Ain Shams University
Faculty of Engineering

4th CSE Computer Networks

Project documentation

Names:

Ahmed Hawaf Abd El-Hakim	Section: 1
Amr Essam Mohamed Barakat	Section: 2
Mohamed Ossama Abu Al-Hassan	Section: 3
Mohamed Hatem Sayed	Section: 3

Submitted to:
Dr. Ayman Bahaa
Eng. Aly Osama

Table of Contents

Overview 3

User manual 4

Code Notes .... **Error! Bookmark not defined.**

Overview

This project is an application that sniffs packets sent and received by your device. It supports both Windows and Unix platforms.

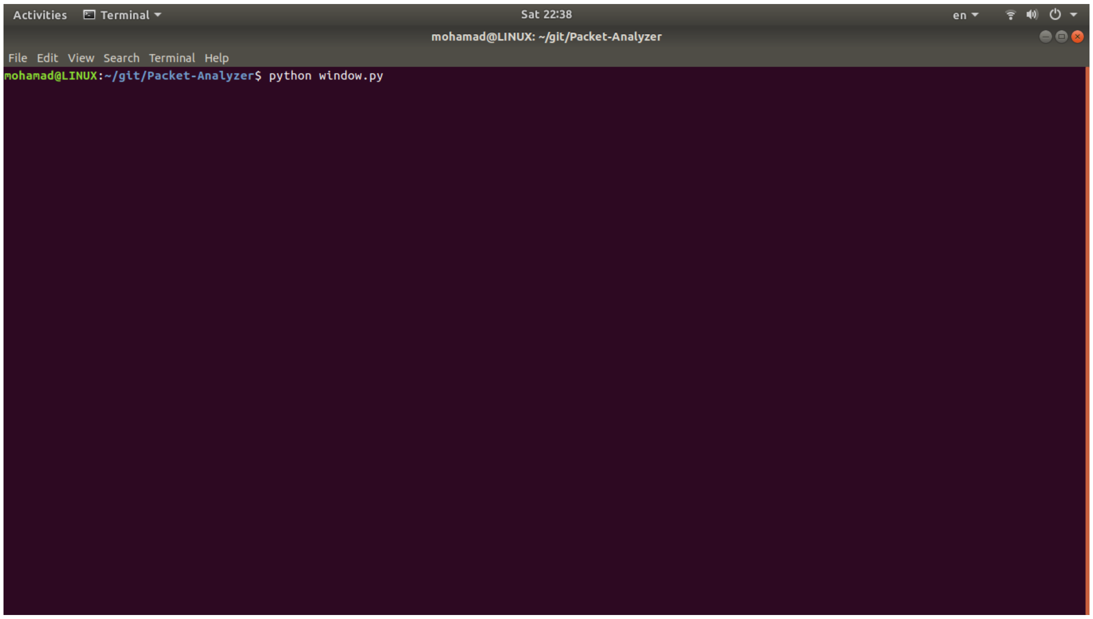
Inside the GUI you can choose an interface to sniff on (e.g. Wireless or Ethernet). On clicking the packet, you will have more details about, that will be described later.

This project is implemented using Python 2.7 and PyQt 4.0, so you’ll have to install both before running this application.

User manual

In this section we’ll show how to use this application’s features.

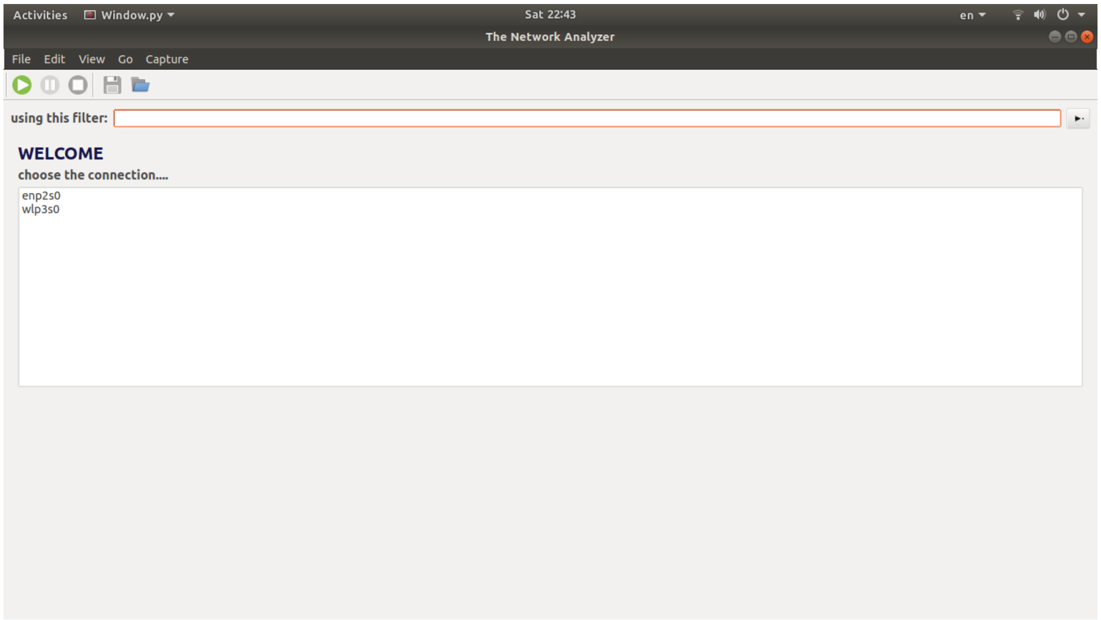
1. Run window.py file using an appropriate way. For example, run it through CLI of UNIX as following.


Activities
Terminal
Sat 22:38
en
mohamad@LINUX: ~/git/Packet-Analyzer
File Edit View Search Terminal Help

```
mohamad@LINUX:~/git/Packet-Analyzer$ python window.py
```

It should be noted that you may need to run the python file using sudo.

2. A window will appear that shows the available interfaces that you can sniff on.



using this filter:

WELCOME

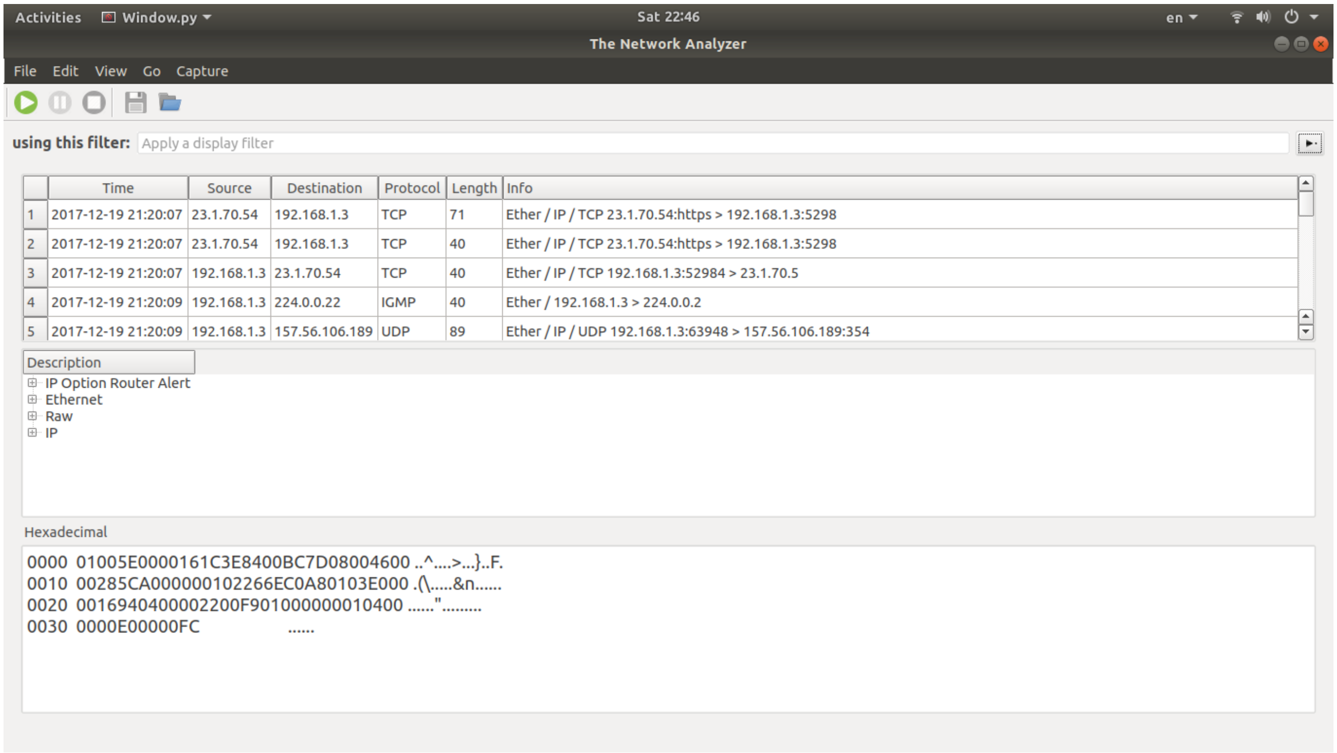
choose the connection....

```
enp2s0
wlp3s0
```

3. Choose an interface then hit the green start button at the top of the window.

4. Packets sent and received will be shown hit the stop button to stop sniffing.

5. A window like the following will appear showing packets and details about it like source, destination, length, protocol and time.



	Time	Source	Destination	Protocol	Length	Info
1	2017-12-19 21:20:07	23.1.70.54	192.168.1.3	TCP	71	Ether / IP / TCP 23.1.70.54:https > 192.168.1.3:5298
2	2017-12-19 21:20:07	23.1.70.54	192.168.1.3	TCP	40	Ether / IP / TCP 23.1.70.54:https > 192.168.1.3:5298
3	2017-12-19 21:20:07	192.168.1.3	23.1.70.54	TCP	40	Ether / IP / TCP 192.168.1.3:52984 > 23.1.70.5
4	2017-12-19 21:20:09	192.168.1.3	224.0.0.22	IGMP	40	Ether / 192.168.1.3 > 224.0.0.2
5	2017-12-19 21:20:09	192.168.1.3	157.56.106.189	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.189:354

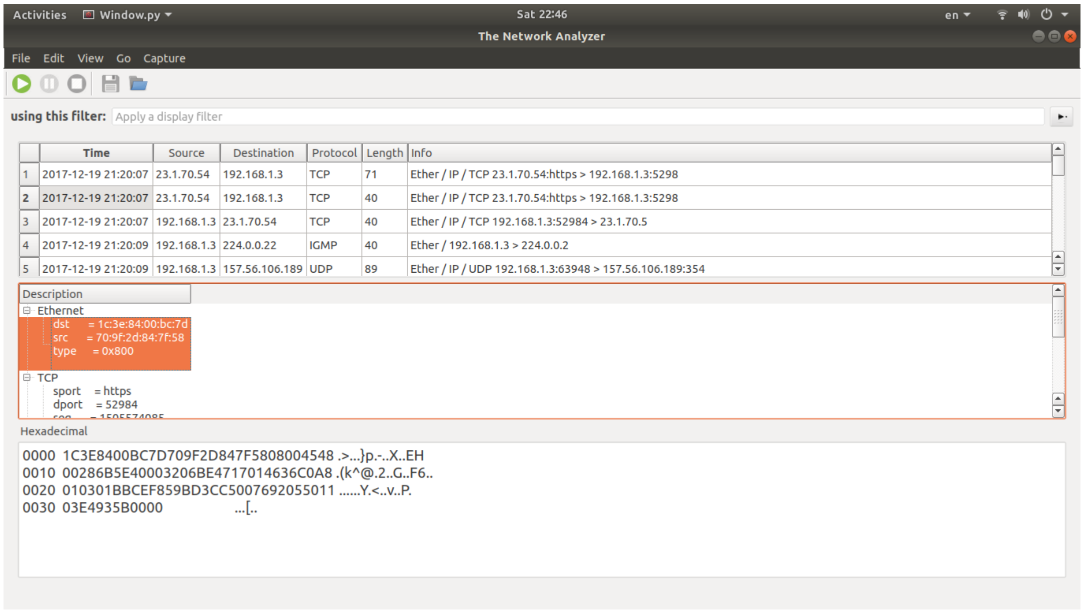
Description

⊞ IP Option Router Alert
⊞ Ethernet
⊞ Raw
⊞ IP

Hexadecimal

```
0000  01005E0000161C3E8400BC7D08004600 ..^....>...}..F.
0010  00285CA000000102266EC0A80103E000 .(\.....&n......
0020  0016940400002200F901000000010400 ......".........
0030  0000E00000FC                ......
```

6. The previous window shows more details about any selected packet. To show these details all you need to do is to click on the packet and expand the fields shown in the second field to view these details.



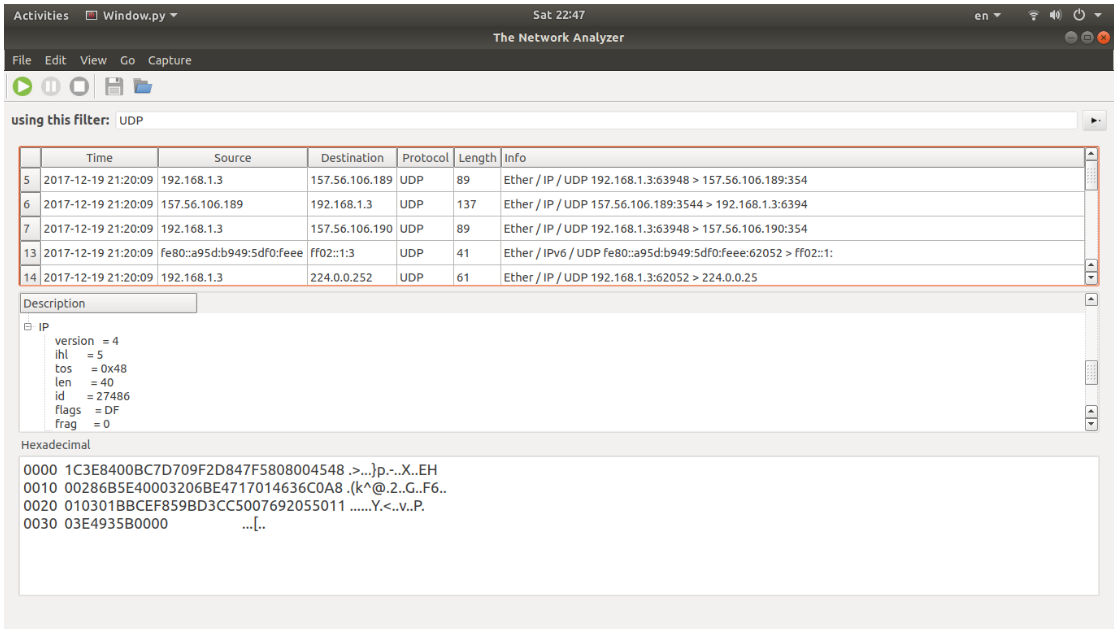
using this filter: Apply a display filter

	Time	Source	Destination	Protocol	Length	Info
1	2017-12-19 21:20:07	23.1.70.54	192.168.1.3	TCP	71	Ether / IP / TCP 23.1.70.54:https > 192.168.1.3:5298
2	2017-12-19 21:20:07	23.1.70.54	192.168.1.3	TCP	40	Ether / IP / TCP 23.1.70.54:https > 192.168.1.3:5298
3	2017-12-19 21:20:07	192.168.1.3	23.1.70.54	TCP	40	Ether / IP / TCP 192.168.1.3:52984 > 23.1.70.5
4	2017-12-19 21:20:09	192.168.1.3	224.0.0.22	IGMP	40	Ether / 192.168.1.3 > 224.0.0.2
5	2017-12-19 21:20:09	192.168.1.3	157.56.106.189	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.189:354

```
Description
⊟ Ethernet
    dst    = 1c:3e:84:00:bc:7d
    src    = 70:9f:2d:84:7f:58
    type   = 0x800
⊟ TCP
    sport  = https
    dport  = 52984
```

Hexadecimal

```
0000  1C3E8400BC7D709F2D847F5808004548 .>...}p.-..X..EH
0010  00286B5E40003206BE4717014636C0A8 .(k^@.2..G..F6..
0020  010301BBCEF859BD3CC5007692055011 ......Y.<..v..P.
0030  03E4935B0000                     ...[..
```



using this filter: UDP

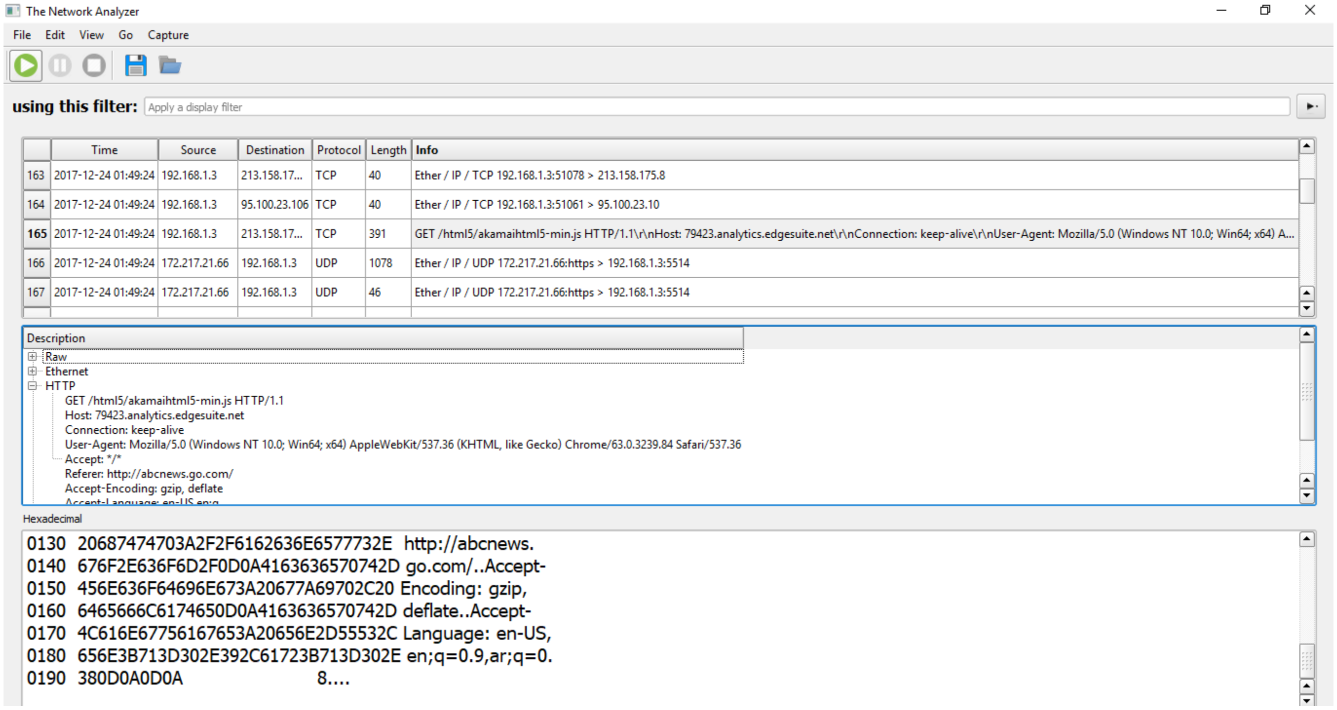
	Time	Source	Destination	Protocol	Length	Info
5	2017-12-19 21:20:09	192.168.1.3	157.56.106.189	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.189:354
6	2017-12-19 21:20:09	157.56.106.189	192.168.1.3	UDP	137	Ether / IP / UDP 157.56.106.189:3544 > 192.168.1.3:6394
7	2017-12-19 21:20:09	192.168.1.3	157.56.106.190	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.190:354
13	2017-12-19 21:20:09	fe80::a95d:b949:5df0:feee	ff02::1:3	UDP	41	Ether / IPv6 / UDP fe80::a95d:b949:5df0:feee:62052 > ff02::1:
14	2017-12-19 21:20:09	192.168.1.3	224.0.0.252	UDP	61	Ether / IP / UDP 192.168.1.3:62052 > 224.0.0.25

```
Description
⊟ IP
    version  = 4
    ihl      = 5
    tos      = 0x48
    len      = 40
    id       = 27486
    flags    = DF
    frag     = 0
```

Hexadecimal

```
0000  1C3E8400BC7D709F2D847F5808004548 .>...}p.-..X..EH
0010  00286B5E40003206BE4717014636C0A8 .(k^@.2..G..F6..
0020  010301BBCEF859BD3CC5007692055011 ......Y.<..v..P.
0030  03E4935B0000                     ...[..
```

Another Example of showing the details of an Http packet is shown below



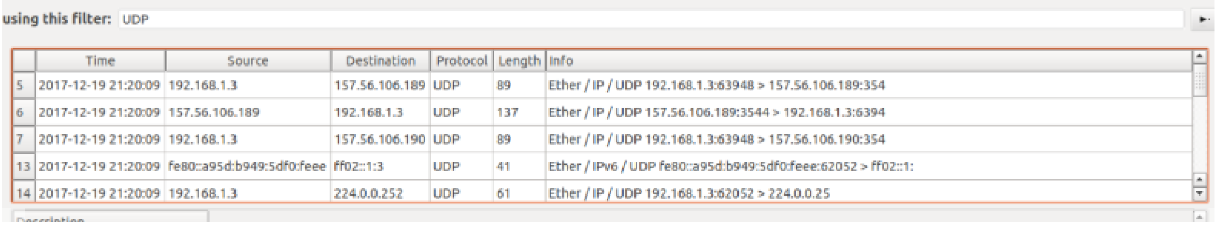
using this filter: Apply a display filter

	Time	Source	Destination	Protocol	Length	Info
163	2017-12-24 01:49:24	192.168.1.3	213.158.17...	TCP	40	Ether / IP / TCP 192.168.1.3:51078 > 213.158.175.8
164	2017-12-24 01:49:24	192.168.1.3	95.100.23.106	TCP	40	Ether / IP / TCP 192.168.1.3:51061 > 95.100.23.10
165	2017-12-24 01:49:24	192.168.1.3	213.158.17...	TCP	391	GET /html5/akamaihtml5-min.js HTTP/1.1\r\nHost: 79423.analytics.edgesuite.net\r\nConnection: keep-alive\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...
166	2017-12-24 01:49:24	172.217.21.66	192.168.1.3	UDP	1078	Ether / IP / UDP 172.217.21.66:https > 192.168.1.3:5514
167	2017-12-24 01:49:24	172.217.21.66	192.168.1.3	UDP	46	Ether / IP / UDP 172.217.21.66:https > 192.168.1.3:5514

```
Description
⊞ Raw
⊞ Ethernet
⊟ HTTP
    GET /html5/akamaihtml5-min.js HTTP/1.1
    Host: 79423.analytics.edgesuite.net
    Connection: keep-alive
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36
    Accept: */*
    Referer: http://abcnews.go.com/
    Accept-Encoding: gzip, deflate
    Accept-Language: en-US,en;q
```

```
Hexadecimal
0130  20687474703A2F2F6162636E6577732E  http://abcnews.
0140  676F2E636F6D2F0D0A4163636570742D go.com/..Accept-
0150  456E636F64696E673A20677A69702C20 Encoding: gzip,
0160  6465666C6174650D0A4163636570742D deflate..Accept-
0170  4C616E67756167653A20656E2D55532C Language: en-US,
0180  656E3B713D302E392C61723B713D302E en;q=0.9,ar;q=0.
0190  380D0A0D0A                       8....
```

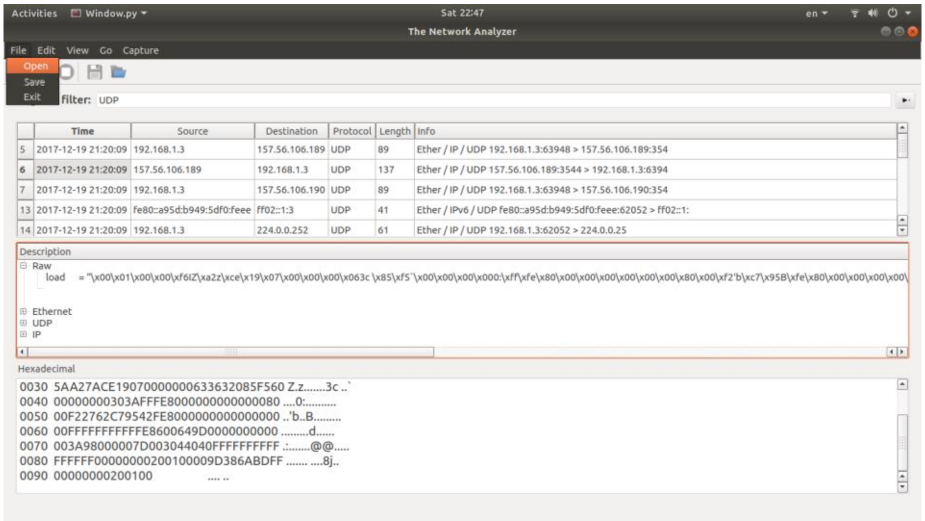
7. You can also apply a filter by entering the filtering value in the text box and press the button on the right to show the packets after applying this filter.



using this filter: UDP

	Time	Source	Destination	Protocol	Length	Info
5	2017-12-19 21:20:09	192.168.1.3	157.56.106.189	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.189:354
6	2017-12-19 21:20:09	157.56.106.189	192.168.1.3	UDP	137	Ether / IP / UDP 157.56.106.189:3544 > 192.168.1.3:6394
7	2017-12-19 21:20:09	192.168.1.3	157.56.106.190	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.190:354
13	2017-12-19 21:20:09	fe80::a95d:b949:5df0:feee	ff02::1:3	UDP	41	Ether / IPv6 / UDP fe80::a95d:b949:5df0:feee:62052 > ff02::1:
14	2017-12-19 21:20:09	192.168.1.3	224.0.0.252	UDP	61	Ether / IP / UDP 192.168.1.3:62052 > 224.0.0.25

8. To save or load packets details: press the file button and select save. Then you will be directed to a window to browse the save or load location for this file as shown.



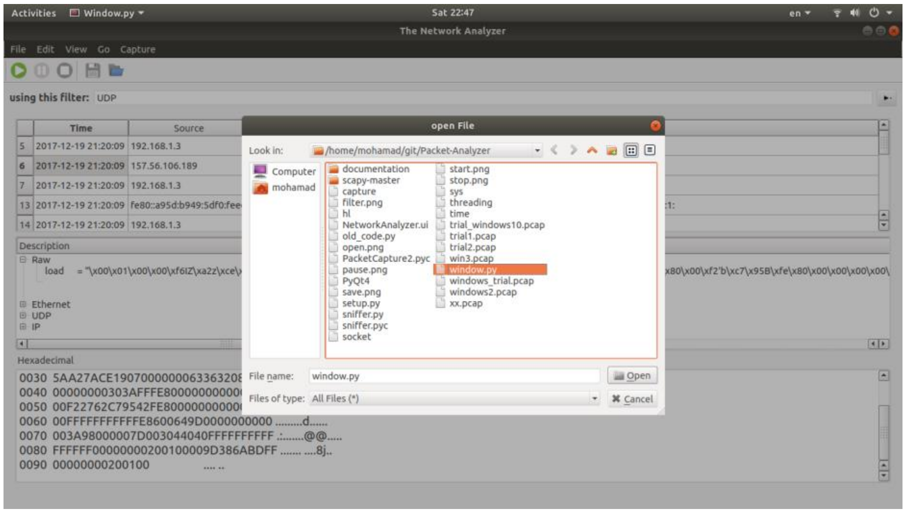
filter: UDP

	Time	Source	Destination	Protocol	Length	Info
5	2017-12-19 21:20:09	192.168.1.3	157.56.106.189	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.189:354
6	2017-12-19 21:20:09	157.56.106.189	192.168.1.3	UDP	137	Ether / IP / UDP 157.56.106.189:3544 > 192.168.1.3:6394
7	2017-12-19 21:20:09	192.168.1.3	157.56.106.190	UDP	89	Ether / IP / UDP 192.168.1.3:63948 > 157.56.106.190:354
13	2017-12-19 21:20:09	fe80::a95d:b949:5df0:feee	ff02::1:3	UDP	41	Ether / IPv6 / UDP fe80::a95d:b949:5df0:feee:62052 > ff02::1:
14	2017-12-19 21:20:09	192.168.1.3	224.0.0.252	UDP	61	Ether / IP / UDP 192.168.1.3:62052 > 224.0.0.25

```
Description
⊟ Raw
    load    = "\x00\x01\x00\x00\xf6lZ\xa2z\xce\x19\x07\x00\x00\x00\x063c \x85\xf5`\x00\x00\x00\x000:\xff\xfe\x80\x00\x00\x00\x00\x00\x00\x80\x00\xf2'b\xc7\x95B\xfe\x80\x00\x00\x00\x00\

⊞ Ethernet
⊞ UDP
⊞ IP
```

```
Hexadecimal
0030  5AA27ACE19070000000633632085F560 Z.z.......3c ..`
0040  00000000303AFFFE8000000000000080 ....0:..........
0050  00F22762C79542FE8000000000000000 ..'b..B.........
0060  00FFFFFFFFFFFE8600649D0000000000 .........d......
0070  003A98000007D003044040FFFFFFFFFF .:........@@.....
0080  FFFFFF00000000200100009D386ABDFF ....... ....8j..
0090  00000000200100              .... ..
```



using this filter: UDP

	Time	Source
5	2017-12-19 21:20:09	192.168.1.3
6	2017-12-19 21:20:09	157.56.106.189
7	2017-12-19 21:20:09	192.168.1.3
13	2017-12-19 21:20:09	fe80::a95d:b949:5df0:fee
14	2017-12-19 21:20:09	192.168.1.3

Description

```
Raw
    load    = "\x00\x01\x00\x00\xf6IZ\xa2z\xce\x    x80\x00\xf2'b\xc7\x95B\xfe\x80\x00\x00\x00\x00\
```

Look in: /home/mohamad/git/Packet-Analyzer

File name: window.py

Files of type: All Files (*)

Hexadecimal

```
0030  5AA27ACE19070000000063363208
0040  00000000303AFFFE8000000000000
0050  00F22762C79542FE80000000000
0060  00FFFFFFFFFFFE8600649D0000000000 .........d......
0070  003A98000007D003044040FFFFFFFFFF .:........@@.....
0080  FFFFFF0000000200100009D386ABDFF ....... ....8j..
0090  00000000200100                   .... ..
```

Implementation and Features Notes

- The code relies on a python library called Scapy , but this library don't handle http so it was handled by modifying the code in Scapy library and parsing the output.
- The GUI is made using PyQt4 and the used python version is python 2.7
- The GUI runs in the main thread and the sniffing (Background process) runs in another thread that sniffs using the Scapy library.
- The using of Scapy is abstracted by a class called Sniffer that handles and parse all the output from the Scapy library and passes it to the GUI.
- You can save and load file in pcap extention and it was tested on wireshark.
- The length column specifies the Packet length.
- You can apply filter to any column.
- All types of packets are sniffed, some of them were handled manually by parsing the output of Scapy such as Http and IPv6.