CS 4404 – Written Assignment 2 Instructions

Follow the instructions below to help you carry out the assignment:

I. Close all open web browsers

II. Launch Wireshark.

III. Once the Wireshark is open and running, it will display all network interfaces on your computer. Please choose the appropriate interface (WiFi for the wireless interface or Local LAN for the wired interface). Please pay close attention to the interface and choose only the interface with network activity (indicated by the graph lines in front of the interface).

IV. Double click on the chosen network interface (card). Network capture begins automatically. Notice that there may be little or no activity recorded/displayed by Wireshark.

V. Open a new web browser and visit the Uopeople student portal (https://your.uopeople.edu/login?ReturnUrl=/).

VI. Login with your username and password.

VII. In the UoPeople student portal, open up the Course and Announcement forums.

VIII. Now open a command prompt window on your PC;

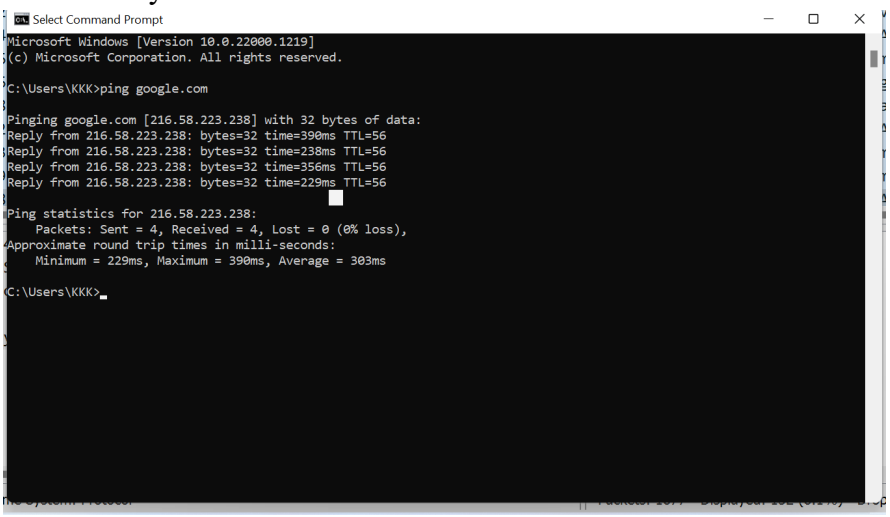
a. For Windows OS: https://www.wikihow.com/Open-the-Command-Prompt-in-Windows

b. For Mac OS: https://www.wikihow.com/Get-to-the-Command-Line-on-a-Mac

c. For Linux OS: https://www.geeksforgeeks.org/how-to-open-terminal-in-linux/

IX. We shall now ping a public DNS IP address as follows:

a. In the command prompt, type the following command (in lower case): ping google.com The following (or similar) result should be displayed if done correctly:

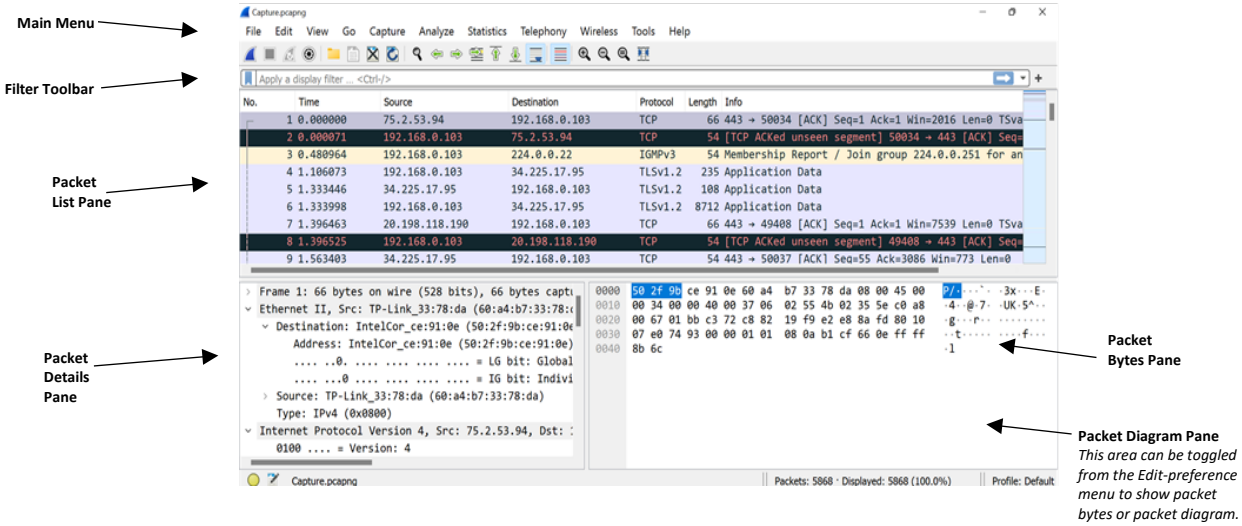


- Refer to this link to see how to ping in different OS: https://chemicloud.com/kb/article/how-to-perform-a-ping-test-in-windows-mac-os-and-linux/

b. Once you obtain the above results, close and exit command prompt.

X. Once (IX) has been accomplished, go back to the menu bar of Wireshark and click on capture, then navigate to the stop option and click on it. This ends the capture process.

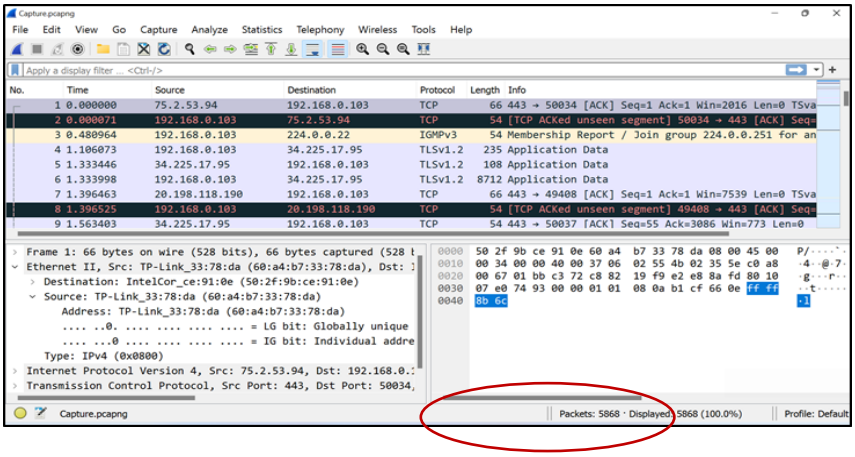
Most people avoid analyzing network traffic because the hundreds (maybe thousands) of result lines could seem utterly confusing. One has to learn how to manage and interpret these results, to know its importance. Let's begin with understanding the Wireshark's advanced user interface. The Wireshark's advanced user interface consists of five major parts (as shown in the figure below):



For more details, please refer to the textbook reading: https://www.wireshark.org/docs/wsug_html_chunked/ChapterUsing.html.

XI. The packet list pane as earlier explained contains the results of all captured packets. Scroll up and down this result window and observe the captured packets listed. Pay attention to the PROTOCOL column. This tells you what kind of protocol has been captured, such as HTTP, UDP, and so on. How many distinct protocols can you see? Name as many of these as you can identify.

XII. To filter for packets, simply type the name of the protocol (in lower case) in the filter toolbar field and hit the enter key (make sure that the protocol is spelled correctly). For instance, type dns and hit enter, this displays all the results with the DNS protocol. To see the total number of packets captured or total number of displayed packets, look to the bottom right-hand corner (as shown in the figure below), you will see several statistics including PACKETS (represents the total number of packets captured), DISPLAYED (total number of packets displayed) and DROPPED (percentage of dropped packets).



XIII. Filter for all required protocols and take a screenshot of your results. You are to submit all screenshots for questions 3(b) to 3(e) with your answers.

Congratulations! You just successfully carried out your first network packet analysis operation.

References:

- akashmomale. (2022, July 27). *How to open terminal in linux?* GeeksforGeeks. Retrieved January 6, 2023, from https://www.geeksforgeeks.org/how-to-open-terminal-in-linux/
- *How to perform a ping test in windows, mac OS, and linux*. (2020, August 9). ChemiCloud. https://chemicloud.com/kb/article/how-to-perform-a-ping-test-in-windows-mac-os-and-linux/
- Levine, N. (2022, December 26). *How to get to the command line on a mac*. wikiHow. https://www.wikihow.com/Get-to-the-Command-Line-on-a-Mac
- Oppido, L., & Lloyd, J. (2022, April 20). *How to open the command prompt in windows*. wikiHow. https://www.wikihow.com/Open-the-Command-Prompt-in-Windows