**NETWORK LAB REPORT**

**NAME:** ANURAN CHAKRABORTY

**ROLL NO.:** 20

**CLASS:** BCSE-III

**SECTION:** A1

**ASSIGNMENT NUMBER:** 5

**PROBLEM STATEMENT:**

Packet tracer and traffic analysis with Wireshark.

**DEADLINE:** 4TH APRIL, 2019

**SUBMITTED ON:** 4TH APRIL, 2019

**REPORT SUBMITTED ON:** 11TH APRIL, 2019

1. **Generate some ICMP traffic by using the Ping command line tool to check the connectivity of a neighbouring machine (or router). Note the results in Wireshark. The initial ARP request broadcast from your PC determines the physical MAC address of the network IP Address, and the ARP reply from the neighboring system. After the ARP request, the pings (ICMP echo request and replies) can be seen.**

|  |
| --- |
|  |
| **Fig 1.** The ARP Requests can be seen asking for the physical address of the machine. |
|  |
| **Fig 2.** The ICMP packets which are sent |

* 1. **2. Generate some web traffic and**
  2. **a. find the list the different protocols that appear in the protocol column in the unfiltered packet-listing window of Wireshark.**

The different protocols that were found were:

* TCP
* TLSv1.2
* DNS
* GQUIC
* UDP
* SSDP
* MDNS
  1. **b. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)**

|  |
| --- |
|  |
| **Fig 3**. Showing the HTTP get and OK reply |

It can be seen from fig 3. That it took approximately 0.054 seconds from the OF reply to be received after the last get has been dispatched.

* 1. **c. What is the Internet address of the website? What is the Internet address of your computer?**

From Fig. 3. It can be seen that for the HTTP get message the source is 192.168.0.106 and the destination address is 14.139.40.44. Thus, IP address of the website is: **14.139.40.44** and that of the computer is:

**192.168.0.106.**

* 1. **d. Search back through your capture, and find an HTTP packet containing a GET command. Click on the packet in the Packet List Panel. Then expand the HTTP layer in the Packet Details Panel, from the packet.**

|  |
| --- |
|  |
| **Fig 4.** Packet details panel of HTTP get message. |

* 1. **e. Find out the value of the Host from the Packet Details Panel, within the GET command.**

From **Fig 4.** It can be seen that the Host is **www.ignou.ac.in.**

* 1. **3. Highlight the Hex and ASCII representations of the packet in the Packet Bytes Panel.**

|  |
| --- |
| ASCII representation  Hex representation |
| **Fig 5.** Hex and ASCII regions of packet. |

**4. Find out the first 4 bytes of the Hex value of the Host parameter from the Packet Bytes Panel.**

|  |
| --- |
|  |
| **Fig 6.** First 4 bytes of host |

* 1. **5. Filter packets with http, TCP, DNS and other protocols.**
  2. a. **Find out what are those packets contain by following one of the conversations (also called network flows), select one of the packets and press the right mouse button..click on follow**.

|  |
| --- |
|  |
|  |
| **Fig 7.** Network flow |

* 1. **6. Search through your capture, and find an HTTP packet coming back from the server (TCP Source Port == 80). Expand the Ethernet layer in the Packet Details Panel.**

|  |
| --- |
|  |
| **Fig 8.** Ethernet details of packet coming from host |

* 1. **7. What are the manufacturers of your PC’s Network Interface Card (NIC), and the servers NIC?**

PC’s Network Interface Card (NIC): **Gigabyte.**

Server’s NIC: **TP-Link.**

* 1. **8. What are the Hex values (shown the raw bytes panel) of the two NICS Manufacturers OUIs?**

|  |
| --- |
|  |
| **Fig 9.** Hex value of Gigabyte NIC |
|  |
| **Fig 10.** Hex value of TP-Link Router |

* 1. **9. Find the following statistics:**

|  |
| --- |
|  |
| **Fig 11.** Statistics of packets |

* 1. **a. What percentage of packets in your capture are TCP, and give an example of the higher-level protocol which uses TCP?**

**48.65%** of packets are TCP. **FTP** is a higher-level protocol that uses TCP.

* 1. **b. What percentage of packets in your capture are UDP, and give an example of the higher-level protocol which uses UDP?**

**51.35%** of packets are TCP. **DNS** is a higher-level protocol that uses TCP.

* 1. **10. Find the traffic flow Select the Statistics->Flow Graph menu option. Choose General Flow and Network Source options, and click the OK button.**

|  |
| --- |
|  |
| **Fig 12.** Network flow graph |