

# CSEC 101 Lab 2: Network Traffic Sniffer

---

**Name:** Sanchit Monga

Before starting each activity, review the questions to ensure that all observations and data necessary to complete your report are recorded.

Use this word document to insert your answers in the space immediately following the questions. Use as much space as needed.

**Note: All commands are shown in quotes, to be typed without the quotes**



## Activity 1 - Setup

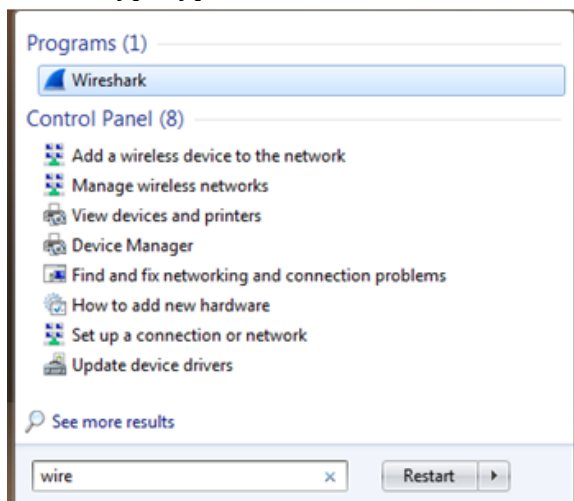
- **Before beginning any lab, reboot Windows on your Lab PC.**
- Using MS Windows: you can do this by clicking on Restart button or by pressing CTRL-ALT-DEL keys at the same time and then selecting Restart.

## Activity 2 – Examine Network Traffic using the Packet Sniffer Wireshark

- open Wireshark: . Click on the Windows icon,



or click the on the  if using Win 7 or  for Win 10, on the 'search' field at the bottom, type type “wireshark” in the search box.



Then click on the Wireshark icon to open the application.

## CSEC 101 Lab 2: Network Traffic Sniffer

---

- For **newer** version of Wireshark:
  - a. select Capture -> Options
  - b. In the "Wireshark - Capture Interfaces" , on its Input tab, under "Interface"
  - c. select the Ethernet 2 (or the one matching the Ethernet connected to the RIT network)
  - d. click on "Start"
- For **older** version of Wireshark:
  - a. select Capture -> Interfaces
  - b. under "Devices" select the Ethernet 2 (or the one matching the Ethernet connected to the RIT network)
  - c. click on "Start"
- In the text bar just under the menu ribbon

For **newer** version of Wireshark the text bar shown as : "Apply a display filter ... <Ctrl-/>

For **older** version of Wireshark it is labeled as: "Filter"

1. (2 points) In that text bar, type "icmp", hit return, it should turn green if all is working  
OK  
Turned green

Note: ICMP (Internet Control Message Protocol) is the protocol use by the “ping” application command

### Activity 5 – Analyzing the Wireshark data

To be able to examine the data later to answer the questions in this section:

- Save the Wireshark capture to record data you see, to a file,
- And save the cmd widow data you entered, saving it to a text file or take a snapshot of the image

➤ Obtain the IP Address of the PC next to you, from the student next to you.

➤ at the cmd window, type: “ping <ip address> -n 1”

Note: < > marks the location for the field you have to enter but without the <>. In this case is the IP address from step # 1.

And hit return

2. (10 points) How many new entries you see on cmd widow? And what are they  
-n represents the number of pings sent to the particular IP address. Therefore, only one ping would be sent, which will bring one reply.

Pinging 10.100.66.128 with 32 bytes of data:

Reply from 10.100.66.128: bytes=32 time=78ms TTL=63

3. (10 points) What does the Wireshark frame capture show in the "Protocol" and "Information" columns?

The protocol column shows the protocol used when sending the ping to the IP.

And the information shows the type of echo ping request or reply present in that packet.

4. (10 points) Why do the Wireshark names in "Protocol" and "Information" columns vary from the “ping” command you used in the cmd window ?

The wireshark shows whether the packet is a request or a reply. The protocol shows which protocol was used to send data.

5. (10 points) How many new entries you see on Wireshark ? And what are they  
There are two entries on Wireshark window, one is for reply and other is for request.

6. (10 points) For the same ping packet, the value in the cmd window for "bytes=" is different than the values shown in Wireshark in the "Length" column. Explain why?  
The length contains the data as well as the ICMP header, IP header and the ethernet frame of the packet, therefore it will always be greater than the number of bytes sent through ping.

## CSEC 101 Lab 2: Network Traffic Sniffer

---

- at the cmd window, type: `ping <ip address> -n 1 -l 1000`  
And hit return
- 7. (10 points) How many new entries you see on Wireshark ? And what are they  
There are 2 entries that can be seen on Wireshark, request and reply.
- 8. (10 points) For the same ping packet, the value in the cmd window for "bytes=" is different than the values shown in Wireshark in the "Length" column. Explain why?  
The length (1042 bytes) contains the data as well as the ICMP header, IP header and the ethernet frame of the packet, therefore it will always be greater than the number of bytes sent through ping (which was 1000).
- at the cmd window, type: `ping <ip address> -n 1 -l 4000`  
And hit return
- 9. (10 points) How many new entries you see on Wireshark ? And what are they  
There are 2 entries that can be seen on Wireshark, Echo ping request and Echo ping reply.
- 10. (10 points) For the same ping packet, the value in the cmd window for "bytes=" is different than the values shown in Wireshark in the "Length" column. Explain why?  
The length of the ping packet on Wireshark is 1082. The length is less than the number of bytes shown on cmd because it exceeds the limit.
- 11. (8 points) Out of all the options where can you find online help for Wireshark, which one would you select as your primary source?  
[Wiki.wireshark.org](http://Wiki.wireshark.org)