##### Chapter 4 Wireshark Activity

Perform the following steps to capture and analyse network traffic using Wireshark Software:

Task #1:

1. Ask your classmate for his IP address.
2. Ping your classmate’s IP address infinitely (Example: **ping x.x.x.x -t**)
3. From Wireshark start capturing traffic from your connected network interface card.
4. We are only interested in certain traffic from the captured list in Wireshark.
5. From the filter section in Wireshark type **ICMP.**
6. From the captured list look for ICMP request and then record the following:

|  |  |
| --- | --- |
| Source & Destination MAC address |  |
| Source & Destination IP address |  |
| Time to Live |  |
| Version |  |

1. Repeat step 6 for ICMP response and then record the following:

|  |  |
| --- | --- |
| Source & Destination MAC address |  |
| Source & Destination IP address |  |
| Time to Live |  |
| Version |  |

Task #2:

1. From Wireshark start capturing traffic from your connected network interface card.
2. Open your browser and request the following page <http://www.polytechnic.bh>.
3. Stop the capture.
4. We are only interested in certain traffic from the captured list in Wireshark.
5. Go to the filter section in Wireshark and type **tcp.port == 80**
6. We can also filter traffic based on both ports **tcp.port == 80 || tcp.port == 443**
7. Select the first packet from Wireshark and record the following:

|  |  |
| --- | --- |
| Source & Destination MAC address |  |
| Source & Destination IP address |  |
| Source & Destination port Numbers |  |
| Sequence Number |  |
| Acknowledgment Number |  |
| SYN Flag |  |
| ACK Flag |  |
| Windows Size |  |

1. Repeat step 5 for the second and third captured packets.