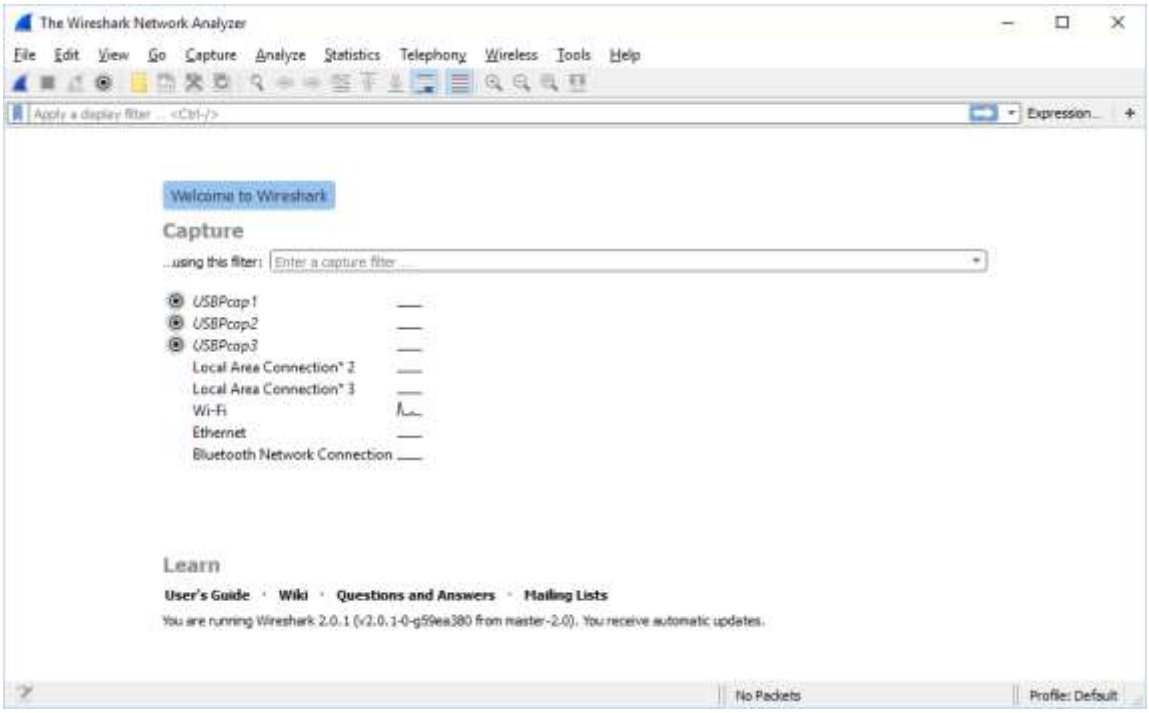
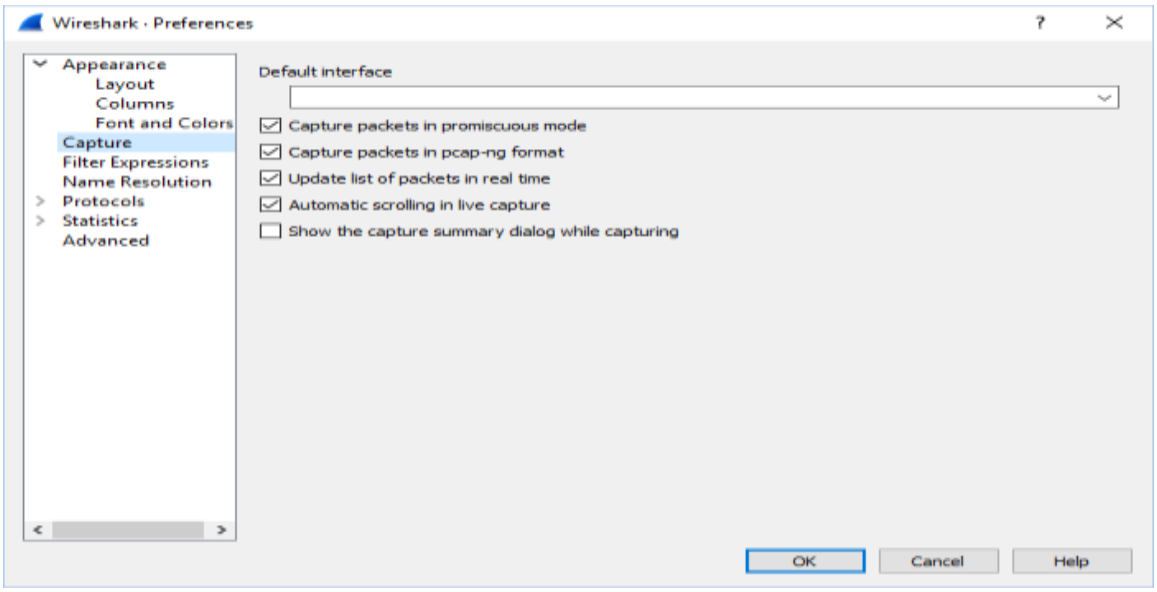
# Lab 1

(All your answers should be validated with the screen shots that you take during this exercise)

1. For this lab you'll need the Wireshark program installed, which can be obtained from http://www.wireshark.org. It is a free software and supports many platforms.
2. When you first start Wireshark you will be brought to the default startup screen, similar to one given below. In order to begin a network capture you will need to choose a network device to use.



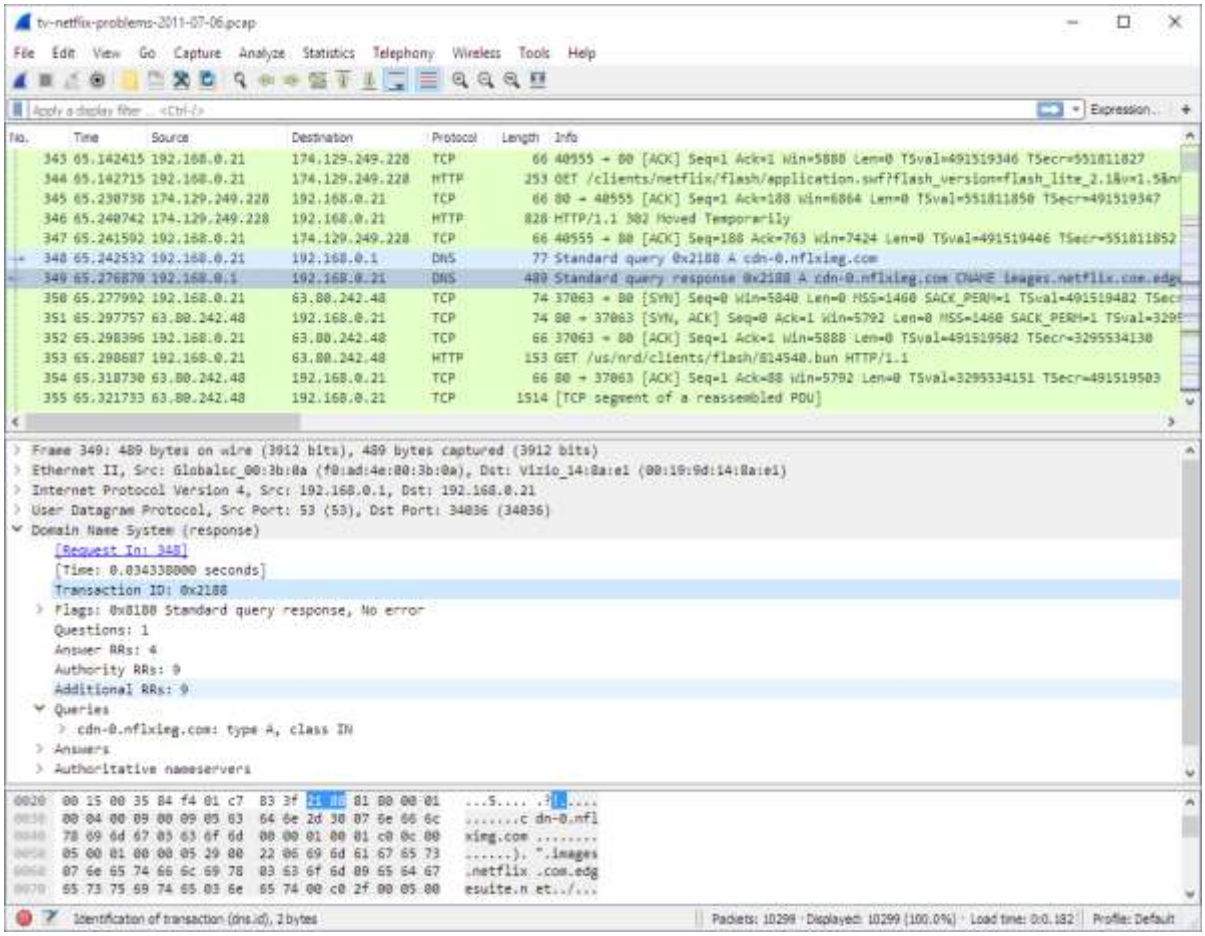

If you want to capture packets sent directly to your device only, that you have to uncheck the "Capture packets in promiscuous mode" checkbox.



Then click Capture->Start from the menu and if your network card is working you should very quickly start to see lines appearing in your packet capture window (see example below).

## The Main window

Wireshark's main window consists of parts that are commonly known from many other GUI programs.




You can see, that the main window consists of three different panes: Packet list pane, Packet details pane, and Packet bytes pane.

Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes.

There are different columns in the list pane, but the default columns will show:

- **No.** The number of the packet in the capture file. This number won't change, even if a display filter is used.
- **Time** The timestamp of the packet.
- **Source** The address where this packet is coming from.

- **Destination** The address where this packet is going to.
- **Protocol** The protocol name in a short (perhaps abbreviated) version.
- **Length** The length of each packet.
- **Info** Additional information about the packet content.

If you double click on the packet line you can obtain more details about that specific packet.

While your capture is running, you can stop it by hitting the Capture->Stop, or pressing the "stop capture" button (red square). You can save the capture by clicking on the "save capture button" in your selected folder. By now, you should have enough data to start to analyze.

## Filtering packets

Wireshark can filter packets while capturing or displaying. Display filters allow you to concentrate on the packets you are interested in while hiding the currently uninteresting ones. They allow you to select packets by:

- **Protocol**
- **The presence of a field**
- **The values of fields**
- **A comparison between fields etc.**

## Examining the Packet Capture

- Start a new Capture
- Open the Browser
- Type a web page address (ex. www.mercy.edu)
- Apply a filter for "TCP" protocol.
- Stop the Capture.
- Now you can isolate a TCP stream.
- Right click on a packet in the Packet List and select Follow TCP Stream. This creates an automatic Display Filter which displays packets from that TCP session only.
- It also displays a session window, which is by default, an ASCII representation of the TCP session, where the client packets are in red and the server packets in blue. Change to Hex Dump Mode and view the payloads in raw Hex.
- Wireshark automatically creates a display filter to filter out this TCP conversation.

1. From your Wireshark Capture, write the **IP Addresses** and **Port Numbers** for the Client and the Server.

2. What **HTTP** version is your browser running? What version of **HTTP** is the server running?

3. Identify the **TCP** segments that are used to initiate the **TCP** connection between the client computer and www.mercy.edu.

4. For each packet in the **TCP 3-way** handshake, write the Sequence and Acknowledgement numbers.

- You can see the flow traffic with **Statistics->Flow Graph** menu option, too.

5. What are the sequence numbers of the first four **data-carrying segments** in the TCP connection?

6. What is the length of each of these four **TCP segments**? The length of the TCP segment is only the number of data bytes carried inside the segment (excluding the headers).

- Run ***nslookup*** to determine the authoritative **DNS** servers for your university.
- Enter "***dns && ip.addr == host_IP_address***" into the display filter, where you obtain ***host_IP_address*** with ***ipconfig***.
- Locate the **DNS query** and **response** messages.

7. Are they transported using **UDP** or **TCP**? Explain why or why not.

8. What is the destination port for the **DNS query** message?

9. What is the source port of **DNS response** message?

10. With **statistics -> conversations**, find which hosts sent and received the most packets?