

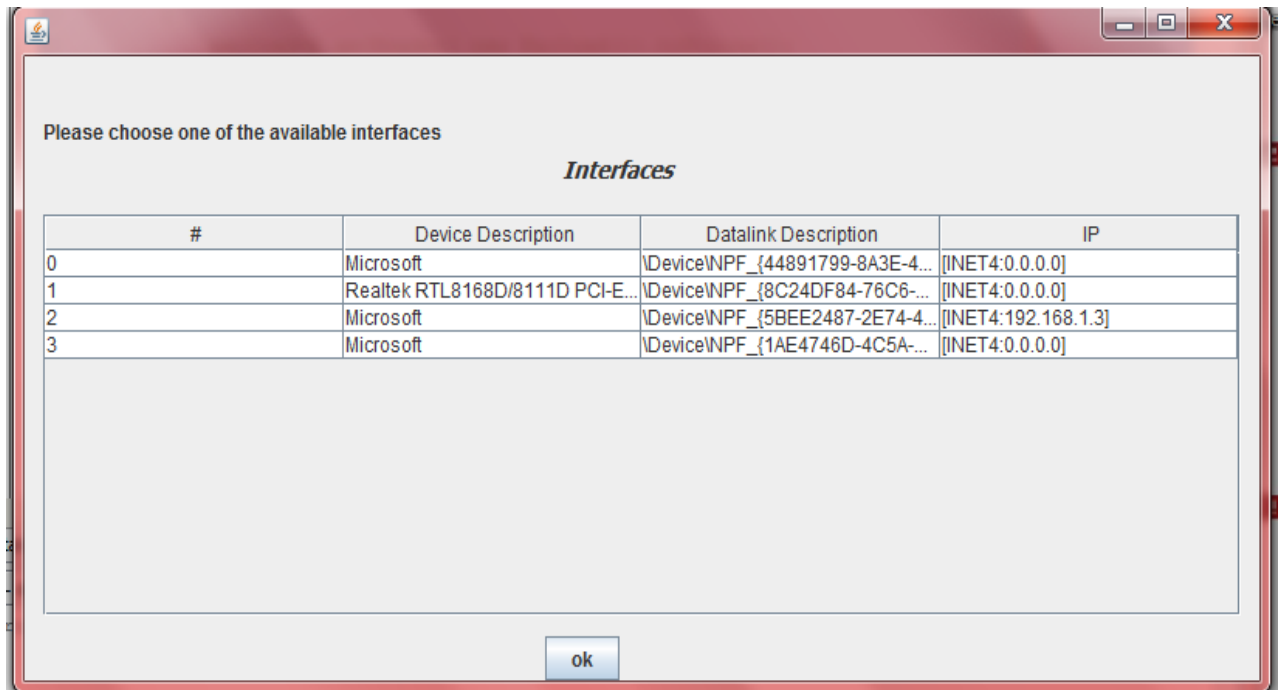
WiresharkNAS project

Table of Contents

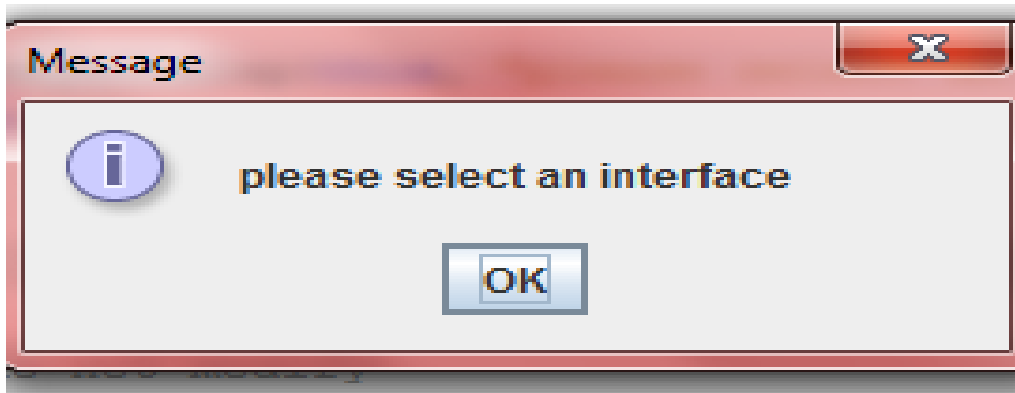
User Guide	2
Program Functionalities	4
Project's Github Repository.....	9
General Notes:-	9
TODO	9
Used Library.....	9
REFERENCES	10

User Guide

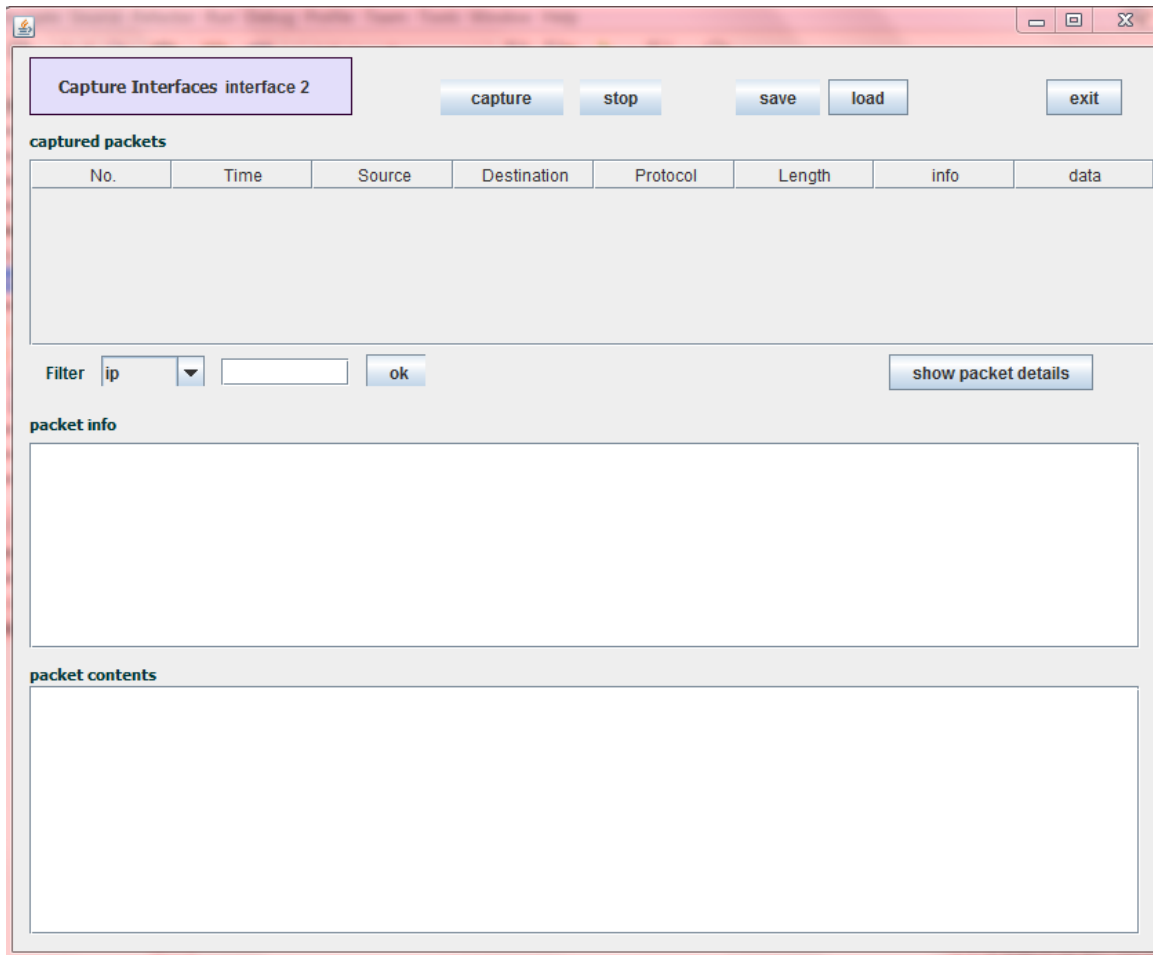
1-user should choose on of the available interfaces



Otherwise, he will be asked to choose one



2- a window will appear displaying the interface chosen



Program Functionalities

- Capture live packets and the stop whenever he wants to
- Whenever show packet details is clicked, different protocols displayed such as Ethernet, ARP, TCP, UDP, HTTP

The screenshot shows a network packet capture application interface. At the top, there's a section for 'Capture Interfaces interface 2' with buttons for 'capture', 'stop', 'save', 'load', and 'exit'. Below this is a table of 'captured packets' with columns: No., Time, Source, Destination, Protocol, Length, info, and data. The table lists 7 packets, with packet 5 selected. Below the table is a 'Filter' section with a dropdown set to 'ip' and an 'ok' button. To the right is a 'show packet details' button. Below the filter is the 'packet info' section, which displays details for the selected packet (packet 5):
Udp: ***** Udp offset=54 (0x36) length=8
Udp:
Udp: source = 53598
Udp: destination = 1900
Udp: length = 154
Udp: checksum = 0xB2D6 (45782) [correct]
Udp:
Below the packet info is the 'packet contents' section, which displays the raw data of the selected packet in hexadecimal and ASCII format:
003e: 4d 2d 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f M-SEARCH * HTTP/
004e: 31 2e 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 1.1..Host:[FF02:
005e: 3a 43 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 72 6e :C]:1900.ST:urn
006e: 3a 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f :Microsoft Windo
007e: 77 73 20 50 65 65 72 20 4e 61 6d 65 20 52 65 73 ws Peer Name Res
008e: 6f 6c 75 74 69 6f 6e 20 50 72 6f 74 6f 63 6f 6c olution Protocol
009e: 3a 20 56 34 3a 49 50 56 36 3a 4c 69 6e 6b 4c 6f :V4:IPv6:LinkLo
00ae: 63 61 6c 0d 0a 4d 61 6e 3a 22 73 73 64 70 3a 64 cal..Man:"ssdp:d
00be: 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 33 0d 0a iscover"..MX:3..
00ce: 0d 0a ..

- Filters can be applied on the captured packets from the drop down menu

The screenshot shows a network packet capture tool interface. At the top, there's a section for 'Capture Interfaces interface 2' with buttons for 'capture', 'stop', 'save', 'load', and 'exit'. Below this is a table of 'captured packets' with columns for No., Time, Source, Destination, Protocol, Length, info, and data. The table lists several HTTP packets. Below the table is a 'Filter' section with a dropdown menu set to 'protocol' and a text box containing 'HTTP', along with an 'ok' button and a 'show packet details' button. The 'packet info' section displays details for an Ethernet frame, including destination and source MAC addresses and LG/IG bits. The 'packet contents' section shows the raw data of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	info	data
33	1517295658994	93.184.220.29	192.168.43.98	HTTP	842	Eth: ***** Ethe...	Data: ***** Pa...
119	1517295732289	192.168.43.98	5.45.62.116	HTTP	356	Eth: ***** Ethe...	
120	1517295733552	192.168.43.98	5.45.62.116	HTTP	356	Eth: ***** Ethe...	
124	1517295736208	5.45.62.116	192.168.43.98	HTTP	234	Eth: ***** Ethe...	Data: ***** Pa...
136	1517295739487	192.168.43.98	192.168.43.1	HTTP	296	Eth: ***** Ethe...	
170	1517295806105	5.45.62.116	192.168.43.98	HTTP	208	Eth: ***** Ethe...	
173	1517295808065	192.168.43.98	5.45.62.116	HTTP	356	Eth: ***** Ethe...	

Filter: protocol ▼ HTTP ok show packet details

packet info

```

Eth: ***** Ethernet - "Ethernet" - offset=0 (0x0) length=14 protocol suite=LAN
Eth:
Eth:      destination = 70:1a:04:dd:a8:2b
Eth:      ....0. .... = [0] LG bit
Eth:      ....0. .... = [2] IG bit
Eth:      source = e4:32:cb:f7:02:d1
Eth:      ....0. .... = [0] LG bit
Eth:      ....0. .... = [2] IG bit
  
```

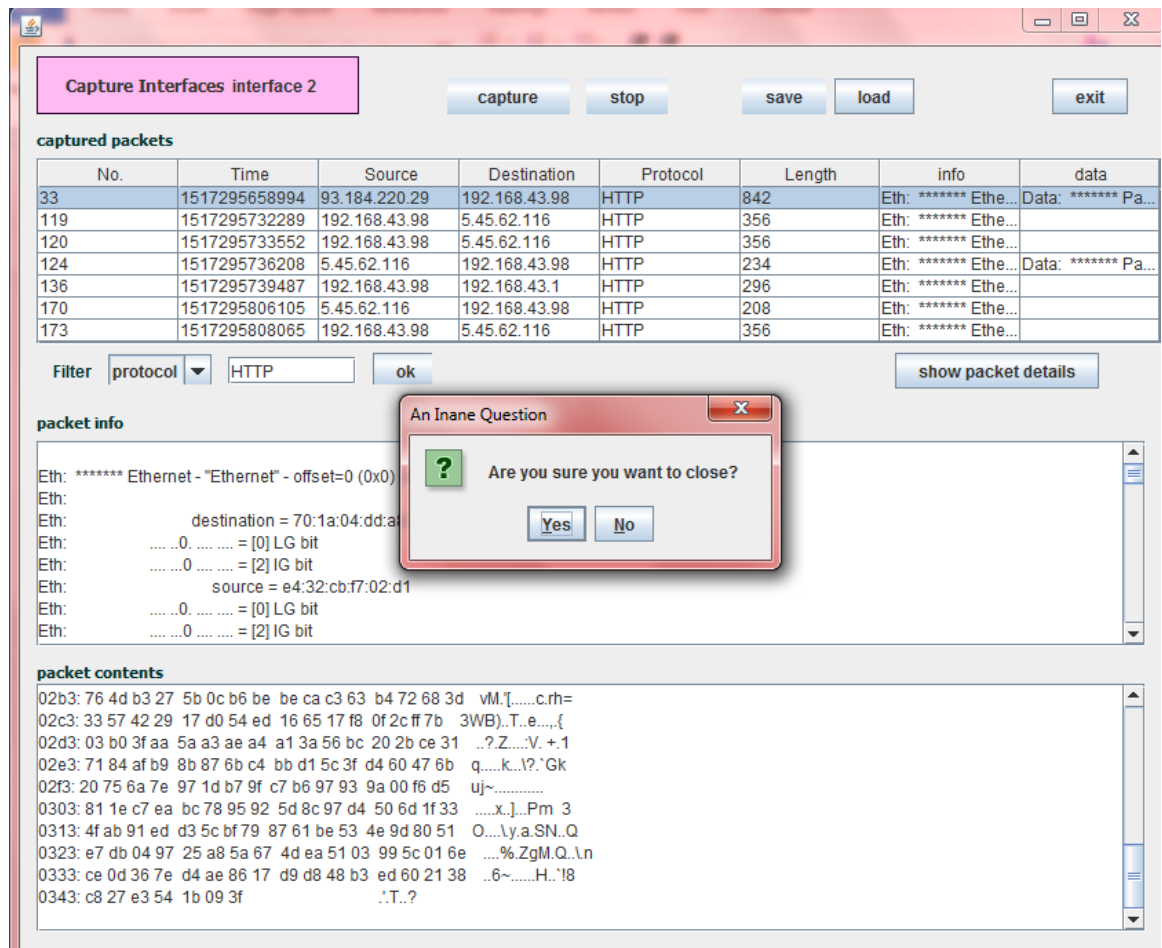
packet contents

```

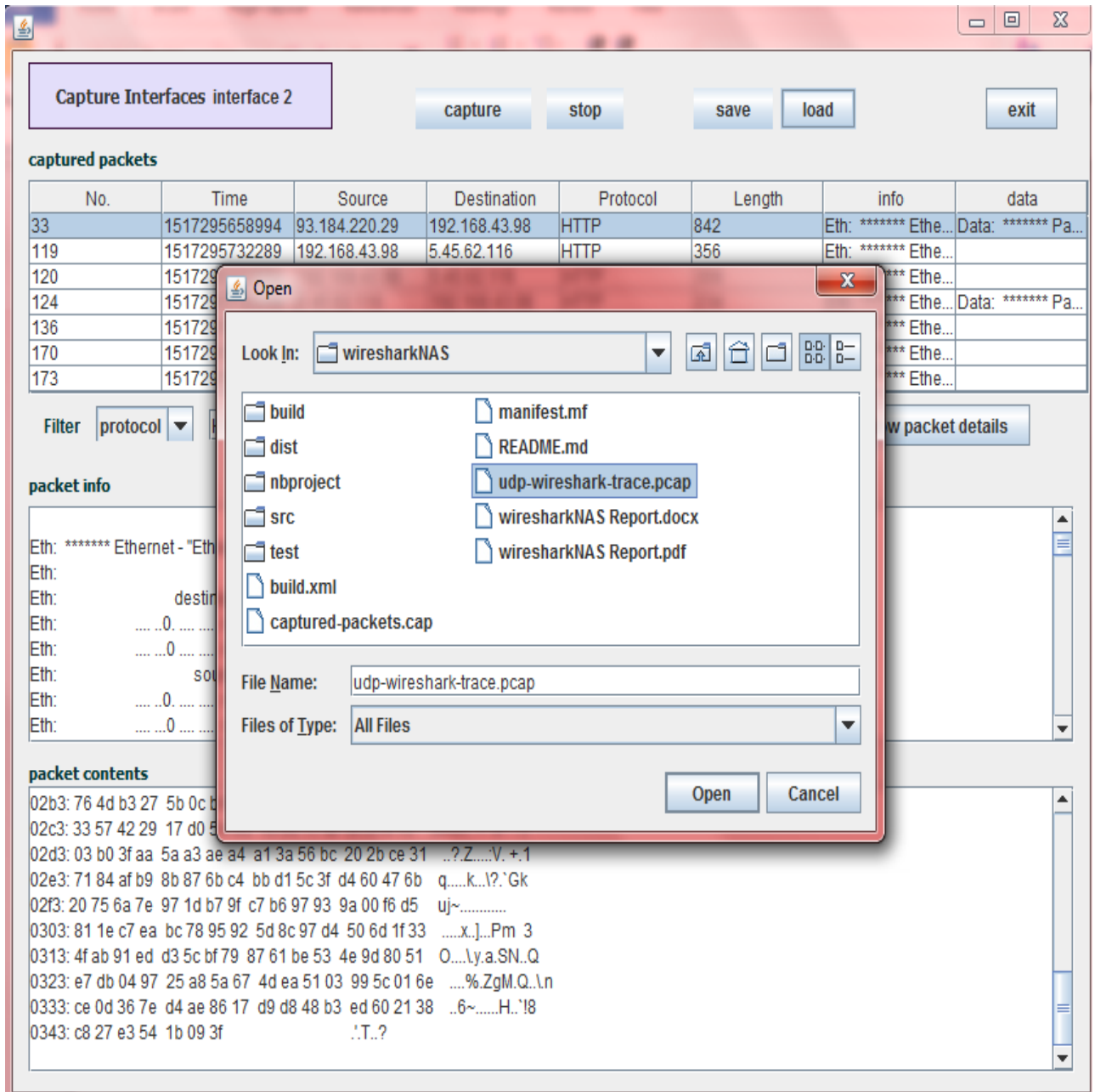
02b3: 76 4d b3 27 5b 0c b6 be be ca c3 63 b4 72 68 3d  vM.[.....c.rh=
02c3: 33 57 42 29 17 d0 54 ed 16 65 17 f8 0f 2c ff 7b  3WB)..T.e....{
02d3: 03 b0 3f aa 5a a3 ae a4 a1 3a 56 bc 20 2b ce 31  ..?Z....V.+.1
02e3: 71 84 af b9 8b 87 6b c4 bb d1 5c 3f d4 60 47 6b  q....k..\'Gk
02f3: 20 75 6a 7e 97 1d b7 9f c7 b6 97 93 9a 00 f6 d5  uj~.....
0303: 81 1e c7 ea bc 78 95 92 5d 8c 97 d4 50 6d 1f 33  ....x.]..Pm 3
0313: 4f ab 91 ed d3 5c bf 79 87 61 be 53 4e 9d 80 51  O....\y.a.SN..Q
0323: e7 db 04 97 25 a8 5a 67 4d ea 51 03 99 5c 01 6e  ....%ZgM.Q..\n
0333: ce 0d 36 7e d4 ae 86 17 d9 d8 48 b3 ed 60 21 38  ..6~.....H..!8
0343: c8 27 e3 54 1b 09 3f          .!T..?
  
```

Can filter with protocol, ip address, and length of the captured packets

- Chooses to go back to the list of interfaces by clicking on Capture Interface area



- Can load previously captured packets in cap or pcap file formats



Project's Github Repository

<https://github.com/nouraali3/WiresharkNAS.git>

General Notes:-

1. Program is tested on windows 7
2. npf driver should be running

TODO

1. save the captured packets

Used Library

Jnetpcap1.4

The following line should be added for the library to work well, but with replacing the dots with the path of the jar file

-Djava.library.path=.....

REFERENCES

1. <http://inetpcap.com/node/69>
2. <http://inetpcap.com/node/68>