

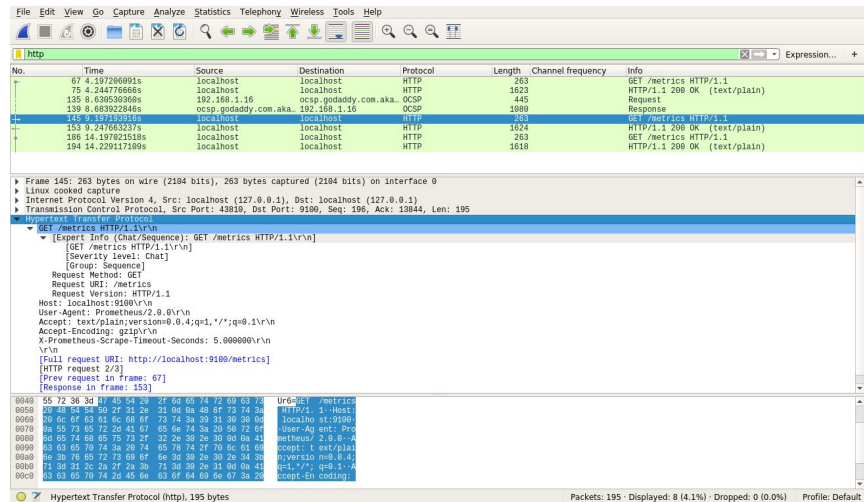
ACN - CS5060

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

Wireshark · Capture File Properties · wlp2s0

Details

File

Name: /tmp/wireshark_wlp2s0_20200908223533_eOj3go.pcapng
Length: 36 kB
Hash (SHA256): f44d7c65022bb6ae9a7df965e64a6654e6bbc145a9fc71bdd2481b71efc62e35
Hash (RIPEMD160): 80d2606ec840d4d4ca01631b619bd8136f73bd56
Hash (SHA1): 53750fcf87d22774c2e00396afe3bd6f79ae0dd
Format: Wireshark/... - pcapng
Encapsulation: Ethernet

Time

First packet: 2020-09-08 22:35:34
Last packet: 2020-09-08 22:35:39
Elapsed: 00:00:04

Capture

Hardware: Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz (with SSE4.2)
OS: Linux 4.15.0-112-generic
Application: Dumpcap (Wireshark) 3.0.10 (Git commit aa0261e8ddf3)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
wlp2s0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	132	132 (100.0%)	—
Time span, s	4.830	4.830	—
Average pps	27.3	27.3	—
Average packet size, B	241	241	—

Capture file comments

Refresh Save Comments Close Copy To Clipboard Help

Wireshark · Conversations · wlp2s0

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
34.73.232.153	192.168.1.16	3	270	2	166	1	104	4.390208	0.2819	4.711	2.951
172.217.26.206	192.168.1.16	20	7.851	10	1,458	10	6.393	0.021021	0.4638	25 k	110 k
172.217.160.142	192.168.1.16	69	15 k	37	5,325	32	10 k	0.006470	4.8237	8.831	17 k
172.217.163.110	192.168.1.16	9	4,986	5	2,093	4	2.893	0.167444	0.1122	149 k	206 k
192.168.1.1	192.168.1.16	26	2,661	13	1,641	13	1,020	0.000000	4.7788	2,747	1,707
192.168.1.16	213.227.170.132	2	156	1	90	1	66	3.212738	0.1668	4.317	3.166

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Conversation Types

Copy Follow Stream... Graph... Close Help

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/>