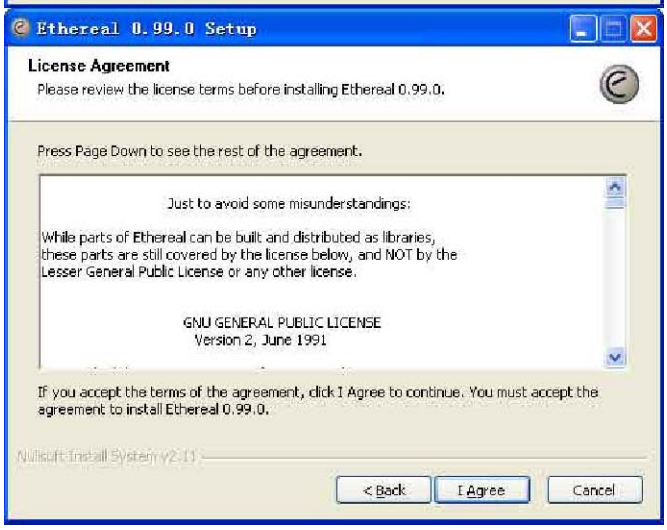
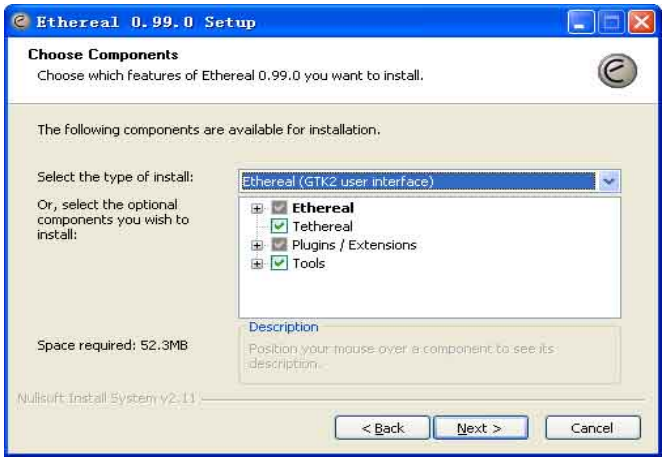
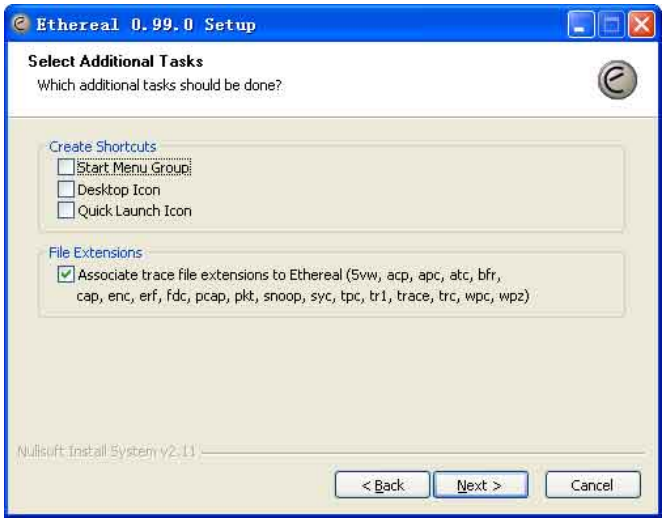
# Ethereal的安装

执行ethereal-setup-0.99.exe 即可。安装过程如下:

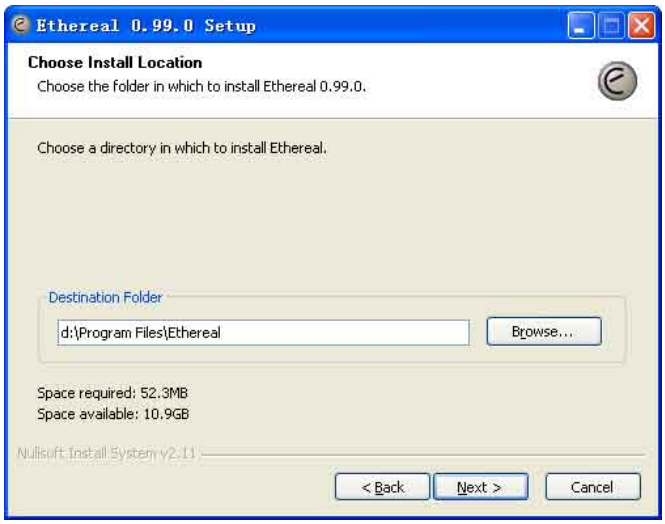




选择预安装的选件，一般选择默认即可

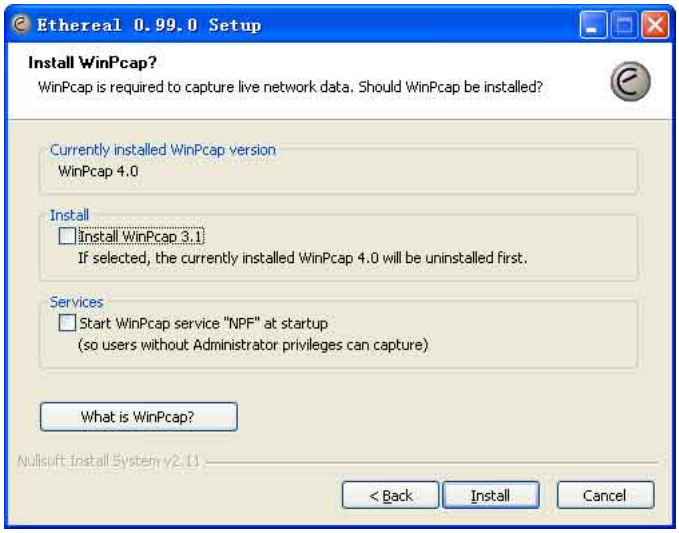





选择安装的目录



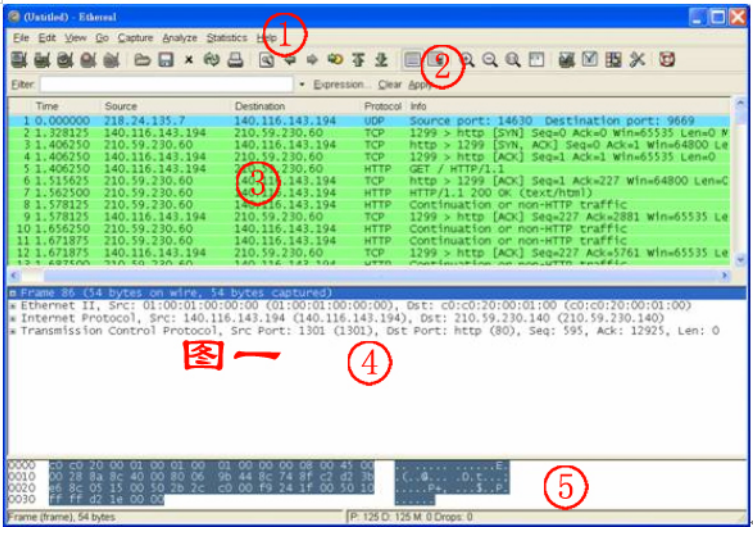

Ethereal 是透过WinPcap 来截取网络上的数据包。如果当前系统未安装WinPcap，钩选Install WinPcap 3.1项




安装完毕！

# Ethereal的基本使用

Ethereal的程序窗口：

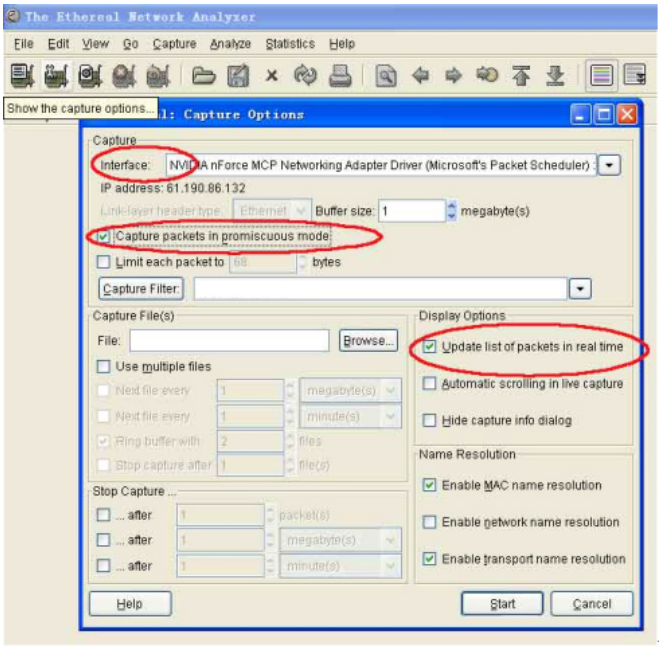


由上而下分别是

1) 菜单
2) 快捷工具栏
3) 俘获分组列表
4) 被高亮选中的分组首部明细
5) 以ASCII码和十六进制两种格式显示被俘获帧的完整内容。

一个完整的截取包过程：

1. 截取方式设置




点击快捷方式中的“show the capture options”进行适当设置，其中：

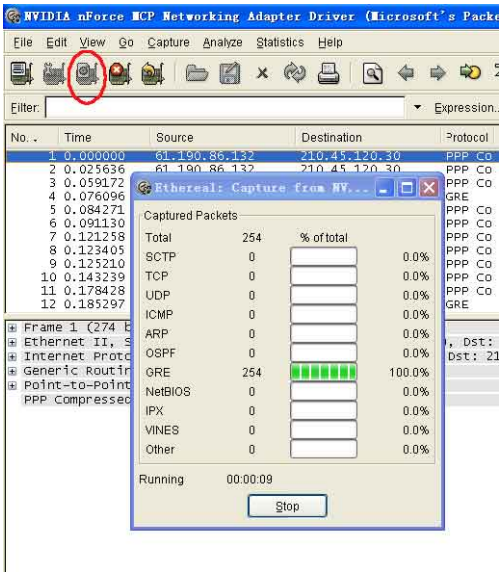
interface:选择本机网卡。

capture packets in promiscuous mode mode:是否打开混杂抓取模式。如果打开，抓取所有的数据包。如只需要监听本机收到、发出的包，则关闭这个选项。

Update list of packets in real time:实时显示抓取的分组列表。

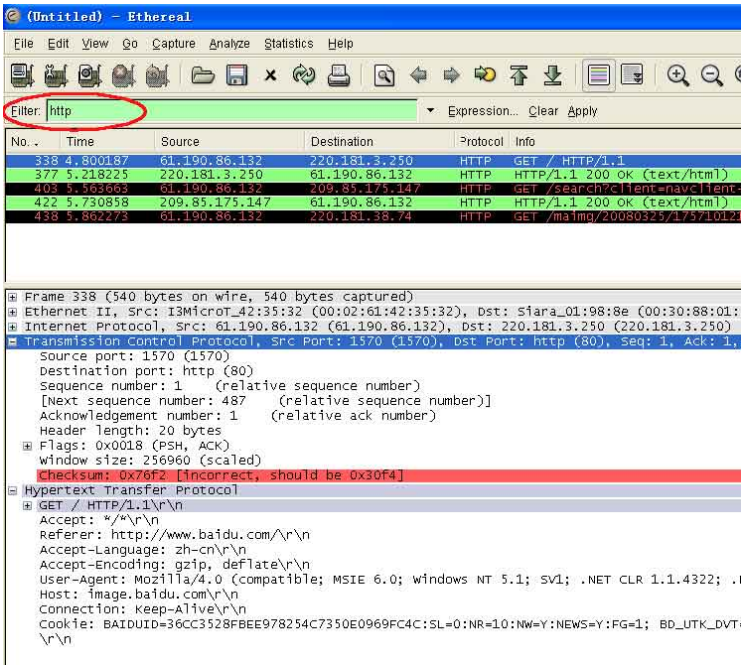
设置完毕后，点Start开始截取数据包。

2. 开始一个新截取



点击快捷方式中的“start a new live capture”开始截取数据包，此时可进行任意的网络连接行为（如通过IE访问一个网址），该窗口统计显示各类已俘获分组的数量。点击“stop”则停止截获。

3.利用filter筛选数据包




截包完毕后，在Filter中可输入筛选条件（书写过程中输入框背景为绿色时，表示筛选条件书写合法，红色则说明条件不合法），回车或选择“Apply”后对俘获分组列表进行筛选，筛选条件如：

http：选择http协议包，同样也可输入dns，ftp等

ip.src == 61.190.86.132：选择从61.190.86.132发出的数据包

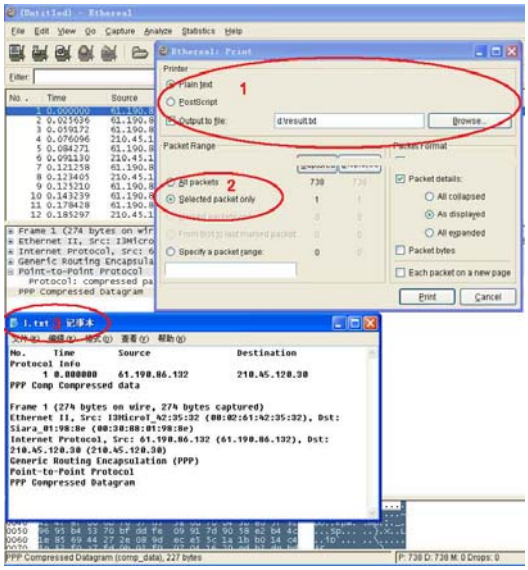
ip.dst == 61.190.86.132：选择发向61.190.86.132的数据包

ip.src == 61.190.86.132 and http：选择从61.190.86.132发出的http数据包

Ethereal筛选条件书写方式为类C，用==,!=,>,<,>=,<=限制条件，用and、or连接选择条件。点击输入框后的“Expression”可看到更多的条件选项。

4.两种方式保存数据包数据

方式一：保存“被高亮选中的数据包”




菜单file -> print 打开虚拟打印窗口。

按上图“1”处设置文件保存方式与保存地址(注意文件后缀应该写.txt，以方便查看)。

按上图“2”处选择需要的保存数据包。（选择“Selected packet only”则保存当前高亮选择的分组首部明细；选择“All packets”则保存所有截获的分组首部明细；选择“Specify a packets range”那么同时应在下方的输入框中输入一个数字串，如“1,10,20”，则保存截获的序号为1，10，20的分组首部明细）

点击“print”确认保存。

如上图“3”，可在指定目录下找到一个txt文件，其中保存了选定的分组首部明细。

注：这种保存方式可以称为“所见即所得方式”，即txt中保存的内容就是“图一”中第4部分所呈现的内容，所以为了得到完整的内容，需要在高亮选中一个分组的同时，右键点击第4部分，选择“expand all”，将信息树完全展开。

方式二：保存本次捕获所有数据包

菜单file->save，填写保存文件名，如packet080402.cap，注意要加“.cap”后缀。

这种方式将本次捕获所有数据包保存为一个.cap文件，通过菜单file->open可以打开.cap文件。

以上仅为Ethereal的基本使用，更多使用可查看 http://www.ethereal.com/ 或在网络上查询。