a large hex dump section.

5. Http:



Department of Computer Engineering

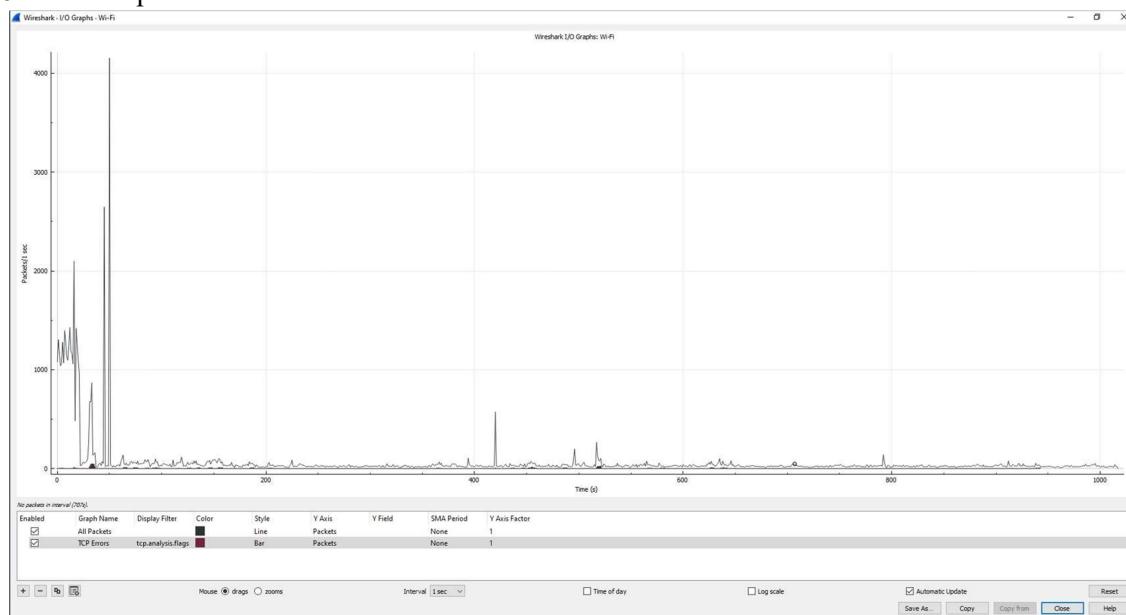
Class: S.Y. B.Tech.

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

6. I/O Graph:



Conclusion: Thus, we have simulated Packet Capturing in Wireshark.