**EX.No.10.**

**Wireshark**

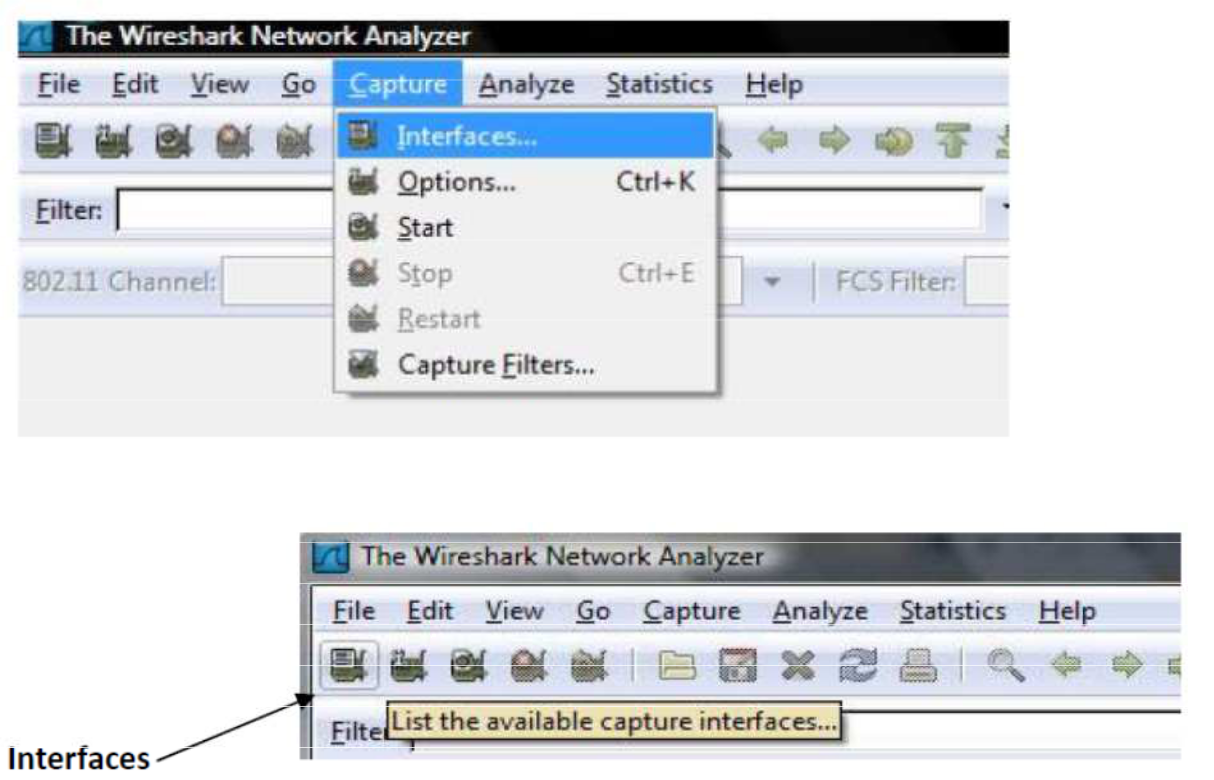
Wireshark is a network protocol analyzer, also known as a network sniffer. Formerly known as Ethereal, wireshark is computer application that captures and decodes packets of information from a network. “Wireshark can capture live network traffic or read data from a file and translate the data to be presented in a format the user can understand”.

Wireshark is a valuable tool for administrators that allow them to monitor all traffic that passes on a network. It is very useful for analyzing, diagnosing and troubleshooting problems that may occur.

Some features of wireshark.

* Data can be captured from a network connection or read from previous records of captured packets.
* Live data can be read from Ethernet, FDDI, PPP, token ring, IEEE 802.11, classical IP over ATM, and loopback interfaces (at least on some platforms; not all of those types are supported on all platforms).
* Captured files can be programmatically edited or converted via command-line switches to the “editcap” program.
* Captured network data can be browsed via a GUI, or via the terminal((command line) version of the utility tshark.
* Display filters can also be used to selectively highlight and color packet summary information.
* Data display can be refined using a display filter
* Hundreds of protocols can be dissected.

**i. Packet Capture Using Wire shark**

To start capturing packets you need to select the interface which is connected to the internet. This can be done by choosing Capture>>Interfaces from the Menu bar

**ii. Starting Wire shark**

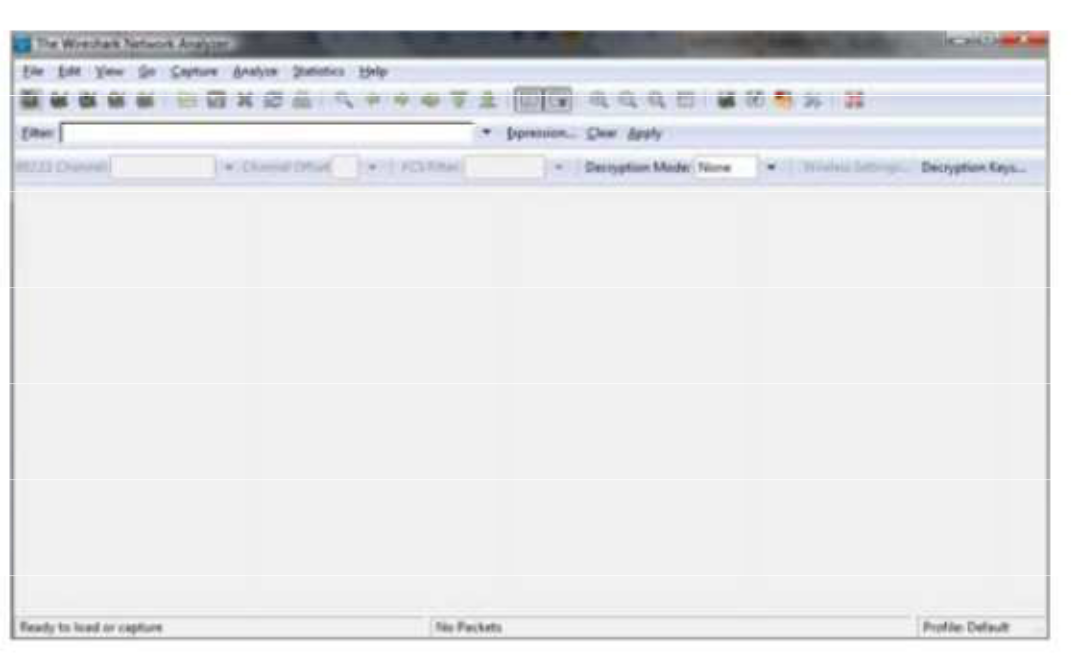
Wireshark can be downloaded from website www.wireshark.org .

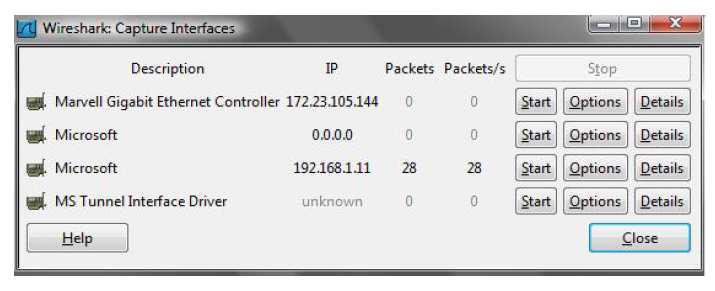


Wireshark has a friendly graphical user interface that makes it easier for the to analyze and diagnose packets that passing through the network. No data will initially be displayed when the user runs wireshark.

The environment and usage of wireshark will be explained further in this document.

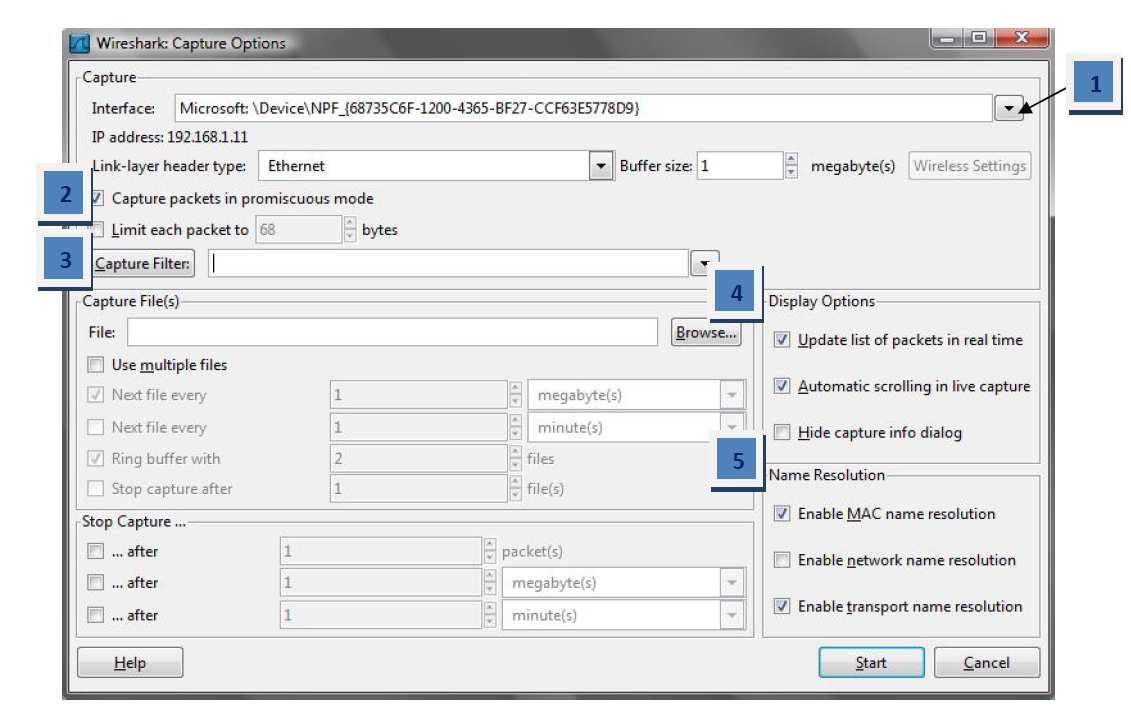
The different interfaces available that WinPcap driver sees in the machine are shown and you can either click start or click options for more options regarding capturing packets before starting the capture.



** iii. Viewing Captured Traffic**

.

The following figure represents the Capture Option's Window



**Steps**

1. Switch between different interfaces.You can only capture on one of the interfaces that Wireshark found on the system at a time.
2. Capture packets in promiscuous mode checkbox allows Wireshark not only to capture the packets going to or from your computer, but also all packets on your LAN segment.
3. Limit each packet to n bytes field allows you to specify the maximum amount of data that will be captured for each packet and is sometimes referred to as the snapien.
4. Capture filters are to be explained thoroughly in the next document. The default is not choosing any filters when capturing.
5. Display Options:

Update list of packets in real time to display the packets right away once captured.If it is not chosen Wireshark will display the packets captured when you stop the capture. It is important to know that choosing this option decreases the ability to capture packets in high rates.

Automatic scrolling in live capture automatically scrolls down to the last packet captured. If this option is not chosen Wireshark adds new packets to the end of the list, but does not scroll to the end of the packets pane. You can toggle this off from the commands menu at any time as shown in the following page.

Hide capture info dialog: Toggle on/off to hide/show the capture info dialog while capturing.

1. Name Resolution Options:

Enable MAC name resolution option: Toggle on/off to allow whether Wireshark translates MAC addresses into names or not.

Enable network name resolution option: Toggle on/off to allow whether Wireshark translates network addresses into names or not.

Enable transport name resolution option: Toggle on/off to allow whether Wireshark translates transport addresses into protocols or not.

An interesting way to set up the environment in Wireshark is by clicking the preferences icon from the commands menu and choosing the Capture tab.Options similar to those found in the Capture options dialog box can be found.

