The Department of Electrical and Computer Engineering

The University of Alabama in Huntsville

CPE 435 Lab-10

Introduction to Wireshark and Packet Analysis

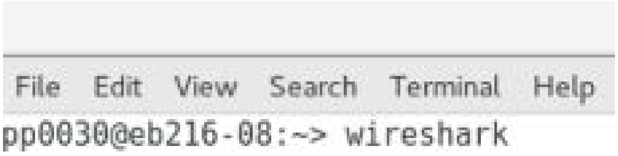
Introduction to Wireshark

Wireshark is a packet analyser tool. Apart from being a packet analyser, it is also a network sniffer tool. So it provides the option of capturing packets flowing in and out of a network as well as analyse and troubleshoot with a nice GUI. It allows live capture of packets which means you can capture and save information about the networks packets from a live network in real time.

To run live capture, a user needs sufficient privileges. However, you can analyze the packet-data based on trace files without super user privileges.

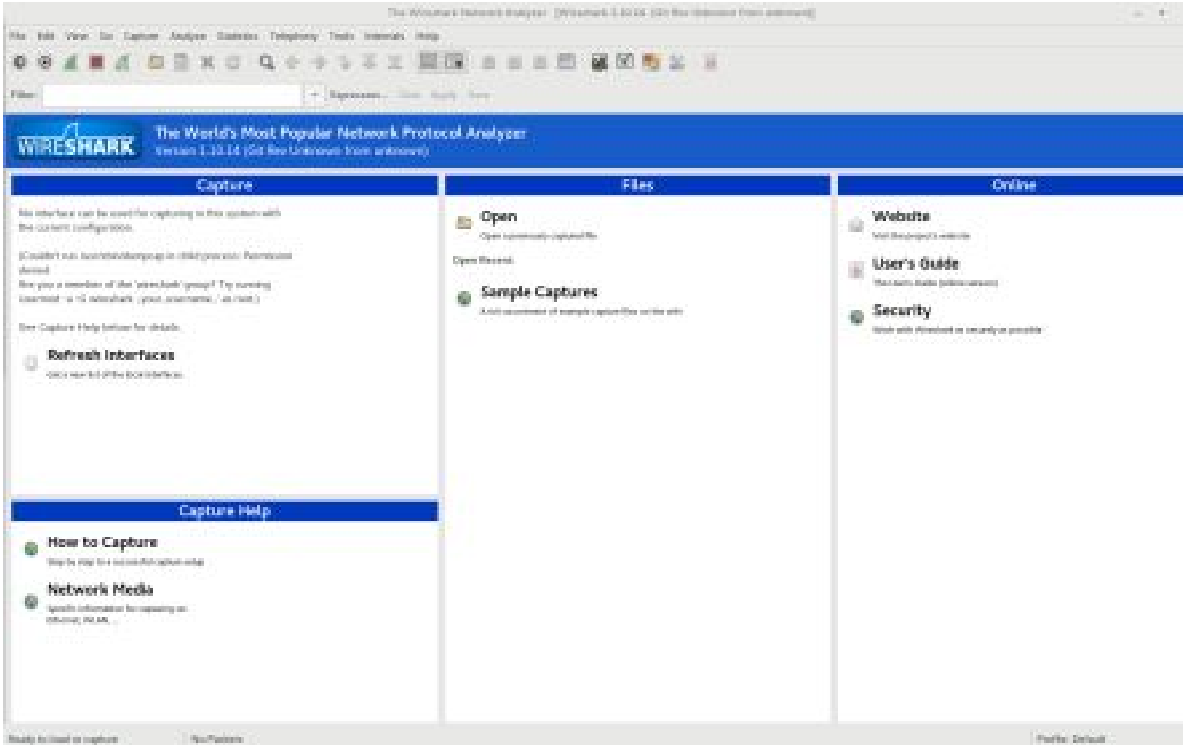
How to run Wireshark on Linux

Open a terminal (type **Ctrl+Alt+t**). Once you are inside terminal, type **wireshark** and hit enter. You should see a screen as in following figure.



```
pp0030@eb216-08:~> wireshark
```

It should open the GUI as shown in the following figure.



We will download trace files that are available online and then analyze them to extract some information.

In your report, please make sure that you include screenshots of all the steps as you perform them as a proof of your work even if the assignment does not mention explicitly.

How to run Wireshark on Windows or Mac

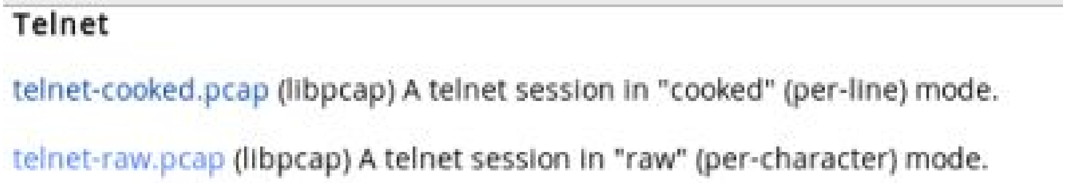
You may go to the following link to download wireshark for Windows or Mac machines.

How to run Wireshark on WSL2

Please refer to the course WSL 2 document provided along with the lab module if you wish to run wireshark from WSL2.

Subtask 1 (Introduction)

1. Go to SampleCaptures - The Wireshark Wiki. This website contains a list of sample trace files that are output of network capturing. let us find a simple unencrypted trace file, load it in wireshark and analyze it.
2. Go to number 20, which should give you telnet packets as the following figure shows.



Telnet

telnet-cooked.pcap (libpcap) A telnet session in "cooked" (per-line) mode.

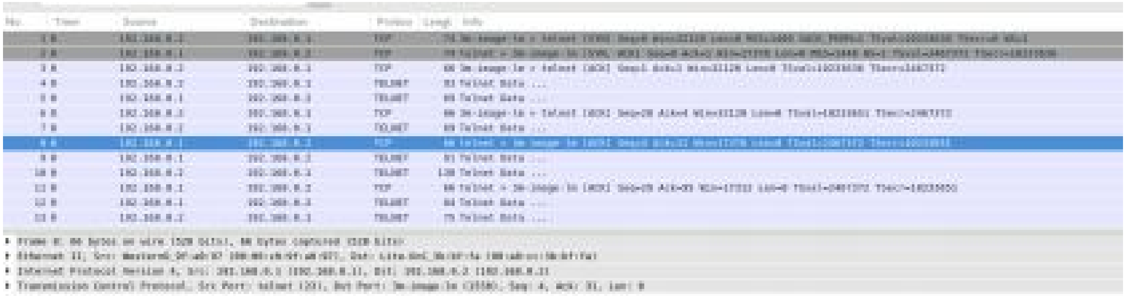
telnet-raw.pcap (libpcap) A telnet session in "raw" (per-character) mode.

3.

Download the first pcap file **telnet-cooker.pcap**

4. On the wireshark window, select **File->Open** to open a dialog box that lets you choose the pcap file. Navigate and open the pcap file that you downloaded earlier.

5. Once you select **Open**, you will see a window something like the following figure.



Assignments

1. How many packets are captured in the .pcap file that you loaded?
2. List all the communicating parties in the .pcap file? Can you also identify the ports being used by each of them?
3. What protocols are used for communication by the communicating parties ? 4. What is the total duration of the communication? (You may want to see the first and last frame)
5. What is the frame length and number of the longest frame transferred? Who is the source and destination of that packet?

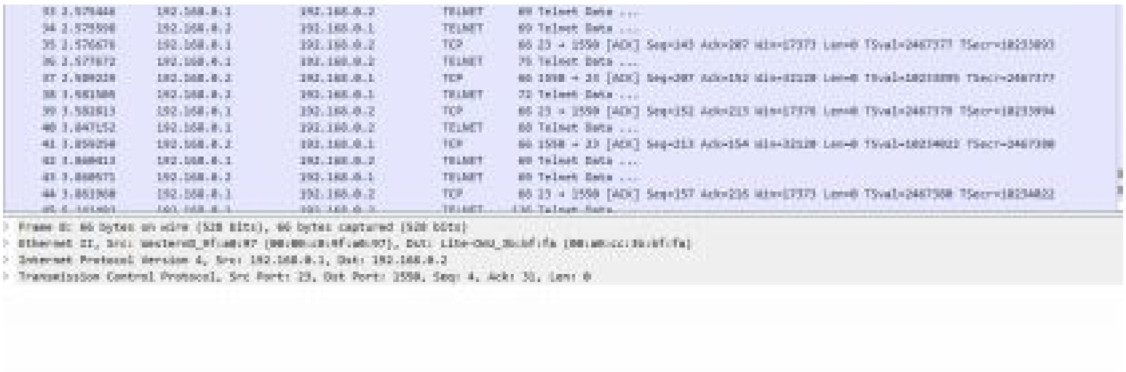
Subtask 2 (Real Hacking and Stuff)

Now that you have sniffed someone in a network and got the data that is being tranferred. You also know who is involved in communication. Now we want to see if we can get something of real value for us. May be someone has transferred his/her username and password over the network that we sniffed.

Assignments

6. Select frame number 8. Who is the sender and receiver of this frame?

7. On the window that appears below the listing of all the frames (as shown below), expand Internet Protocol Version 4. What is the Time To Live of this frame? What does this mean?



```
33 3.575448    192.168.0.1    192.168.0.2    TELNET   69 Telnet Data ...
34 3.575550    192.168.0.2    192.168.0.1    TELNET   69 Telnet Data ...
35 3.576676    192.168.0.1    192.168.0.2    TCP      66 23 → 1550 [ACK] Seq=145 Ack=207 Win=17373 Len=0 TSval=2467377 TSecr=18233093
36 3.577672    192.168.0.1    192.168.0.2    TELNET   75 Telnet Data ...
37 3.580228    192.168.0.2    192.168.0.1    TCP      66 1550 → 23 [ACK] Seq=207 Ack=152 Win=32120 Len=0 TSval=18233095 TSecr=2467377
38 3.581505    192.168.0.2    192.168.0.1    TELNET   72 Telnet Data ...
39 3.582813    192.168.0.1    192.168.0.2    TCP      66 23 → 1550 [ACK] Seq=152 Ack=213 Win=17376 Len=0 TSval=2467378 TSecr=18233094
40 3.647152    192.168.0.1    192.168.0.2    TELNET   69 Telnet Data ...
41 3.850258    192.168.0.2    192.168.0.1    TCP      66 1550 → 23 [ACK] Seq=213 Ack=154 Win=32120 Len=0 TSval=18234022 TSecr=2467398
42 3.860813    192.168.0.1    192.168.0.2    TELNET   69 Telnet Data ...
43 3.860571    192.168.0.2    192.168.0.1    TELNET   69 Telnet Data ...
44 3.851368    192.168.0.1    192.168.0.2    TCP      66 23 → 1550 [ACK] Seq=157 Ack=216 Win=17373 Len=0 TSval=2467388 TSecr=18234022

> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: WesternD_9f:a0:97 (00:00:c0:9f:a0:97), Dst: Lite-OnU_3b:bf:fa (00:a0:cc:3b:bf:fa)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.2
> Transmission Control Protocol, Src Port: 23, Dst Port: 1550, Seq: 4, Ack: 31, Len: 0
```

8. Select frame 8 again. Right click on it, and select **Follow TCP Stream**. What information can you see? What is the username and password that is transferred?
9. Repeat the same procedure in **telnet-raw.pcap**. Find the login information used to verify credentials. (Select frame 8 again)
10. What do you think is wrong with these two files that you analyzed? How can you not allow anyone to know your password that you send for authentication?
11. Load the file **uftp_v3_transfer.pcapng**. The protocol used is UFTP. What is UFTP? Can you identify two parties that are involved in file transfer. (Use your intelligent guessing) 12. Write differences between TCP and UDP.

Subtask 3 (Decrypting The Encrypted)

Let us now work on encrypted protocol.

12. What is the difference between **https://** and **http://**? What is the encryption standard used by them, if any?
13. Download the file **mysql_complete_pcap**. Is it encrypted? Please justify.
14. Download the file **mysql-ssl-larger.pcapng**. Is it encrypted? Please justify.
15. Download the zipped file **snakeoil2_070531.tgz**. Extract the content in your local folder. Load the .pcap file in wireshark. Is it encrypted?
16. Perform the decryption of the .pcap file as demonstrated in class by the instructor.
    1. What frame number requests the image apache_pb.png?
    2. Does the server provide the image? What is the status code that implies the response has payload?
    3. Attach the image apache_pb.png to your report.
17. What is the response that the server provided when requested for openlogo-25.jpg? Can you see the html code sent as a response? If yes, copy and paste it in a .html file and load it in your favourite browser. Attach the screenshot of how the response looks like in the web browser.

Subtask 4 (Vulnerability Analysis)

The following assignment is to be done at the **students own machine**. You do not have permission and user rights to do this on campus machines. Please make sure that you do not reveal any important information to your reports when you attach screenshots. (Please blur out any sensitive information)

18. The first thing that you will do is capture packets. You can use wireshark or tcpdump to capture packets. While you can capture packets from wireshark, I suggest you to use

tcpdump so that you can be familiar with a new tool. Following are the procedures that you will follow:

1. Find the interface that is connected to the internet. Do **ifconfig** in the terminal and select the one which is connected to the internet. Wireshark should show you the interface in its GUI.
2. Start packet capture in tcpdump using **tcpdump -i <interface> -s 65535 -w <filename>**. Or select the bluefin below File menu in wireshark after you select the interface if you wish to use wireshark.

3. Please visit the website http://weevil.info/ What is wrong with this website? 4. After it is completely loaded, stop the capture. You can select the button in Wireshark GUI or kill the tcpdump process if you are using tcpdump.

5. Load the file in wireshark. If you are using wireshark, it is already loaded. 6. Try to find at least two images that are sent by the server to your machine and attach them to your report.

7. What are the vulnerabilities of the website that you can see right away? 8. Repeat similar operation for https://www.foxnews.com/. Attach two images sent from the server to your machine if you can.

Deliverables

Lab Report

The following material in each section is expected:

1. Cover page with your name, lab number, course name, and dates
2. Observations and Answers
   a. Please include answers to any questions from the lab document, as well as any necessary supporting documentation in the order they appear. This includes screenshots from wireshark to support your answers.

The report should be submitted as a single pdf document with the source code for your program within it.

Recorded Demonstration

The following material in each section is expected:

1. Introduce yourself and give the name of the lab
2. Walk through sub task 3 and 4 in their entirety
3. Recordings should be around 5 to 7 minutes on average

The recorded demonstration should be submitted as an mp4 file.