Wireshark Lab 1: Introduction

What is Wireshark?

Wireshark is a network protocol analyzer, also known as a network sniffer. Formerly known as Ethereal, wireshark is a 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”[1].

Why Wireshark?

Wireshark is a valuable tool for administrators that allows 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[2]:

- 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.

[1] netsecurity.about.com/od/securitytoolprofiles/p/wireshark.htm
[2] en.wikipedia.org/wiki/Wireshark

How to get Wireshark?

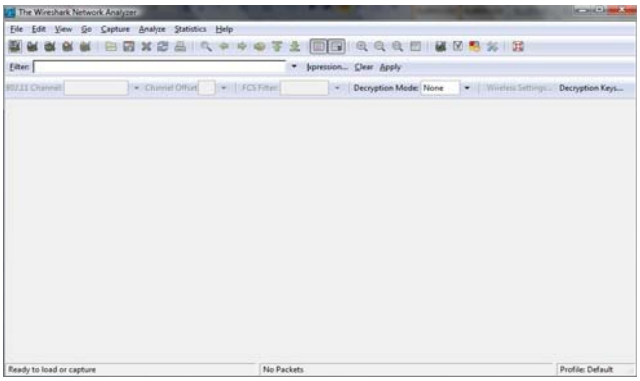
The latest copy/version of wireshark can be found on the official website:

http://www.wireshark.org

Each download package comes with the latest pcap (also known as libcap) for UNIX operating systems or WinPcap, a device driver and dynamic link library (DLL) that provides a pcap interface for Windows programs which is required for live packet capture.

If needed, the latest release of WinPcap can be found on: http://www.winpcap.org/install/default.htm

Getting started with Wireshark



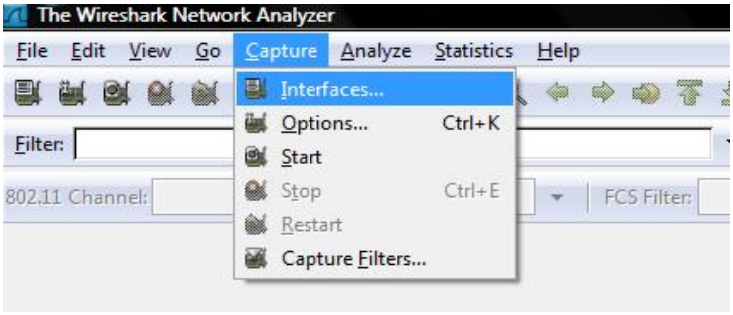
Wireshark has a friendly graphical user interface (GUI) that makes it easier for the user to analyze and diagnose packets that are passing through the network.

No data will initially be displayed when the user runs wireshark.

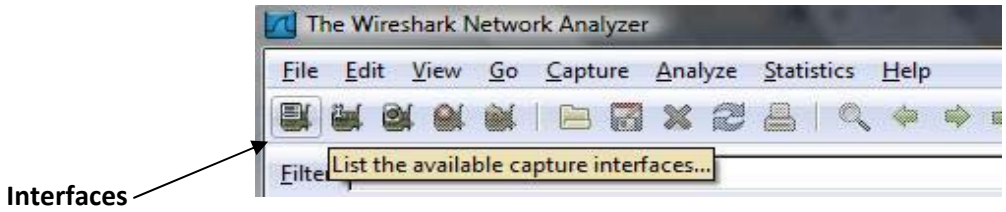
The environment and usage of wireshark will be explained further in this document.

To start capturing packets you need to select the interface which is connected to the network.

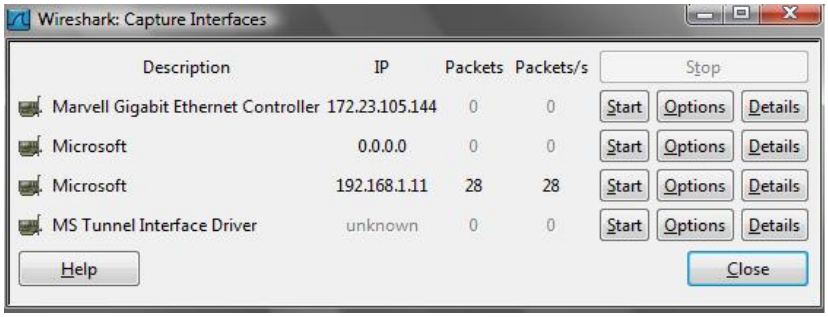
This can be done by choosing Capture >> Interfaces from the Menu bar.



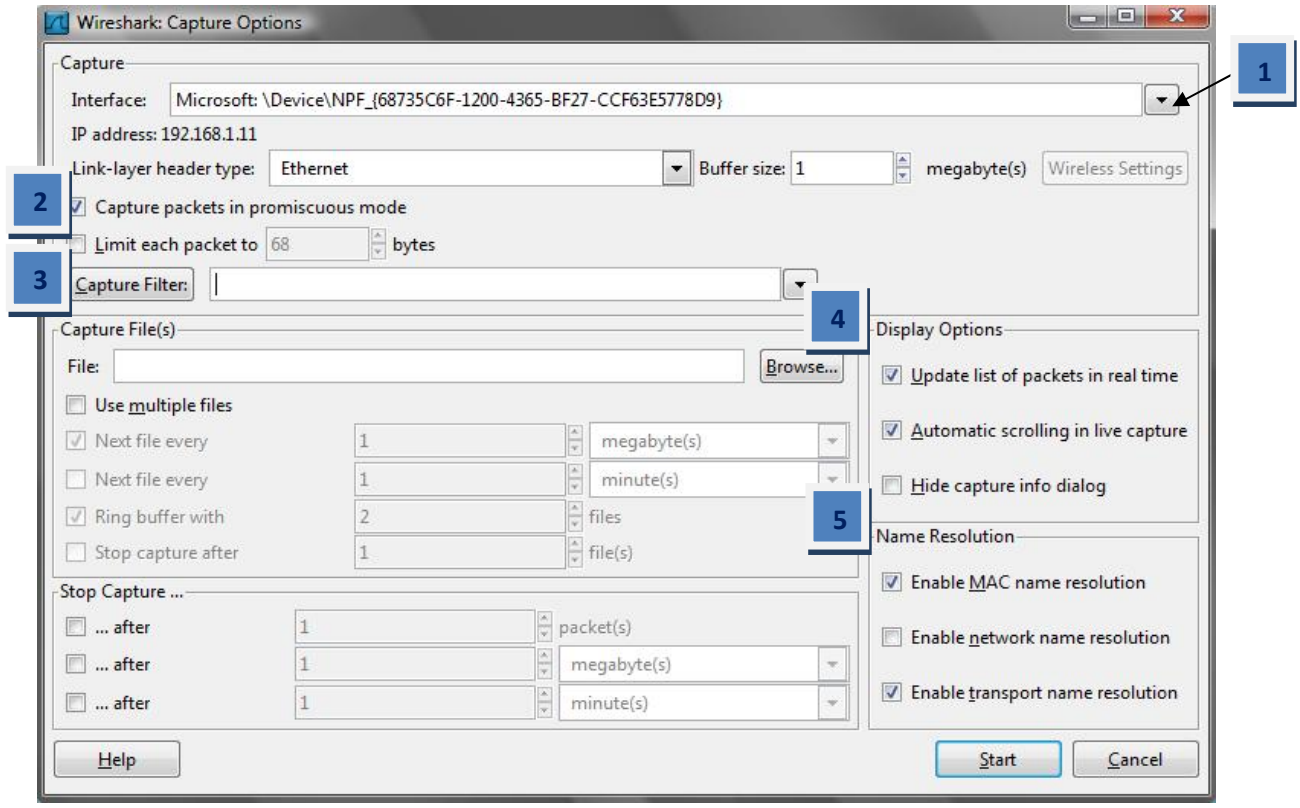
Or by clicking the first icon on the Commands menu



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.



The following figure represents the Capture Option's Window



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.

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 snaplen[3].

3 Capture filters are to be explained thoroughly in the next document. The default is not choosing any filters when capturing.

4 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.

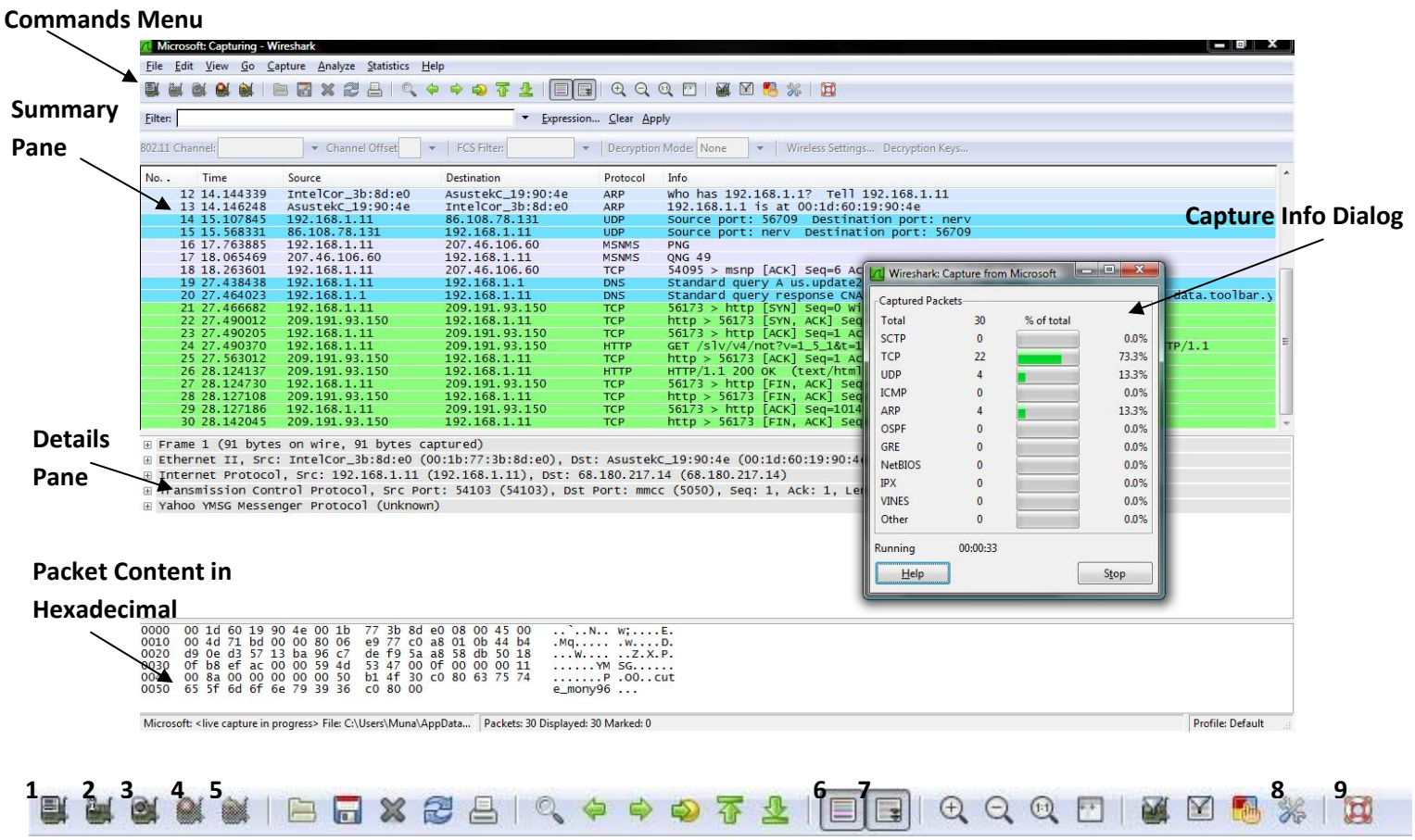
5 Name Resolution Options:

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.

[3] http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureOptions.html#ChCapCaptureOptionsDialog



1 List available capture interfaces

2 Show the capture options

3 Start a new live capture

4 Stop the running live capture

5 Restart the running live capture

6 Colorize packet list (Toggle button)

7 Auto scroll packet list in live capture (Toggle button)

8 Edit preferences

9 Show some help

An interesting way to set up the environment in wireshark to a default interface and some default options instead of choosing them each and every time you run 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.