**5-2 Identifying the TCP/IP layers in frame:**

1. By opening Wireshark, type tcp port http in capture filter selected interface box and click start.

2. Now open any web browser, load the complete page, and exit the browser parallelly observe the capturing field on Wireshark.

3. Now, click on the top pane of HTTP protocol filed which has an info starting with GET.

4.Now examine the ethernet II by expanding it. Observer the fields in it.

From textbook, write which layer of the TCP/IP model the Ethernet II header represents, and then click again to collapse this header: Network Layer

**Graphical user interface, application

Description automatically generated with medium confidenceScreenshot of Ethernet II**

5. Now expand Internet Protocol and examine all the fields.

From textbook, write which layer of the TCP/IP model the Internet Protocol header represents, and then click again to collapse this header: Internetwork Layer

**A picture containing calendar

Description automatically generatedScreenshot of Internet Protocol**

6. Now expand Transmission Control Protocol and examine fields.

From textbook, write which layer of the TCP/IP model the Transmission Control Protocol header represents, and then click again to collapse this header: Transport Layer

**A picture containing calendar

Description automatically generatedScreenshot of Transmission Control Protocol**

7. Now expand Hypertext Transfer protocol and observe all the information and data portion of frame of the web server.

From textbook, write which layer of the TCP/IP model the HTTP protocol represents, and then click again to collapse this header: Application Layer

**Graphical user interface, application, Word

Description automatically generatedScreenshot of HTTP protocol**

**5-5 Examining the Internetwork Layer:**

1. Open Wireshark, click icmp on Capture filter textbox by starting the start icon on toolbar.

2. Now, open command prompt and ping the default gateway (type ipconfig to know the default gateway address) and parallelly observe the packets on the Wireshark.

3. Now, stop the running live capture by stop button on the tool bar and click on the ICMP from the protocol field and examine the Internet protocol fields by expanding it as shown below.

**Screenshot of Internet Protocol**

Graphical user interface, text, application

Description automatically generated

4. Now expand the Internet Control Message protocol and observe the type fields and the data portion of the ICMP which is simple string of letters as below.

Graphical user interface, text, application

Description automatically generated**Screenshot of Internet Control Message Protocol**

**Observed below values in the Version, Time to live, Protocol, and Checksum fields:**

Version: 4

Time to live: 128

Protocol: ICMP (1)

Checksum: 0x82ab

**5-6 Capturing ARP and ICMP packets on Wireshark:**

1. Open Wireshark and type icmp on Capture Filter text box.

2. Now open Command prompt and type tracert books.tomsho.com until the trace is finished. Parallelly observe the behavior of packets on Wireshark.

3.Now, stop the running live capture toolbar icon on the Wireshark. Type arp on the Capture Filter text box and observe the info on the capture page as shown below.

Graphical user interface, text, application

Description automatically generated**Screenshot of ARP packets**

4.Now, click on the packet summary line and see the destination address and expand Ethernet II line, examine the internetwork-layer protocol as 0x806 as below.

Text

Description automatically generated**Screenshot of Ethernet 11 of ARP packet**

5. Click on Address Resolution Protocol(request) line and examine the fields under it which indicates technology and protocol type of Network access layer and MAC address.

6. Now, click on the Address Resolution Protocol(reply) line and observe that MAC address of the default gateway as shown in below.

**Screenshot of ARP (reply)**

Graphical user interface

Description automatically generated

7.Now, type icmp on Capture options and click on the ICMP echo line and expand the Internet protocol and notice the “Time to live” as 1 as below. The same value is seen for the next two lines of ICMP echo.

Text, application

Description automatically generated**Screenshot of TTL for ICMP echo (first line)**

8. Now, click on the fourth line of ICMP echo and observe the “Time to live” as 2 which again continues for the next two lines and tracert follows this pattern until the packet reaches to last router with followed line having the message as “Time-to-live-exceeded” as per the below shown image.

**Screenshot of TTL for ICMP echo (fourth line)**

Text

Description automatically generated

**5-8 Examining the network interface & IP protocol status & statistics using netstat program:**

1. Open command prompt, type netstat -e to see the statistics of the interface which includes number of bytes and packets received as shown below.

Text

Description automatically generated**Screenshot of Interface statistics**

2.Now type netstat -s to view all the protocols statistics and type netstat -ps IP for viewing to the limited display.

3. Now type netstat -ps ICMP to view the ICMP messages received and sent as show below.

Text

Description automatically generated**Screenshot of ICMP statistics**

4. Now trace books.tomosho.com by using tracert books.tomsho.com and again type netstat -ps ICMP to see the increase in Time Exceeded value as below.

Text

Description automatically generated**Screenshot of view the Time Exceeded value**

5. Now, type netstat -r which gives the routing table which is used to view the interface to send the packets as shown below.

Text

Description automatically generated**Screenshot of routing table**