How to capture the packet using Ethereal.

1. What is Ethereal ?

Ethereal is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

2. Where to get Ethereal ?

You can get the latest copy of the program from the Ethereal website: http://www.ethereal.com/download.html

3. Installing Ethereal

You must follow two steps:

-. Install WinPcap.

You will find a single installer exe called something like "auto-installer", which can be installed under various Windows systems. This installer is located at: http://winpcap.polito.it/install/Default.htm. You should download the latest released version (the latest one not marked "beta") and execute it.

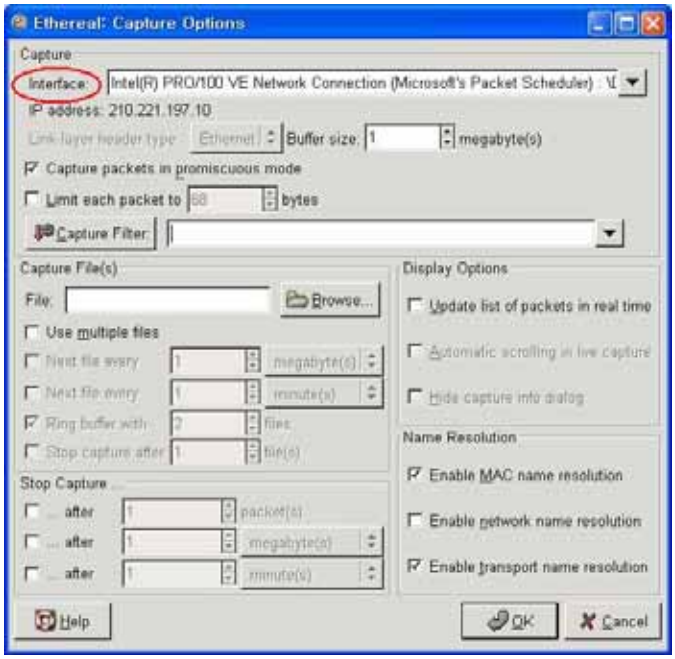
-. Install Ethereal.

http://www.ethereal.com/download.html#binaries.

Download the installer and execute it.

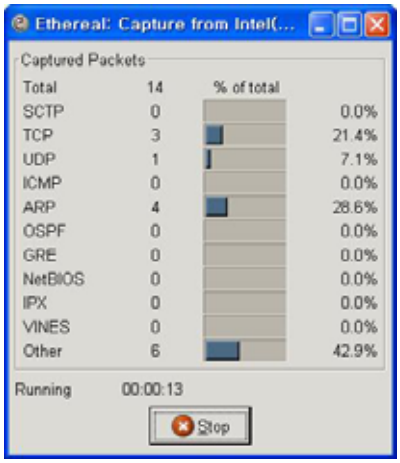
4. Capturing Network Data

-. By starting Ethereal and then selecting Start... from the Capture menu this brings up the Capture Options dialog box.

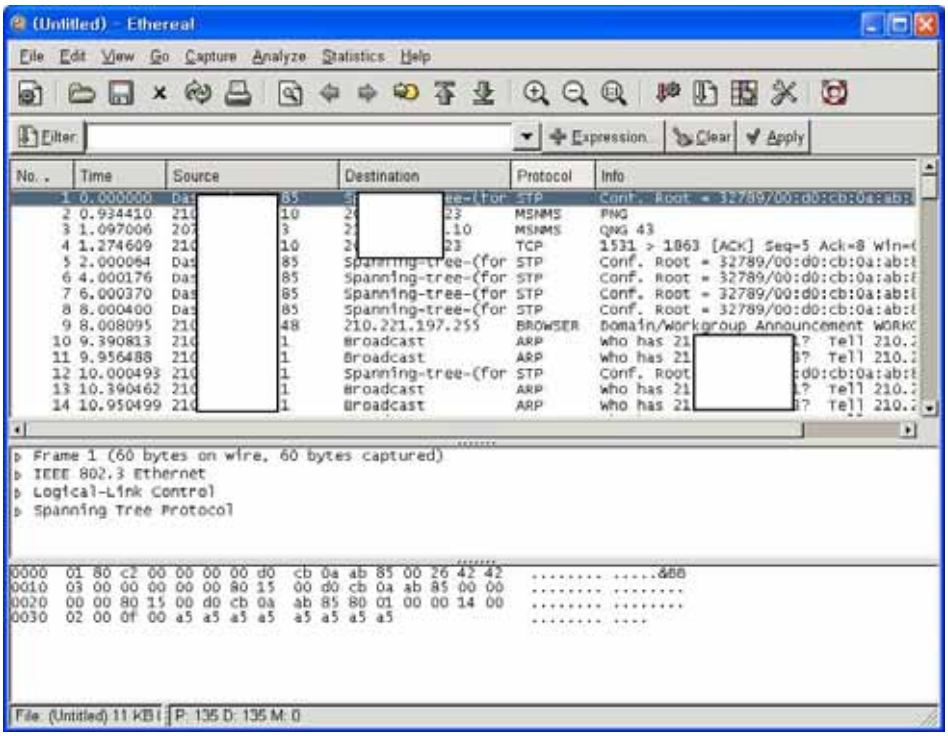


-. **Interface** : This field specifies the interface you want to capture on. You can only capture on one interface, and you can only capture on interfaces that Ethereal has found on the system.

While the capture is running, the following dialog box is shown:



This dialog box will inform you about the number of captured packets and the time since the capture was started.



5. Saving captured packets

You can save captured packets simply by using the Save As... menu item from the File menu under Ethereal.