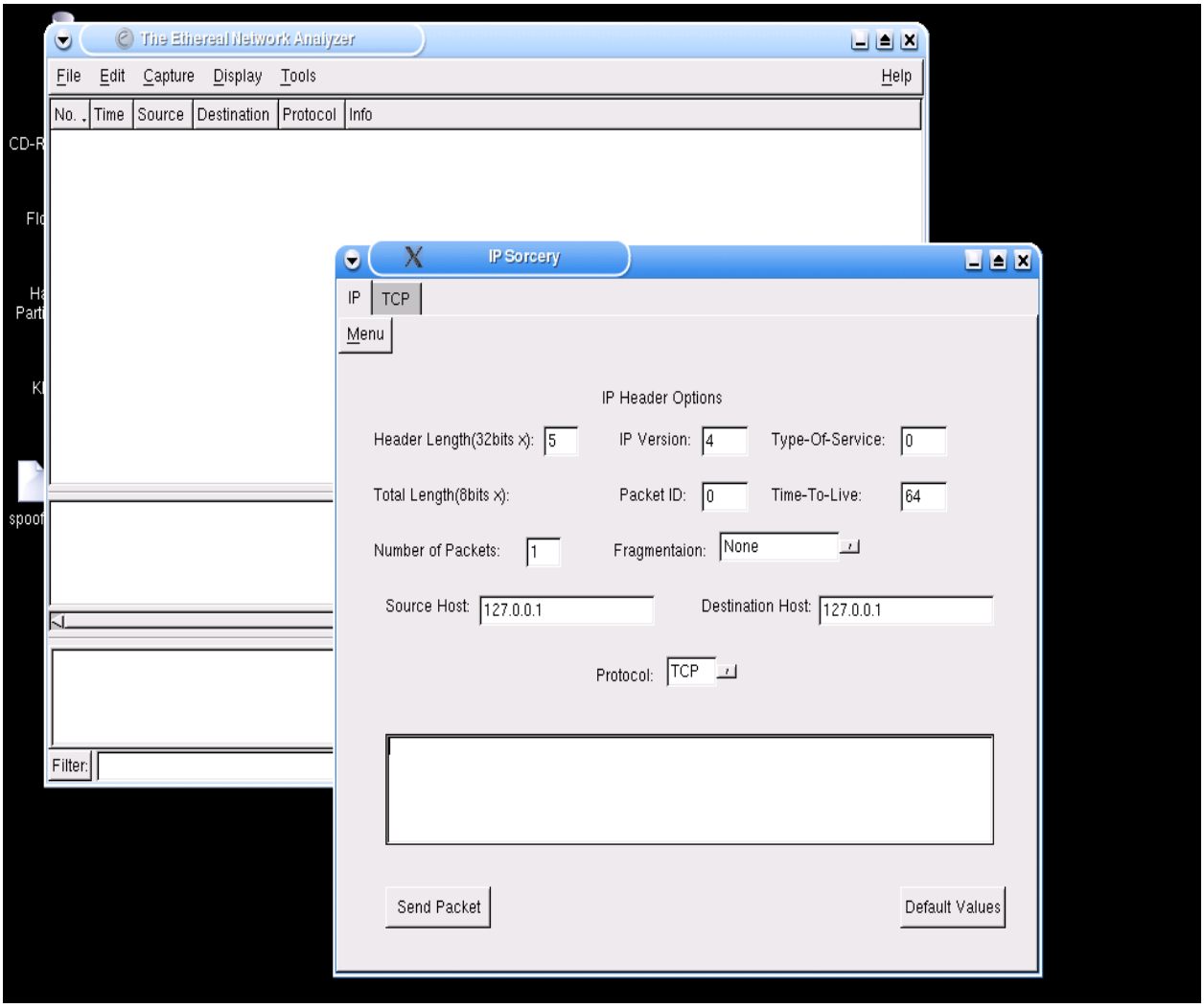
ADDRESS RESOLUTION PROTOCOL
2.2.1

SPOOFING IP ADDRESSES

(IP SORCERY)



Laboratory Overview

Objective

At the end of this lab students will be able to demonstrate how to spoof data packets using IPSorcery. These packets will be monitored as part of the network traffic using the Ethereal Network Analyzer.

Information for Laboratory

A. Students will be using the Knoppix Security Tools Distribution of the Linux Operating System.
B. Students will experiment with the available options of the IPSorcery Packet Injection application.
C. Students will observe spoofed traffic using the Ethereal Network Analyzer.

Student Preparation

The student will have completed requisite reading. The student will need two computers networked together or a partner student in order to facilitate completion of this lab. If neither is available to you, you will not be able to actually capture packets sent from another computer. But do each part of the lab separately on your computer so that you would know how to do it, even if the lab won't 'work' for you.

Student Preparation

Students must have a Knoppix-STD CD-ROM. Knoppix-STD includes both IPSorcery and Ethereal, the two security tools this lab will utilize.

NOTE:
Some systems require additional command line support. For example: a newer Dell System requires @boot command prompt:
knoppix login=root vga=normal xmodule=nv

More information on system specifics can be found at www.knoppix.net

Estimated Completion Time

30 Minutes

IP Address Spoofing

Spoofing is the art of injecting forged data packets onto a network. Attackers may utilize spoofing against target networks with the intention of creating a Denial Of Service (DOS) condition, or to exploit trust relationships between hosts.

IPSorcery

IPSorcery is packet generating device which can be used to inject TCP, UDP, ICMP, and IP packets onto a network. Packet Injection tools can be useful when troubleshooting network connections, and auditing your organization's firewalls.

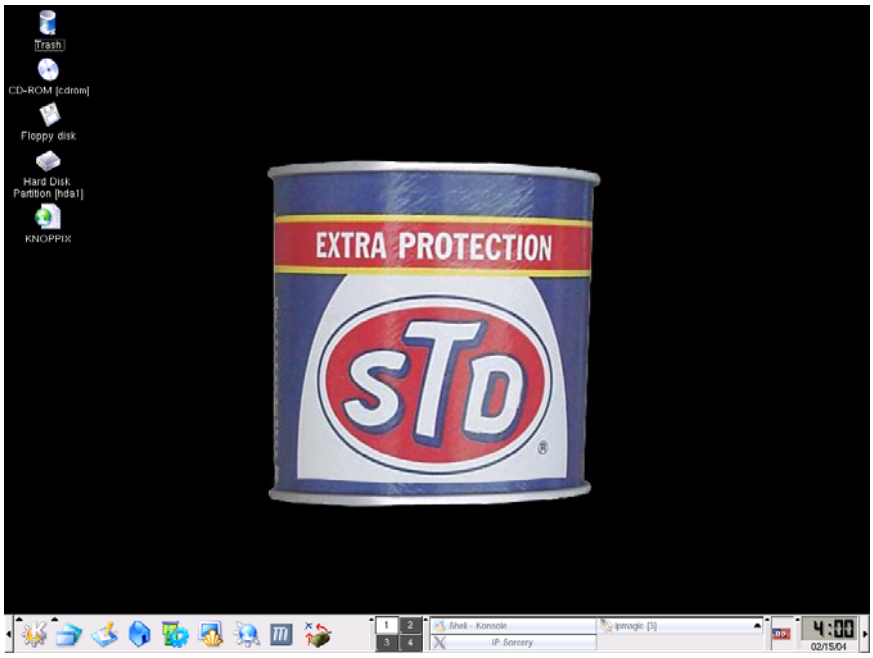
Ethereal

Ethereal is a network analyzer. This genre of security tool is often referred to as a packet sniffer. Ethereal can be used to monitor data packets as they traverse your network.

Step 1:

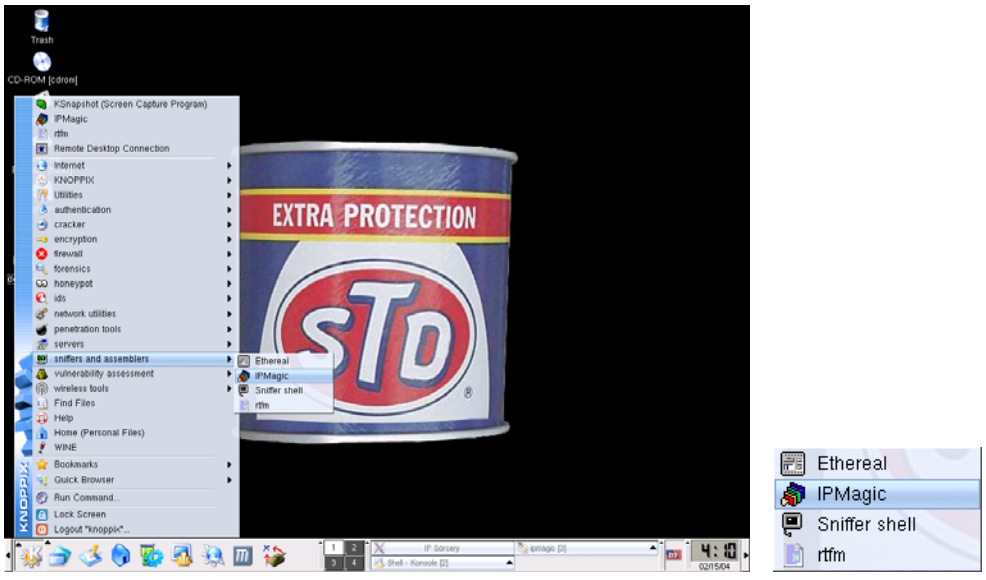
Insert the CD-ROM into the CD-ROM drive, and reboot your computer. Knoppix-STD is a bootable CD which contains many tools useful to the Information Security Professional. Knoppix-STD is based on the Linux Operating System.

After you have rebooted your machine, Knoppix-STD will automatically identify and configure your system's devices and drivers. After these steps have completed, an X-window session will start and you will be presented with a screen similar to the one below.

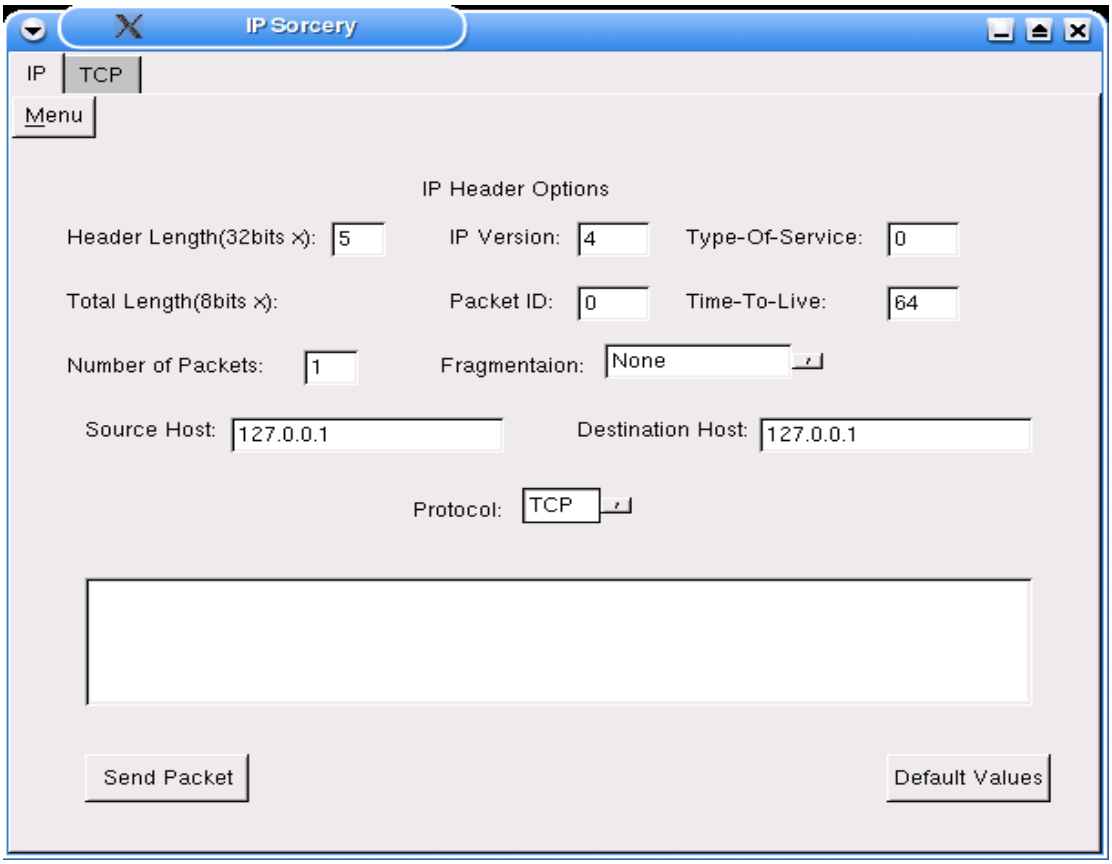


Step 2:

The next step is to launch the IPSorcery application. To do this click on the KDE (Start Button) on the Lower Left Side of your screen. Move your mouse up to the Sniffers and Assemblers section of the menu. Select the program entitled IPMagic.

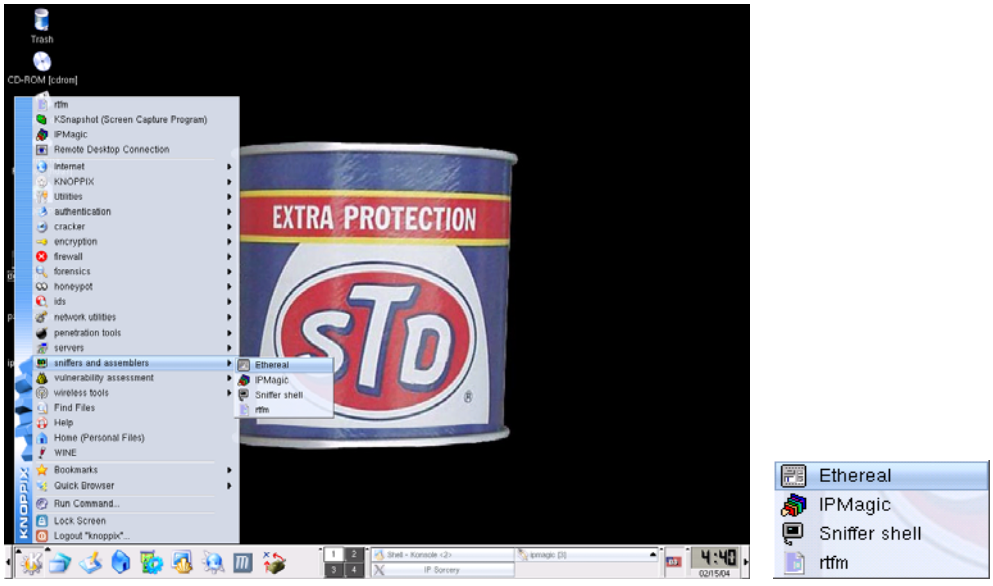


You will be presented with the following screen.

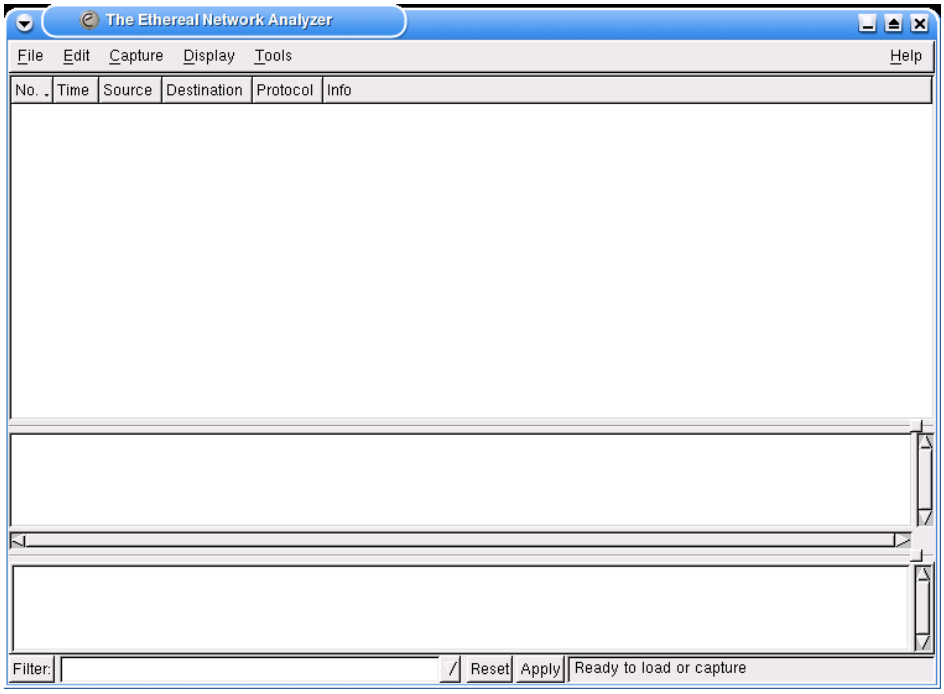


Step 3:

On your partner's machine launch the Ethereal Network Analyzer. Ethereal is located under the Sniffers and Assemblers menu.

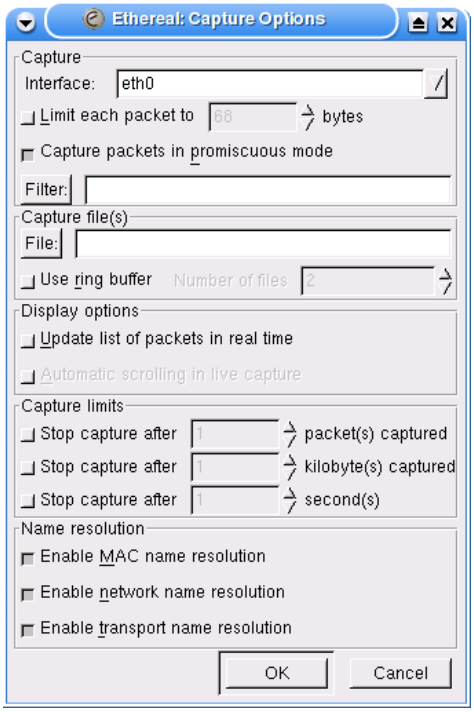


The following window should appear.

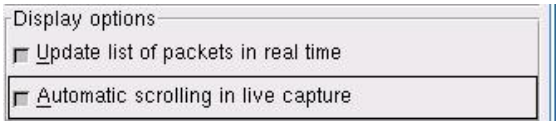


Step 4:

Click on the Capture tab of Ethereal, and then click on Start. You should see the following window appear.



In order to view the data packets in real time as they cross your network, you need to select the ‘Update list of packets in real time option’, and also the ‘Automatic scrolling in live capture’ option.



With the above buttons selected, **click on the OK button** at the bottom of the window.

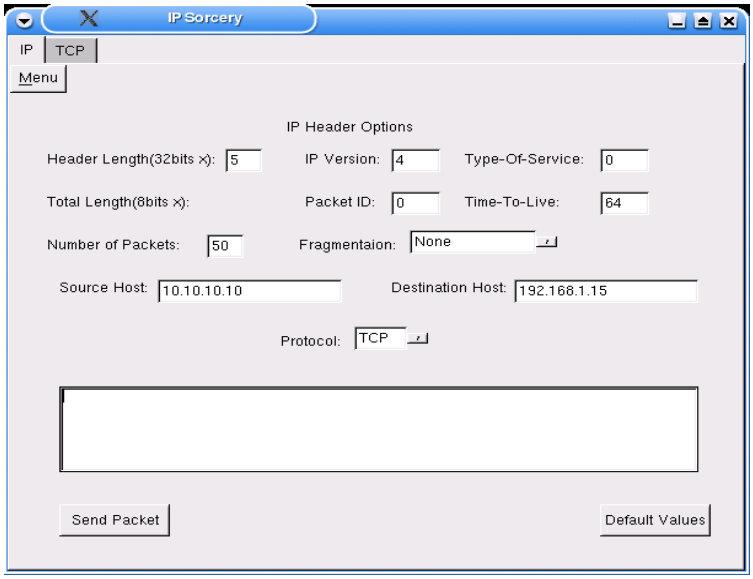
Step 5:

Using IPSorcery, assign your Source Host a spoofed IP address.
This is the address your forged packets will appear to have come from.
Next fill in the correct value in the Destination Host field. This is the IP address of the machine you will be sending spoofed packets to.

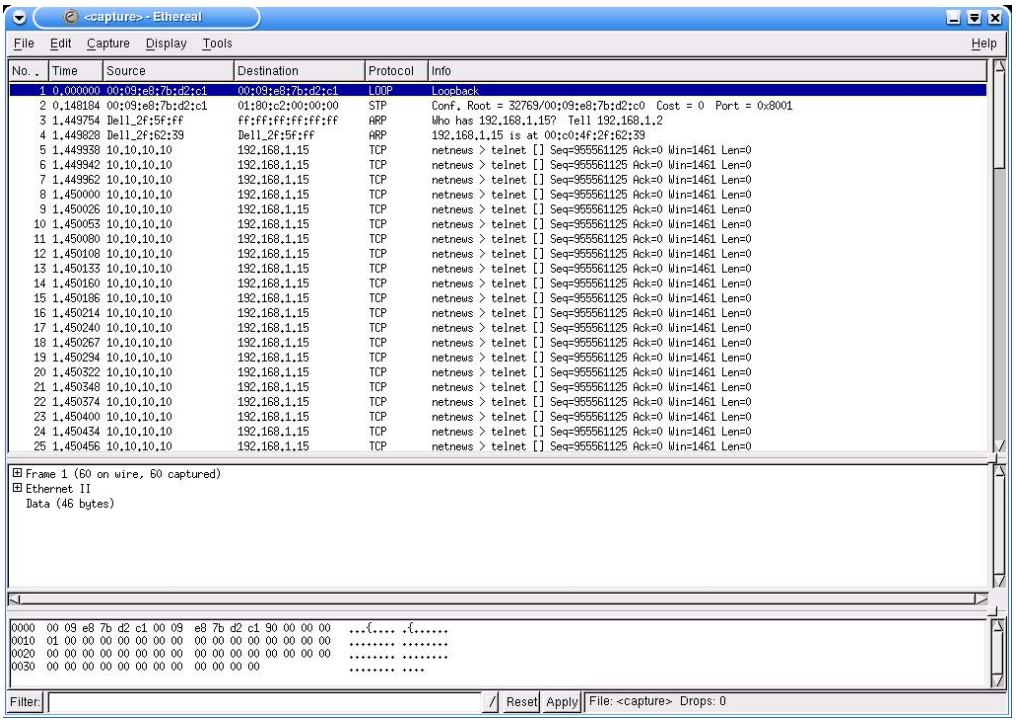
Additionally, you may find it useful to increase the Number of Packets option.

Step 6:

With the appropriate values filled in, click on the Send Packet option at the bottom of the screen.



You will immediately see the forged packets appear on the machine using Ethereal.



If You Want To Learn More

IP Spoofing, An Introduction
http://www.securityfocus.com/infocus/1674

IP Spoofing Demystified
http://www.phrack.org/show.php?p=48&a=14

Appendix

The latest version of Ethereal can be found at http://www.ethereal.com
IPSorcery can be found at http://www.legions.org/~phric/ipsorcery.html

The Operating System used for this lab is Linux Knoppix-STD. More information can be found at http://www.knoppix-std.org/