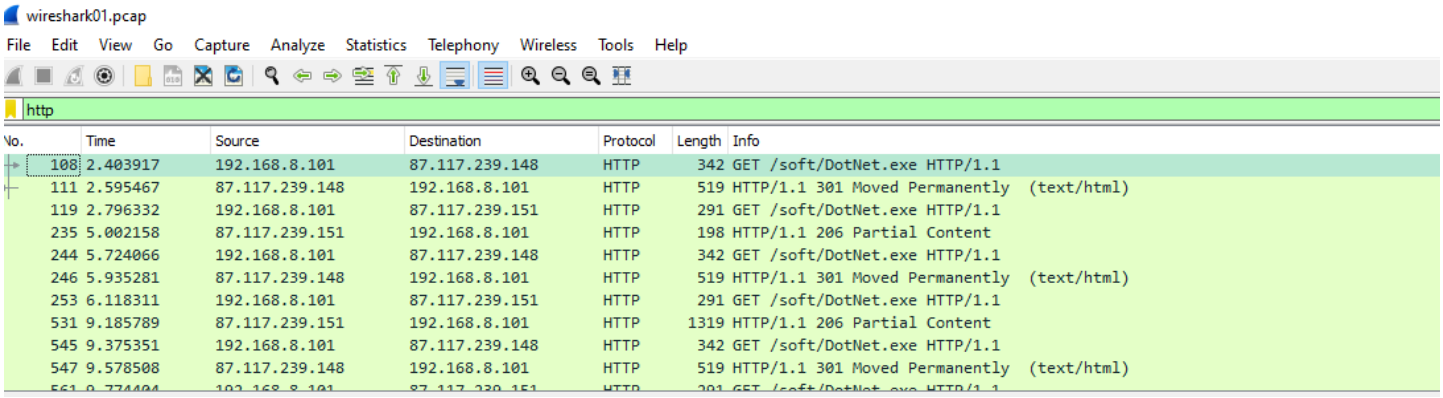
Wireshark Practical
IS2111
Practical 05

B.G.S.S.W.Jayaweera
Index : 19020376

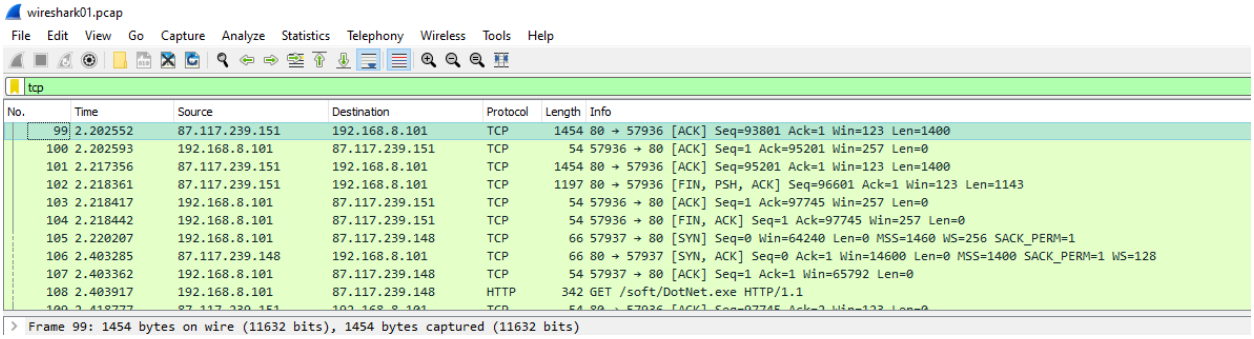
1. Enter following simple protocol names as filters and check whether such packets exist. Once you apply one filter, don't forget to click the clear button before applying another filter. Just deleting the text you entered does not clear the previous filter unless you click on the clear button.

http



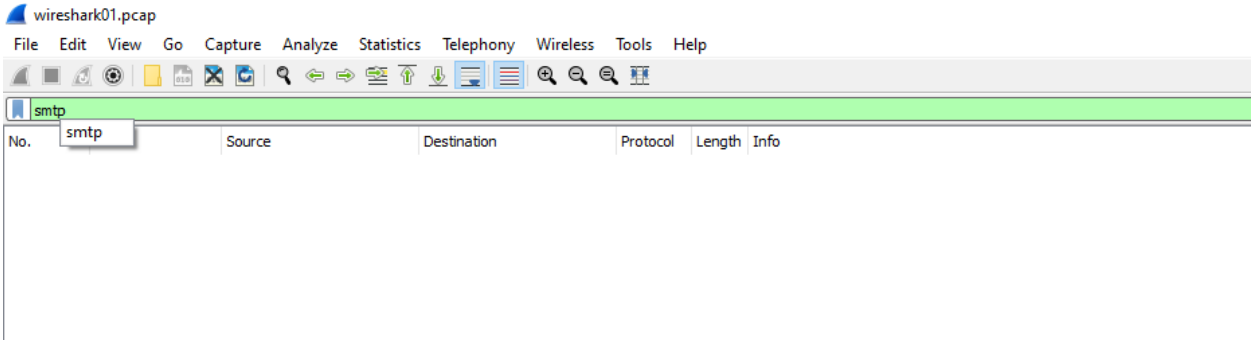
No.	Time	Source	Destination	Protocol	Length	Info
108	2.403917	192.168.8.101	87.117.239.148	HTTP	342	GET /soft/DotNet.exe HTTP/1.1
111	2.595467	87.117.239.148	192.168.8.101	HTTP	519	HTTP/1.1 301 Moved Permanently (text/html)
119	2.796332	192.168.8.101	87.117.239.151	HTTP	291	GET /soft/DotNet.exe HTTP/1.1
235	5.002158	87.117.239.151	192.168.8.101	HTTP	198	HTTP/1.1 206 Partial Content
244	5.724066	192.168.8.101	87.117.239.148	HTTP	342	GET /soft/DotNet.exe HTTP/1.1
246	5.935281	87.117.239.148	192.168.8.101	HTTP	519	HTTP/1.1 301 Moved Permanently (text/html)
253	6.118311	192.168.8.101	87.117.239.151	HTTP	291	GET /soft/DotNet.exe HTTP/1.1
531	9.185789	87.117.239.151	192.168.8.101	HTTP	1319	HTTP/1.1 206 Partial Content
545	9.375351	192.168.8.101	87.117.239.148	HTTP	342	GET /soft/DotNet.exe HTTP/1.1
547	9.578508	87.117.239.148	192.168.8.101	HTTP	519	HTTP/1.1 301 Moved Permanently (text/html)

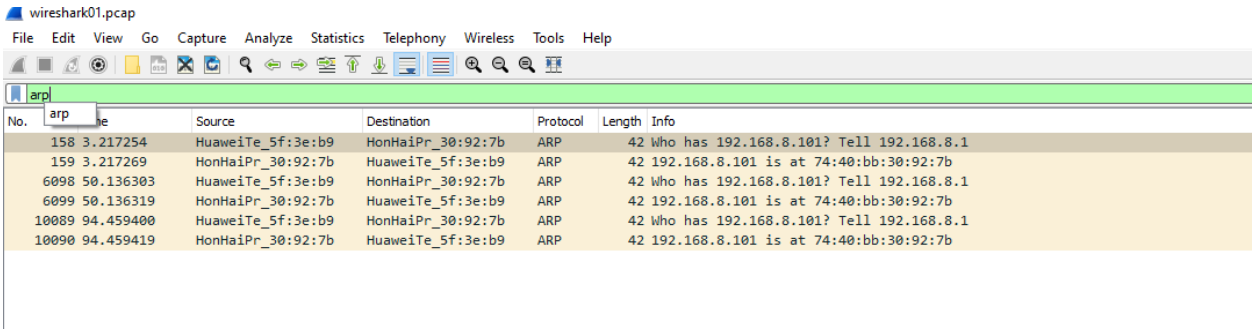
tcp



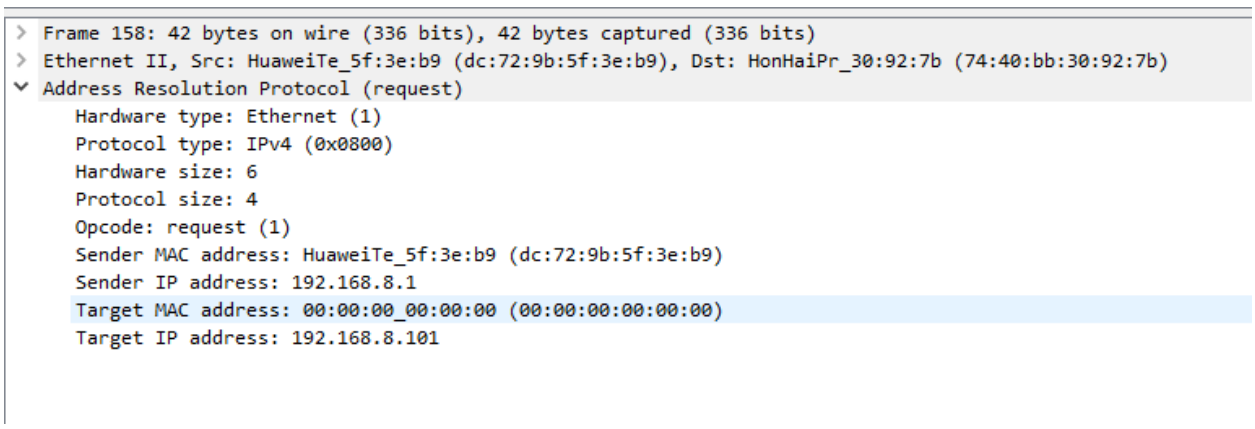
No.	Time	Source	Destination	Protocol	Length	Info
99	2.202552	87.117.239.151	192.168.8.101	TCP	1454	80 → 57936 [ACK] Seq=93801 Ack=1 Win=123 Len=1400
100	2.202593	192.168.8.101	87.117.239.151	TCP	54	57936 → 80 [ACK] Seq=1 Ack=95201 Win=257 Len=0
101	2.217356	87.117.239.151	192.168.8.101	TCP	1454	80 → 57936 [ACK] Seq=95201 Ack=1 Win=123 Len=1400
102	2.218361	87.117.239.151	192.168.8.101	TCP	1197	80 → 57936 [FIN, PSH, ACK] Seq=96601 Ack=1 Win=123 Len=1143
103	2.218417	192.168.8.101	87.117.239.151	TCP	54	57936 → 80 [ACK] Seq=1 Ack=97745 Win=257 Len=0
104	2.218442	192.168.8.101	87.117.239.151	TCP	54	57936 → 80 [FIN, ACK] Seq=1 Ack=97745 Win=257 Len=0
105	2.220207	192.168.8.101	87.117.239.148	TCP	66	57937 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
106	2.403285	87.117.239.148	192.168.8.101	TCP	66	80 → 57937 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1 WS=128
107	2.403362	192.168.8.101	87.117.239.148	TCP	54	57937 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
108	2.403917	192.168.8.101	87.117.239.148	HTTP	342	GET /soft/DotNet.exe HTTP/1.1

smtp





2. Select ARP request and analyse it. Clearly mentioned about the MAC & IP address of sender and target.



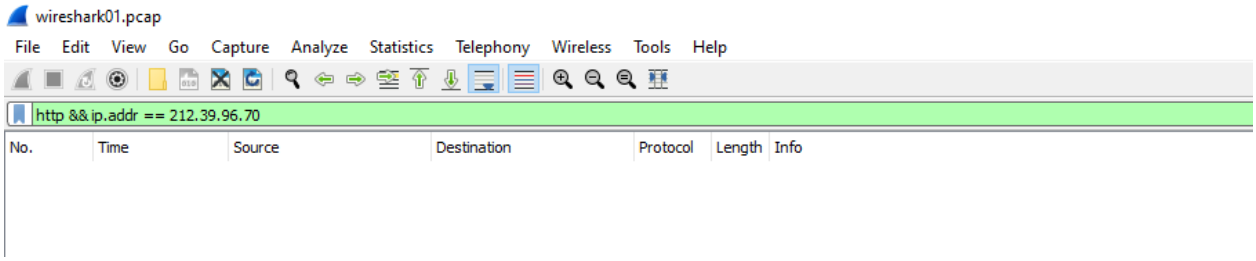
Sender MAC address: dc : 72 : 9b: 5f: 3e : b9

Sender Ip address : 192.168.8.1

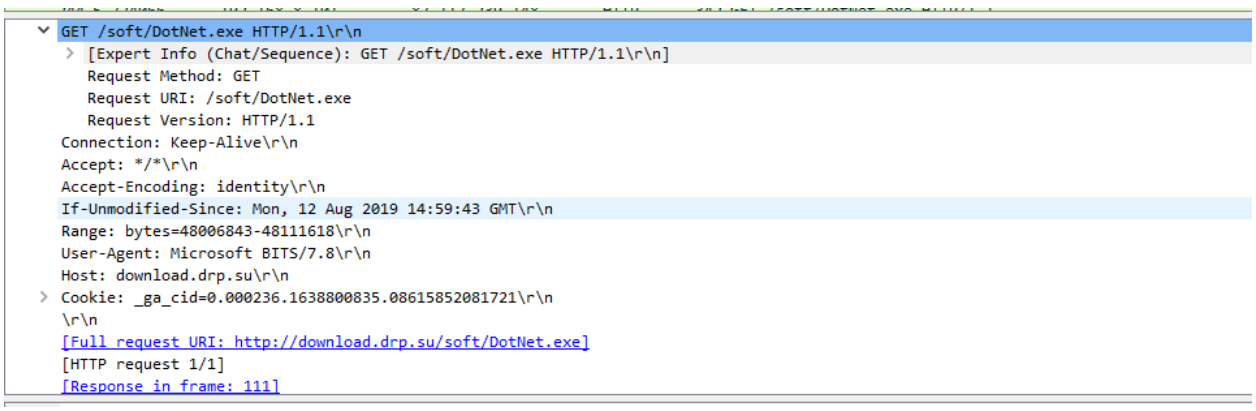
Target MAC address: 00:00:00:00:00:00

Target Ip address: 192.168.8.101

3. Write down and apply a filter to view packets where the IP address 212.39.96.70 and the protocol is HTTP.



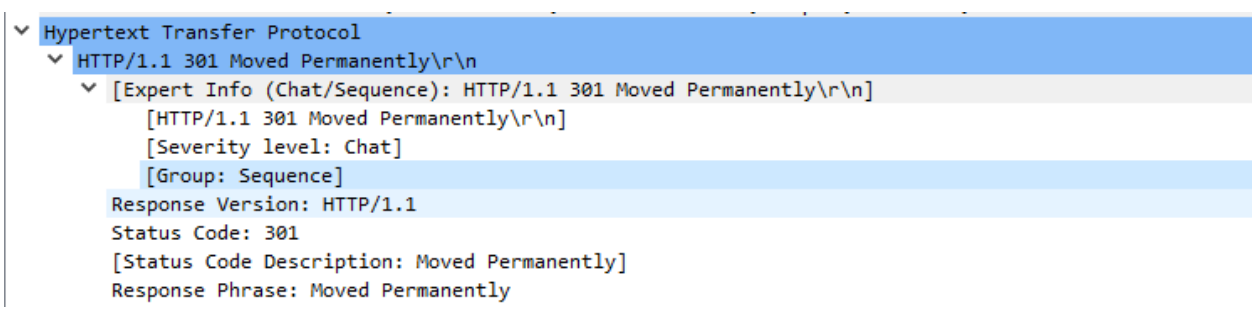
4. Analyze the first HTTP GET request under the HTTP header.



a. What is the requested version? HTTP/1.1

b. What is the requested URI? http://download.drp.su/soft/DotNet.exe

5. Analyze the server's response to the GET request.



a. What is the status code? 301

b. What does that status code mean? HTTP status code is a server response to browser request.301 -Moved Permanently

c. What is the value of the response phase?

Moved Permanently.

6. Analyze the IP header of the same packet

```
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.8.101, Dst: 87.117.239.148
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0xc8d0 (51408)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x20c8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.8.101
    Destination Address: 87.117.239.148
```

a. What is the IP version? **version 4**

b. What is the length of the header? **20 bytes**

c. What is the total length of the packet? **328**

d. Value of fragment offset? **0**

e. Value of Time to Live? **128**

f. Value of the header checksum? **0x20c8**

g. IP addresses of the source and destination?

Source Address : 192.168.8.101

Destination Address : 87.117.239.148