Assignments:-1

Module:- NDC(WireShark)

Name:- Bhushan Pathrabe

Lab Assignment :-

Objective: Network Traffic Monitoring and Analysis using Wireshark

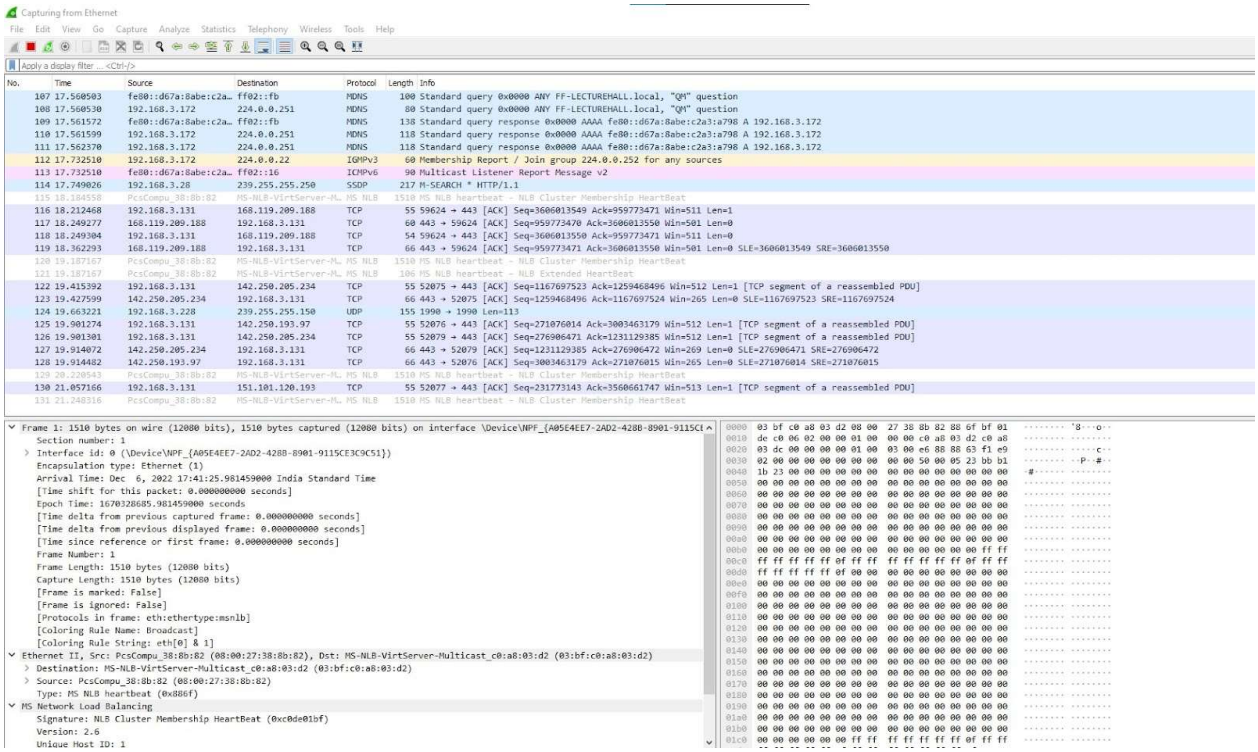
Tool Used: Wireshark

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

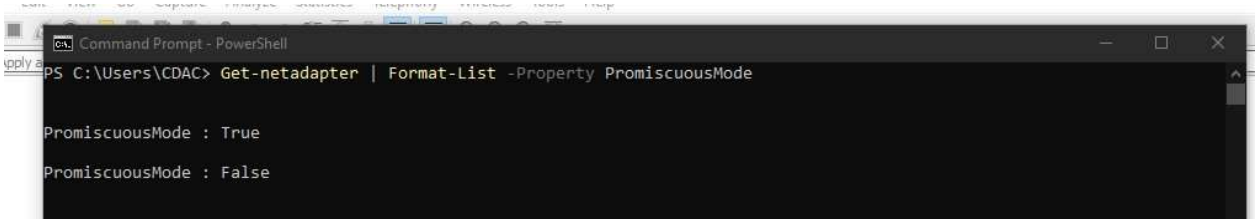
Person Duration: 3 Hours

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

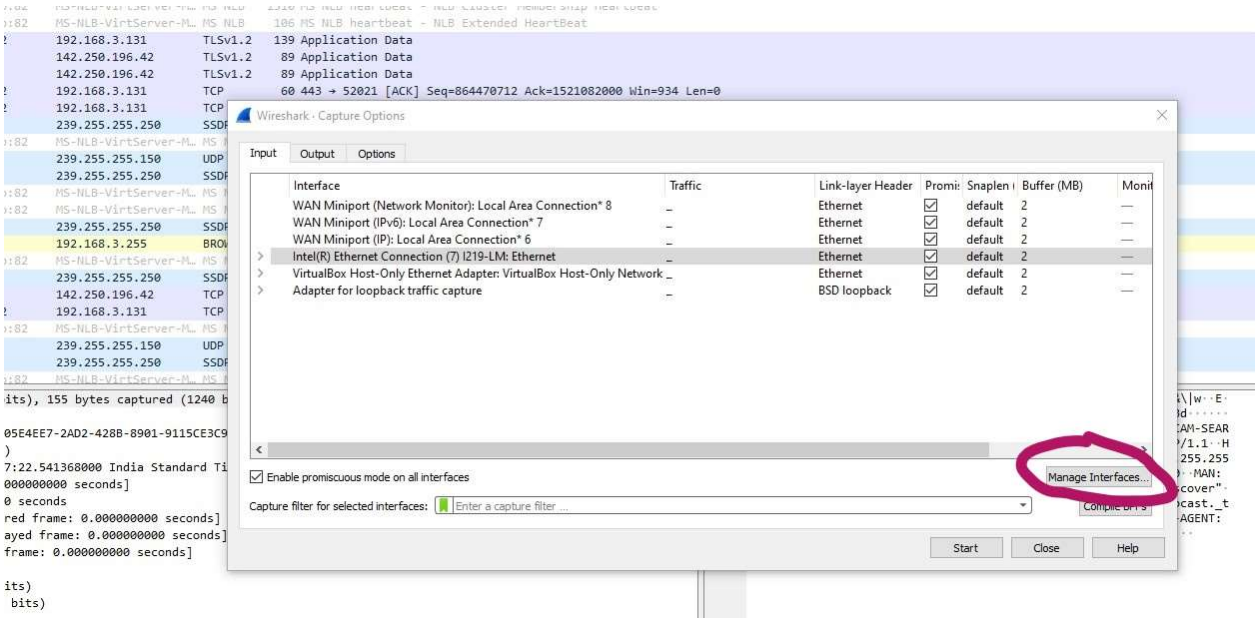


2. Check whether the network interface of your machine is in Promiscous mode. If it is not in promiscous mode, change it in to promiscous mode.

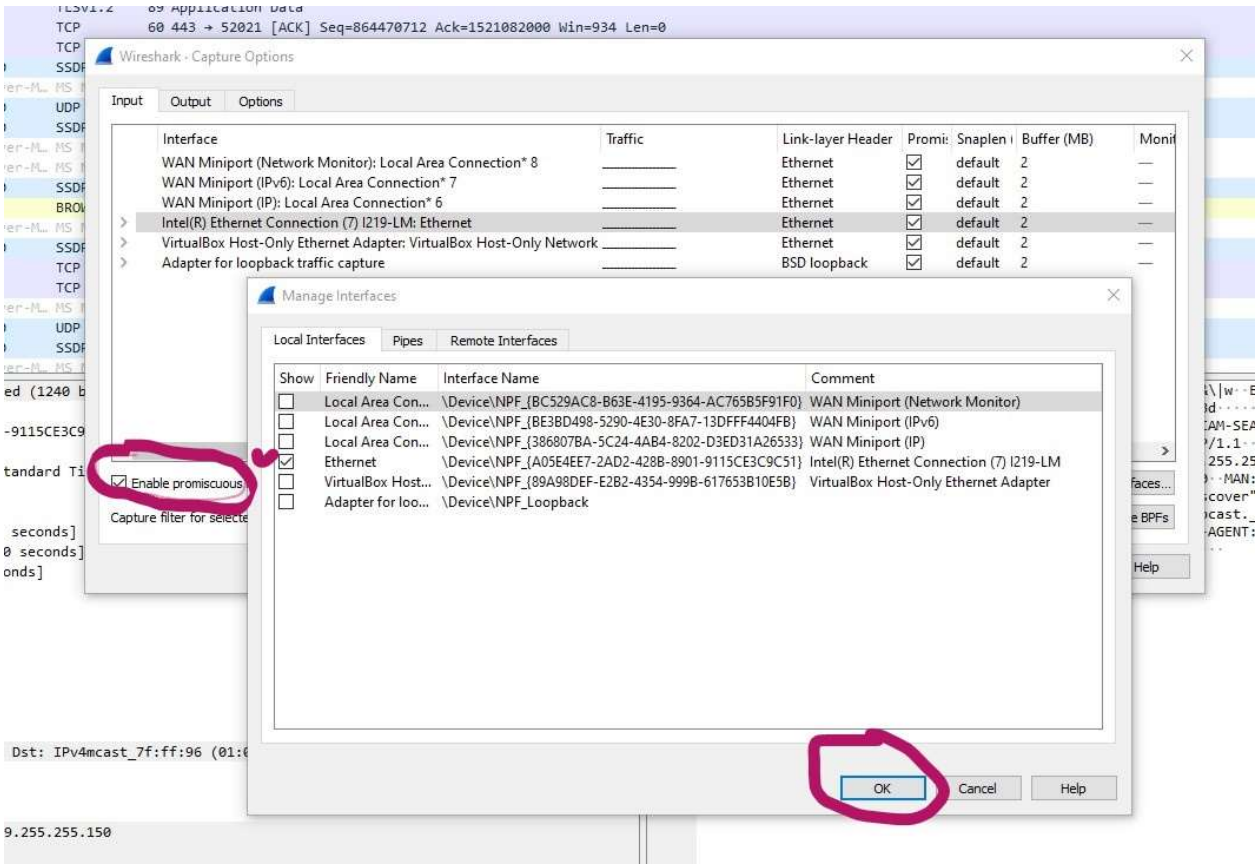
Step-1:- Go to Command Prompt And Check Promiscous mode



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



Step-3:- Enable promiscous and Click OK



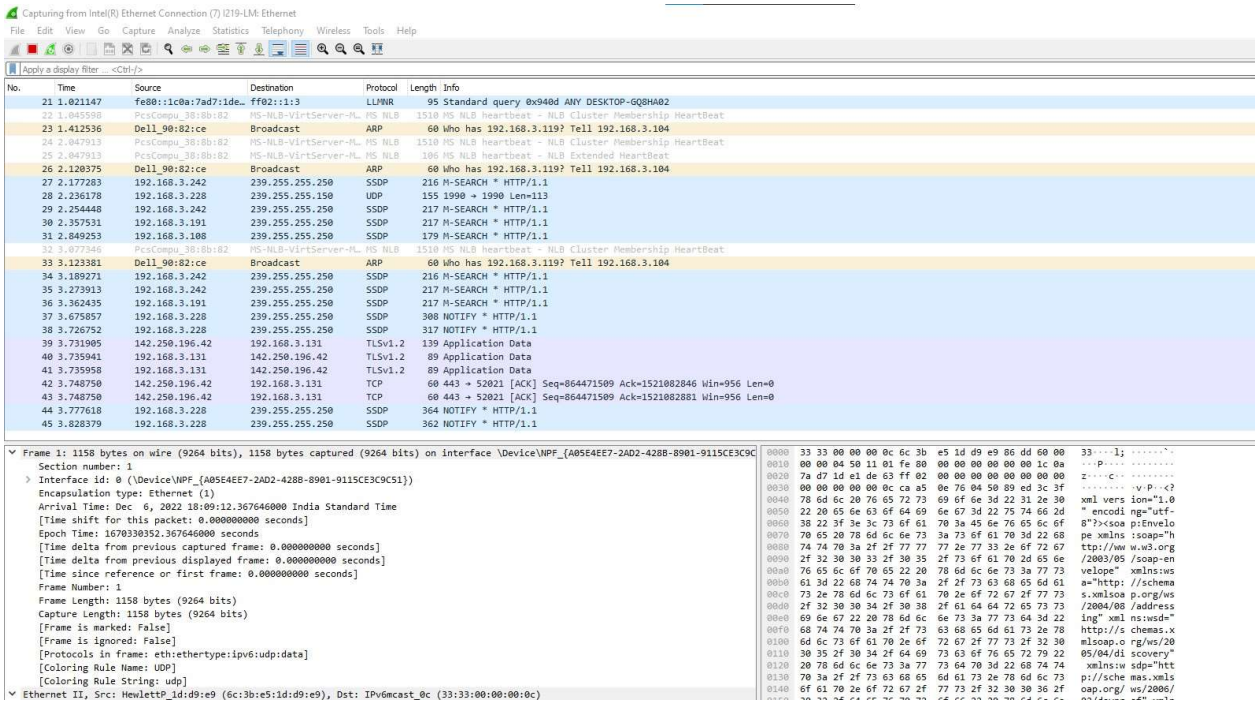
Step-3:- Check Changeable promiscous Mode on Command Prompt

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

PromiscuousMode : False

PromiscuousMode : False
```

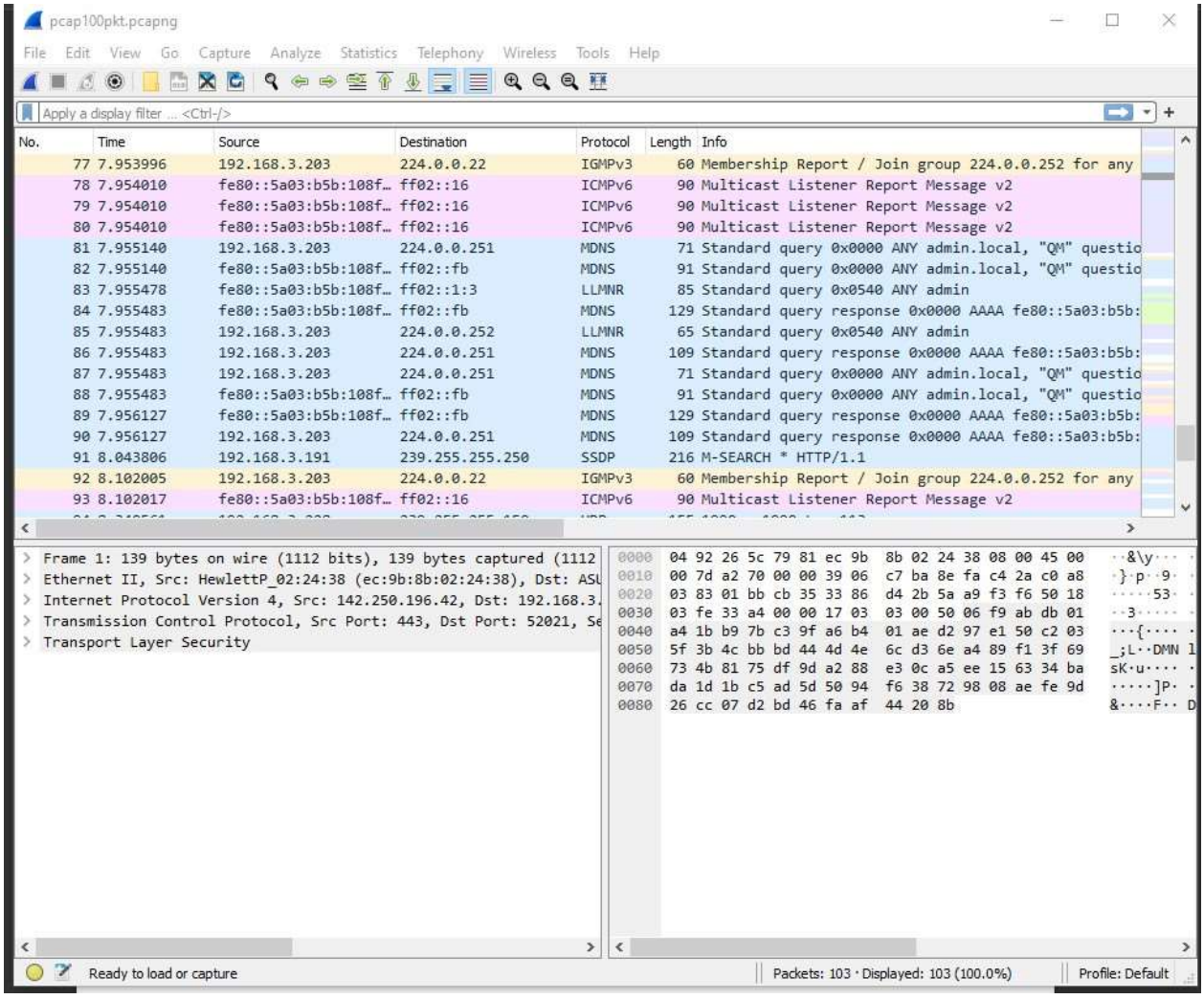
Step-4:- OPen Wire Shark and Run It



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

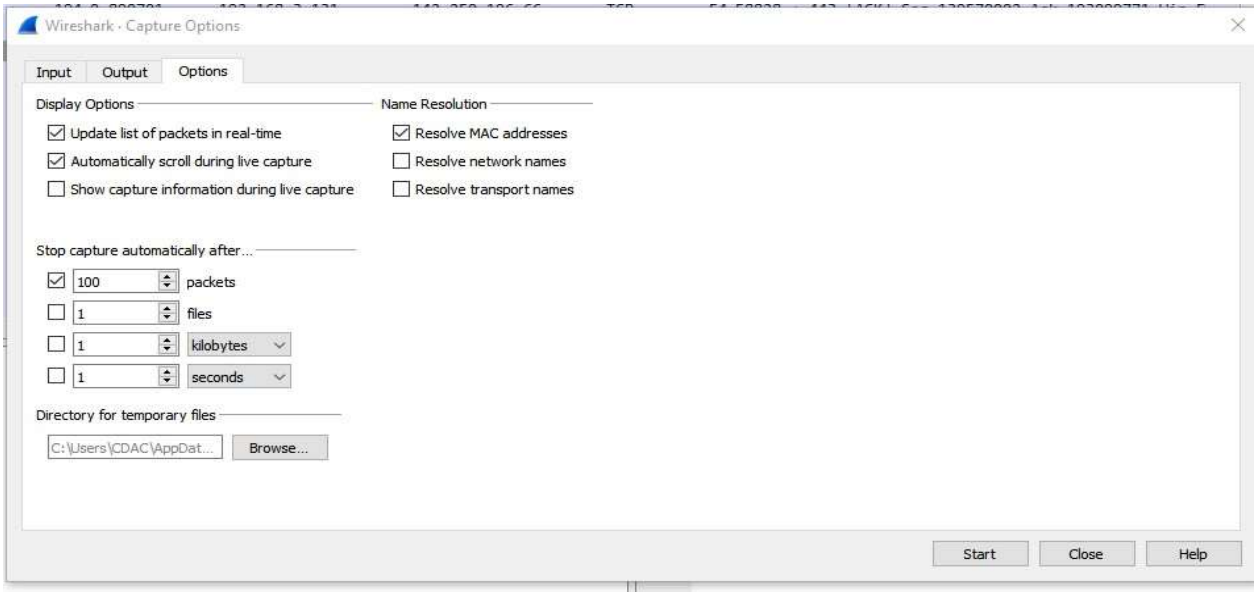
3.a) Stop after 100 packets and store in to a file “pcap100pkt”.

Open WireShark



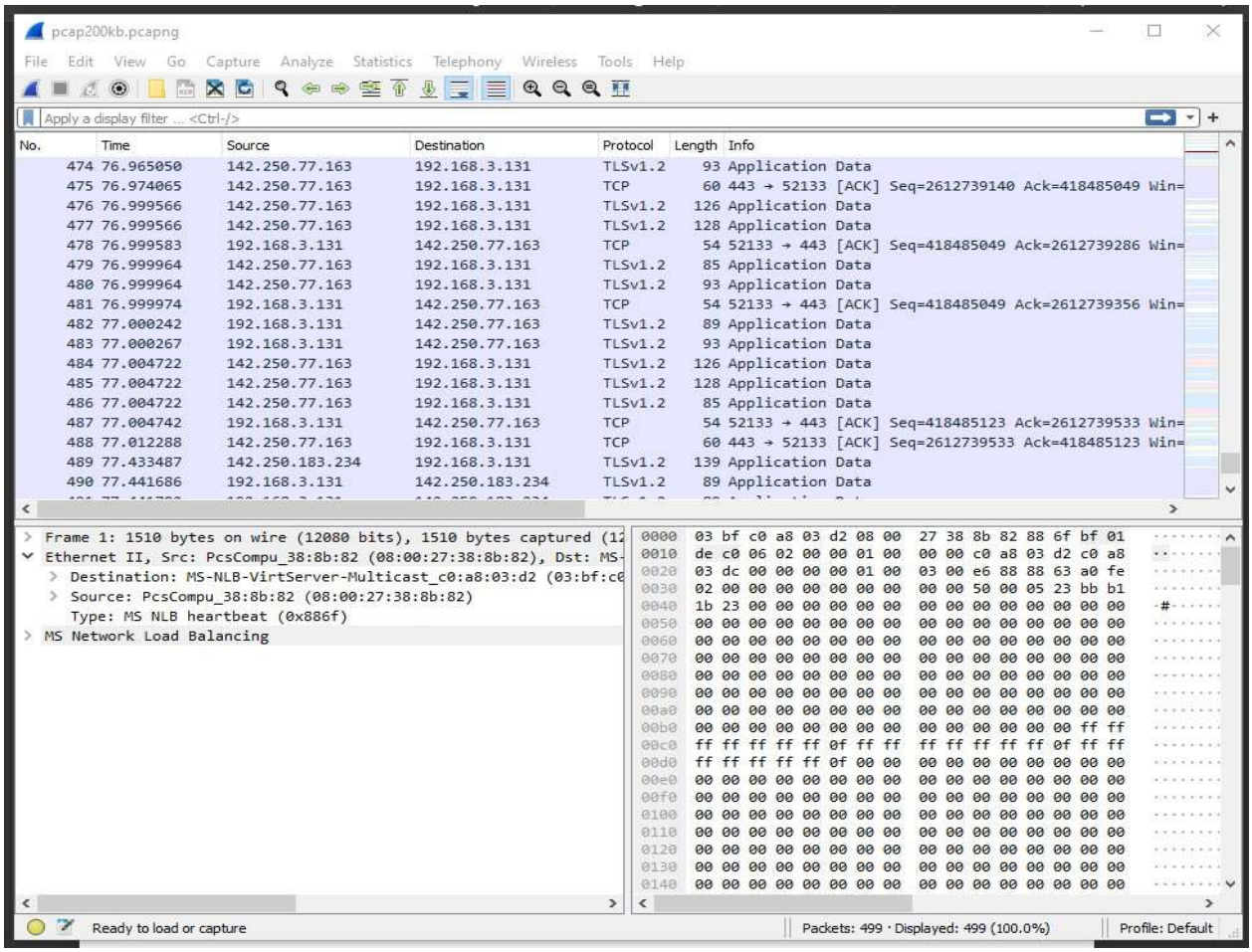
Go to Capture Option —-->Right Click —-->Select Option and Set packets=100

Start the WireShark
Save the file = pcap100pkt.pcap



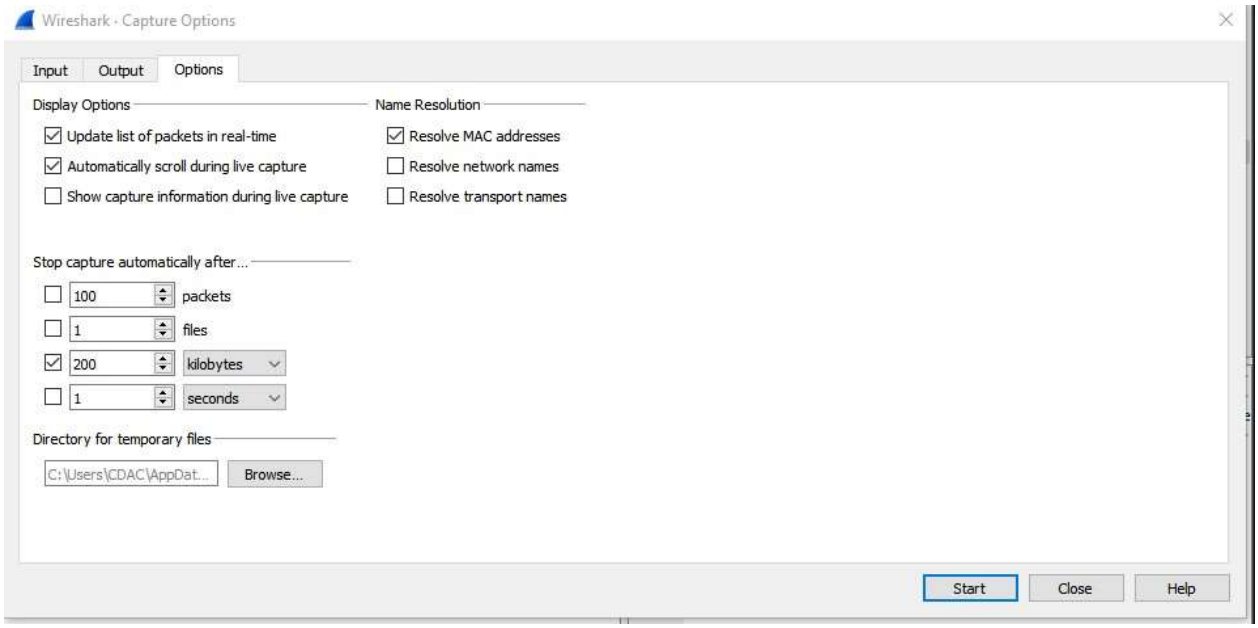
3.b)Stop after 200 Kb and store in to a file “pcap200kb”.

Open the Wire Shark



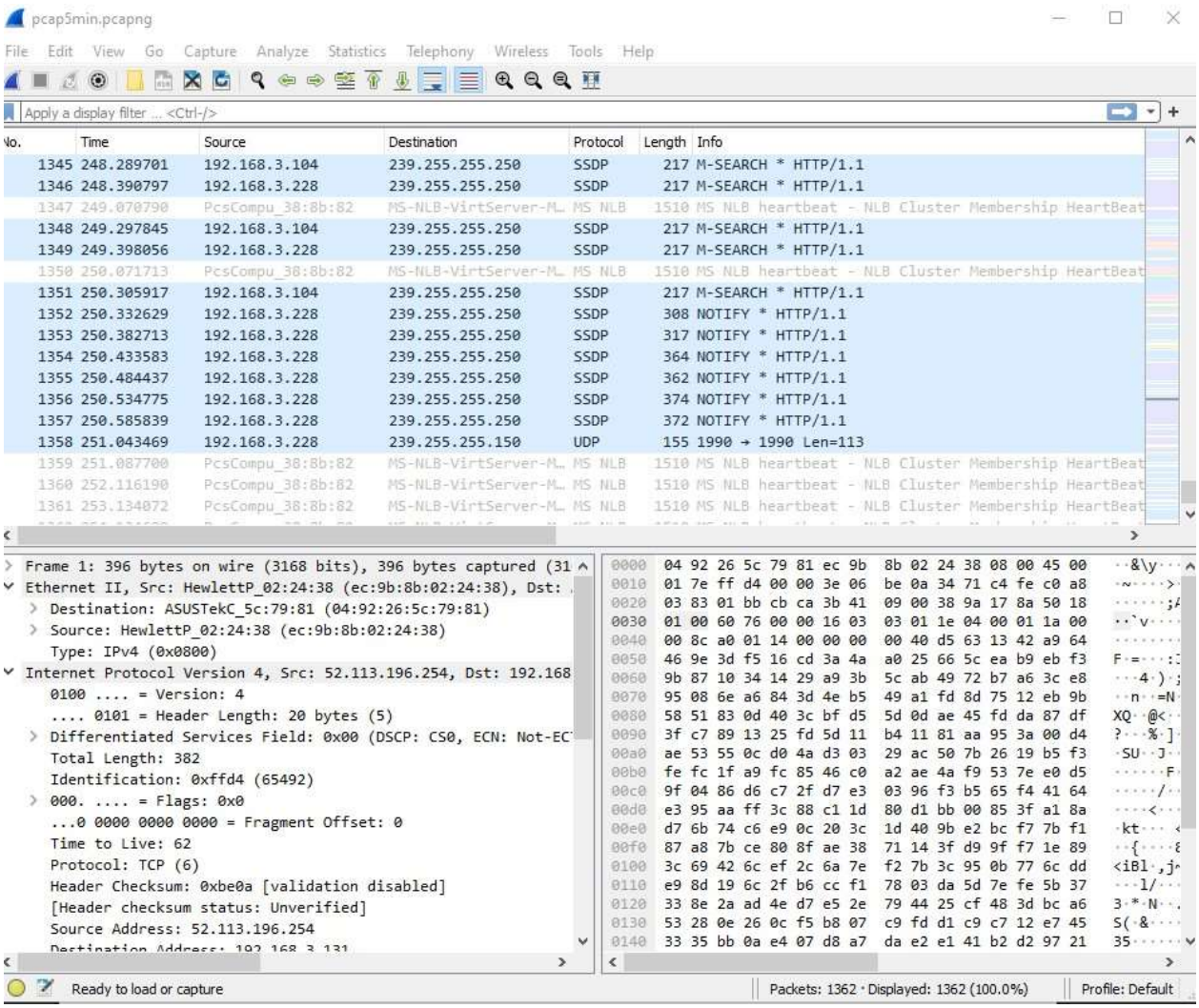
Go to Capture Option —-->Right Click —---->Select Option and Set Size=200kb

Start the WireShark
Save the file = pcap200kb.pcap



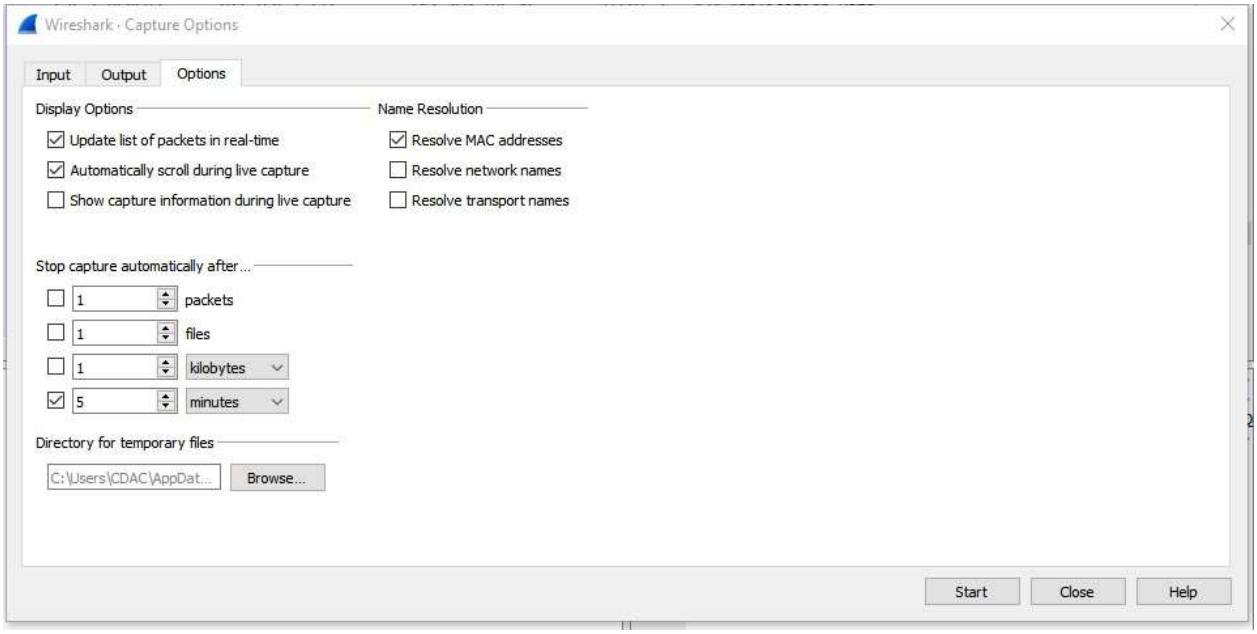
3.c) Stop after 5 minutes and store in to a file “pcap5min” .

Open the Wire Shark



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

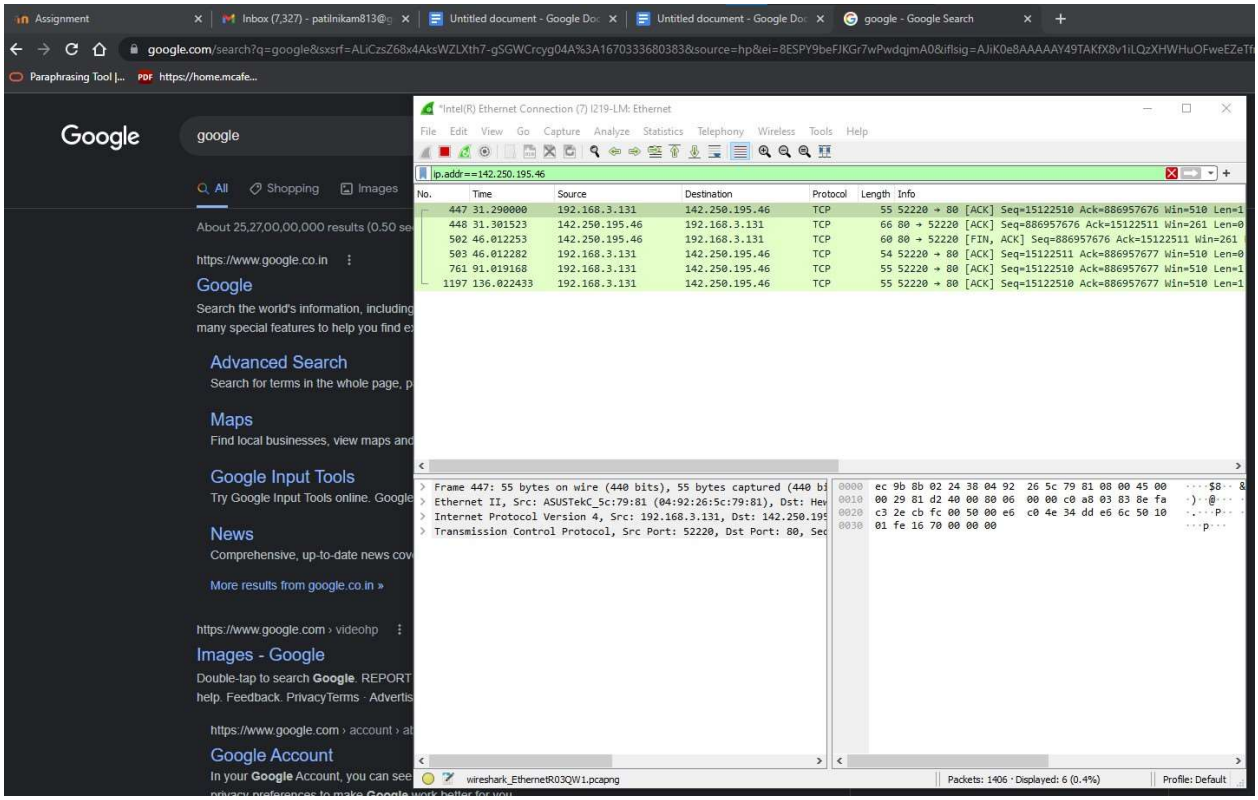
Start the WireShark
Save the file = pcap5min.pcap



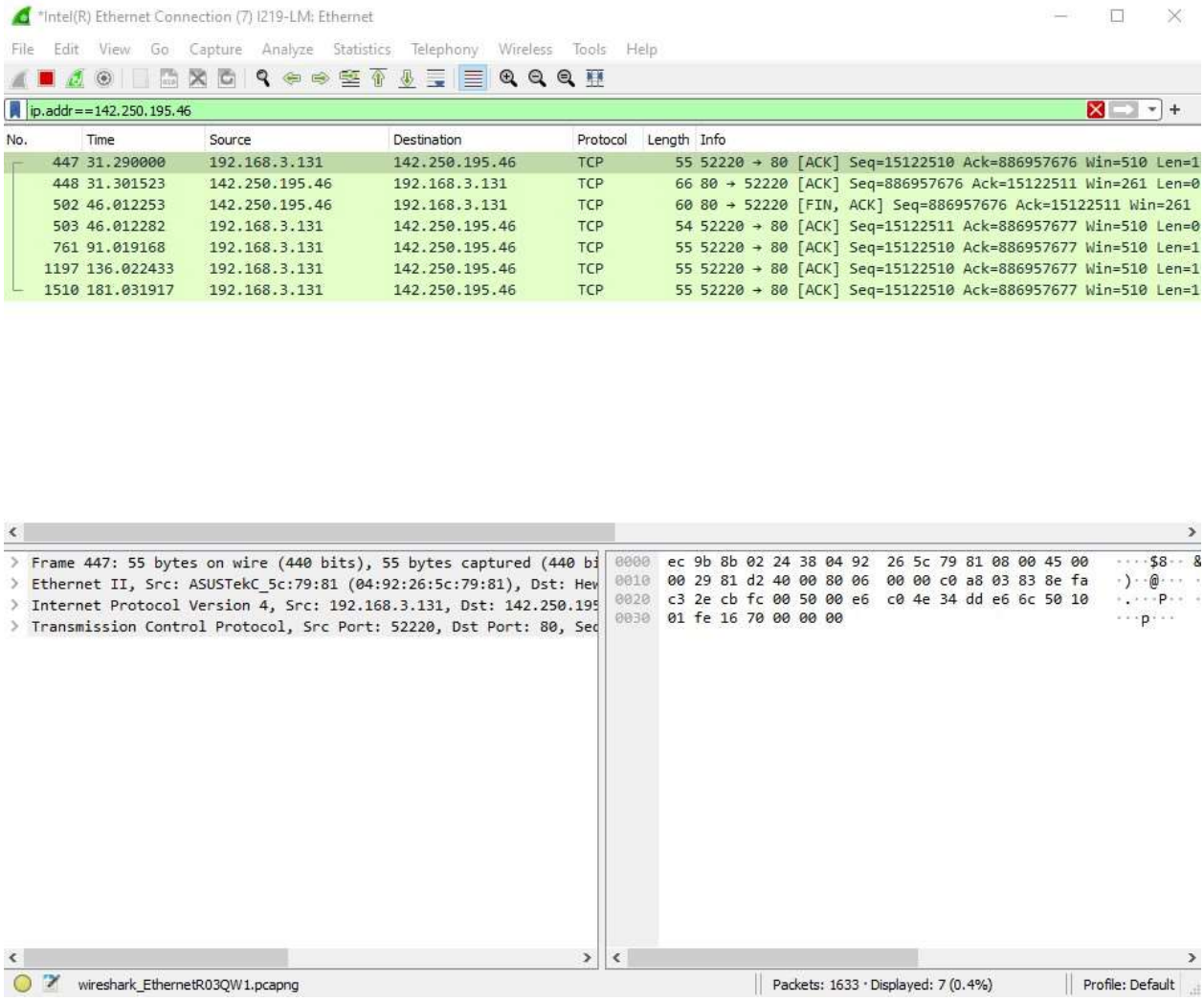
4. Capture live traffic from a particulat host (e.g from www.google.com) and store the captured file as “pcaphost.pcap”.

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

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

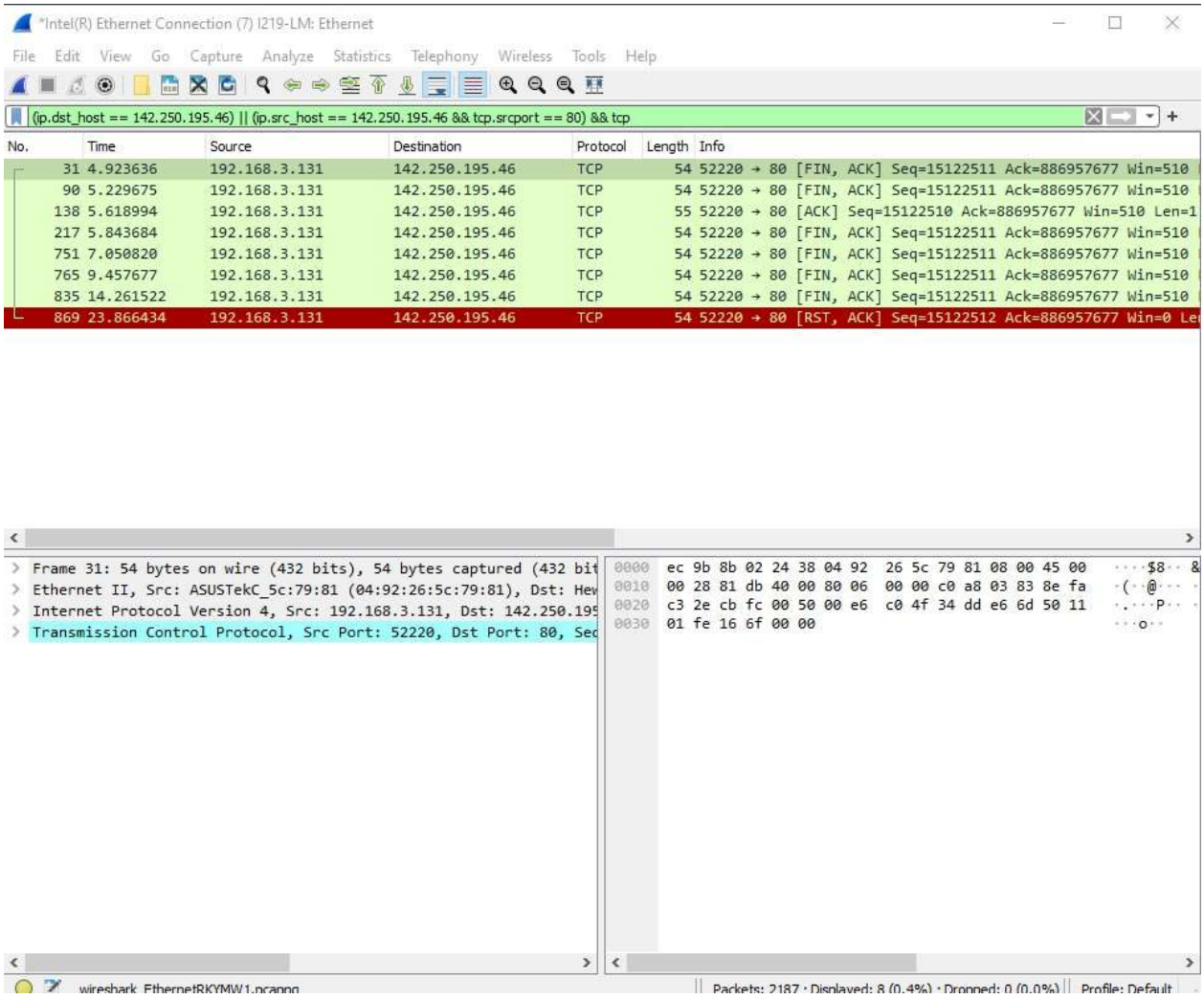


Step-3:- Now Capture The Live traffic through- ip.addr=-142.250.195.46



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

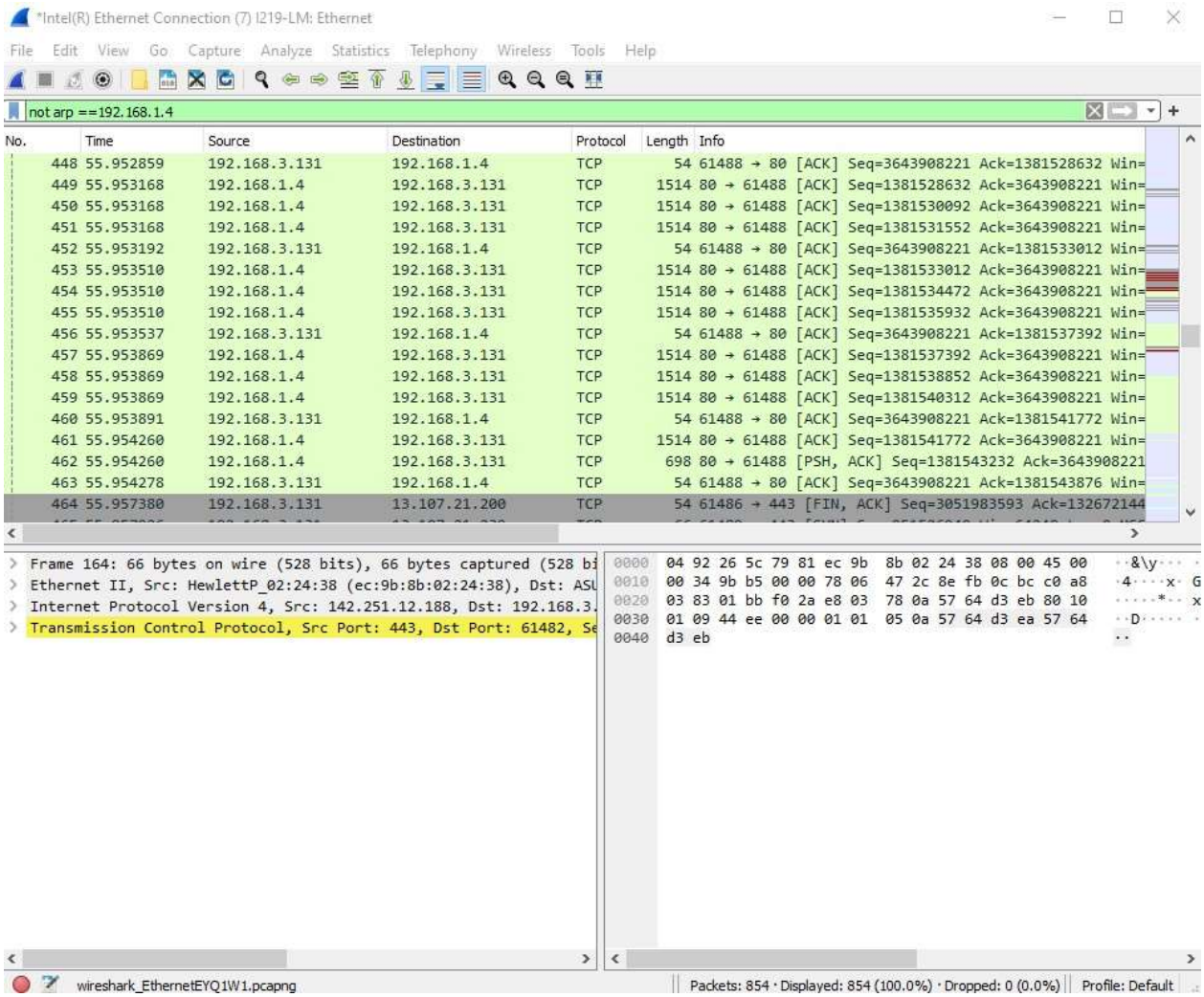
Step-1:- Capture the Live Traffic on port 80 using-(ip.dst_host==142.250.195.46)||(ip.src_host==142.250.195.46&&tcp.srcport==80)&&tcp



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



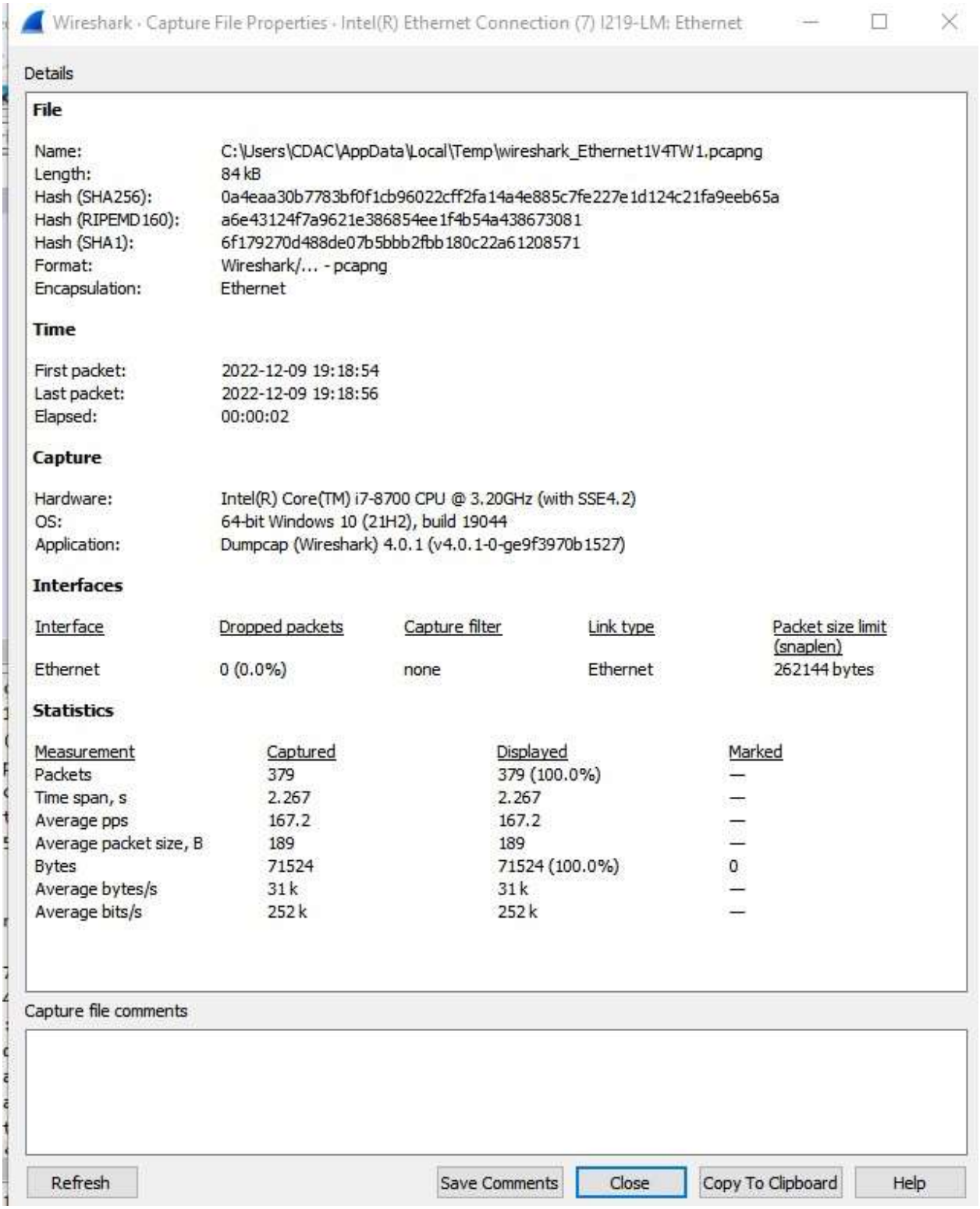
7. Display the summary of the following

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

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

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

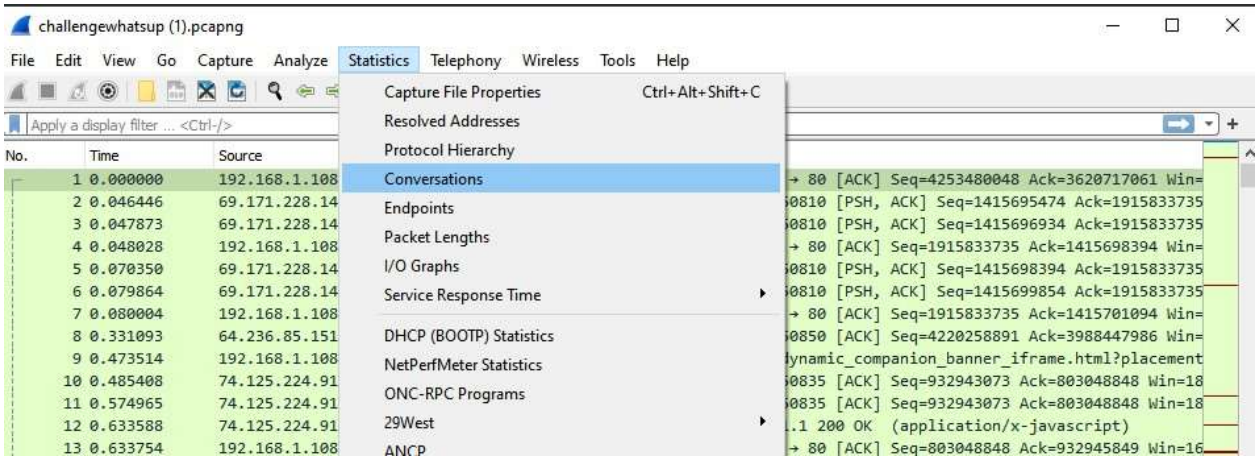
Open Wireshark—-->Go to Statistics —--->Select Capture Filter Property

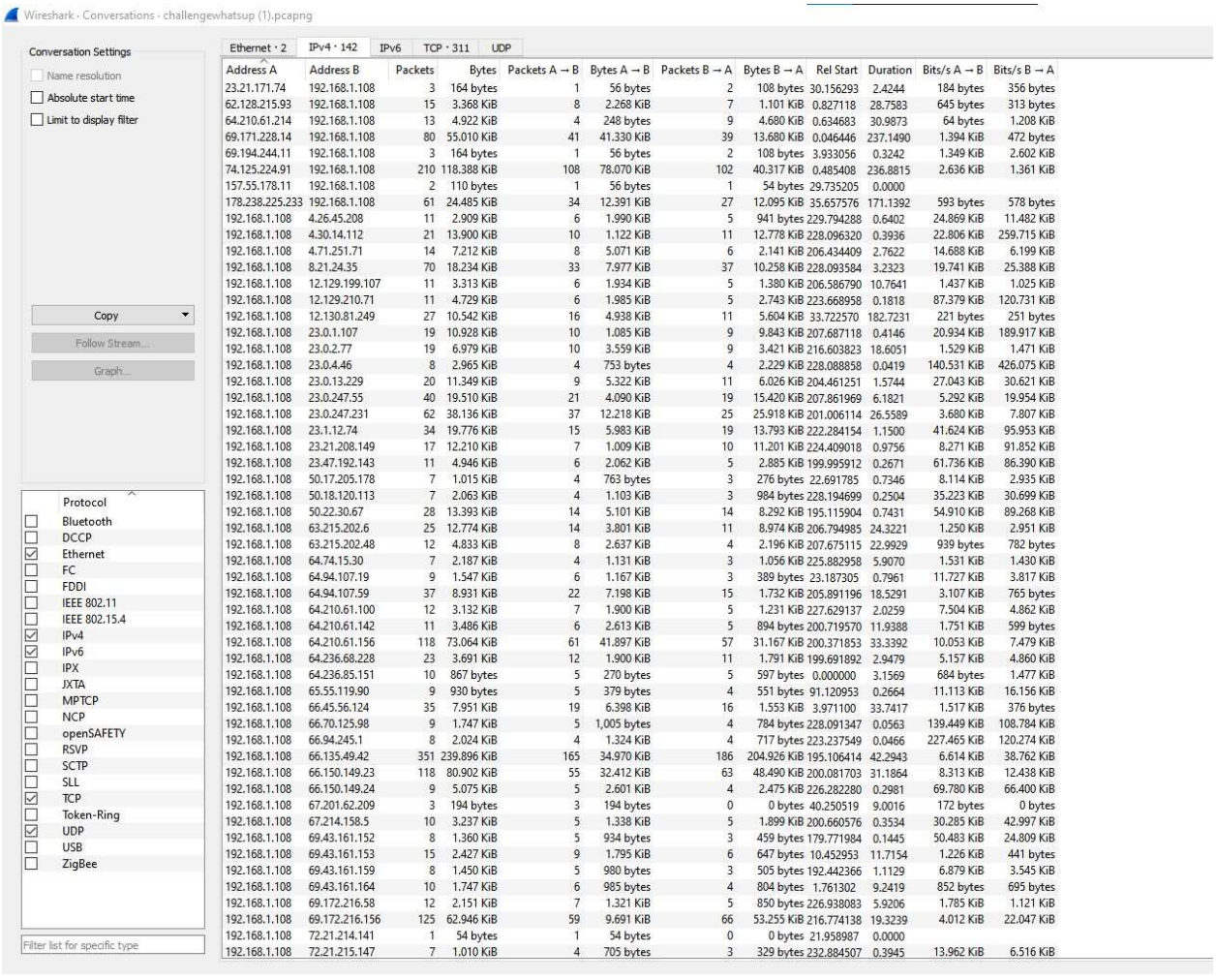

Wireshark · Capture File Properties · Intel(R) Ethernet Connection (7) I219-LM: Ethernet
Details
File
Name: C:\Users\CDAC\AppData\Local\Temp\wireshark_Ethernet1V4TW1.pcapng
Length: 84 kB
Hash (SHA256): 0a4eaa30b7783bf0f1cb96022cff2fa14a4e885c7fe227e1d124c21fa9eeb65a
Hash (RIPEMD160): a6e43124f7a9621e386854ee1f4b54a438673081
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
Refresh
Save Comments
Close
Copy To Clipboard
Help

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

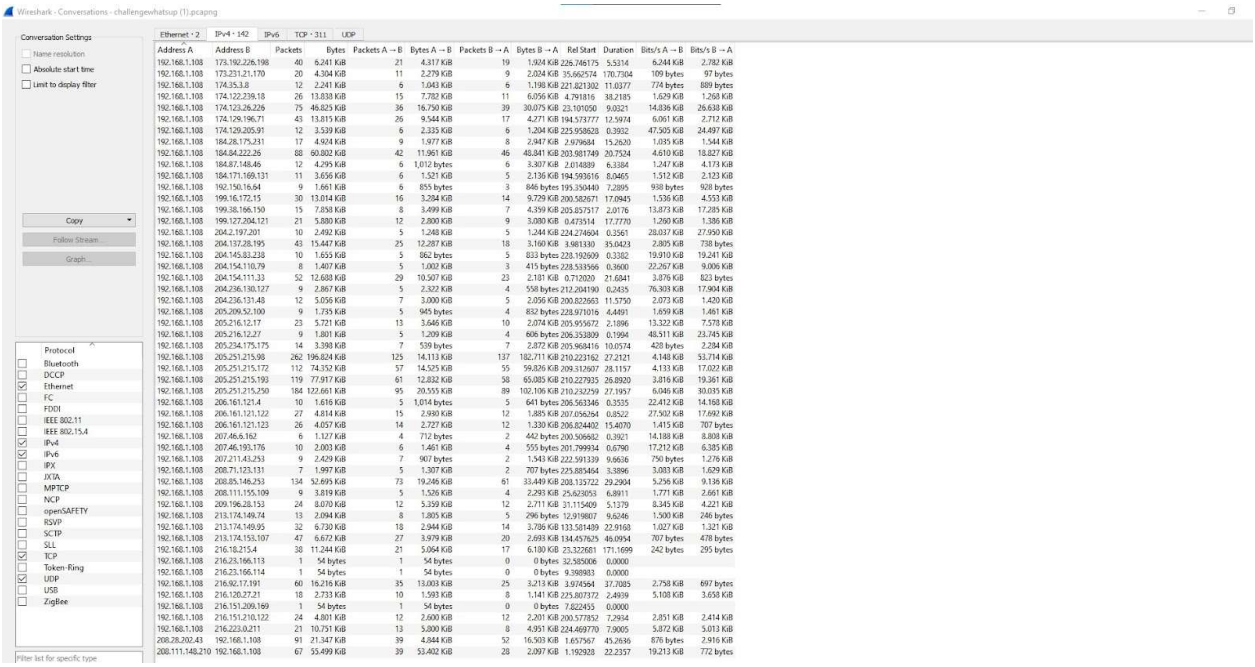
10. How many different IP hosts is A's machine is communicating with?

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





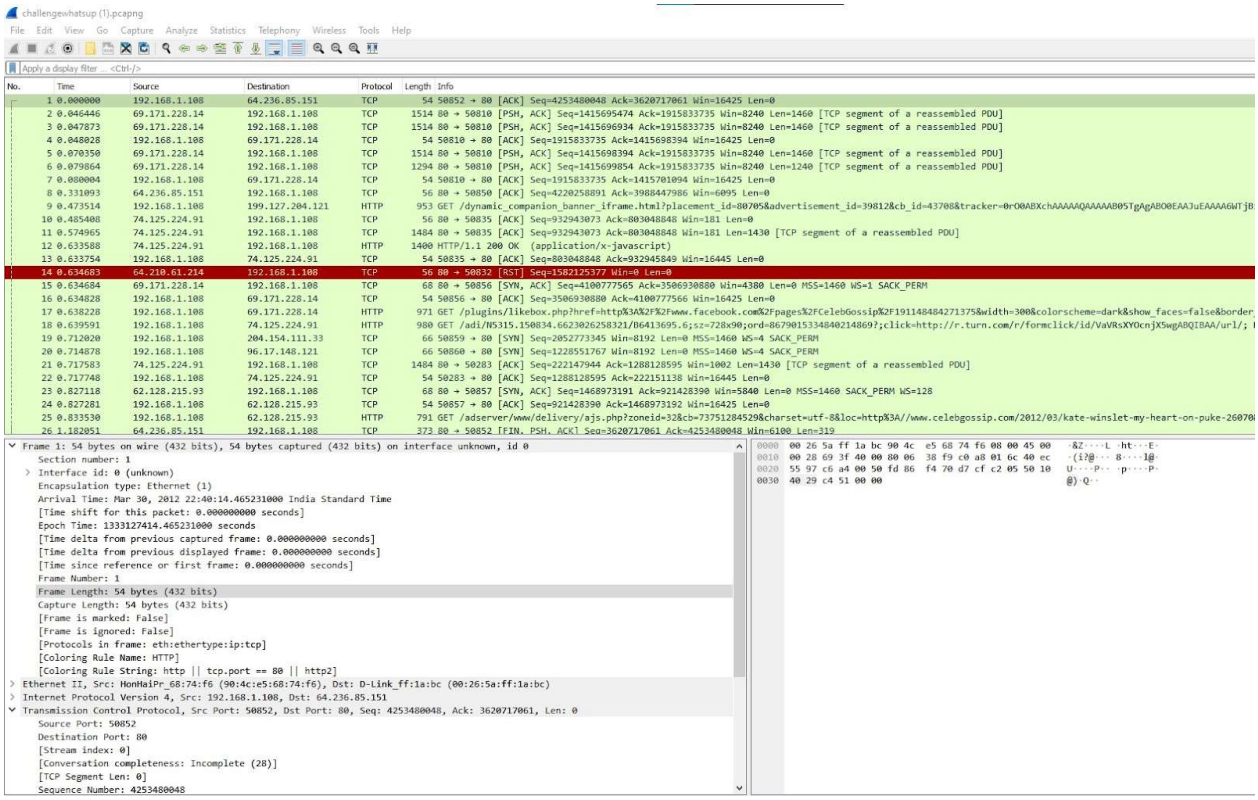
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
23.21.171.74	192.168.1.108	3	164 bytes	1	56 bytes	2	108 bytes	30.156293	2.4244	184 bytes	356 bytes
62.128.215.93	192.168.1.108	15	3.368 KiB	8	2.268 KiB	7	1.101 KiB	0.827118	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



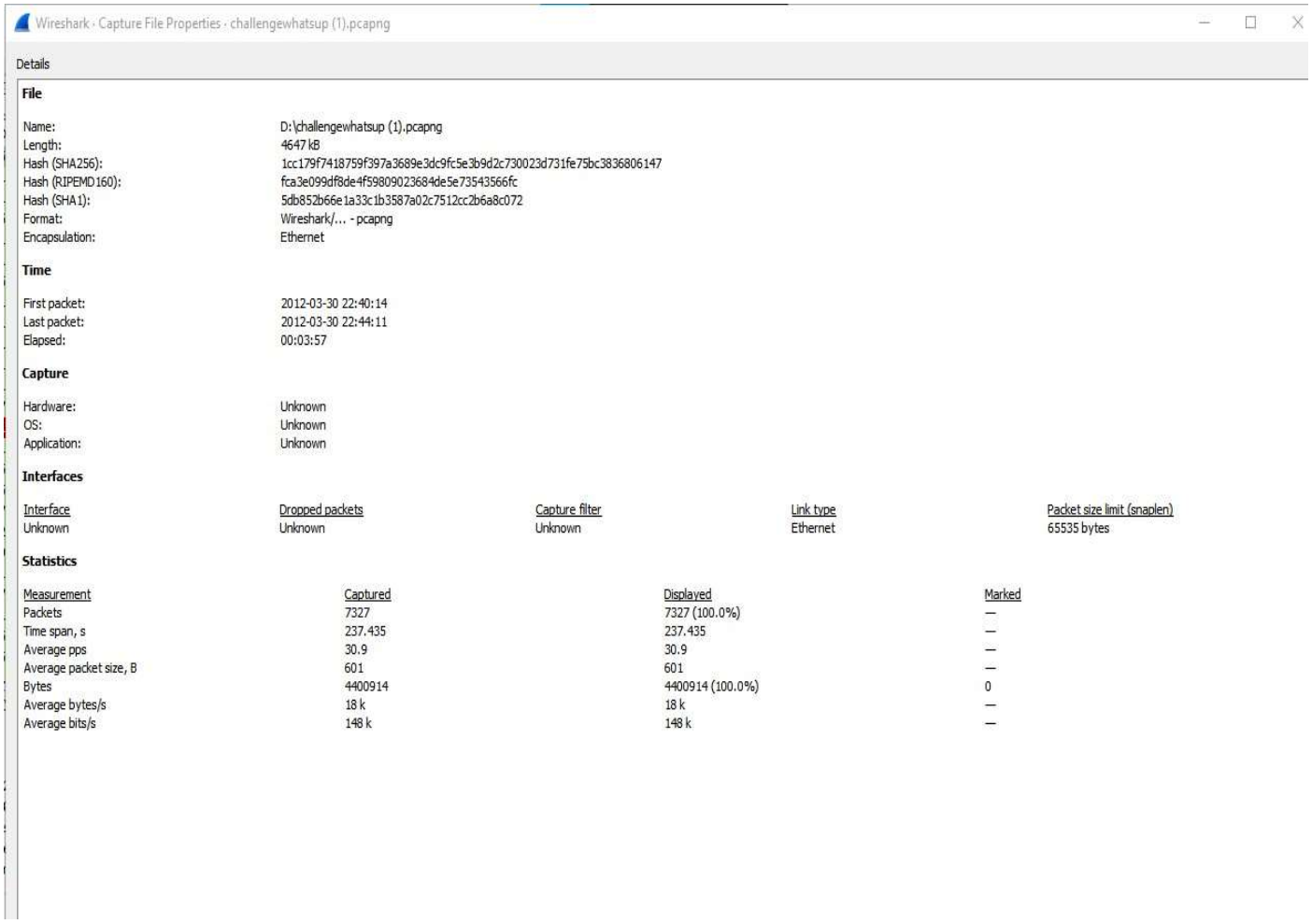
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.108	173.192.226.198	40	6.241 KiB	21	4.317 KiB	19	1.924 KiB	226.746175	5.5314	6.244 KiB	2.782 KiB
192.168.1.108	173.231.21.170	20	4.304 KiB	11	2.279 KiB	9	2.024 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	225.958828	0.3952	47.505 KiB	24.497 KiB
192.168.1.108	184.28.175.231	17	4.904 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	2.014839	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	205.206.52.100	9	1.735 KiB	5	945 bytes	4	852 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	210.232759	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	2.980 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	200.506692	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	133.581439	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	216.151.209.189	1	54 bytes	1	54 bytes	0	0 bytes	7.622455	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



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

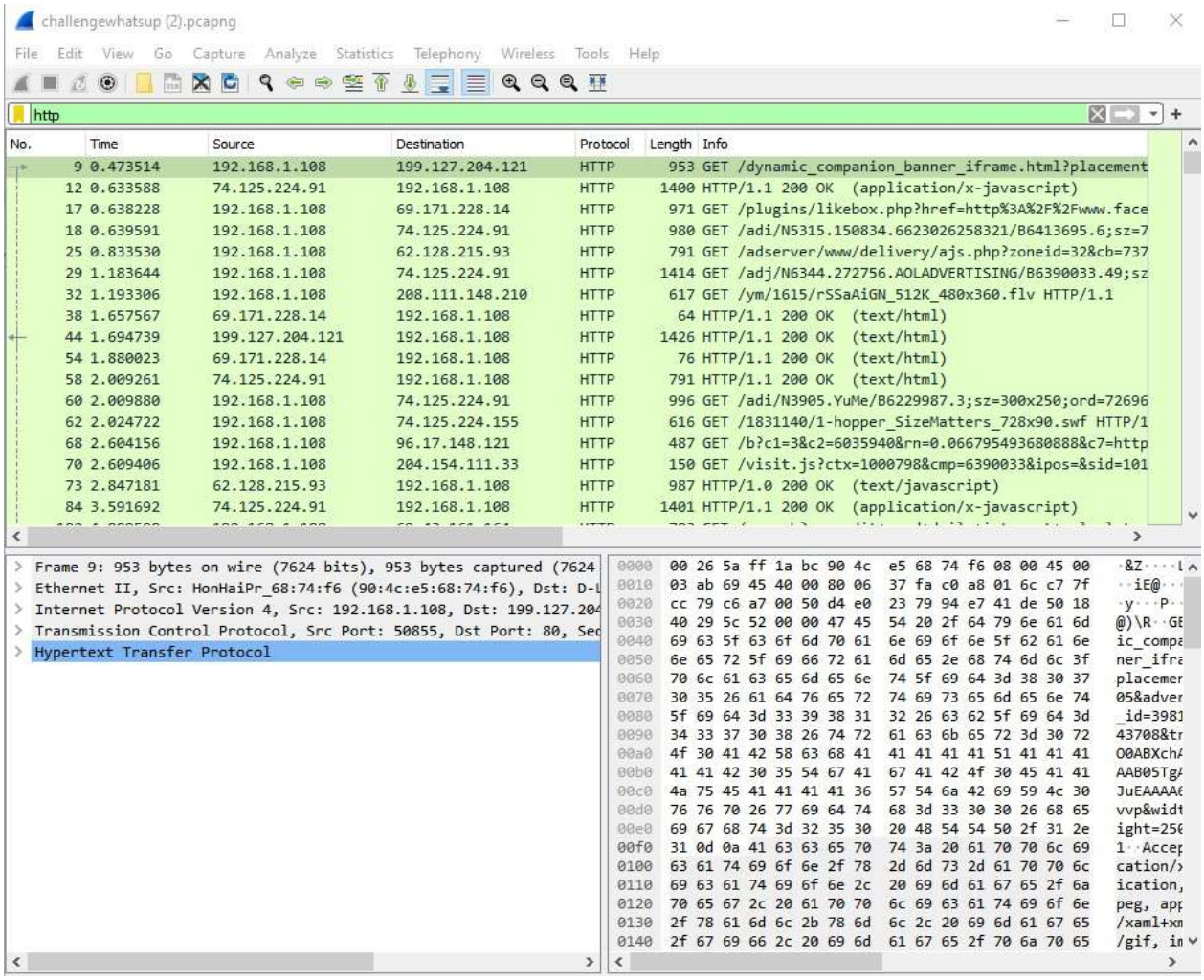
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

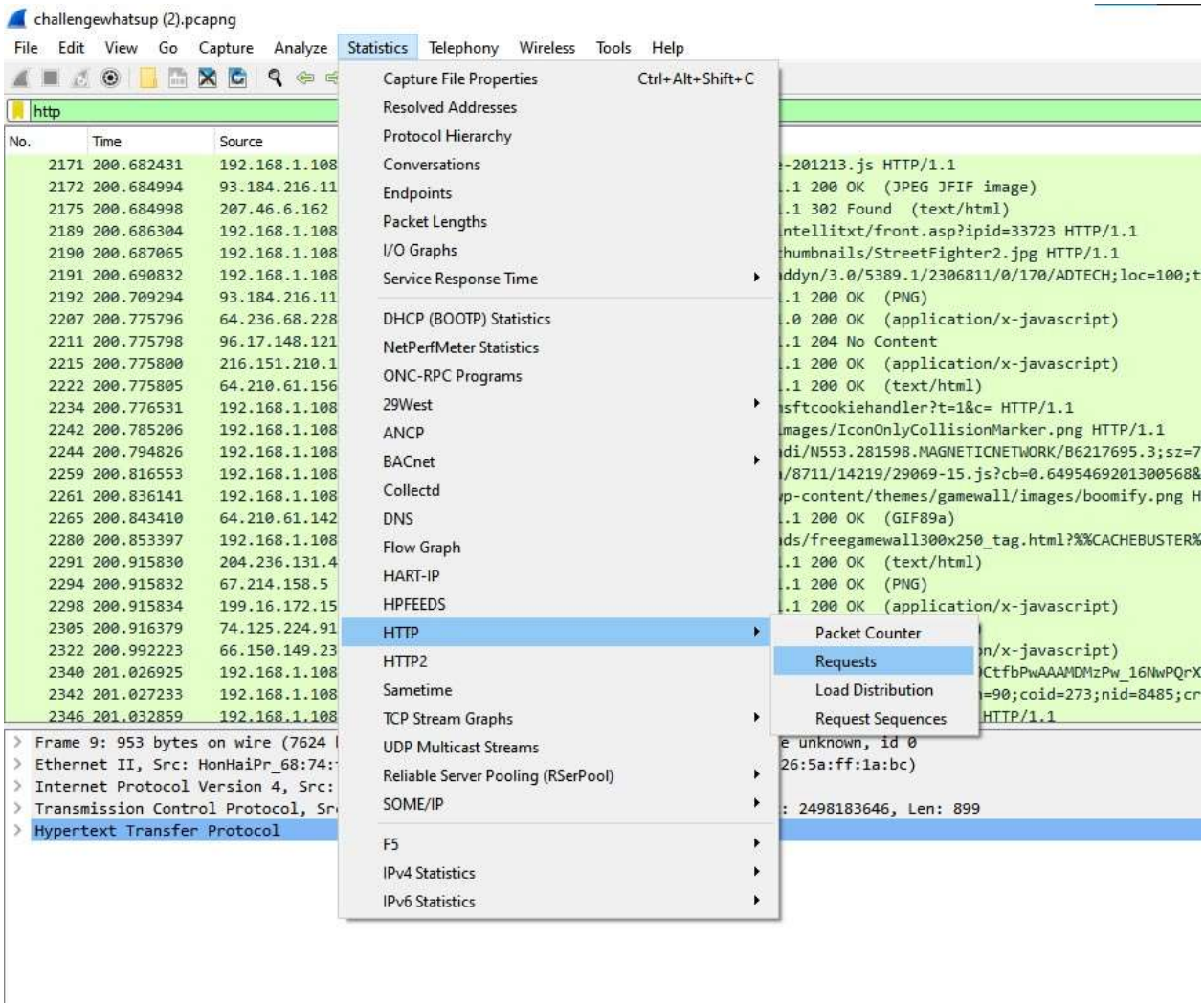
Measurement	Captured	Displayed	Marked
Packets	7327	7327 (100.0%)	—
Time span, s	237.435	237.435	—
Average pps	30.9	30.9	—
Average packet size, B	601	601	—
Bytes	4400914	4400914 (100.0%)	0
Average bytes/s	18 k	18 k	—
Average bits/s	148 k	148 k	—

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

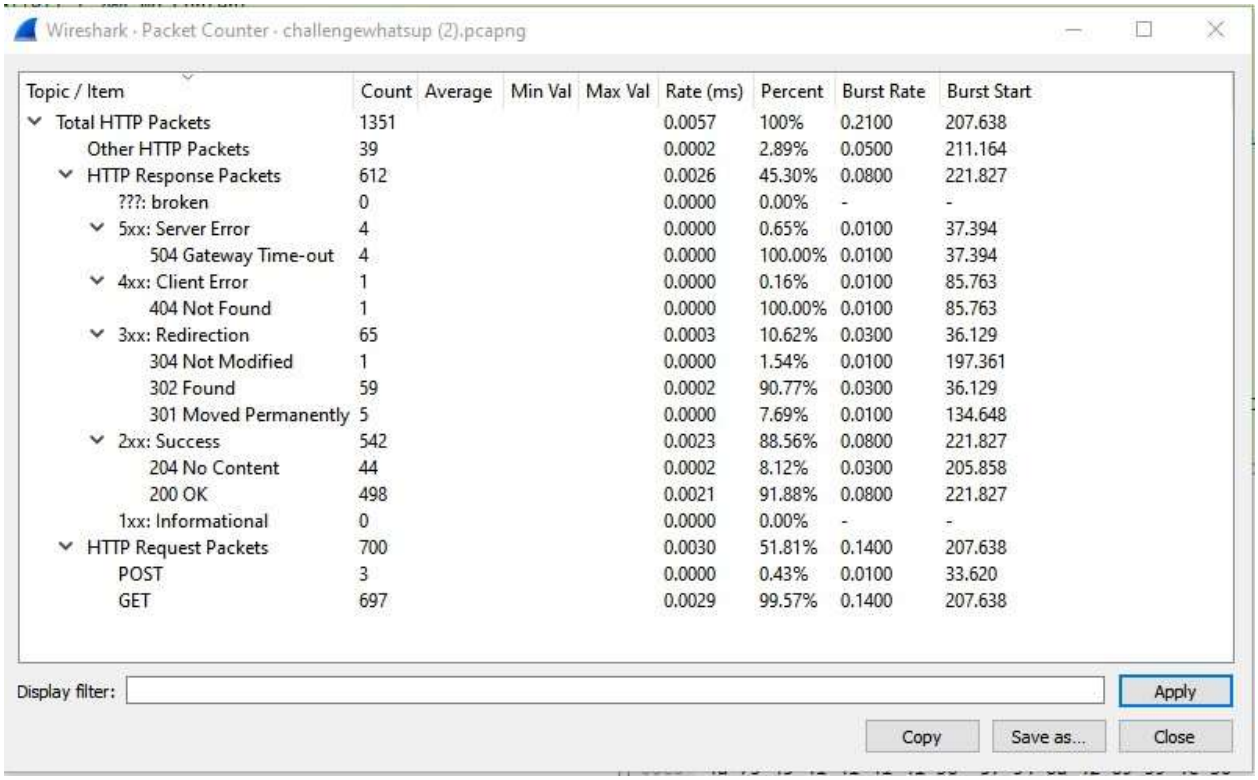
Step-1:- Now open the challengewhatsup.pcapng file



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

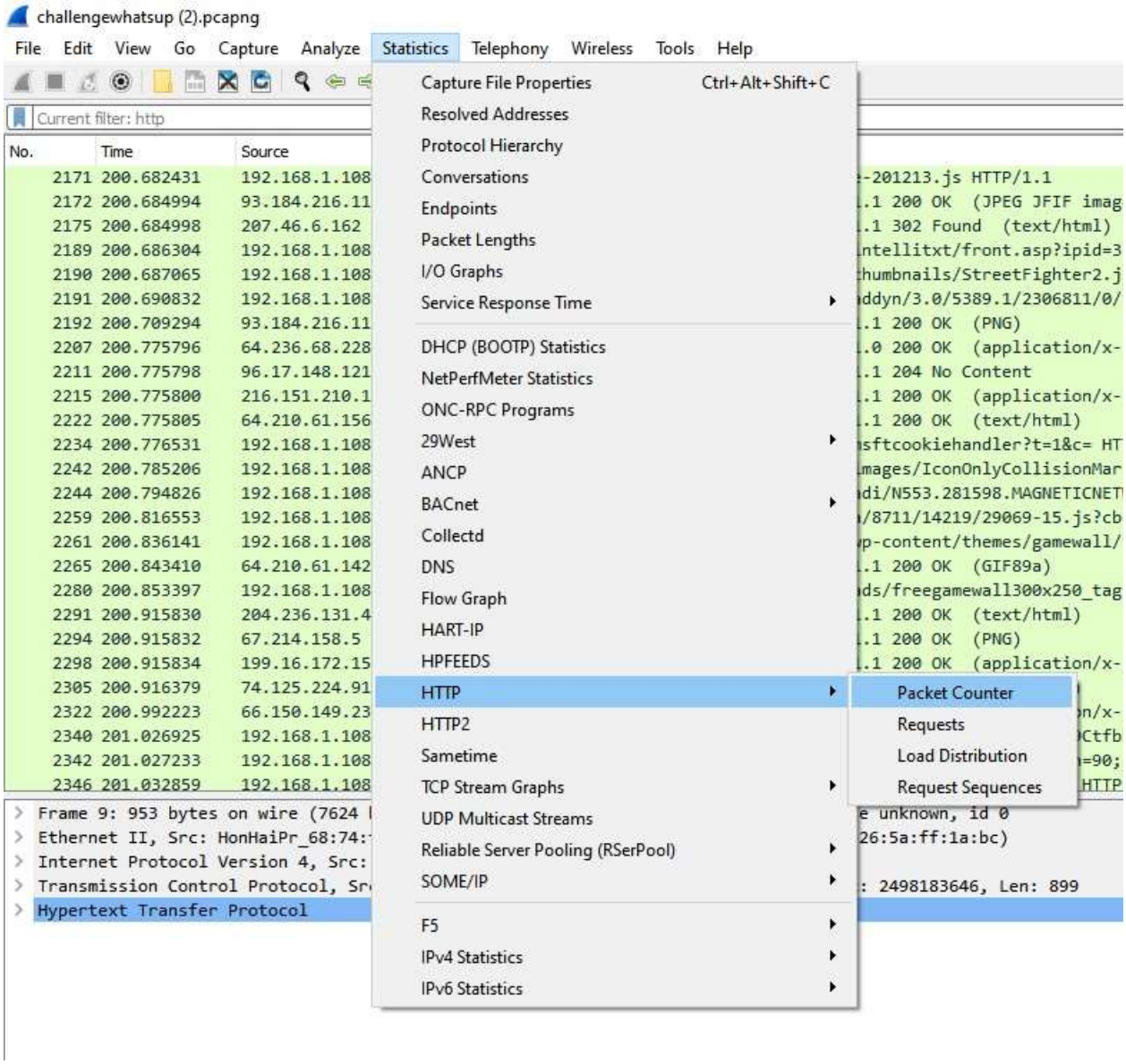


Step-3:- HTTP Post request

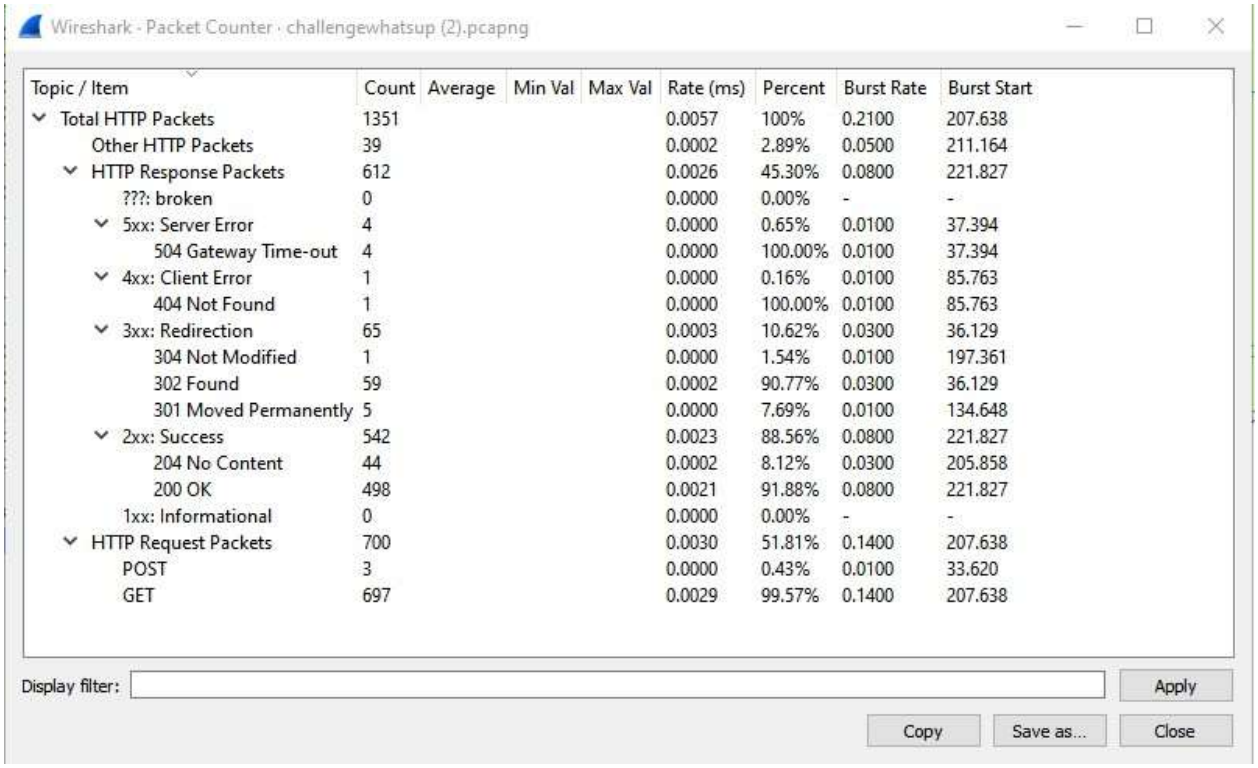


13. What application appears to be generating the GET/POST requests?

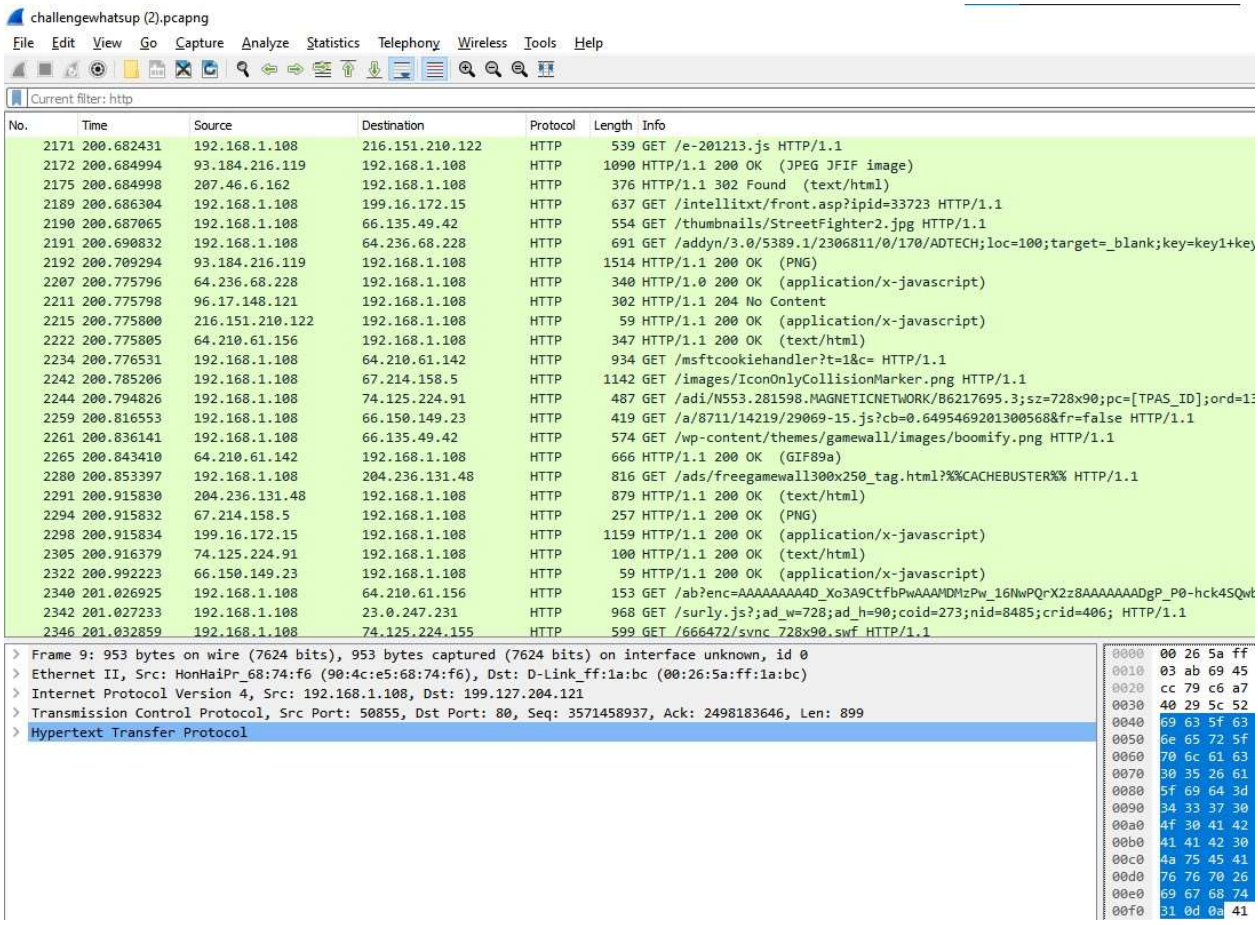
Step-1:- Open Wireshark—-->Go to Statistics —--->Select HTTP —--->Packet Counter


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
2172 200.684994 93.184.216.11
2175 200.684998 207.46.6.162
2189 200.686304 192.168.1.108
2190 200.687065 192.168.1.108
2191 200.690832 192.168.1.108
2192 200.709294 93.184.216.11
2207 200.775796 64.236.68.228
2211 200.775798 96.17.148.121
2215 200.775800 216.151.210.1
2222 200.775805 64.210.61.156
2234 200.776531 192.168.1.108
2242 200.785206 192.168.1.108
2244 200.794826 192.168.1.108
2259 200.816553 192.168.1.108
2261 200.836141 192.168.1.108
2265 200.843410 64.210.61.142
2280 200.853397 192.168.1.108
2291 200.915830 204.236.131.4
2294 200.915832 67.214.158.5
2298 200.915834 199.16.172.15
2305 200.916379 74.125.224.91
2322 200.992223 66.150.149.23
2340 201.026925 192.168.1.108
2342 201.027233 192.168.1.108
2346 201.032859 192.168.1.108
Frame 9: 953 bytes on wire (7624
Ethernet II, Src: HonHaiPr_68:74:
Internet Protocol Version 4, Src:
Transmission Control Protocol, Sr
Hypertext Transfer Protocol
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
SOME/IP
F5
IPv4 Statistics
IPv6 Statistics
Packet Counter
Requests
Load Distribution
Request Sequences

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:
Apply
Copy
Save as...
Close

Step-3:-


challengewhatsup (2).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
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=13
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_16NwPQrX2z8AAAAAADgP_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