Finolex Academy of Management and Technology, Ratnagiri

Department of Information Technology

Subject:	**Networking Lab (ITL401)**		
Class:	**SE IT / Semester – IV (CBCGS) / Academic year: 2017-18**		
Name of Student:	**Kazi Jawwad A Rahim**		
Roll No:	**28**	**Date of performance (DOP) :**	
Experiment No:	**10**	**Date of checking (DOC) :**	
Title: To analyze the packets using Packet sniffer Wireshark.			
Marks:		**Teacher's Signature:**	

1. Aim: **To analysis the packets using Packet sniffer Wireshark**

2. Prerequisites:

Knowledge of

1. Ubuntu Commands
2. NS2 commands

3. Hardware Requirements:

1. PC with minimum 2GB RAM

4. Software Requirements:

1. Linux (Ubuntu 10.04)
2. ns-2.34 package
3. Wireshark package

5. Learning Objectives:

1. To analyze the contents the packets of different protocols
2. To install packet sniffer Wireshark on Ubuntu.

6. Course Objectives Applicable: LO 4

7. Program Outcomes Applicable: PO2, PO4

8. Program Education Objectives Applicable: 1, 3

9. Theory:

Wireshark is an open source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorizing packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files.

Wireshark can be used for network troubleshooting, to investigate security issues, and to analyse and understand network protocols. The packet sniffer can exploit information passed in plaintext, i.e. not encrypted. Examples of protocols which pass information in plaintext are Telnet, FTP, SNMP, POP, and HTTP.

Procedure:

Running Wireshark When run the Wireshark program, the Wireshark graphical user interface shown in Figure 1 will be displayed. Initially, no data will be displayed in the various windows.

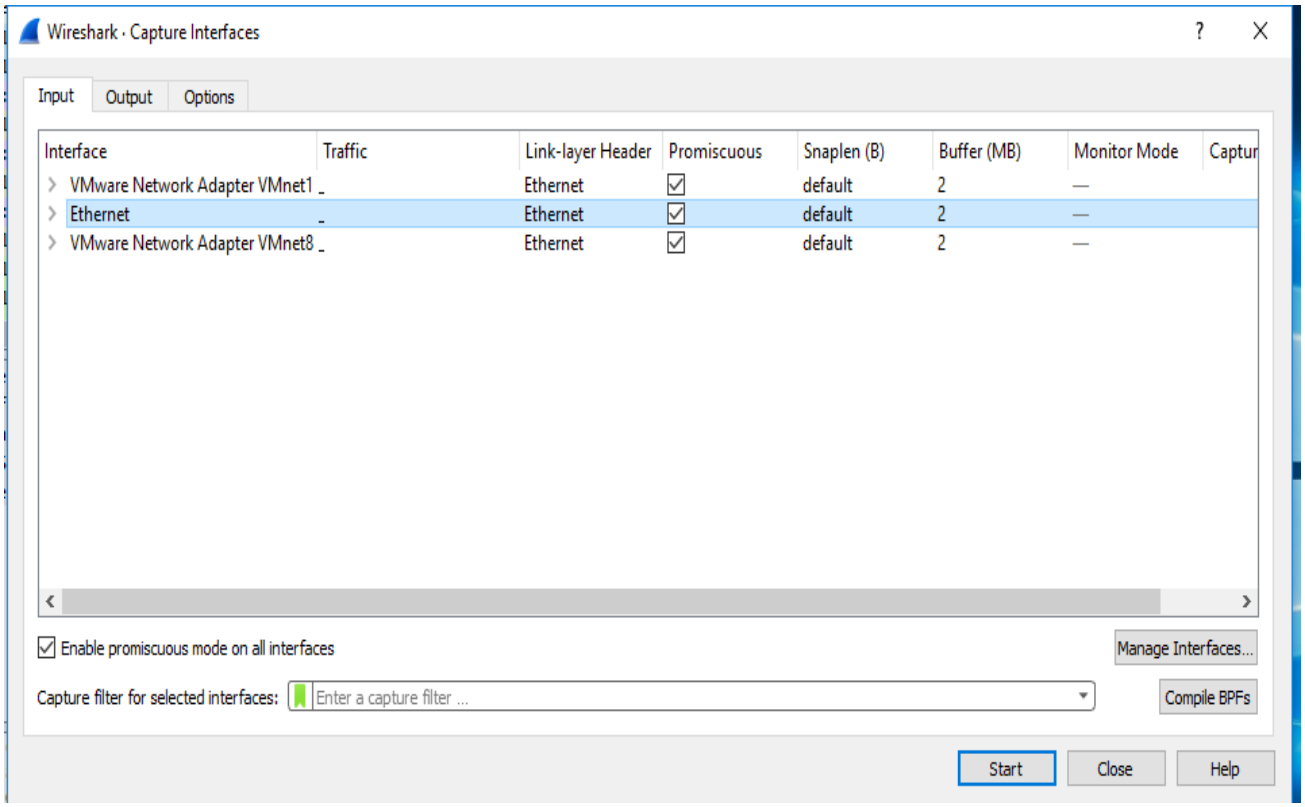

Figure 1- Selecting an interface on which to perform your packet capture

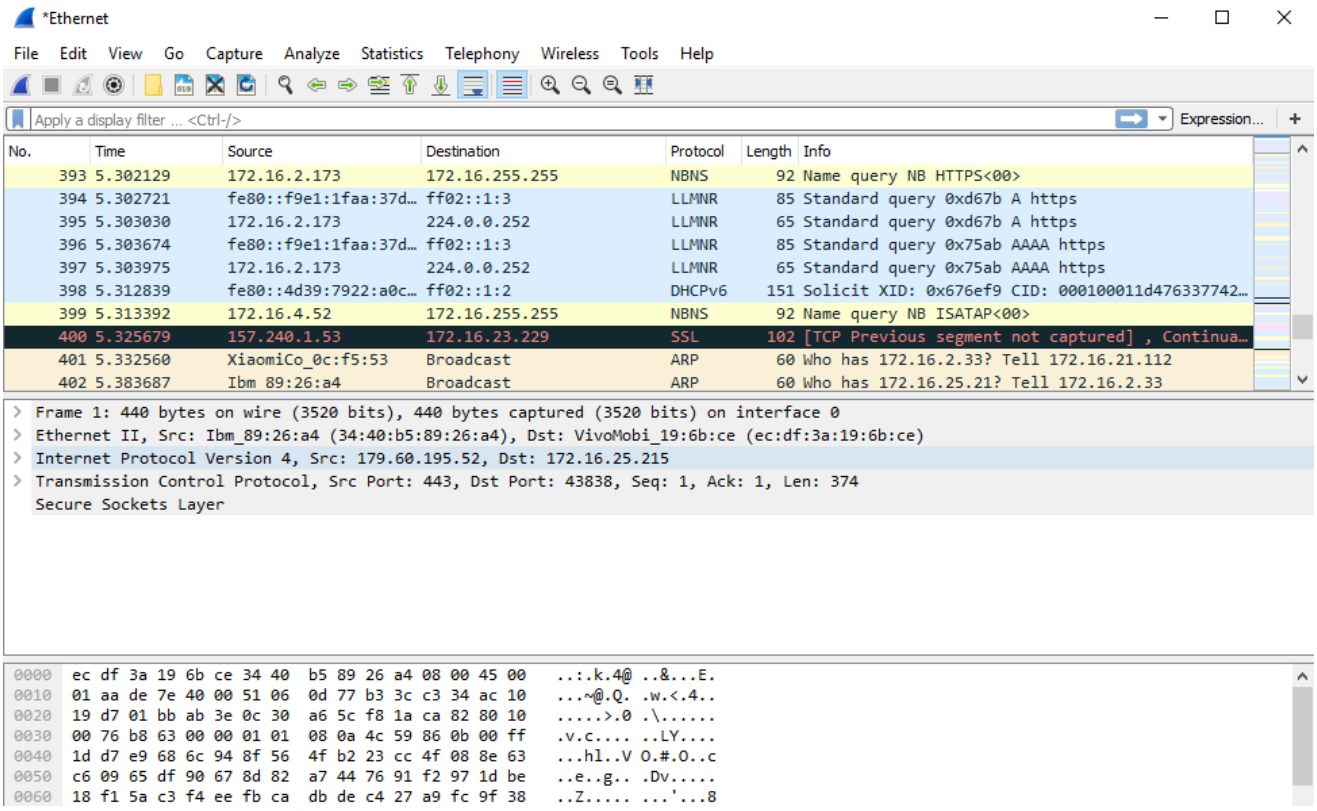

Figure 2- The Wireshark main window uses a three-pane design.

In figure 2 all of the packets captured are displayed and broken down into a more understandable format.
Here's what each pane contains:

Packet List:-
The top pane displays a table containing all packets in the current capture file. It has columns containing the packet number, the relative time the packet was captured, the source and destination of the packet, the packet's protocol, and some general information found in the packet.

Packet Details:-
The middle pane contains a hierarchical display of information about a single packet. This display can be collapsed and expanded to show all of the information collected about an individual packet.

Packet Bytes:-
The lower pane—perhaps the most confusing—displays a packet in its raw, unprocessed form; that is, it shows what the packet looks like as it travels across the wire. This is raw information with nothing warm or fuzzy to make it easier to follow.

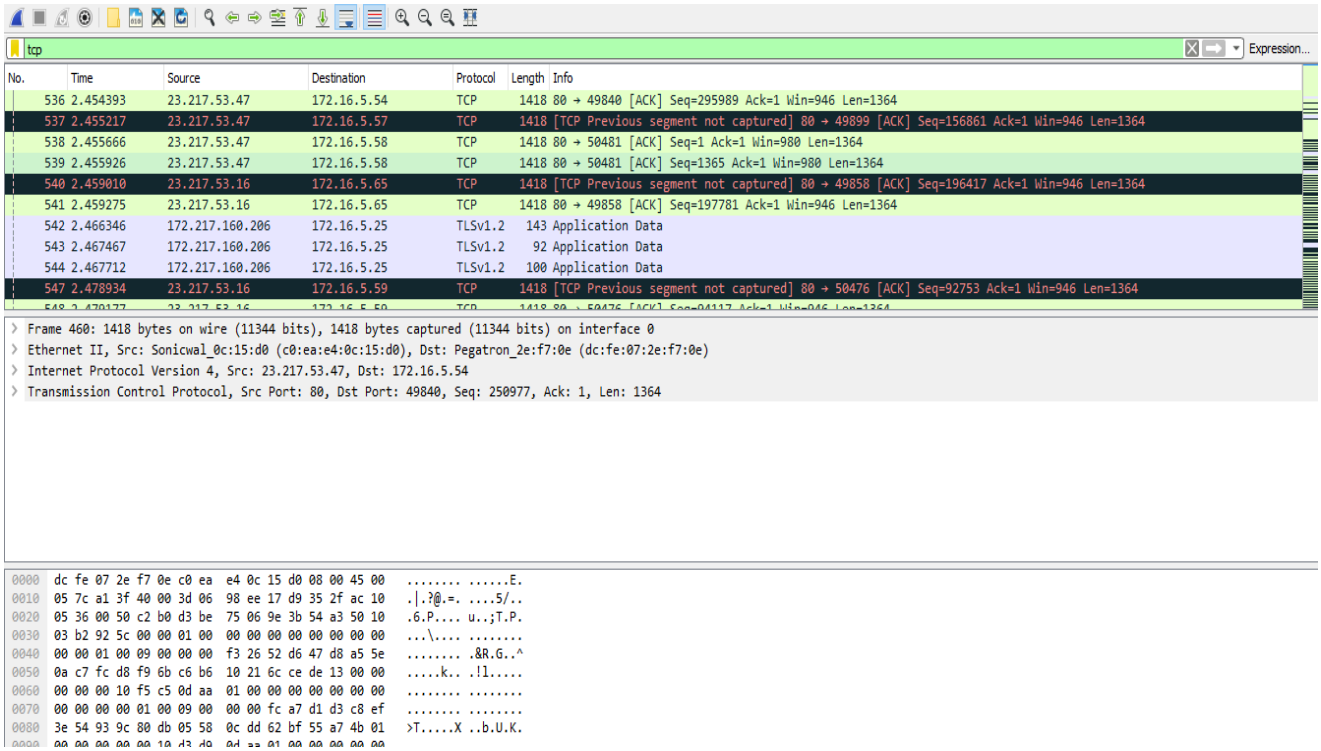

Figure 3- Wireshark's color coding allows for quick protocol identification

Each packet is displayed as a certain color for a reason. These colors reflect the packet's protocol. For example, all DNS traffic is blue, and all HTTP traffic is green. The color coding allows you to quickly differentiate between various protocols so that you don't need to read the protocol field in the Packet List pane for each individual packet.
Wireshark makes it easy to see which colors are assigned to each protocol through the Coloring Rules window, shown in Figure 3.

13. Experiment/Assignment Evaluation

SR	Parameters	Weight	Excellent	Good	Average	Poor	Not as per requirement
		Scale Factor ->	5	4	3	2	0
1	Technical Understanding	25					
2	Performance / Execution	25					
3	Question Answers	20					
4	Punctuality	20					
5	Presentation	10					
	Total out of 100 --> #(to be converted as per term-work evaluation applicable to the subject)		**∑ (Weight * Scale Factor)/5 = _____**				

References:

[1] https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html
[2] https://www.wireshark.org/download.html
[3] http://www.cs.wayne.edu/fengwei/16sp-csc5991/labs/lab1-instruction.pdf

Viva Questions

1. What are the features of Wireshark?
2. If a packet is highlighted by black, what does it mean for the packet?
3. List the different protocols that appear in the protocol column in the unfiltered packet listing window.