



Department of CSE (ICB)

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJS22ICL402

Course Name: Computer Networks Lab

Name: Divy Arun Mav

SAP ID: 60019220133

## Experiment No: 8

**Aim:** To analyze different captured packets using Wireshark tool.

### **Theory:**

Wire shark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Here are some reasons people use Wire shark:

- Network administrators use it to troubleshoot network problems
  - Network security engineers use it to examine security problems
  - QA engineers use it to verify network applications
  - Developers use it to debug protocol implementations
- People use it to learn network protocol internals Features The

following are some of the many features Wire shark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.



Department of CSE (ICB)

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJS22ICL402

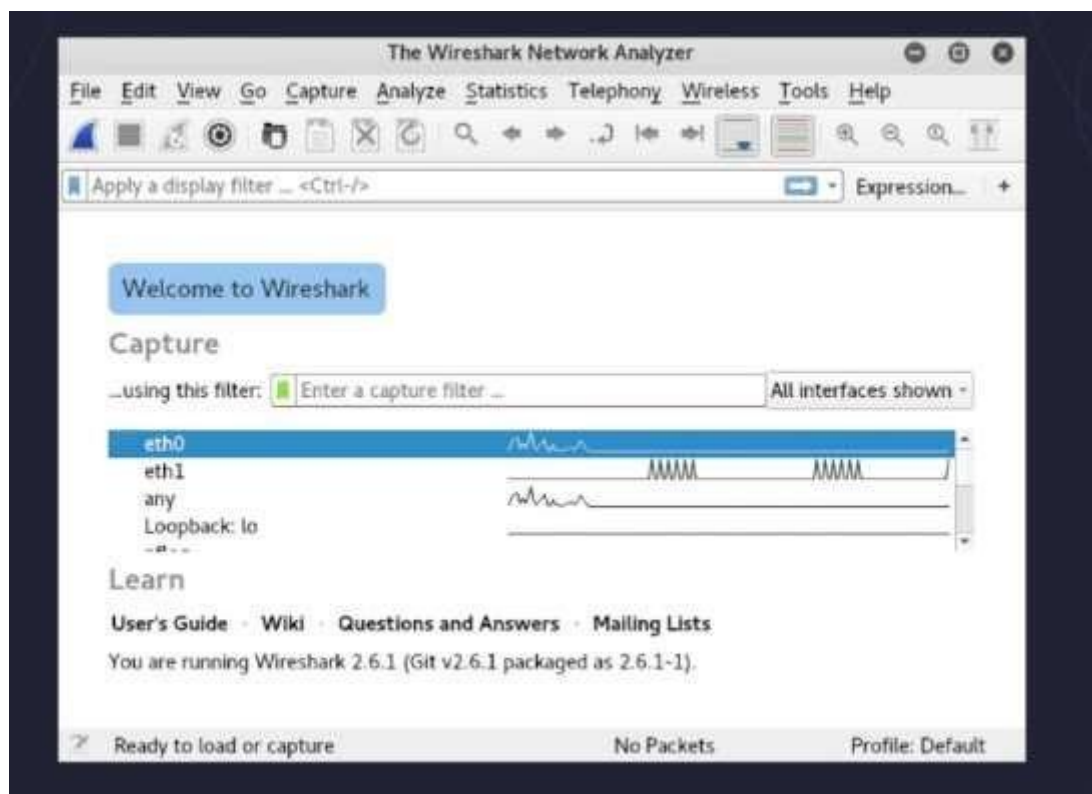
Course Name: Computer Networks Lab

## Data Packets on Wireshark

Now that we have Wireshark installed let's go over how to enable the Wireshark packet sniffer and then analyze the network traffic.

## Capturing Data Packets on Wireshark

When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see



You can select one or more of the network interfaces using “shift left-click.” Once you have the network interface selected, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled “Start Capturing Packets.”



SHRI VILEPARLE KELAVANI MANDAL'S  
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING  
(Autonomous College Affiliated to the University of Mumbai)  
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



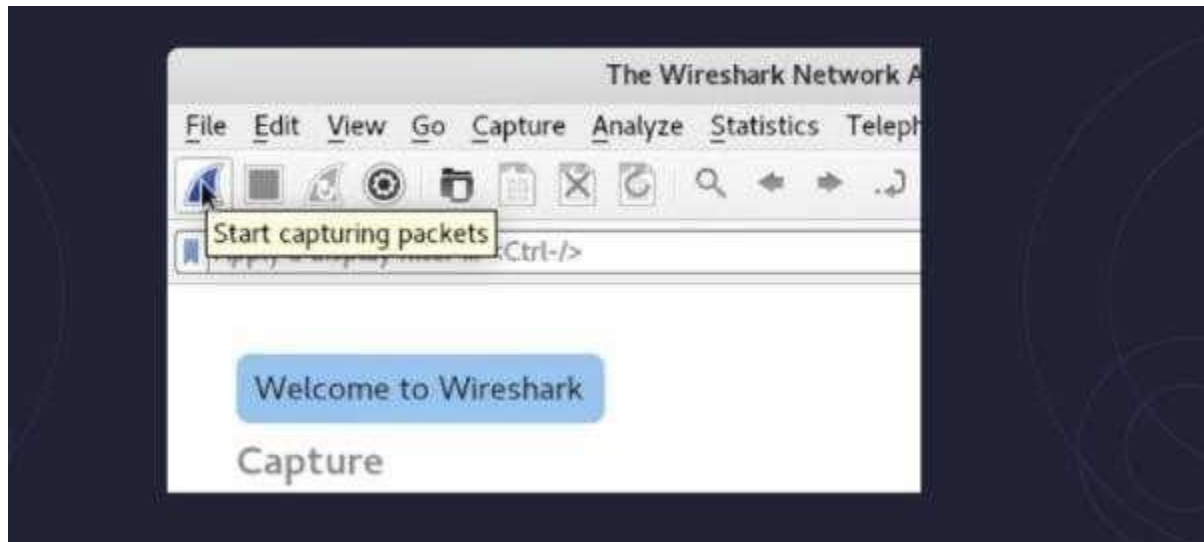
Department of CSE (ICB)

Class: S.Y. B.Tech.

Semester: IV

Course Code: DJS22ICL402

Course Name: Computer Networks Lab



You can select the menu item Capture -> Start.



**SHRI VILEPARLE KELAVANI MANDAL'S  
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**

(Autonomous College Affiliated to the University of Mumbai)

NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

Department of Computer Science and engineering(IoT, Cyber security with block chain technology)



**Class: S.Y. B.Tech.**

**Semester: IV**

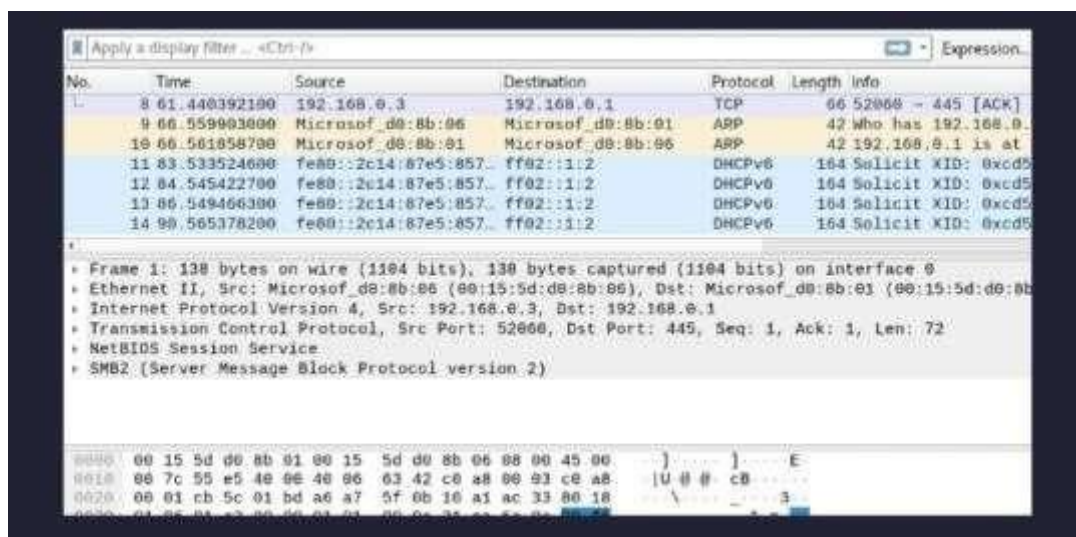
**Course Code: DJS22ICL402**

**Course Name: Computer Networks Lab**



Or you could use the keystroke Control – E.

During the capture, Wire shark will show you the packets that it captures in real-time.



Student should Capture packet of TCP,UDP, HTTP, FTP using wireshark



**SHRI VILEPARLE KELAVANI MANDAL'S  
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**  
(Autonomous College Affiliated to the University of Mumbai)



NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

Department of Computer Science and engineering(IoT, Cyber security with block chain technology)

**Class: S.Y. B.Tech.**

**Semester: IV**

**Course Code: DJS22ICL402**

**Course Name: Computer Networks Lab**

Wireshark packet capture analysis of an ARP request. The packet list shows an ARP request from 10.120.31.230 to 235.5.5.5. The packet details show the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes show the raw data of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.120.31.230	235.5.5.5	UDP	180	42605 → 58581 Len=138
2	0.002436	10.120.31.230	10.120.31.255	UDP	180	42996 → 58581 Len=138
3	0.144117	169.254.80.102	235.5.5.5	UDP	180	33869 → 58581 Len=138
4	0.151231	169.254.80.102	169.254.255.255	UDP	180	36777 → 58581 Len=138
5	0.281375	Cisco:c8:2a:c9	Broadcast	ARP	60	Who has 10.120.34.26? Tell 10.120.34.1
6	0.387751	SamsungE_d4:0b:8d	Broadcast	ARP	60	Who has 10.120.31.17? Tell 10.120.31.230
7	0.396338	HP:95:ea:1b	Broadcast	ARP	60	Who has 10.120.34.50? Tell 10.120.34.21
8	0.502449	10.120.31.230	235.5.5.5	UDP	180	42605 → 58581 Len=138
9	0.505337	10.120.31.230	10.120.31.255	UDP	180	42996 → 58581 Len=138
10	0.541698	10.120.31.121	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
11	0.554910	Cisco:c8:2a:c9	Broadcast	ARP	60	Who has 10.120.34.73? Tell 10.120.34.1
12	0.646967	169.254.80.102	235.5.5.5	UDP	180	33869 → 58581 Len=138
13	0.653597	169.254.80.102	169.254.255.255	UDP	180	36777 → 58581 Len=138
14	0.916196	10.120.34.54	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
15	1.005388	10.120.31.230	235.5.5.5	UDP	180	42605 → 58581 Len=138
16	1.007165	10.120.31.230	10.120.31.255	UDP	180	42996 → 58581 Len=138
17	1.149384	169.254.80.102	235.5.5.5	UDP	180	33869 → 58581 Len=138
18	1.156504	169.254.80.102	169.254.255.255	UDP	180	36777 → 58581 Len=138
19	1.201778	10.120.34.32	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
20	1.507310	10.120.31.230	235.5.5.5	UDP	180	42605 → 58581 Len=138
21	1.509306	10.120.31.230	10.120.31.255	UDP	180	42996 → 58581 Len=138
22	1.547743	10.120.31.121	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
23	1.637902	HP:95:ea:1b	Broadcast	ARP	60	Who has 10.120.34.50? Tell 10.120.34.21
24	1.652149	169.254.80.102	235.5.5.5	UDP	180	33869 → 58581 Len=138
25	1.658558	169.254.80.102	169.254.255.255	UDP	180	36777 → 58581 Len=138

Frame 3: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface \Device\NPF\_{248EE483-960F-42CF-9CA1-2283819AE096}

Ethernet II, Src: SamsungE\_d4:0b:9f (8:ea:4d:0b:9f), Dst: IPv4mcast\_05:05:05 (01:00:5e:05:05:05)

Internet Protocol Version 4, Src: 169.254.80.102, Dst: 235.5.5.5

User Datagram Protocol, Src Port: 33869, Dst Port: 58581

Data (138 bytes)

```
0000  01 00 5e 05 05 05 8c ea 48 dd 00 9f 08 00 45 00  ...^...H...E...
0010  00 46 00 55 40 00 40 11 7f 62 a9 fe 50 66 eb 05  ...@B...PF...
0020  05 05 84 d4 e4 d5 00 92 a2 fb af fd 10 01 00 af  ...H...
0030  00 00 00 7e 41 43 5b 53 69 67 6e 61 67 65 5d 20  ...--C[S ignore]
0040  53 61 6d 73 75 6e 67 20 51 46 52 20 53 65 72 69  Samsung QWR SerI
0050  65 73 3e 3e 3e 3e 30 58 30 37 3e 3e 3e 3e 30 3e  es>>>BX 07>>>B
0060  3e 3e 3e 30 58 30 31 3e 3e 3e 34 37 36 34 39  >>>X01> >>>47649
0070  31 37 37 36 30 3e 3e 3e 3e 34 35 30 38 34 33 34  17760>> >4580434
0080  34 33 32 3e 3e 3e 3e 54 2d 4b 54 4d 32 45 4c 41  432>>>T <T02ELA
0090  4b 55 43 2d 32 32 32 30 2e 35 3e 3e 3e 3e 38 63  KUC-2220 >5>>>8c
00a0  3a 65 61 3a 34 38 3a 64 64 3a 30 62 3a 39 66 3e  rea:48:d d:0b:9f>
00b0  3e 3e 3e 30 >>>B
```

**Conclusion:** Successfully analyzed different captured packets using Wireshark tool.