Computer Networks Lab (Trace Route, Ping)

Instructions:

1. This assignment requires you to self-study the manual or associated support material of the traceroute and ping commands and the related literature. The commands would be introduced to you in the class.
2. For each of your answer paste a screen dump of your screen in support of justification of your answer, wherever applicable.

To Do:

1. Enumerate the steps and briefly discuss how the utility `traceroute` works using an illustrative website as the argument to it. In your explanation of the tool operation discuss the answers to following questions w. r. to `traceroute`
   - What if there was no `TTL` field in the invocation of the `traceroute` at all?
   - How will the routers in between determine whether the `TTL` value limit has reached?
   - Should an intermediate router that receives a `traceroute` packet always respond with an ICMP `TTL` exceeded message? If the answer is a yes, reason why and if the answer is a no, then argue how do we know the address of all the routers/hops in between us and the destination?
   - Why does `traceroute` make use of a destination UDP port number which is invalid - i.e. it sends a packet to a UDP port in the range ⟨33434 to 33534⟩?
   - How do we know the address of all the routers/hops in between us and the destination when using the `traceroute`?
   - How is `traceroute` latency calculated?
2. Execute the `traceroute` command with http://www.yahoo.com as argument. Write down the IP address of yahoo.com that was used for the trace route. Determine the number of iterations required to determine route. Enlist the IP addresses of all the machines between the source and the destination. What is the average round trip time of the packet that reached the destination?
3. [optional] With respect to the question no 2, run `traceroute` on one window/linux of your OS and run tcpdump on the other window/linux. Analyze the output of tcpdump. Answer the following questions giving appropriate highlighted snapshots in support of your answer :

   a. How many packets are send by `traceroute` in each iteration? How can you prove this using the tcpdump output.
   b. Consider one specific iteration of `traceroute` invocation/iteration. For this specific iteration, what are the individual round trip times of each of the three probes sent? What is the average round trip time? Does it match with the round trip time returned by `traceroute`?
   c. In each iteration of `traceroute` does it use the same port number for the destination? IF yes, reason why and if no, then also argue why does it do so.

4. Use the Visual `traceroute` command at `https://www.monitis.com/traceroute/`. What is the source address and the destination address of these packets?

5. If you think a firewall stopped the packet, how can one know that a firewall has come in the way? What do you think the IP address of that firewall is based on where the trace route stopped?

6. If a firewall stopped has not obstructed the packet sent, what does the last IP address appearing in the trace route list indicate?
7. Enlist and briefly explain all the usages of the ping program - explain each use with the help of an example.
8. Write a small shell script that uses ping to simulate the working of `traceroute`. Briefly explain the operation of the script.
9. Explain all the approaches that can be used to do a ping sweep.