Mawlana Bhashani Science and Technology University

Lab-Report

Report No:04

Course code: ICT-4202

Course title: Wireless and Mobile Communication Lab

Date of Performance:11.09.20

Date of Submission:18.09.20

Submitted by

Name: Amrita kamkar

ID:IT-14060

4th year 2ndsemester

Session: 2013-2014

Dept. of ICT

MBSTU.

Submitted To

Nazrul Islam

Assistant Professor

Dept. of ICT

MBSTU.

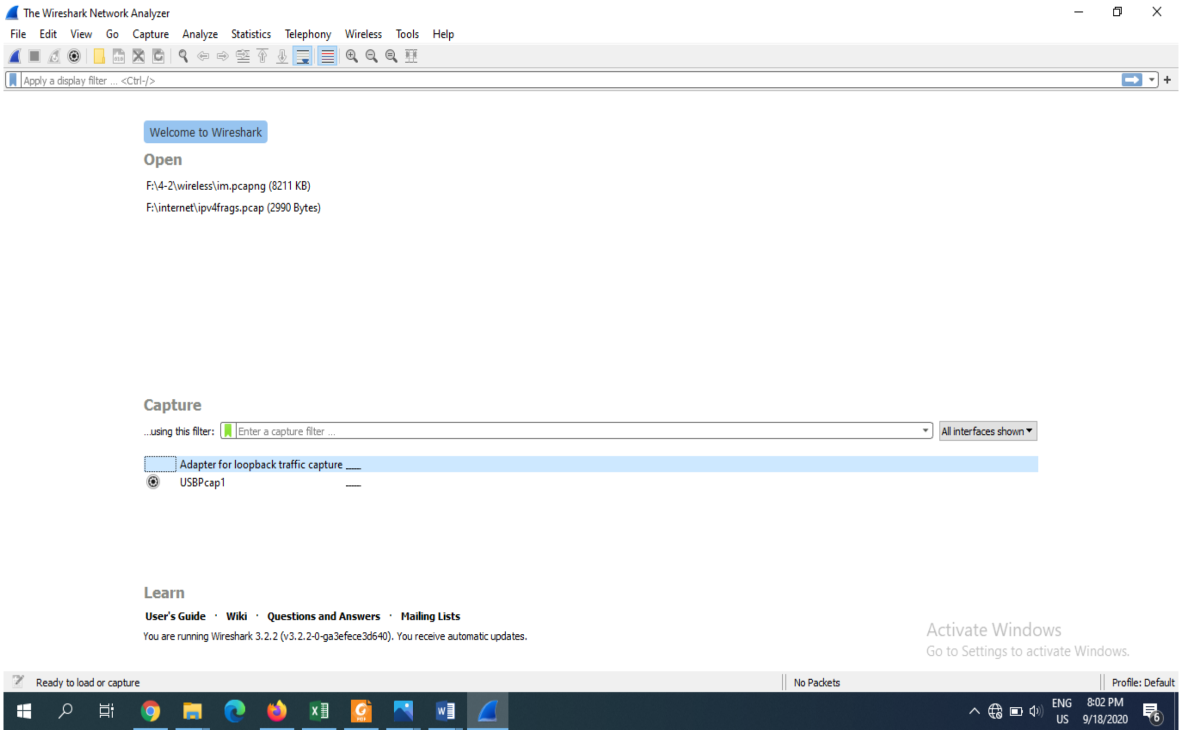
Experiment No:04

Experiment Name: Protocol Analysis with Wireshark

Objectives: Wireshark is a network traffic analyzer which is also an essential tool for any security professional or systems administrator. This free software lets us analyze network traffic in real time. This is one of the troubleshooting issues on our network. In this lab I am going to analyze the wireshark protocol.The capturing of traffic with specific network would be done .

Theoretical Explanation: Wireshark is a network packet analyzer as a measuring device for examining what's happening inside a cable. It can capture traffic from many different network media types including ethernet,wireless LAN,Bluetooth,USB and more. The specific media types supported may be limited by several factors, including our hardware operating system.

Working Procedure for capturing Data packets: There are some steps that to be **followed in this lab.**First of all I open the wireshark.



Apply a display filter ... <Ctrl-/>

F:\4-2\wireless\im.pcapng (8211 KB)

F:\internet\ipv4frags.pcap (2990 Bytes)

...using this filter: Enter a capture filter ...

Adapter for loopback traffic capture

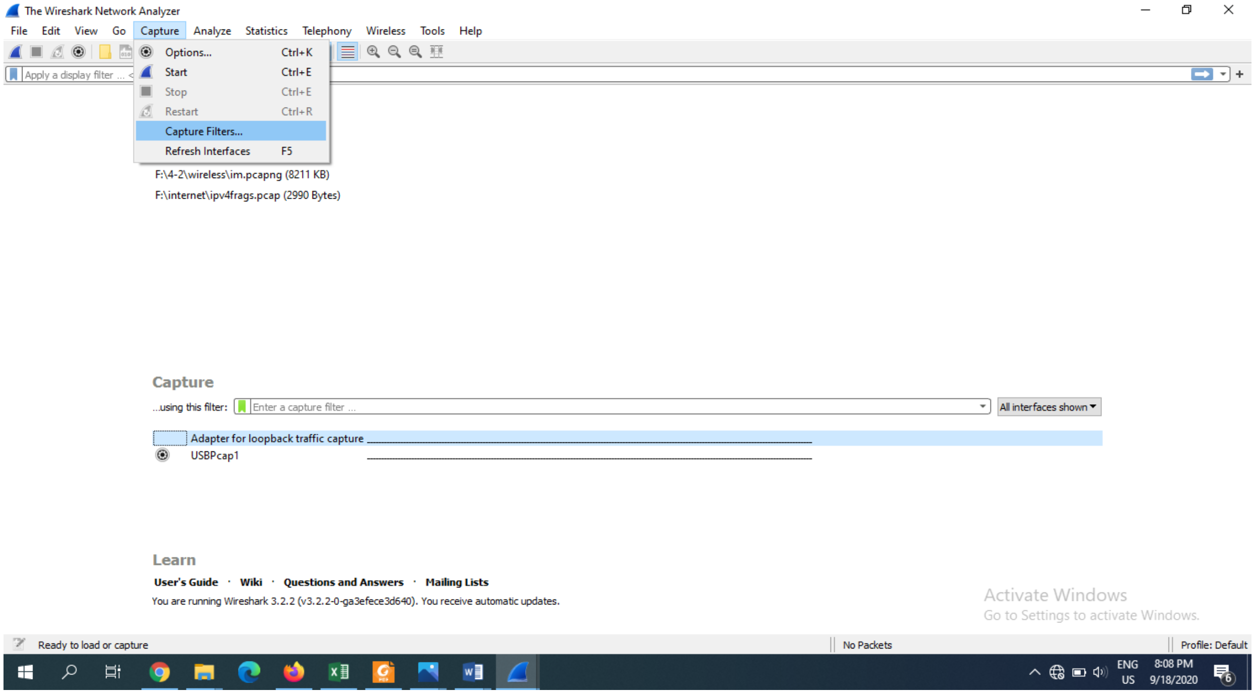
USBPcap1

You are running Wireshark 3.2.2 (v3.2.2-0-ga3efece3d640). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Fig1:Openning wireshark

Then to go to the capture and it's capture filters.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Apply a display filter ...
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Activate Windows
Go to Settings to activate Windows.
No Packets
Profile: Default
ENG US 8:08 PM 9/18/2020

F:\4-2\wireless\im.pcapng (8211 KB)
F:\internet\ipv4frags.pcap (2990 Bytes)

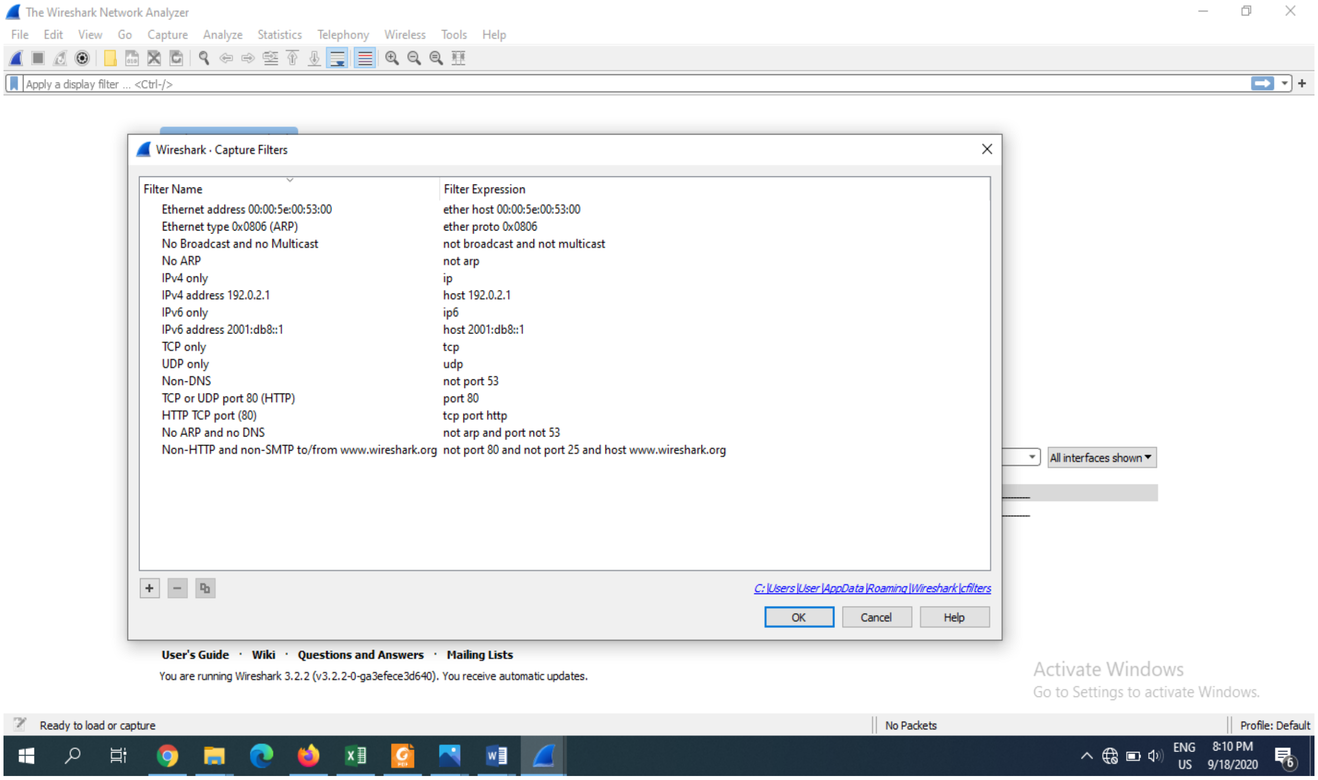
Adapter for loopback traffic capture
USBPcap1

You are running Wireshark 3.2.2 (v3.2.2-0-ga3efece3d640). You receive automatic updates.

Ready to load or capture

Fig2:selecting to capture filters

There would be some networks from where I need to select the one which has it’s IP address.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Wireshark · Capture Filters
OK
Cancel
Help
All interfaces shown
User's Guide · Wiki · Questions and Answers · Mailing Lists
Activate Windows
Go to Settings to activate Windows.
No Packets
Profile: Default
ENG US 8:10 PM 9/18/2020

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

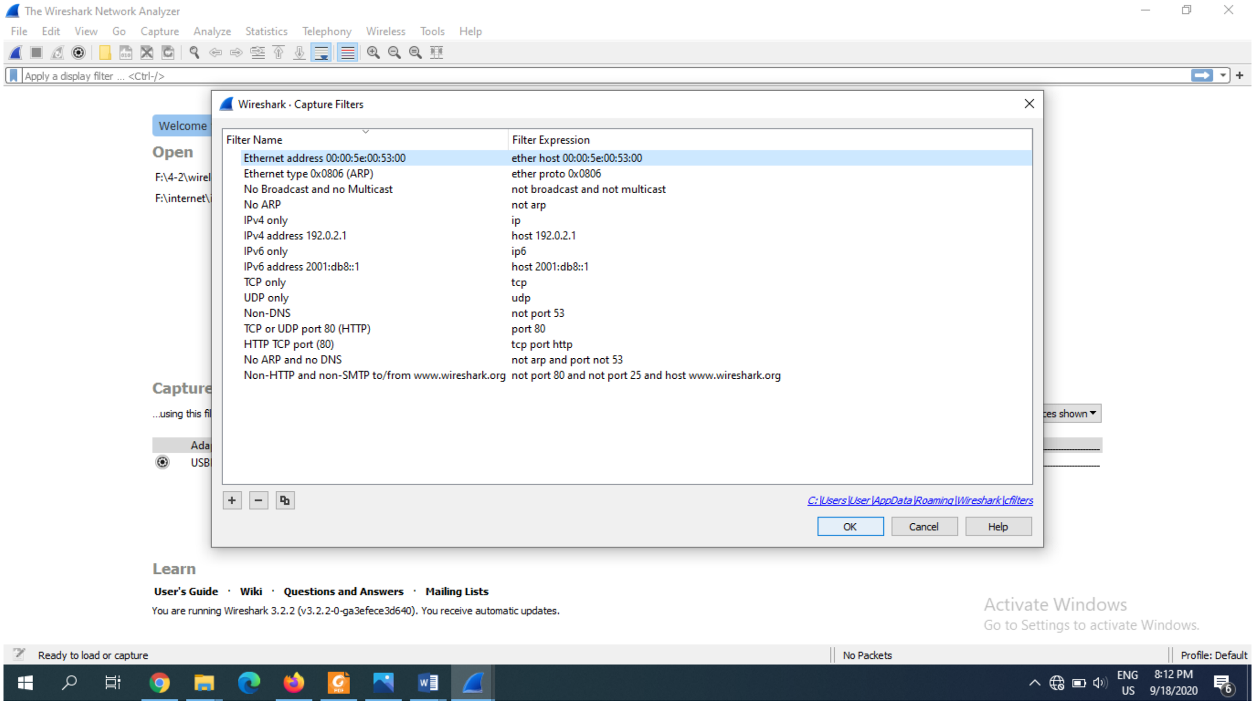
C:\Users\User\AppData\Roaming\Wireshark\cfilters

You are running Wireshark 3.2.2 (v3.2.2-0-ga3efece3d640). You receive automatic updates.

Ready to load or capture

Fig3:selecting the network

I selected the ethernet


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome
Open
F:\4-2\wirel
F:\internet\
Capture
...using this fi
ces shown
Ada
USB
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
Activate Windows
Go to Settings to activate Windows.
ENG US 8:12 PM 9/18/2020

Wireshark · Capture Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org

C:\Users\User\AppData\Roaming\Wireshark\cfilters

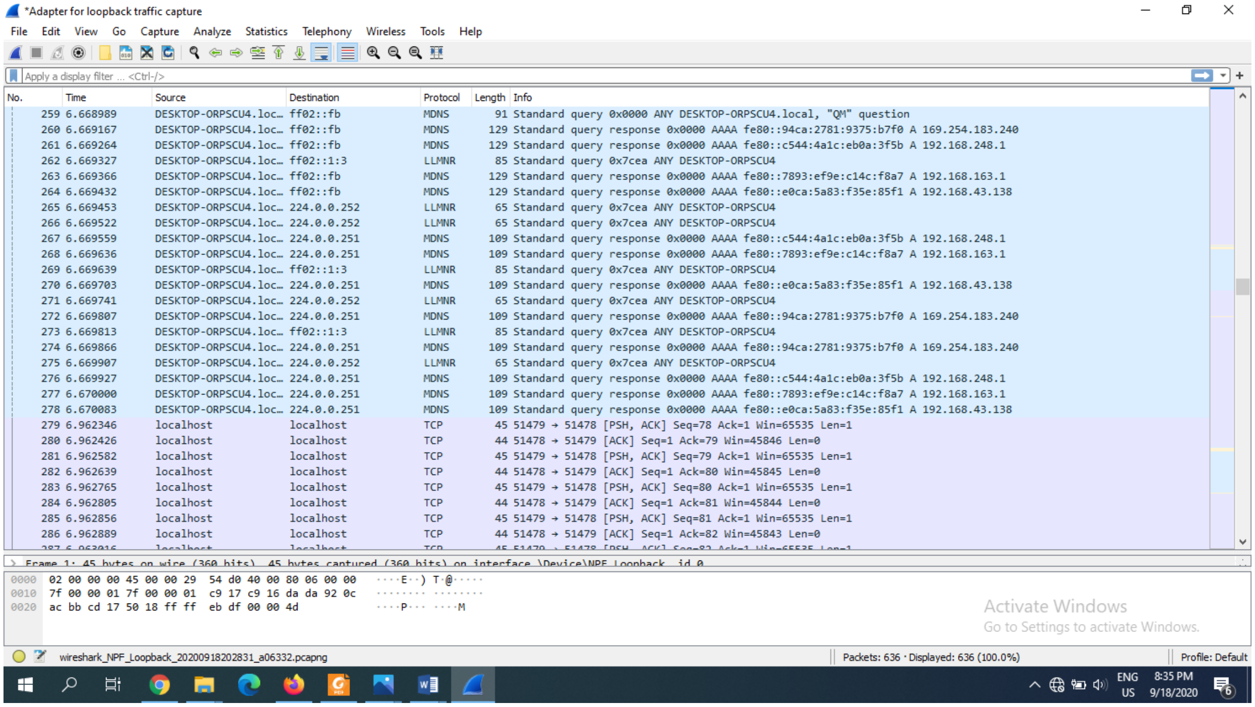
OK Cancel Help

You are running Wireshark 3.2.2 (v3.2.2-0-ga3efece3d640). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Fig4:selecting network

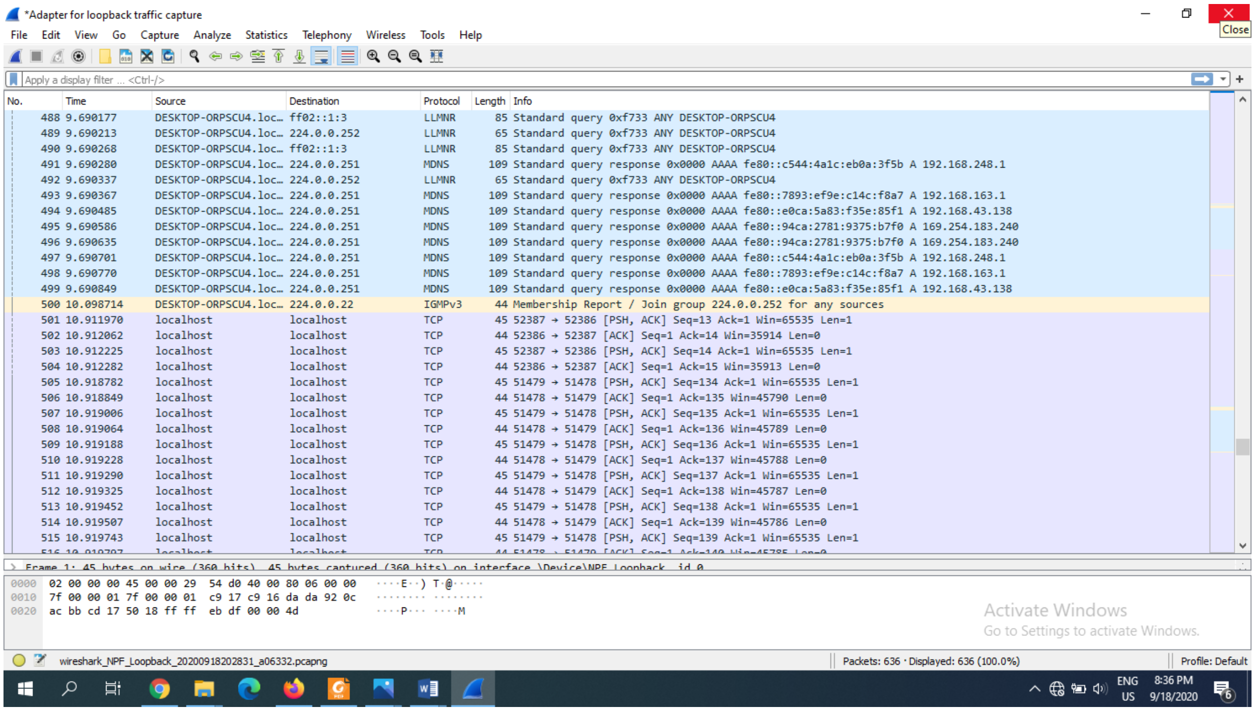
Then it’s needed to be start which would be


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
ENG US 8:35 PM 9/18/2020

```
No.  Time     Source               Destination  Protocol Length Info
 259 6.668989 DESKTOP-ORPSCU4.loc… ff02::fb     MDNS      91 Standard query 0x0000 ANY DESKTOP-ORPSCU4.local, "QM" question
 260 6.669167 DESKTOP-ORPSCU4.loc… ff02::fb     MDNS     129 Standard query response 0x0000 AAAA fe80::94ca:2781:9375:b7f0 A 169.254.183.240
 261 6.669264 DESKTOP-ORPSCU4.loc… ff02::fb     MDNS     129 Standard query response 0x0000 AAAA fe80::c544:4a1c:eb0a:3f5b A 192.168.248.1
 262 6.669327 DESKTOP-ORPSCU4.loc… ff02::1:3    LLMNR     85 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 263 6.669366 DESKTOP-ORPSCU4.loc… ff02::fb     MDNS     129 Standard query response 0x0000 AAAA fe80::7893:ef9e:c14c:f8a7 A 192.168.163.1
 264 6.669432 DESKTOP-ORPSCU4.loc… ff02::fb     MDNS     129 Standard query response 0x0000 AAAA fe80::e0ca:5a83:f35e:85f1 A 192.168.43.138
 265 6.669453 DESKTOP-ORPSCU4.loc… 224.0.0.252  LLMNR     65 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 266 6.669522 DESKTOP-ORPSCU4.loc… 224.0.0.252  LLMNR     65 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 267 6.669559 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::c544:4a1c:eb0a:3f5b A 192.168.248.1
 268 6.669636 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::7893:ef9e:c14c:f8a7 A 192.168.163.1
 269 6.669639 DESKTOP-ORPSCU4.loc… ff02::1:3    LLMNR     85 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 270 6.669703 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::e0ca:5a83:f35e:85f1 A 192.168.43.138
 271 6.669741 DESKTOP-ORPSCU4.loc… 224.0.0.252  LLMNR     65 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 272 6.669807 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::94ca:2781:9375:b7f0 A 169.254.183.240
 273 6.669813 DESKTOP-ORPSCU4.loc… ff02::1:3    LLMNR     85 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 274 6.669866 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::94ca:2781:9375:b7f0 A 169.254.183.240
 275 6.669907 DESKTOP-ORPSCU4.loc… 224.0.0.252  LLMNR     65 Standard query 0x7cea ANY DESKTOP-ORPSCU4
 276 6.669927 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::c544:4a1c:eb0a:3f5b A 192.168.248.1
 277 6.670000 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::7893:ef9e:c14c:f8a7 A 192.168.163.1
 278 6.670083 DESKTOP-ORPSCU4.loc… 224.0.0.251  MDNS     109 Standard query response 0x0000 AAAA fe80::e0ca:5a83:f35e:85f1 A 192.168.43.138
 279 6.962346 localhost            localhost    TCP       45 51479 → 51478 [PSH, ACK] Seq=78 Ack=1 Win=65535 Len=1
 280 6.962426 localhost            localhost    TCP       44 51478 → 51479 [ACK] Seq=1 Ack=79 Win=45846 Len=0
 281 6.962582 localhost            localhost    TCP       45 51479 → 51478 [PSH, ACK] Seq=79 Ack=1 Win=65535 Len=1
 282 6.962639 localhost            localhost    TCP       44 51478 → 51479 [ACK] Seq=1 Ack=80 Win=45845 Len=0
 283 6.962765 localhost            localhost    TCP       45 51479 → 51478 [PSH, ACK] Seq=80 Ack=1 Win=65535 Len=1
 284 6.962805 localhost            localhost    TCP       44 51478 → 51479 [ACK] Seq=1 Ack=81 Win=45844 Len=0
 285 6.962856 localhost            localhost    TCP       45 51479 → 51478 [PSH, ACK] Seq=81 Ack=1 Win=65535 Len=1
 286 6.962889 localhost            localhost    TCP       44 51478 → 51479 [ACK] Seq=1 Ack=82 Win=45843 Len=0
 287 6.963016 localhost            localhost    TCP       45 51479 → 51478 [PSH, ACK] Seq=82 Ack=1 Win=65535 Len=1

> Frame 1: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface \Device\NPF_Loopback, id 0

0000  02 00 00 00 45 00 00 29  54 d0 40 00 80 06 00 00   ····E··) T·@·····
0010  7f 00 00 01 7f 00 00 01  c9 17 c9 16 da da 92 0c   ········ ········
0020  ac bb cd 17 50 18 ff ff  eb df 00 00 4d            ····P··· ····M
```

wireshark_NPF_Loopback_20200918202831_a06332.pcapng | Packets: 636 · Displayed: 636 (100.0%) | Profile: Default

Fig5:starting the capturing

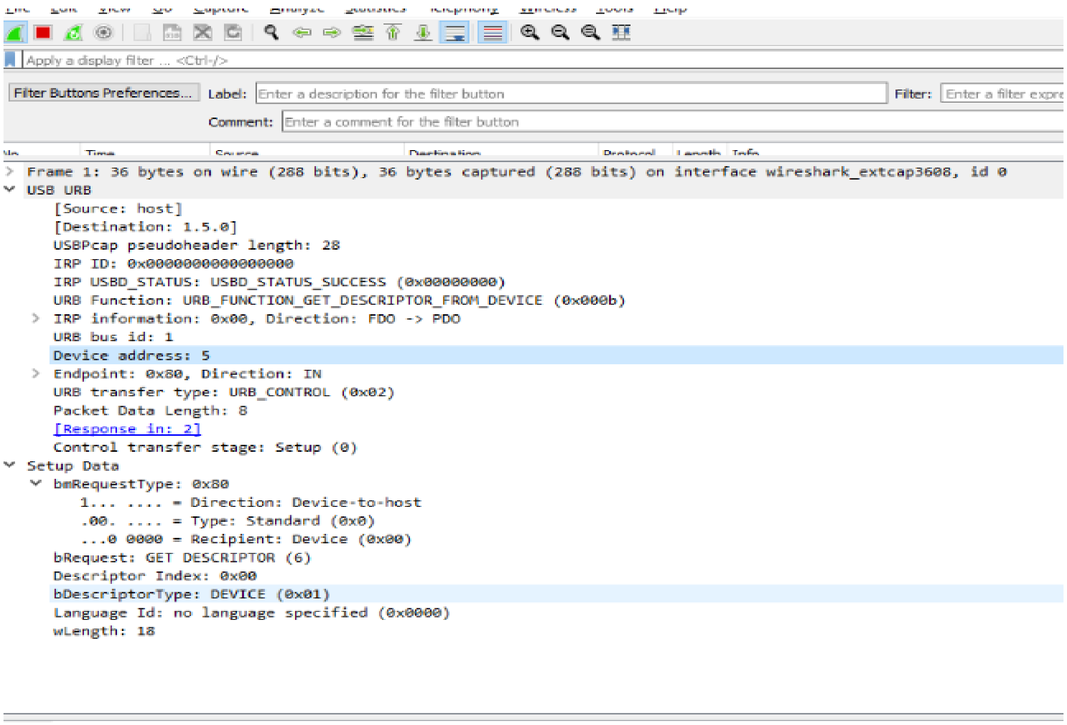


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Close

```
No.    Time       Source                    Destination   Protocol  Length Info
  488 9.690177   DESKTOP-ORPSCU4.loc…  ff02::1:3     LLMNR      85 Standard query 0xf733 ANY DESKTOP-ORPSCU4
  489 9.690213   DESKTOP-ORPSCU4.loc…  224.0.0.252   LLMNR      65 Standard query 0xf733 ANY DESKTOP-ORPSCU4
  490 9.690268   DESKTOP-ORPSCU4.loc…  ff02::1:3     LLMNR      85 Standard query 0xf733 ANY DESKTOP-ORPSCU4
  491 9.690280   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::c544:4a1c:eb0a:3f5b A 192.168.248.1
  492 9.690337   DESKTOP-ORPSCU4.loc…  224.0.0.252   LLMNR      65 Standard query 0xf733 ANY DESKTOP-ORPSCU4
  493 9.690367   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::7893:ef9e:c14c:f8a7 A 192.168.163.1
  494 9.690485   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::e0ca:5a83:f35e:85f1 A 192.168.43.138
  495 9.690586   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::94ca:2781:9375:b7f0 A 169.254.183.240
  496 9.690635   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::94ca:2781:9375:b7f0 A 169.254.183.240
  497 9.690701   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::c544:4a1c:eb0a:3f5b A 192.168.248.1
  498 9.690770   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::7893:ef9e:c14c:f8a7 A 192.168.163.1
  499 9.690849   DESKTOP-ORPSCU4.loc…  224.0.0.251   MDNS      109 Standard query response 0x0000 AAAA fe80::e0ca:5a83:f35e:85f1 A 192.168.43.138
  500 10.098714  DESKTOP-ORPSCU4.loc…  224.0.0.22    IGMPv3     44 Membership Report / Join group 224.0.0.252 for any sources
  501 10.911970  localhost             localhost     TCP        45 52387 → 52386 [PSH, ACK] Seq=13 Ack=1 Win=65535 Len=1
  502 10.912062  localhost             localhost     TCP        44 52386 → 52387 [ACK] Seq=1 Ack=14 Win=35914 Len=0
  503 10.912225  localhost             localhost     TCP        45 52387 → 52386 [PSH, ACK] Seq=14 Ack=1 Win=65535 Len=1
  504 10.912282  localhost             localhost     TCP        44 52386 → 52387 [ACK] Seq=1 Ack=15 Win=35913 Len=0
  505 10.918782  localhost             localhost     TCP        45 51479 → 51478 [PSH, ACK] Seq=134 Ack=1 Win=65535 Len=1
  506 10.918849  localhost             localhost     TCP        44 51478 → 51479 [ACK] Seq=1 Ack=135 Win=45790 Len=0
  507 10.919006  localhost             localhost     TCP        45 51479 → 51478 [PSH, ACK] Seq=135 Ack=1 Win=65535 Len=1
  508 10.919064  localhost             localhost     TCP        44 51478 → 51479 [ACK] Seq=1 Ack=136 Win=45789 Len=0
  509 10.919188  localhost             localhost     TCP        45 51479 → 51478 [PSH, ACK] Seq=136 Ack=1 Win=65535 Len=1
  510 10.919228  localhost             localhost     TCP        44 51478 → 51479 [ACK] Seq=1 Ack=137 Win=45788 Len=0
  511 10.919290  localhost             localhost     TCP        45 51479 → 51478 [PSH, ACK] Seq=137 Ack=1 Win=65535 Len=1
  512 10.919325  localhost             localhost     TCP        44 51478 → 51479 [ACK] Seq=1 Ack=138 Win=45787 Len=0
  513 10.919452  localhost             localhost     TCP        45 51479 → 51478 [PSH, ACK] Seq=138 Ack=1 Win=65535 Len=1
  514 10.919507  localhost             localhost     TCP        44 51478 → 51479 [ACK] Seq=1 Ack=139 Win=45786 Len=0
  515 10.919743  localhost             localhost     TCP        45 51479 → 51478 [PSH, ACK] Seq=139 Ack=1 Win=65535 Len=1

> Frame 1: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface \Device\NPF_Loopback, id 0

0000  02 00 00 00 45 00 00 29  54 d0 40 00 80 06 00 00   ····E··) T·@·····
0010  7f 00 00 01 7f 00 00 01  c9 17 c9 16 da da 92 0c   ········ ········
0020  ac bb cd 17 50 18 ff ff  eb df 00 00 4d            ····P··· ····M
```

Activate Windows
Go to Settings to activate Windows.
wireshark_NPF_Loopback_20200918202831_a06332.pcapng
Packets: 636 · Displayed: 636 (100.0%)
Profile: Default
ENG
US
8:36 PM
9/18/2020

Manually performed analysis

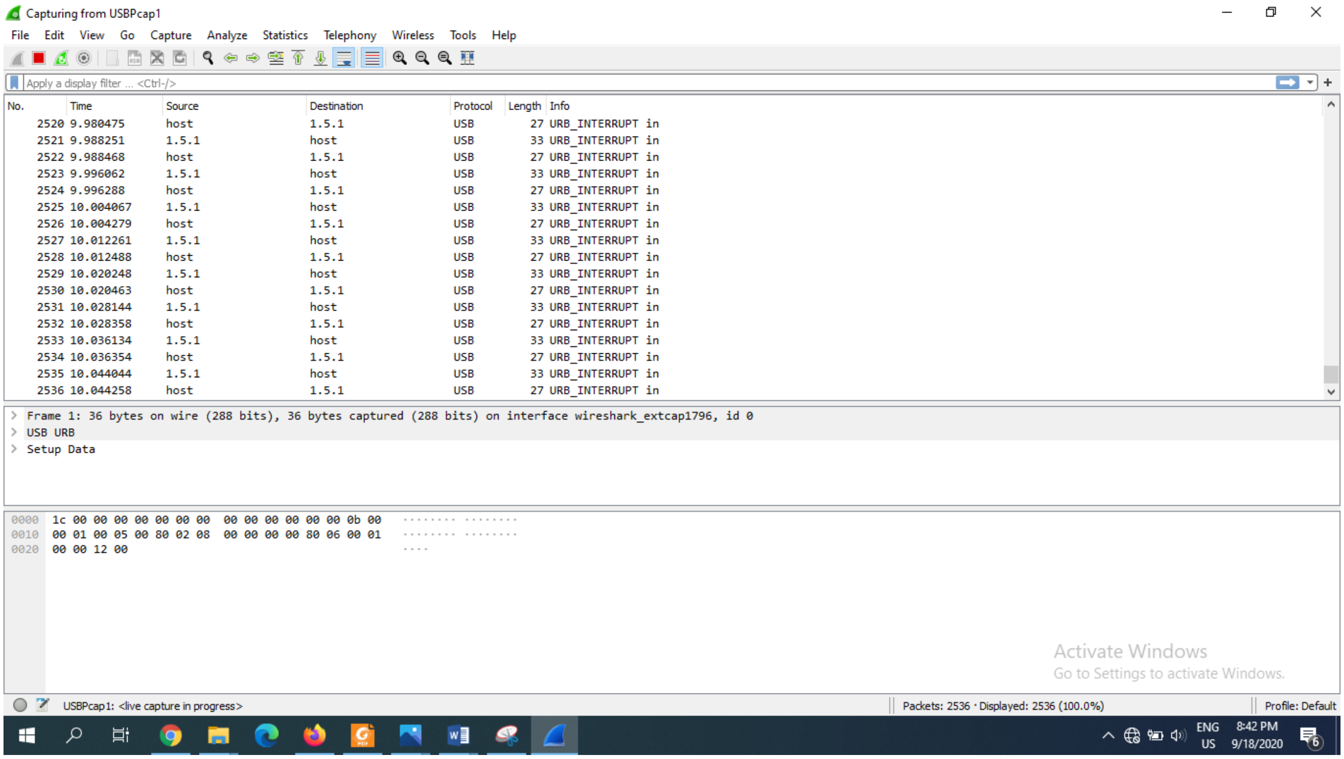


Apply a display filter … <Ctrl-/>
Filter Buttons Preferences...
Label:
Enter a description for the filter button
Filter:
Enter a filter expre
Comment:
Enter a comment for the filter button

```
> Frame 1: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on interface wireshark_extcap3608, id 0
v USB URB
    [Source: host]
    [Destination: 1.5.0]
    USBPcap pseudoheader length: 28
    IRP ID: 0x0000000000000000
    IRP USBD_STATUS: USBD_STATUS_SUCCESS (0x00000000)
    URB Function: URB_FUNCTION_GET_DESCRIPTOR_FROM_DEVICE (0x000b)
  > IRP information: 0x00, Direction: FDO -> PDO
    URB bus id: 1
    Device address: 5
  > Endpoint: 0x80, Direction: IN
    URB transfer type: URB_CONTROL (0x02)
    Packet Data Length: 8
    [Response in: 2]
    Control transfer stage: Setup (0)
v Setup Data
  v bmRequestType: 0x80
        1... .... = Direction: Device-to-host
        .00. .... = Type: Standard (0x0)
        ...0 0000 = Recipient: Device (0x00)
    bRequest: GET DESCRIPTOR (6)
    Descriptor Index: 0x00
    bDescriptorType: DEVICE (0x01)
    Language Id: no language specified (0x0000)
    wLength: 18
```

Fig6:Manuall analysis

Another network that was tried is the USBP cap1.

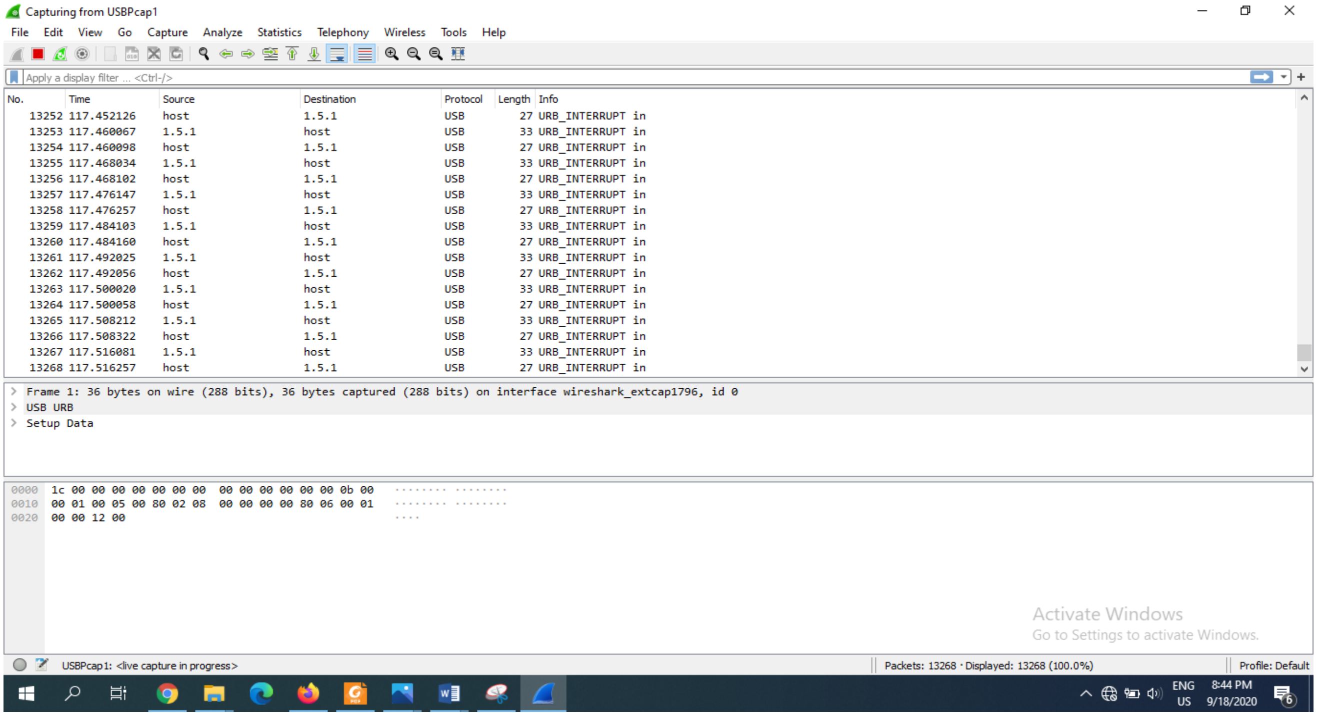

Capturing from USBPcap1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
ENG
US
8:42 PM
9/18/2020

```
No.     Time       Source         Destination    Protocol Length Info
   2520 9.980475   host           1.5.1          USB         27 URB_INTERRUPT in
   2521 9.988251   1.5.1          host           USB         33 URB_INTERRUPT in
   2522 9.988468   host           1.5.1          USB         27 URB_INTERRUPT in
   2523 9.996062   1.5.1          host           USB         33 URB_INTERRUPT in
   2524 9.996288   host           1.5.1          USB         27 URB_INTERRUPT in
   2525 10.004067  1.5.1          host           USB         33 URB_INTERRUPT in
   2526 10.004279  host           1.5.1          USB         27 URB_INTERRUPT in
   2527 10.012261  1.5.1          host           USB         33 URB_INTERRUPT in
   2528 10.012488  host           1.5.1          USB         27 URB_INTERRUPT in
   2529 10.020248  1.5.1          host           USB         33 URB_INTERRUPT in
   2530 10.020463  host           1.5.1          USB         27 URB_INTERRUPT in
   2531 10.028144  1.5.1          host           USB         33 URB_INTERRUPT in
   2532 10.028358  host           1.5.1          USB         27 URB_INTERRUPT in
   2533 10.036134  1.5.1          host           USB         33 URB_INTERRUPT in
   2534 10.036354  host           1.5.1          USB         27 URB_INTERRUPT in
   2535 10.044044  1.5.1          host           USB         33 URB_INTERRUPT in
   2536 10.044258  host           1.5.1          USB         27 URB_INTERRUPT in
```

```
> Frame 1: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on interface wireshark_extcap1796, id 0
> USB URB
> Setup Data
```

```
0000  1c 00 00 00 00 00 00 00  00 00 00 00 00 00 0b 00   ........ ........
0010  00 01 00 05 00 80 02 08  00 00 00 00 80 06 00 01   ........ ........
0020  00 00 12 00                                        ....
```

USBPcap1: <live capture in progress>
Packets: 2536 · Displayed: 2536 (100.0%)
Profile: Default


Capturing from USBPcap1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
ENG
US
8:44 PM
9/18/2020

```
No.     Time        Source         Destination    Protocol Length Info
  13252 117.452126  host           1.5.1          USB         27 URB_INTERRUPT in
  13253 117.460067  1.5.1          host           USB         33 URB_INTERRUPT in
  13254 117.460098  host           1.5.1          USB         27 URB_INTERRUPT in
  13255 117.468034  1.5.1          host           USB         33 URB_INTERRUPT in
  13256 117.468102  host           1.5.1          USB         27 URB_INTERRUPT in
  13257 117.476147  1.5.1          host           USB         33 URB_INTERRUPT in
  13258 117.476257  host           1.5.1          USB         27 URB_INTERRUPT in
  13259 117.484103  1.5.1          host           USB         33 URB_INTERRUPT in
  13260 117.484160  host           1.5.1          USB         27 URB_INTERRUPT in
  13261 117.492025  1.5.1          host           USB         33 URB_INTERRUPT in
  13262 117.492056  host           1.5.1          USB         27 URB_INTERRUPT in
  13263 117.500020  1.5.1          host           USB         33 URB_INTERRUPT in
  13264 117.500058  host           1.5.1          USB         27 URB_INTERRUPT in
  13265 117.508212  1.5.1          host           USB         33 URB_INTERRUPT in
  13266 117.508322  host           1.5.1          USB         27 URB_INTERRUPT in
  13267 117.516081  1.5.1          host           USB         33 URB_INTERRUPT in
  13268 117.516257  host           1.5.1          USB         27 URB_INTERRUPT in
```

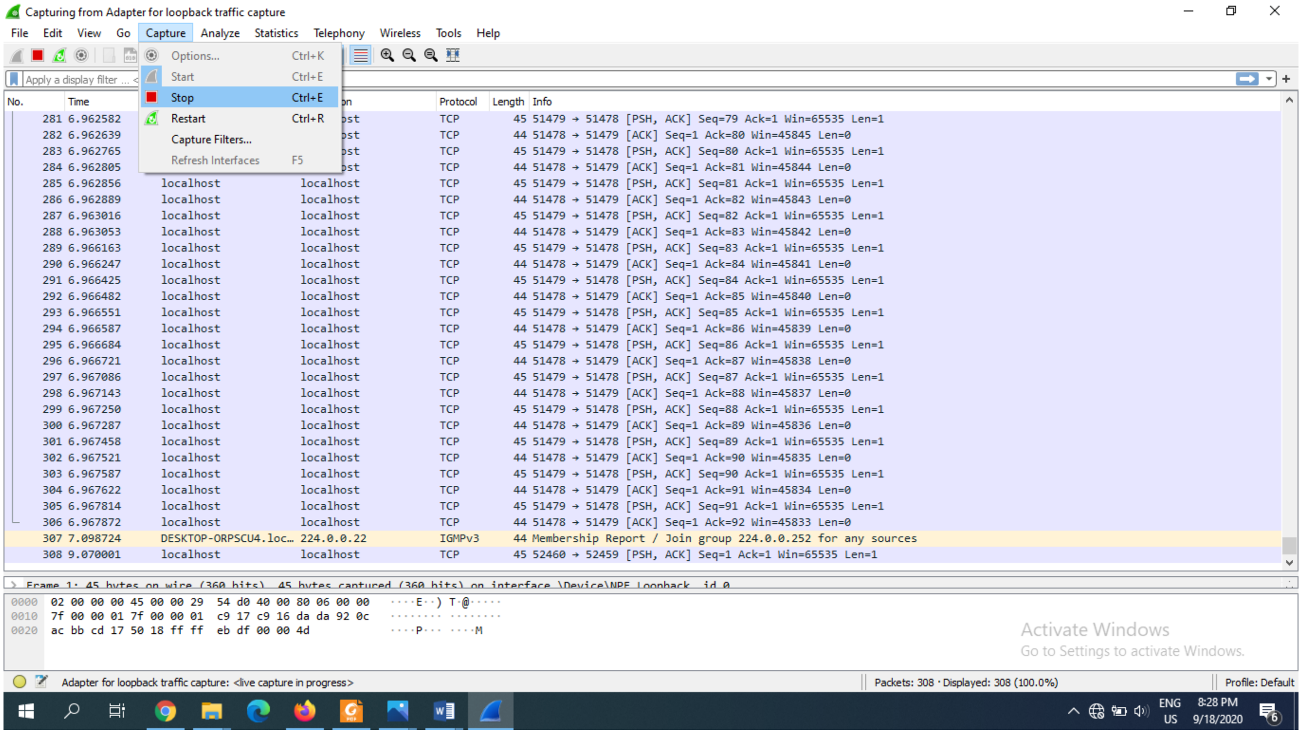
```
> Frame 1: 36 bytes on wire (288 bits), 36 bytes captured (288 bits) on interface wireshark_extcap1796, id 0
> USB URB
> Setup Data
```

```
0000  1c 00 00 00 00 00 00 00  00 00 00 00 00 00 0b 00   ........ ........
0010  00 01 00 05 00 80 02 08  00 00 00 00 80 06 00 01   ........ ........
0020  00 00 12 00                                        ....
```

USBPcap1: <live capture in progress>
Packets: 13268 · Displayed: 13268 (100.0%)
Profile: Default

Fig8:capturing with another network(USBP cap1)

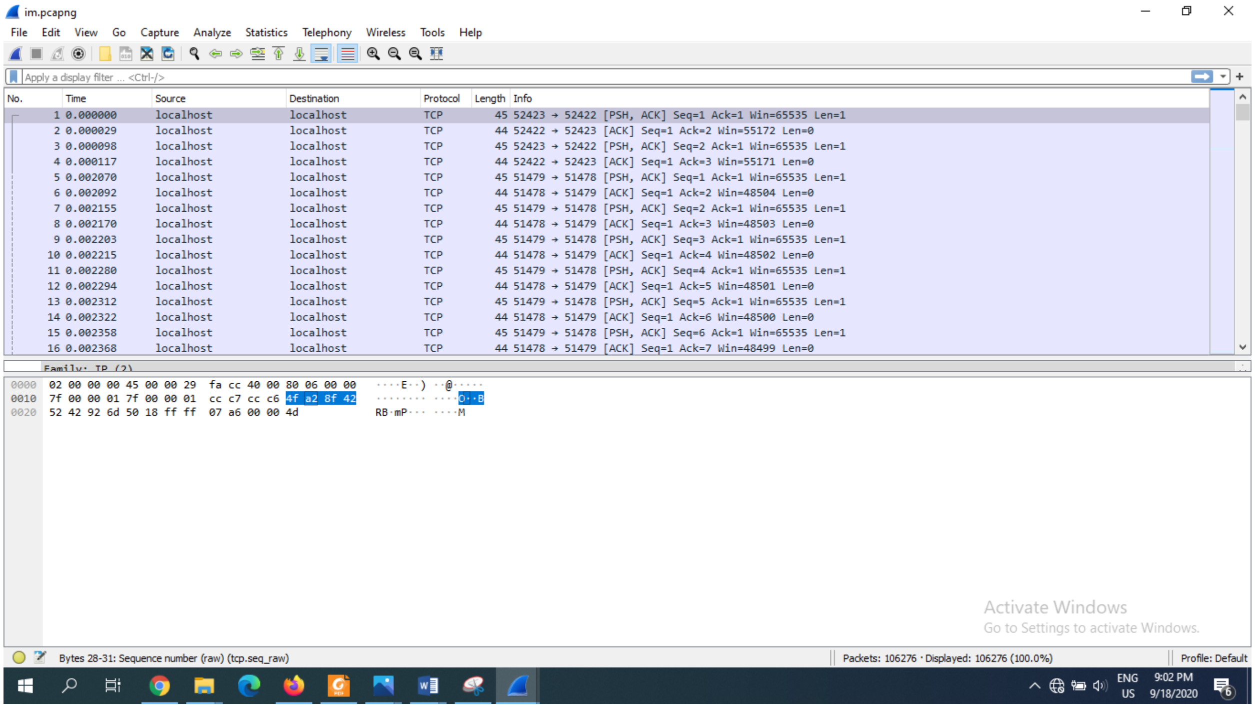
The capturing can be stopped by clicking the stop



```
No.   Time                                    Protocol  Length Info
  281 6.962582                        ost      TCP        45 51479 → 51478 [PSH, ACK] Seq=79 Ack=1 Win=65535 Len=1
  282 6.962639                        ost      TCP        44 51478 → 51479 [ACK] Seq=1 Ack=80 Win=45845 Len=0
  283 6.962765                        ost      TCP        45 51479 → 51478 [PSH, ACK] Seq=80 Ack=1 Win=65535 Len=1
  284 6.962805                        ost      TCP        44 51478 → 51479 [ACK] Seq=1 Ack=81 Win=45844 Len=0
  285 6.962856  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=81 Ack=1 Win=65535 Len=1
  286 6.962889  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=82 Win=45843 Len=0
  287 6.963016  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=82 Ack=1 Win=65535 Len=1
  288 6.963053  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=83 Win=45842 Len=0
  289 6.966163  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=83 Ack=1 Win=65535 Len=1
  290 6.966247  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=84 Win=45841 Len=0
  291 6.966425  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=84 Ack=1 Win=65535 Len=1
  292 6.966482  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=85 Win=45840 Len=0
  293 6.966551  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=85 Ack=1 Win=65535 Len=1
  294 6.966587  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=86 Win=45839 Len=0
  295 6.966684  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=86 Ack=1 Win=65535 Len=1
  296 6.966721  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=87 Win=45838 Len=0
  297 6.967086  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=87 Ack=1 Win=65535 Len=1
  298 6.967143  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=88 Win=45837 Len=0
  299 6.967250  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=88 Ack=1 Win=65535 Len=1
  300 6.967287  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=89 Win=45836 Len=0
  301 6.967458  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=89 Ack=1 Win=65535 Len=1
  302 6.967521  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=90 Win=45835 Len=0
  303 6.967587  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=90 Ack=1 Win=65535 Len=1
  304 6.967622  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=91 Win=45834 Len=0
  305 6.967814  localhost     localhost        TCP        45 51479 → 51478 [PSH, ACK] Seq=91 Ack=1 Win=65535 Len=1
  306 6.967872  localhost     localhost        TCP        44 51478 → 51479 [ACK] Seq=1 Ack=92 Win=45833 Len=0
  307 7.098724  DESKTOP-ORPSCU4.loc… 224.0.0.22 IGMPv3     44 Membership Report / Join group 224.0.0.252 for any sources
  308 9.070001  localhost     localhost        TCP        45 52460 → 52459 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1

> Frame 1: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface \Device\NPF_Loopback, id 0

0000  02 00 00 00 45 00 00 29  54 d0 40 00 80 06 00 00   ····E··) T·@·····
0010  7f 00 00 01 7f 00 00 01  c9 17 c9 16 da da 92 0c   ········ ········
0020  ac bb cd 17 50 18 ff ff  eb df 00 00 4d            ····P··· ····M

Adapter for loopback traffic capture: <live capture in progress>   Packets: 308 · Displayed: 308 (100.0%)   Profile: Default
```

Fig9:stopping the capture

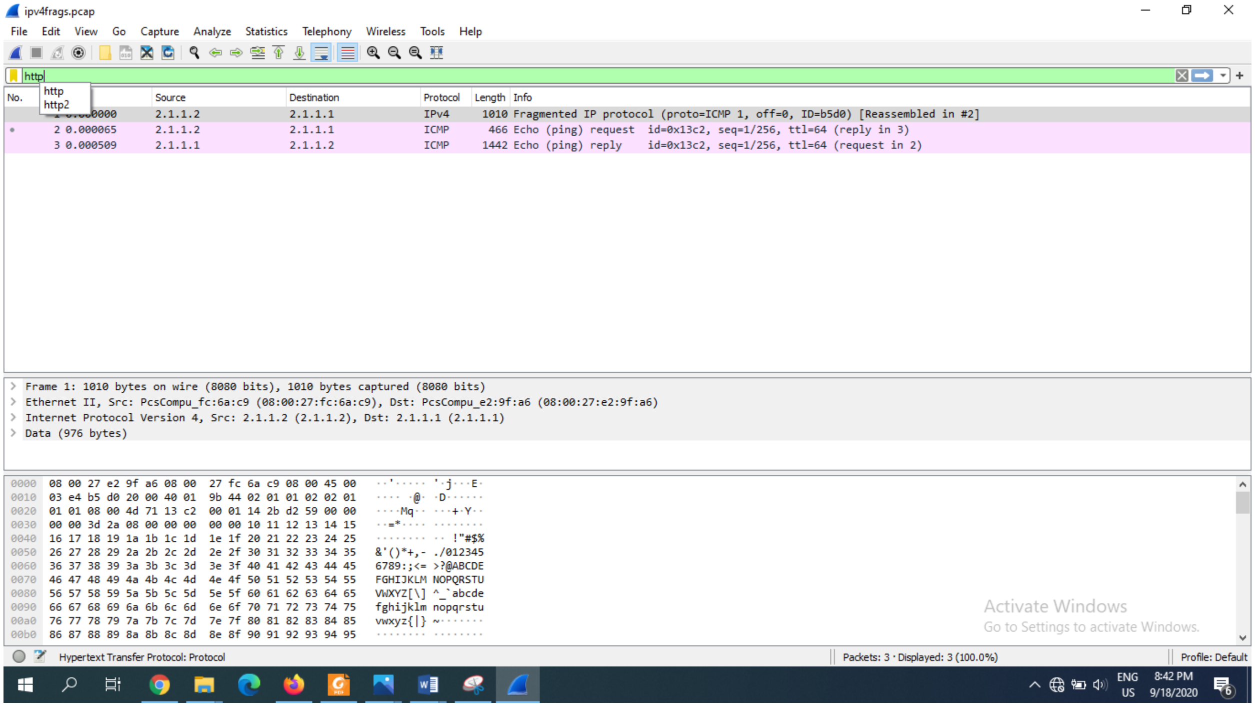
Packet bytes consists of Hex,ASCII and offset fields.



```
No.  Time       Source      Destination  Protocol  Length Info
   1 0.000000   localhost   localhost    TCP         45 52423 → 52422 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1
   2 0.000029   localhost   localhost    TCP         44 52422 → 52423 [ACK] Seq=1 Ack=2 Win=55172 Len=0
   3 0.000098   localhost   localhost    TCP         45 52423 → 52422 [PSH, ACK] Seq=2 Ack=1 Win=65535 Len=1
   4 0.000117   localhost   localhost    TCP         44 52422 → 52423 [ACK] Seq=1 Ack=3 Win=55171 Len=0
   5 0.002070   localhost   localhost    TCP         45 51479 → 51478 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=1
   6 0.002092   localhost   localhost    TCP         44 51478 → 51479 [ACK] Seq=1 Ack=2 Win=48504 Len=0
   7 0.002155   localhost   localhost    TCP         45 51479 → 51478 [PSH, ACK] Seq=2 Ack=1 Win=65535 Len=1
   8 0.002170   localhost   localhost    TCP         44 51478 → 51479 [ACK] Seq=1 Ack=3 Win=48503 Len=0
   9 0.002203   localhost   localhost    TCP         45 51479 → 51478 [PSH, ACK] Seq=3 Ack=1 Win=65535 Len=1
  10 0.002215   localhost   localhost    TCP         44 51478 → 51479 [ACK] Seq=1 Ack=4 Win=48502 Len=0
  11 0.002280   localhost   localhost    TCP         45 51479 → 51478 [PSH, ACK] Seq=4 Ack=1 Win=65535 Len=1
  12 0.002294   localhost   localhost    TCP         44 51478 → 51479 [ACK] Seq=1 Ack=5 Win=48501 Len=0
  13 0.002312   localhost   localhost    TCP         45 51479 → 51478 [PSH, ACK] Seq=5 Ack=1 Win=65535 Len=1
  14 0.002322   localhost   localhost    TCP         44 51478 → 51479 [ACK] Seq=1 Ack=6 Win=48500 Len=0
  15 0.002358   localhost   localhost    TCP         45 51479 → 51478 [PSH, ACK] Seq=6 Ack=1 Win=65535 Len=1
  16 0.002368   localhost   localhost    TCP         44 51478 → 51479 [ACK] Seq=1 Ack=7 Win=48499 Len=0

     Family: IP (2)

0000  02 00 00 00 45 00 00 29  fa cc 40 00 80 06 00 00   ····E··) ··@·····
0010  7f 00 00 01 7f 00 00 01  cc c7 cc c6 4f a2 8f 42   ········ ····O··B
0020  52 42 92 6d 50 18 ff ff  07 a6 00 00 4d            RB·mP··· ····M

Bytes 28-31: Sequence number (raw) (tcp.seq_raw)   Packets: 106276 · Displayed: 106276 (100.0%)   Profile: Default
```

Fig10:consisted data packet fields

The packet details pane is


ipv4frags.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
Activate Windows
Go to Settings to activate Windows.
ENG US 8:42 PM 9/18/2020

```
No.                Source        Destination   Protocol  Length Info
   1 0.000000      2.1.1.2       2.1.1.1       IPv4        1010 Fragmented IP protocol (proto=ICMP 1, off=0, ID=b5d0) [Reassembled in #2]
   2 0.000065      2.1.1.2       2.1.1.1       ICMP         466 Echo (ping) request  id=0x13c2, seq=1/256, ttl=64 (reply in 3)
   3 0.000509      2.1.1.1       2.1.1.2       ICMP        1442 Echo (ping) reply    id=0x13c2, seq=1/256, ttl=64 (request in 2)
```

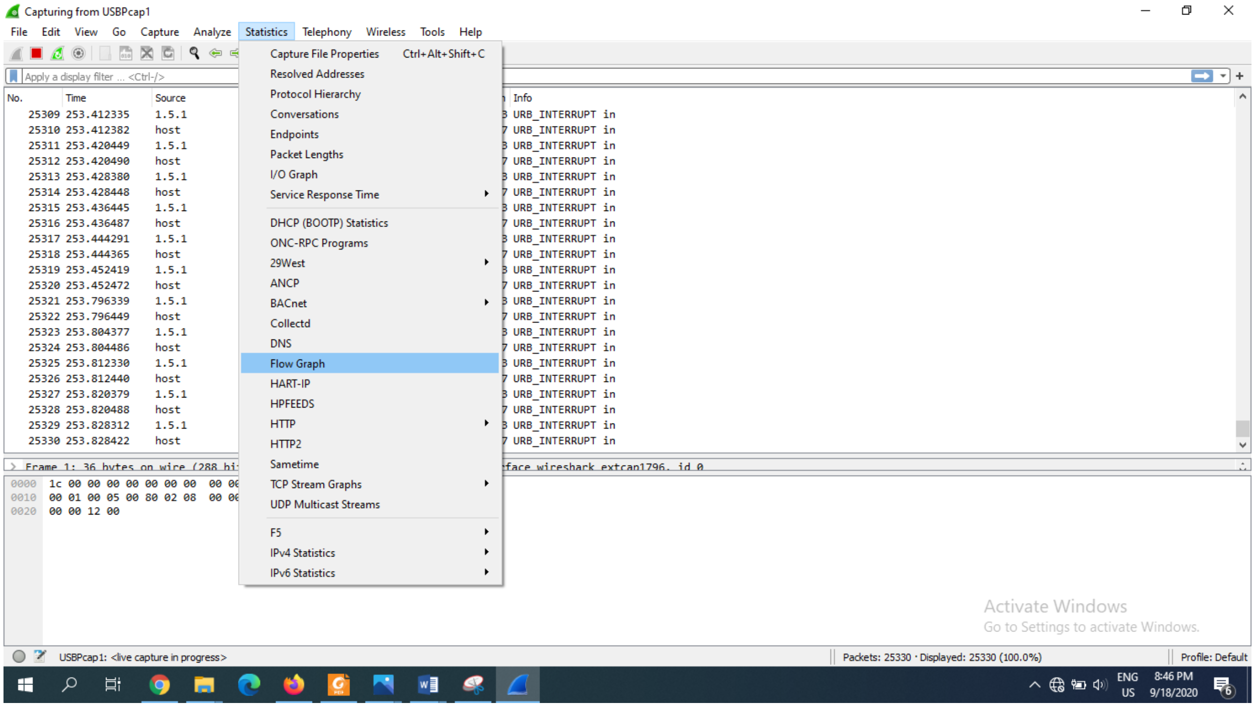
```
> Frame 1: 1010 bytes on wire (8080 bits), 1010 bytes captured (8080 bits)
> Ethernet II, Src: PcsCompu_fc:6a:c9 (08:00:27:fc:6a:c9), Dst: PcsCompu_e2:9f:a6 (08:00:27:e2:9f:a6)
> Internet Protocol Version 4, Src: 2.1.1.2 (2.1.1.2), Dst: 2.1.1.1 (2.1.1.1)
> Data (976 bytes)
```

```
0000  08 00 27 e2 9f a6 08 00  27 fc 6a c9 08 00 45 00   ··'·····  '·j···E·
0010  03 e4 b5 d0 20 00 40 01  9b 44 02 01 01 02 02 01   ···· ·@·  ·D······
0020  01 01 08 00 4d 71 13 c2  00 01 14 2b d2 59 00 00   ····Mq··  ···+·Y··
0030  00 00 3d 2a 08 00 00 00  00 00 10 11 12 13 14 15   ··=*····  ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········  ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,-  ./012345
0060  36 37 38 39 3a 3b 3c 3d  3e 3f 40 41 42 43 44 45   6789:;<=  >?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d  4e 4f 50 51 52 53 54 55   FGHIJKLM  NOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d  5e 5f 60 61 62 63 64 65   VWXYZ[\]  ^_`abcde
0090  66 67 68 69 6a 6b 6c 6d  6e 6f 70 71 72 73 74 75   fghijklm  nopqrstu
00a0  76 77 78 79 7a 7b 7c 7d  7e 7f 80 81 82 83 84 85   vwxyz{|}  ~·······
00b0  86 87 88 89 8a 8b 8c 8d  8e 8f 90 91 92 93 94 95   ········  ········
```

Hypertext Transfer Protocol: Protocol | Packets: 3 · Displayed: 3 (100.0%) | Profile: Default

Fig11:packet details for pane segment

To see the traffic flow, the flow graph option in statistics is then needed to select.

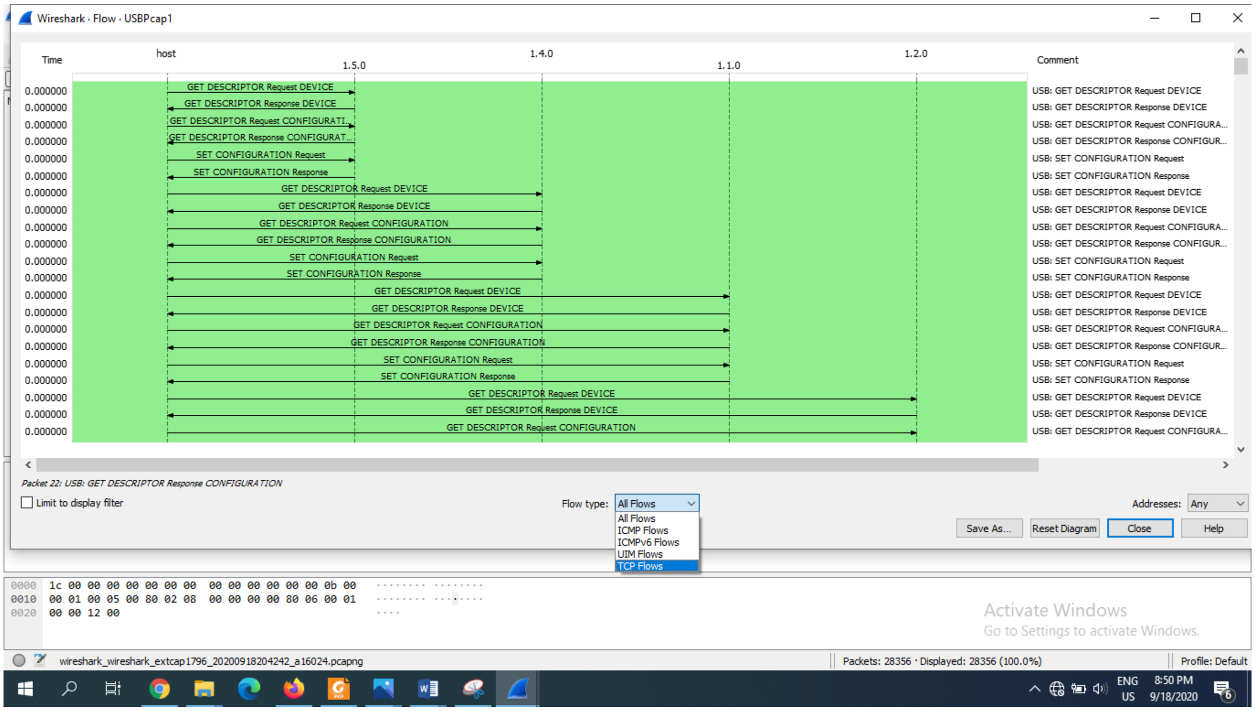


```
No.      Time          Source        Info
   25309 253.412335    1.5.1       3 URB_INTERRUPT in
   25310 253.412382    host        7 URB_INTERRUPT in
   25311 253.420449    1.5.1       3 URB_INTERRUPT in
   25312 253.420490    host        7 URB_INTERRUPT in
   25313 253.428380    1.5.1       3 URB_INTERRUPT in
   25314 253.428448    host        7 URB_INTERRUPT in
   25315 253.436445    1.5.1       3 URB_INTERRUPT in
   25316 253.436487    host        7 URB_INTERRUPT in
   25317 253.444291    1.5.1       3 URB_INTERRUPT in
   25318 253.444365    host        7 URB_INTERRUPT in
   25319 253.452419    1.5.1       3 URB_INTERRUPT in
   25320 253.452472    host        7 URB_INTERRUPT in
   25321 253.796339    1.5.1       3 URB_INTERRUPT in
   25322 253.796449    host        7 URB_INTERRUPT in
   25323 253.804377    1.5.1       3 URB_INTERRUPT in
   25324 253.804486    host        7 URB_INTERRUPT in
   25325 253.812330    1.5.1       3 URB_INTERRUPT in
   25326 253.812440    host        7 URB_INTERRUPT in
   25327 253.820379    1.5.1       3 URB_INTERRUPT in
   25328 253.820488    host        7 URB_INTERRUPT in
   25329 253.828312    1.5.1       3 URB_INTERRUPT in
   25330 253.828422    host        7 URB_INTERRUPT in
```

```
> Frame 1: 36 bytes on wire (288 bi          face wireshark extcap1796, id 0
0000  1c 00 00 00 00 00 00 00  00 00
0010  00 01 00 05 00 80 02 08  00 00
0020  00 00 12 00
```

USBPcap1: <live capture in progress> | Packets: 25330 · Displayed: 25330 (100.0%) | Profile: Default

Then the TCP flow is changed from all flow.



Wireshark · Flow · USBPcap1

```
Time      host          1.5.0          1.4.0          1.1.0          1.2.0      Comment
0.000000  GET DESCRIPTOR Request DEVICE                                          USB: GET DESCRIPTOR Request DEVICE
0.000000  GET DESCRIPTOR Response DEVICE                                         USB: GET DESCRIPTOR Response DEVICE
0.000000  GET DESCRIPTOR Request CONFIGURATI...                                  USB: GET DESCRIPTOR Request CONFIGURA...
0.000000  GET DESCRIPTOR Response CONFIGURAT...                                  USB: GET DESCRIPTOR Response CONFIGUR...
0.000000  SET CONFIGURATION Request                                              USB: SET CONFIGURATION Request
0.000000  SET CONFIGURATION Response                                             USB: SET CONFIGURATION Response
0.000000  GET DESCRIPTOR Request DEVICE                                          USB: GET DESCRIPTOR Request DEVICE
0.000000  GET DESCRIPTOR Response DEVICE                                         USB: GET DESCRIPTOR Response DEVICE
0.000000  GET DESCRIPTOR Request CONFIGURATION                                   USB: GET DESCRIPTOR Request CONFIGURA...
0.000000  GET DESCRIPTOR Response CONFIGURATION                                  USB: GET DESCRIPTOR Response CONFIGUR...
0.000000  SET CONFIGURATION Request                                              USB: SET CONFIGURATION Request
0.000000  SET CONFIGURATION Response                                             USB: SET CONFIGURATION Response
0.000000  GET DESCRIPTOR Request DEVICE                                          USB: GET DESCRIPTOR Request DEVICE
0.000000  GET DESCRIPTOR Response DEVICE                                         USB: GET DESCRIPTOR Response DEVICE
0.000000  GET DESCRIPTOR Request CONFIGURATION                                   USB: GET DESCRIPTOR Request CONFIGURA...
0.000000  GET DESCRIPTOR Response CONFIGURATION                                  USB: GET DESCRIPTOR Response CONFIGUR...
0.000000  SET CONFIGURATION Request                                              USB: SET CONFIGURATION Request
0.000000  SET CONFIGURATION Response                                             USB: SET CONFIGURATION Response
0.000000  GET DESCRIPTOR Request DEVICE                                          USB: GET DESCRIPTOR Request DEVICE
0.000000  GET DESCRIPTOR Response DEVICE                                         USB: GET DESCRIPTOR Response DEVICE
0.000000  GET DESCRIPTOR Request CONFIGURATION                                   USB: GET DESCRIPTOR Request CONFIGURA...
```

Packet 22: USB: GET DESCRIPTOR Response CONFIGURATION

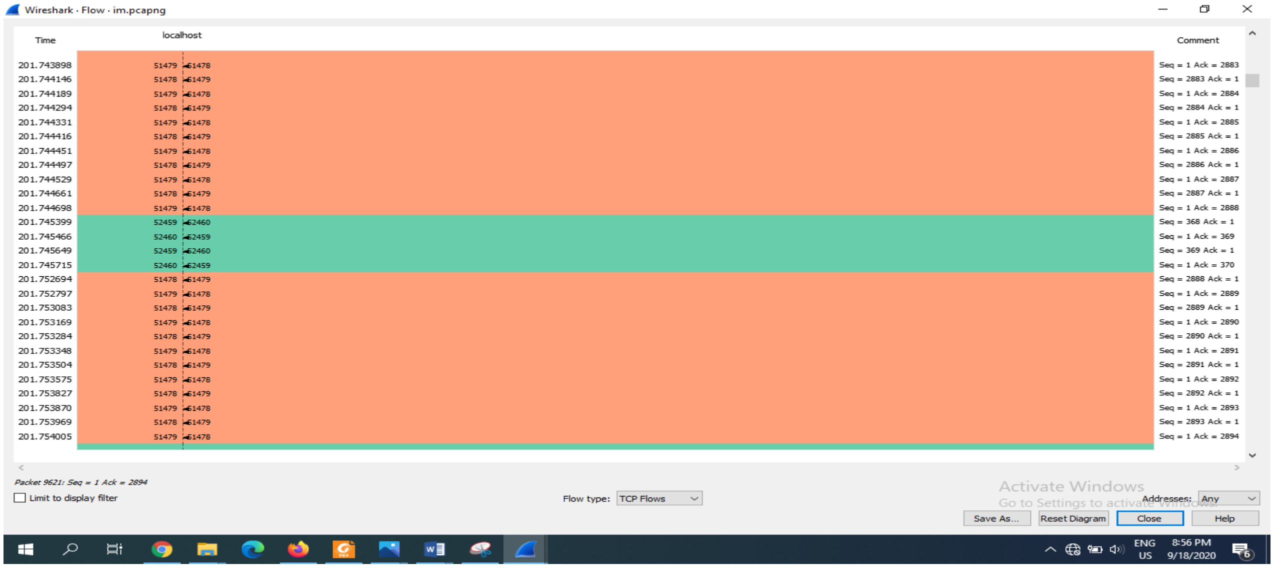
□ Limit to display filter

Flow type: All Flows

```
0000  1c 00 00 00 00 00 00 00  00 00 00 00 00 00 0b 00   ........ ........
0010  00 01 00 05 00 80 02 08  00 00 00 00 80 06 00 01   ........ ........
0020  00 00 12 00                                        ....
```

wireshark_wireshark_extcap1796_20200918204242_a16024.pcapng | Packets: 28356 · Displayed: 28356 (100.0%) | Profile: Default

The TCP flows are



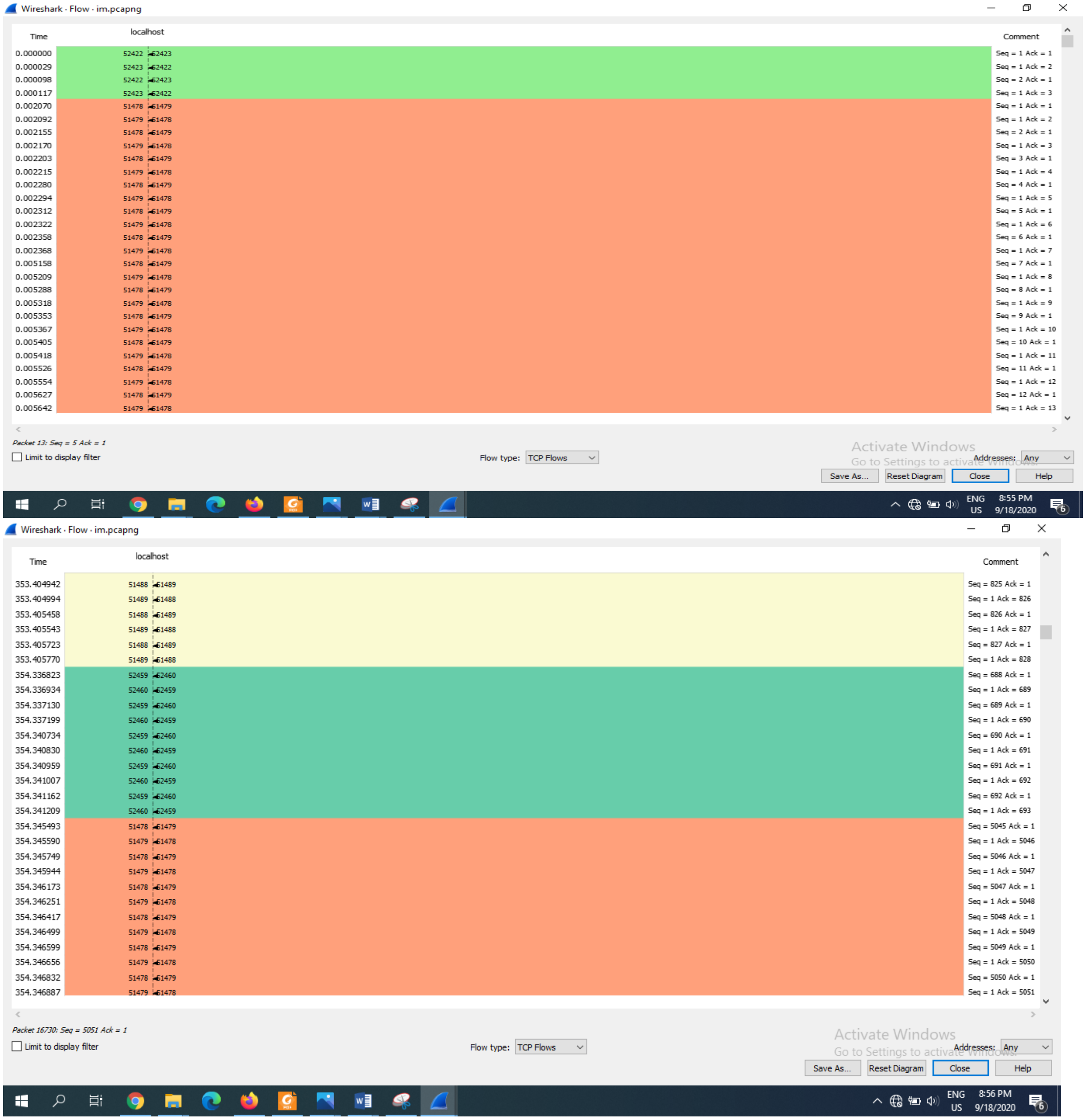
Wireshark · Flow · im.pcapng

```
Time        localhost            Comment
201.743898  51479  61478         Seq = 1 Ack = 2883
201.744146  51478  61479         Seq = 2883 Ack = 1
201.744189  51479  61478         Seq = 1 Ack = 2884
201.744294  51478  61479         Seq = 2884 Ack = 1
201.744331  51479  61478         Seq = 1 Ack = 2885
201.744416  51478  61479         Seq = 2885 Ack = 1
201.744451  51479  61478         Seq = 1 Ack = 2886
201.744497  51478  61479         Seq = 2886 Ack = 1
201.744529  51479  61478         Seq = 1 Ack = 2887
201.744661  51478  61479         Seq = 2887 Ack = 1
201.744698  51479  61478         Seq = 1 Ack = 2888
201.745399  52459  62460         Seq = 368 Ack = 1
201.745466  52460  62459         Seq = 1 Ack = 369
201.745649  52459  62460         Seq = 369 Ack = 1
201.745715  52460  62459         Seq = 1 Ack = 370
201.752694  51478  61479         Seq = 2888 Ack = 1
201.752797  51479  61478         Seq = 1 Ack = 2889
201.753083  51478  61479         Seq = 2889 Ack = 1
201.753169  51479  61478         Seq = 1 Ack = 2890
201.753284  51478  61479         Seq = 2890 Ack = 1
201.753348  51479  61478         Seq = 1 Ack = 2891
201.753504  51478  61479         Seq = 2891 Ack = 1
201.753575  51479  61478         Seq = 1 Ack = 2892
201.753827  51478  61479         Seq = 2892 Ack = 1
201.753870  51479  61478         Seq = 1 Ack = 2893
201.753969  51478  61479         Seq = 2893 Ack = 1
201.754005  51479  61478         Seq = 1 Ack = 2894
```

Packet 9621: Seq = 1 Ack = 2894

□ Limit to display filter

Flow type: TCP Flows



Time	localhost		Comment
0.000000	52422	52423	Seq = 1 Ack = 1
0.000029	52423	52422	Seq = 1 Ack = 2
0.000098	52422	52423	Seq = 2 Ack = 1
0.000117	52423	52422	Seq = 1 Ack = 3
0.002070	51478	51479	Seq = 1 Ack = 1
0.002092	51479	51478	Seq = 1 Ack = 2
0.002155	51478	51479	Seq = 2 Ack = 1
0.002170	51479	51478	Seq = 1 Ack = 3
0.002203	51478	51479	Seq = 3 Ack = 1
0.002215	51479	51478	Seq = 1 Ack = 4
0.002280	51478	51479	Seq = 4 Ack = 1
0.002294	51479	51478	Seq = 1 Ack = 5
0.002312	51478	51479	Seq = 5 Ack = 1
0.002322	51479	51478	Seq = 1 Ack = 6
0.002358	51478	51479	Seq = 6 Ack = 1
0.002368	51479	51478	Seq = 1 Ack = 7
0.005158	51478	51479	Seq = 7 Ack = 1
0.005209	51479	51478	Seq = 1 Ack = 8
0.005288	51478	51479	Seq = 8 Ack = 1
0.005318	51479	51478	Seq = 1 Ack = 9
0.005353	51478	51479	Seq = 9 Ack = 1
0.005367	51479	51478	Seq = 1 Ack = 10
0.005405	51478	51479	Seq = 10 Ack = 1
0.005418	51479	51478	Seq = 1 Ack = 11
0.005526	51478	51479	Seq = 11 Ack = 1
0.005554	51479	51478	Seq = 1 Ack = 12
0.005627	51478	51479	Seq = 12 Ack = 1
0.005642	51479	51478	Seq = 1 Ack = 13

Packet 13: Seq = 5 Ack = 1

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any

Time	localhost		Comment
353.404942	51488	51489	Seq = 825 Ack = 1
353.404994	51489	51488	Seq = 1 Ack = 826
353.405458	51488	51489	Seq = 826 Ack = 1
353.405543	51489	51488	Seq = 1 Ack = 827
353.405723	51488	51489	Seq = 827 Ack = 1
353.405770	51489	51488	Seq = 1 Ack = 828
354.336823	52459	52460	Seq = 688 Ack = 1
354.336934	52460	52459	Seq = 1 Ack = 689
354.337130	52459	52460	Seq = 689 Ack = 1
354.337199	52460	52459	Seq = 1 Ack = 690
354.340734	52459	52460	Seq = 690 Ack = 1
354.340830	52460	52459	Seq = 1 Ack = 691
354.340959	52459	52460	Seq = 691 Ack = 1
354.341007	52460	52459	Seq = 1 Ack = 692
354.341162	52459	52460	Seq = 692 Ack = 1
354.341209	52460	52459	Seq = 1 Ack = 693
354.345493	51478	51479	Seq = 5045 Ack = 1
354.345590	51479	51478	Seq = 1 Ack = 5046
354.345749	51478	51479	Seq = 5046 Ack = 1
354.345944	51479	51478	Seq = 1 Ack = 5047
354.346173	51478	51479	Seq = 5047 Ack = 1
354.346251	51479	51478	Seq = 1 Ack = 5048
354.346417	51478	51479	Seq = 5048 Ack = 1
354.346499	51479	51478	Seq = 1 Ack = 5049
354.346599	51478	51479	Seq = 5049 Ack = 1
354.346656	51479	51478	Seq = 1 Ack = 5050
354.346832	51478	51479	Seq = 5050 Ack = 1
354.346887	51479	51478	Seq = 1 Ack = 5051

Packet 16730: Seq = 5051 Ack = 1

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any

Fig12: Graph of TCP flow statistics

Discussion: This lab, required some steps to be followed after installing the free software wireshark. Which is a traffic analyzer tool.Through the steps the capturing and analysis of traffic was done.After the capture the traffic flow was also elaborated.