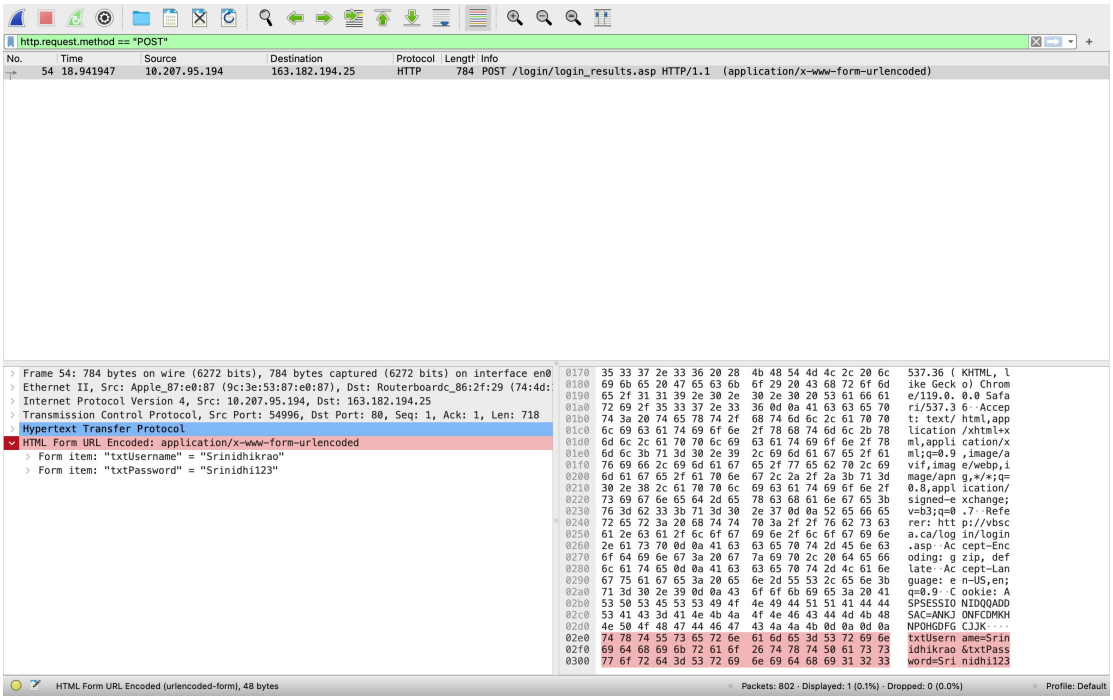
COMPUTER NETWORK ASSSIGNMENT -2

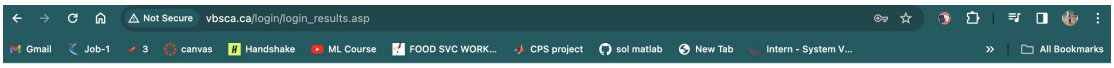
WIRESHARK

Submitted By:
Srinidhi Kadapanatham
1002111809

Find a situation in which you may use Wireshark to observe or track protocols as they are being used while engaging with a network application of your choice. Write a brief report that details, step by step, how Wireshark is being used to examine or follow protocols.
2. Go to any unsecured website (Example: http://vbsca.ca/login/login.asp) and use Wireshark to check if the password is encrypted. Provide screenshots from Wireshark.HINT: Use contains filter
3. Using Wireshark demonstrate TCP three-way handshake. Explain tcp.completeness == 31
4. For a request, capture the TCP flow using the Wireshark Flow chart that highlights the [SYN], [SYN,ACK],[ACK] and [FIN,ACK]. Explain what it does.
5. Using nslookup find your host's MAC address and compare it using WireShark.
6. What is the Internet address of the google.com? What is the Internet address of your computer?
7. Which version of HTTP—1.0 or 1.1—is your browser using?
Click the following URL http://gaia.cs.umass.edu/ethereal-labs/INTRO-ethereal-file1.html To
load the above page what version of HTTP is the server using?

Solution for 2:
Steps for this:
Step 1:open wireshark run the packets
Step 2:open the unsecured website http://vbsca.ca/login/login.asp
Step 3:Then stop the packets using filter serach for the login packet by using http.request.method=POST
Step 4 :Under HTML form url we can see in wireshark that the details used to login the webpage is unencrpyted and same can be seen in the webpage when we inspect the webpage as well the user id and password is unencrypted which can seen be in the screenshot.





Login Test

Sorry, but the username that you entered does not exist.

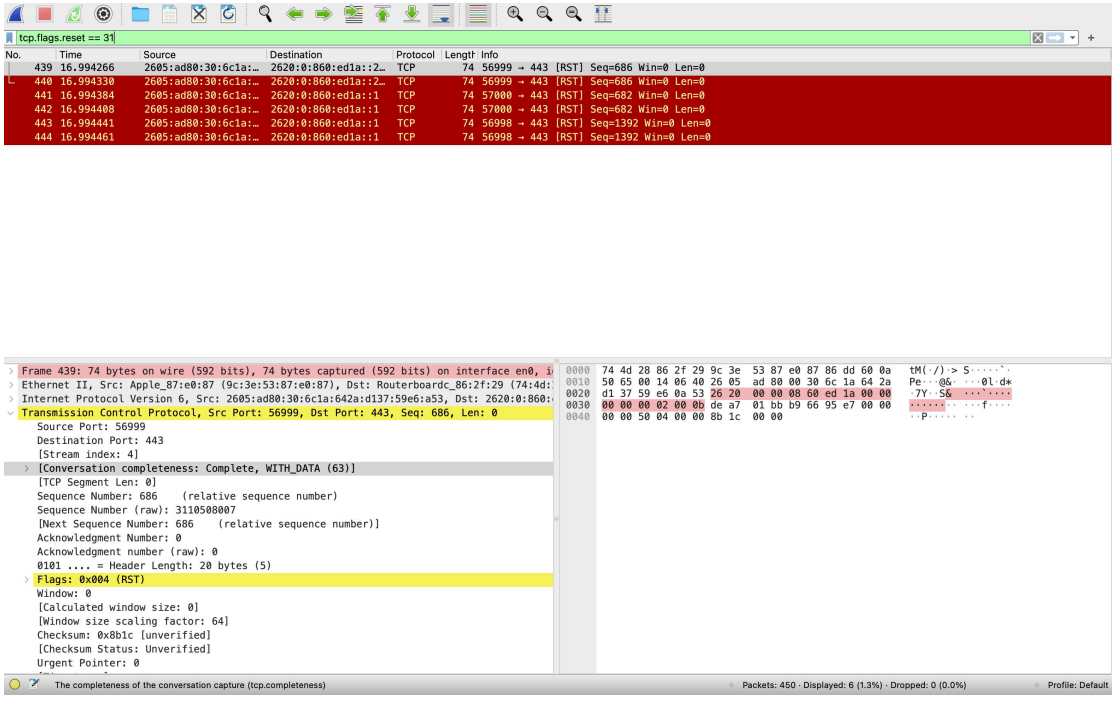
Solution for 3:

3 way Hnadhshake:Establishing a dependable communication channel between two devices over a TCP/IP network is done through the TCP three-way handshake. It is an essential component of the TCP protocol, guaranteeing that data is prepared for transmission and reception on both ends. The handshake consists of these three steps:

1. SYN:Client sends a TCP packet with SYN flag to tell that it wants to establish connection.

SYN-ACK:The server responds with a TCP packet that has both the SYN and ACK flags set, acknowledging the client's request and showing its readiness to establish a connection.
ACK:he client sends a TCP packet with the ACK flag set, acknowledging the server's response. At this point, the connection is established, and data can start flowing in both directions.
Step 1:once the packets are captured in wireshark.
Step 2:Open a website www.wikipedia.org.
Step 3:Then apply filter for tcp traffic by using tcp in filter box.(tcp.flags.reset==31)
Step 4:We can see here SYN,SYN-ACK and ACK.
Step 5:At SYN check for source and destination IP addresses,it indicates its a SYN packet.
Step 6:Second packet is SYN-ACK,it should show the acknowledgment of SYN packet with both SYN and ACK.
Step 7:In the third selected packet ACK,it acknowledges the SYN-ACK that it wants to establish connection and wants to acknowledge the same and thus completes 3 way handshake

Regarding the tcp.completeness == 31, this is likely a display filter in Wireshark that filters for packets where the TCP segment is complete, meaning all the expected data has been received. The completeness value of 31 may indicate a fully captured TCP segment.

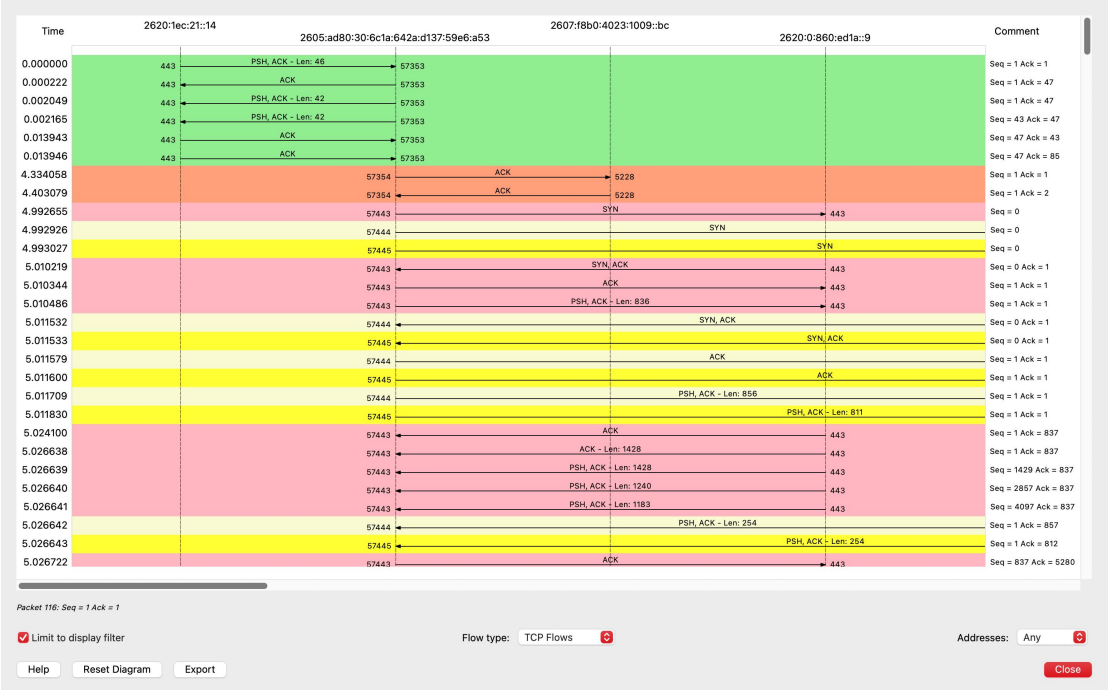


Solution for 4:
Step 1:Start capturing packets in wireshark.
Step 2:open any webbrowser and navigate to www.wikepedia.org.
Step 3:Stop the capturing of packets and analyse the captured data.
Step 4:From menu bar select statistics->Flow graph
Step 5:Observe the graph generated by filtering out some additional information.
TCP flow information is as follows:

1. The initial Connection is established with a 3 way handshakeSYN,SYN-ACK,ACK.
2. Data is transmitted with a Push(PSH) flag and acknowledged.
3. The connection is terminated with a FIN-ACK and a final ACK.
4. A reset (RST) pocket is sent to terminate the connection abruptly.

This includes information about different TCP communication events such as SYN (synchronization), ACK (acknowledgment), PSH (push), and data lengths the data includes timestamps and IP addresses associated with these communication events. This type of data is commonly used for network analysis and troubleshooting to understand the flow of communication and identify any potential issues or anomalies.

5.



Solution for 5:

Step 1:open wireshark run the packets

Steo 2 :open a website (www.sephora.com)

Step 3:pause the packets on wireshark, open the website and once that is compeleted,open terminal type ifconfig

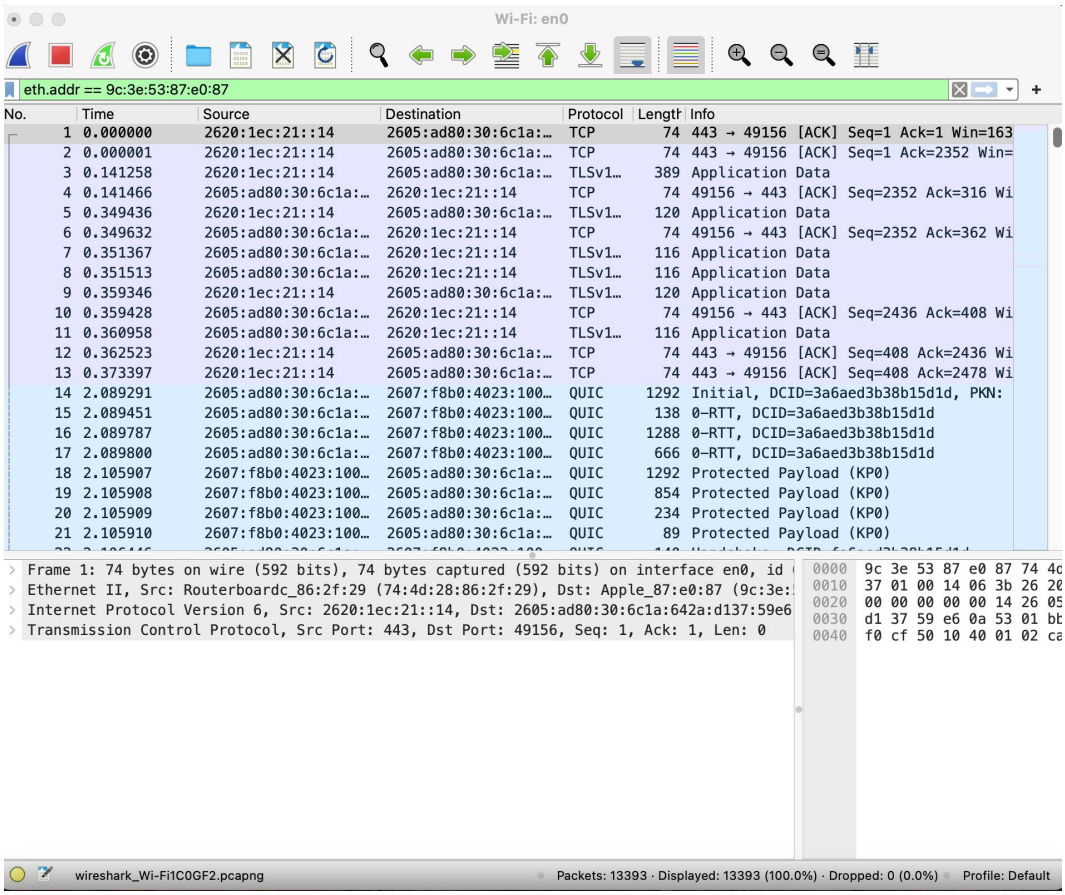
Step 4:Once the ip address and mac address of the system is visible choose en0 and select ether and copy this address on notepad.

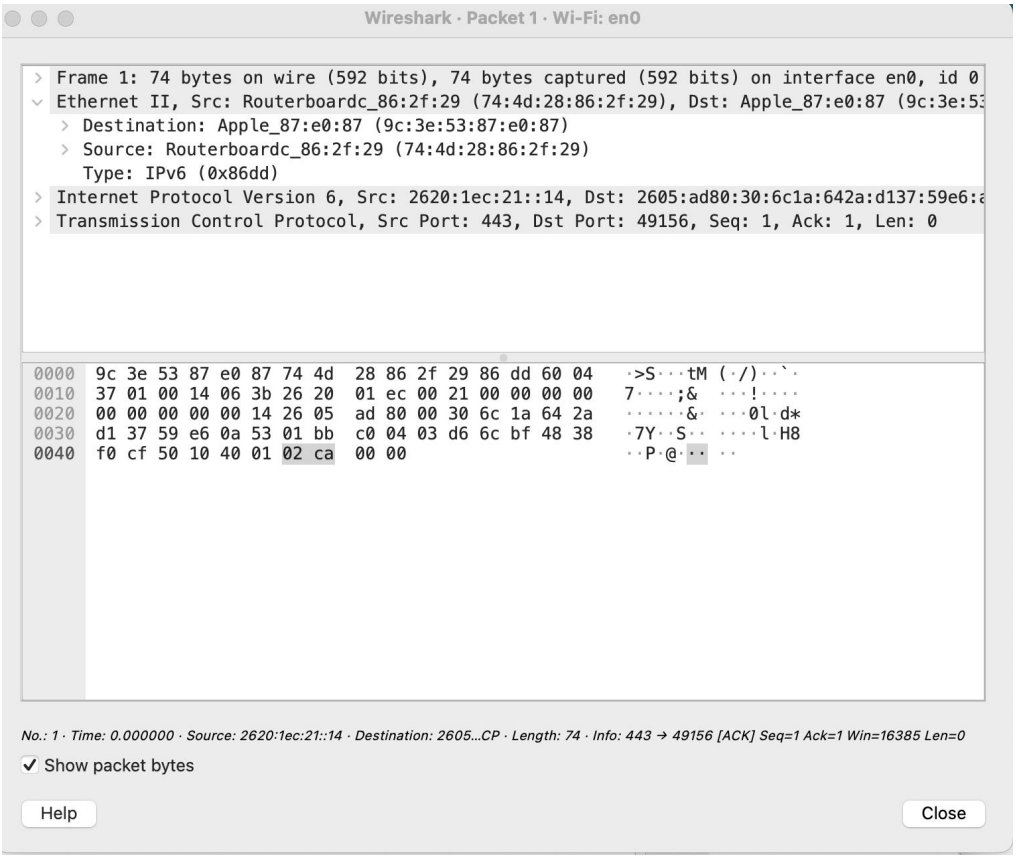
Step 5: Once this is compeleted compare the address with wireshark by using this filter etr.addr=MAC address of the pc.

Step 6:Expand the ethernet II src and check for source MAC address,since this will be same we can

In this way we can compare both the PC Mac address and compare it to wreshark.

```
stf0: flags=0<> mtu 1280
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 82:f7:fa:cc:12:22
        media: none
        status: inactive
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 82:f7:fa:cc:12:21
        media: none
        status: inactive
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 82:f7:fa:cc:12:01
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 82:f7:fa:cc:12:02
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:ad:b1:59:2f:40
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:ad:b1:59:2f:44
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 36:ad:b1:59:2f:40
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 8 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
ap1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether be:3e:53:87:e0:87
        inet6 fe80::bc3e:53ff:fe87:e087%ap1 prefixlen 64 scopeid 0xb
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (<unknown type>)
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 9c:3e:53:87:e0:87
        inet6 fe80::823:e427:58e2:9eb3%en0 prefixlen 64 secured scopeid 0xc
        inet6 2605:ad80:30:6c1a:14ff:844f:ddc4:f966 prefixlen 64 autoconf secured
        inet6 2605:ad80:30:6c1a:642a:d137:59e6:a53 prefixlen 64 autoconf temporary
        inet 10.207.95.194 netmask 0xffffffc0 broadcast 10.207.95.255
        nd6 options=201<PERFORMNUD,DAD>
```

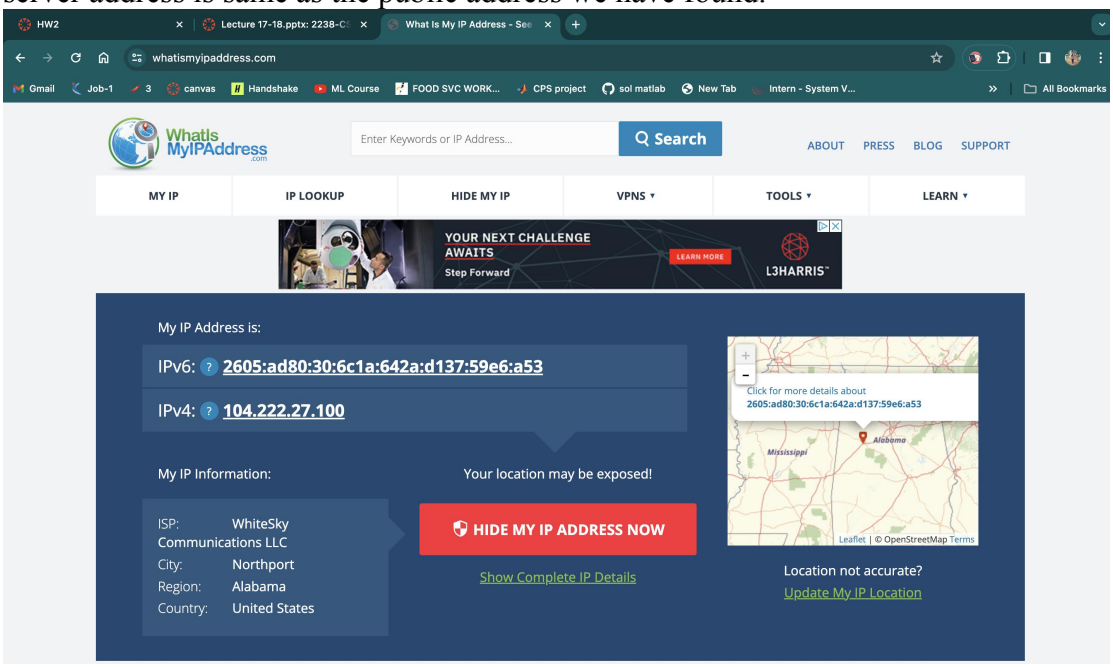




Solution for 6:

Step 1:in a web browser check for pc s public ip address using what's my ip? and hence you get the below ip address.

Step 2:Now go to terminal type the command nslookup google.com we can see the server address is same as the public address we have found.



IP of google.com

```
(base) srinidhik@Srinidhis-MacBook-Pro ~ % lookup google.com
zsh: command not found: lookup
(base) srinidhik@Srinidhis-MacBook-Pro ~ % nslookup google.com
Server:         2605:ad80:1f:c000::6
Address:        2605:ad80:1f:c000::6#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.115.102
Name:   google.com
Address: 142.250.115.139
Name:   google.com
Address: 142.250.115.100
Name:   google.com
Address: 142.250.115.138
Name:   google.com
Address: 142.250.115.101
Name:   google.com
Address: 142.250.115.113

(base) srinidhik@Srinidhis-MacBook-Pro ~ %
```

Solution for 7:

Step 1:Here packets are filters using http and thus there are 4 packets for a particular website given in the question I have found 4 packets of http and its using 1.1