CpE/NIS 654
Exercise on Wireshark

As a part of the course on Design and Analysis of Network Systems, we want to expose you to some of the analysis and simulation tools which have been found to be very useful by practicing engineers. As we described in the lecture part of this course, one of the tools that is often used to study, analyze, and evaluate the performance of a network is Wireshark. We have, therefore created this exercise for you get familiarized with this tool. There is no due date for this exercise and you do not have anything to submit, and there is no grade associated with this exercise. It is strictly for your benefit, should you have interest learning more about such tools. Here is the exercise, enjoy.

- First get introduced to Wireshark. It is easy to find tutorials, lectures, and user guides on the web on Wireshark. Here are two sources to help you out.

  - Go to www.youtube.com and type in “tutorial wireshrk” or some phrase with wireshark name and find and watch a video or a turorial on wireshark.

  - Go to: https://www.wireshark.org/docs/wsug_html_chunked and read through a few pages as you feel or need, or print some out for reference.

- Now having familiarized yourself about the tool. set up your Wireshark on your computer to capture from your local Access Point. Now you are ready to learn about it and play with it.

- Open a web browser, and go to Google, Youtube or a site of your choice that can provide rich http content.

- Start capturing the traffic from your pc, by clicking on “Capture” tab then choose the “Interfaces …” option. A window opens with the interfaces available and the ones with traffic on them. Click “Start” on one of the interfaces (maybe the only one) with traffic on it.

- Do a search on your site and wait for results to download.

- Stop the capture, either by going to the “Capture” tab and choosing the “Stop” or by pushing the stop button on the bar below the tabs with the standard buttons.

- Go to the “Statistics” tab and choose the “Summary” option.

- Carefully study the report on the traffic captured, especially on the bottom of the window.

- Find the IO graph of the traffic by clicking the “Statistics” tab and choosing the “IO Graphs” option.

- Choose the filters in IO Graph to show different traffic types in different colors. Learn how to zoom by playing with X-axis and Y-axis parameter settings.

- Go to “Statistics” tab and choose the “Flow Graph…” option. Play with different parameters to get the idea of how the flow graphs will show up.

- Go to the “Statistics” tab and choose the “Conversation List” option. Choose the “Ethernet” option play with and study the window that opens up.

- Go to the “Statistics” tab and choose the “Endpoint Lists” option. Choose the “Ethernet” option play with and study the window that opens up.

- Go to the “Statistics” tab and choose the “Endpoint Lists” option. Choose the “TCP” option play with and study the window that opens up.

- Go to the “Statistics” tab and choose the “Endpoint Lists” option. Choose the “UDP” option play with and study the window that opens up.

- Type in “http” in the “Filter:” bar on top of the Wireshark window (third row from top), press Apply and watch the new captured data shown.

- Type in “udp” in the “Filter:” bar on top of the Wireshark window (third row from top), press Apply and watch the new captured data shown.

Now it is matter of playing with its features and capabilities, using the tutorial referenced above and reviewing the lecture slides posted for you to becoming a guru on Wireshark with practice – Happy Wiresharking