جامعة عين شمس

كلية الهندسة

CSE335 : Computer Networks Mini-Wireshark Project

Team members:

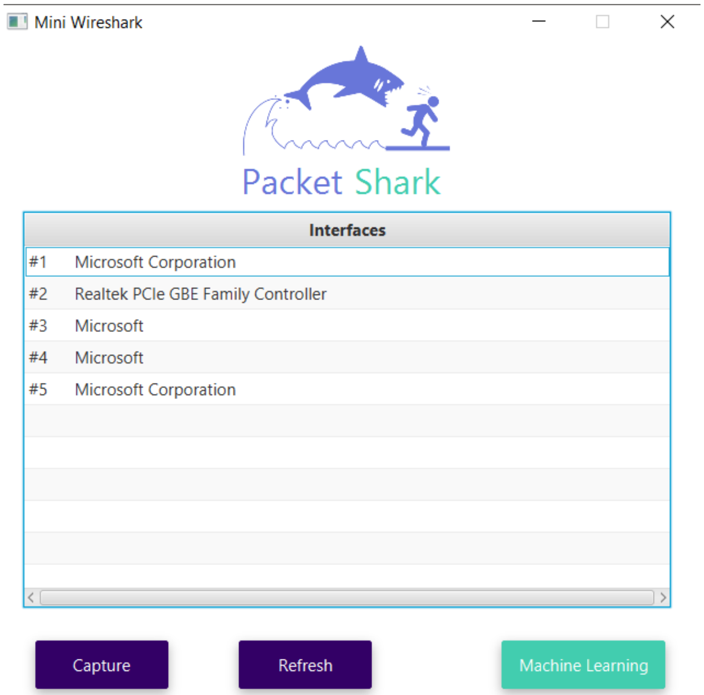
Ahmed Salah Abdel-Hakim	14p3069
Mohamed Mostafa Amin	14p6087
Mohamed Mostafa El Tair	14p1087
Mohamed Wagih Ahmed	14p6080

DESCRIPTION , FEATURES & SCREENSHOTS

Mini-wireshark is an open source packet analyzer , after running the file called "mwshark.jar" a small window will appear showing all the available network cards devices on your machine.

Source code link :

https://github.com/mohamedeltair/5061636b657420536e6966666572

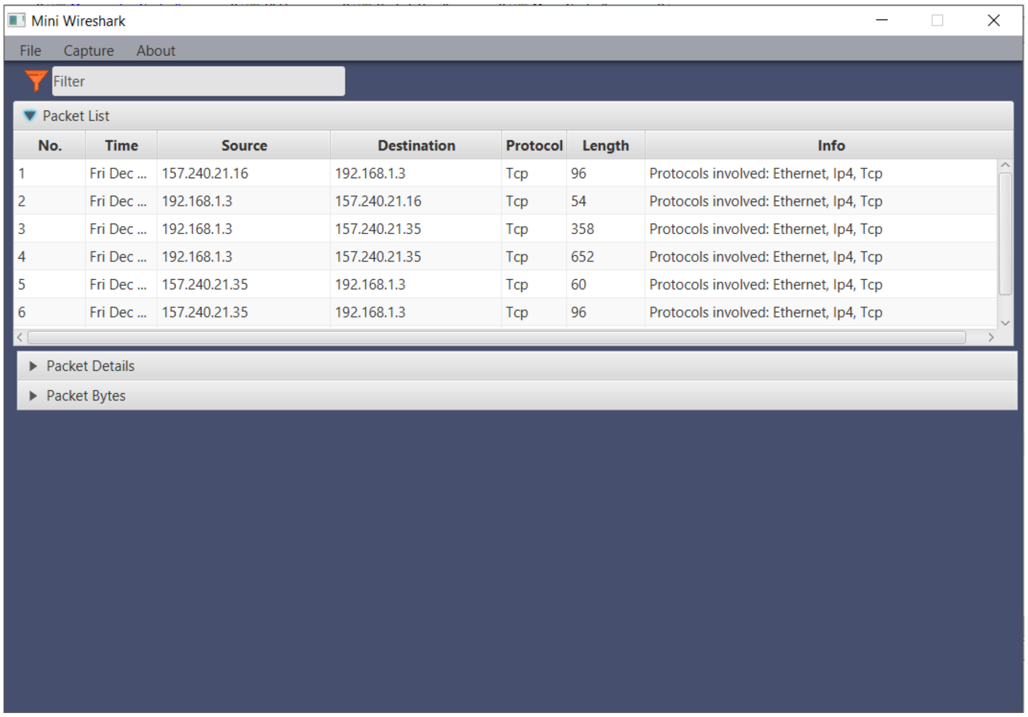


	Interfaces
#1	Microsoft Corporation
#2	Realtek PCIe GBE Family Controller
#3	Microsoft
#4	Microsoft
#5	Microsoft Corporation

You can select a device from the list then click capture or click refresh if nothing is displayed or go to the machine learning section.

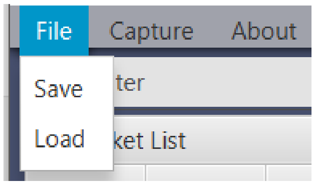
PART A | CAPTURING AND ANALYZING PACKETS

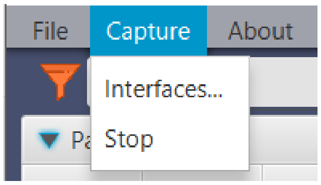
After selecting the preferred device another window will show up displaying 5 sections.

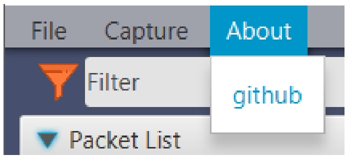


No.	Time	Source	Destination	Protocol	Length	Info
1	Fri Dec ...	157.240.21.16	192.168.1.3	Tcp	96	Protocols involved: Ethernet, Ip4, Tcp
2	Fri Dec ...	192.168.1.3	157.240.21.16	Tcp	54	Protocols involved: Ethernet, Ip4, Tcp
3	Fri Dec ...	192.168.1.3	157.240.21.35	Tcp	358	Protocols involved: Ethernet, Ip4, Tcp
4	Fri Dec ...	192.168.1.3	157.240.21.35	Tcp	652	Protocols involved: Ethernet, Ip4, Tcp
5	Fri Dec ...	157.240.21.35	192.168.1.3	Tcp	60	Protocols involved: Ethernet, Ip4, Tcp
6	Fri Dec ...	157.240.21.35	192.168.1.3	Tcp	96	Protocols involved: Ethernet, Ip4, Tcp

Section #1 Menu bar which contains File , Capture and About







a. File -> Save : You can save the current captured packets at the preferred location.

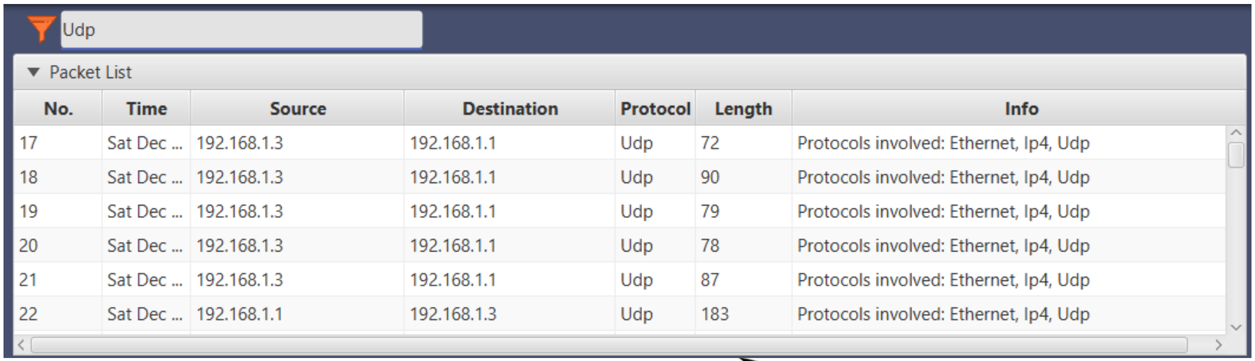
b. File -> Load : You can load a pcap file to the program.

c. Capture -> Interfaces... :You can select a new device from the interfaces list.

d. Capture -> Stop : Stop capturing packets.

e. About -> github : A hyperlink to the project's contributors on github.

Section #2 Filter , You can organize the table based on what protocol you want to display only (example Udp) or any other standard protocol of your choice.

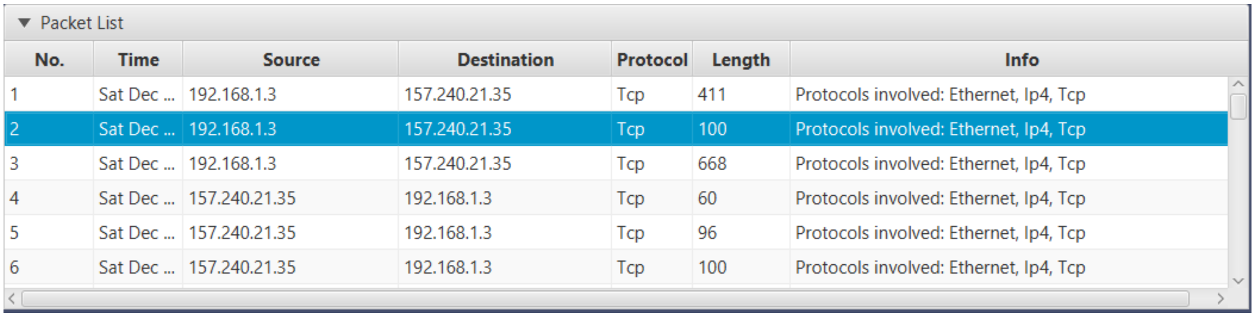

Udp

Packet List

No.	Time	Source	Destination	Protocol	Length	Info
17	Sat Dec ...	192.168.1.3	192.168.1.1	Udp	72	Protocols involved: Ethernet, Ip4, Udp
18	Sat Dec ...	192.168.1.3	192.168.1.1	Udp	90	Protocols involved: Ethernet, Ip4, Udp
19	Sat Dec ...	192.168.1.3	192.168.1.1	Udp	79	Protocols involved: Ethernet, Ip4, Udp
20	Sat Dec ...	192.168.1.3	192.168.1.1	Udp	78	Protocols involved: Ethernet, Ip4, Udp
21	Sat Dec ...	192.168.1.3	192.168.1.1	Udp	87	Protocols involved: Ethernet, Ip4, Udp
22	Sat Dec ...	192.168.1.1	192.168.1.3	Udp	183	Protocols involved: Ethernet, Ip4, Udp

Section #3 Packet List Pane which contains the table that displays all the captured packets in addition its number , time , source & destination IPs , protocol , length and additional information.

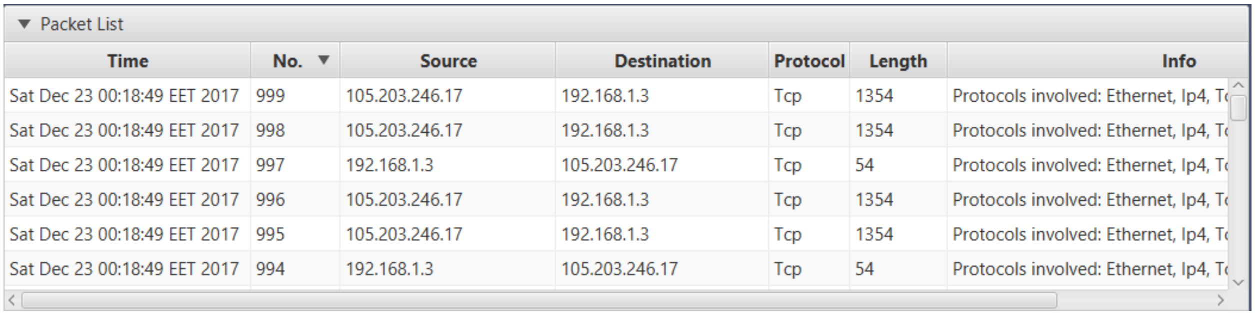
You can select any of the packets to display it's details and it's bytes form in the Packet Details and Packet Bytes Panes.


Packet List

No.	Time	Source	Destination	Protocol	Length	Info
1	Sat Dec ...	192.168.1.3	157.240.21.35	Tcp	411	Protocols involved: Ethernet, Ip4, Tcp
2	Sat Dec ...	192.168.1.3	157.240.21.35	Tcp	100	Protocols involved: Ethernet, Ip4, Tcp
3	Sat Dec ...	192.168.1.3	157.240.21.35	Tcp	668	Protocols involved: Ethernet, Ip4, Tcp
4	Sat Dec ...	157.240.21.35	192.168.1.3	Tcp	60	Protocols involved: Ethernet, Ip4, Tcp
5	Sat Dec ...	157.240.21.35	192.168.1.3	Tcp	96	Protocols involved: Ethernet, Ip4, Tcp
6	Sat Dec ...	157.240.21.35	192.168.1.3	Tcp	100	Protocols involved: Ethernet, Ip4, Tcp

NOTE We will use this packet for the rest of the documentation to display it in more details and forms.

You can also sort the table's columns in ascending or descending order or which column to be displayed first before the other.

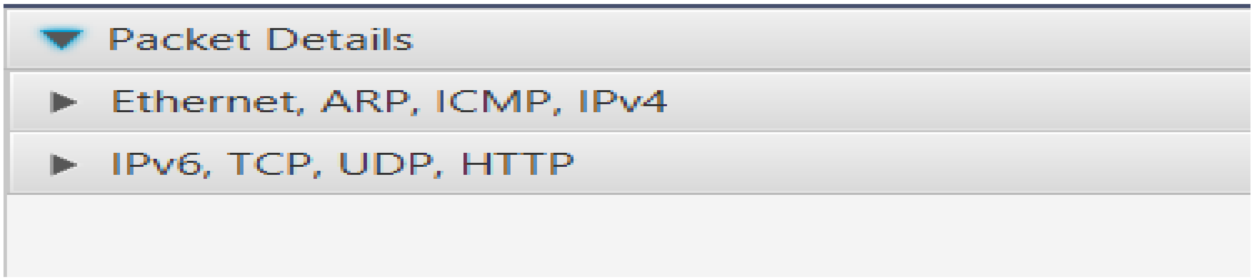


▼ Packet List

Time	No. ▼	Source	Destination	Protocol	Length	Info
Sat Dec 23 00:18:49 EET 2017	999	105.203.246.17	192.168.1.3	Tcp	1354	Protocols involved: Ethernet, Ip4, Tc
Sat Dec 23 00:18:49 EET 2017	998	105.203.246.17	192.168.1.3	Tcp	1354	Protocols involved: Ethernet, Ip4, Tc
Sat Dec 23 00:18:49 EET 2017	997	192.168.1.3	105.203.246.17	Tcp	54	Protocols involved: Ethernet, Ip4, Tc
Sat Dec 23 00:18:49 EET 2017	996	105.203.246.17	192.168.1.3	Tcp	1354	Protocols involved: Ethernet, Ip4, Tc
Sat Dec 23 00:18:49 EET 2017	995	105.203.246.17	192.168.1.3	Tcp	1354	Protocols involved: Ethernet, Ip4, Tc
Sat Dec 23 00:18:49 EET 2017	994	192.168.1.3	105.203.246.17	Tcp	54	Protocols involved: Ethernet, Ip4, Tc

Here I made the "No." column display packets in descending order of their capturing and the time column before the the "No." column.

Section #4 Packet Details Pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. The pane shows two accordions "Ethernet , ARP , ICMP , IPv4" and "IPv6 , TCP , UDP , HTTP" . if anyone of them exists it will show it's details otherwise you'll see a "protocol doesn't exist text"



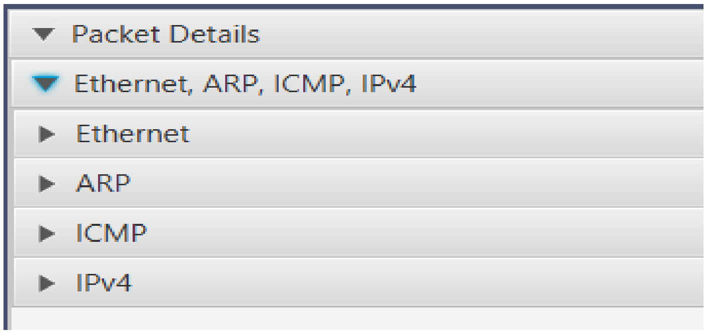
▼ Packet Details

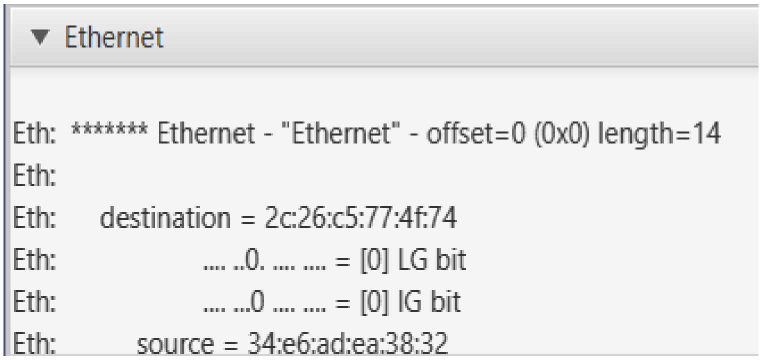
▶ Ethernet, ARP, ICMP, IPv4

▶ IPv6, TCP, UDP, HTTP

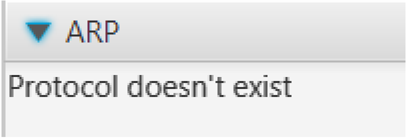
You can expand each one for more details.

The first accordion :

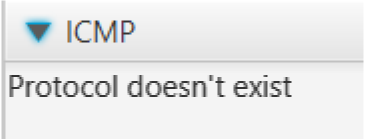




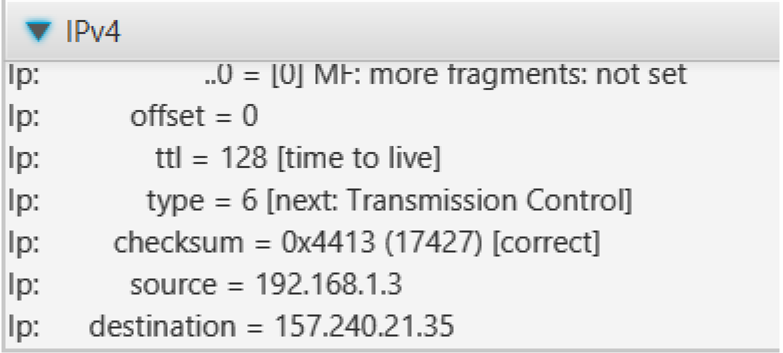
```
Eth:  ******* Ethernet - "Ethernet" - offset=0 (0x0) length=14
Eth:
Eth:     destination = 2c:26:c5:77:4f:74
Eth:                   .... ..0. .... .... = [0] LG bit
Eth:                   .... ...0 .... .... = [0] IG bit
Eth:          source = 34:e6:ad:ea:38:32
```



Protocol doesn't exist

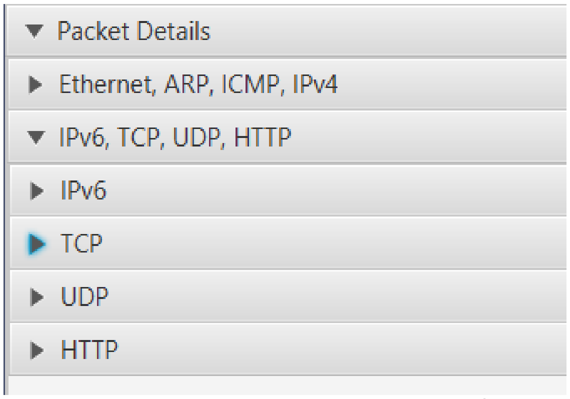


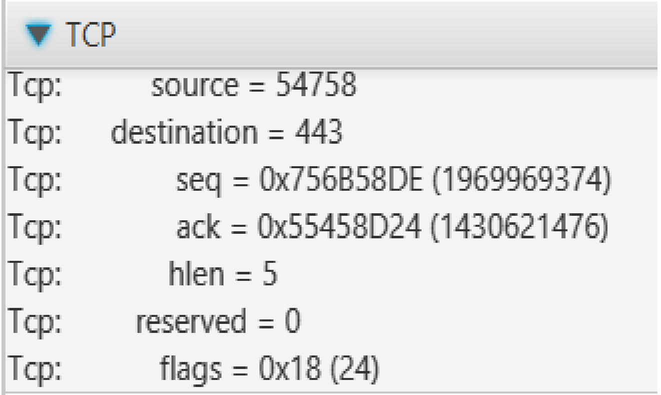
Protocol doesn't exist



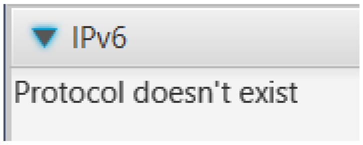
```
Ip:                   ..0 = [0] MF: more fragments: not set
Ip:         offset = 0
Ip:            ttl = 128 [time to live]
Ip:           type = 6 [next: Transmission Control]
Ip:       checksum = 0x4413 (17427) [correct]
Ip:         source = 192.168.1.3
Ip:    destination = 157.240.21.35
```

The second accordion :

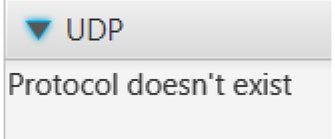




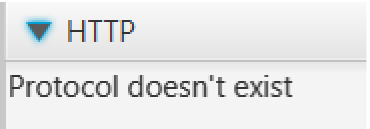
```
Tcp:          source = 54758
Tcp:     destination = 443
Tcp:             seq = 0x756B58DE (1969969374)
Tcp:             ack = 0x55458D24 (1430621476)
Tcp:            hlen = 5
Tcp:        reserved = 0
Tcp:           flags = 0x18 (24)
```



Protocol doesn't exist

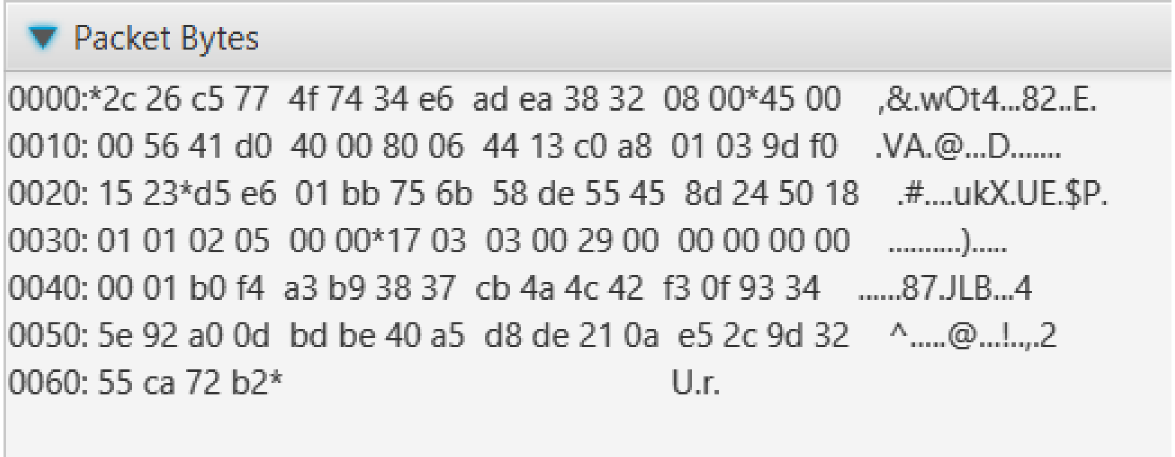


Protocol doesn't exist



Protocol doesn't exist

Section #5 Packet Bytes Pane shows the data of the current packet (selected in the "Packet List" pane) in a hexdump style



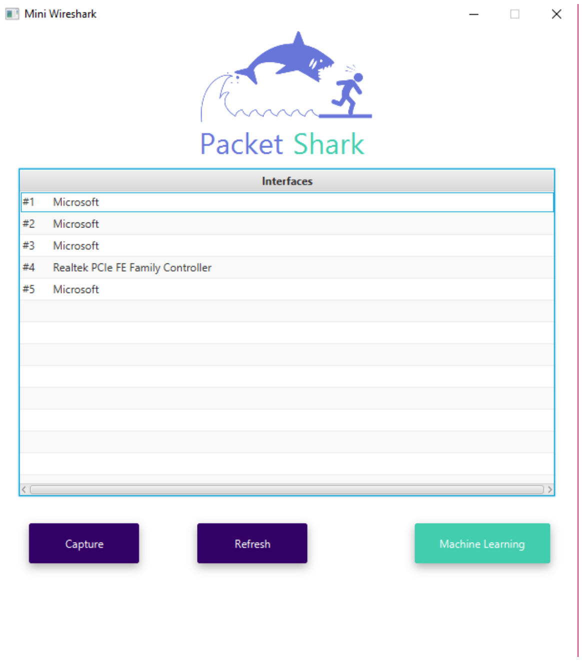
```
0000:*2c 26 c5 77  4f 74 34 e6  ad ea 38 32  08 00*45 00   ,&.wOt4...82..E.
0010: 00 56 41 d0  40 00 80 06  44 13 c0 a8  01 03 9d f0   .VA.@...D.......
0020: 15 23*d5 e6  01 bb 75 6b  58 de 55 45  8d 24 50 18   .#....ukX.UE.$P.
0030: 01 01 02 05  00 00*17 03  03 00 29 00  00 00 00 00   ..........).....
0040: 00 01 b0 f4  a3 b9 38 37  cb 4a 4c 42  f3 0f 93 34   ......87.JLB...4
0050: 5e 92 a0 0d  bd be 40 a5  d8 de 21 0a  e5 2c 9d 32   ^.....@...!..,.2
0060: 55 ca 72 b2*                                         U.r.
```

PART B | Machine Learning

Using the decision tree methodology, examples (packets) in pcap format are supplied to the program using the learn button, so the program is trained on them. After that, using the recognize button, another samples (in pcap format) can be supplied to the program, and the program tries to recognize their protocols and outputs them.

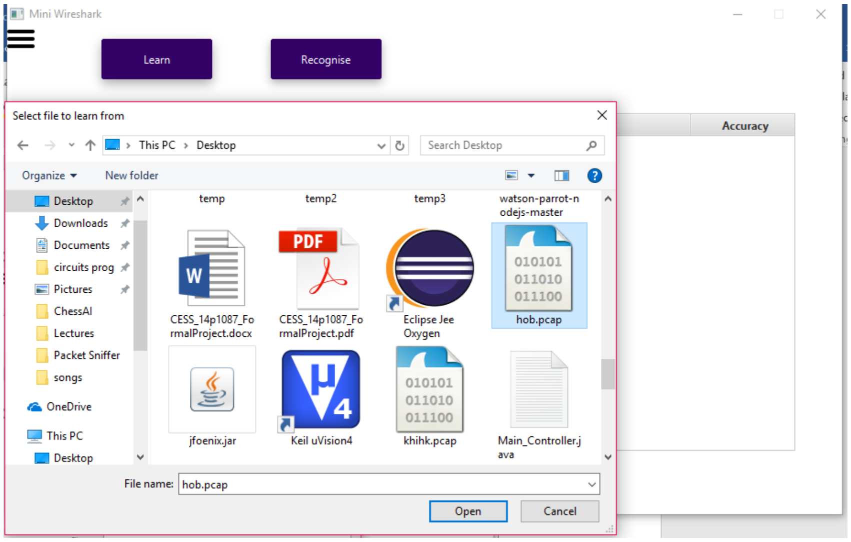
Note: The program currently can be trained to recognize: Ethernet, ARP, IP4, IP6, ICMP, TCP, UDP.

Click on Machine Learning button



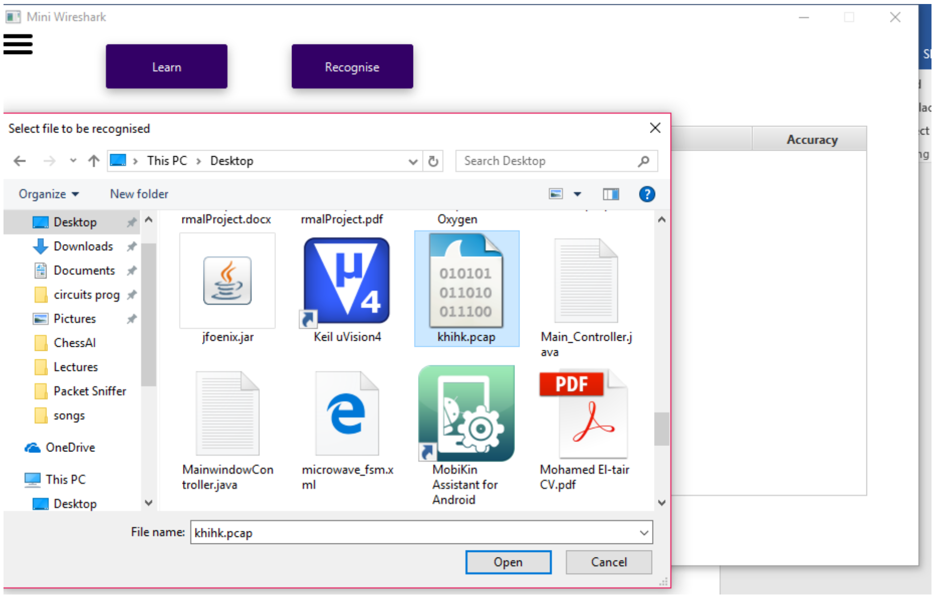
	Interfaces
#1	Microsoft
#2	Microsoft
#3	Microsoft
#4	Realtek PCIe FE Family Controller
#5	Microsoft

Select the file you want to train the program on



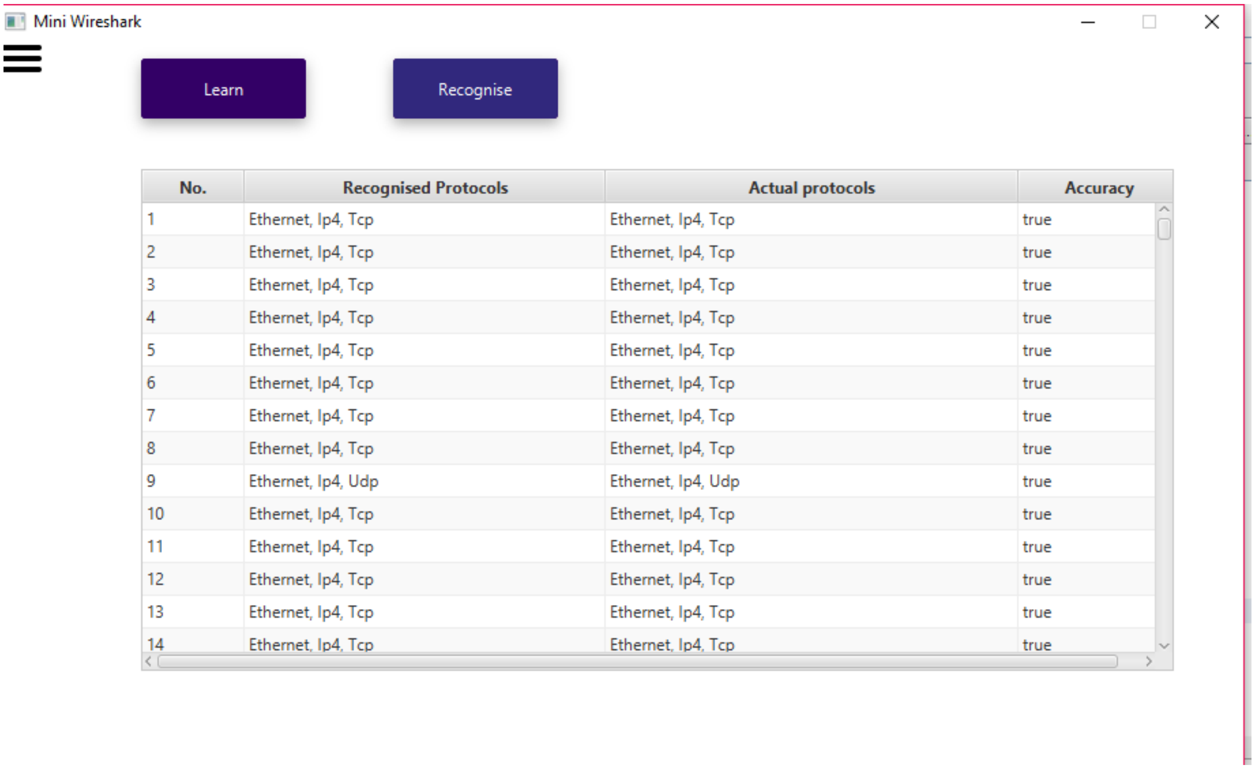
File name: hob.pcap

Select the file you want the program to recognize



File name: khihk.pcap

Then see the results!



No.	Recognised Protocols	Actual protocols	Accuracy
1	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
2	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
3	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
4	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
5	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
6	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
7	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
8	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
9	Ethernet, Ip4, Udp	Ethernet, Ip4, Udp	true
10	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
11	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
12	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
13	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true
14	Ethernet, Ip4, Tcp	Ethernet, Ip4, Tcp	true