Networking Lab – 2

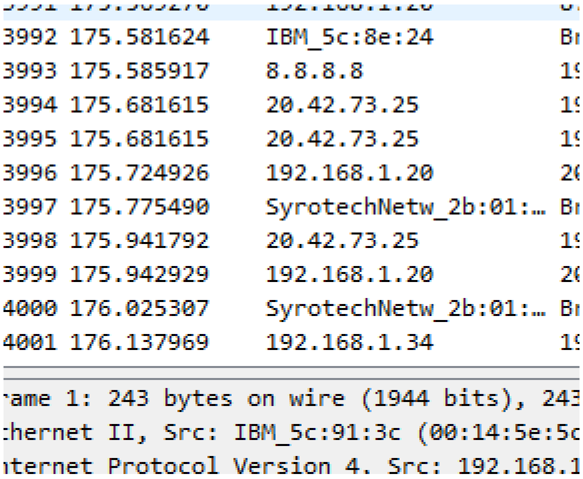
OBJECTIVE:

To capture packets of data across your network using Wireshark.

PRE-REQUISITES:

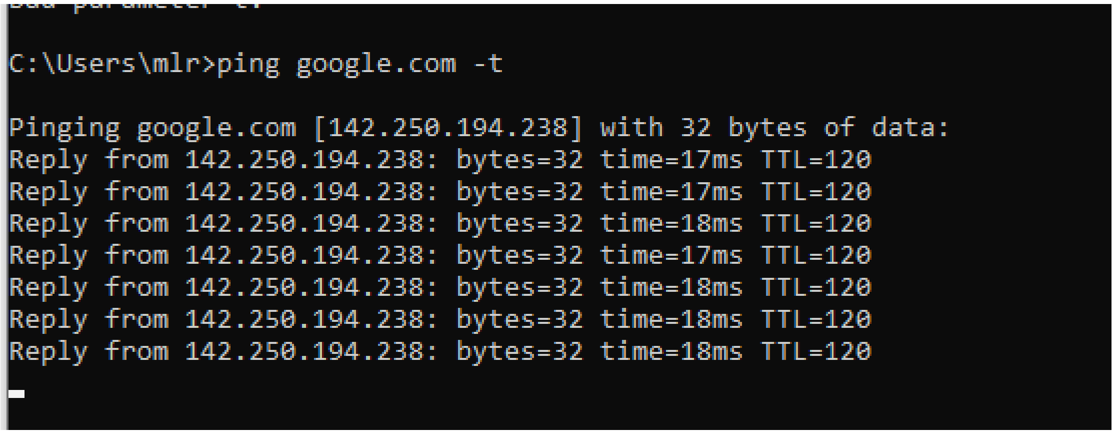
Wireshark software installed.

Q1:- Open Wireshark software and select the network connection on your system.

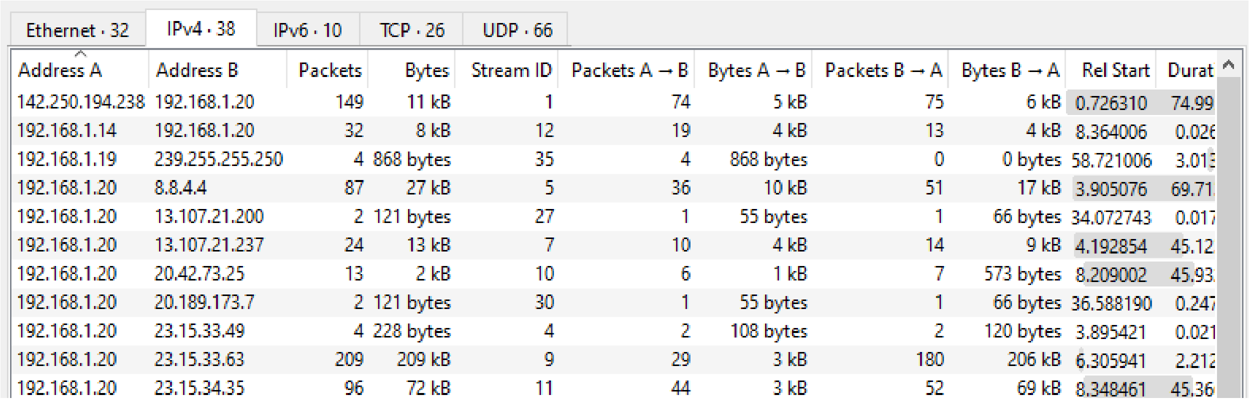


```
3991 175.565276    192.168.1.20       8.
3992 175.581624    IBM_5c:8e:24       Br
3993 175.585917    8.8.8.8            19
3994 175.681615    20.42.73.25        19
3995 175.681615    20.42.73.25        19
3996 175.724926    192.168.1.20       20
3997 175.775490    SyrotechNetw_2b:01:… Br
3998 175.941792    20.42.73.25        19
3999 175.942929    192.168.1.20       20
4000 176.025307    SyrotechNetw_2b:01:… Br
4001 176.137969    192.168.1.34       19

rame 1: 243 bytes on wire (1944 bits), 243
hernet II, Src: IBM_5c:91:3c (00:14:5e:5c
nternet Protocol Version 4. Src: 192.168.1
```

Q2:- In the command prompt, ping “google.com” and check Wireshark thereafter for echo request and echo reply

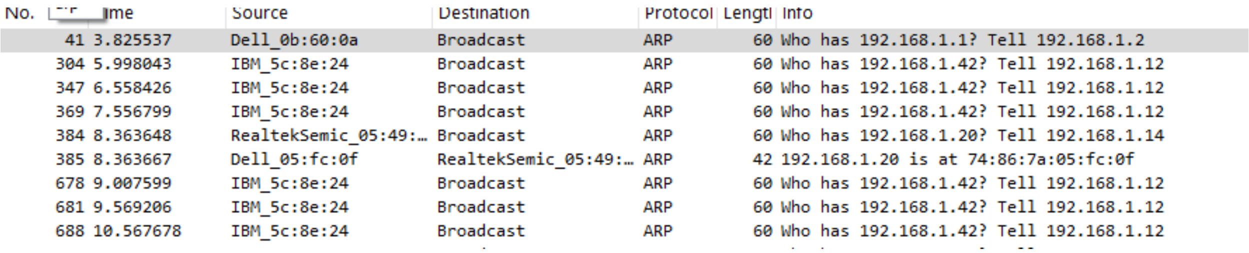


```
Bad parameter -t.

C:\Users\mlr>ping google.com -t

Pinging google.com [142.250.194.238] with 32 bytes of data:
Reply from 142.250.194.238: bytes=32 time=17ms TTL=120
Reply from 142.250.194.238: bytes=32 time=17ms TTL=120
Reply from 142.250.194.238: bytes=32 time=18ms TTL=120
Reply from 142.250.194.238: bytes=32 time=17ms TTL=120
Reply from 142.250.194.238: bytes=32 time=18ms TTL=120
Reply from 142.250.194.238: bytes=32 time=18ms TTL=120
Reply from 142.250.194.238: bytes=32 time=18ms TTL=120
_
```



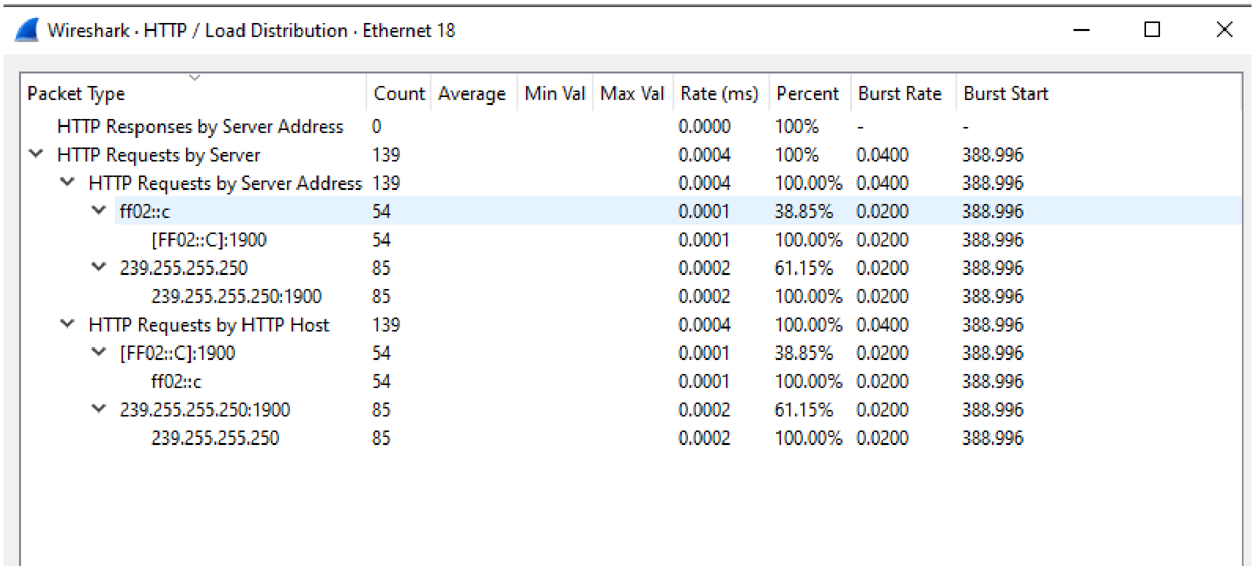
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Durat
142.250.194.238	192.168.1.20	149	11 kB	1	74	5 kB	75	6 kB	0.726310	74.99
192.168.1.14	192.168.1.20	32	8 kB	12	19	4 kB	13	4 kB	8.364006	0.026
192.168.1.19	239.255.255.250	4	868 bytes	35	4	868 bytes	0	0 bytes	58.721006	3.013
192.168.1.20	8.8.4.4	87	27 kB	5	36	10 kB	51	17 kB	3.905076	69.71
192.168.1.20	13.107.21.200	2	121 bytes	27	1	55 bytes	1	66 bytes	34.072743	0.017
192.168.1.20	13.107.21.237	24	13 kB	7	10	4 kB	14	9 kB	4.192854	45.12
192.168.1.20	20.42.73.25	13	2 kB	10	6	1 kB	7	573 bytes	8.209002	45.93
192.168.1.20	20.189.173.7	2	121 bytes	30	1	55 bytes	1	66 bytes	36.588190	0.247
192.168.1.20	23.15.33.49	4	228 bytes	4	2	108 bytes	2	120 bytes	3.895421	0.021
192.168.1.20	23.15.33.63	209	209 kB	9	29	3 kB	180	206 kB	6.305941	2.212
192.168.1.20	23.15.34.35	96	72 kB	11	44	3 kB	52	69 kB	8.348461	45.36

Q3 :- Try pinging an ip that does not exist on your network, and look for ARP data.



No.	Time	Source	Destination	Protocol	Lengt	Info
41	3.825537	Dell_0b:60:0a	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.2
304	5.998043	IBM_5c:8e:24	Broadcast	ARP	60	Who has 192.168.1.42? Tell 192.168.1.12
347	6.558426	IBM_5c:8e:24	Broadcast	ARP	60	Who has 192.168.1.42? Tell 192.168.1.12
369	7.556799	IBM_5c:8e:24	Broadcast	ARP	60	Who has 192.168.1.42? Tell 192.168.1.12
384	8.363648	RealtekSemic_05:49:…	Broadcast	ARP	60	Who has 192.168.1.20? Tell 192.168.1.14
385	8.363667	Dell_05:fc:0f	RealtekSemic_05:49:…	ARP	42	192.168.1.20 is at 74:86:7a:05:fc:0f
678	9.007599	IBM_5c:8e:24	Broadcast	ARP	60	Who has 192.168.1.42? Tell 192.168.1.12
681	9.569206	IBM_5c:8e:24	Broadcast	ARP	60	Who has 192.168.1.42? Tell 192.168.1.12
688	10.567678	IBM_5c:8e:24	Broadcast	ARP	60	Who has 192.168.1.42? Tell 192.168.1.12

Q4:- Also, try pinging any other ip or domain name, or any other web-activity in a browser, and click the Stop button

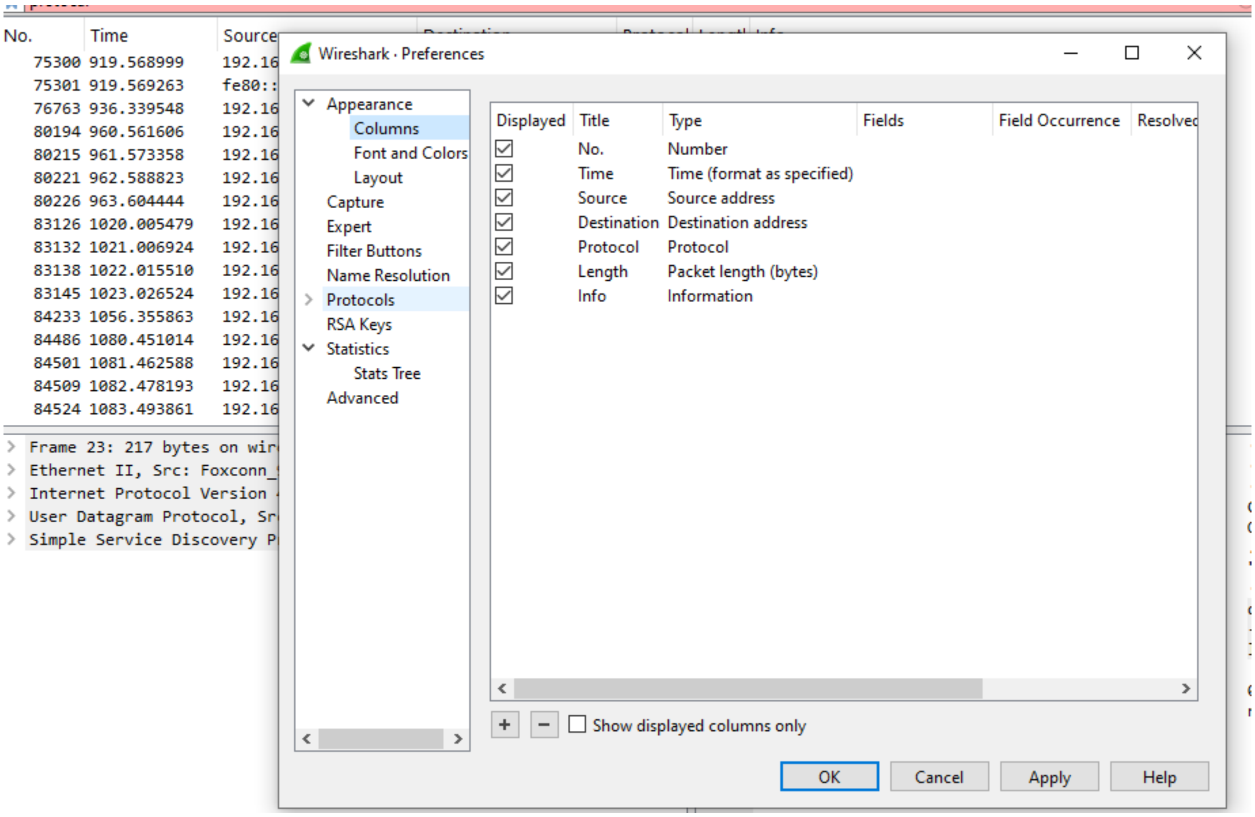


Wireshark · HTTP / Load Distribution · Ethernet 18

Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Responses by Server Address	0				0.0000	100%	-	-
HTTP Requests by Server	139				0.0004	100%	0.0400	388.996
HTTP Requests by Server Address	139				0.0004	100.00%	0.0400	388.996
ff02::c	54				0.0001	38.85%	0.0200	388.996
[FF02::C]:1900	54				0.0001	100.00%	0.0200	388.996
239.255.255.250	85				0.0002	61.15%	0.0200	388.996
239.255.255.250:1900	85				0.0002	100.00%	0.0200	388.996
HTTP Requests by HTTP Host	139				0.0004	100.00%	0.0400	388.996
[FF02::C]:1900	54				0.0001	38.85%	0.0200	388.996
ff02::c	54				0.0001	100.00%	0.0200	388.996
239.255.255.250:1900	85				0.0002	61.15%	0.0200	388.996
239.255.255.250	85				0.0002	100.00%	0.0200	388.996

Url- https://youtu.be/YGotjq3gxis?si=gLFRKXdLyUFZ373P

Q5:- You can also filter different protocols in the search bar, to look for data flow across the network using the respective protocols.



```
No.   Time          Source
  75300 919.568999  192.16
  75301 919.569263  fe80::
  76763 936.339548  192.16
  80194 960.561606  192.16
  80215 961.573358  192.16
  80221 962.588823  192.16
  80226 963.604444  192.16
  83126 1020.005479 192.16
  83132 1021.006924 192.16
  83138 1022.015510 192.16
  83145 1023.026524 192.16
  84233 1056.355863 192.16
  84486 1080.451014 192.16
  84501 1081.462588 192.16
  84509 1082.478193 192.16
  84524 1083.493861 192.16

> Frame 23: 217 bytes on wir
> Ethernet II, Src: Foxconn_
> Internet Protocol Version
> User Datagram Protocol, Sr
> Simple Service Discovery P
```

Displayed	Title	Type	Fields	Field Occurrence	Resolved
☑	No.	Number			
☑	Time	Time (format as specified)			
☑	Source	Source address			
☑	Destination	Destination address			
☑	Protocol	Protocol			
☑	Length	Packet length (bytes)			
☑	Info	Information			

+ − □ Show displayed columns only

Url- https://youtu.be/hKrSeKg_yX4?si=NOayBim9VhOPTC6Q

Wireshark software installed.