NAME:THULASI.S EXPERIMENT:14

ROLL:NO:241901118 DATE:16/10/25

TO CAPTURE,SAVE AND ANALYZE NETWORK TRAFFIC USING WIRESHARK TOOL

AIM:

To capture,save and analyze network traffic on TCP / UDP/ IP/ HTTP/ DHCP/ ARP/ICMP/DNS using Wireshark Tool.

INTRODUCTION:

This experiment teaches you how to capture live network traffic with Wireshark, save captures for later review, and analyze protocol-level behavior across common network protocols . You will learn how to identify normal vs. anomalous packet patterns, extract useful metadata and use filters to focus analysis.

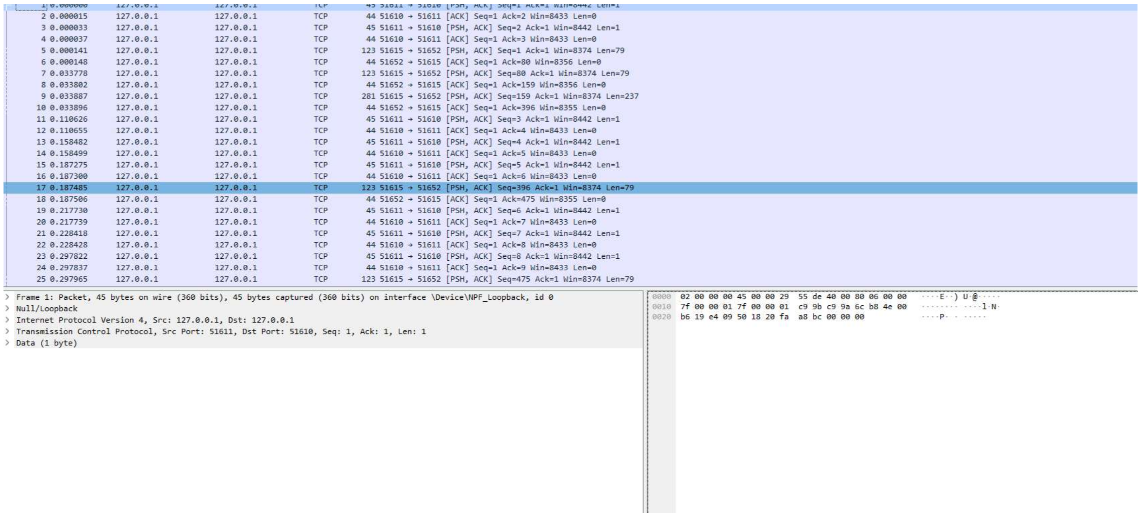
CAPTURING PACKETS:

1.select local area network in wireshark.

2.go to capture option and select stop.

3.then click start and select save the packets.

OUTPUT



```
    1 0.000000    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=1
    2 0.000015    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=2 Win=8433 Len=0
    3 0.000033    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=1
    4 0.000037    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=3 Win=8433 Len=0
    5 0.000141    127.0.0.1     127.0.0.1     TCP    123 51615 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8374 Len=79
    6 0.000148    127.0.0.1     127.0.0.1     TCP     44 51652 → 51615 [ACK] Seq=1 Ack=80 Win=8356 Len=0
    7 0.033778    127.0.0.1     127.0.0.1     TCP    123 51615 → 51652 [PSH, ACK] Seq=80 Ack=1 Win=8374 Len=79
    8 0.033802    127.0.0.1     127.0.0.1     TCP     44 51652 → 51615 [ACK] Seq=1 Ack=159 Win=8356 Len=0
    9 0.033887    127.0.0.1     127.0.0.1     TCP    281 51615 → 51652 [PSH, ACK] Seq=159 Ack=1 Win=8374 Len=237
   10 0.033896    127.0.0.1     127.0.0.1     TCP     44 51652 → 51615 [ACK] Seq=1 Ack=396 Win=8355 Len=0
   11 0.110626    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=1
   12 0.110655    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=4 Win=8433 Len=0
   13 0.158482    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Len=1
   14 0.158499    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=5 Win=8433 Len=0
   15 0.187275    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=1
   16 0.187300    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=6 Win=8433 Len=0
   17 0.187485    127.0.0.1     127.0.0.1     TCP    123 51615 → 51652 [PSH, ACK] Seq=396 Ack=1 Win=8374 Len=79
   18 0.187506    127.0.0.1     127.0.0.1     TCP     44 51652 → 51615 [ACK] Seq=1 Ack=475 Win=8355 Len=0
   19 0.217730    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Len=1
   20 0.217739    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=7 Win=8433 Len=0
   21 0.228418    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Len=1
   22 0.228428    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=8 Win=8433 Len=0
   23 0.297822    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=8 Ack=1 Win=8442 Len=1
   24 0.297837    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=9 Win=8433 Len=0
   25 0.297965    127.0.0.1     127.0.0.1     TCP    123 51615 → 51652 [PSH, ACK] Seq=475 Ack=1 Win=8374 Len=79
```

```
> Frame 1: Packet, 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 51611, Dst Port: 51610, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)
```

```
0000  02 00 00 00 45 00 00 29  55 de 40 00 80 06 00 00   ····E··) U·@·····
0010  7f 00 00 01 7f 00 00 01  c9 9b c9 9a 6c b8 4e 00   ········ ····l·N·
0020  b6 19 e4 09 50 18 20 fa  a8 bc 00 00 00            ····P· · ·····
```

CAPTURING ONLY TCP/UDP PACKETS:

1.select local area network in wireshark.

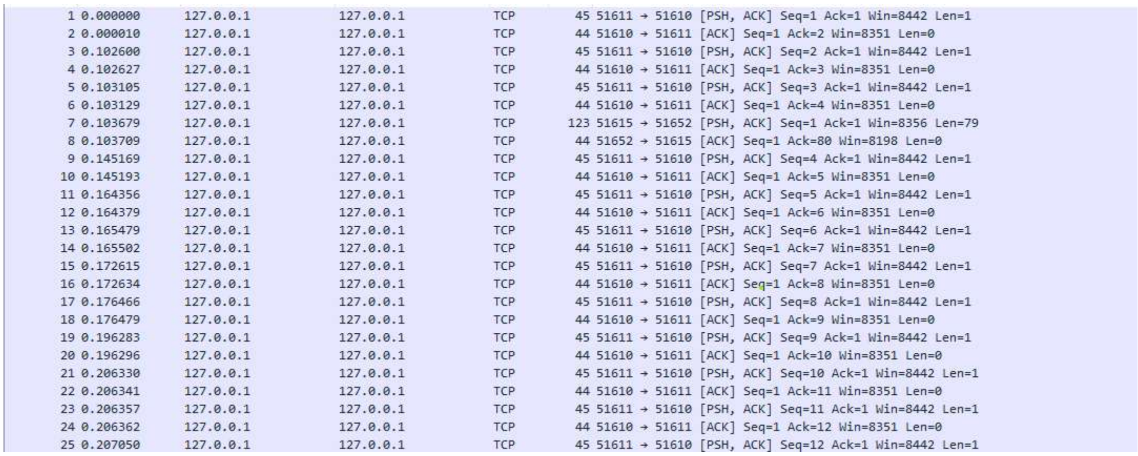
2.go to capture option and select stop.

3.then click start.

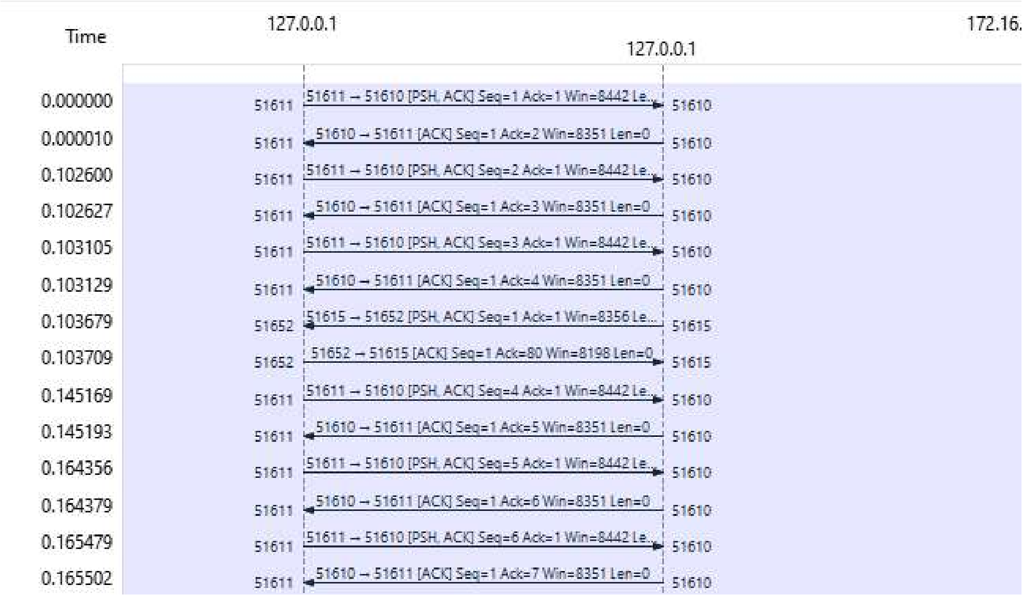
4.search TCP packets in search bar.

5.to see flowgraph click statistics > flowgraph and save the packets.

OUTPUT



```
    1 0.000000    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=1
    2 0.000010    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0
    3 0.102600    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=1
    4 0.102627    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=3 Win=8351 Len=0
    5 0.103105    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=1
    6 0.103129    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=4 Win=8351 Len=0
    7 0.103679    127.0.0.1     127.0.0.1     TCP    123 51615 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Len=79
    8 0.103709    127.0.0.1     127.0.0.1     TCP     44 51652 → 51615 [ACK] Seq=1 Ack=80 Win=8198 Len=0
    9 0.145169    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Len=1
   10 0.145193    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=5 Win=8351 Len=0
   11 0.164356    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=1
   12 0.164379    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=6 Win=8351 Len=0
   13 0.165479    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Len=1
   14 0.165502    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=7 Win=8351 Len=0
   15 0.172615    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Len=1
   16 0.172634    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=8 Win=8351 Len=0
   17 0.176466    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=8 Ack=1 Win=8442 Len=1
   18 0.176479    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=9 Win=8351 Len=0
   19 0.196283    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=9 Ack=1 Win=8442 Len=1
   20 0.196296    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=10 Win=8351 Len=0
   21 0.206330    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=10 Ack=1 Win=8442 Len=1
   22 0.206341    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=11 Win=8351 Len=0
   23 0.206357    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=11 Ack=1 Win=8442 Len=1
   24 0.206362    127.0.0.1     127.0.0.1     TCP     44 51610 → 51611 [ACK] Seq=1 Ack=12 Win=8351 Len=0
   25 0.207050    127.0.0.1     127.0.0.1     TCP     45 51611 → 51610 [PSH, ACK] Seq=12 Ack=1 Win=8442 Len=1
```



Time	127.0.0.1		127.0.0.1	172.16.
0.000000	51611	51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Le...	51610	
0.000010	51611	51610 → 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0	51610	
0.102600	51611	51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Le...	51610	
0.102627	51611	51610 → 51611 [ACK] Seq=1 Ack=3 Win=8351 Len=0	51610	
0.103105	51611	51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Le...	51610	
0.103129	51611	51610 → 51611 [ACK] Seq=1 Ack=4 Win=8351 Len=0	51610	
0.103679	51652	51615 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Le...	51615	
0.103709	51652	51652 → 51615 [ACK] Seq=1 Ack=80 Win=8198 Len=0	51615	
0.145169	51611	51611 → 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Le...	51610	
0.145193	51611	51610 → 51611 [ACK] Seq=1 Ack=5 Win=8351 Len=0	51610	
0.164356	51611	51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Le...	51610	
0.164379	51611	51610 → 51611 [ACK] Seq=1 Ack=6 Win=8351 Len=0	51610	
0.165479	51611	51611 → 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Le...	51610	
0.165502	51611	51610 → 51611 [ACK] Seq=1 Ack=7 Win=8351 Len=0	51610	

CAPTURING ONLY ARP PACKETS:

1.select local area network in wireshark.

2.go to capture option and select stop.

3.then click start.

4.search ARP packets in search bar.

5.to see flowgraph click statistics > flowgraph and save the packets.

CAPTURING ONLY DNS PACKETS:

1.select local area network in wireshark.

2.go to capture option and select stop.

3.then click start.

4.search DNS packets in search bar and save it.

CAPTURING ONLY HTTP PACKETS:

1.select local area network in wireshark.

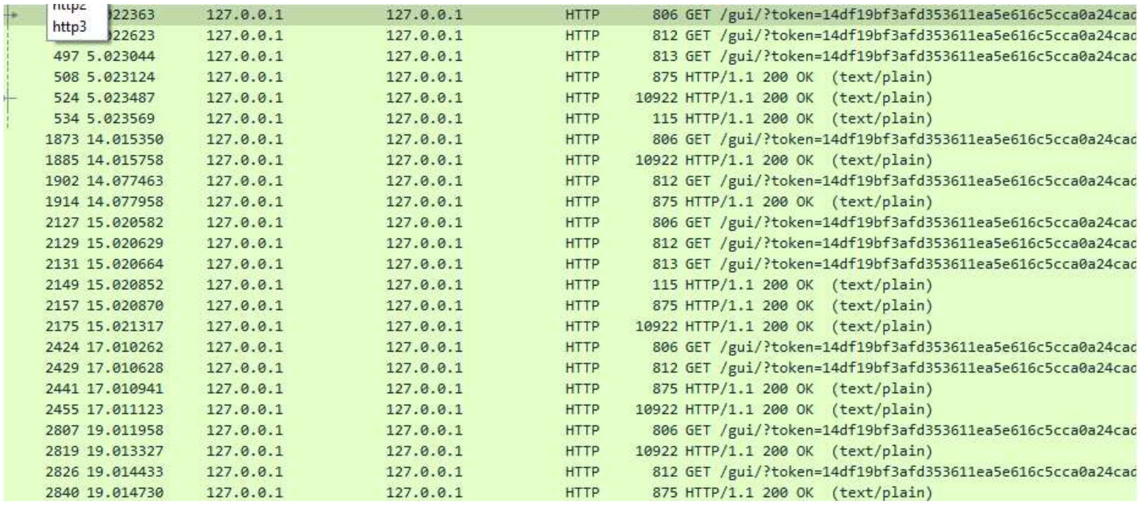
2.go to capture option and select stop.

3.then click start.

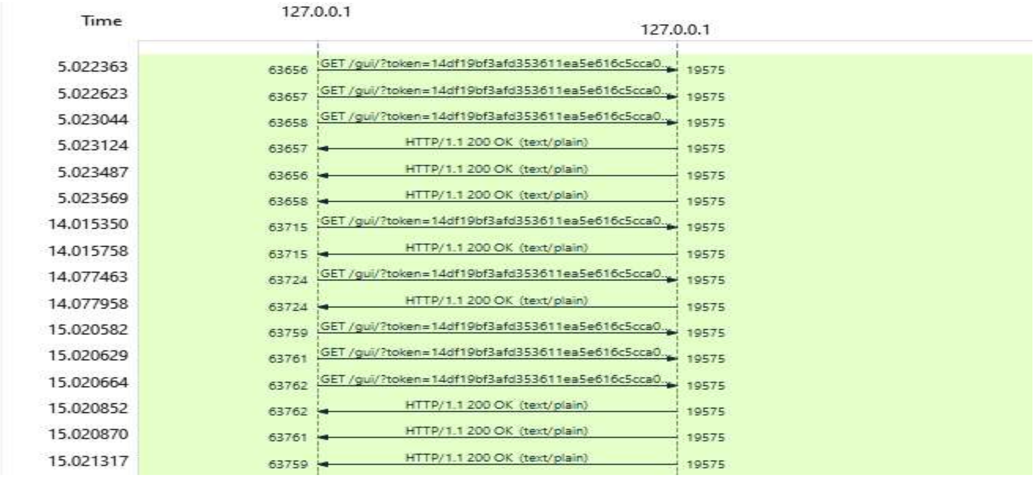
4.search HTTP packets in search bar.

5.to see flowgraph click statistics > flowgraph and save the packets.

OUTPUT



```
         22363   127.0.0.1       127.0.0.1       HTTP    806 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
         22623   127.0.0.1       127.0.0.1       HTTP    812 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
    497 5.023044   127.0.0.1       127.0.0.1       HTTP    813 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
    508 5.023124   127.0.0.1       127.0.0.1       HTTP    875 HTTP/1.1 200 OK  (text/plain)
    524 5.023487   127.0.0.1       127.0.0.1       HTTP  10922 HTTP/1.1 200 OK  (text/plain)
    534 5.023569   127.0.0.1       127.0.0.1       HTTP    115 HTTP/1.1 200 OK  (text/plain)
   1873 14.015350  127.0.0.1       127.0.0.1       HTTP    806 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   1885 14.015758  127.0.0.1       127.0.0.1       HTTP  10922 HTTP/1.1 200 OK  (text/plain)
   1902 14.077463  127.0.0.1       127.0.0.1       HTTP    812 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   1914 14.077958  127.0.0.1       127.0.0.1       HTTP    875 HTTP/1.1 200 OK  (text/plain)
   2127 15.020582  127.0.0.1       127.0.0.1       HTTP    806 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2129 15.020629  127.0.0.1       127.0.0.1       HTTP    812 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2131 15.020664  127.0.0.1       127.0.0.1       HTTP    813 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2149 15.020852  127.0.0.1       127.0.0.1       HTTP    115 HTTP/1.1 200 OK  (text/plain)
   2157 15.020870  127.0.0.1       127.0.0.1       HTTP    875 HTTP/1.1 200 OK  (text/plain)
   2175 15.021317  127.0.0.1       127.0.0.1       HTTP  10922 HTTP/1.1 200 OK  (text/plain)
   2424 17.010262  127.0.0.1       127.0.0.1       HTTP    806 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2429 17.010628  127.0.0.1       127.0.0.1       HTTP    812 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2441 17.010941  127.0.0.1       127.0.0.1       HTTP    875 HTTP/1.1 200 OK  (text/plain)
   2455 17.011123  127.0.0.1       127.0.0.1       HTTP  10922 HTTP/1.1 200 OK  (text/plain)
   2807 19.011958  127.0.0.1       127.0.0.1       HTTP    806 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2819 19.013327  127.0.0.1       127.0.0.1       HTTP  10922 HTTP/1.1 200 OK  (text/plain)
   2826 19.014433  127.0.0.1       127.0.0.1       HTTP    812 GET /gui/?token=14df19bf3afd353611ea5e616c5cca0a24cad
   2840 19.014730  127.0.0.1       127.0.0.1       HTTP    875 HTTP/1.1 200 OK  (text/plain)
```



```
Time          127.0.0.1                                                   127.0.0.1

5.022363      63656  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
5.022623      63657  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
5.023044      63658  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
5.023124      63657  <--  HTTP/1.1 200 OK (text/plain)                       19575
5.023487      63656  <--  HTTP/1.1 200 OK (text/plain)                       19575
5.023569      63658  <--  HTTP/1.1 200 OK (text/plain)                       19575
14.015350     63715  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
14.015758     63715  <--  HTTP/1.1 200 OK (text/plain)                       19575
14.077463     63724  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
14.077958     63724  <--  HTTP/1.1 200 OK (text/plain)                       19575
15.020582     63759  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
15.020629     63761  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
15.020664     63762  GET /gui/?token=14df19bf3afd353611ea5e616c5cca0..  -->  19575
15.020852     63762  <--  HTTP/1.1 200 OK (text/plain)                       19575
15.020870     63761  <--  HTTP/1.1 200 OK (text/plain)                       19575
15.021317     63759  <--  HTTP/1.1 200 OK (text/plain)                       19575
```

CAPTURING ONLY IP/ICMP PACKETS:

1.select local area network in wireshark.

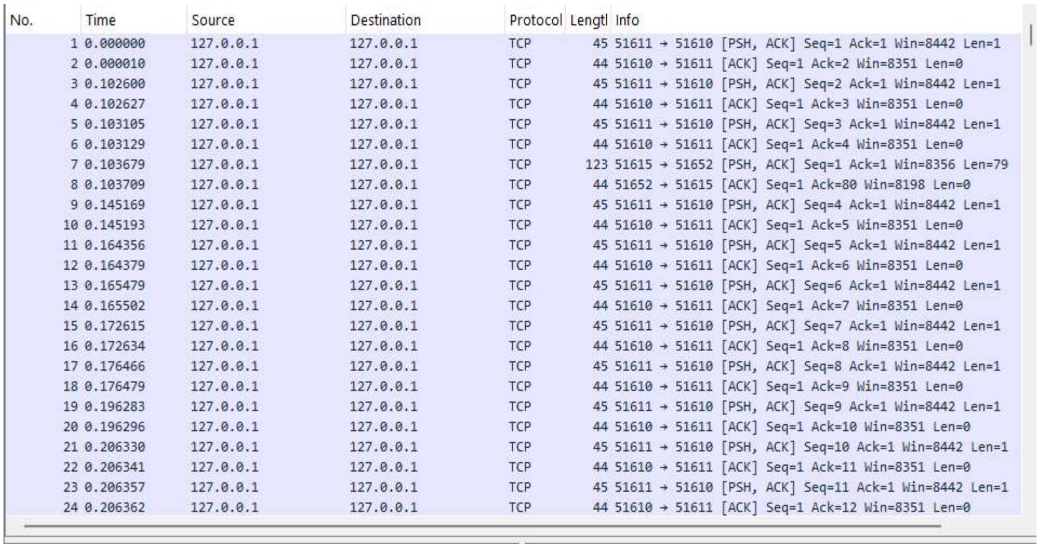
2.go to capture option and select stop.

3.then click start.

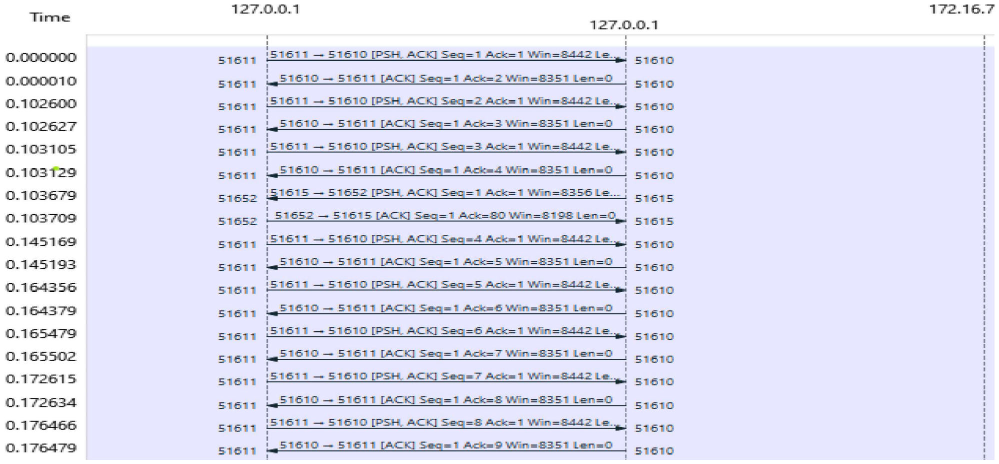
4.search IP/ICMP packets in search bar.

5.to see flowgraph click statistics > flowgraph and save the packets.

OUTPUT



```
No.   Time      Source      Destination  Protocol Lengtl Info
    1 0.000000  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=1
    2 0.000010  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0
    3 0.102600  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=1
    4 0.102627  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=3 Win=8351 Len=0
    5 0.103105  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=1
    6 0.103129  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=4 Win=8351 Len=0
    7 0.103679  127.0.0.1   127.0.0.1    TCP      123 51615 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Len=79
    8 0.103709  127.0.0.1   127.0.0.1    TCP       44 51652 → 51615 [ACK] Seq=1 Ack=80 Win=8198 Len=0
    9 0.145169  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Len=1
   10 0.145193  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=5 Win=8351 Len=0
   11 0.164356  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=1
   12 0.164379  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=6 Win=8351 Len=0
   13 0.165479  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Len=1
   14 0.165502  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=7 Win=8351 Len=0
   15 0.172615  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Len=1
   16 0.172634  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=8 Win=8351 Len=0
   17 0.176466  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=8 Ack=1 Win=8442 Len=1
   18 0.176479  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=9 Win=8351 Len=0
   19 0.196283  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=9 Ack=1 Win=8442 Len=1
   20 0.196296  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=10 Win=8351 Len=0
   21 0.206330  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=10 Ack=1 Win=8442 Len=1
   22 0.206341  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=11 Win=8351 Len=0
   23 0.206357  127.0.0.1   127.0.0.1    TCP       45 51611 → 51610 [PSH, ACK] Seq=11 Ack=1 Win=8442 Len=1
   24 0.206362  127.0.0.1   127.0.0.1    TCP       44 51610 → 51611 [ACK] Seq=1 Ack=12 Win=8351 Len=0
```



```
Time             127.0.0.1                                              127.0.0.1                   172.16.7
0.000000  51611  51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Le..   51610
0.000010  51611  51610 → 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0       51610
0.102600  51611  51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Le..   51610
0.102627  51611  51610 → 51611 [ACK] Seq=1 Ack=3 Win=8351 Len=0       51610
0.103105  51611  51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Le..   51610
0.103129  51611  51610 → 51611 [ACK] Seq=1 Ack=4 Win=8351 Len=0       51610
0.103679  51652  51615 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Le...  51615
0.103709  51652  51652 → 51615 [ACK] Seq=1 Ack=80 Win=8198 Len=0      51615
0.145169  51611  51611 → 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Le..   51610
0.145193  51611  51610 → 51611 [ACK] Seq=1 Ack=5 Win=8351 Len=0       51610
0.164356  51611  51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Le..   51610
0.164379  51611  51610 → 51611 [ACK] Seq=1 Ack=6 Win=8351 Len=0       51610
0.165479  51611  51611 → 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Le..   51610
0.165502  51611  51610 → 51611 [ACK] Seq=1 Ack=7 Win=8351 Len=0       51610
0.172615  51611  51611 → 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Le..   51610
0.172634  51611  51610 → 51611 [ACK] Seq=1 Ack=8 Win=8351 Len=0       51610
0.176466  51611  51611 → 51610 [PSH, ACK] Seq=8 Ack=1 Win=8442 Le..   51610
0.176479  51611  51610 → 51611 [ACK] Seq=1 Ack=9 Win=8351 Len=0       51610
```

CAPTURING ONLY DHCP PACKETS:

1.select local area network in wireshark.

2.go to capture option and select stop.

3.then click start.

4.search DHCP packets in search bar.

5.to see flowgraph click statistics > flowgraph and save the packets.

RESULT:

Thus,analyzing the network traffic using Wireshark Tool is done.