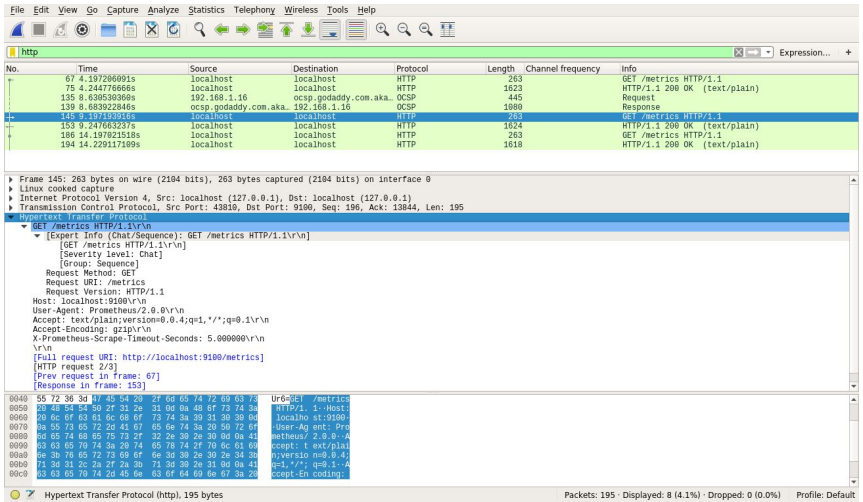
ACN - CS5060
Tutorial

What is it

- An Open Source Software tool
- A network packet analyzer.
- GUI as well TShark utility from command line
- Mainly used to troubleshoot or debug network problems.



Purpose

- Troubleshoot Network problems
- Examine security problems
- Verify network applications
- Debugging protocol implementations
- Learning network protocol internals

Features

- Available for Unix (flavors) and Windows.
- Capture live packet data from a network interface.
- Save captured packet data.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Create various statistics.
- Open files containing packet data captured with tcpdump/WinDump
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Colorize packet display based on filters.

Wireshark from Command line

To start capture

- $ sudo wireshark -i <interface_name>
- For eg:
  - $ sudo wireshark -i wlan0 => wireless interface
  - $ sudo wireshark -i eth0 => wired interface

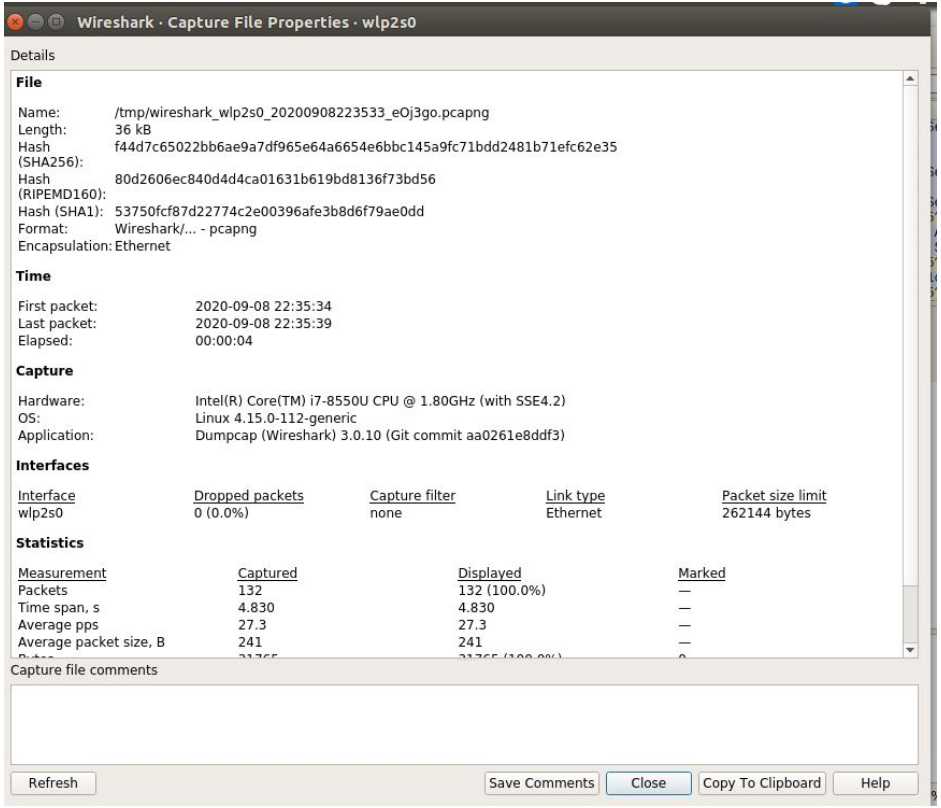
To save file

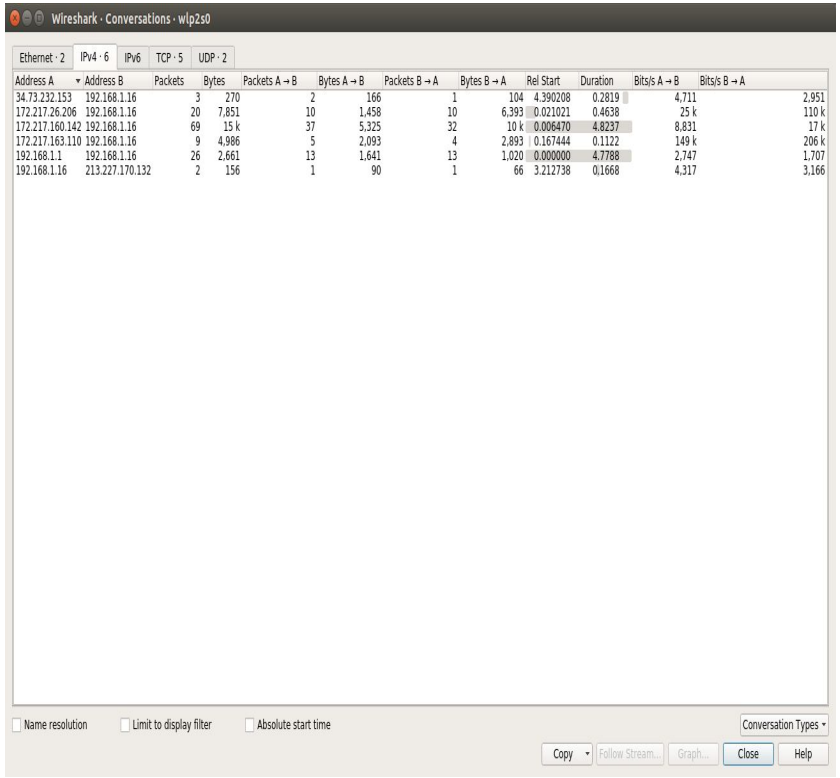
- $ sudo wireshark -i <interface_name> -w <file_name>
- For eg:
  - $ sudo mkdir wireshark
  - $ cd wireshark
  - $ sudo wireshark -i wlan0 -w test

Statistics Analysis

- Capture File Properties
- Conversations:
  - A network conversation is the traffic between two specific endpoints.
- Packet Lengths:
  - Shows the distribution of packet lengths and related information.
- Endpoints
  - Details on specific endpoints
- HTTP Statistics
  - Requests, Responses
- I/O Graphs
- Flow Graphs

Statistics Analysis





What is it not

- An intrusion detection system.
- Manipulate things on the network, it will only “measure” things from it.
- Send packets on the network or do other active things

Start using

Installation and usage guide:
https://docs.google.com/document/d/1HGi6MOTzQkggLSBHnVmYBxo1wxCyWtrQgkqVf1i0xWk/edit?usp=sharing

Start Capture, Duration, Stop Capture, Analyze

Task 1

Capture Internet traffic using Wireshark for 5 minutes, check how many TCP, UDP, ICMP packets in the trace by using appropriate filters. Submit a detailed observation and analysis report with specific details on

- UDP : Take DNS Packets (Run nslookup iith.ac.in during the capture from terminal)
- TCP: Take HTTP/SSL Packets from your most favourite university website in India
- ICMP: Ping iith.ac.in from terminal
- Endpoints, conversations, flow graphs, I/O graphs

Task 2

Run iperf3 communication program locally using server-client modes. Capture its Wireshark trace and prepare an analysis report on the overall conversation with specific details on IP Addresses, TCP/UDP conversation being used in the communication, Ports, Ethernet interface.

Report Submission

Prepare a detailed observation and analysis report including Task1 and Task2 with specific details asked in individual tasks' slides. Submit it to google classroom in the assignment link https://classroom.google.com/u/0/w/MTUzNjcxOTYyNTA3/t/all

References

- https://www.wireshark.org/
- https://www.wireshark.org/docs/wsug_html_chunked/AppProtocols.html
- https://www.wireshark.org/docs/wsug_html_chunked/
- https://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- https://jvns.ca/blog/2018/06/19/what-i-use-wireshark-for/
- https://iperf.fr/