

Terna Engineering College

Computer Engineering Department

Class: TE

Sem.: VI

Course: System Security Lab

PART A

(PART A: TO BE REFERRED BY STUDENTS)

Experiment No.05

A.1 Aim:

Design a network and implement packet sniffing on telnet traffic using Wireshark.

A.2 Prerequisite:

Basic Knowledge of IP addresses, port numbers, TCP and UDP Protocols.

A.3 Outcome:

After the successful completion of this experiment, students will be able to apply basic network commands to gather basic network information.

A.4 Theory:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real-time and display them in a human-readable format. Wireshark includes filters, colour-coding and other features that let you dig deep into network traffic and inspect individual packets.

Features of Wireshark :

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

Capturing Packets

After downloading and installing Wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

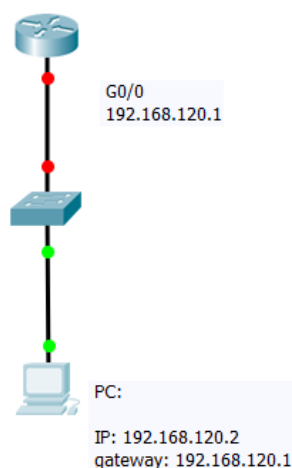
Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large number of packets to sift through. That's where Wireshark's filters come in. The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type `—dnsll` and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

A5. Interface Configuration table

SNO.	NAME OF THE DEVICE	INTERFACE	IP ADDRESS	Subnet Mask	Default Gateway
1.	Router 0	g0/0	192.168.120.1	255.255.255.0	-----
2.	PC	Fast Ethernet	192.168.120.2	255.255.255.0	192.168.120.1

A6. Design



PART B

(PART B: TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)

Roll No. 50	Name: AMEY THAKUR
Class: Comps TE B	Batch: B3
Date of Experiment: 30/03/2021	Date of Submission: 30/03/2021
Grade:	

B.1 Output

The screenshot shows the Wireshark interface with a capture of network traffic on the 'Wi-Fi' interface. The packet list shows 30 UDP packets from 142.250.82.17 to 192.168.43.246. The details pane for the first packet (No. 1) is expanded, showing the following structure:

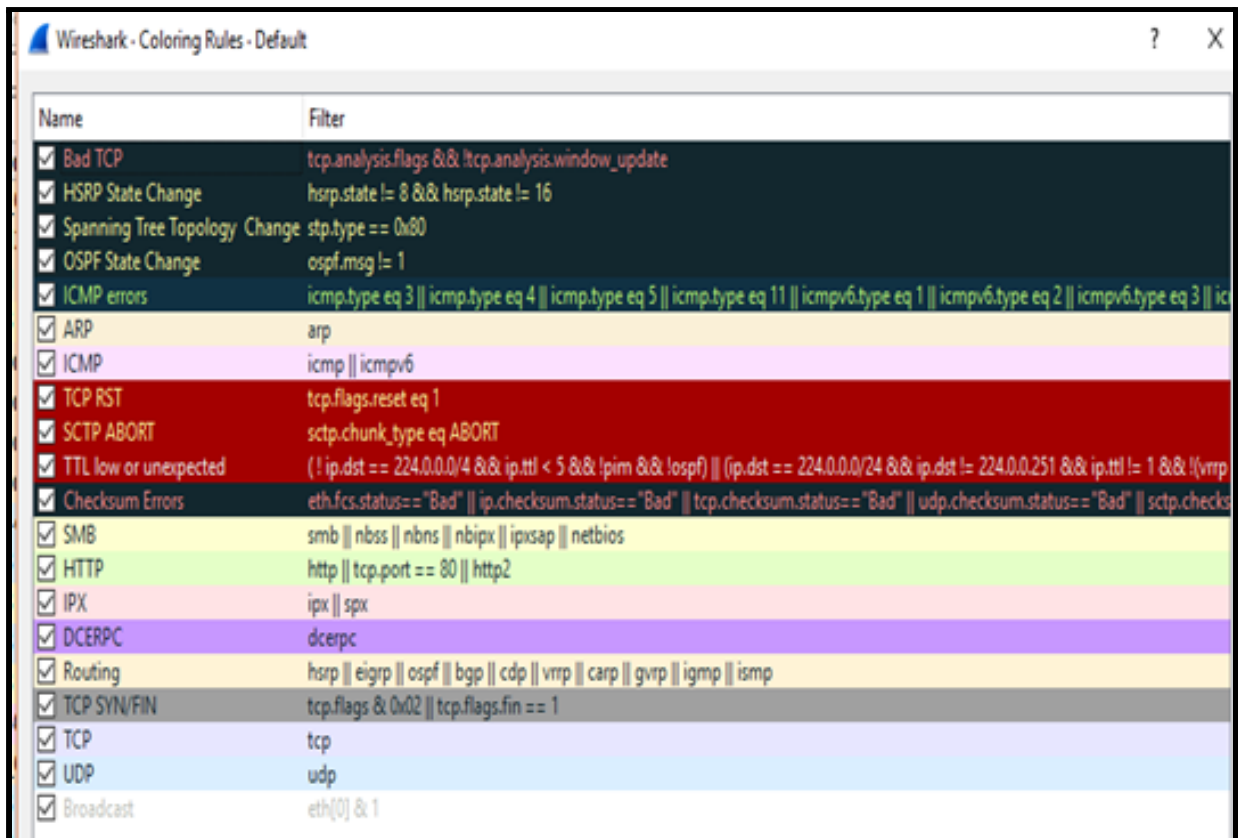
- Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0
- Ethernet II, Src: 76:c1:61:1e:a6:6b (76:c1:61:1e:a6:6b), Dst: 66:a1:ec:eb:9b:7d (66:a1:ec:eb:9b:7d)
- Internet Protocol Version 4, Src: 142.250.82.17, Dst: 192.168.43.246
- User Datagram Protocol, Src Port: 19305, Dst Port: 59156
- Data (38 bytes)

The raw data (hex and ASCII) for the first packet is as follows:

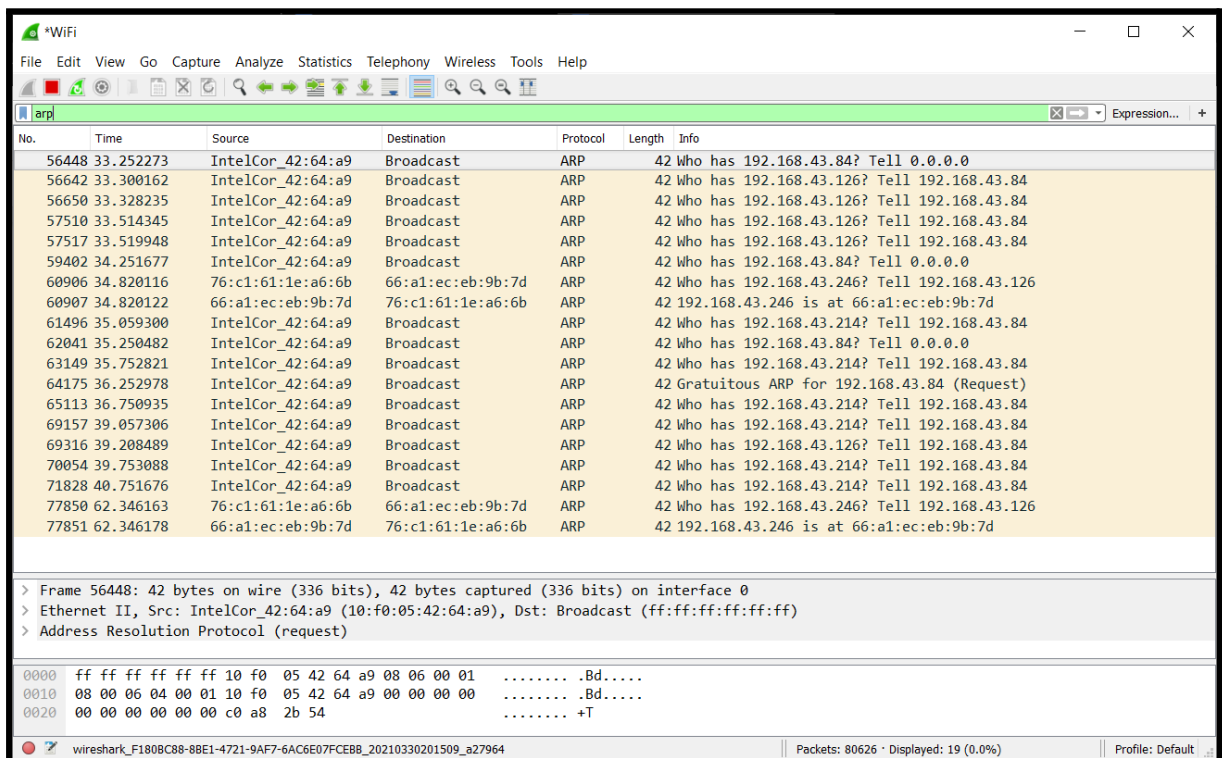
```

0000  66 a1 ec eb 9b 7d 76 c1 61 1e a6 6b 08 00 45 60  f....}v. a..k..E`
0010  00 42 07 ac 00 00 3b 11 a9 f5 8e fa 52 11 c0 a8  .B....;. ....R...
0020  2b f6 4b 69 e7 14 00 2e 05 6d 8f cd 00 05 07 c1  +.Ki.... .m.....
0030  9e 95 81 b5 2d e9 34 59 4a 60 34 c5 9a 47 05 de  ....-4Y J`4..G...
0040  07 a0 80 00 01 38 92 f0 30 91 cc ac 11 b8 95 d1  ....8.. 0.....
  
```

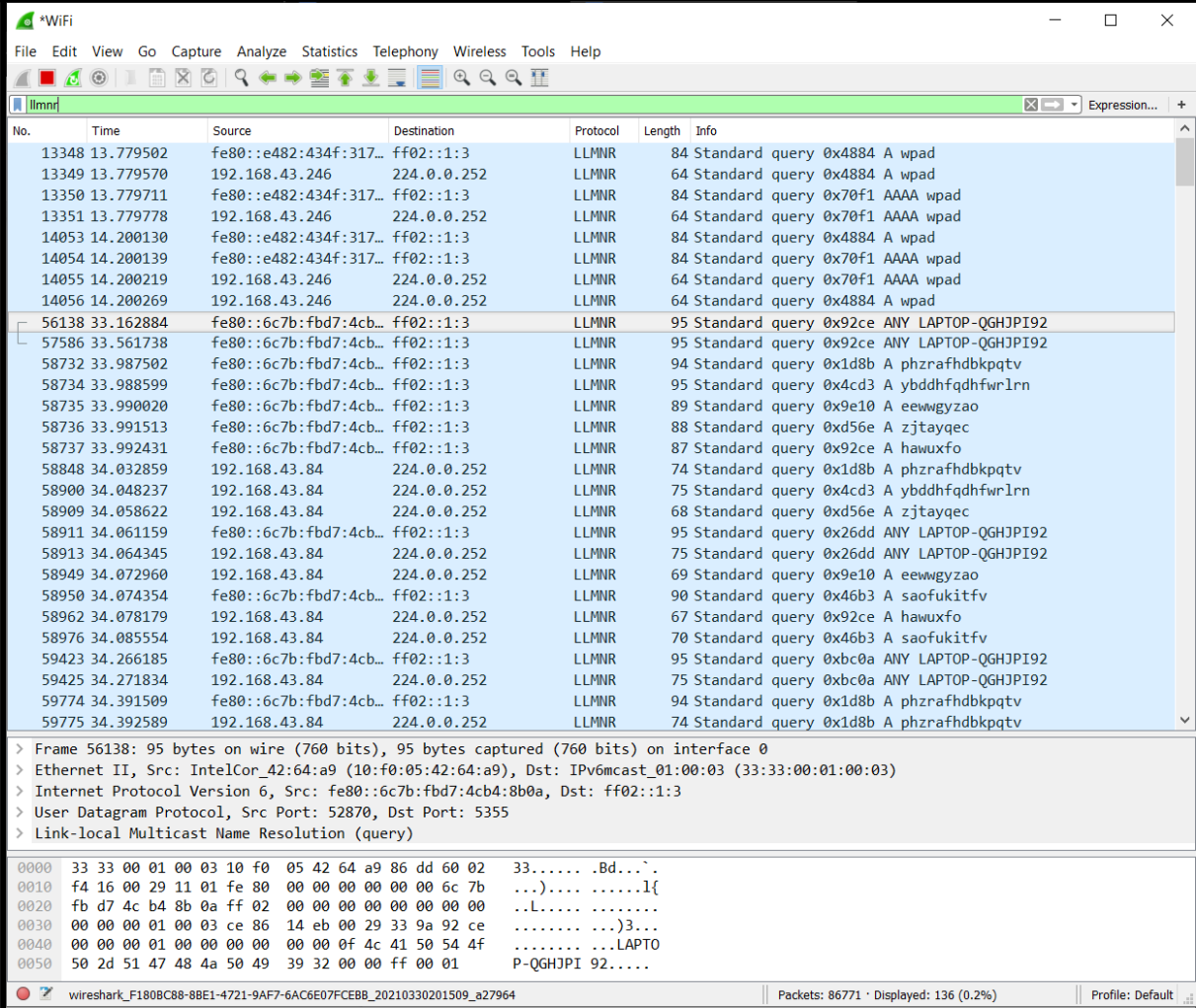
At the bottom, the status bar indicates: wireshark_F180BC88-8BE1-4721-9AF7-6AC6E07FCEB8_20210330201142_a30460 | Packets: 3736 · Displayed: 3736 (100.0%) | Profile: Default



Filtering of packets(ARP):



Filtering packets (LLMNR):



Wireshark packet capture showing LLMNR queries. The packet list shows multiple LLMNR queries from source 192.168.43.246 to destination ff02::1:3. The packet details for frame 56138 show the LLMNR query structure.

No.	Time	Source	Destination	Protocol	Length	Info
13348	13.779502	fe80::e482:434f:317...	ff02::1:3	LLMNR	84	Standard query 0x4884 A wpad
13349	13.779570	192.168.43.246	224.0.0.252	LLMNR	64	Standard query 0x4884 A wpad
13350	13.779711	fe80::e482:434f:317...	ff02::1:3	LLMNR	84	Standard query 0x70f1 AAAA wpad
13351	13.779778	192.168.43.246	224.0.0.252	LLMNR	64	Standard query 0x70f1 AAAA wpad
14053	14.200130	fe80::e482:434f:317...	ff02::1:3	LLMNR	84	Standard query 0x4884 A wpad
14054	14.200139	fe80::e482:434f:317...	ff02::1:3	LLMNR	84	Standard query 0x70f1 AAAA wpad
14055	14.200219	192.168.43.246	224.0.0.252	LLMNR	64	Standard query 0x70f1 AAAA wpad
14056	14.200269	192.168.43.246	224.0.0.252	LLMNR	64	Standard query 0x4884 A wpad
56138	33.162884	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	95	Standard query 0x92ce ANY LAPTOP-QGHJPI92
57586	33.561738	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	95	Standard query 0x92ce ANY LAPTOP-QGHJPI92
58732	33.987502	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	94	Standard query 0x1d8b A phzrafhdbkptv
58734	33.988599	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	95	Standard query 0x4cd3 A ybdfhfdhfwlrln
58735	33.990020	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	89	Standard query 0x9e10 A eewwgyzao
58736	33.991513	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	88	Standard query 0xd56e A zjtayqec
58737	33.992431	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	87	Standard query 0x92ce A hawuxfo
58848	34.032859	192.168.43.84	224.0.0.252	LLMNR	74	Standard query 0x1d8b A phzrafhdbkptv
58900	34.048237	192.168.43.84	224.0.0.252	LLMNR	75	Standard query 0x4cd3 A ybdfhfdhfwlrln
58909	34.058622	192.168.43.84	224.0.0.252	LLMNR	68	Standard query 0xd56e A zjtayqec
58911	34.061159	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	95	Standard query 0x26dd ANY LAPTOP-QGHJPI92
58913	34.064345	192.168.43.84	224.0.0.252	LLMNR	75	Standard query 0x26dd ANY LAPTOP-QGHJPI92
58949	34.072960	192.168.43.84	224.0.0.252	LLMNR	69	Standard query 0x9e10 A eewwgyzao
58950	34.074354	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	90	Standard query 0x46b3 A saofukitfv
58962	34.078179	192.168.43.84	224.0.0.252	LLMNR	67	Standard query 0x92ce A hawuxfo
58976	34.085554	192.168.43.84	224.0.0.252	LLMNR	70	Standard query 0x46b3 A saofukitfv
59423	34.266185	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	95	Standard query 0xbc0a ANY LAPTOP-QGHJPI92
59425	34.271834	192.168.43.84	224.0.0.252	LLMNR	75	Standard query 0xbc0a ANY LAPTOP-QGHJPI92
59774	34.391509	fe80::6c7b:fb7:4cb...	ff02::1:3	LLMNR	94	Standard query 0x1d8b A phzrafhdbkptv
59775	34.392589	192.168.43.84	224.0.0.252	LLMNR	74	Standard query 0x1d8b A phzrafhdbkptv

Frame 56138: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
Ethernet II, Src: IntelCor_42:64:a9 (10:f0:05:42:64:a9), Dst: IPv6mcast_01:00:03 (33:33:00:01:00:03)
Internet Protocol Version 6, Src: fe80::6c7b:fb7:4cb4:8b0a, Dst: ff02::1:3
User Datagram Protocol, Src Port: 52870, Dst Port: 5355
Link-local Multicast Name Resolution (query)

0000 33 33 00 01 00 03 10 f0 05 42 64 a9 86 dd 60 02 33.....Bd...
0010 f4 16 00 29 11 01 fe 80 00 00 00 00 00 00 6c 7b ...}).....1{
0020 fb d7 4c b4 8b 0a ff 02 00 00 00 00 00 00 00 00 ..L.....
0030 00 00 00 01 00 03 ce 86 14 eb 00 29 33 9a 92 ce})3...
0040 00 00 00 01 00 00 00 00 00 00 0f 4c 41 50 54 4fLAPTO
0050 50 2d 51 47 48 4a 50 49 39 32 00 00 ff 00 01 P-QGHJPI 92.....

B.2 Commands/tools used with the syntax:

- WIFI PACKET SNIFFING
- arp
- llmnr

B.3 Question of Curiosity:

1. Which command is need to configure telnet in the router?

Ans:

SWITCH command.

2. What are the steps needed to extract data from sniffed traffic?

Ans:

Step 1: Isolate the desired data stream

- This is most easily done by selecting a packet within the stream containing the data you want to extract and selecting "Follow TCP (or UDP) Stream" from the right-click context menu. Wireshark applies a display filter to the packet list so that only packets from the selected stream are shown, and it invokes the stream content window

Step 2: Extract raw unidirectional data

- Wireshark marks transmitted and received data in red and blue, respectively. For this example, we're only interested in the received data, so we restrict the stream parser to show only inbound (blue) packets by selecting that direction from the option at the bottom.
 - Now to extract this data. Ensure that the Raw option is selected and click Save As to export the binary data. For our example, I've saved the dump to disk as "example.raw".
 - What we have now is an HTTP response and a JPEG image smooshed together in a single binary blob; this isn't of much use.
 - `$ file example.raw`
 - `example.raw: data`
 - We can use the foremost forensics utility to sift through this blob and extract any recognizable binary data structures (e.g. a JPEG image).
 - `$ foremost -v -i example.raw`
3. What type of packets to be filtered for accessing remote login username and a password of a router?

Ans:

- The main protection against unauthorized access to a router is a password. Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) authentication servers are the most effective method of password management and use the Cisco AAA method. It is rare for a router not to have local password privileged access.
- The command that is used to set the password for privileged administrative access to the system enables secret. The enable secret password should always be set. The enable password command uses a weak encryption algorithm and should not be used. Always ensure that enable secret is set on the router. Failure to set the enabled secret password may result in the console password being able to get privileged access even from a remote virtual type terminal (VTY) session.

B.4 Conclusion:

(Write an appropriate conclusion.)

We learned to design a network and implement packet sniffing on telnet traffic using Wireshark.