PROJECT-2

• This project requires you to download and install WIRESHARK , a packet-sniffing tool.

• The idea of this project is to make you aware of how packets are sent and received by your machine while using your favorite network application (web browser) and to let you know about some of the protocols that are used by your web browser application.

**Installing the Wireshark Packet Sniffer**

**$sudo apt-get install wireshark**

**To run wireshark**

**$sudo wireshark**

PROCEDURE: (All figures referenced are at the end of the description)

1) Start wireshark and you should see the homescreen as in Figure-1

2) Choose the interface that is being used for your internet connection. Refer Figure-2 & Figure-3. After choosing the interface, click ‘start’next to it.

(Note: Your interface names may be different from the ones shown in figure. You must choose the interface that is being used for your internet connection. You can know this by seeing the non-zero values under the packets field)

3) You will now see screen as in Figure-4 that shows the packets that are being captured.

4) Start running your web browser and use it normally to browse webpages.

5) After a minute or so, go to wireshark and stop capture as shown in Figure-5

6) You can filter out packets from this huge list by protocol names using the filter tool as shown in Figure-6

7) Now, analyze the packets that are listed and answer the following questions. If you select any packet in the list, the details about that particular packet will be displayed in wireshark as shown in Figure-7.

**Questions:**

1) Answer the following: (You must attach appropriate screenshots of wireshark results that helped you answer the following questions – otherwise you won’t get full credit)

i) Port number used by the application (web browser) you were using : (Answer based on

the information from wireshark)

ii) IP address that the application (web browser) used: (your computer’s address – find from the information from wireshark)

iii) IP address of the remote machine to which your application(web browser) was talking to: (Answer based on the information from wireshark)

iv) Port number (in the remote machine) of the application to which your web browser was

talking to: (Answer based on the information from wireshark)

2) Answer the following:

a) Give 3 different protocol names that you came across in the wireshark capture output.

b) Choose anyone of the 3 protocols you mentioned in (a) and give the functions of that protocol. (You can refer to information in websites like Wikipedia) – A good answer will mention the most important function of the protocol in simple terms. (A one line answer will do).

c) State how the functions of the protocol you chose in (b) were used in achieving the purpose of your application (web browser).

d) Give the header format for the protocol you chose in answer (b) (you may use internet to search for this format if you can’t find it in your books)

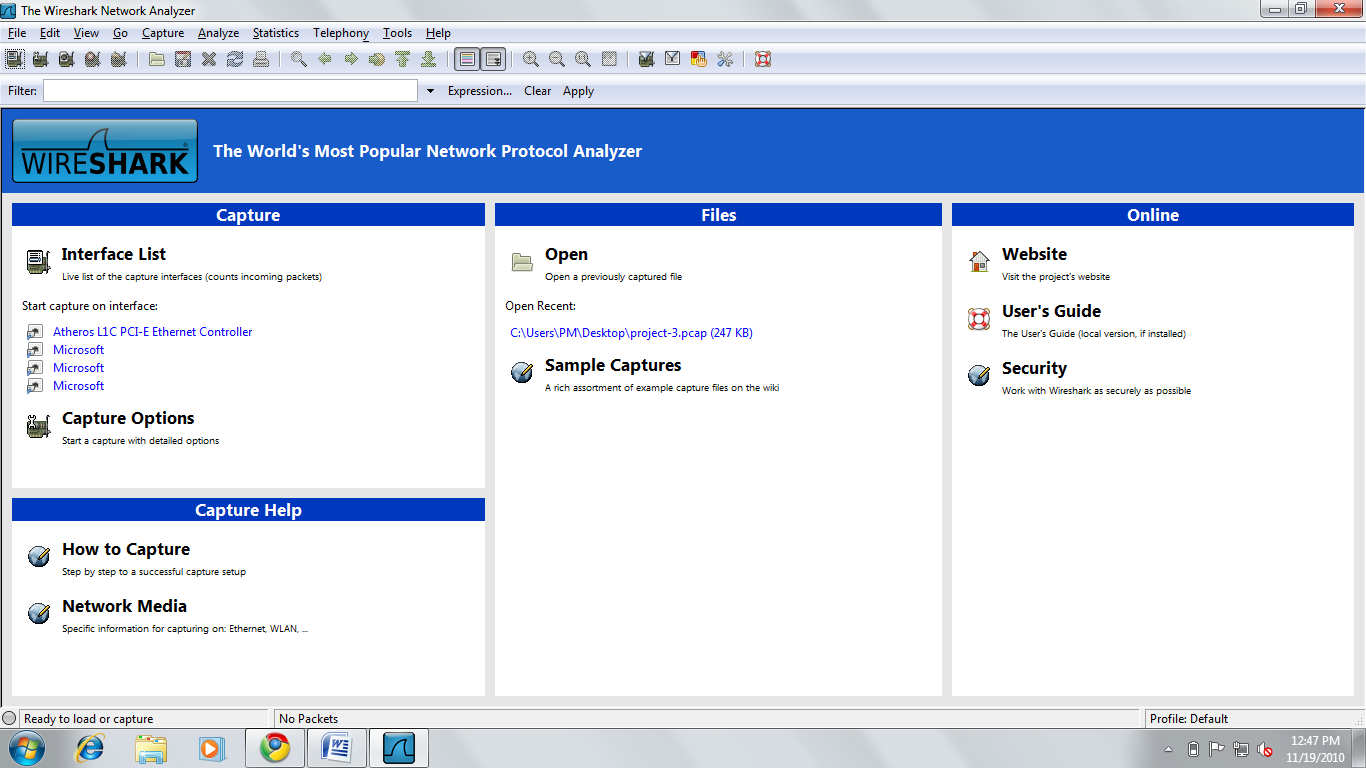
e) Try to give values for as many fields as possible in the header format in answer (d). These are not made up values but you must make use of the wireshark output. (Attach wireshark screenshot to support your answer)

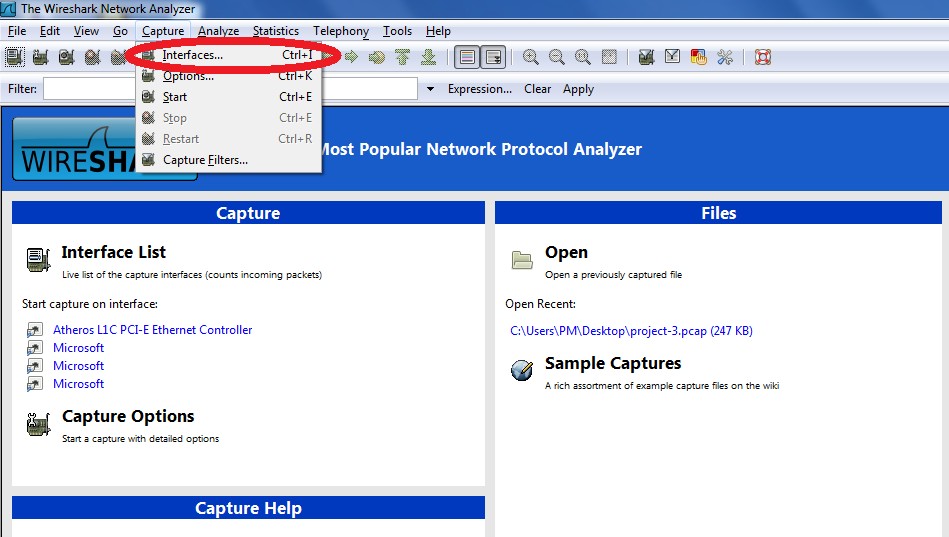
Submission Instructions:

Submit your report along with the necessary screenshots.

Figures referenced in the ‘Procedure’

Figure-1





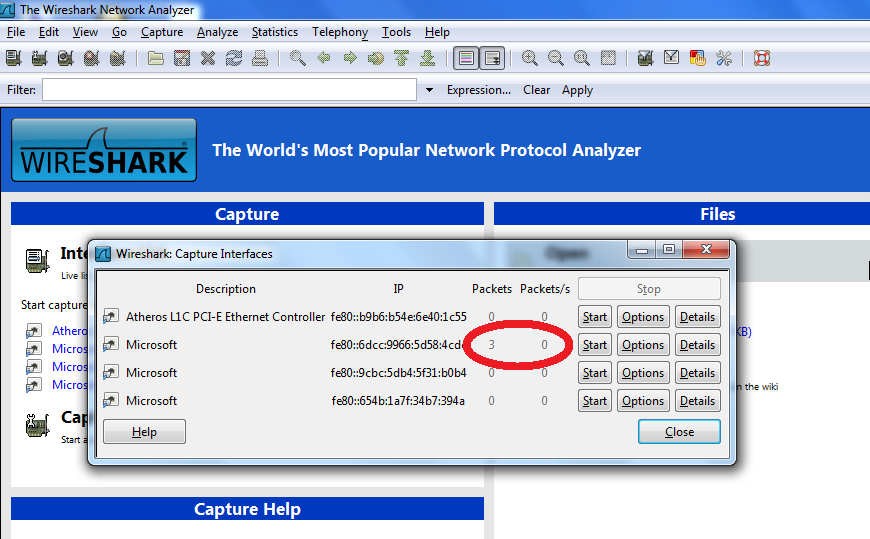
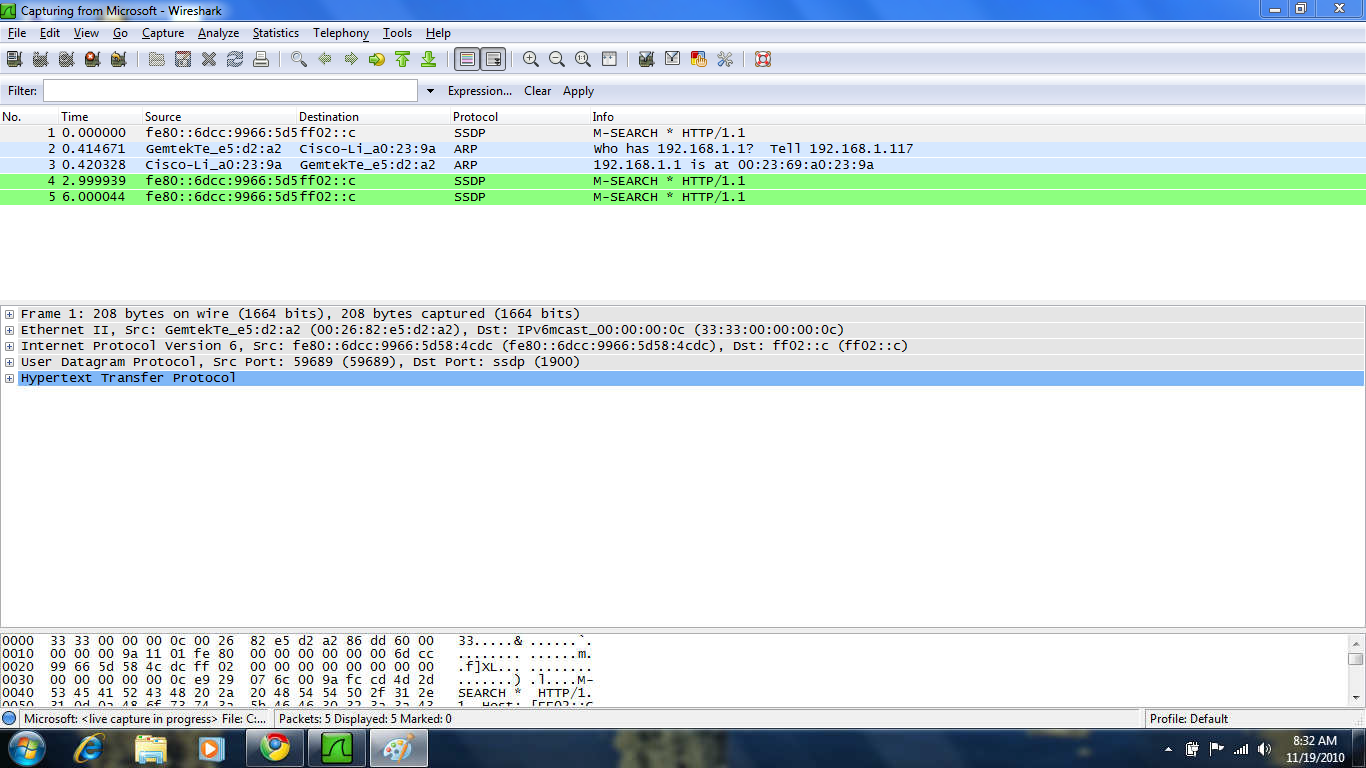


Figure-3



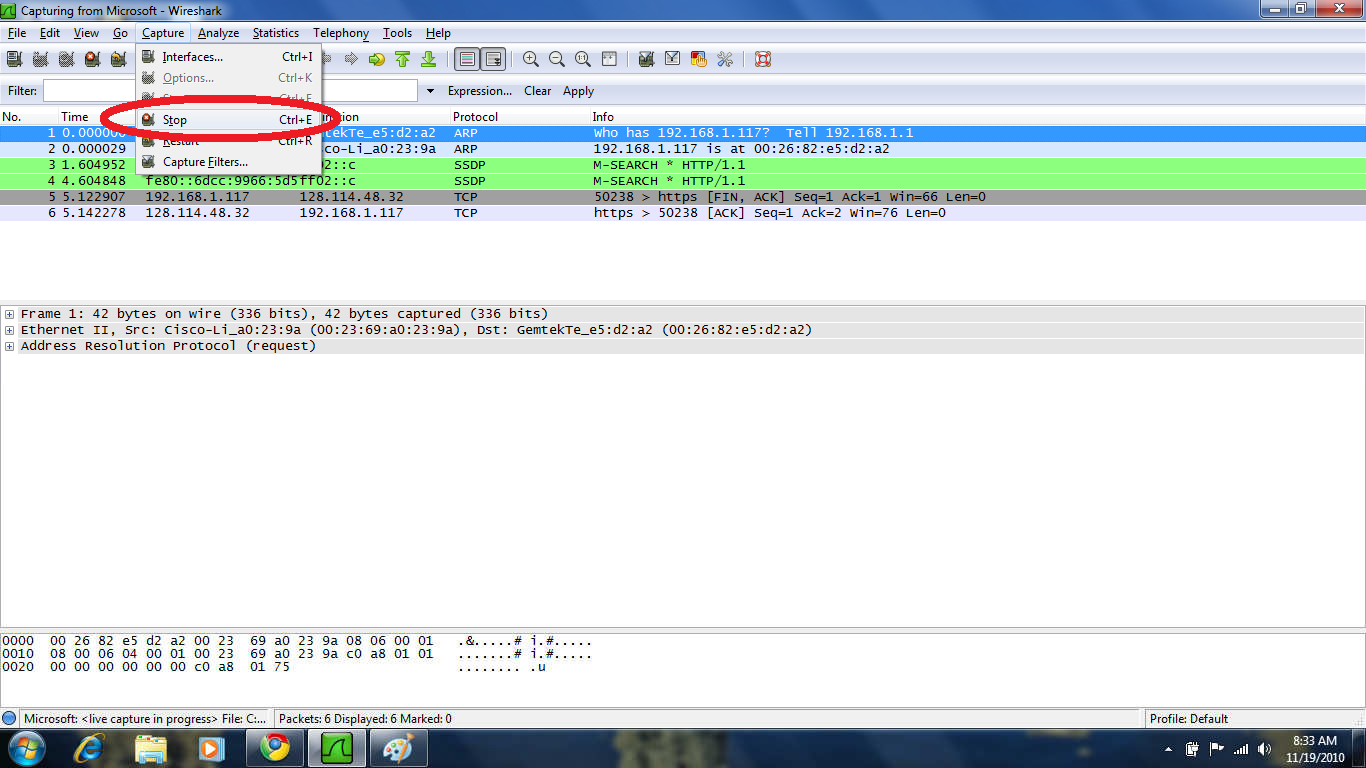
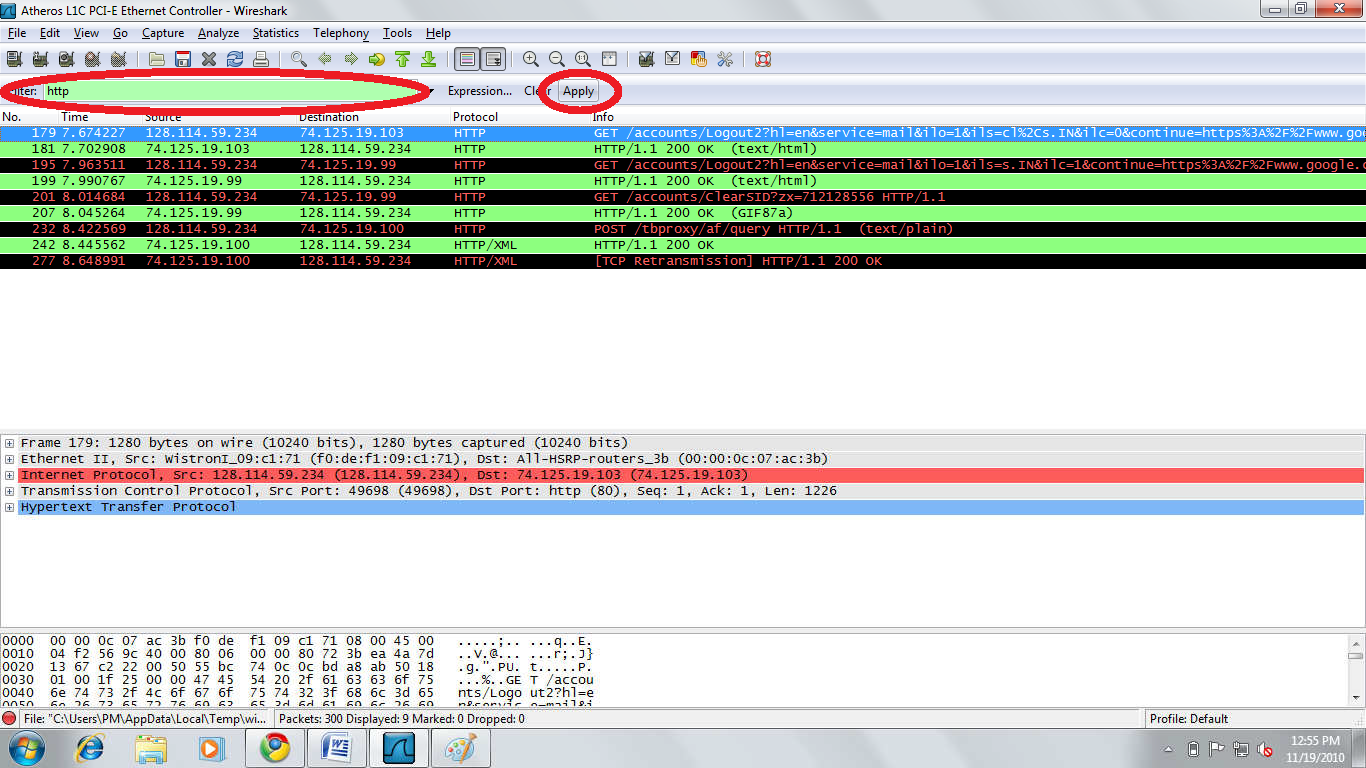


Figure-5



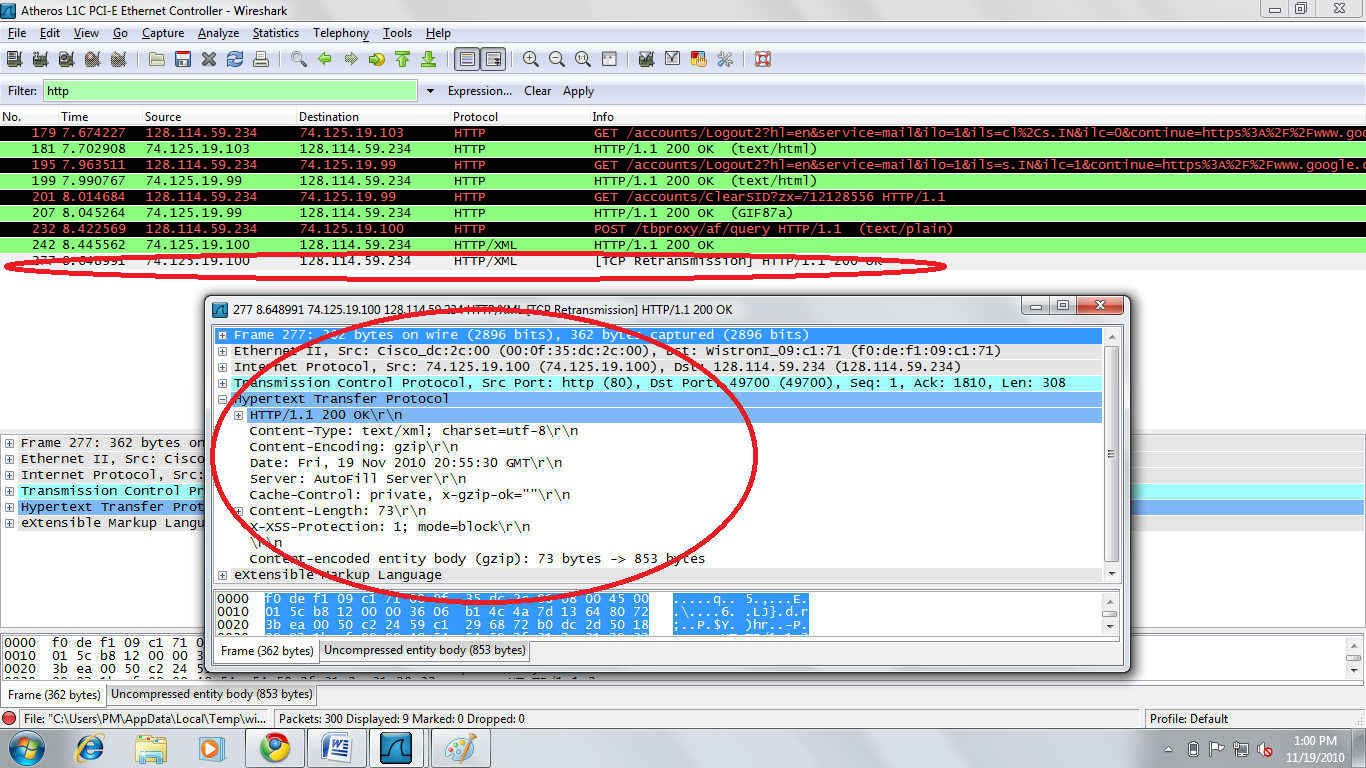


Figure-7