Assignments:-1

Module:- NDC(WireShark)
Name:- Vivek Nishad

Lab Assignment :-

Objective: Network Traffic Monitoring and Analysis using Wireshark

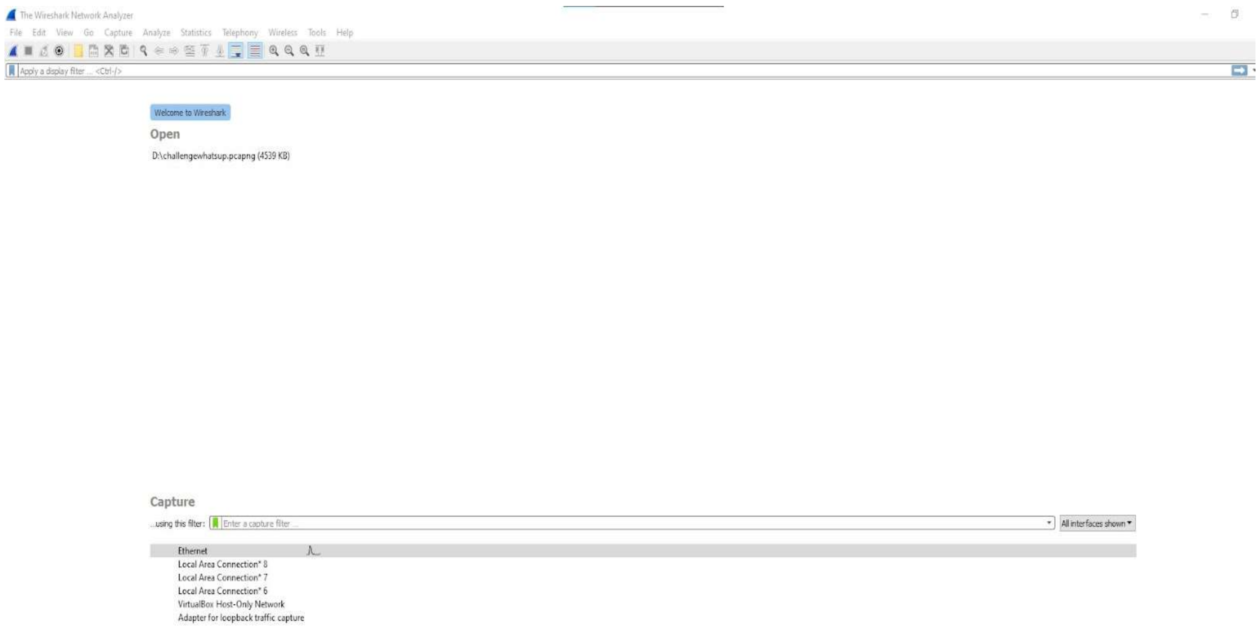
Tool Used: Wireshark

It is a network packet analyzer tool which captures network packets and tries to display that packet data as detailed as possible.

Team Size: 1

Person Duration: 3 Hours

1. List down the network interfaces connected to your host.Identify the ethernet interface



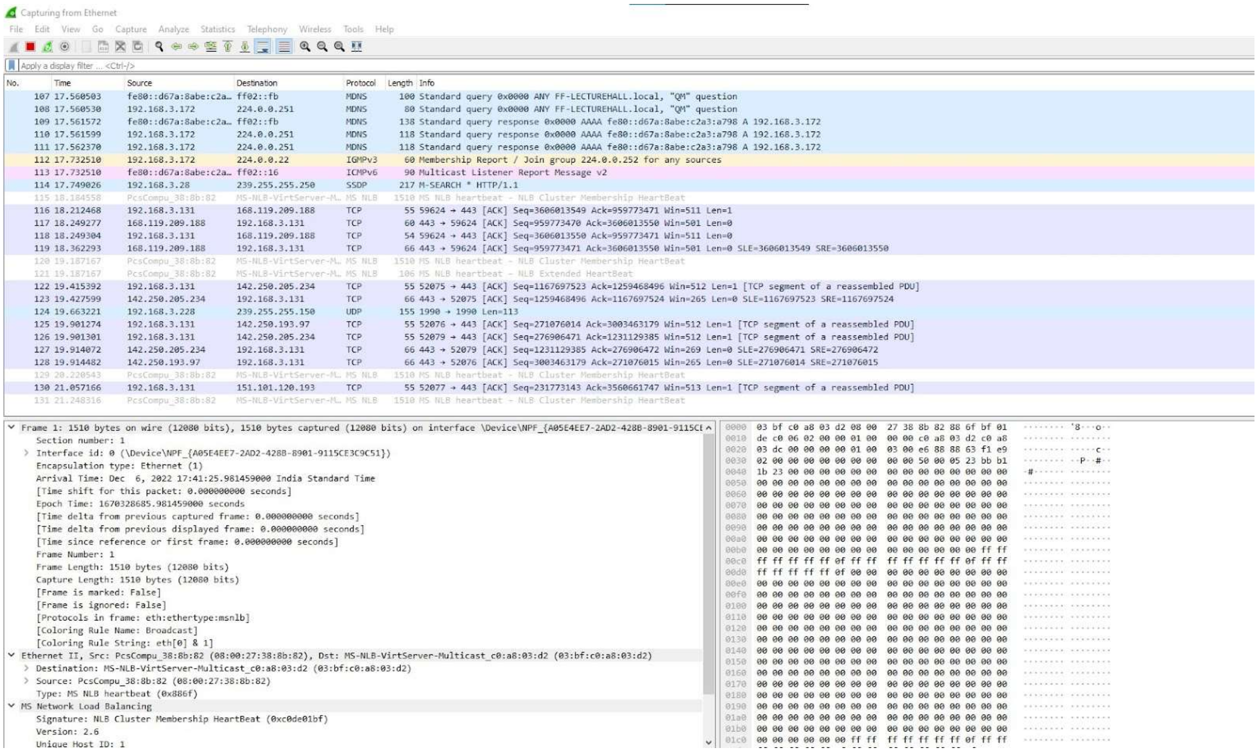
Open

D:\challengewhatsup.pcapng (4539 KB)

Capture

...using this filter:

Ethernet
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
VirtualBox Host-Only Network
Adapter for loopback traffic capture



Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

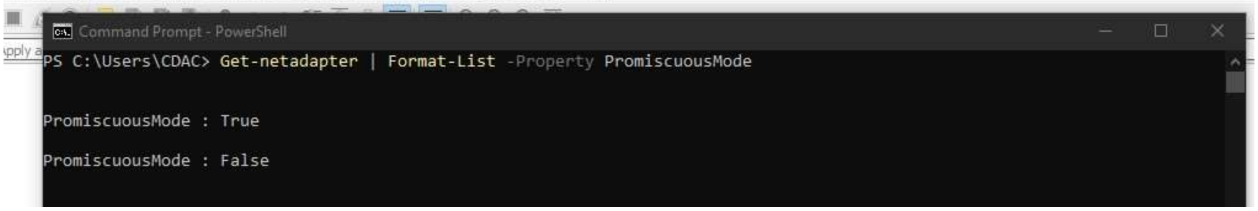
```
No.   Time       Source                 Destination            Protocol Length Info
  107 17.560503  fe80::d67a:8abe:c2a…   ff02::fb               MDNS      100 Standard query 0x0000 ANY FF-LECTUREHALL.local, "QM" question
  108 17.560530  192.168.3.172          224.0.0.251            MDNS       80 Standard query 0x0000 ANY FF-LECTUREHALL.local, "QM" question
  109 17.561572  fe80::d67a:8abe:c2a…   ff02::fb               MDNS      138 Standard query response 0x0000 AAAA fe80::d67a:8abe:c2a3:a798 A 192.168.3.172
  110 17.561599  192.168.3.172          224.0.0.251            MDNS      118 Standard query response 0x0000 AAAA fe80::d67a:8abe:c2a3:a798 A 192.168.3.172
  111 17.562370  192.168.3.172          224.0.0.251            MDNS      118 Standard query response 0x0000 AAAA fe80::d67a:8abe:c2a3:a798 A 192.168.3.172
  112 17.732510  192.168.3.172          224.0.0.22             IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
  113 17.732510  fe80::d67a:8abe:c2a…   ff02::16               ICMPv6     90 Multicast Listener Report Message v2
  114 17.749026  192.168.3.28           239.255.255.250        SSDP      217 M-SEARCH * HTTP/1.1
  115 18.184558  PcsCompu_38:8b:82      MS-NLB-VirtServer-M…   MS NLB   1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
  116 18.212468  192.168.3.131          168.119.209.188        TCP        55 59624 → 443 [ACK] Seq=3606013549 Ack=959773471 Win=511 Len=1
  117 18.249277  168.119.209.188        192.168.3.131          TCP        60 443 → 59624 [ACK] Seq=959773470 Ack=3606013550 Win=501 Len=0
  118 18.249304  192.168.3.131          168.119.209.188        TCP        54 59624 → 443 [ACK] Seq=3606013550 Ack=959773471 Win=511 Len=0
  119 18.362293  168.119.209.188        192.168.3.131          TCP        66 443 → 59624 [ACK] Seq=959773471 Ack=3606013550 Win=501 Len=0 SLE=3606013549 SRE=3606013550
  120 19.187167  PcsCompu_38:8b:82      MS-NLB-VirtServer-M…   MS NLB   1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
  121 19.187167  PcsCompu_38:8b:82      MS-NLB-VirtServer-M…   MS NLB    106 MS NLB heartbeat - NLB Extended HeartBeat
  122 19.415392  192.168.3.131          142.250.205.234        TCP        55 52075 → 443 [ACK] Seq=1167697523 Ack=1259468496 Win=512 Len=1 [TCP segment of a reassembled PDU]
  123 19.427599  142.250.205.234        192.168.3.131          TCP        66 443 → 52075 [ACK] Seq=1259468496 Ack=1167697524 Win=265 Len=0 SLE=1167697523 SRE=1167697524
  124 19.663221  192.168.3.228          239.255.255.150        UDP       155 1990 → 1990 Len=113
  125 19.901274  192.168.3.131          142.250.193.97         TCP        55 52076 → 443 [ACK] Seq=271076014 Ack=3003463179 Win=512 Len=1 [TCP segment of a reassembled PDU]
  126 19.901301  192.168.3.131          142.250.205.234        TCP        55 52079 → 443 [ACK] Seq=276906471 Ack=1231129385 Win=512 Len=1 [TCP segment of a reassembled PDU]
  127 19.914072  142.250.205.234        192.168.3.131          TCP        66 443 → 52079 [ACK] Seq=1231129385 Ack=276906472 Win=269 Len=0 SLE=276906471 SRE=276906472
  128 19.914482  142.250.193.97         192.168.3.131          TCP        66 443 → 52076 [ACK] Seq=3003463179 Ack=271076015 Win=265 Len=0 SLE=271076014 SRE=271076015
  129 20.220543  PcsCompu_38:8b:82      MS-NLB-VirtServer-M…   MS NLB   1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
  130 21.057166  192.168.3.131          151.101.120.193        TCP        55 52077 → 443 [ACK] Seq=231773143 Ack=3560661747 Win=513 Len=1 [TCP segment of a reassembled PDU]
  131 21.248316  PcsCompu_38:8b:82      MS-NLB-VirtServer-M…   MS NLB   1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
```

```
v Frame 1: 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits) on interface \Device\NPF_{A05E4EE7-2AD2-428B-8901-9115CE
    Section number: 1
  > Interface id: 0 (\Device\NPF_{A05E4EE7-2AD2-428B-8901-9115CE3C9C51})
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec  6, 2022 17:41:25.981459000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1670328685.981459000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 1510 bytes (12080 bits)
    Capture Length: 1510 bytes (12080 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:msnlb]
    [Coloring Rule Name: Broadcast]
    [Coloring Rule String: eth[0] & 1]
v Ethernet II, Src: PcsCompu_38:8b:82 (08:00:27:38:8b:82), Dst: MS-NLB-VirtServer-Multicast_c0:a8:03:d2 (03:bf:c0:a8:03:d2)
  > Destination: MS-NLB-VirtServer-Multicast_c0:a8:03:d2 (03:bf:c0:a8:03:d2)
  > Source: PcsCompu_38:8b:82 (08:00:27:38:8b:82)
    Type: MS NLB heartbeat (0x886f)
v MS Network Load Balancing
    Signature: NLB Cluster Membership HeartBeat (0xc0de01bf)
    Version: 2.6
    Unique Host ID: 1
```

```
0000  03 bf c0 a8 03 d2 08 00  27 38 8b 82 88 6f bf 01   ········ '8···o··
0010  de c0 06 02 00 00 01 00  00 00 c0 a8 03 d2 c0 a8   ········ ········
0020  03 dc 00 00 00 00 01 00  03 00 e6 88 88 63 f1 e9   ········ ·····c··
0030  02 00 00 00 00 00 00 00  00 00 50 00 05 23 bb b1   ········ ··P··#··
0040  1b 23 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·#······ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff   ········ ········
00c0  ff ff ff ff ff 0f ff ff  ff ff ff ff ff 0f ff ff   ········ ········
00d0  ff ff ff ff ff 0f 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
01b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
01c0  00 00 00 00 00 00 ff ff  ff ff ff ff ff 0f ff ff   ········ ········
```

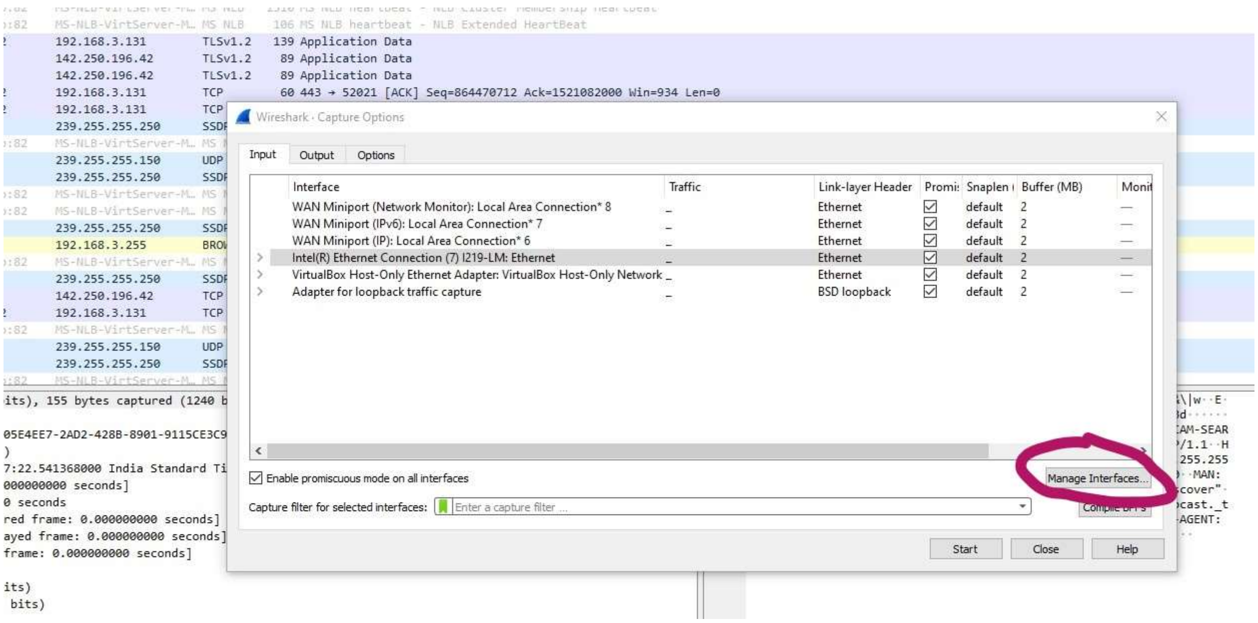
2. Check whether the network interface of your machine is in Promiscous mode. If it is not in promiscous mode, change it in to promiscous mode.

Step-1:- Go to Command Prompt And Check Promiscous mode



```
PS C:\Users\CDAC> Get-netadapter | Format-List -Property PromiscuousMode


PromiscuousMode : True

PromiscuousMode : False
```

Step-2:- Go to Open Wire Shark and Select Capture Option—> manage Interface



```
:82   MS-NLB-VirtServer-M… MS NLB    106 MS NLB heartbeat - NLB Extended HeartBeat
      192.168.3.131        TLSv1.2   139 Application Data
      142.250.196.42       TLSv1.2    89 Application Data
      142.250.196.42       TLSv1.2    89 Application Data
      192.168.3.131        TCP        60 443 → 52021 [ACK] Seq=864470712 Ack=1521082000 Win=934 Len=0
      192.168.3.131        TCP
      239.255.255.250      SSDP
:82   MS-NLB-VirtServer-M… MS
      239.255.255.150      UDP
      239.255.255.250      SSDP
:82   MS-NLB-VirtServer-M… MS
:82   MS-NLB-VirtServer-M… MS
      239.255.255.250      SSDP
      192.168.3.255        BROW
:82   MS-NLB-VirtServer-M… MS
      239.255.255.250      SSDP
      142.250.196.42       TCP
      192.168.3.131        TCP
:82   MS-NLB-VirtServer-M… MS
      239.255.255.150      UDP
      239.255.255.250      SSDP
its), 155 bytes captured (1240 b
05E4EE7-2AD2-428B-8901-9115CE3C9
)
7:22.541368000 India Standard Ti
000000000 seconds]
0 seconds
red frame: 0.000000000 seconds]
ayed frame: 0.000000000 seconds]
frame: 0.000000000 seconds]

its)
 bits)
```

Wireshark · Capture Options

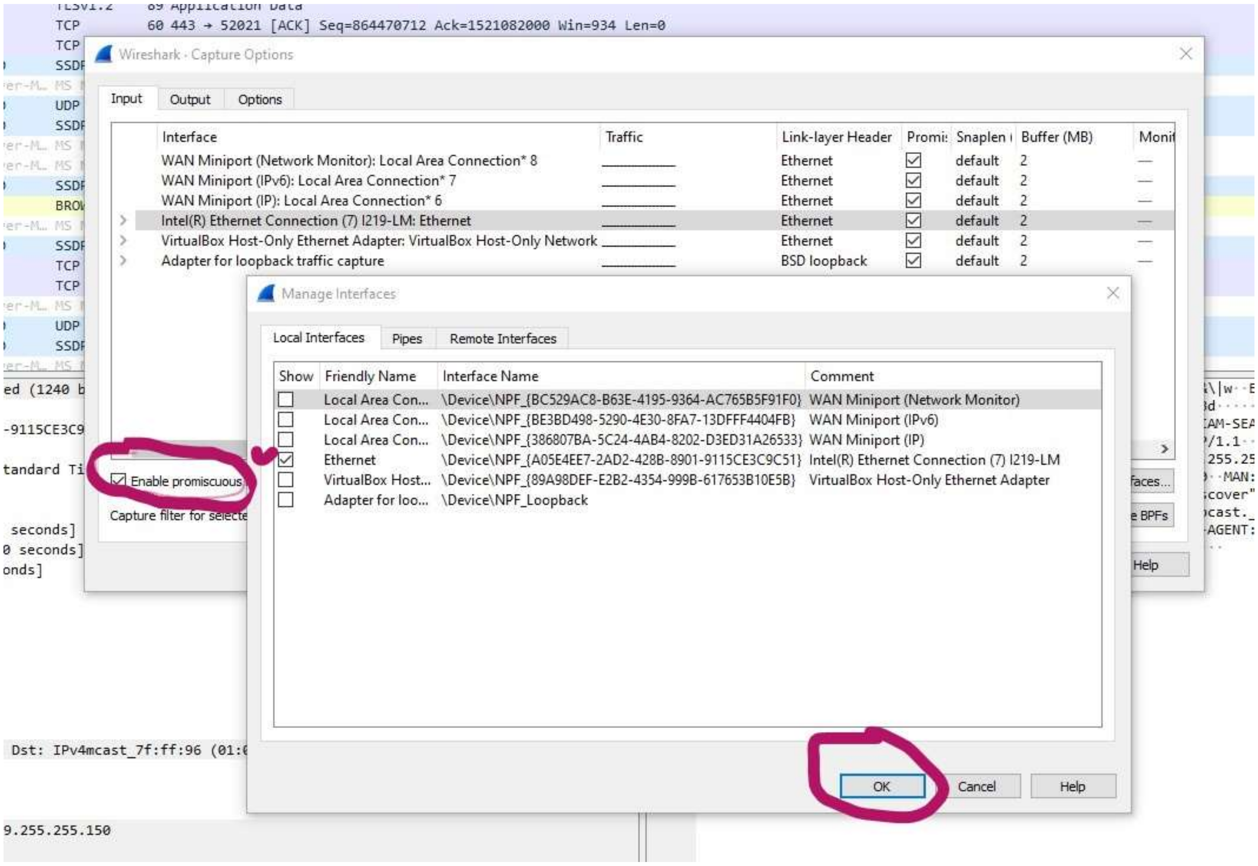
Input | Output | Options

	Interface	Traffic	Link-layer Header	Promi:	Snaplen	Buffer (MB)	Monit
	WAN Miniport (Network Monitor): Local Area Connection* 8		Ethernet	☑	default	2	—
	WAN Miniport (IPv6): Local Area Connection* 7		Ethernet	☑	default	2	—
	WAN Miniport (IP): Local Area Connection* 6		Ethernet	☑	default	2	—
>	Intel(R) Ethernet Connection (7) I219-LM: Ethernet		Ethernet	☑	default	2	—
>	VirtualBox Host-Only Ethernet Adapter: VirtualBox Host-Only Network		Ethernet	☑	default	2	—
>	Adapter for loopback traffic capture		BSD loopback	☑	default	2	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Step-3:- Enable promiscous and Click OK



```
TLSv1.2   89 Application Data
TCP       60 443 → 52021 [ACK] Seq=864470712 Ack=1521082000 Win=934 Len=0
TCP
SSDP
er-M… MS
UDP
SSDP
er-M… MS
er-M… MS
SSDP
BROW
er-M… MS
SSDP
TCP
TCP
er-M… MS
UDP
SSDP
er-M… MS
ed (1240 b
-9115CE3C9
tandard Ti
 seconds]
0 seconds]
onds]

Dst: IPv4mcast_7f:ff:96 (01:0

9.255.255.150
```

Wireshark · Capture Options

Input | Output | Options

	Interface	Traffic	Link-layer Header	Promi:	Snaplen	Buffer (MB)	Monit
	WAN Miniport (Network Monitor): Local Area Connection* 8		Ethernet	☑	default	2	—
	WAN Miniport (IPv6): Local Area Connection* 7		Ethernet	☑	default	2	—
	WAN Miniport (IP): Local Area Connection* 6		Ethernet	☑	default	2	—
>	Intel(R) Ethernet Connection (7) I219-LM: Ethernet		Ethernet	☑	default	2	—
>	VirtualBox Host-Only Ethernet Adapter: VirtualBox Host-Only Network		Ethernet	☑	default	2	—
>	Adapter for loopback traffic capture		BSD loopback	☑	default	2	—

☑ Enable promiscuous

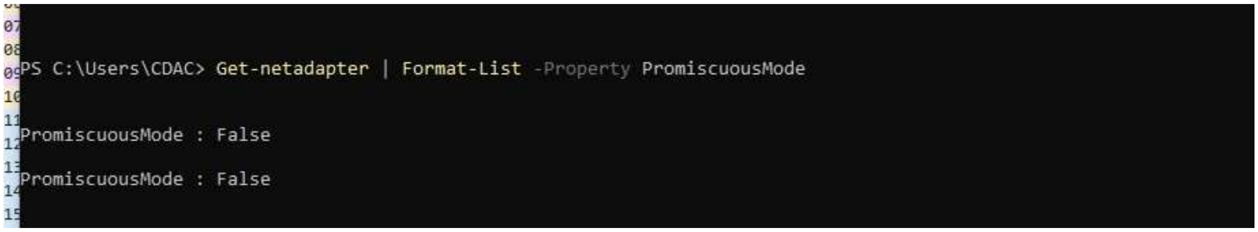
Capture filter for selecte

Manage Interfaces

Local Interfaces | Pipes | Remote Interfaces

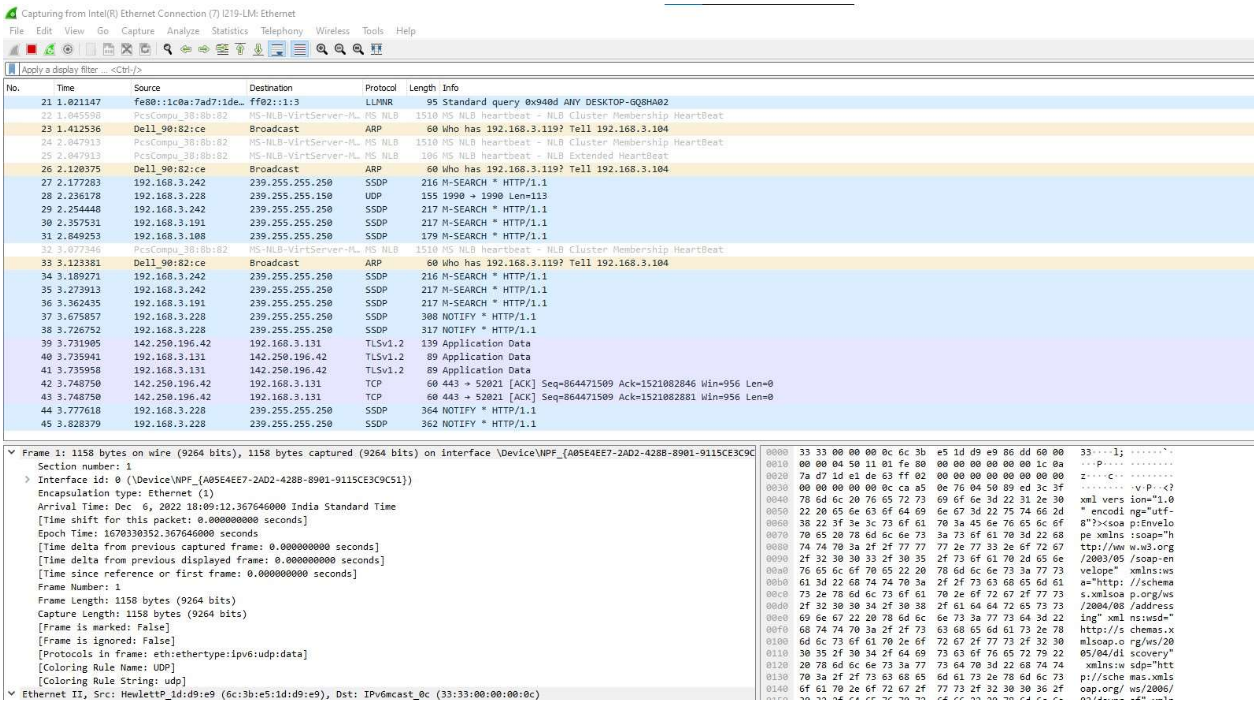
Show	Friendly Name	Interface Name	Comment
☐	Local Area Con…	\Device\NPF_{BC529AC8-B63E-4195-9364-AC765B5F91F0}	WAN Miniport (Network Monitor)
☐	Local Area Con…	\Device\NPF_{BE3BD498-5290-4E30-8FA7-13DFFF4404FB}	WAN Miniport (IPv6)
☐	Local Area Con…	\Device\NPF_{386807BA-5C24-4AB4-8202-D3ED31A26533}	WAN Miniport (IP)
☑	Ethernet	\Device\NPF_{A05E4EE7-2AD2-428B-8901-9115CE3C9C51}	Intel(R) Ethernet Connection (7) I219-LM
☐	VirtualBox Host…	\Device\NPF_{89A98DEF-E2B2-4354-999B-617653B10E5B}	VirtualBox Host-Only Ethernet Adapter
☐	Adapter for loo…	\Device\NPF_Loopback	

Step-3:- Check Changeable promiscous Mode on Command Prompt



```
PS C:\Users\CDAC> Get-netadapter | Format-List -Property PromiscuousMode

PromiscuousMode : False

PromiscuousMode : False
```

Step-4:- OPen Wire Shark and Run It



Capturing from Intel(R) Ethernet Connection (7) I219-LM: Ethernet
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

```
No.      Time        Source                Destination          Protocol  Length Info
      21 1.021147    fe80::1c0a:7ad7:1de…  ff02::1:3            LLMNR       95 Standard query 0x940d ANY DESKTOP-GQ8HA02
      22 1.045598    PcsCompu_38:8b:82     MS-NLB-VirtServer-M… MS NLB    1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
      23 1.412536    Dell_90:82:ce         Broadcast            ARP         60 Who has 192.168.3.119? Tell 192.168.3.104
      24 2.047913    PcsCompu_38:8b:82     MS-NLB-VirtServer-M… MS NLB    1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
      25 2.047913    PcsCompu_38:8b:82     MS-NLB-VirtServer-M… MS NLB     106 MS NLB heartbeat - NLB Extended HeartBeat
      26 2.120375    Dell_90:82:ce         Broadcast            ARP         60 Who has 192.168.3.119? Tell 192.168.3.104
      27 2.177283    192.168.3.242         239.255.255.250      SSDP       216 M-SEARCH * HTTP/1.1
      28 2.236178    192.168.3.228         239.255.255.150      UDP        155 1990 → 1990 Len=113
      29 2.254448    192.168.3.242         239.255.255.250      SSDP       217 M-SEARCH * HTTP/1.1
      30 2.357531    192.168.3.191         239.255.255.250      SSDP       217 M-SEARCH * HTTP/1.1
      31 2.849253    192.168.3.108         239.255.255.250      SSDP       179 M-SEARCH * HTTP/1.1
      32 3.077346    PcsCompu_38:8b:82     MS-NLB-VirtServer-M… MS NLB    1510 MS NLB heartbeat - NLB Cluster Membership HeartBeat
      33 3.123381    Dell_90:82:ce         Broadcast            ARP         60 Who has 192.168.3.119? Tell 192.168.3.104
      34 3.189271    192.168.3.242         239.255.255.250      SSDP       216 M-SEARCH * HTTP/1.1
      35 3.273913    192.168.3.242         239.255.255.250      SSDP       217 M-SEARCH * HTTP/1.1
      36 3.362435    192.168.3.191         239.255.255.250      SSDP       217 M-SEARCH * HTTP/1.1
      37 3.675857    192.168.3.228         239.255.255.250      SSDP       308 NOTIFY * HTTP/1.1
      38 3.726752    192.168.3.228         239.255.255.250      SSDP       317 NOTIFY * HTTP/1.1
      39 3.731905    142.250.196.42        192.168.3.131        TLSv1.2    139 Application Data
      40 3.735941    192.168.3.131         142.250.196.42       TLSv1.2     89 Application Data
      41 3.735958    192.168.3.131         142.250.196.42       TLSv1.2     89 Application Data
      42 3.748750    142.250.196.42        192.168.3.131        TCP         60 443 → 52021 [ACK] Seq=864471509 Ack=1521082846 Win=956 Len=0
      43 3.748750    142.250.196.42        192.168.3.131        TCP         60 443 → 52021 [ACK] Seq=864471509 Ack=1521082881 Win=956 Len=0
      44 3.777618    192.168.3.228         239.255.255.250      SSDP       364 NOTIFY * HTTP/1.1
      45 3.828379    192.168.3.228         239.255.255.250      SSDP       362 NOTIFY * HTTP/1.1
```

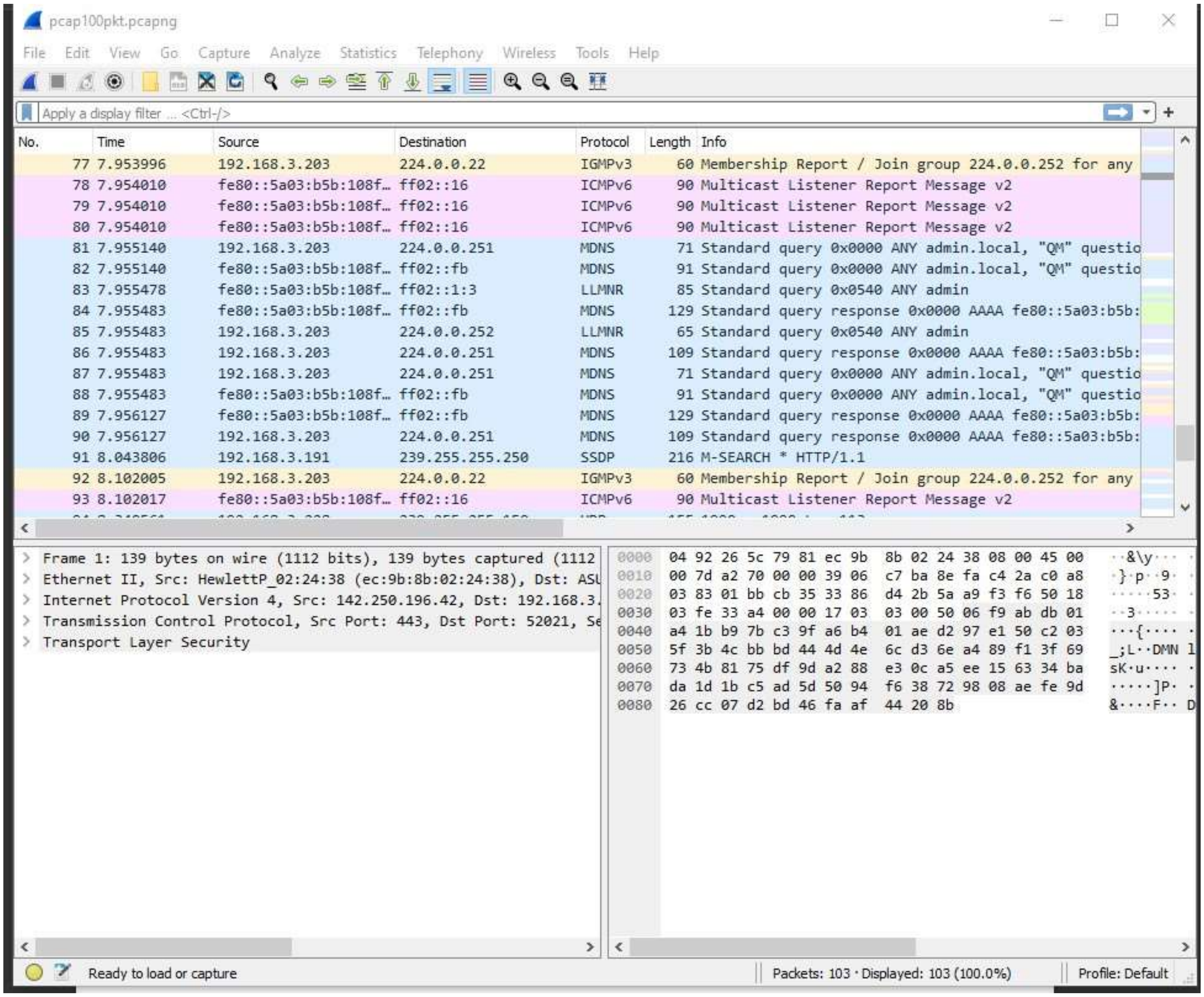
```
v Frame 1: 1158 bytes on wire (9264 bits), 1158 bytes captured (9264 bits) on interface \Device\NPF_{A05E4EE7-2AD2-428B-8901-9115CE3C9C
     Section number: 1
   > Interface id: 0 (\Device\NPF_{A05E4EE7-2AD2-428B-8901-9115CE3C9C51})
     Encapsulation type: Ethernet (1)
     Arrival Time: Dec  6, 2022 18:09:12.367646000 India Standard Time
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1670330352.367646000 seconds
     [Time delta from previous captured frame: 0.000000000 seconds]
     [Time delta from previous displayed frame: 0.000000000 seconds]
     [Time since reference or first frame: 0.000000000 seconds]
     Frame Number: 1
     Frame Length: 1158 bytes (9264 bits)
     Capture Length: 1158 bytes (9264 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ipv6:udp:data]
     [Coloring Rule Name: UDP]
     [Coloring Rule String: udp]
v Ethernet II, Src: HewlettP_1d:d9:e9 (6c:3b:e5:1d:d9:e9), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
```

```
0000  33 33 00 00 00 0c 6c 3b  e5 1d d9 e9 86 dd 60 00   33····l; ······`·
0010  00 00 04 50 11 01 fe 80  00 00 00 00 00 00 1c 0a   ···P···· ········
0020  7a d7 1d e1 de 63 ff 02  00 00 00 00 00 00 00 00   z····c·· ········
0030  00 00 00 00 00 0c ca a5  0e 76 04 50 89 ed 3c 3f   ········ ·v·P··<?
0040  78 6d 6c 20 76 65 72 73  69 6f 6e 3d 22 31 2e 30   xml vers ion="1.0
0050  22 20 65 6e 63 6f 64 69  6e 67 3d 22 75 74 66 2d   " encodi ng="utf-
0060  38 22 3f 3e 3c 73 6f 61  70 3a 45 6e 76 65 6c 6f   8"?><soa p:Envelo
0070  70 65 20 78 6d 6c 6e 73  3a 73 6f 61 70 3d 22 68   pe xmlns :soap="h
0080  74 74 70 3a 2f 2f 77 77  77 2e 77 33 2e 6f 72 67   ttp://ww w.w3.org
0090  2f 32 30 30 33 2f 30 35  2f 73 6f 61 70 2d 65 6e   /2003/05 /soap-en
00a0  76 65 6c 6f 70 65 22 20  78 6d 6c 6e 73 3a 77 73   velope"  xmlns:ws
00b0  61 3d 22 68 74 74 70 3a  2f 2f 73 63 68 65 6d 61   a="http: //schema
00c0  73 2e 78 6d 6c 73 6f 61  70 2e 6f 72 67 2f 77 73   s.xmlsoa p.org/ws
00d0  2f 32 30 30 34 2f 30 38  2f 61 64 64 72 65 73 73   /2004/08 /address
00e0  69 6e 67 22 20 78 6d 6c  6e 73 3a 77 73 64 3d 22   ing" xml ns:wsd="
00f0  68 74 74 70 3a 2f 2f 73  63 68 65 6d 61 73 2e 78   http://s chemas.x
0100  6d 6c 73 6f 61 70 2e 6f  72 67 2f 77 73 2f 32 30   mlsoap.o rg/ws/20
0110  30 35 2f 30 34 2f 64 69  73 63 6f 76 65 72 79 22   05/04/di scovery"
0120  20 78 6d 6c 6e 73 3a 77  73 64 70 3d 22 68 74 74    xmlns:w sdp="htt
0130  70 3a 2f 2f 73 63 68 65  6d 61 73 2e 78 6d 6c 73   p://sche mas.xmls
0140  6f 61 70 2e 6f 72 67 2f  77 73 2f 32 30 30 36 2f   oap.org/ ws/2006/
```

3. Configure the capture stop option of the wireshark in following settings

3.a) Stop after 100 packets and store in to a file “pcap100pkt”.

Open WireShark



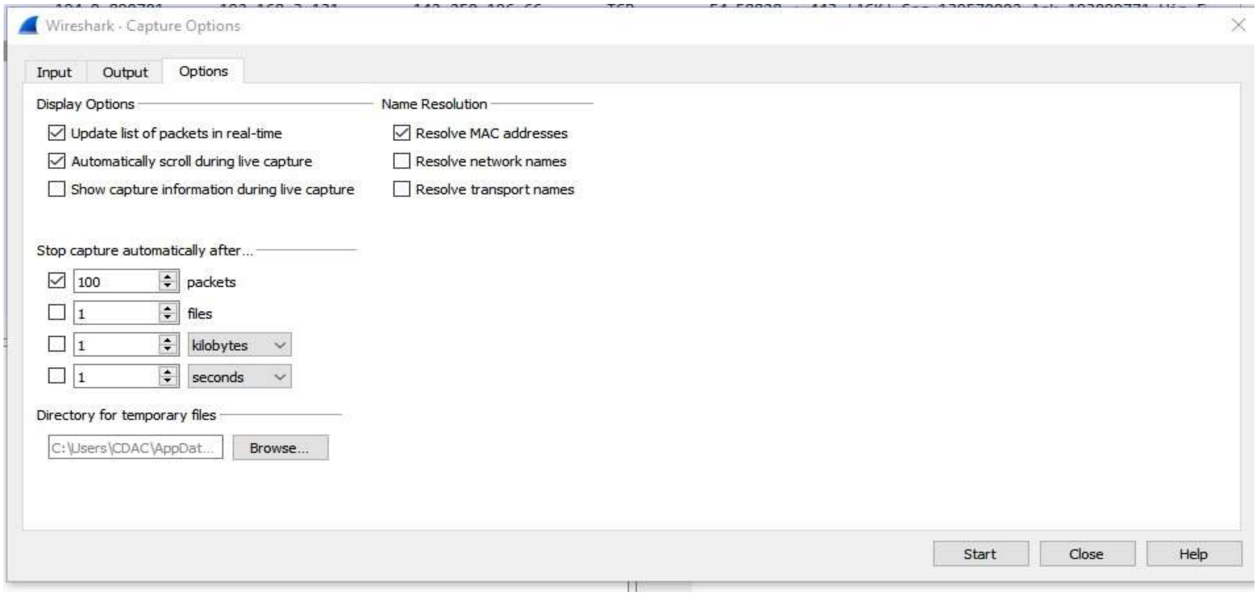
```
No.       Time        Source                   Destination       Protocol  Length Info
      77 7.953996    192.168.3.203            224.0.0.22        IGMPv3       60 Membership Report / Join group 224.0.0.252 for any
      78 7.954010    fe80::5a03:b5b:108f…     ff02::16          ICMPv6       90 Multicast Listener Report Message v2
      79 7.954010    fe80::5a03:b5b:108f…     ff02::16          ICMPv6       90 Multicast Listener Report Message v2
      80 7.954010    fe80::5a03:b5b:108f…     ff02::16          ICMPv6       90 Multicast Listener Report Message v2
      81 7.955140    192.168.3.203            224.0.0.251       MDNS         71 Standard query 0x0000 ANY admin.local, "QM" questio
      82 7.955140    fe80::5a03:b5b:108f…     ff02::fb          MDNS         91 Standard query 0x0000 ANY admin.local, "QM" questio
      83 7.955478    fe80::5a03:b5b:108f…     ff02::1:3         LLMNR        85 Standard query 0x0540 ANY admin
      84 7.955483    fe80::5a03:b5b:108f…     ff02::fb          MDNS        129 Standard query response 0x0000 AAAA fe80::5a03:b5b:
      85 7.955483    192.168.3.203            224.0.0.252       LLMNR        65 Standard query 0x0540 ANY admin
      86 7.955483    192.168.3.203            224.0.0.251       MDNS        109 Standard query response 0x0000 AAAA fe80::5a03:b5b:
      87 7.955483    192.168.3.203            224.0.0.251       MDNS         71 Standard query 0x0000 ANY admin.local, "QM" questio
      88 7.955483    fe80::5a03:b5b:108f…     ff02::fb          MDNS         91 Standard query 0x0000 ANY admin.local, "QM" questio
      89 7.956127    fe80::5a03:b5b:108f…     ff02::fb          MDNS        129 Standard query response 0x0000 AAAA fe80::5a03:b5b:
      90 7.956127    192.168.3.203            224.0.0.251       MDNS        109 Standard query response 0x0000 AAAA fe80::5a03:b5b:
      91 8.043806    192.168.3.191            239.255.255.250   SSDP        216 M-SEARCH * HTTP/1.1
      92 8.102005    192.168.3.203            224.0.0.22        IGMPv3       60 Membership Report / Join group 224.0.0.252 for any
      93 8.102017    fe80::5a03:b5b:108f…     ff02::16          ICMPv6       90 Multicast Listener Report Message v2
```

```
> Frame 1: 139 bytes on wire (1112 bits), 139 bytes captured (1112
> Ethernet II, Src: HewlettP_02:24:38 (ec:9b:8b:02:24:38), Dst: ASU
> Internet Protocol Version 4, Src: 142.250.196.42, Dst: 192.168.3.
> Transmission Control Protocol, Src Port: 443, Dst Port: 52021, Se
> Transport Layer Security
```

```
0000  04 92 26 5c 79 81 ec 9b  8b 02 24 38 08 00 45 00   ··&\y···
0010  00 7d a2 70 00 00 39 06  c7 ba 8e fa c4 2a c0 a8   ·}·p··9·
0020  03 83 01 bb cb 35 33 86  d4 2b 5a a9 f3 f6 50 18   ·····53·
0030  03 fe 33 a4 00 00 17 03  03 00 50 06 f9 ab db 01   ··3·····
0040  a4 1b b9 7b c3 9f a6 b4  01 ae d2 97 e1 50 c2 03   ···{····
0050  5f 3b 4c bb bd 44 4d 4e  6c d3 6e a4 89 f1 3f 69   _;L··DMN
0060  73 4b 81 75 df 9d a2 88  e3 0c a5 ee 15 63 34 ba   sK·u····
0070  da 1d 1b c5 ad 5d 50 94  f6 38 72 98 08 ae fe 9d   ·····]P·
0080  26 cc 07 d2 bd 46 fa af  44 20 8b                  &····F··
```

Go to Capture Option —-->Right Click —--->Select Option and Set packets=100

Start the WireShark
Save the file = pcap100pkt.pcap



Wireshark · Capture Options

Display Options

- ☑ Update list of packets in real-time
- ☑ Automatically scroll during live capture
- ☐ Show capture information during live capture

Name Resolution

- ☑ Resolve MAC addresses
- ☐ Resolve network names
- ☐ Resolve transport names

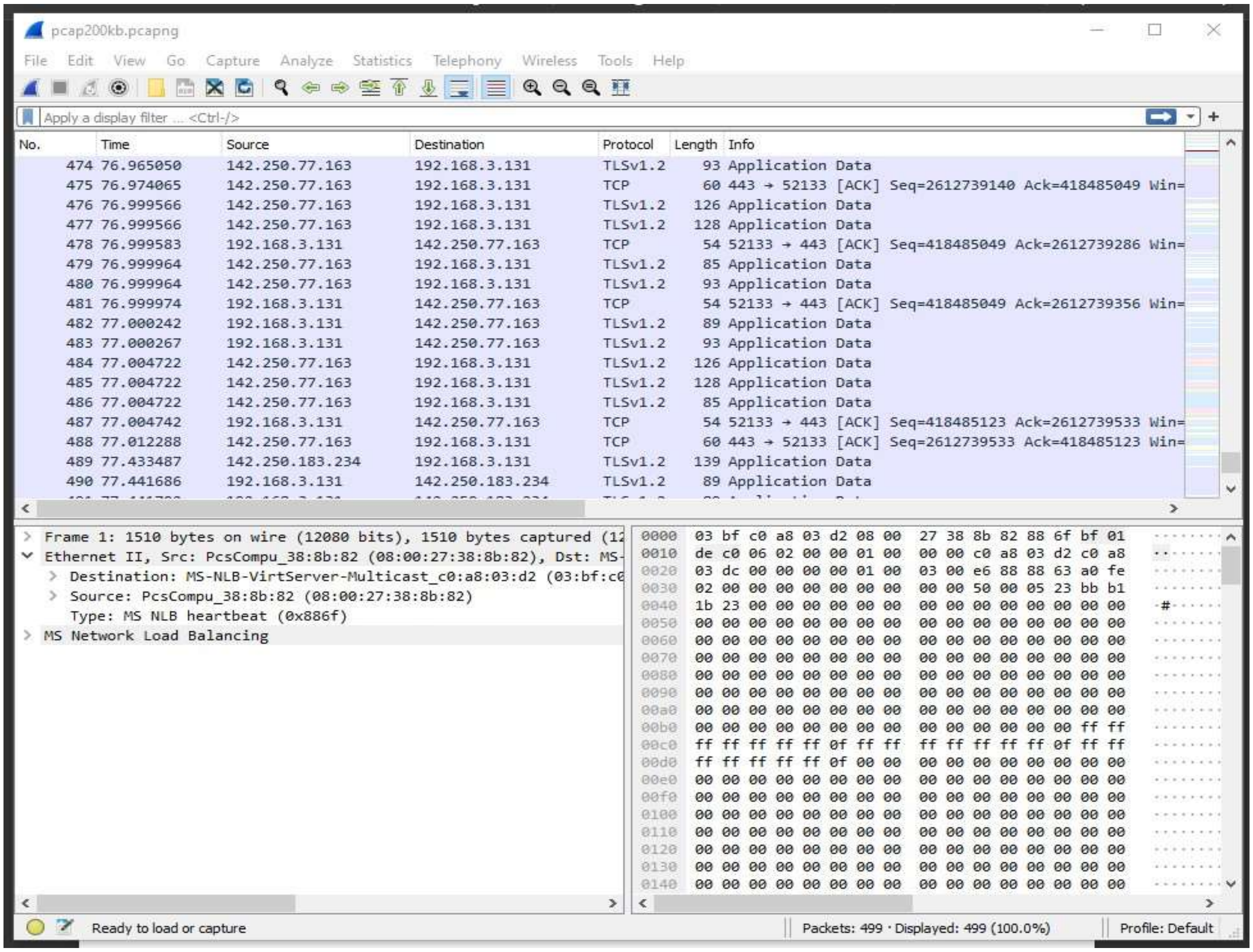
Stop capture automatically after...

- ☑ 100 packets
- ☐ 1 files
- ☐ 1 kilobytes
- ☐ 1 seconds

Directory for temporary files

C:\Users\CDAC\AppDat...

3.b)Stop after 200 Kb and store in to a file "pcap200kb".
Open the Wire Shark



pcap200kb.pcapng

```
No.    Time       Source           Destination      Protocol  Length Info
   474 76.965050  142.250.77.163   192.168.3.131    TLSv1.2   93 Application Data
   475 76.974065  142.250.77.163   192.168.3.131    TCP       60 443 → 52133 [ACK] Seq=2612739140 Ack=418485049 Win=
   476 76.999566  142.250.77.163   192.168.3.131    TLSv1.2  126 Application Data
   477 76.999566  142.250.77.163   192.168.3.131    TLSv1.2  128 Application Data
   478 76.999583  192.168.3.131    142.250.77.163   TCP       54 52133 → 443 [ACK] Seq=418485049 Ack=2612739286 Win=
   479 76.999964  142.250.77.163   192.168.3.131    TLSv1.2   85 Application Data
   480 76.999964  142.250.77.163   192.168.3.131    TLSv1.2   93 Application Data
   481 76.999974  192.168.3.131    142.250.77.163   TCP       54 52133 → 443 [ACK] Seq=418485049 Ack=2612739356 Win=
   482 77.000242  192.168.3.131    142.250.77.163   TLSv1.2   89 Application Data
   483 77.000267  192.168.3.131    142.250.77.163   TLSv1.2   93 Application Data
   484 77.004722  142.250.77.163   192.168.3.131    TLSv1.2  126 Application Data
   485 77.004722  142.250.77.163   192.168.3.131    TLSv1.2  128 Application Data
   486 77.004722  142.250.77.163   192.168.3.131    TLSv1.2   85 Application Data
   487 77.004742  192.168.3.131    142.250.77.163   TCP       54 52133 → 443 [ACK] Seq=418485123 Ack=2612739533 Win=
   488 77.012288  142.250.77.163   192.168.3.131    TCP       60 443 → 52133 [ACK] Seq=2612739533 Ack=418485123 Win=
   489 77.433487  142.250.183.234  192.168.3.131    TLSv1.2  139 Application Data
   490 77.441686  192.168.3.131    142.250.183.234  TLSv1.2   89 Application Data
```

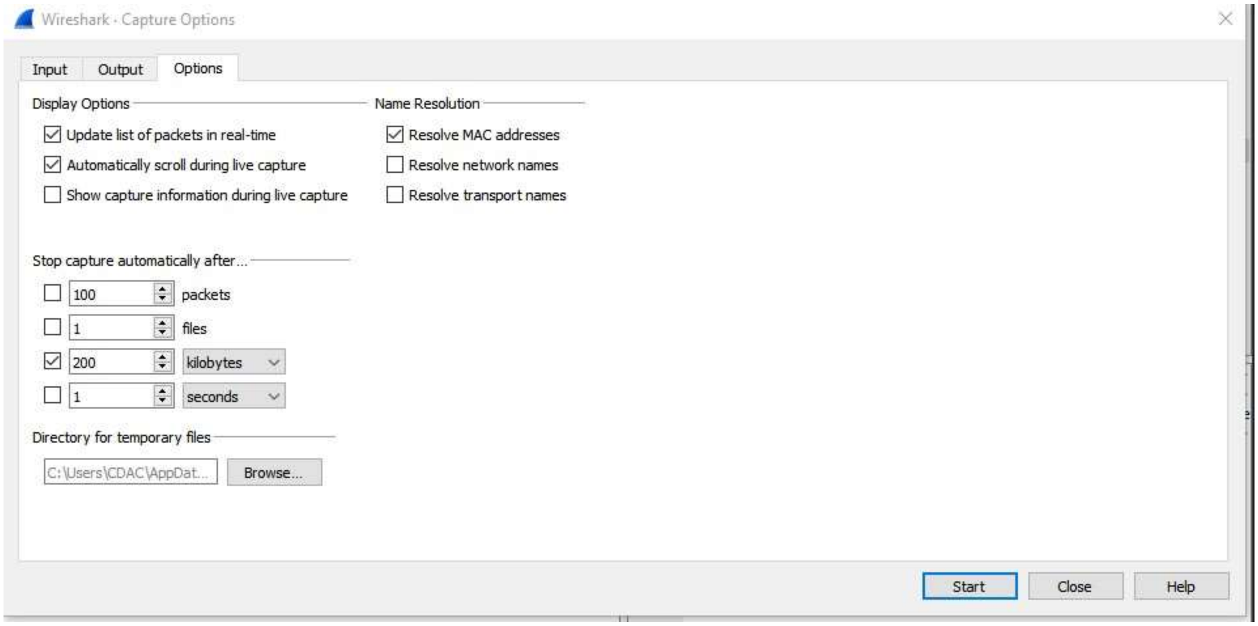
```
> Frame 1: 1510 bytes on wire (12080 bits), 1510 bytes captured (12
v Ethernet II, Src: PcsCompu_38:8b:82 (08:00:27:38:8b:82), Dst: MS-
  > Destination: MS-NLB-VirtServer-Multicast_c0:a8:03:d2 (03:bf:c0
  > Source: PcsCompu_38:8b:82 (08:00:27:38:8b:82)
    Type: MS NLB heartbeat (0x886f)
> MS Network Load Balancing
```

```
0000  03 bf c0 a8 03 d2 08 00  27 38 8b 82 88 6f bf 01   ........
0010  de c0 06 02 00 00 01 00  00 00 c0 a8 03 d2 c0 a8   ........
0020  03 dc 00 00 00 00 01 00  03 00 e6 88 88 63 a0 fe   ........
0030  02 00 00 00 00 00 00 00  00 00 50 00 05 23 bb b1   ........
0040  1b 23 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .#......
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 ff ff   ........
00c0  ff ff ff ff ff 0f ff ff  ff ff ff ff ff 0f ff ff   ........
00d0  ff ff ff ff ff 0f 00 00  00 00 00 00 00 00 00 00   ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........
```

Ready to load or capture | Packets: 499 · Displayed: 499 (100.0%) | Profile: Default

Go to Capture Option ——>Right Click ——-->Select Option and Set Size=200kb

Start the WireShark
Save the file = pcap200kb.pcap



Display Options

☑ Update list of packets in real-time
☑ Automatically scroll during live capture
☐ Show capture information during live capture

Name Resolution

☑ Resolve MAC addresses
☐ Resolve network names
☐ Resolve transport names

Stop capture automatically after...

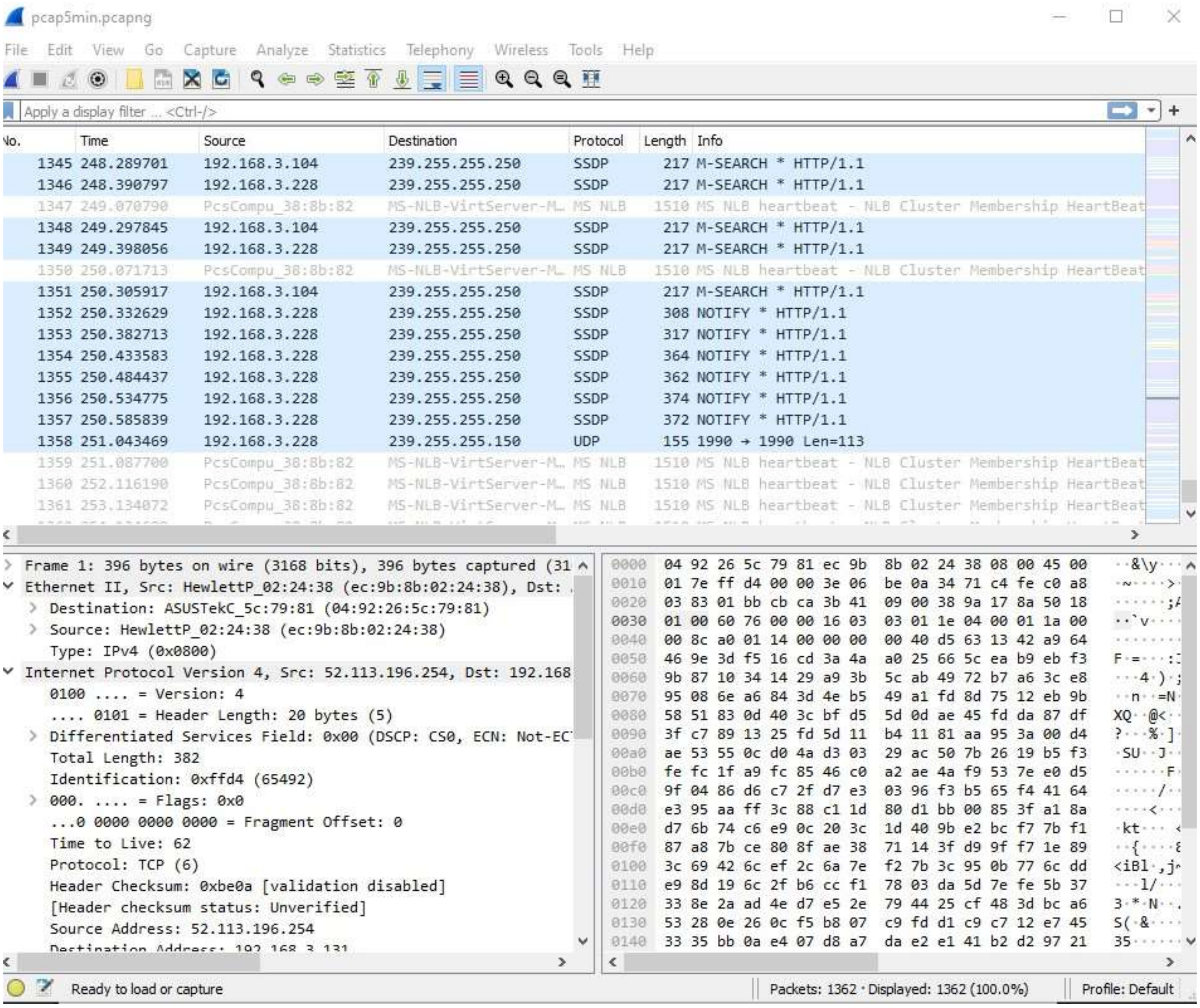
☐ 100 packets
☐ 1 files
☑ 200 kilobytes
☐ 1 seconds

Directory for temporary files

C:\Users\CDAC\AppDat... Browse...

3.c) Stop after 5 minutes and store in to a file “pcap5min” .

Open the Wire Shark


pcap5min.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1345	248.289701	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1346	248.390797	192.168.3.228	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1347	249.070790	PcsCompu_38:8b:82	MS-NLB-VirtServer-M…	MS NLB	1510	MS NLB heartbeat - NLB Cluster Membership HeartBeat
1348	249.297845	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1349	249.398056	192.168.3.228	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1350	250.071713	PcsCompu_38:8b:82	MS-NLB-VirtServer-M…	MS NLB	1510	MS NLB heartbeat - NLB Cluster Membership HeartBeat
1351	250.305917	192.168.3.104	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1352	250.332629	192.168.3.228	239.255.255.250	SSDP	308	NOTIFY * HTTP/1.1
1353	250.382713	192.168.3.228	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
1354	250.433583	192.168.3.228	239.255.255.250	SSDP	364	NOTIFY * HTTP/1.1
1355	250.484437	192.168.3.228	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
1356	250.534775	192.168.3.228	239.255.255.250	SSDP	374	NOTIFY * HTTP/1.1
1357	250.585839	192.168.3.228	239.255.255.250	SSDP	372	NOTIFY * HTTP/1.1
1358	251.043469	192.168.3.228	239.255.255.150	UDP	155	1990 → 1990 Len=113
1359	251.087700	PcsCompu_38:8b:82	MS-NLB-VirtServer-M…	MS NLB	1510	MS NLB heartbeat - NLB Cluster Membership HeartBeat
1360	252.116190	PcsCompu_38:8b:82	MS-NLB-VirtServer-M…	MS NLB	1510	MS NLB heartbeat - NLB Cluster Membership HeartBeat
1361	253.134072	PcsCompu_38:8b:82	MS-NLB-VirtServer-M…	MS NLB	1510	MS NLB heartbeat - NLB Cluster Membership HeartBeat

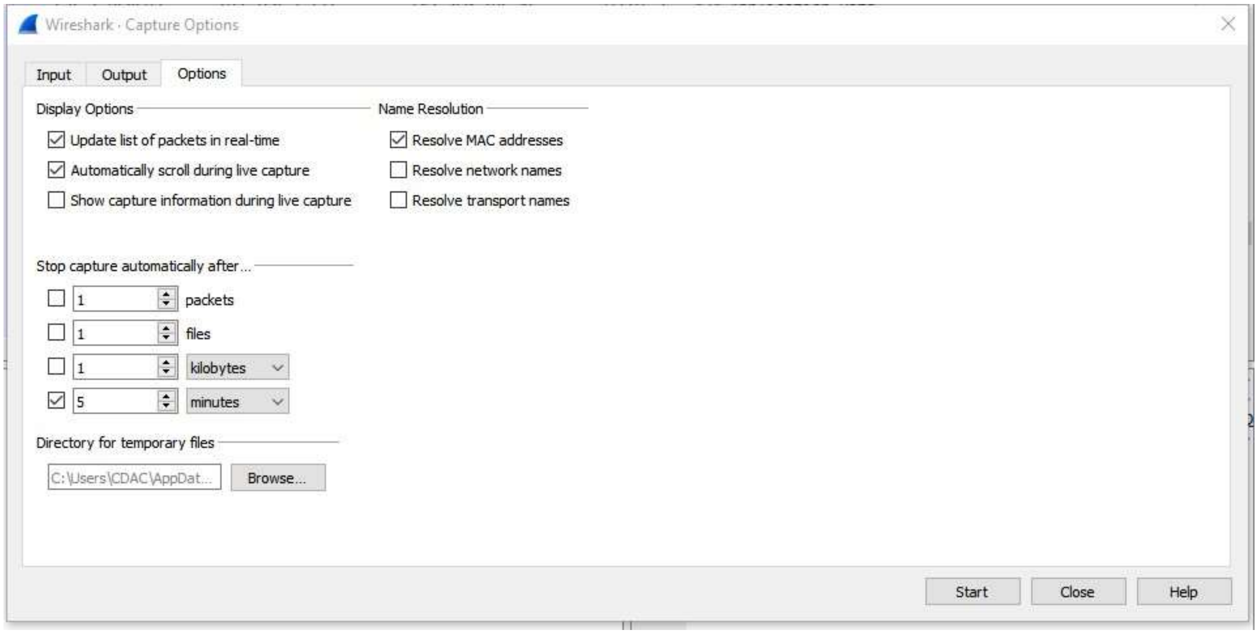
```
> Frame 1: 396 bytes on wire (3168 bits), 396 bytes captured (31
v Ethernet II, Src: HewlettP_02:24:38 (ec:9b:8b:02:24:38), Dst: .
    > Destination: ASUSTekC_5c:79:81 (04:92:26:5c:79:81)
    > Source: HewlettP_02:24:38 (ec:9b:8b:02:24:38)
      Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 52.113.196.254, Dst: 192.168
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-EC
      Total Length: 382
      Identification: 0xffd4 (65492)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 62
      Protocol: TCP (6)
      Header Checksum: 0xbe0a [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 52.113.196.254
      Destination Address: 192.168.3.131
```

```
0000  04 92 26 5c 79 81 ec 9b  8b 02 24 38 08 00 45 00   ··&\y···
0010  01 7e ff d4 00 00 3e 06  be 0a 34 71 c4 fe c0 a8   ·~····>·
0020  03 83 01 bb cb ca 3b 41  09 00 38 9a 17 8a 50 18   ······;A
0030  01 00 60 76 00 00 16 03  03 01 1e 04 00 01 1a 00   ··`v····
0040  00 8c a0 01 14 00 00 00  00 40 d5 63 13 42 a9 64   ········
0050  46 9e 3d f5 16 cd 3a 4a  a0 25 66 5c ea b9 eb f3   F·=···:J
0060  9b 87 10 34 14 29 a9 3b  5c ab 49 72 b7 a6 3c e8   ···4·)·;
0070  95 08 6e a6 84 3d 4e b5  49 a1 fd 8d 75 12 eb 9b   ··n··=N·
0080  58 51 83 0d 40 3c bf d5  5d 0d ae 45 fd da 87 df   XQ··@<··
0090  3f c7 89 13 25 fd 5d 11  b4 11 81 aa 95 3a 00 d4   ?···%·]·
00a0  ae 53 55 0c d0 4a d3 03  29 ac 50 7b 26 19 b5 f3   ·SU··J··
00b0  fe fc 1f a9 fc 85 46 c0  a2 ae 4a f9 53 7e e0 d5   ······F·
00c0  9f 04 86 d6 c7 2f d7 e3  03 96 f3 b5 65 f4 41 64   ·····/··
00d0  e3 95 aa ff 3c 88 c1 1d  80 d1 bb 00 85 3f a1 8a   ····<···
00e0  d7 6b 74 c6 e9 0c 20 3c  1d 40 9b e2 bc f7 7b f1   ·kt··· <
00f0  87 a8 7b ce 80 8f ae 38  71 14 3f d9 9f f7 1e 89   ··{····8
0100  3c 69 42 6c ef 2c 6a 7e  f2 7b 3c 95 0b 77 6c dd   <iBl·,j~
0110  e9 8d 19 6c 2f b6 cc f1  78 03 da 5d 7e fe 5b 37   ···l/···
0120  33 8e 2a ad 4e d7 e5 2e  79 44 25 cf 48 3d bc a6   3·*·N··.
0130  53 28 0e 26 0c f5 b8 07  c9 fd d1 c9 c7 12 e7 45   S(·&····
0140  33 35 bb 0a e4 07 d8 a7  da e2 e1 41 b2 d2 97 21   35······
```

Ready to load or capture | Packets: 1362 · Displayed: 1362 (100.0%) | Profile: Default

Go to Capture Option —-->Right Click —--->Select Option and Set time=5 min

Start the WireShark
Save the file = pcap5min.pcap



Wireshark · Capture Options

Input | Output | Options

Display Options

☑ Update list of packets in real-time

☑ Automatically scroll during live capture

□ Show capture information during live capture

Name Resolution

☑ Resolve MAC addresses

□ Resolve network names

□ Resolve transport names

Stop capture automatically after...

□ 1 packets

□ 1 files

□ 1 kilobytes

☑ 5 minutes

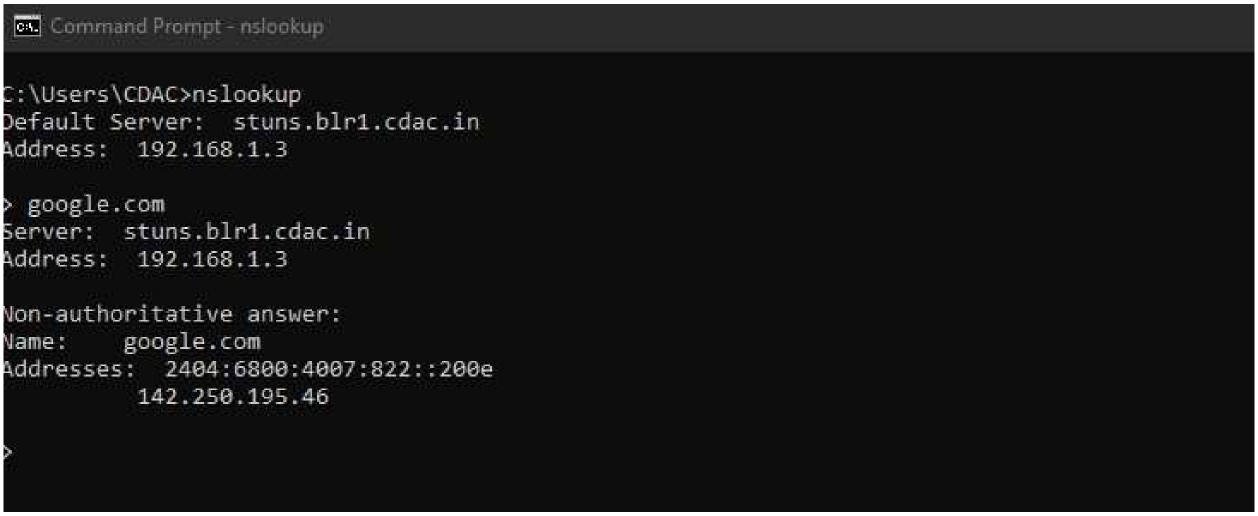
Directory for temporary files

C:\Users\CDAC\AppDat... Browse...

Start Close Help

4. Capture live traffic from a particulat host (e.g from www.google.com) and store the captured file as “pcaphost.pcap”.

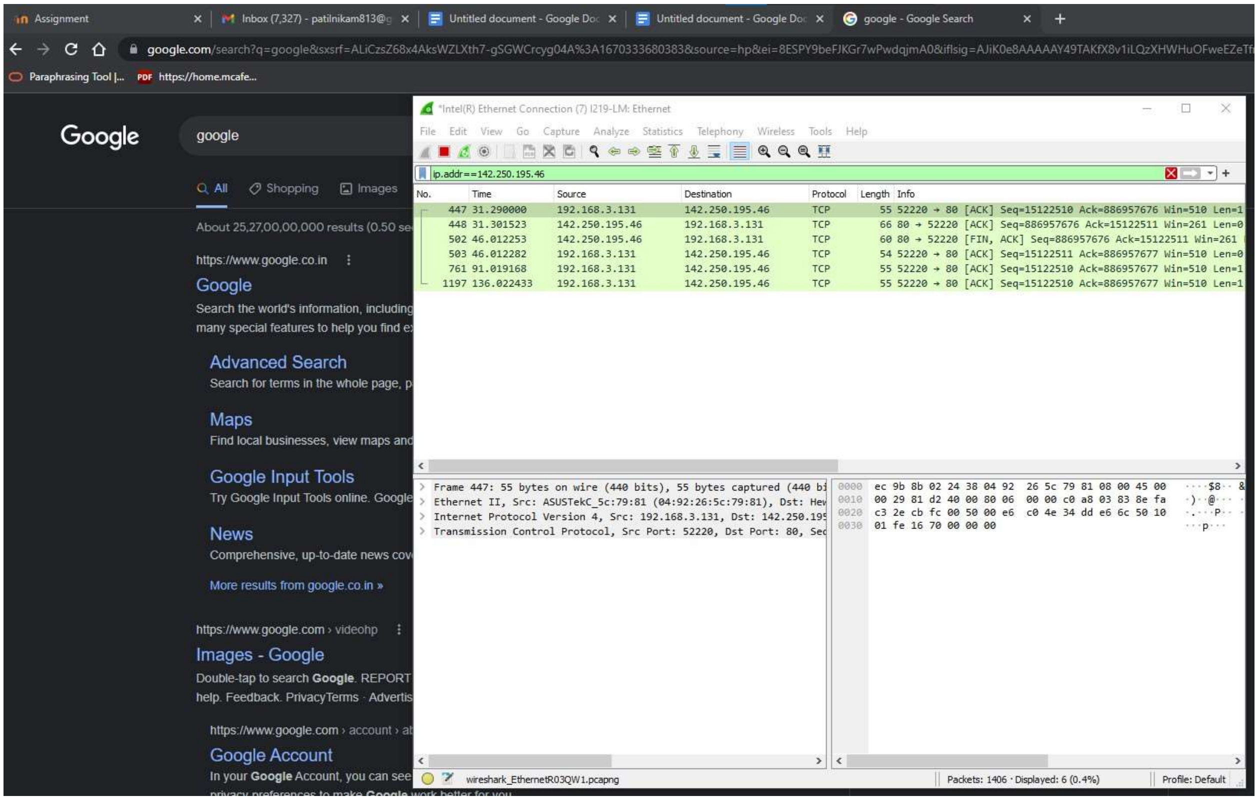
Step-1:- Go to command prom pt and check the host(www.google.com) IP



Command Prompt - nslookup

```
C:\Users\CDAC>nslookup
Default Server:  stuns.blr1.cdac.in
Address:  192.168.1.3

> google.com
Server:  stuns.blr1.cdac.in
Address:  192.168.1.3

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4007:822::200e
          142.250.195.46

>
```

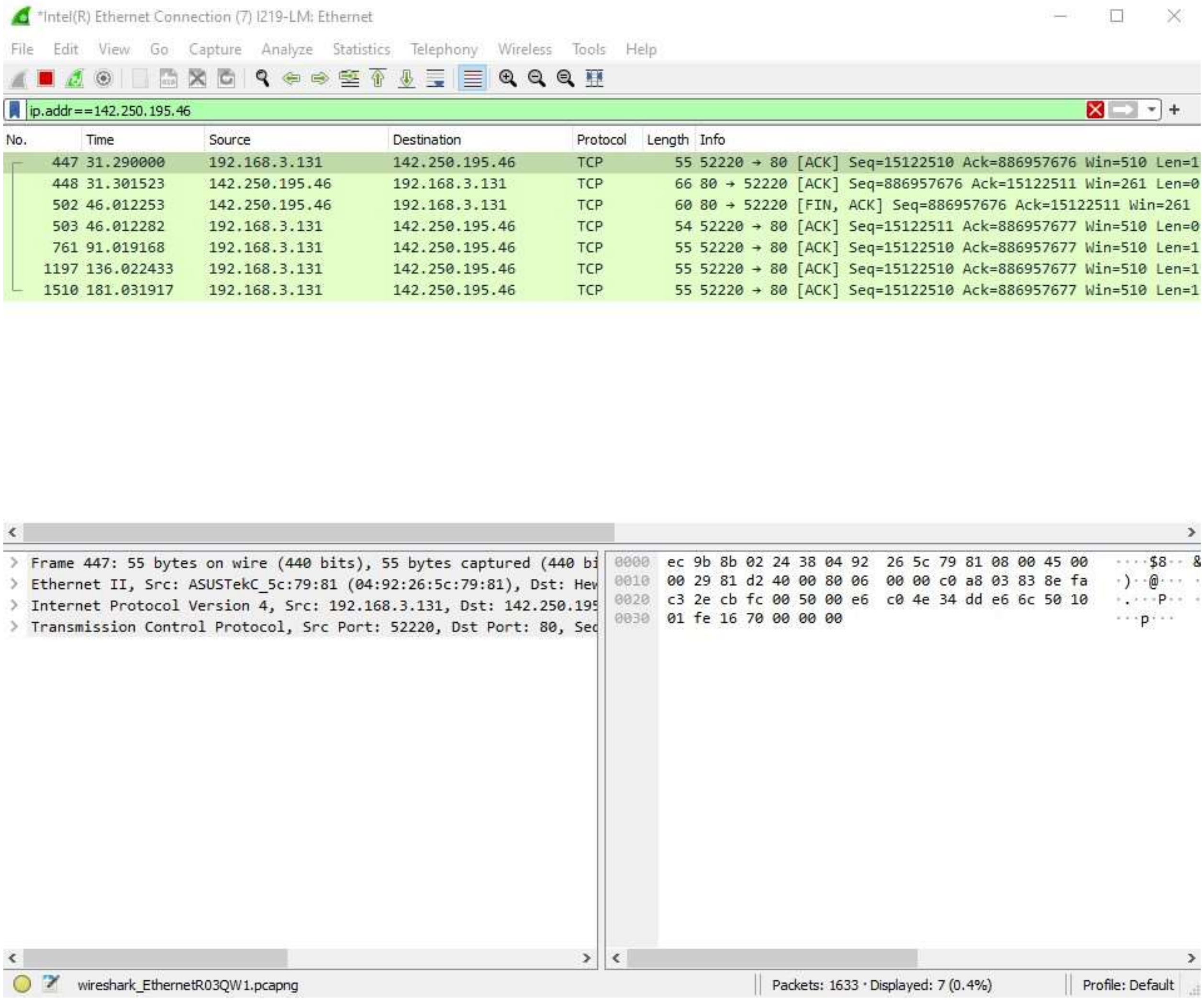
Step-2:- OPen the WireShark as well as run the Google.com on web Browser



```
ip.addr==142.250.195.46

No.   Time        Source          Destination     Protocol Length Info
  447 31.290000   192.168.3.131   142.250.195.46  TCP      55 52220 → 80 [ACK] Seq=15122510 Ack=886957676 Win=510 Len=1
  448 31.301523   142.250.195.46  192.168.3.131   TCP      66 80 → 52220 [ACK] Seq=886957676 Ack=15122511 Win=261 Len=0
  502 46.012253   142.250.195.46  192.168.3.131   TCP      60 80 → 52220 [FIN, ACK] Seq=886957676 Ack=15122511 Win=261
  503 46.012282   192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [ACK] Seq=15122511 Ack=886957677 Win=510 Len=0
  761 91.019168   192.168.3.131   142.250.195.46  TCP      55 52220 → 80 [ACK] Seq=15122510 Ack=886957677 Win=510 Len=1
 1197 136.022433  192.168.3.131   142.250.195.46  TCP      55 52220 → 80 [ACK] Seq=15122510 Ack=886957677 Win=510 Len=1

> Frame 447: 55 bytes on wire (440 bits), 55 bytes captured (440 bi
> Ethernet II, Src: ASUSTekC_5c:79:81 (04:92:26:5c:79:81), Dst: Hew
> Internet Protocol Version 4, Src: 192.168.3.131, Dst: 142.250.195
> Transmission Control Protocol, Src Port: 52220, Dst Port: 80, Seq

0000  ec 9b 8b 02 24 38 04 92  26 5c 79 81 08 00 45 00   ····$8·· &
0010  00 29 81 d2 40 00 80 06  00 00 c0 a8 03 83 8e fa   ·)··@··· ·
0020  c3 2e cb fc 00 50 00 e6  c0 4e 34 dd e6 6c 50 10   ·.···P·· ·
0030  01 fe 16 70 00 00 00                               ···p···

wireshark_EthernetR03QW1.pcapng    Packets: 1406 · Displayed: 6 (0.4%)    Profile: Default
```

*Intel(R) Ethernet Connection (7) I219-LM: Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
google - Google Search

Step-3:- Now Capture The Live traffic through-ip.addr=-142.250.195.46


*Intel(R) Ethernet Connection (7) I219-LM: Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==142.250.195.46

```
No.     Time        Source           Destination      Protocol  Length Info
   447 31.290000    192.168.3.131    142.250.195.46   TCP       55 52220 → 80 [ACK] Seq=15122510 Ack=886957676 Win=510 Len=1
   448 31.301523    142.250.195.46   192.168.3.131    TCP       66 80 → 52220 [ACK] Seq=886957676 Ack=15122511 Win=261 Len=0
   502 46.012253    142.250.195.46   192.168.3.131    TCP       60 80 → 52220 [FIN, ACK] Seq=886957676 Ack=15122511 Win=261
   503 46.012282    192.168.3.131    142.250.195.46   TCP       54 52220 → 80 [ACK] Seq=15122511 Ack=886957677 Win=510 Len=0
   761 91.019168    192.168.3.131    142.250.195.46   TCP       55 52220 → 80 [ACK] Seq=15122510 Ack=886957677 Win=510 Len=1
  1197 136.022433   192.168.3.131    142.250.195.46   TCP       55 52220 → 80 [ACK] Seq=15122510 Ack=886957677 Win=510 Len=1
  1510 181.031917   192.168.3.131    142.250.195.46   TCP       55 52220 → 80 [ACK] Seq=15122510 Ack=886957677 Win=510 Len=1
```

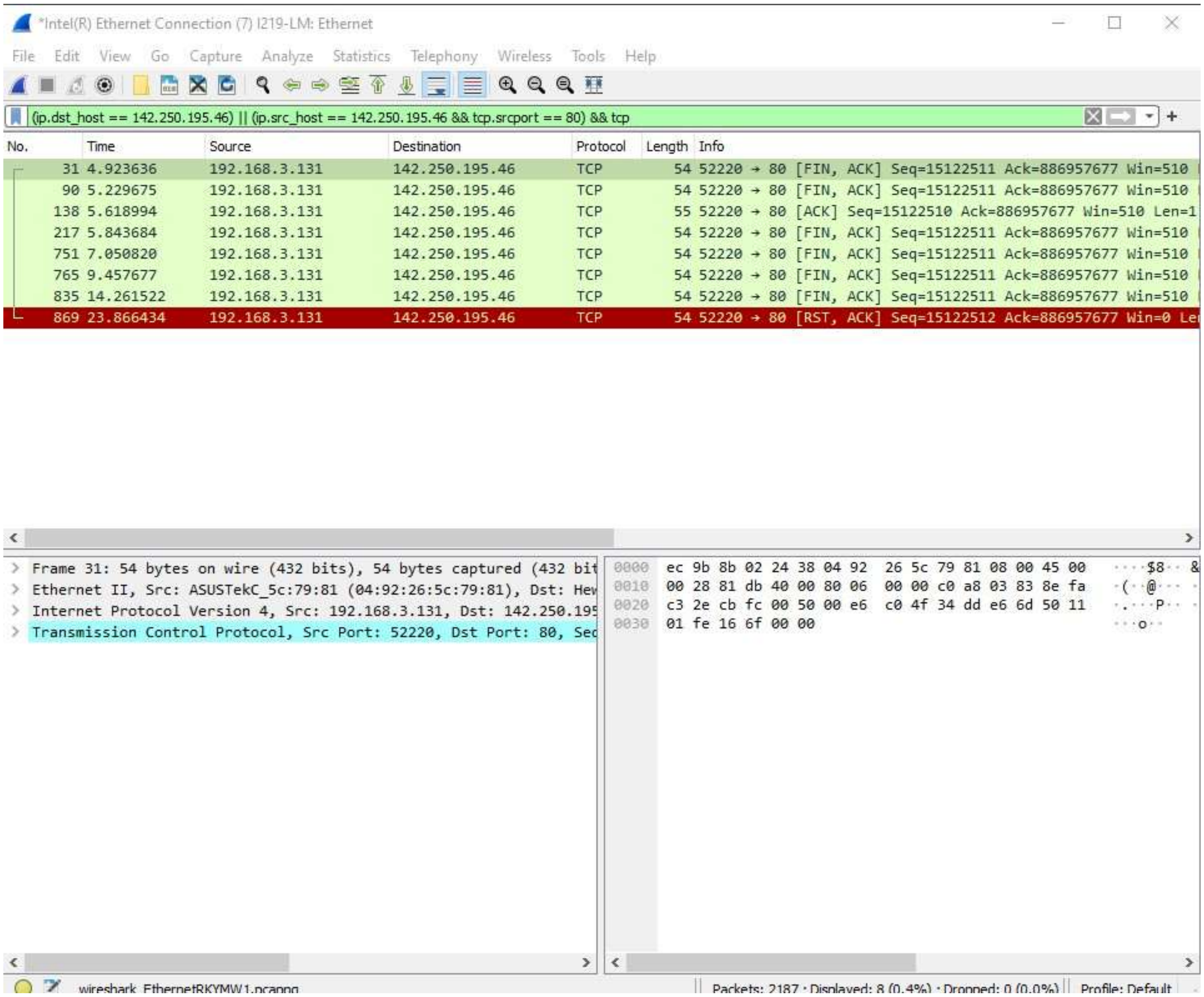
```
> Frame 447: 55 bytes on wire (440 bits), 55 bytes captured (440 bi
> Ethernet II, Src: ASUSTekC_5c:79:81 (04:92:26:5c:79:81), Dst: Hew
> Internet Protocol Version 4, Src: 192.168.3.131, Dst: 142.250.195
> Transmission Control Protocol, Src Port: 52220, Dst Port: 80, Sec
```

```
0000  ec 9b 8b 02 24 38 04 92  26 5c 79 81 08 00 45 00   ····$8·· &
0010  00 29 81 d2 40 00 80 06  00 00 c0 a8 03 83 8e fa   ·)··@··· ·
0020  c3 2e cb fc 00 50 00 e6  c0 4e 34 dd e6 6c 50 10   ·.···P·· ·
0030  01 fe 16 70 00 00 00                               ···p···
```

wireshark_EthernetR03QW1.pcapng | Packets: 1633 · Displayed: 7 (0.4%) | Profile: Default

5. Capture live traffic from a port (e.g port 80) and store the captured file as “pcapport.pcap”.

Step-1:- Capture the Live Traffic on port 80 using- (ip.dst_host==142.250.195.46)||(ip.src_host==142.250.195.46&&tcp.srcport==80)&&tcp



*Intel(R) Ethernet Connection (7) I219-LM: Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(ip.dst_host == 142.250.195.46) || (ip.src_host == 142.250.195.46 && tcp.srcport == 80) && tcp
```

```
No.   Time       Source          Destination     Protocol Length Info
   31 4.923636   192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [FIN, ACK] Seq=15122511 Ack=886957677 Win=510
   90 5.229675   192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [FIN, ACK] Seq=15122511 Ack=886957677 Win=510
  138 5.618994   192.168.3.131   142.250.195.46  TCP      55 52220 → 80 [ACK] Seq=15122510 Ack=886957677 Win=510 Len=1
  217 5.843684   192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [FIN, ACK] Seq=15122511 Ack=886957677 Win=510
  751 7.050820   192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [FIN, ACK] Seq=15122511 Ack=886957677 Win=510
  765 9.457677   192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [FIN, ACK] Seq=15122511 Ack=886957677 Win=510
  835 14.261522  192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [FIN, ACK] Seq=15122511 Ack=886957677 Win=510
  869 23.866434  192.168.3.131   142.250.195.46  TCP      54 52220 → 80 [RST, ACK] Seq=15122512 Ack=886957677 Win=0 Le
```

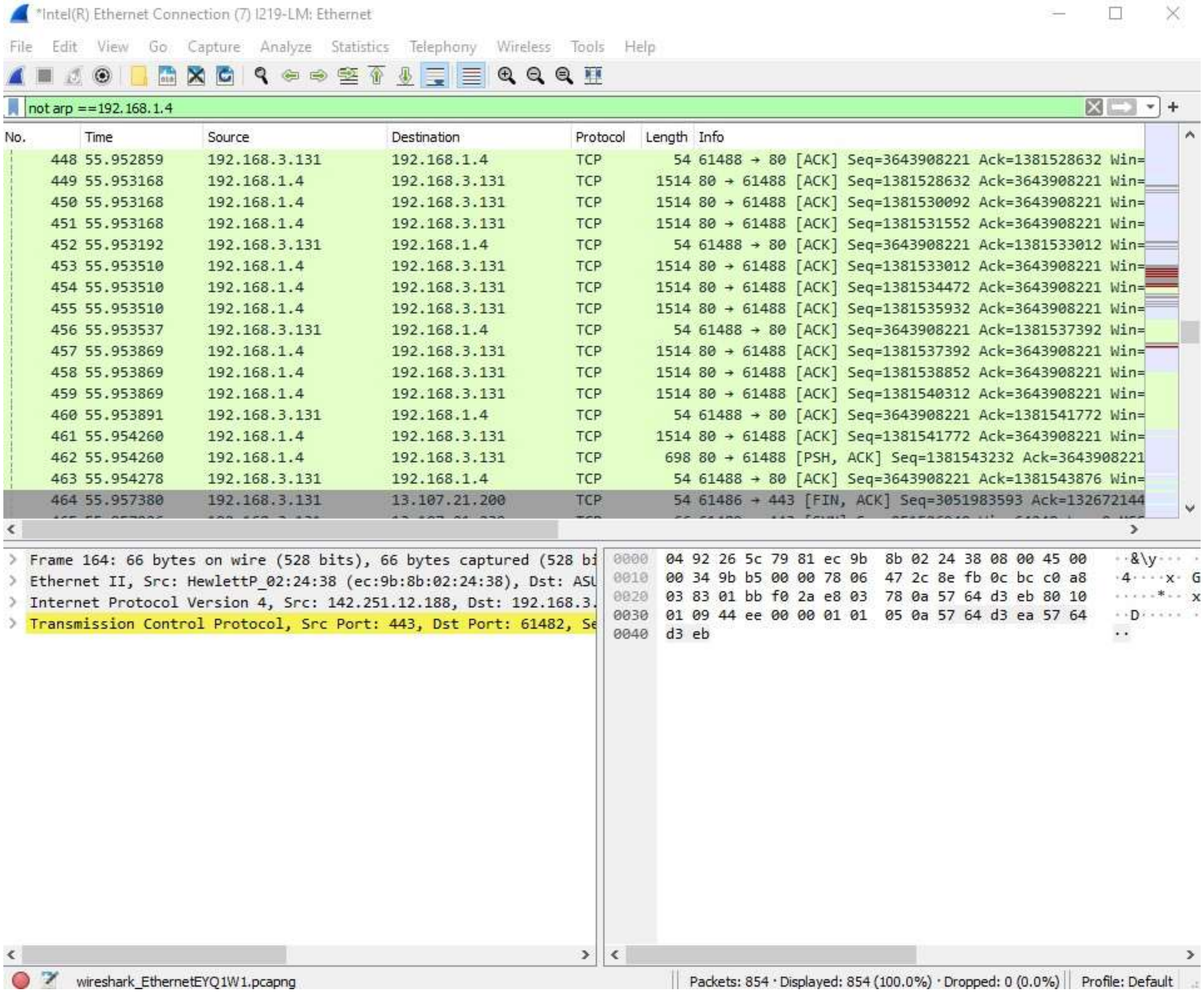
```
> Frame 31: 54 bytes on wire (432 bits), 54 bytes captured (432 bit
> Ethernet II, Src: ASUSTekC_5c:79:81 (04:92:26:5c:79:81), Dst: Hev
> Internet Protocol Version 4, Src: 192.168.3.131, Dst: 142.250.195
> Transmission Control Protocol, Src Port: 52220, Dst Port: 80, Sec
```

```
0000  ec 9b 8b 02 24 38 04 92  26 5c 79 81 08 00 45 00   ····$8·· &
0010  00 28 81 db 40 00 80 06  00 00 c0 a8 03 83 8e fa   ·(··@···
0020  c3 2e cb fc 00 50 00 e6  c0 4f 34 dd e6 6d 50 11   ·.···P··
0030  01 fe 16 6f 00 00                                  ···o··
```

```
wireshark_EthernetRKYMW1.pcapng    Packets: 2187 · Displayed: 8 (0.4%) · Dropped: 0 (0.0%)    Profile: Default
```

6. Capture all non arp traffic using capturing filter operators and store the captured file as "nonarp.pcap".

Now Capture the Non ARP packets
Not arp==192.168.1.4



```
not arp ==192.168.1.4
```

```
No.     Time       Source          Destination     Protocol Length Info
    448 55.952859  192.168.3.131   192.168.1.4     TCP        54 61488 → 80 [ACK] Seq=3643908221 Ack=1381528632 Win=
    449 55.953168  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381528632 Ack=3643908221 Win=
    450 55.953168  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381530092 Ack=3643908221 Win=
    451 55.953168  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381531552 Ack=3643908221 Win=
    452 55.953192  192.168.3.131   192.168.1.4     TCP        54 61488 → 80 [ACK] Seq=3643908221 Ack=1381533012 Win=
    453 55.953510  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381533012 Ack=3643908221 Win=
    454 55.953510  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381534472 Ack=3643908221 Win=
    455 55.953510  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381535932 Ack=3643908221 Win=
    456 55.953537  192.168.3.131   192.168.1.4     TCP        54 61488 → 80 [ACK] Seq=3643908221 Ack=1381537392 Win=
    457 55.953869  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381537392 Ack=3643908221 Win=
    458 55.953869  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381538852 Ack=3643908221 Win=
    459 55.953869  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381540312 Ack=3643908221 Win=
    460 55.953891  192.168.3.131   192.168.1.4     TCP        54 61488 → 80 [ACK] Seq=3643908221 Ack=1381541772 Win=
    461 55.954260  192.168.1.4     192.168.3.131   TCP      1514 80 → 61488 [ACK] Seq=1381541772 Ack=3643908221 Win=
    462 55.954260  192.168.1.4     192.168.3.131   TCP       698 80 → 61488 [PSH, ACK] Seq=1381543232 Ack=3643908221
    463 55.954278  192.168.3.131   192.168.1.4     TCP        54 61488 → 80 [ACK] Seq=3643908221 Ack=1381543876 Win=
    464 55.957380  192.168.3.131   13.107.21.200   TCP        54 61486 → 443 [FIN, ACK] Seq=3051983593 Ack=132672144
```

```
> Frame 164: 66 bytes on wire (528 bits), 66 bytes captured (528 bi
> Ethernet II, Src: HewlettP_02:24:38 (ec:9b:8b:02:24:38), Dst: ASU
> Internet Protocol Version 4, Src: 142.251.12.188, Dst: 192.168.3.
> Transmission Control Protocol, Src Port: 443, Dst Port: 61482, Se
```

```
0000  04 92 26 5c 79 81 ec 9b  8b 02 24 38 08 00 45 00   ··&\y···  ·
0010  00 34 9b b5 00 00 78 06  47 2c 8e fb 0c bc c0 a8   ·4····x· G
0020  03 83 01 bb f0 2a e8 03  78 0a 57 64 d3 eb 80 10   ·····*·· x
0030  01 09 44 ee 00 00 01 01  05 0a 57 64 d3 ea 57 64   ··D·····  ·
0040  d3 eb                                              ··
```

```
wireshark_EthernetEYQ1W1.pcapng    Packets: 854 · Displayed: 854 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

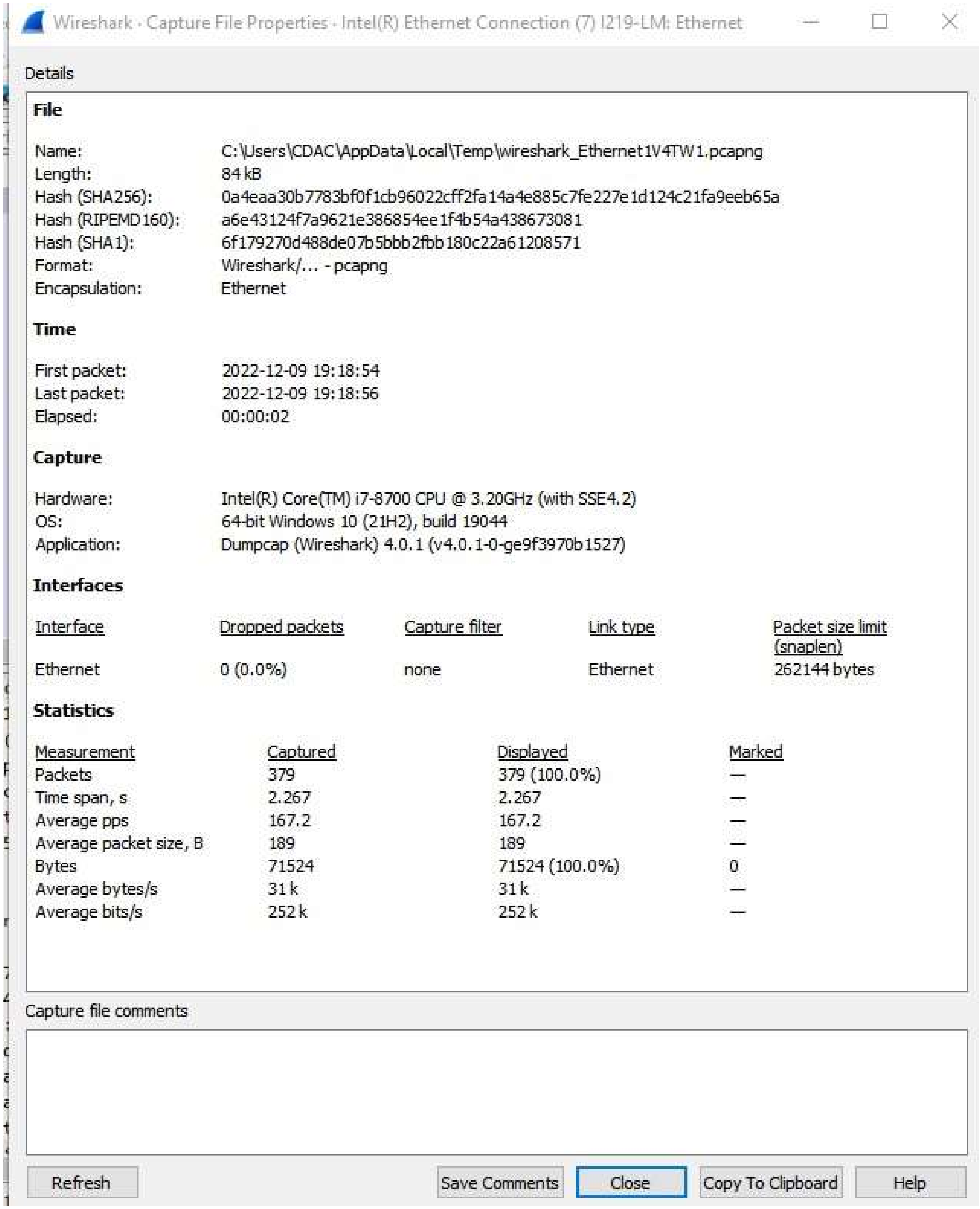
7. Display the summary of the following

*** No. of packet captured, total bytes transferred**

*** Average packets/sec, average packet size**

*** Bandwidth usage (Average bytes/ sec)**

Open Wireshark—-->Go to Statistics —--->Select Capture Filter Property


Wireshark · Capture File Properties · Intel(R) Ethernet Connection (7) I219-LM: Ethernet

Details

File

Name:	C:\Users\CDAC\AppData\Local\Temp\wireshark_Ethernet1V4TW1.pcapng
Length:	84 kB
Hash (SHA256):	0a4eaa30b7783bf0f1cb96022cff2fa14a4e885c7fe227e1d124c21fa9eeb65a
Hash (RIPEMD160):	a6e43124f7a9621e386854ee1f4b54a438673081
Hash (SHA1):	6f179270d488de07b5bbb2fbb180c22a61208571
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2022-12-09 19:18:54
Last packet:	2022-12-09 19:18:56
Elapsed:	00:00:02

Capture

Hardware:	Intel(R) Core(TM) i7-8700 CPU @ 3.20GHz (with SSE4.2)
OS:	64-bit Windows 10 (21H2), build 19044
Application:	Dumpcap (Wireshark) 4.0.1 (v4.0.1-0-ge9f3970b1527)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

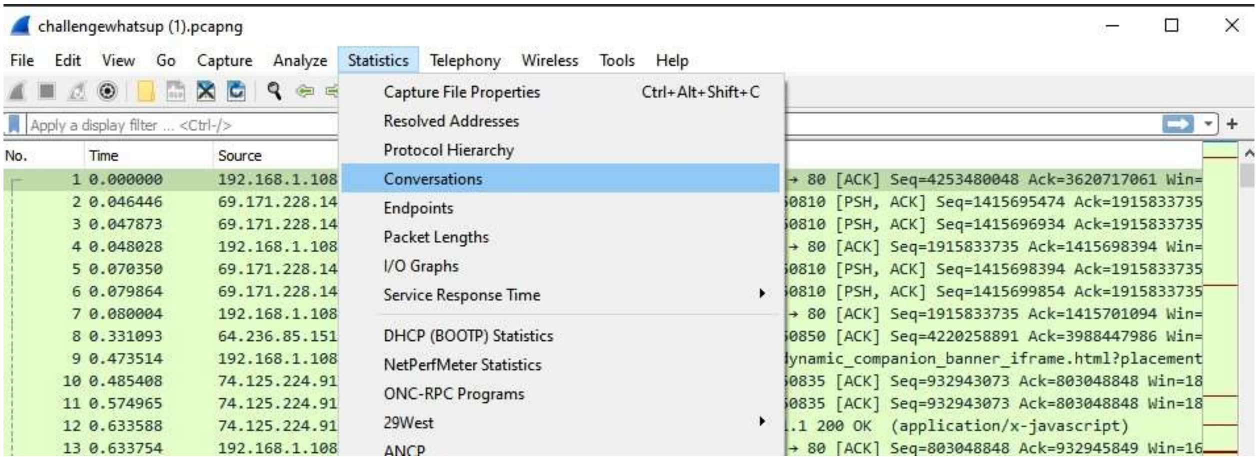
Measurement	Captured	Displayed	Marked
Packets	379	379 (100.0%)	—
Time span, s	2.267	2.267	—
Average pps	167.2	167.2	—
Average packet size, B	189	189	—
Bytes	71524	71524 (100.0%)	0
Average bytes/s	31 k	31 k	—
Average bits/s	252 k	252 k	—

Capture file comments

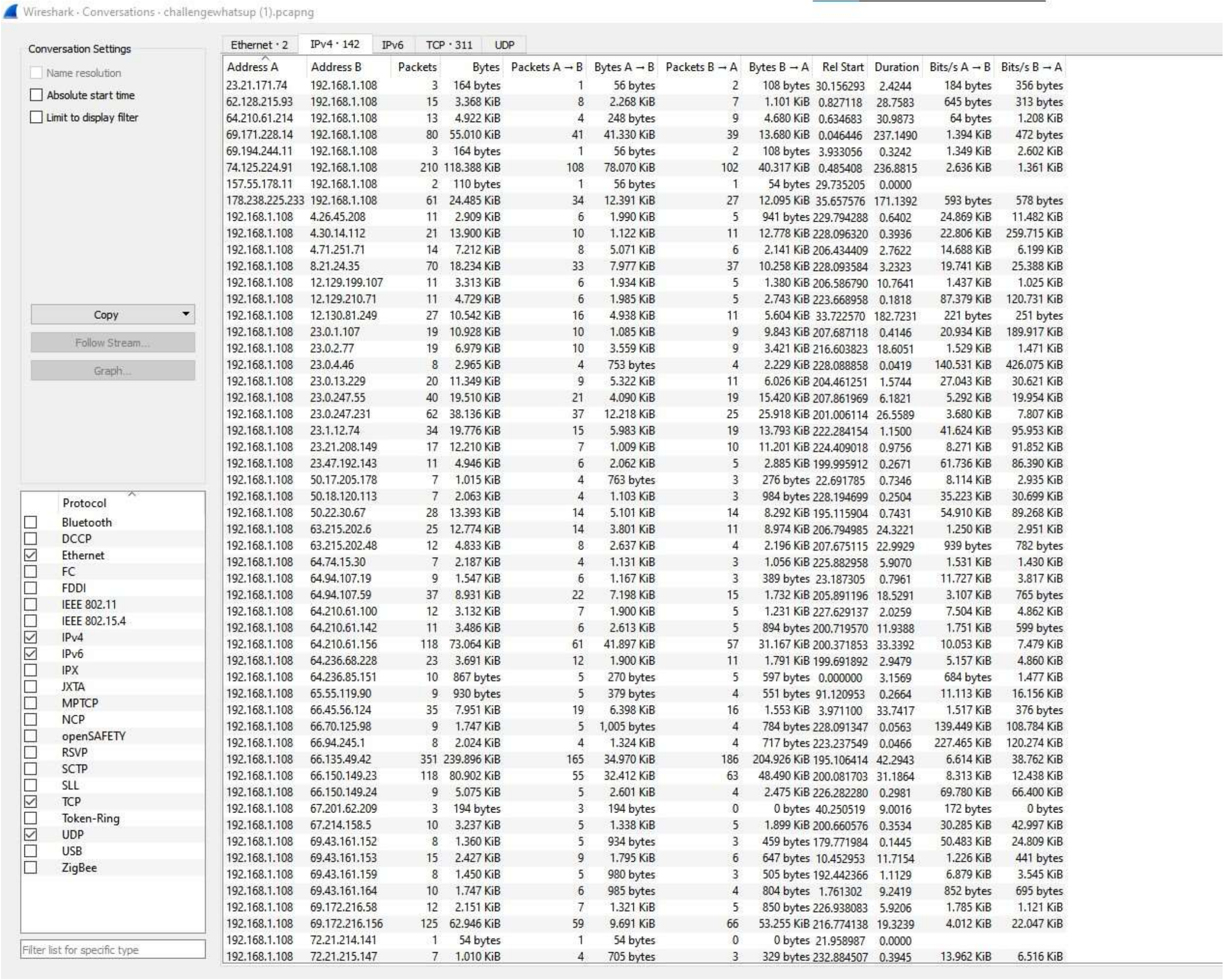
Use the challengewhatsup.pcapng for solving the problems from 10 to 13

10. How many different IP hosts is A’s machine is communicating with?

Step-1:- Now open the challengewhatsup.pcapng file —-->go to —-> Statistics —--->Select Conversion —->Open It



```
No.   Time       Source
   1 0.000000    192.168.1.108     → 80 [ACK] Seq=4253480048 Ack=3620717061 Win=
   2 0.046446    69.171.228.14     0810 [PSH, ACK] Seq=1415695474 Ack=1915833735
   3 0.047873    69.171.228.14     0810 [PSH, ACK] Seq=1415696934 Ack=1915833735
   4 0.048028    192.168.1.108     → 80 [ACK] Seq=1915833735 Ack=1415698394 Win=
   5 0.070350    69.171.228.14     0810 [PSH, ACK] Seq=1415698394 Ack=1915833735
   6 0.079864    69.171.228.14     0810 [PSH, ACK] Seq=1415699854 Ack=1915833735
   7 0.080004    192.168.1.108     → 80 [ACK] Seq=1915833735 Ack=1415701094 Win=
   8 0.331093    64.236.85.151     0850 [ACK] Seq=4220258891 Ack=3988447986 Win=
   9 0.473514    192.168.1.108     ynamic_companion_banner_iframe.html?placement
  10 0.485408    74.125.224.91     0835 [ACK] Seq=932943073 Ack=803048848 Win=18
  11 0.574965    74.125.224.91     0835 [ACK] Seq=932943073 Ack=803048848 Win=18
  12 0.633588    74.125.224.91     .1 200 OK  (application/x-javascript)
  13 0.633754    192.168.1.108     → 80 [ACK] Seq=803048848 Ack=932945849 Win=16
```



Wireshark · Conversations · challengewhatsup (1).pcapng

Conversation Settings

☐ Name resolution
☐ Absolute start time
☐ Limit to display filter

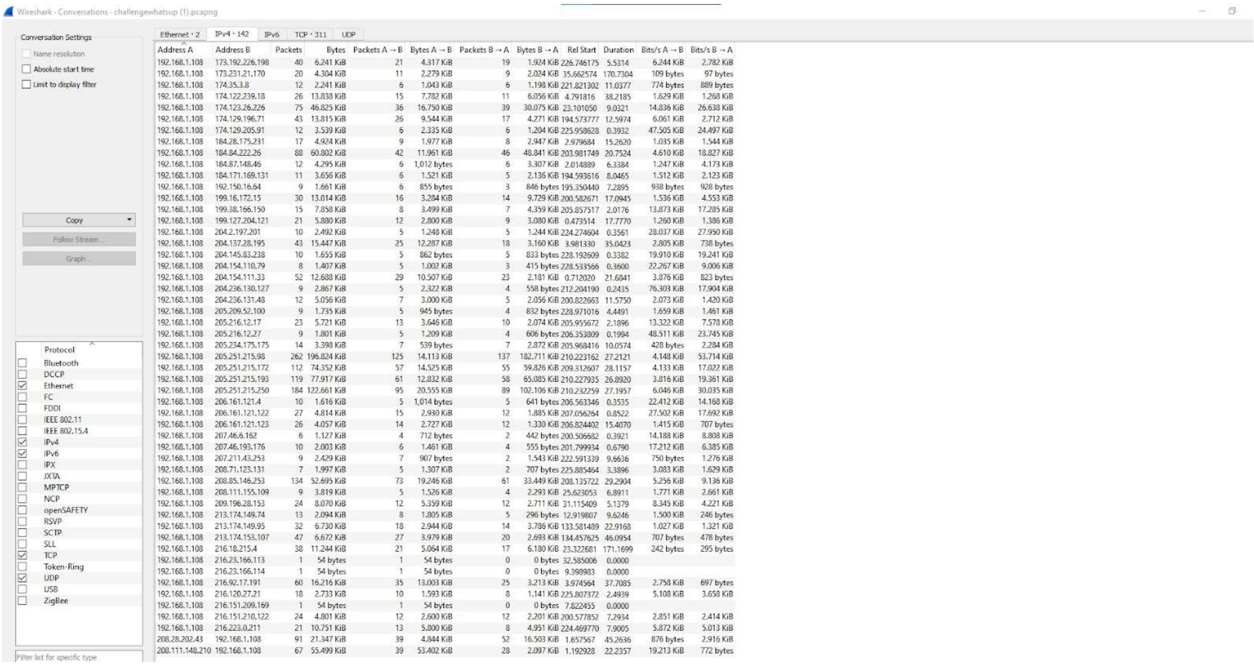
Protocol

☐ Bluetooth
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ MPTCP
☐ NCP
☐ openSAFETY
☐ RSVP
☐ SCTP
☐ SLL
☑ TCP
☐ Token-Ring
☑ UDP
☐ USB
☐ ZigBee

Filter list for specific type

Ethernet · 2 | IPv4 · 142 | IPv6 | TCP · 311 | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
23.21.171.74	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	30.156293	2.4244	184 bytes	356 bytes
62.128.215.93	192.168.1.108	15	3.368 KiB	8	2.268 KiB	7	1.101 KiB	0.827118	28.7583	645 bytes	313 bytes
64.210.61.214	192.168.1.108	13	4.922 KiB	4	248 bytes	9	4.680 KiB	0.634683	30.9873	64 bytes	1.208 KiB
69.171.228.14	192.168.1.108	80	55.010 KiB	41	41.330 KiB	39	13.680 KiB	0.046446	237.1490	1.394 KiB	472 bytes
69.194.244.11	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	3.933056	0.3242	1.349 KiB	2.602 KiB
74.125.224.91	192.168.1.108	210	118.388 KiB	108	78.070 KiB	102	40.317 KiB	0.485408	236.8815	2.636 KiB	1.361 KiB
157.55.178.11	192.168.1.108	2	110 bytes	1	56 bytes	1	54 bytes	29.735205	0.0000		
178.238.225.233	192.168.1.108	61	24.485 KiB	34	12.391 KiB	27	12.095 KiB	35.657576	171.1392	593 bytes	578 bytes
192.168.1.108	4.26.45.208	11	2.909 KiB	6	1.990 KiB	5	941 bytes	229.794288	0.6402	24.869 KiB	11.482 KiB
192.168.1.108	4.30.14.112	21	13.900 KiB	10	1.122 KiB	11	12.778 KiB	228.096320	0.3936	22.806 KiB	259.715 KiB
192.168.1.108	4.71.251.71	14	7.212 KiB	8	5.071 KiB	6	2.141 KiB	206.434409	2.7622	14.688 KiB	6.199 KiB
192.168.1.108	8.21.24.35	70	18.234 KiB	33	7.977 KiB	37	10.258 KiB	228.093584	3.2323	19.741 KiB	25.388 KiB
192.168.1.108	12.129.199.107	11	3.313 KiB	6	1.934 KiB	5	1.380 KiB	206.586790	10.7641	1.437 KiB	1.025 KiB
192.168.1.108	12.129.210.71	11	4.729 KiB	6	1.985 KiB	5	2.743 KiB	223.668958	0.1818	87.379 KiB	120.731 KiB
192.168.1.108	12.130.81.249	27	10.542 KiB	16	4.938 KiB	11	5.604 KiB	33.722570	182.7231	221 bytes	251 bytes
192.168.1.108	23.0.1.107	19	10.928 KiB	10	1.085 KiB	9	9.843 KiB	207.687118	0.4146	20.934 KiB	189.917 KiB
192.168.1.108	23.0.2.77	19	6.979 KiB	10	3.559 KiB	9	3.421 KiB	216.603823	18.6051	1.529 KiB	1.471 KiB
192.168.1.108	23.0.4.46	8	2.965 KiB	4	753 bytes	4	2.229 KiB	228.088858	0.0419	140.531 KiB	426.075 KiB
192.168.1.108	23.0.13.229	20	11.349 KiB	9	5.322 KiB	11	6.026 KiB	204.461251	1.5744	27.043 KiB	30.621 KiB
192.168.1.108	23.0.247.55	40	19.510 KiB	21	4.090 KiB	19	15.420 KiB	207.861969	6.1821	5.292 KiB	19.954 KiB
192.168.1.108	23.0.247.231	62	38.136 KiB	37	12.218 KiB	25	25.918 KiB	201.006114	26.5589	3.680 KiB	7.807 KiB
192.168.1.108	23.1.12.74	34	19.776 KiB	15	5.983 KiB	19	13.793 KiB	222.284154	1.1500	41.624 KiB	95.953 KiB
192.168.1.108	23.21.208.149	17	12.210 KiB	7	1.009 KiB	10	11.201 KiB	224.409018	0.9756	8.271 KiB	91.852 KiB
192.168.1.108	23.47.192.143	11	4.946 KiB	6	2.062 KiB	5	2.885 KiB	199.995912	0.2671	61.736 KiB	86.390 KiB
192.168.1.108	50.17.205.178	7	1.015 KiB	4	763 bytes	3	276 bytes	22.691785	0.7346	8.114 KiB	2.935 KiB
192.168.1.108	50.18.120.113	7	2.063 KiB	4	1.103 KiB	3	984 bytes	228.194699	0.2504	35.223 KiB	30.699 KiB
192.168.1.108	50.22.30.67	28	13.393 KiB	14	5.101 KiB	14	8.292 KiB	195.115904	0.7431	54.910 KiB	89.268 KiB
192.168.1.108	63.215.202.6	25	12.774 KiB	14	3.801 KiB	11	8.974 KiB	206.794985	24.3221	1.250 KiB	2.951 KiB
192.168.1.108	63.215.202.48	12	4.833 KiB	8	2.637 KiB	4	2.196 KiB	207.675115	22.9929	939 bytes	782 bytes
192.168.1.108	64.74.15.30	7	2.187 KiB	4	1.131 KiB	3	1.056 KiB	225.882958	5.9070	1.531 KiB	1.430 KiB
192.168.1.108	64.94.107.19	9	1.547 KiB	6	1.167 KiB	3	389 bytes	23.187305	0.7961	11.727 KiB	3.817 KiB
192.168.1.108	64.94.107.59	37	8.931 KiB	22	7.198 KiB	15	1.732 KiB	205.891196	18.5291	3.107 KiB	765 bytes
192.168.1.108	64.210.61.100	12	3.132 KiB	7	1.900 KiB	5	1.231 KiB	227.629137	2.0259	7.504 KiB	4.862 KiB
192.168.1.108	64.210.61.142	11	3.486 KiB	6	2.613 KiB	5	894 bytes	200.719570	11.9388	1.751 KiB	599 bytes
192.168.1.108	64.210.61.156	118	73.064 KiB	61	41.897 KiB	57	31.167 KiB	200.371853	33.3392	10.053 KiB	7.479 KiB
192.168.1.108	64.236.68.228	23	3.691 KiB	12	1.900 KiB	11	1.791 KiB	199.691892	2.9479	5.157 KiB	4.860 KiB
192.168.1.108	64.236.85.151	10	867 bytes	5	270 bytes	5	597 bytes	0.000000	3.1569	684 bytes	1.477 KiB
192.168.1.108	65.55.119.90	9	930 bytes	5	379 bytes	4	551 bytes	91.120953	0.2664	11.113 KiB	16.156 KiB
192.168.1.108	66.45.56.124	35	7.951 KiB	19	6.398 KiB	16	1.553 KiB	3.971100	33.7417	1.517 KiB	376 bytes
192.168.1.108	66.70.125.98	9	1.747 KiB	5	1,005 bytes	4	784 bytes	228.091347	0.0563	139.449 KiB	108.784 KiB
192.168.1.108	66.94.245.1	8	2.024 KiB	4	1.324 KiB	4	717 bytes	223.237549	0.0466	227.465 KiB	120.274 KiB
192.168.1.108	66.135.49.42	351	239.896 KiB	165	34.970 KiB	186	204.926 KiB	195.106414	42.2943	6.614 KiB	38.762 KiB
192.168.1.108	66.150.149.23	118	80.902 KiB	55	32.412 KiB	63	48.490 KiB	200.081703	31.1864	8.313 KiB	12.438 KiB
192.168.1.108	66.150.149.24	9	5.075 KiB	5	2.601 KiB	4	2.475 KiB	226.282280	0.2981	69.780 KiB	66.400 KiB
192.168.1.108	67.201.62.209	3	194 bytes	3	194 bytes	0	0 bytes	40.250519	9.0016	172 bytes	0 bytes
192.168.1.108	67.214.158.5	10	3.237 KiB	5	1.338 KiB	5	1.899 KiB	200.660576	0.3534	30.285 KiB	42.997 KiB
192.168.1.108	69.43.161.152	8	1.360 KiB	5	934 bytes	3	459 bytes	179.771984	0.1445	50.483 KiB	24.809 KiB
192.168.1.108	69.43.161.153	15	2.427 KiB	9	1.795 KiB	6	647 bytes	10.452953	11.7154	1.226 KiB	441 bytes
192.168.1.108	69.43.161.159	8	1.450 KiB	5	980 bytes	3	505 bytes	192.442366	1.1129	6.879 KiB	3.545 KiB
192.168.1.108	69.43.161.164	10	1.747 KiB	6	985 bytes	4	804 bytes	1.761302	9.2419	852 bytes	695 bytes
192.168.1.108	69.172.216.58	12	2.151 KiB	7	1.321 KiB	5	850 bytes	226.938083	5.9206	1.785 KiB	1.121 KiB
192.168.1.108	69.172.216.156	125	62.946 KiB	59	9.691 KiB	66	53.255 KiB	216.774138	19.3239	4.012 KiB	22.047 KiB
192.168.1.108	72.21.214.141	1	54 bytes	1	54 bytes	0	0 bytes	21.958987	0.0000		
192.168.1.108	72.21.215.147	7	1.010 KiB	4	705 bytes	3	329 bytes	232.884507	0.3945	13.962 KiB	6.516 KiB



Wireshark · Conversations · challengewhatsup (1).pcapng

Conversation Settings

☐ Name resolution
☐ Absolute start time
☐ Limit to display filter

Protocol

☐ Bluetooth
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ MPTCP
☐ NCP
☐ openSAFETY
☐ RSVP
☐ SCTP
☐ SLL
☑ TCP
☐ Token-Ring
☑ UDP
☐ USB
☐ ZigBee

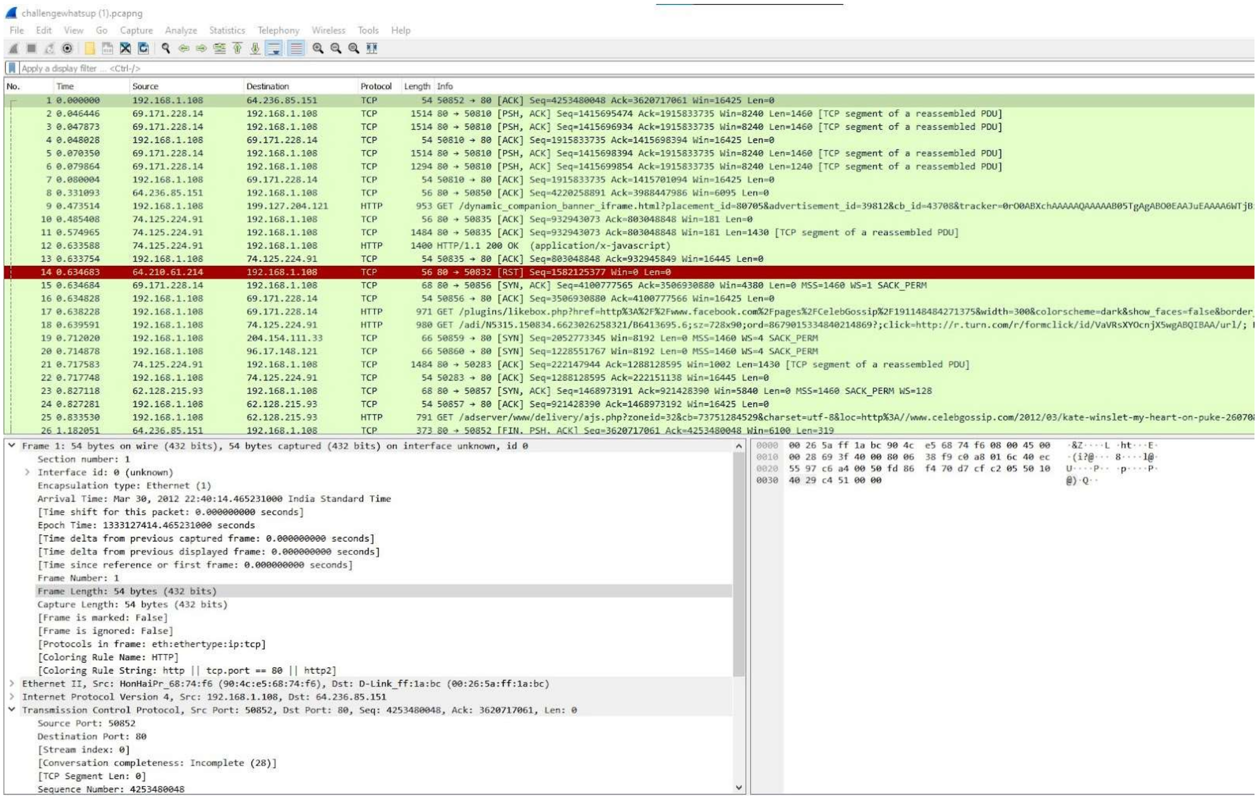
Filter list for specific type

Ethernet · 2 | IPv4 · 142 | IPv6 | TCP · 311 | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.108	173.192.226.198	40	6.241 KiB	21	4.317 KiB	19	1.924 KiB	226.746175	5.5314	6.244 KiB	2.782 KiB
192.168.1.108	173.231.21.170	20	4.304 KiB	11	2.279 KiB	9	2.024 KiB	35.662574	170.7304	109 bytes	97 bytes
192.168.1.108	174.35.3.8	12	2.241 KiB	6	1.043 KiB	6	1.198 KiB	221.821302	11.0377	774 bytes	889 bytes
192.168.1.108	174.122.239.18	26	13.838 KiB	15	7.782 KiB	11	6.056 KiB	4.791816	38.2185	1.629 KiB	1.268 KiB
192.168.1.108	174.123.26.226	75	46.825 KiB	36	16.750 KiB	39	30.075 KiB	23.101050	9.0321	14.836 KiB	26.638 KiB
192.168.1.108	174.129.196.71	43	13.815 KiB	26	9.544 KiB	17	4.271 KiB	194.573777	12.5974	6.061 KiB	2.712 KiB
192.168.1.108	174.129.205.91	12	3.539 KiB	6	2.335 KiB	6	1.204 KiB	225.958628	0.3932	47.505 KiB	24.497 KiB
192.168.1.108	184.28.175.231	17	4.924 KiB	9	1.977 KiB	8	2.947 KiB	2.979684	15.2620	1.035 KiB	1.544 KiB
192.168.1.108	184.84.222.26	88	60.802 KiB	42	11.961 KiB	46	48.841 KiB	203.981749	20.7524	4.610 KiB	18.827 KiB
192.168.1.108	184.87.148.46	12	4.295 KiB	6	1,012 bytes	6	3.307 KiB	2.014889	6.3384	1.247 KiB	4.173 KiB
192.168.1.108	184.171.169.131	11	3.656 KiB	6	1.521 KiB	5	2.136 KiB	194.593616	8.0465	1.512 KiB	2.123 KiB
192.168.1.108	192.150.16.64	9	1.661 KiB	6	855 bytes	3	846 bytes	195.350440	7.2895	938 bytes	928 bytes
192.168.1.108	199.16.172.15	30	13.014 KiB	16	3.284 KiB	14	9.729 KiB	200.582671	17.0945	1.536 KiB	4.553 KiB
192.168.1.108	199.38.166.150	15	7.858 KiB	8	3.499 KiB	7	4.359 KiB	205.857517	2.0176	13.873 KiB	17.285 KiB
192.168.1.108	199.127.204.121	21	5.880 KiB	12	2.800 KiB	9	3.080 KiB	0.473514	17.7770	1.260 KiB	1.386 KiB
192.168.1.108	204.2.197.201	10	2.492 KiB	5	1.248 KiB	5	1.244 KiB	224.274604	0.3561	28.037 KiB	27.950 KiB
192.168.1.108	204.137.28.195	43	15.447 KiB	25	12.287 KiB	18	3.160 KiB	3.981330	35.0423	2.805 KiB	738 bytes
192.168.1.108	204.145.83.238	10	1.655 KiB	5	862 bytes	5	833 bytes	228.192609	0.3382	19.910 KiB	19.241 KiB
192.168.1.108	204.154.110.79	8	1.407 KiB	5	1.002 KiB	3	415 bytes	228.533566	0.3600	22.267 KiB	9.006 KiB
192.168.1.108	204.154.111.33	52	12.688 KiB	29	10.507 KiB	23	2.181 KiB	0.712020	21.6841	3.876 KiB	823 bytes
192.168.1.108	204.236.130.127	9	2.867 KiB	5	2.322 KiB	4	558 bytes	212.204190	0.2435	76.303 KiB	17.904 KiB
192.168.1.108	204.236.131.48	12	5.056 KiB	7	3.000 KiB	5	2.056 KiB	200.822663	11.5750	2.073 KiB	1.420 KiB
192.168.1.108	205.209.52.100	9	1.735 KiB	5	945 bytes	4	832 bytes	228.971016	4.4491	1.659 KiB	1.461 KiB
192.168.1.108	205.216.12.17	23	5.721 KiB	13	3.646 KiB	10	2.074 KiB	205.955672	2.1896	13.322 KiB	7.578 KiB
192.168.1.108	205.216.12.27	9	1.801 KiB	5	1.209 KiB	4	606 bytes	206.353809	0.1994	48.511 KiB	23.745 KiB
192.168.1.108	205.234.175.175	14	3.398 KiB	7	539 bytes	7	2.872 KiB	205.968416	10.0574	428 bytes	2.284 KiB
192.168.1.108	205.251.215.98	262	196.824 KiB	125	14.113 KiB	137	182.711 KiB	210.223162	27.2121	4.148 KiB	53.714 KiB
192.168.1.108	205.251.215.172	112	74.352 KiB	57	14.525 KiB	55	59.826 KiB	209.312607	28.1157	4.133 KiB	17.022 KiB
192.168.1.108	205.251.215.193	119	77.917 KiB	61	12.832 KiB	58	65.085 KiB	210.227935	26.8920	3.816 KiB	19.361 KiB
192.168.1.108	205.251.215.250	184	122.661 KiB	95	20.555 KiB	89	102.106 KiB	210.232259	27.1957	6.046 KiB	30.035 KiB
192.168.1.108	206.161.121.4	10	1.616 KiB	5	1,014 bytes	5	641 bytes	206.563346	0.3535	22.412 KiB	14.168 KiB
192.168.1.108	206.161.121.122	27	4.814 KiB	15	2.930 KiB	12	1.885 KiB	207.056264	0.8522	27.502 KiB	17.692 KiB
192.168.1.108	206.161.121.123	26	4.057 KiB	14	2.727 KiB	12	1.330 KiB	206.824402	15.4070	1.415 KiB	707 bytes
192.168.1.108	207.46.6.162	6	1.127 KiB	4	712 bytes	2	442 bytes	200.506682	0.3921	14.188 KiB	8.808 KiB
192.168.1.108	207.46.193.176	10	2.003 KiB	6	1.461 KiB	4	555 bytes	201.799934	0.6790	17.212 KiB	6.385 KiB
192.168.1.108	207.211.43.253	9	2.429 KiB	7	907 bytes	2	1.543 KiB	222.591339	9.6636	750 bytes	1.276 KiB
192.168.1.108	208.71.123.131	7	1.997 KiB	5	1.307 KiB	2	707 bytes	225.885464	3.3896	3.083 KiB	1.629 KiB
192.168.1.108	208.85.146.253	134	52.695 KiB	73	19.246 KiB	61	33.449 KiB	208.135722	29.2904	5.256 KiB	9.136 KiB
192.168.1.108	208.111.155.109	9	3.819 KiB	5	1.526 KiB	4	2.293 KiB	25.623053	6.8911	1.771 KiB	2.661 KiB
192.168.1.108	209.196.28.153	24	8.070 KiB	12	5.359 KiB	12	2.711 KiB	31.115409	5.1379	8.345 KiB	4.221 KiB
192.168.1.108	213.174.149.74	13	2.094 KiB	8	1.805 KiB	5	296 bytes	12.919807	9.6246	1.500 KiB	246 bytes
192.168.1.108	213.174.149.95	32	6.730 KiB	18	2.944 KiB	14	3.786 KiB	133.581489	22.9168	1.027 KiB	1.321 KiB
192.168.1.108	213.174.153.107	47	6.672 KiB	27	3.979 KiB	20	2.693 KiB	134.457625	46.0954	707 bytes	478 bytes
192.168.1.108	216.18.215.4	38	11.244 KiB	21	5.064 KiB	17	6.180 KiB	23.322681	171.1699	242 bytes	295 bytes
192.168.1.108	216.23.166.113	1	54 bytes	1	54 bytes	0	0 bytes	32.585006	0.0000		
192.168.1.108	216.23.166.114	1	54 bytes	1	54 bytes	0	0 bytes	9.398983	0.0000		
192.168.1.108	216.92.17.191	60	16.216 KiB	35	13.003 KiB	25	3.213 KiB	3.974564	37.7085	2.758 KiB	697 bytes
192.168.1.108	216.120.27.21	18	2.733 KiB	10	1.593 KiB	8	1.141 KiB	225.807372	2.4939	5.108 KiB	3.658 KiB
192.168.1.108	216.151.209.169	1	54 bytes	1	54 bytes	0	0 bytes	7.822455	0.0000		
192.168.1.108	216.151.210.122	24	4.801 KiB	12	2.600 KiB	12	2.201 KiB	200.577852	7.2934	2.851 KiB	2.414 KiB
192.168.1.108	216.223.0.211	21	10.751 KiB	13	5.800 KiB	8	4.951 KiB	224.469770	7.9005	5.872 KiB	5.013 KiB
208.28.202.43	192.168.1.108	91	21.347 KiB	39	4.844 KiB	52	16.503 KiB	1.657567	45.2636	876 bytes	2.916 KiB
208.111.148.210	192.168.1.108	67	55.499 KiB	39	53.402 KiB	28	2.097 KiB	1.192928	22.2357	19.213 KiB	772 bytes

11. What is the average packets per second rate seen in trace file?

Step-1:- Now open the challengewhatsup.pcapng file

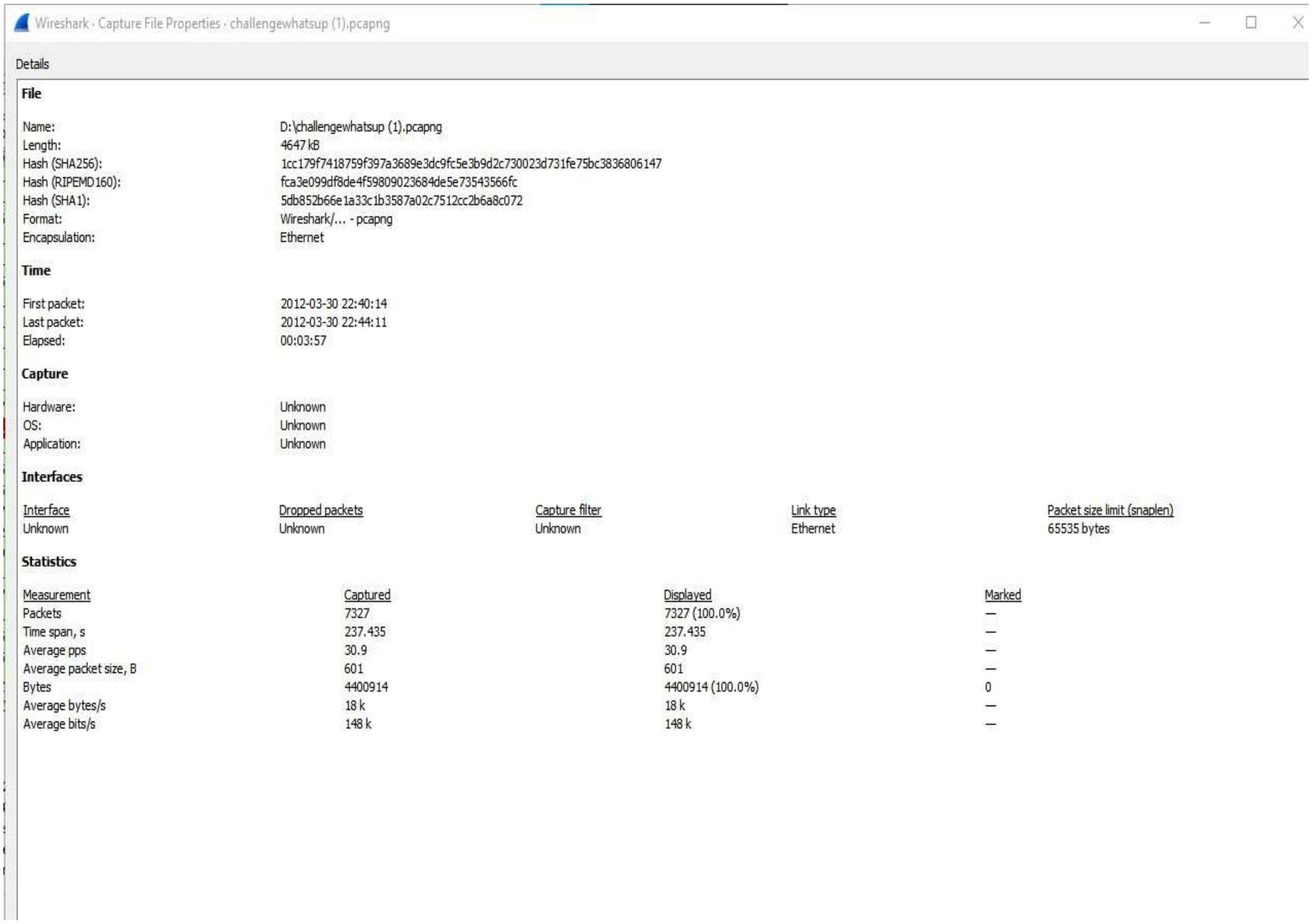


```
No.  Time      Source          Destination      Protocol Length Info
   1 0.000000  192.168.1.108   64.236.85.151    TCP        54 50852 → 80 [ACK] Seq=4253480048 Ack=3620717061 Win=16425 Len=0
   2 0.046446  69.171.228.14   192.168.1.108    TCP      1514 80 → 50810 [PSH, ACK] Seq=1415695474 Ack=1915833735 Win=8240 Len=1460 [TCP segment of a reassembled PDU]
   3 0.047873  69.171.228.14   192.168.1.108    TCP      1514 80 → 50810 [PSH, ACK] Seq=1415696934 Ack=1915833735 Win=8240 Len=1460 [TCP segment of a reassembled PDU]
   4 0.048028  192.168.1.108   69.171.228.14    TCP        54 50810 → 80 [ACK] Seq=1915833735 Ack=1415698394 Win=16425 Len=0
   5 0.070350  69.171.228.14   192.168.1.108    TCP      1514 80 → 50810 [PSH, ACK] Seq=1415698394 Ack=1915833735 Win=8240 Len=1460 [TCP segment of a reassembled PDU]
   6 0.079864  69.171.228.14   192.168.1.108    TCP      1294 80 → 50810 [PSH, ACK] Seq=1415699854 Ack=1915833735 Win=8240 Len=1240 [TCP segment of a reassembled PDU]
   7 0.080004  192.168.1.108   69.171.228.14    TCP        54 50810 → 80 [ACK] Seq=1915833735 Ack=1415701094 Win=16425 Len=0
   8 0.331093  64.236.85.151   192.168.1.108    TCP        56 80 → 50850 [ACK] Seq=4220258891 Ack=3988447986 Win=6095 Len=0
   9 0.473514  192.168.1.108   199.127.204.121  HTTP      953 GET /dynamic_companion_banner_iframe.html?placement_id=80705&advertisement_id=39812&cb_id=43708&tracker=0rO0ABXchAAAAAQAAAAAB05TgAgABO0EAAJuEAAAA6WTjB
  10 0.485408  74.125.224.91   192.168.1.108    TCP        56 80 → 50835 [ACK] Seq=932943073 Ack=803048848 Win=181 Len=0
  11 0.574965  74.125.224.91   192.168.1.108    TCP      1484 80 → 50835 [ACK] Seq=932943073 Ack=803048848 Win=181 Len=1430 [TCP segment of a reassembled PDU]
  12 0.633588  74.125.224.91   192.168.1.108    HTTP     1400 HTTP/1.1 200 OK  (application/x-javascript)
  13 0.633754  192.168.1.108   74.125.224.91    TCP        54 50835 → 80 [ACK] Seq=803048848 Ack=932945849 Win=16445 Len=0
  14 0.634683  64.210.61.214   192.168.1.108    TCP        56 80 → 50832 [RST] Seq=1582125377 Win=0 Len=0
  15 0.634684  69.171.228.14   192.168.1.108    TCP        68 80 → 50856 [SYN, ACK] Seq=4100777565 Ack=3506930880 Win=4380 Len=0 MSS=1460 WS=1 SACK_PERM
  16 0.634828  192.168.1.108   69.171.228.14    TCP        54 50856 → 80 [ACK] Seq=3506930880 Ack=4100777566 Win=16425 Len=0
  17 0.638228  192.168.1.108   69.171.228.14    HTTP      971 GET /plugins/likebox.php?href=http%3A%2F%2Fwww.facebook.com%2Fpages%2FCelebGossip%2F191148484271375&width=300&colorscheme=dark&show_faces=false&border_
  18 0.639591  192.168.1.108   74.125.224.91    HTTP      980 GET /adi/N5315.150834.6623026258321/B6413695.6;sz=728x90;ord=8679015334840214869?;click=http://r.turn.com/r/formclick/id/VaVRsXYOcnjX5wgABQIBAA/url/;
  19 0.712020  192.168.1.108   204.154.111.33   TCP        66 50859 → 80 [SYN] Seq=2052773345 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
  20 0.714878  192.168.1.108   96.17.148.121    TCP        66 50860 → 80 [SYN] Seq=1228551767 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
  21 0.717583  74.125.224.91   192.168.1.108    TCP      1484 80 → 50283 [ACK] Seq=222147944 Ack=1288128595 Win=1002 Len=1430 [TCP segment of a reassembled PDU]
  22 0.717748  192.168.1.108   74.125.224.91    TCP        54 50283 → 80 [ACK] Seq=1288128595 Ack=222151138 Win=16445 Len=0
  23 0.827118  62.128.215.93   192.168.1.108    TCP        68 80 → 50857 [SYN, ACK] Seq=1468973191 Ack=921428390 Win=5840 Len=0 MSS=1460 SACK_PERM WS=128
  24 0.827281  192.168.1.108   62.128.215.93    TCP        54 50857 → 80 [ACK] Seq=921428390 Ack=1468973192 Win=16425 Len=0
  25 0.833530  192.168.1.108   62.128.215.93    HTTP      791 GET /adserver/www/delivery/ajs.php?zoneid=32&cb=73751284529&charset=utf-8&loc=http%3A//www.celebgossip.com/2012/03/kate-winslet-my-heart-on-puke-26070
  26 1.182051  64.236.85.151   192.168.1.108    TCP       373 80 → 50852 [FIN, PSH, ACK] Seq=3620717061 Ack=4253480048 Win=6100 Len=319
```

```
v Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface unknown, id 0
    Section number: 1
  > Interface id: 0 (unknown)
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 30, 2012 22:40:14.465231000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1333127414.465231000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: HonHaiPr_68:74:f6 (90:4c:e5:68:74:f6), Dst: D-Link_ff:1a:bc (00:26:5a:ff:1a:bc)
> Internet Protocol Version 4, Src: 192.168.1.108, Dst: 64.236.85.151
v Transmission Control Protocol, Src Port: 50852, Dst Port: 80, Seq: 4253480048, Ack: 3620717061, Len: 0
    Source Port: 50852
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Incomplete (28)]
    [TCP Segment Len: 0]
    Sequence Number: 4253480048
```

```
0000  00 26 5a ff 1a bc 90 4c  e5 68 74 f6 08 00 45 00   ·&Z····L ·ht···E·
0010  00 28 69 3f 40 00 80 06  38 f9 c0 a8 01 6c 40 ec   ·(i?@··· 8····l@·
0020  55 97 c6 a4 00 50 fd 86  f4 70 d7 cf c2 05 50 10   U····P·· ·p····P·
0030  40 29 c4 51 00 00                                  @)·Q··
```

Step-2:- Open Wireshark—-->Go to Statistics —--->Select Capture Filter Property



Wireshark · Capture File Properties · challengewhatsup (1).pcapng

Details

File

Name:	D:\challengewhatsup (1).pcapng
Length:	4647 kB
Hash (SHA256):	1cc179f7418759f397a3689e3dc9fc5e3b9d2c730023d731fe75bc3836806147
Hash (RIPEMD160):	fca3e099df8de4f59809023684de5e73543566fc
Hash (SHA1):	5db852b66e1a33c1b3587a02c7512cc2b6a8c072
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2012-03-30 22:40:14
Last packet:	2012-03-30 22:44:11
Elapsed:	00:03:57

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

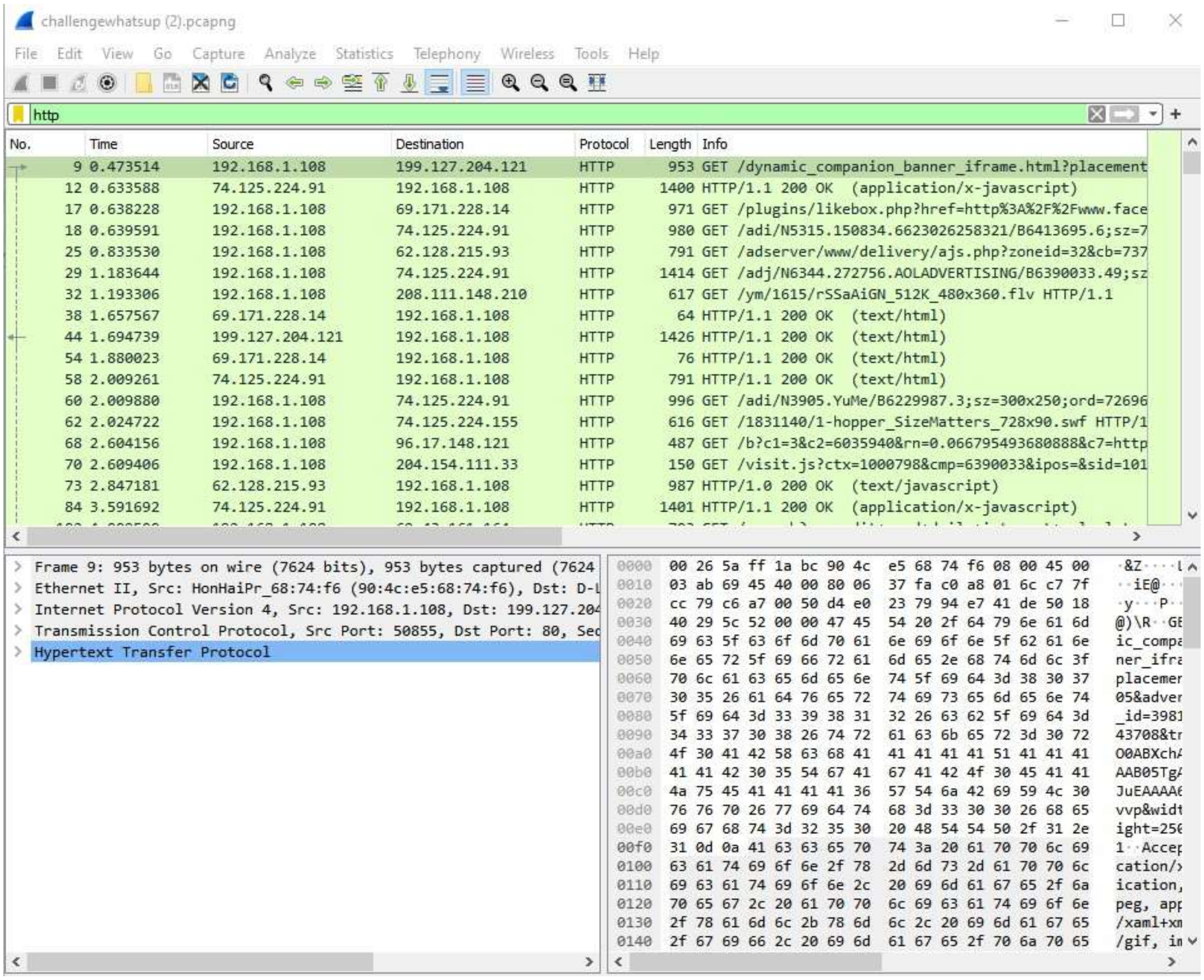
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	7327	7327 (100.0%)	—
Time span, s	237.435	237.435	—
Average pps	30.9	30.9	—
Average packet size, B	601	601	—
Bytes	4400914	4400914 (100.0%)	0
Average bytes/s	18 k	18 k	—
Average bits/s	148 k	148 k	—

12. How many HTTP POST requests did A's machine send?

Step-1:- Now open the challengewhatsup.pcapng file


challengewhatsup (2).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

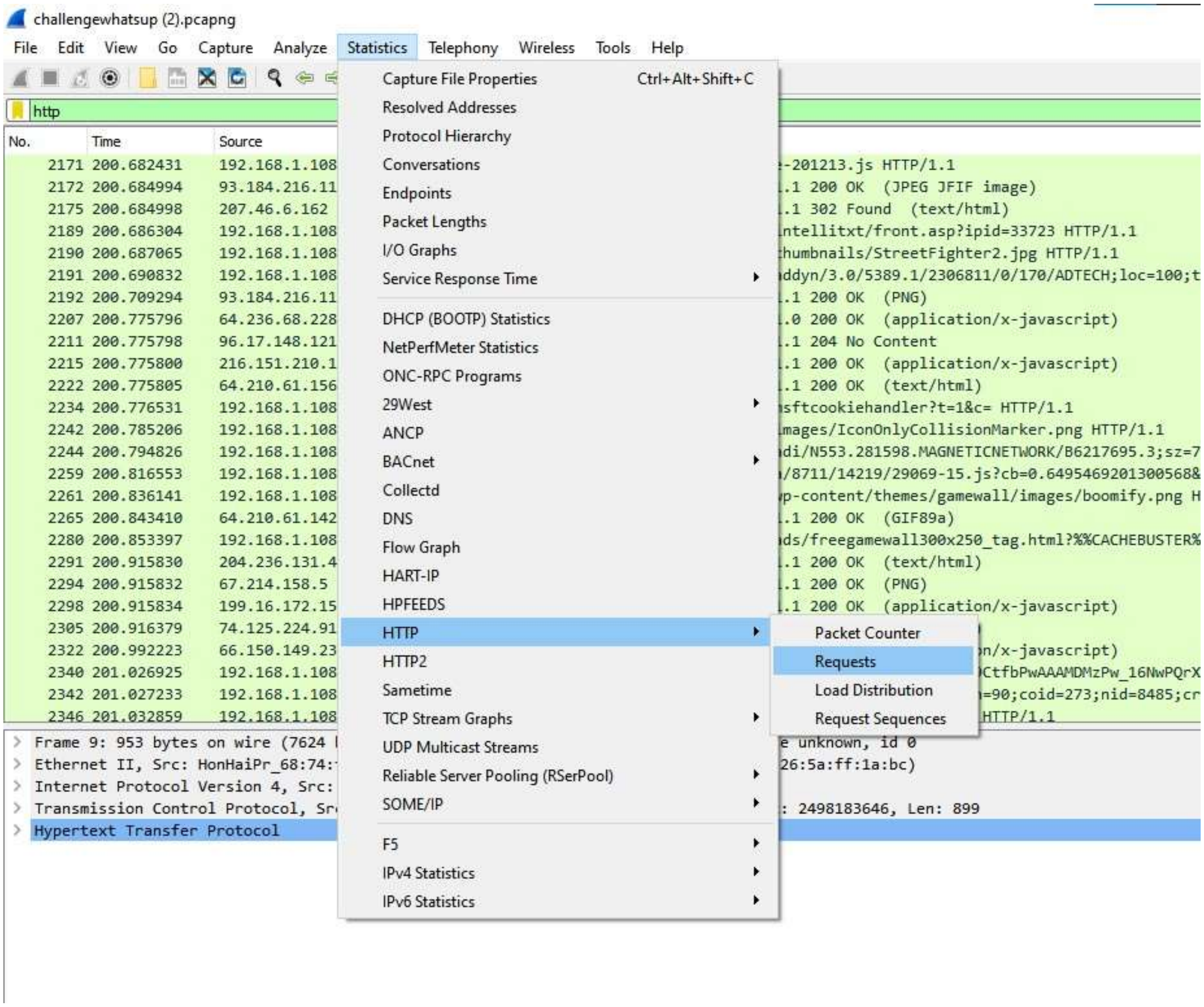
```
http
```

```
No.     Time        Source           Destination       Protocol  Length Info
      9 0.473514    192.168.1.108    199.127.204.121   HTTP        953 GET /dynamic_companion_banner_iframe.html?placement
     12 0.633588    74.125.224.91    192.168.1.108     HTTP       1400 HTTP/1.1 200 OK  (application/x-javascript)
     17 0.638228    192.168.1.108    69.171.228.14     HTTP        971 GET /plugins/likebox.php?href=http%3A%2F%2Fwww.face
     18 0.639591    192.168.1.108    74.125.224.91     HTTP        980 GET /adi/N5315.150834.6623026258321/B6413695.6;sz=7
     25 0.833530    192.168.1.108    62.128.215.93     HTTP        791 GET /adserver/www/delivery/ajs.php?zoneid=32&cb=737
     29 1.183644    192.168.1.108    74.125.224.91     HTTP       1414 GET /adj/N6344.272756.AOLADVERTISING/B6390033.49;sz
     32 1.193306    192.168.1.108    208.111.148.210   HTTP        617 GET /ym/1615/rSSaAiGN_512K_480x360.flv HTTP/1.1
     38 1.657567    69.171.228.14    192.168.1.108     HTTP         64 HTTP/1.1 200 OK  (text/html)
     44 1.694739    199.127.204.121  192.168.1.108     HTTP       1426 HTTP/1.1 200 OK  (text/html)
     54 1.880023    69.171.228.14    192.168.1.108     HTTP         76 HTTP/1.1 200 OK  (text/html)
     58 2.009261    74.125.224.91    192.168.1.108     HTTP        791 HTTP/1.1 200 OK  (text/html)
     60 2.009880    192.168.1.108    74.125.224.91     HTTP        996 GET /adi/N3905.YuMe/B6229987.3;sz=300x250;ord=72696
     62 2.024722    192.168.1.108    74.125.224.155    HTTP        616 GET /1831140/1-hopper_SizeMatters_728x90.swf HTTP/1
     68 2.604156    192.168.1.108    96.17.148.121     HTTP        487 GET /b?c1=3&c2=6035940&rn=0.066795493680888&c7=http
     70 2.609406    192.168.1.108    204.154.111.33    HTTP        150 GET /visit.js?ctx=1000798&cmp=6390033&ipos=&sid=101
     73 2.847181    62.128.215.93    192.168.1.108     HTTP        987 HTTP/1.0 200 OK  (text/javascript)
     84 3.591692    74.125.224.91    192.168.1.108     HTTP       1401 HTTP/1.1 200 OK  (application/x-javascript)
```

```
> Frame 9: 953 bytes on wire (7624 bits), 953 bytes captured (7624
> Ethernet II, Src: HonHaiPr_68:74:f6 (90:4c:e5:68:74:f6), Dst: D-L
> Internet Protocol Version 4, Src: 192.168.1.108, Dst: 199.127.204
> Transmission Control Protocol, Src Port: 50855, Dst Port: 80, Sec
> Hypertext Transfer Protocol
```

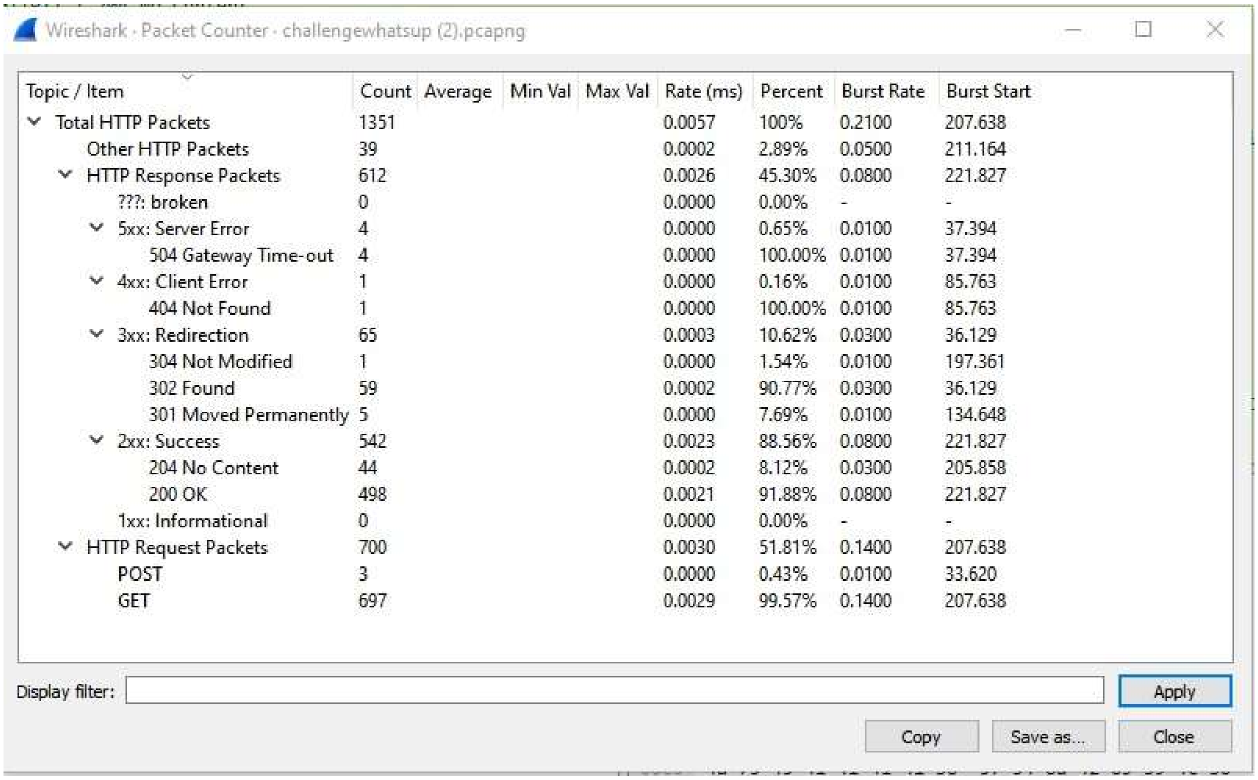
```
0000  00 26 5a ff 1a bc 90 4c  e5 68 74 f6 08 00 45 00   ·&Z····L
0010  03 ab 69 45 40 00 80 06  37 fa c0 a8 01 6c c7 7f   ··iE@···
0020  cc 79 c6 a7 00 50 d4 e0  23 79 94 e7 41 de 50 18   ·y···P··
0030  40 29 5c 52 00 00 47 45  54 20 2f 64 79 6e 61 6d   @)\R··GE
0040  69 63 5f 63 6f 6d 70 61  6e 69 6f 6e 5f 62 61 6e   ic_compa
0050  6e 65 72 5f 69 66 72 61  6d 65 2e 68 74 6d 6c 3f   ner_ifra
0060  70 6c 61 63 65 6d 65 6e  74 5f 69 64 3d 38 30 37   placemen
0070  30 35 26 61 64 76 65 72  74 69 73 65 6d 65 6e 74   05&adver
0080  5f 69 64 3d 33 39 38 31  32 26 63 62 5f 69 64 3d   _id=3981
0090  34 33 37 30 38 26 74 72  61 63 6b 65 72 3d 30 72   43708&tr
00a0  4f 30 41 42 58 63 68 41  41 41 41 41 51 41 41 41   O0ABXchA
00b0  41 41 42 30 35 54 67 41  67 41 42 4f 30 45 41 41   AAB05TgA
00c0  4a 75 45 41 41 41 41 36  57 54 6a 42 69 59 4c 30   JuEAAAA6
00d0  76 76 70 26 77 69 64 74  68 3d 33 30 30 26 68 65   vvp&widt
00e0  69 67 68 74 3d 32 35 30  20 48 54 54 50 2f 31 2e   ight=250
00f0  31 0d 0a 41 63 63 65 70  74 3a 20 61 70 70 6c 69   1··Accep
0100  63 61 74 69 6f 6e 2f 78  2d 6d 73 2d 61 70 70 6c   cation/x
0110  69 63 61 74 69 6f 6e 2c  20 69 6d 61 67 65 2f 6a   ication,
0120  70 65 67 2c 20 61 70 70  6c 69 63 61 74 69 6f 6e   peg, app
0130  2f 78 61 6d 6c 2b 78 6d  6c 2c 20 69 6d 61 67 65   /xaml+xm
0140  2f 67 69 66 2c 20 69 6d  61 67 65 2f 70 6a 70 65   /gif, im
```

Step-2:- Open Wireshark—-->Go to Statistics —--->Select HTTP



```
No.     Time        Source
  2171 200.682431  192.168.1.108                                     -201213.js HTTP/1.1
  2172 200.684994  93.184.216.11                                     .1 200 OK  (JPEG JFIF image)
  2175 200.684998  207.46.6.162                                      .1 302 Found  (text/html)
  2189 200.686304  192.168.1.108                                     ntellitxt/front.asp?ipid=33723 HTTP/1.1
  2190 200.687065  192.168.1.108                                     humbnails/StreetFighter2.jpg HTTP/1.1
  2191 200.690832  192.168.1.108                                     ddyn/3.0/5389.1/2306811/0/170/ADTECH;loc=100;t
  2192 200.709294  93.184.216.11                                     .1 200 OK  (PNG)
  2207 200.775796  64.236.68.228                                     .0 200 OK  (application/x-javascript)
  2211 200.775798  96.17.148.121                                     .1 204 No Content
  2215 200.775800  216.151.210.1                                     .1 200 OK  (application/x-javascript)
  2222 200.775805  64.210.61.156                                     .1 200 OK  (text/html)
  2234 200.776531  192.168.1.108                                     sftcookiehandler?t=1&c= HTTP/1.1
  2242 200.785206  192.168.1.108                                     mages/IconOnlyCollisionMarker.png HTTP/1.1
  2244 200.794826  192.168.1.108                                     di/N553.281598.MAGNETICNETWORK/B6217695.3;sz=7
  2259 200.816553  192.168.1.108                                     /8711/14219/29069-15.js?cb=0.6495469201300568&
  2261 200.836141  192.168.1.108                                     p-content/themes/gamewall/images/boomify.png H
  2265 200.843410  64.210.61.142                                     .1 200 OK  (GIF89a)
  2280 200.853397  192.168.1.108                                     ds/freegamewall300x250_tag.html?%%CACHEBUSTER%
  2291 200.915830  204.236.131.4                                     .1 200 OK  (text/html)
  2294 200.915832  67.214.158.5                                      .1 200 OK  (PNG)
  2298 200.915834  199.16.172.15                                     .1 200 OK  (application/x-javascript)
  2305 200.916379  74.125.224.91
  2322 200.992223  66.150.149.23                                                           n/x-javascript)
  2340 201.026925  192.168.1.108                                                           CtfbPwAAAMDMzPw_16NwPQrX
  2342 201.027233  192.168.1.108                                                           =90;coid=273;nid=8485;cr
  2346 201.032859  192.168.1.108                                                           HTTP/1.1

> Frame 9: 953 bytes on wire (7624                                   e unknown, id 0
> Ethernet II, Src: HonHaiPr_68:74:                                  26:5a:ff:1a:bc)
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr                                  : 2498183646, Len: 899
> Hypertext Transfer Protocol
```

Step-3:- HTTP Post request



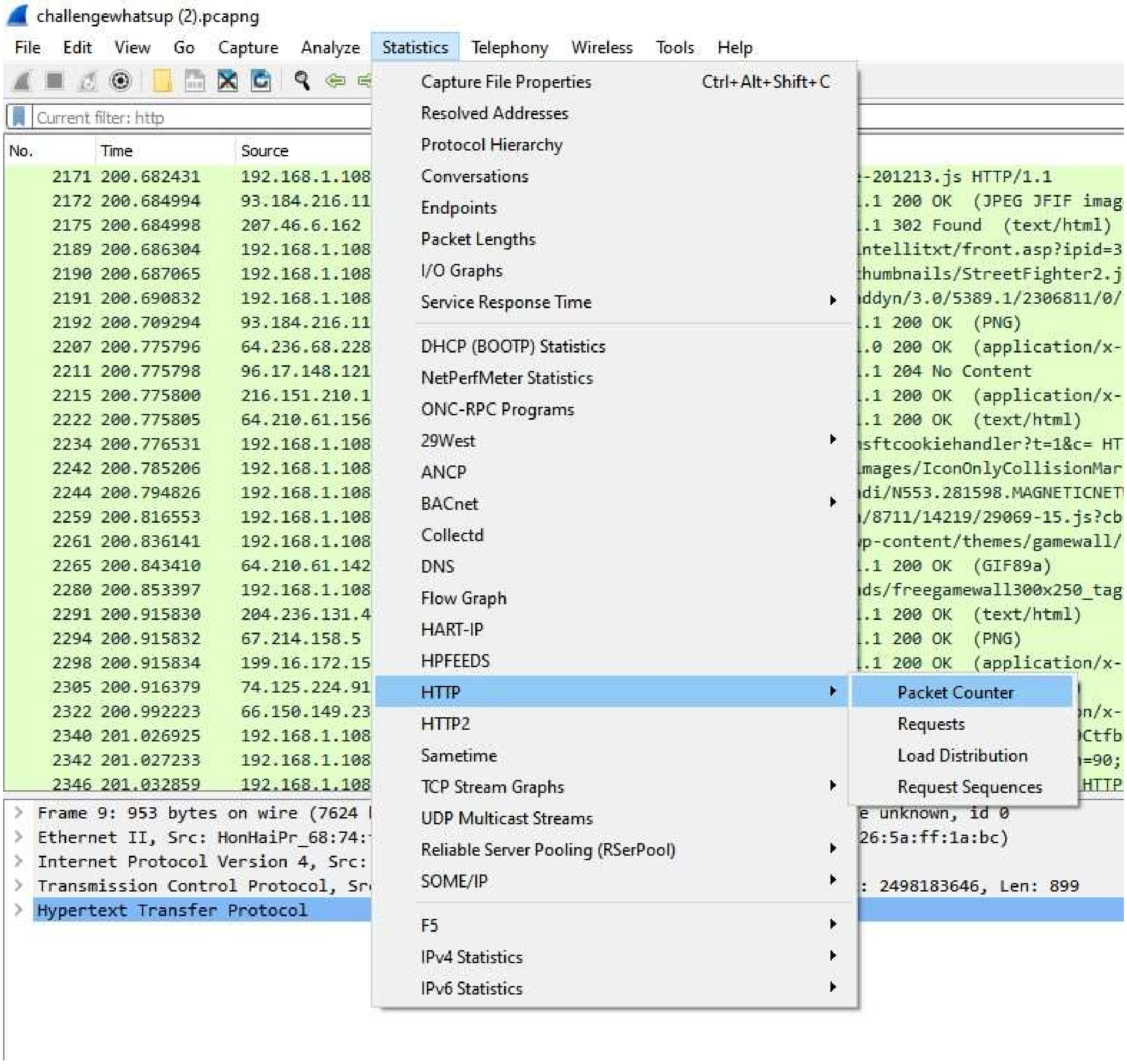
Wireshark · Packet Counter · challengewhatsup (2).pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	1351				0.0057	100%	0.2100	207.638
Other HTTP Packets	39				0.0002	2.89%	0.0500	211.164
HTTP Response Packets	612				0.0026	45.30%	0.0800	221.827
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	4				0.0000	0.65%	0.0100	37.394
504 Gateway Time-out	4				0.0000	100.00%	0.0100	37.394
4xx: Client Error	1				0.0000	0.16%	0.0100	85.763
404 Not Found	1				0.0000	100.00%	0.0100	85.763
3xx: Redirection	65				0.0003	10.62%	0.0300	36.129
304 Not Modified	1				0.0000	1.54%	0.0100	197.361
302 Found	59				0.0002	90.77%	0.0300	36.129
301 Moved Permanently	5				0.0000	7.69%	0.0100	134.648
2xx: Success	542				0.0023	88.56%	0.0800	221.827
204 No Content	44				0.0002	8.12%	0.0300	205.858
200 OK	498				0.0021	91.88%	0.0800	221.827
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	700				0.0030	51.81%	0.1400	207.638
POST	3				0.0000	0.43%	0.0100	33.620
GET	697				0.0029	99.57%	0.1400	207.638

Display filter:

13. What application appears to be generating the GET/POST requests?

Step-1:- Open Wireshark—-->Go to Statistics —--->Select HTTP —--->Packet Counter



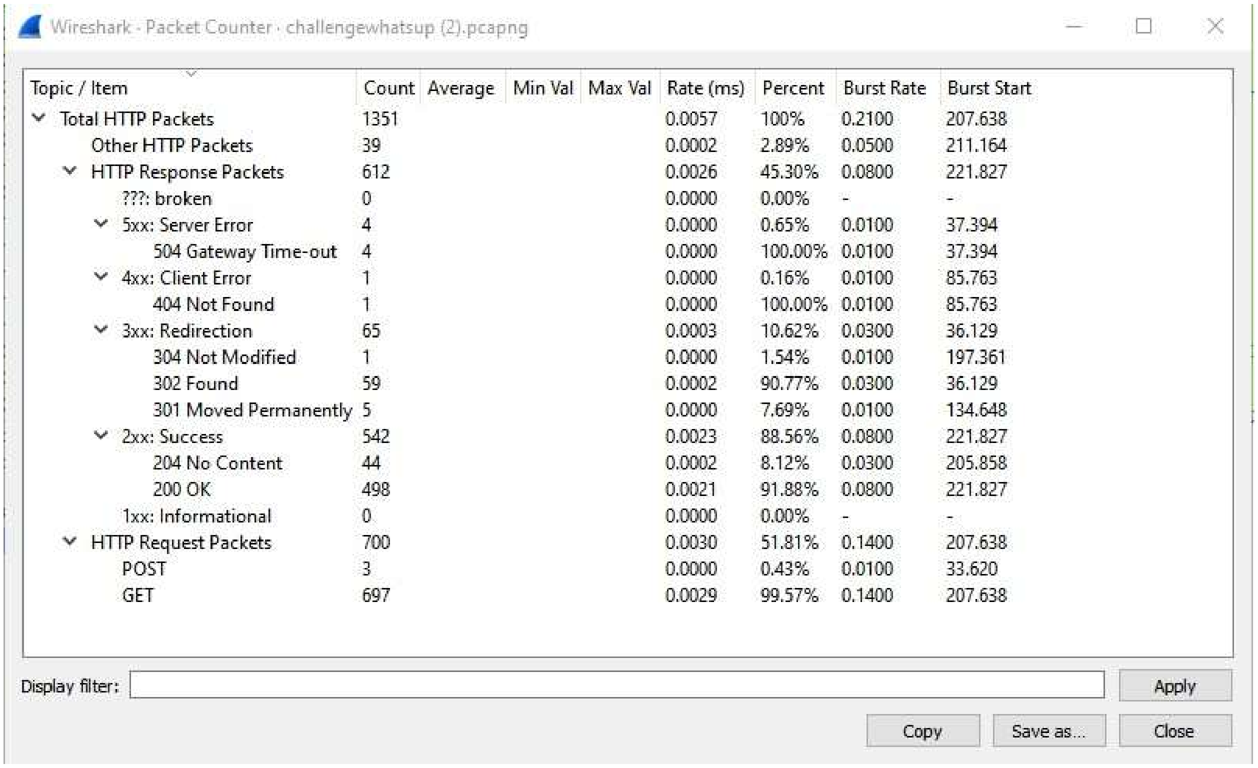
challengewhatsup (2).pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

```
No.   Time         Source
2171 200.682431   192.168.1.108     -201213.js HTTP/1.1
2172 200.684994   93.184.216.11     .1 200 OK  (JPEG JFIF imag
2175 200.684998   207.46.6.162      .1 302 Found  (text/html)
2189 200.686304   192.168.1.108     ntellitxt/front.asp?ipid=3
2190 200.687065   192.168.1.108     humbnails/StreetFighter2.j
2191 200.690832   192.168.1.108     ddyn/3.0/5389.1/2306811/0/
2192 200.709294   93.184.216.11     .1 200 OK  (PNG)
2207 200.775796   64.236.68.228     .0 200 OK  (application/x-
2211 200.775798   96.17.148.121     .1 204 No Content
2215 200.775800   216.151.210.1     .1 200 OK  (application/x-
2222 200.775805   64.210.61.156     .1 200 OK  (text/html)
2234 200.776531   192.168.1.108     sftcookiehandler?t=1&c= HT
2242 200.785206   192.168.1.108     mages/IconOnlyCollisionMar
2244 200.794826   192.168.1.108     di/N553.281598.MAGNETICNET
2259 200.816553   192.168.1.108     /8711/14219/29069-15.js?cb
2261 200.836141   192.168.1.108     p-content/themes/gamewall/
2265 200.843410   64.210.61.142     .1 200 OK  (GIF89a)
2280 200.853397   192.168.1.108     ds/freegamewall300x250_tag
2291 200.915830   204.236.131.4     .1 200 OK  (text/html)
2294 200.915832   67.214.158.5      .1 200 OK  (PNG)
2298 200.915834   199.16.172.15     .1 200 OK  (application/x-
2305 200.916379   74.125.224.91     )
2322 200.992223   66.150.149.23     n/x-
2340 201.026925   192.168.1.108     Ctfb
2342 201.027233   192.168.1.108     =90;
2346 201.032859   192.168.1.108     HTTP

> Frame 9: 953 bytes on wire (7624        e unknown, id 0
> Ethernet II, Src: HonHaiPr_68:74:        26:5a:ff:1a:bc)
> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr        : 2498183646, Len: 899
> Hypertext Transfer Protocol
```

Step-2:-

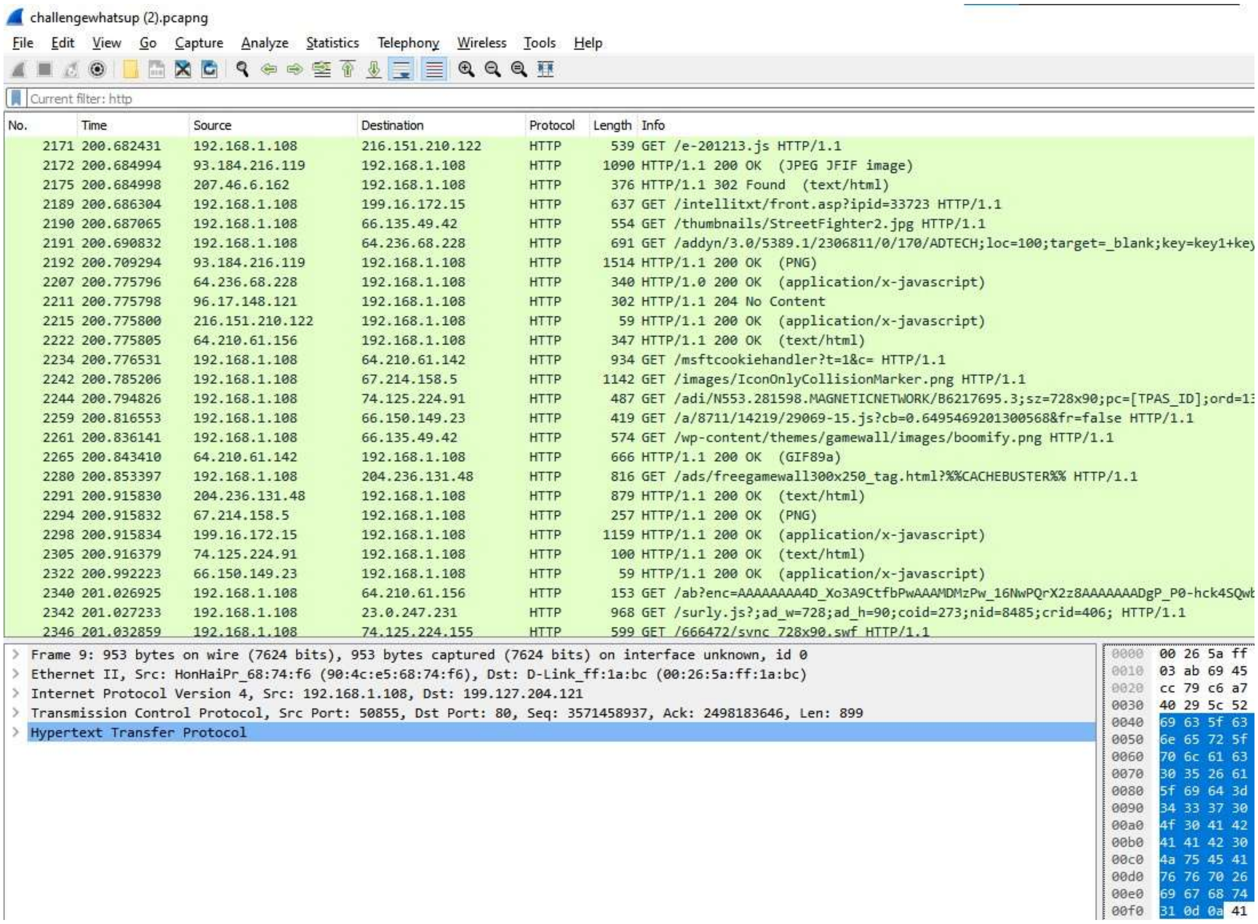


Wireshark · Packet Counter · challengewhatsup (2).pcapng

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	1351				0.0057	100%	0.2100	207.638
Other HTTP Packets	39				0.0002	2.89%	0.0500	211.164
HTTP Response Packets	612				0.0026	45.30%	0.0800	221.827
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	4				0.0000	0.65%	0.0100	37.394
504 Gateway Time-out	4				0.0000	100.00%	0.0100	37.394
4xx: Client Error	1				0.0000	0.16%	0.0100	85.763
404 Not Found	1				0.0000	100.00%	0.0100	85.763
3xx: Redirection	65				0.0003	10.62%	0.0300	36.129
304 Not Modified	1				0.0000	1.54%	0.0100	197.361
302 Found	59				0.0002	90.77%	0.0300	36.129
301 Moved Permanently	5				0.0000	7.69%	0.0100	134.648
2xx: Success	542				0.0023	88.56%	0.0800	221.827
204 No Content	44				0.0002	8.12%	0.0300	205.858
200 OK	498				0.0021	91.88%	0.0800	221.827
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	700				0.0030	51.81%	0.1400	207.638
POST	3				0.0000	0.43%	0.0100	33.620
GET	697				0.0029	99.57%	0.1400	207.638

Display filter:

Step-3:-



Current filter: http

```
No.      Time         Source            Destination       Protocol  Length Info
    2171 200.682431   192.168.1.108     216.151.210.122   HTTP       539 GET /e-201213.js HTTP/1.1
    2172 200.684994   93.184.216.119    192.168.1.108     HTTP      1090 HTTP/1.1 200 OK  (JPEG JFIF image)
    2175 200.684998   207.46.6.162      192.168.1.108     HTTP       376 HTTP/1.1 302 Found  (text/html)
    2189 200.686304   192.168.1.108     199.16.172.15     HTTP       637 GET /intellitxt/front.asp?ipid=33723 HTTP/1.1
    2190 200.687065   192.168.1.108     66.135.49.42      HTTP       554 GET /thumbnails/StreetFighter2.jpg HTTP/1.1
    2191 200.690832   192.168.1.108     64.236.68.228     HTTP       691 GET /addyn/3.0/5389.1/2306811/0/170/ADTECH;loc=100;target=_blank;key=key1+key
    2192 200.709294   93.184.216.119    192.168.1.108     HTTP      1514 HTTP/1.1 200 OK  (PNG)
    2207 200.775796   64.236.68.228     192.168.1.108     HTTP       340 HTTP/1.0 200 OK  (application/x-javascript)
    2211 200.775798   96.17.148.121     192.168.1.108     HTTP       302 HTTP/1.1 204 No Content
    2215 200.775800   216.151.210.122   192.168.1.108     HTTP        59 HTTP/1.1 200 OK  (application/x-javascript)
    2222 200.775805   64.210.61.156     192.168.1.108     HTTP       347 HTTP/1.1 200 OK  (text/html)
    2234 200.776531   192.168.1.108     64.210.61.142     HTTP       934 GET /msftcookiehandler?t=1&c= HTTP/1.1
    2242 200.785206   192.168.1.108     67.214.158.5      HTTP      1142 GET /images/IconOnlyCollisionMarker.png HTTP/1.1
    2244 200.794826   192.168.1.108     74.125.224.91     HTTP       487 GET /adi/N553.281598.MAGNETICNETWORK/B6217695.3;sz=728x90;pc=[TPAS_ID];ord=1:
    2259 200.816553   192.168.1.108     66.150.149.23     HTTP       419 GET /a/8711/14219/29069-15.js?cb=0.6495469201300568&fr=false HTTP/1.1
    2261 200.836141   192.168.1.108     66.135.49.42      HTTP       574 GET /wp-content/themes/gamewall/images/boomify.png HTTP/1.1
    2265 200.843410   64.210.61.142     192.168.1.108     HTTP       666 HTTP/1.1 200 OK  (GIF89a)
    2280 200.853397   192.168.1.108     204.236.131.48    HTTP       816 GET /ads/freegamewall300x250_tag.html?%%CACHEBUSTER%% HTTP/1.1
    2291 200.915830   204.236.131.48    192.168.1.108     HTTP       879 HTTP/1.1 200 OK  (text/html)
    2294 200.915832   67.214.158.5      192.168.1.108     HTTP       257 HTTP/1.1 200 OK  (PNG)
    2298 200.915834   199.16.172.15     192.168.1.108     HTTP      1159 HTTP/1.1 200 OK  (application/x-javascript)
    2305 200.916379   74.125.224.91     192.168.1.108     HTTP       100 HTTP/1.1 200 OK  (text/html)
    2322 200.992223   66.150.149.23     192.168.1.108     HTTP        59 HTTP/1.1 200 OK  (application/x-javascript)
    2340 201.026925   192.168.1.108     64.210.61.156     HTTP       153 GET /ab?enc=AAAAAAAA4D_Xo3A9CtfbPwAAAMDMzPw_16NwPQrX2z8AAAAAAADgP_P0-hck4SQwb
    2342 201.027233   192.168.1.108     23.0.247.231      HTTP       968 GET /surly.js?;ad_w=728;ad_h=90;coid=273;nid=8485;crid=406; HTTP/1.1
    2346 201.032859   192.168.1.108     74.125.224.155    HTTP       599 GET /666472/sync 728x90.swf HTTP/1.1
```

```
> Frame 9: 953 bytes on wire (7624 bits), 953 bytes captured (7624 bits) on interface unknown, id 0
> Ethernet II, Src: HonHaiPr_68:74:f6 (90:4c:e5:68:74:f6), Dst: D-Link_ff:1a:bc (00:26:5a:ff:1a:bc)
> Internet Protocol Version 4, Src: 192.168.1.108, Dst: 199.127.204.121
> Transmission Control Protocol, Src Port: 50855, Dst Port: 80, Seq: 3571458937, Ack: 2498183646, Len: 899
> Hypertext Transfer Protocol
```

```
0000  00 26 5a ff
0010  03 ab 69 45
0020  cc 79 c6 a7
0030  40 29 5c 52
0040  69 63 5f 63
0050  6e 65 72 5f
0060  70 6c 61 63
0070  30 35 26 61
0080  5f 69 64 3d
0090  34 33 37 30
00a0  4f 30 41 42
00b0  41 41 42 30
00c0  4a 75 45 41
00d0  76 76 70 26
00e0  69 67 68 74
00f0  31 0d 0a 41
```