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.

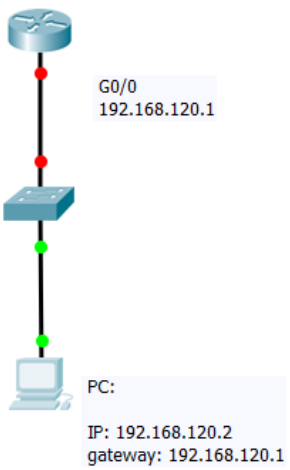
Filtering Packets

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 ―dns‖ 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



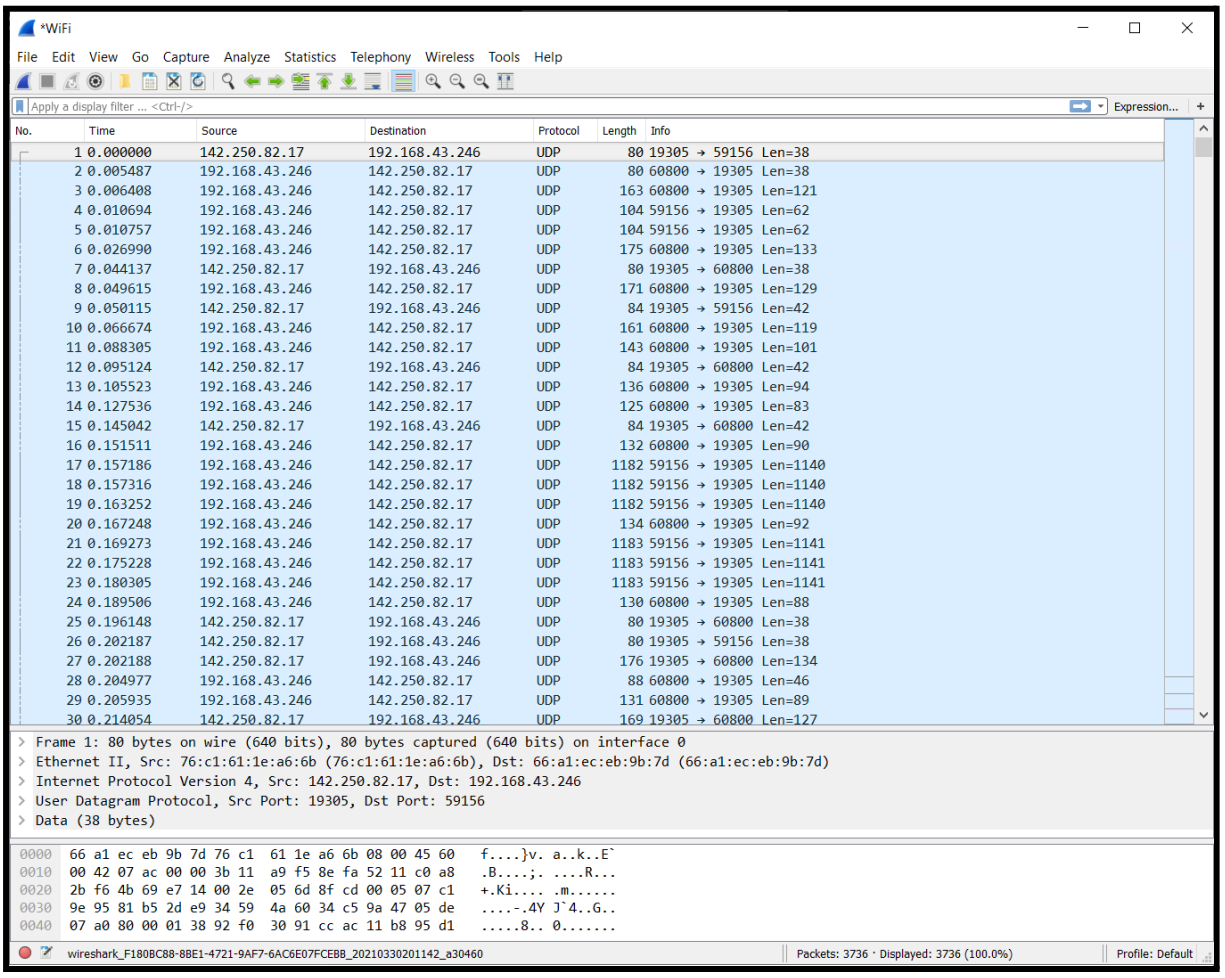
PART B

(PART B: TO BE COMPLETED BY STUDENTS)

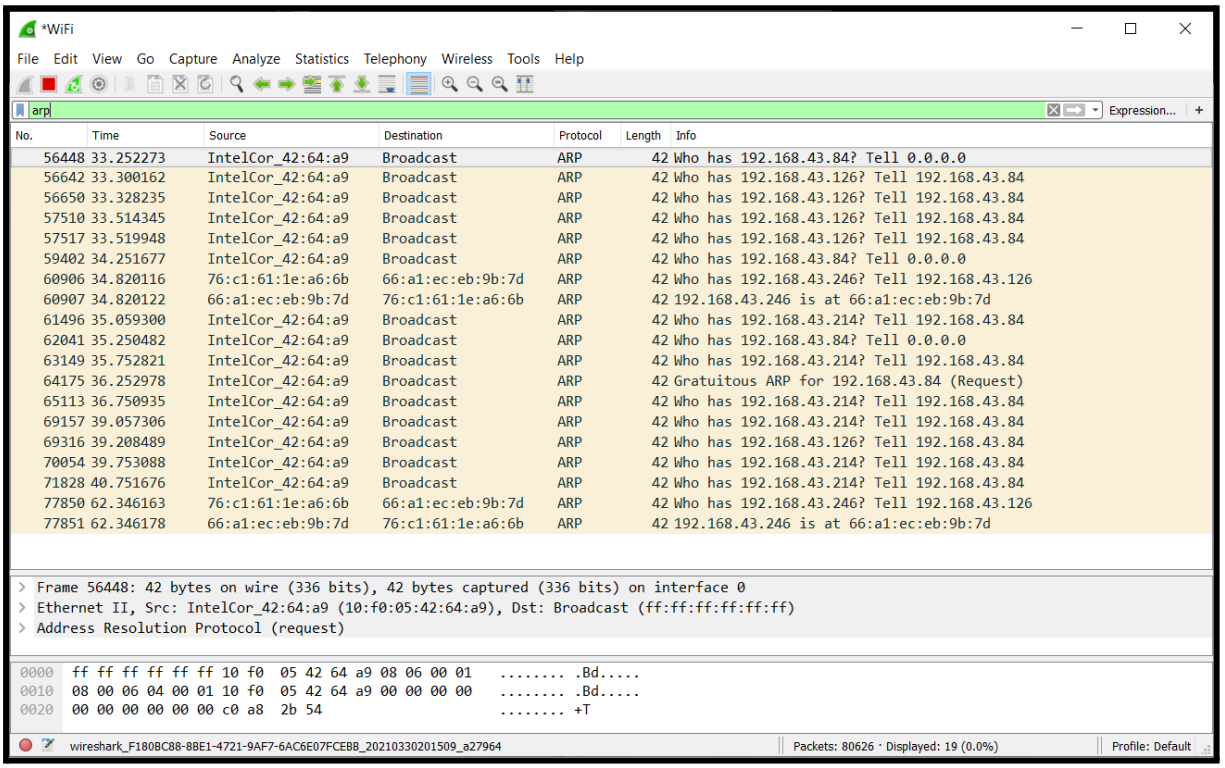
(Students must submit the soft copy as per the following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case there is no Blackboard access available)

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:	

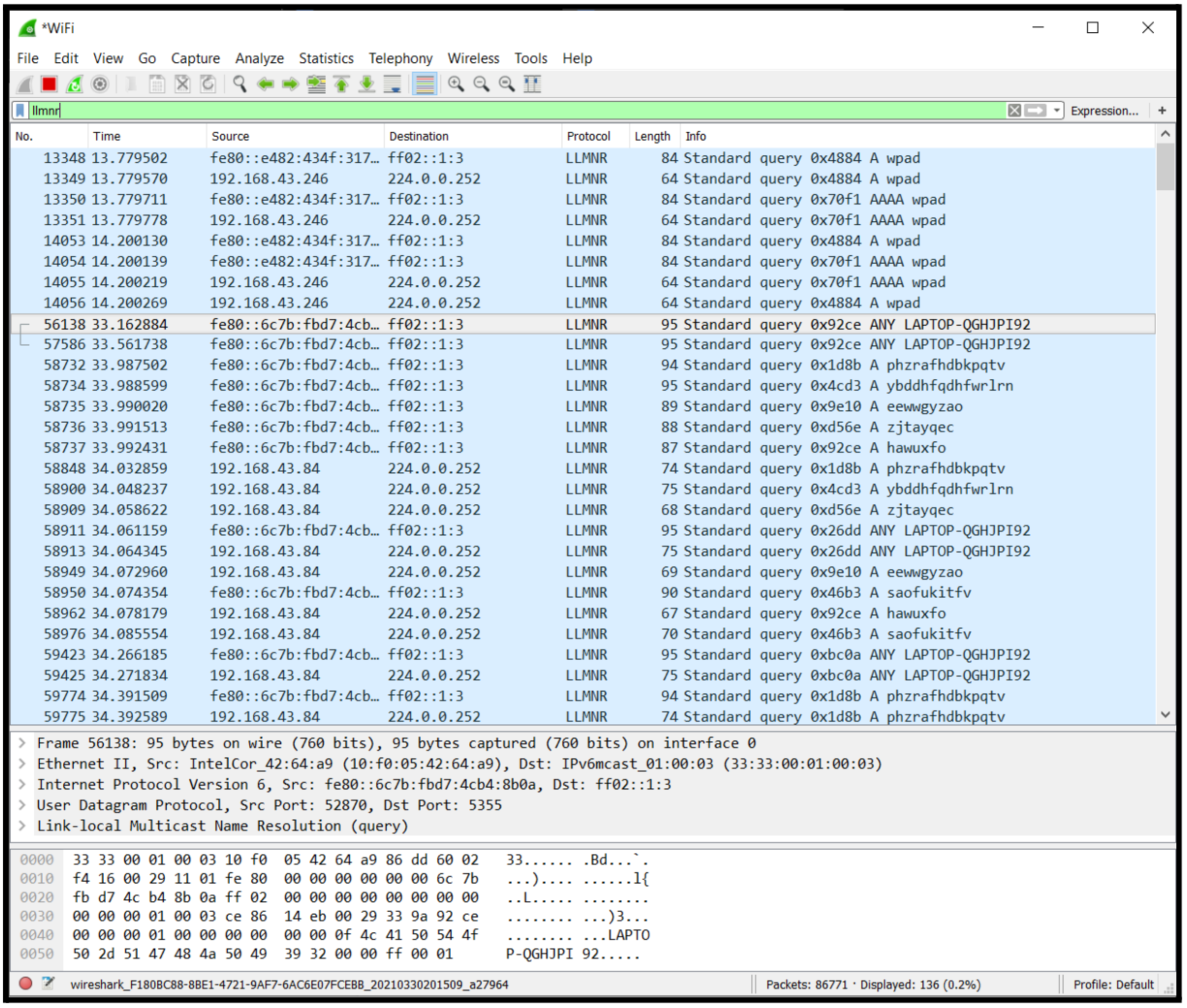
B.1 Output



Filtering of packets(ARP):



Filtering packets (LLMNR):



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.