Mawlana Bhashani Science And Technology University

Lab Report

Lab Report No: 08

Lab Report Name: Lab-wireshark-display lecture

Group member ID: IT-18019 and IT-18037

Date of Performance:

Date of Submission:

Submitted by

Name: Anamul Haque
ID: IT-18037.
3rd Year 2nd Semester
Session: 2017-2018
Dept. of ICT,MBSTU

}

Submitted To

Nazrul Islam
Assistant Professor
Dept. of ICT
MBSTU.

1. Objectives :

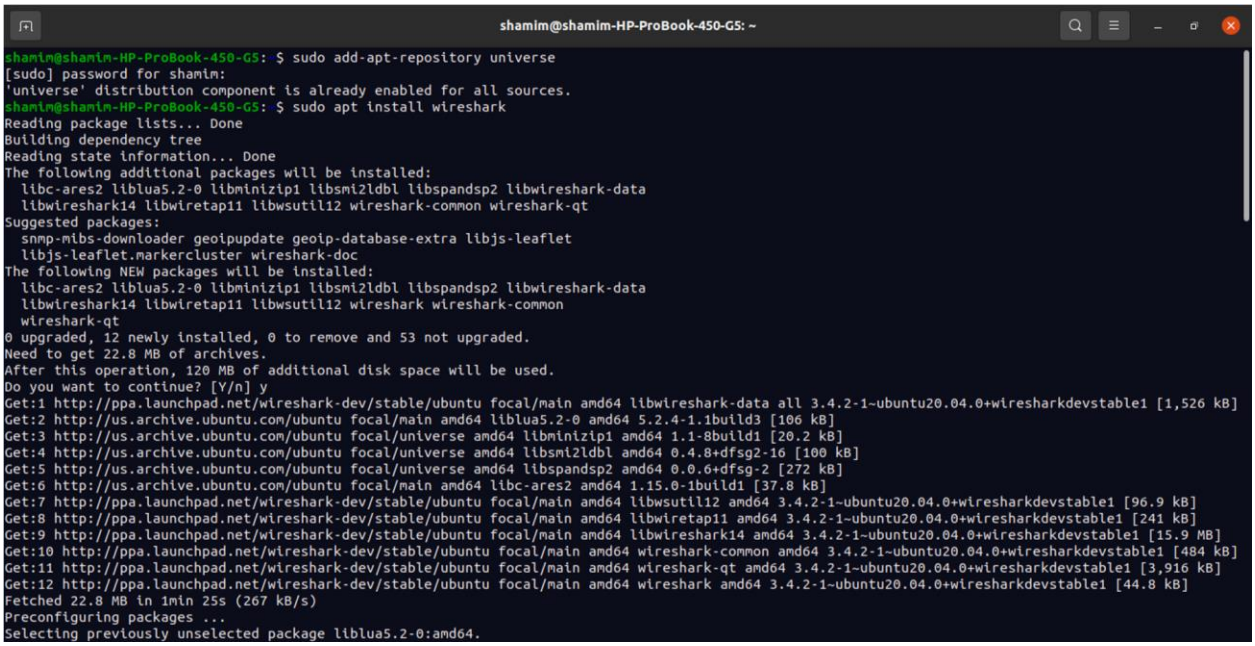
Wireshark is a network protocol analyzer captures network packets displays packet data in details
www.wireshark.org
First released in 1998 by Gerald Combs as Ethereal many contributors around the world Open source and free software
Graphical alternative to tcpdump

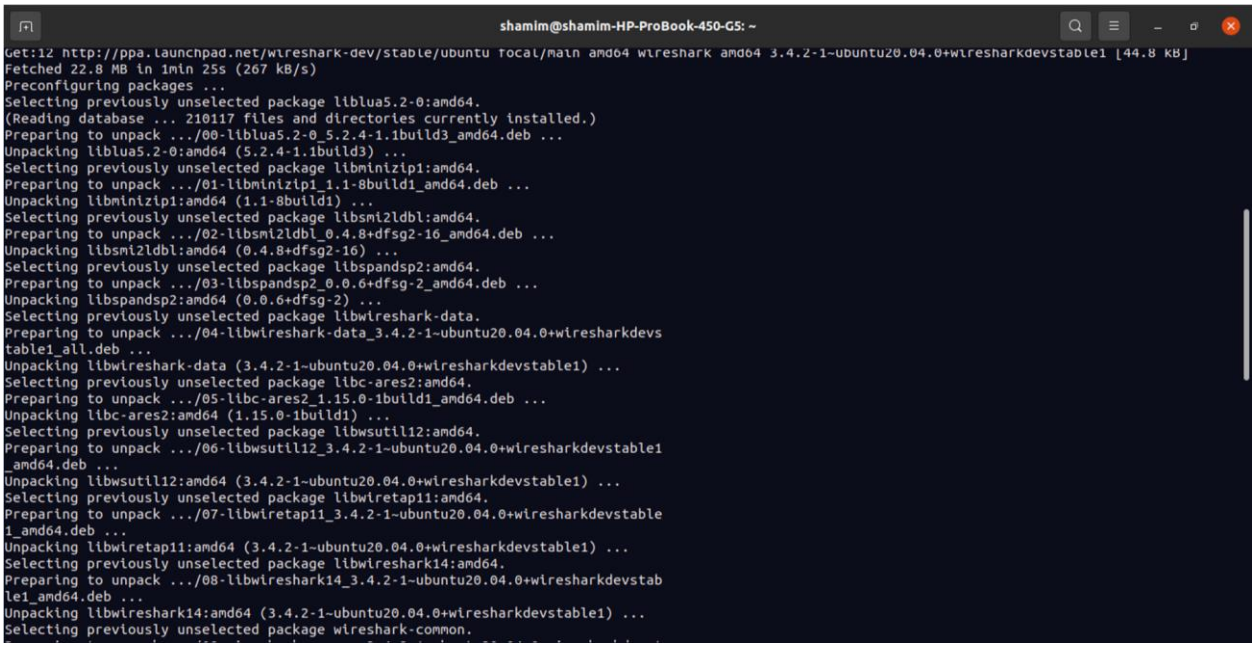
2. Theory :

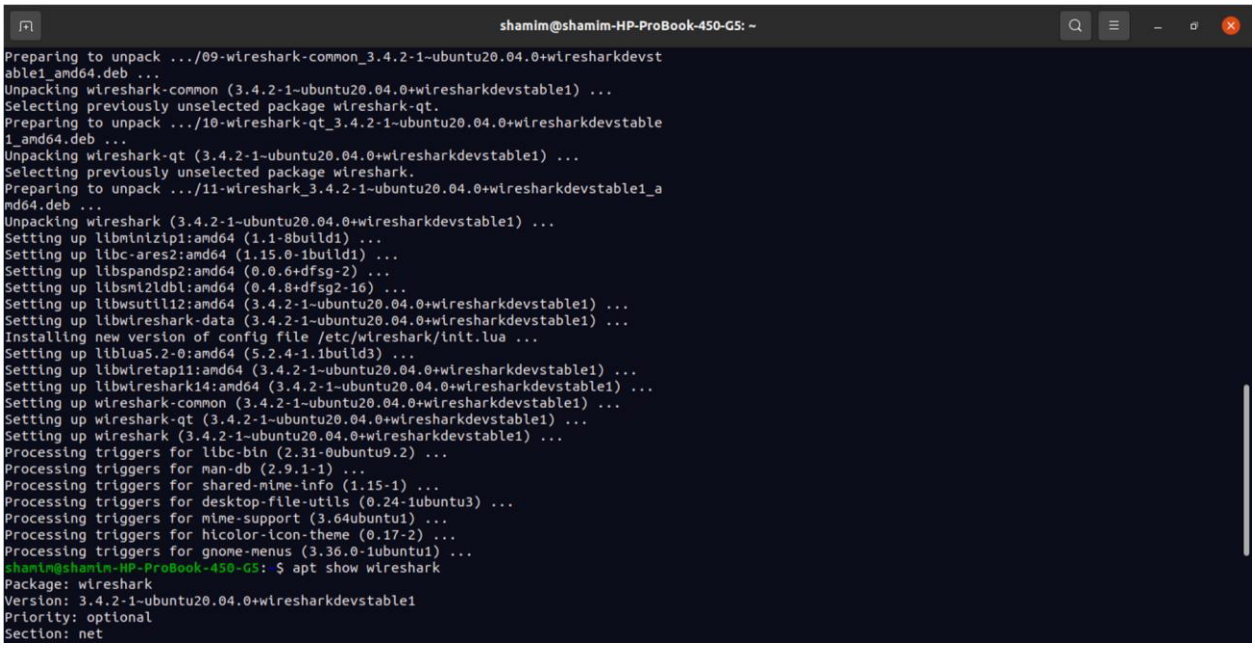
Powerful tool for troubleshooting network problems examining security problems debugging protocol implementations learning network protocol internals Used in industry and academia

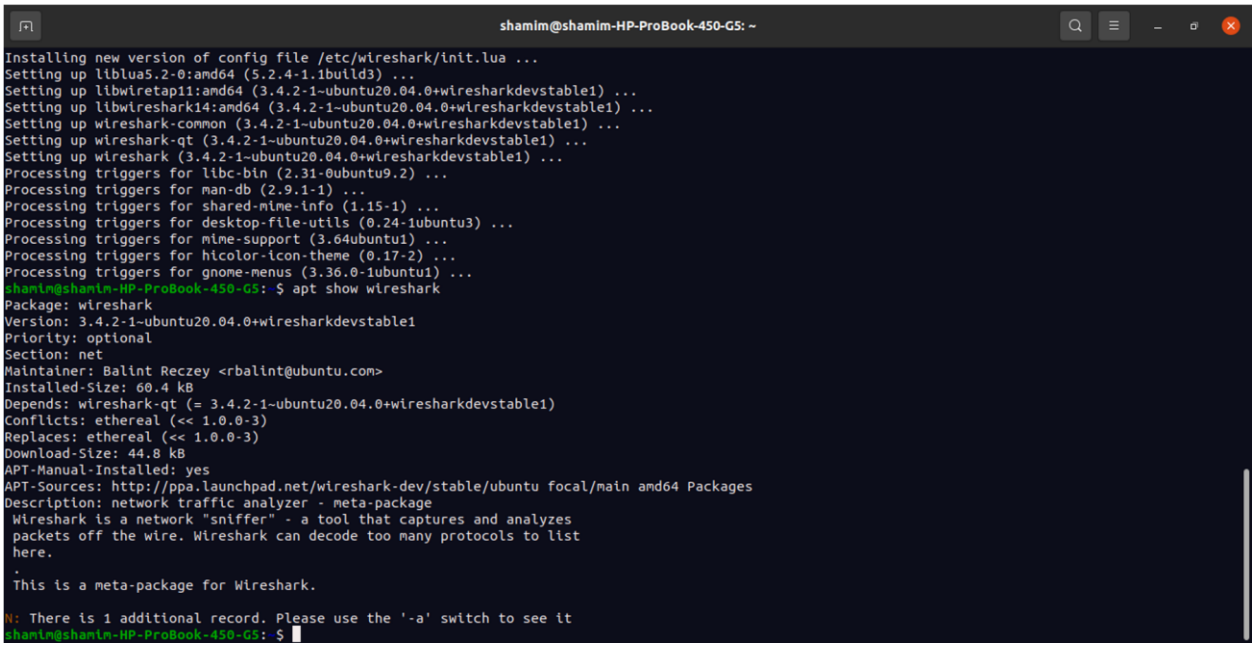
3. Methodology

Wireshark Installation

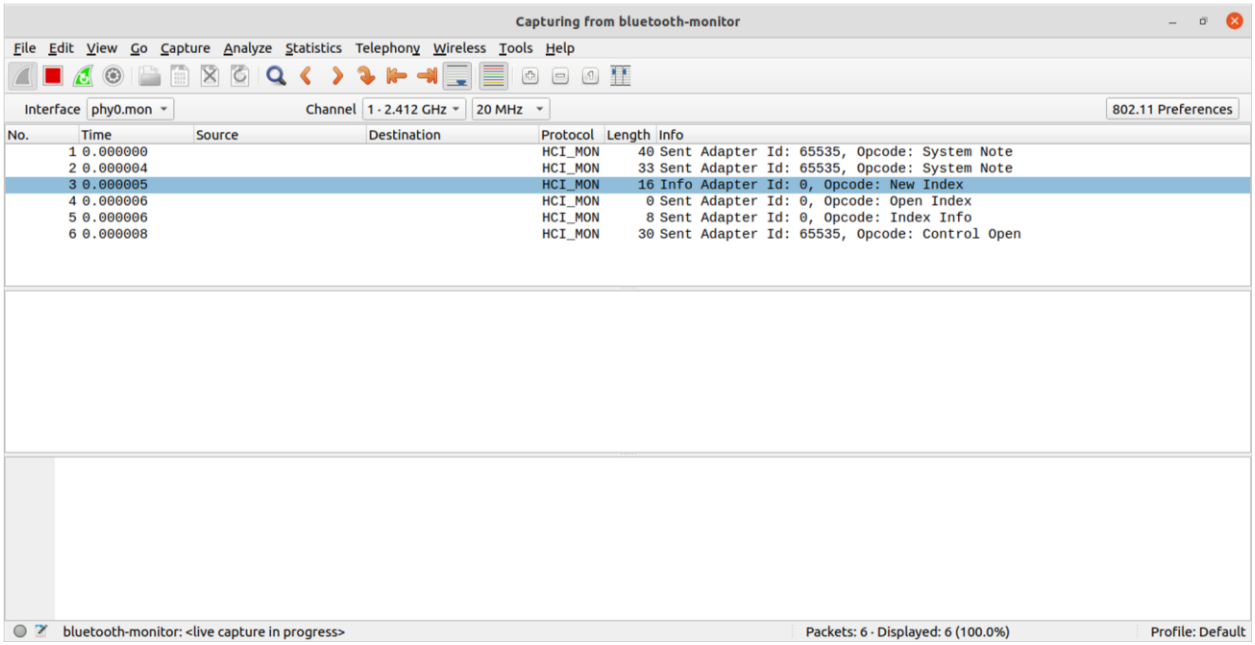


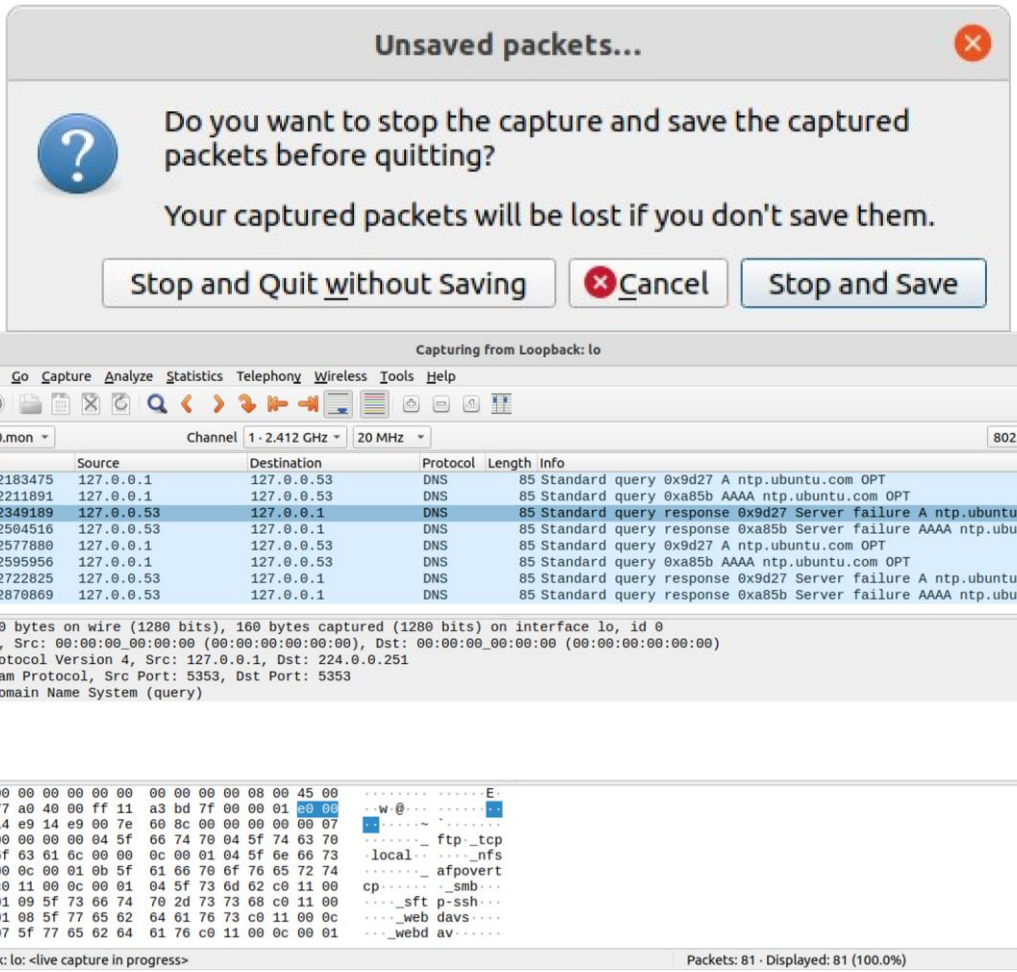

shamim@shamim-HP-ProBook-450-G5: ~
Get:12 http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main amd64 wireshark amd64 3.4.2-1~ubuntu20.04.0+wiresharkdevstable1 [44.8 kB]
Fetched 22.8 MB in 1min 25s (267 kB/s)
Preconfiguring packages ...
Selecting previously unselected package liblua5.2-0:amd64.
(Reading database ... 210117 files and directories currently installed.)
Preparing to unpack .../00-liblua5.2-0_5.2.4-1.1build3_amd64.deb ...
Unpacking liblua5.2-0:amd64 (5.2.4-1.1build3) ...
Selecting previously unselected package libminizip1:amd64.
Preparing to unpack .../01-libminizip1_1.1-8build1_amd64.deb ...
Unpacking libminizip1:amd64 (1.1-8build1) ...
Selecting previously unselected package libsmi2ldbl:amd64.
Preparing to unpack .../02-libsmi2ldbl_0.4.8+dfsg2-16_amd64.deb ...
Unpacking libsmi2ldbl:amd64 (0.4.8+dfsg2-16) ...
Selecting previously unselected package libspandsp2:amd64.
Preparing to unpack .../03-libspandsp2_0.0.6+dfsg-2_amd64.deb ...
Unpacking libspandsp2:amd64 (0.0.6+dfsg-2) ...
Selecting previously unselected package libwireshark-data.
Preparing to unpack .../04-libwireshark-data_3.4.2-1~ubuntu20.04.0+wiresharkdevs
table1_all.deb ...
Unpacking libwireshark-data (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Selecting previously unselected package libc-ares2:amd64.
Preparing to unpack .../05-libc-ares2_1.15.0-1build1_amd64.deb ...
Unpacking libc-ares2:amd64 (1.15.0-1build1) ...
Selecting previously unselected package libwsutil12:amd64.
Preparing to unpack .../06-libwsutil12_3.4.2-1~ubuntu20.04.0+wiresharkdevstable1
_amd64.deb ...
Unpacking libwsutil12:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Selecting previously unselected package libwiretap11:amd64.
Preparing to unpack .../07-libwiretap11_3.4.2-1~ubuntu20.04.0+wiresharkdevstable
1_amd64.deb ...
Unpacking libwiretap11:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Selecting previously unselected package libwireshark14:amd64.
Preparing to unpack .../08-libwireshark14_3.4.2-1~ubuntu20.04.0+wiresharkdevstab
le1_amd64.deb ...
Unpacking libwireshark14:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Selecting previously unselected package wireshark-common.

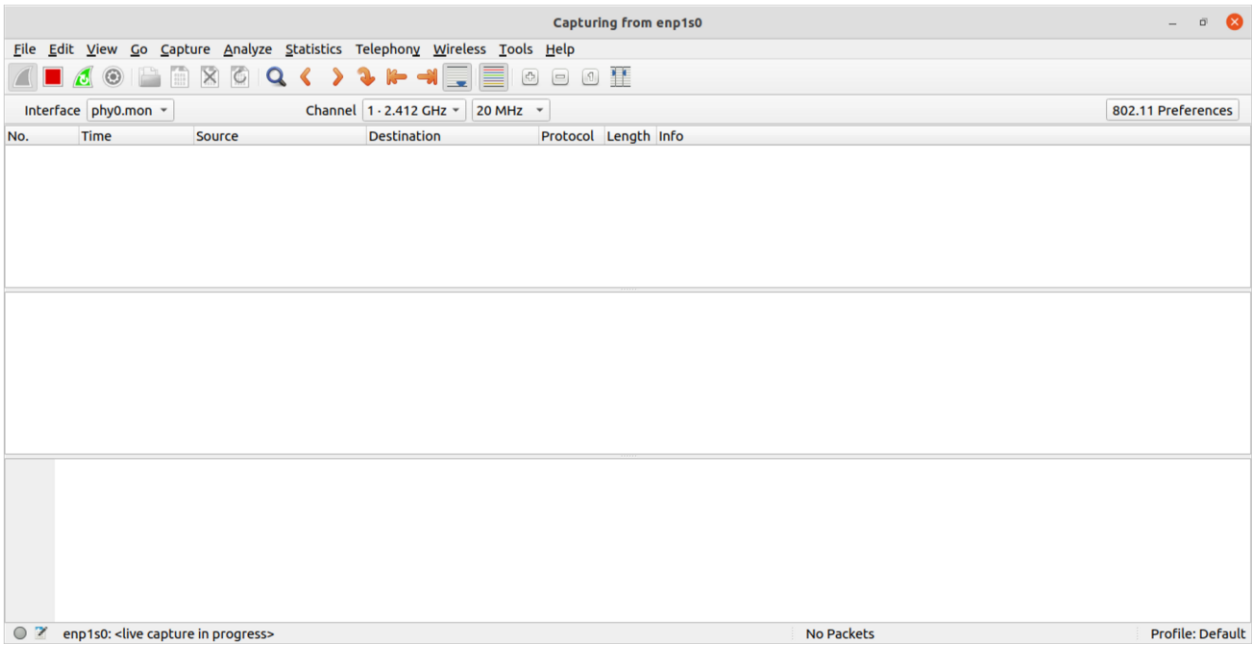

shamim@shamim-HP-ProBook-450-G5: ~
Preparing to unpack .../09-wireshark-common_3.4.2-1~ubuntu20.04.0+wiresharkdevst
able1_amd64.deb ...
Unpacking wireshark-common (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Selecting previously unselected package wireshark-qt.
Preparing to unpack .../10-wireshark-qt_3.4.2-1~ubuntu20.04.0+wiresharkdevstable
1_amd64.deb ...
Unpacking wireshark-qt (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Selecting previously unselected package wireshark.
Preparing to unpack .../11-wireshark_3.4.2-1~ubuntu20.04.0+wiresharkdevstable1_a
md64.deb ...
Unpacking wireshark (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up libminizip1:amd64 (1.1-8build1) ...
Setting up libc-ares2:amd64 (1.15.0-1build1) ...
Setting up libspandsp2:amd64 (0.0.6+dfsg-2) ...
Setting up libsmi2ldbl:amd64 (0.4.8+dfsg2-16) ...
Setting up libwsutil12:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up libwireshark-data (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Installing new version of config file /etc/wireshark/init.lua ...
Setting up liblua5.2-0:amd64 (5.2.4-1.1build3) ...
Setting up libwiretap11:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up libwireshark14:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up wireshark-common (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up wireshark-qt (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up wireshark (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for shared-mime-info (1.15-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
shamim@shamim-HP-ProBook-450-G5: $ apt show wireshark
Package: wireshark
Version: 3.4.2-1~ubuntu20.04.0+wiresharkdevstable1
Priority: optional
Section: net

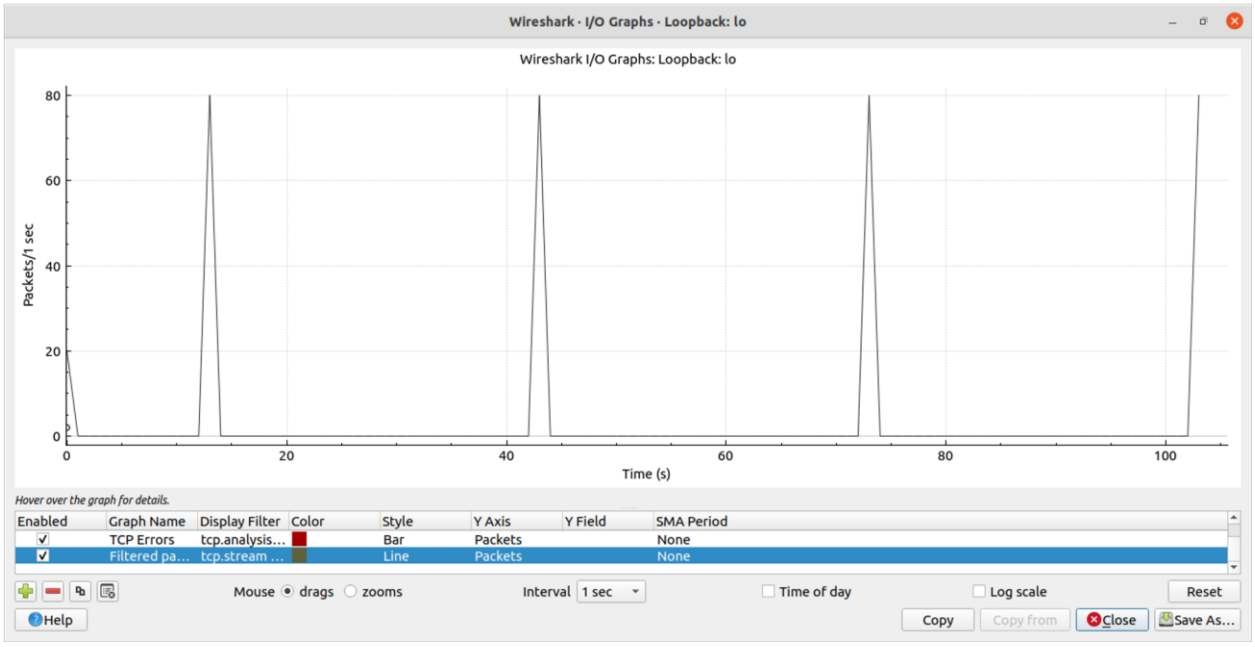

shamim@shamim-HP-ProBook-450-G5: ~
Installing new version of config file /etc/wireshark/init.lua ...
Setting up liblua5.2-0:amd64 (5.2.4-1.1build3) ...
Setting up libwiretap11:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up libwireshark14:amd64 (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up wireshark-common (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up wireshark-qt (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Setting up wireshark (3.4.2-1~ubuntu20.04.0+wiresharkdevstable1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for shared-mime-info (1.15-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
shamim@shamim-HP-ProBook-450-G5: $ apt show wireshark
Package: wireshark
Version: 3.4.2-1~ubuntu20.04.0+wiresharkdevstable1
Priority: optional
Section: net
Maintainer: Balint Reczey <rbalint@ubuntu.com>
Installed-Size: 60.4 kB
Depends: wireshark-qt (= 3.4.2-1~ubuntu20.04.0+wiresharkdevstable1)
Conflicts: ethereal (<< 1.0.0-3)
Replaces: ethereal (<< 1.0.0-3)
Download-Size: 44.8 kB
APT-Manual-Installed: yes
APT-Sources: http://ppa.launchpad.net/wireshark-dev/stable/ubuntu focal/main amd64 Packages
Description: network traffic analyzer - meta-package
 Wireshark is a network "sniffer" - a tool that captures and analyzes
 packets off the wire. Wireshark can decode too many protocols to list
 here.
 .
 This is a meta-package for Wireshark.
N: There is 1 additional record. Please use the '-a' switch to see it
shamim@shamim-HP-ProBook-450-G5: $

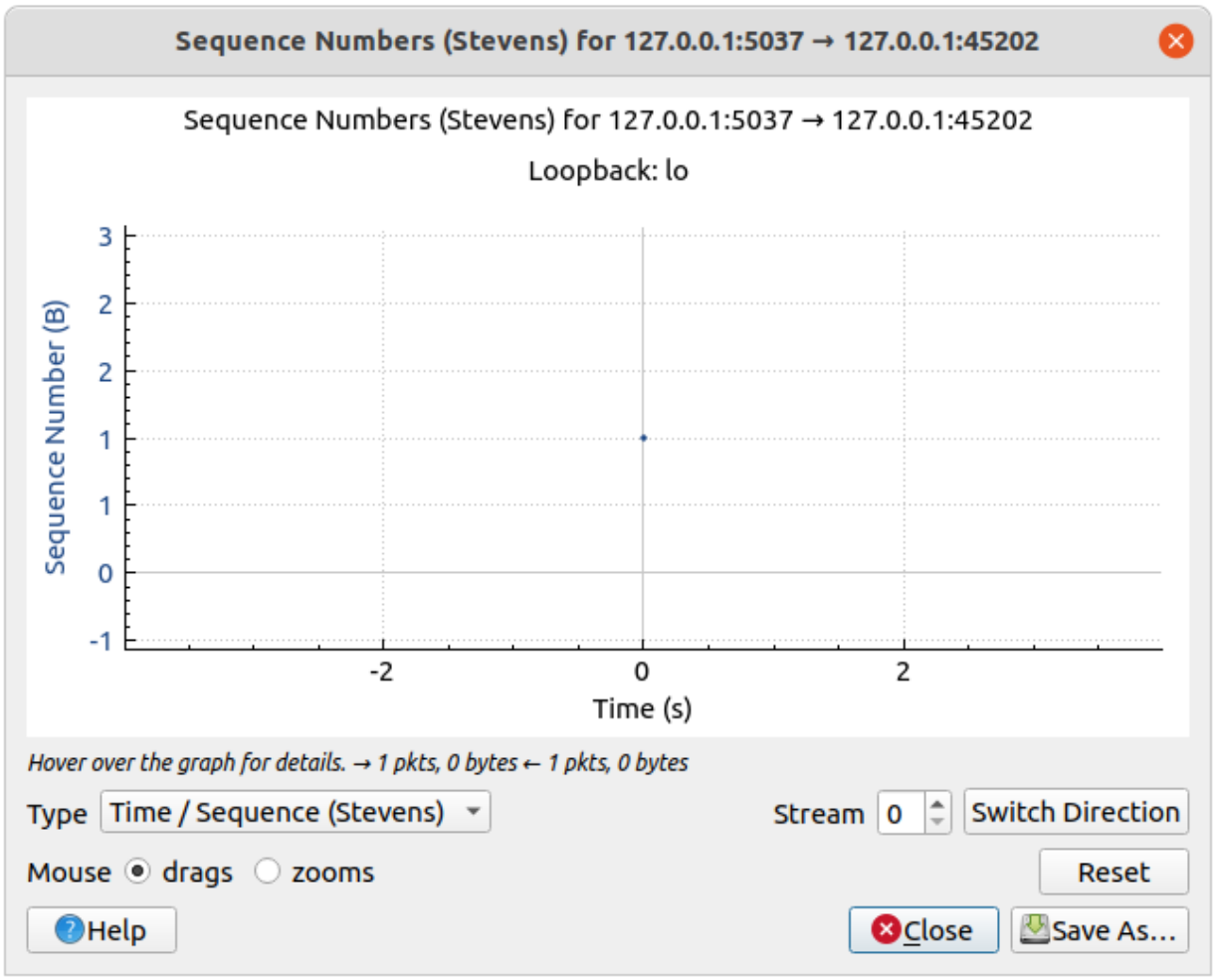
4. Exercises :

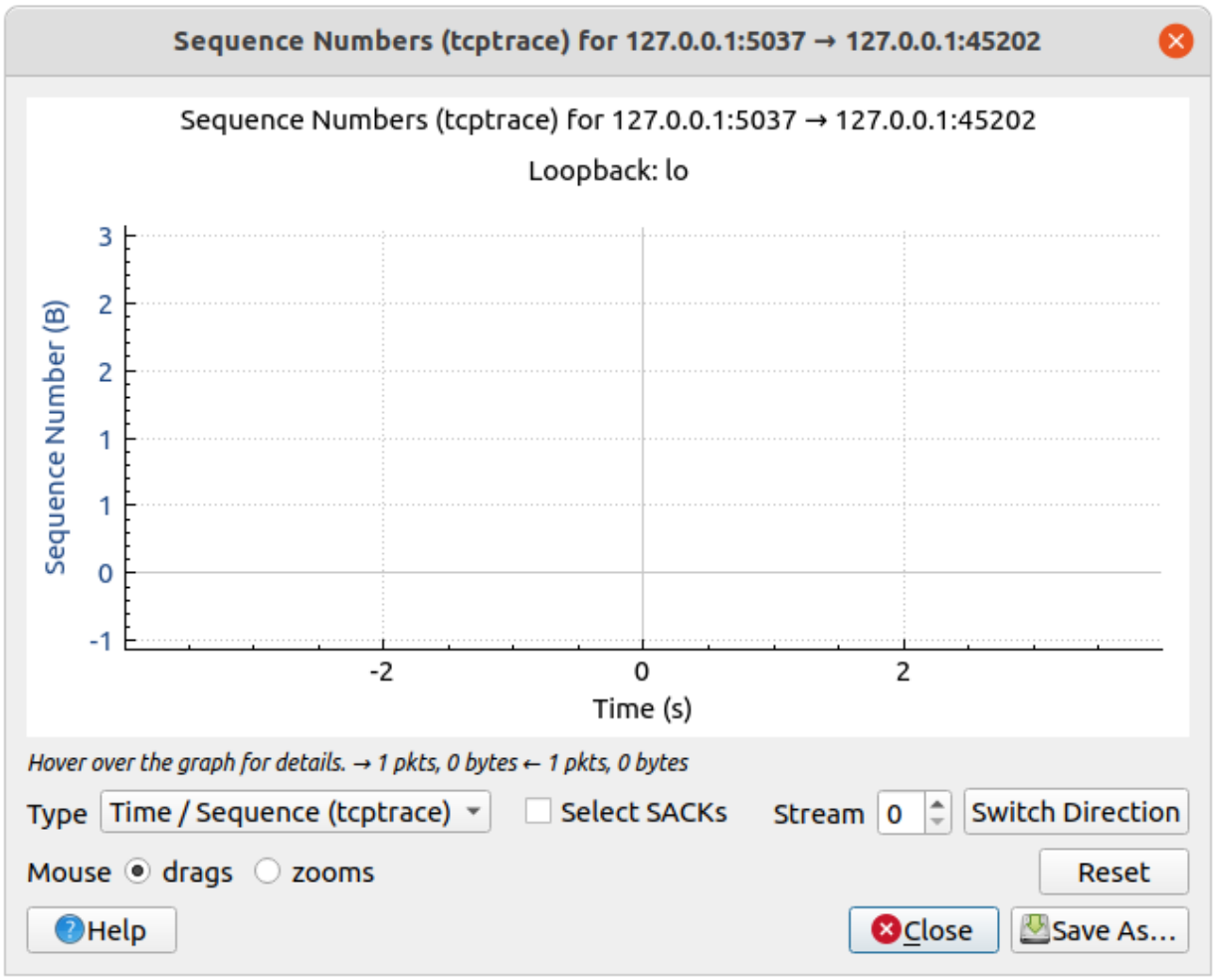

Capturing from bluetooth-monitor
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
No. Time Source Destination Protocol Length Info
1 0.000000 HCI_MON 40 Sent Adapter Id: 65535, Opcode: System Note
2 0.000004 HCI_MON 33 Sent Adapter Id: 65535, Opcode: System Note
3 0.000005 HCI_MON 16 Info Adapter Id: 0, Opcode: New Index
4 0.000006 HCI_MON 0 Sent Adapter Id: 0, Opcode: Open Index
5 0.000006 HCI_MON 8 Sent Adapter Id: 0, Opcode: Index Info
6 0.000008 HCI_MON 30 Sent Adapter Id: 65535, Opcode: Control Open
bluetooth-monitor: <live capture in progress>
Packets: 6 · Displayed: 6 (100.0%)
Profile: Default

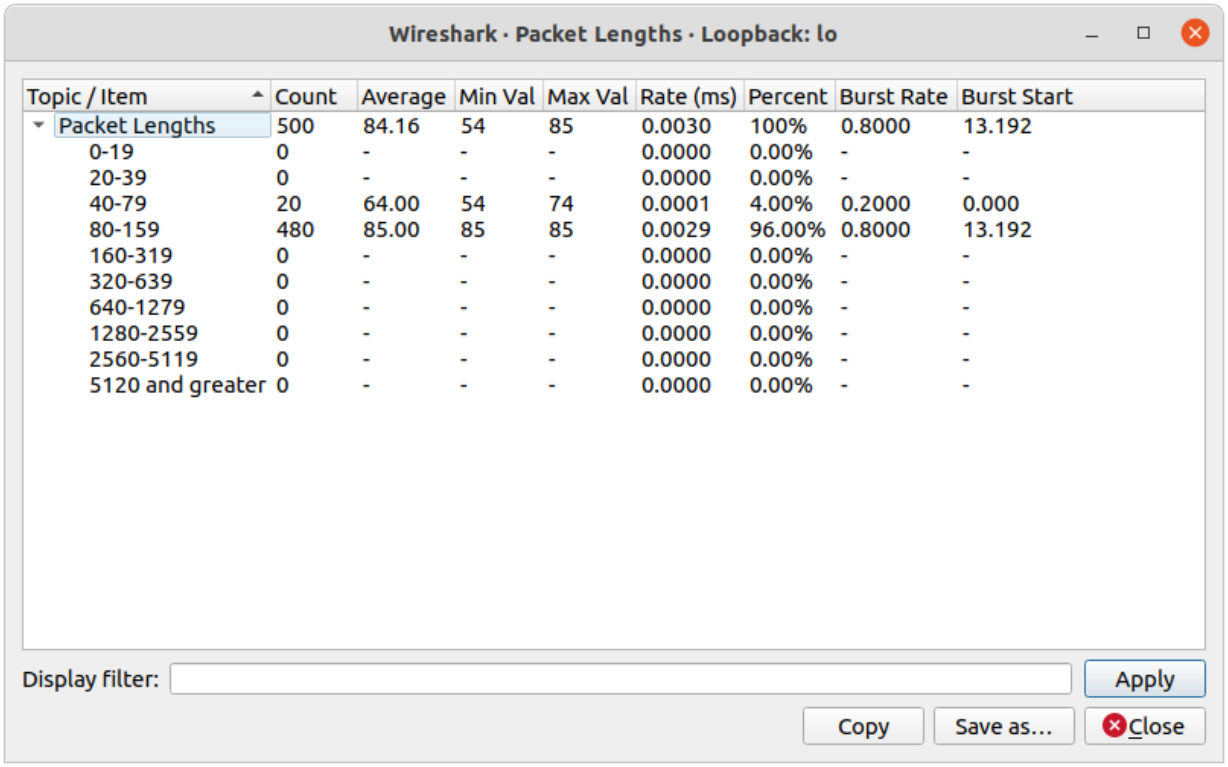

Unsaved packets...
Do you want to stop the capture and save the captured packets before quitting?
Your captured packets will be lost if you don't save them.
Stop and Quit without Saving
Cancel
Stop and Save
Capturing from Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
No. Time Source Destination Protocol Length Info
74 1.642183475 127.0.0.1 127.0.0.53 DNS 85 Standard query 0x9d27 A ntp.ubuntu.com OPT
75 1.642211891 127.0.0.1 127.0.0.53 DNS 85 Standard query 0xa85b AAAA ntp.ubuntu.com OPT
76 1.642349189 127.0.0.53 127.0.0.1 DNS 85 Standard query response 0x9d27 Server failure A ntp.ubuntu.com OPT
77 1.642504516 127.0.0.53 127.0.0.1 DNS 85 Standard query response 0xa85b Server failure AAAA ntp.ubuntu.com OPT
78 1.642577880 127.0.0.1 127.0.0.53 DNS 85 Standard query 0x9d27 A ntp.ubuntu.com OPT
79 1.642595956 127.0.0.1 127.0.0.53 DNS 85 Standard query 0xa85b AAAA ntp.ubuntu.com OPT
80 1.642722825 127.0.0.53 127.0.0.1 DNS 85 Standard query response 0x9d27 Server failure A ntp.ubuntu.com OPT
81 1.642870869 127.0.0.53 127.0.0.1 DNS 85 Standard query response 0xa85b Server failure AAAA ntp.ubuntu.com OPT
Frame 1: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 92 77 a0 40 00 ff 11 a3 bd 7f 00 00 01 e0 00
0020 00 fb 14 e9 14 e9 00 7e 60 8c 00 00 00 00 00 07
0030 00 00 00 00 00 00 04 5f 66 74 70 04 5f 74 63 70
0040 05 6c 6f 63 61 6c 00 00 0c 00 01 04 5f 6e 66 73
0050 c0 11 00 0c 00 01 0b 5f 61 66 70 6f 76 65 72 74
0060 63 70 c0 11 00 0c 00 01 04 5f 73 6d 62 c0 11 00
0070 0c 00 01 09 5f 73 66 74 70 2d 73 73 68 c0 11 00
0080 0c 00 01 08 5f 77 65 62 64 61 76 73 c0 11 00 0c
0090 00 01 07 5f 77 65 62 64 61 76 c0 11 00 0c 00 01
Loopback: lo: <live capture in progress>
Packets: 81 · Displayed: 81 (100.0%)
Profile: Default

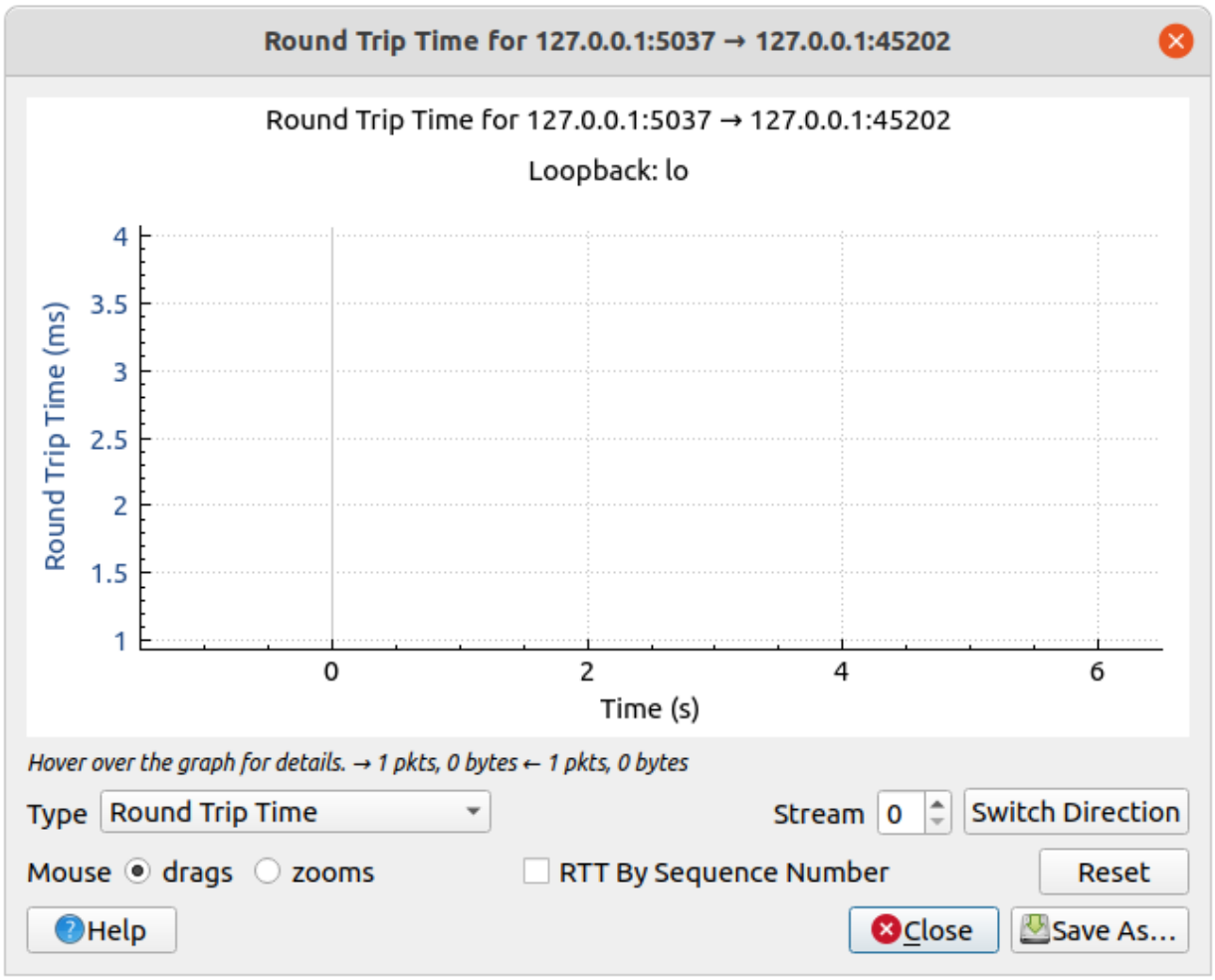

Capturing from enp1s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences
No. Time Source Destination Protocol Length Info
enp1s0: <live capture in progress>
No Packets
Profile: Default

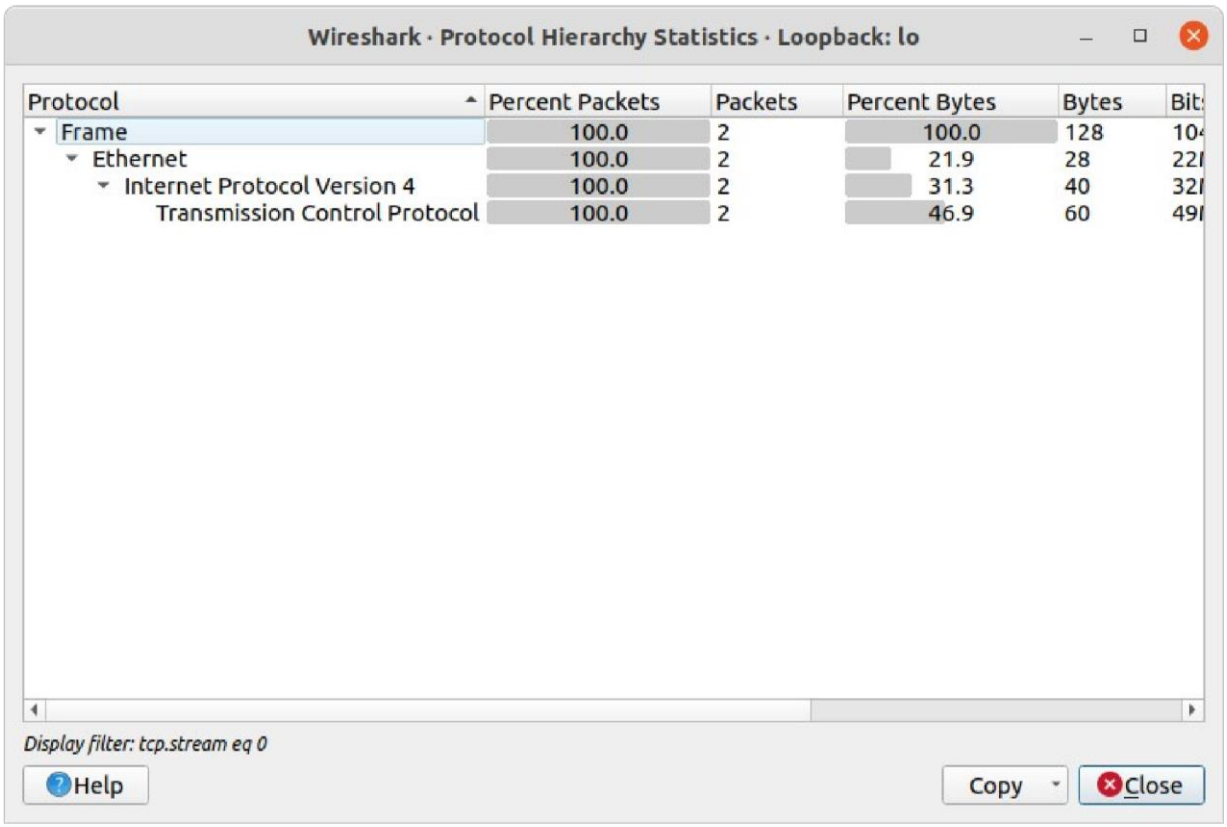

Wireshark · I/O Graphs · Loopback: lo
Wireshark I/O Graphs: Loopback: lo
Packets/1 sec
Time (s)
0
20
40
60
80
100
Hover over the graph for details.
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period
TCP Errors tcp.analysis... Bar Packets None
Filtered pa... tcp.stream ... Line Packets None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Help
Copy
Copy from
Close
Save As...


Sequence Numbers (Stevens) for 127.0.0.1:5037 → 127.0.0.1:45202
Sequence Numbers (Stevens) for 127.0.0.1:5037 → 127.0.0.1:45202
Loopback: lo
Sequence Number (B)
3
2
2
1
1
0
-1
-2
0
2
Time (s)
Hover over the graph for details. → 1 pkts, 0 bytes ← 1 pkts, 0 bytes
Type
Time / Sequence (Stevens)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Help
Close
Save As…

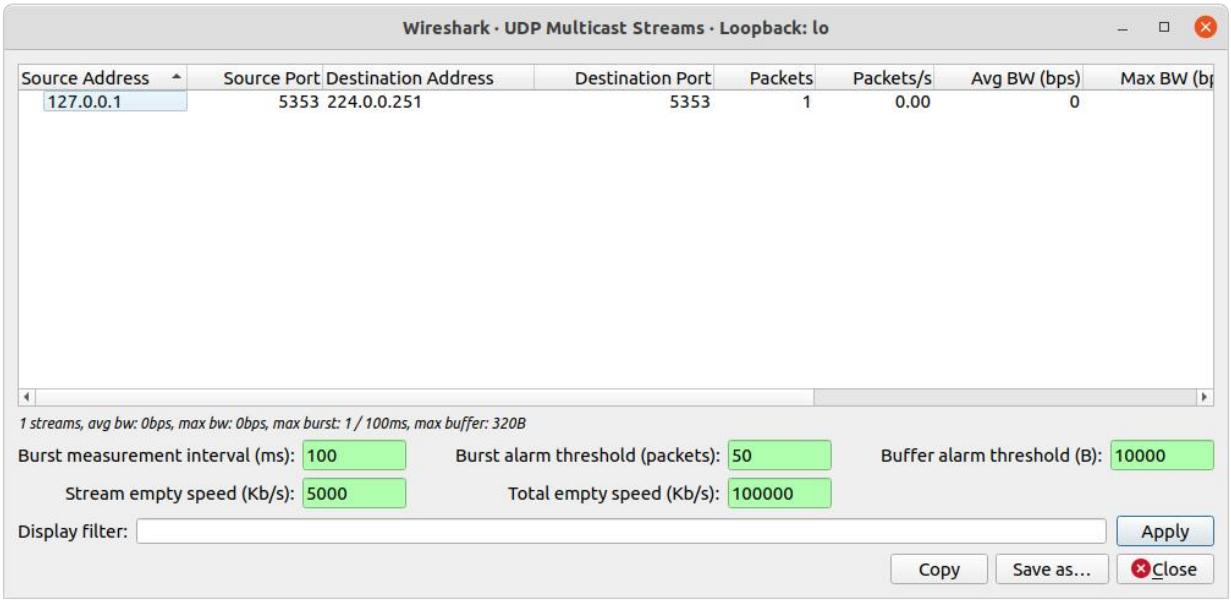

Sequence Numbers (tcptrace) for 127.0.0.1:5037 → 127.0.0.1:45202
Sequence Numbers (tcptrace) for 127.0.0.1:5037 → 127.0.0.1:45202
Loopback: lo
Sequence Number (B)
3
2
2
1
1
0
-1
-2
0
2
Time (s)
Hover over the graph for details. → 1 pkts, 0 bytes ← 1 pkts, 0 bytes
Type
Time / Sequence (tcptrace)
Select SACKs
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Help
Close
Save As…


Wireshark · Packet Lengths · Loopback: lo
Topic / Item
Count
Average
Min Val
Max Val
Rate (ms)
Percent
Burst Rate
Burst Start
Packet Lengths 500 84.16 54 85 0.0030 100% 0.8000 13.192
0-19 0 - - - 0.0000 0.00% - -
20-39 0 - - - 0.0000 0.00% - -
40-79 20 64.00 54 74 0.0001 4.00% 0.2000 0.000
80-159 480 85.00 85 85 0.0029 96.00% 0.8000 13.192
160-319 0 - - - 0.0000 0.00% - -
320-639 0 - - - 0.0000 0.00% - -
640-1279 0 - - - 0.0000 0.00% - -
1280-2559 0 - - - 0.0000 0.00% - -
2560-5119 0 - - - 0.0000 0.00% - -
5120 and greater 0 - - - 0.0000 0.00% - -
Display filter:
Apply
Copy
Save as...
Close


Round Trip Time for 127.0.0.1:5037 → 127.0.0.1:45202
Round Trip Time for 127.0.0.1:5037 → 127.0.0.1:45202
Loopback: lo
Round Trip Time (ms)
4
3.5
3
2.5
2
1.5
1
0
2
4
6
Time (s)
Hover over the graph for details. → 1 pkts, 0 bytes ← 1 pkts, 0 bytes
Type
Round Trip Time
Stream
0
Switch Direction
Mouse
drags
zooms
RTT By Sequence Number
Reset
Help
Close
Save As…




```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ·····E·
0010  00 3c 88 72 40 00 40 06  b4 47 7f 00 00 01 7f 00   ·<·r@·@· ·G·····
0020  00 01 b0 92 13 ad fe 1f  2d 5c 00 00 00 00 a0 02   ·····-\·····
0030  ff d7 fe 30 00 00 02 04  ff d7 04 02 08 0a 32 c0   ···0···· ·····2·
0040  cc df 00 00 00 00 01 03  03 07                     ·····
```


Wireshark · UDP Multicast Streams · Loopback: lo
Source Address
Source Port
Destination Address
Destination Port
Packets
Packets/s
Avg BW (bps)
Max BW (bp
127.0.0.1
5353
224.0.0.251
5353
1
0.00
0
1 streams, avg bw: 0bps, max bw: 0bps, max burst: 1 / 100ms, max buffer: 320B
Burst measurement interval (ms):
100
Burst alarm threshold (packets):
50
Buffer alarm threshold (B):
10000
Stream empty speed (Kb/s):
5000
Total empty speed (Kb/s):
100000
Display filter:
Apply
Copy
Save as…
Close