Ethereal使用入门

【责 编】：AcOol
【作 者】：AcOol整理
【出 处】：协议分析论坛
【字 体】：[小 大]
【时 间】：2005-12-14
【浏 览】：16419

ethereal可以用来从网络上抓包，并能对包进行分析。下面介绍windows下面ethereal 的使用方法。

一、安装

1、下载安装winpcap

http://coolersky.com/download/hacker/aidance/2005/0805/87.html

2、下载安装ethereal

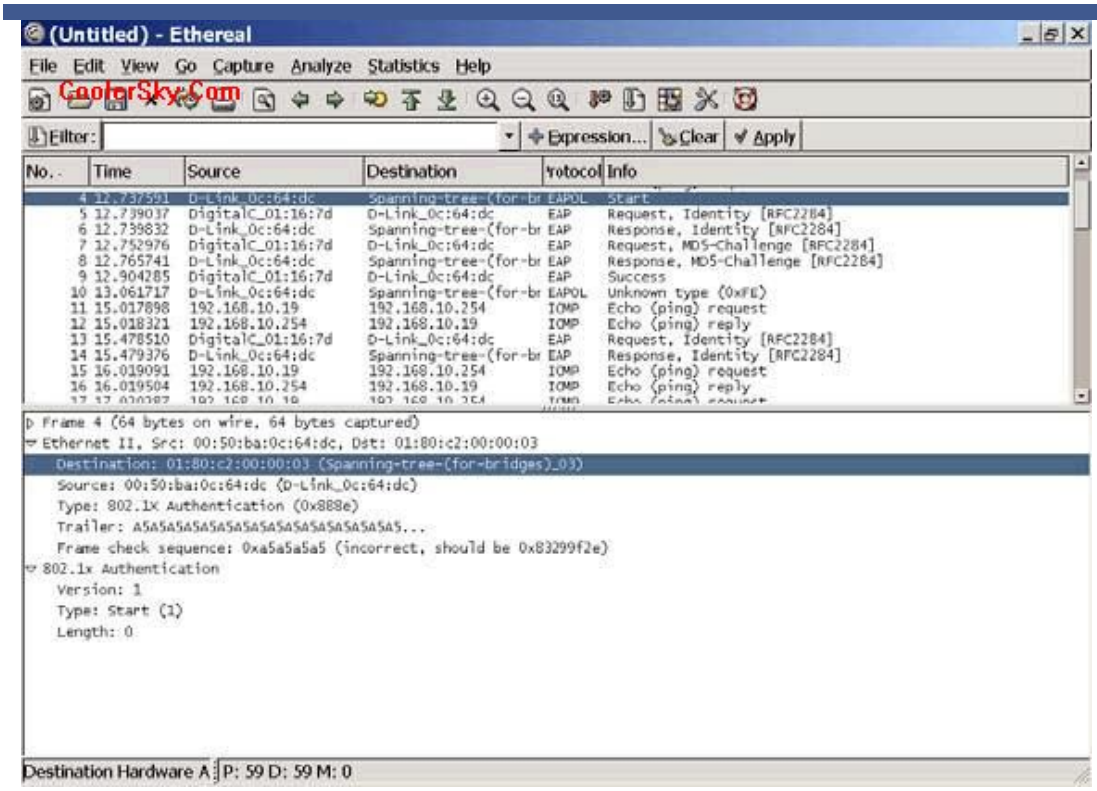
http://coolersky.com/download/hacker/sniffer/2005/1227/152.html

说明：新版本ethereal已经整合winpcap，下载ethereal即可完成安装。

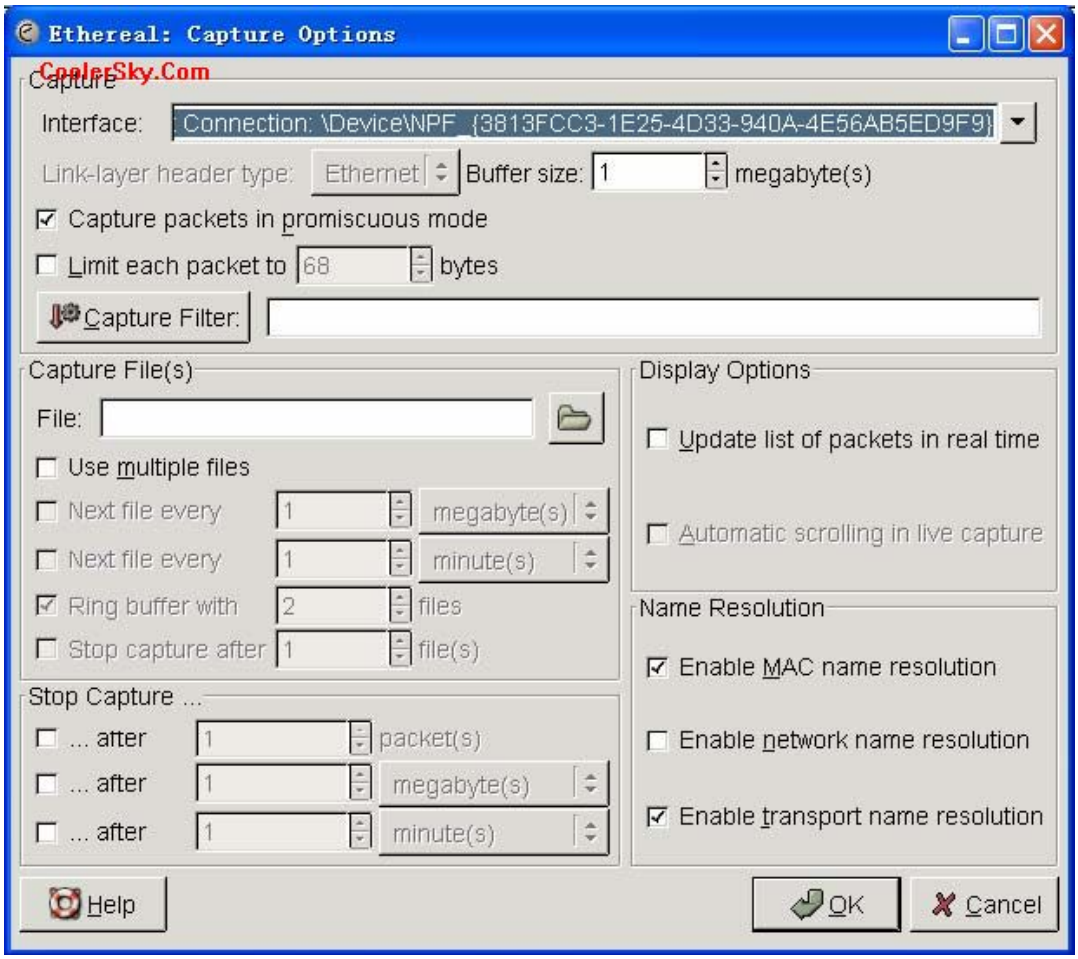
二、使用

启动ethereal以后，选择菜单Capature->Start，就OK了。当你不想抓的时候，按一下stop， 抓的包就会显示在面板中，并且已经分析好了。

下面是一个截图：



1、ethereal使用－capture选项



nterface：指定在哪个接口（网卡）上抓包。一般情况下都是单网卡，所以使用缺省的就可以了。

Limit each packet：限制每个包的大小，缺省情况不限制。

Capture packets in promiscuous mode：是否打开混杂模式。如果打开，抓取所有的数据包。一般情况下只需要监听本机收到或者发出的包，因此应该关闭这个选项。

Filter：过滤器。只抓取满足过滤规则的包（可暂时略过）。

File：如果需要将抓到的包写到文件中，在这里输入文件名称。

use ring buffer：是否使用循环缓冲。缺省情况下不使用，即一直抓包。注意，循环缓冲只有在写文件的时候才有效。如果使用了循环缓冲，还需要设置文件的数目，文件多大时回卷。

其他的项选择缺省的就可以了。

2、ethereal的抓包过滤器

抓包过滤器用来抓取感兴趣的包，用在抓包过程中。抓包过滤器使用的是libcap过滤器语言，在tcpdump的手册中有详细的解释，基本结构是：[not] primitive [and|or [not] primitive ...]

个人观点：如果你想抓取某些特定的数据包时，可以有以下两种方法，你可以任选一种，个人比较偏好第二种方式：

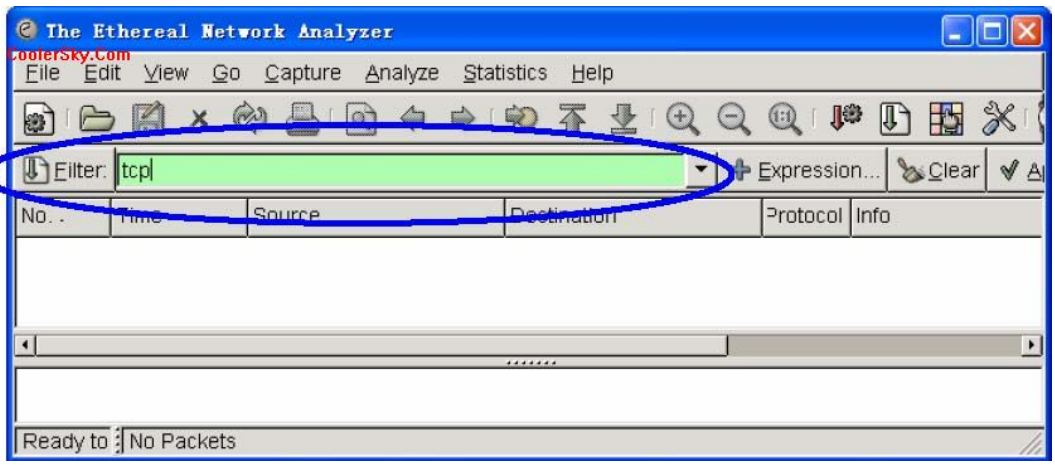
（1）在抓包的时候，就先定义好抓包过滤器，这样结果就是只抓到你设定好的那些类型的数据包；

（2）先不管三七二十一，把本机收到或者发出的包一股脑的抓下来，然后使用下节介绍的显示过滤器，只让Ethereal 显示那些你想要的那些类型的数据包；

3、etheral的显示过滤器（重点内容）

在抓包完成以后，显示过滤器可以用来找到你感兴趣的包，可以根据协议、是否存在某个域、域值、域值之间的比较来查找你感兴趣的包。

举个例子，如果你只想查看使用tcp协议的包，在ethereal窗口的左下角的Filter中输入tcp， 然后回车，ethereal就会只显示tcp 协议的包。如下图所示：



值比较表达式可以使用下面的操作符来构造显示过滤器自然语言类c 表示举例

eq ==

```
ip.addr==10.1.10.20
```

ne !=

```
ip.addr!=10.1.10.20
```

gt >

```
frame.pkt_len>10
```

lt <

```
lt < frame.pkt_len<10
```

ge >=

```
frame.pkt_len>=10
```

le <=

```
frame.pkt_len<=10
```

表达式组合可以使用下面的逻辑操作符将表达式组合起来自然语言类c 表示举例

and &&：逻辑与

```
ip.addr=10.1.10.20&&tcp.flag.fin
```

or ||：逻辑或

```
ip.addr=10.1.10.20||ip.addr=10.1.10.21
```

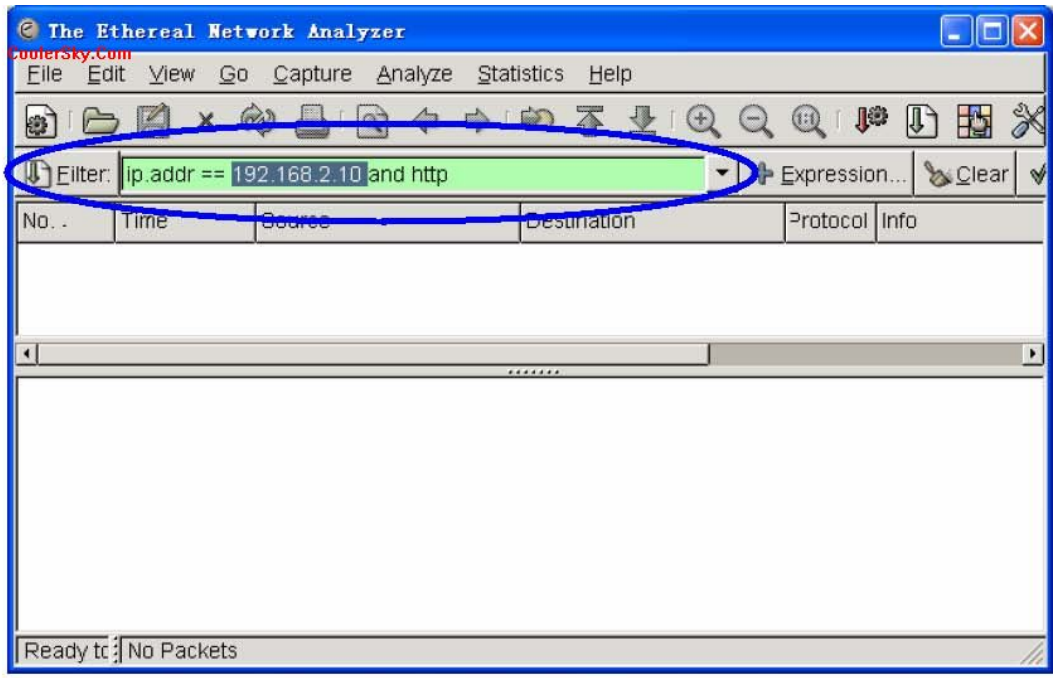
xor ^^：异或

```
tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == not
```

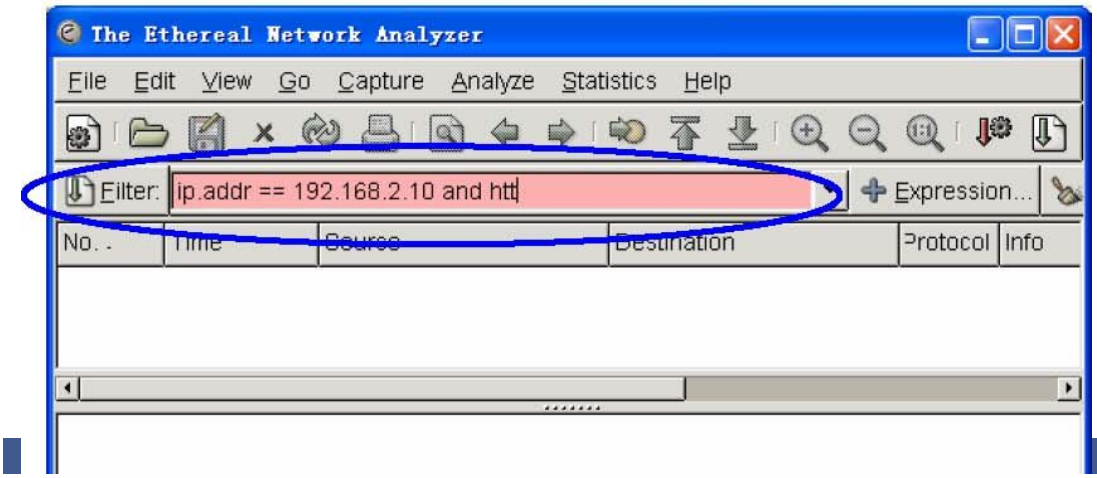
!：逻辑非

```
!llc
```

例如：我想抓取IP地址是192.168.2.10 的主机，它所接收收或发送的所有的HTTP报文，那么合适的显示Filter （过滤器）就是：



请记住一个诀窍：只好在 Filter 的背景是绿色，就证明你设定的 Filter 是合乎规定的，但是当背景是红色时，就说明你设定的 Filter 是 Ethereal 不允许的，是不对的。如：



4、在ethereal 使用协议插件

ethereal 能够支持许多协议，但有些协议需要安装插件以后才能解，比如H.323，以H.323 协议为例：

（1）首先下载ethereal 的H.323 插件，下载地址http://www.voice2sniff.org/

（2）下载完了以后将文件(h323.dll) 解压到ethereal 安装目录的plugin\0.9.x 目录下面，比如我的是0.9.11。

（3）进行一下设置

a、启动ethereal

b、菜单Edit->Preference

c、单击Protocols 前面的"+"号，展开Protocols

d、找到Q931 ，并单击

e、确保"Desegment.... TCP segments" 是选中的（即方框被按下去）

f、单击TCP

g、确保"Allow....TCP streams" 是选中的

h、确保没有选中"Check....TCP checksum" 和"Use....sequence numbers"

i、单击TPKT

j、确保"Desegment....TCP segments" 是选中的

k、点击Save，然后点击Apply ，然后点击OK

当然你也完全可以不断地重新安装新版本winpcap 和ethreal， 这样就可以不需在旧的ethreal 的版本中安装新的插件来支持新的协议插件，这也是懒人的一种做法。

+ 本站推荐 +

· ARP病毒问题的处理
· 千兆以太网技术综述
· 解析来自Autorun.inf文件的攻击
· 破解Windows XP组策略的“锁死
· Linux Kernel 2.6.13 <= 2.6.1

+ 相关文章 +

· 系统漏洞扫描之王——Nmap详解
· 三则黑客的Google搜索技巧简介
· Tcpdump 快速入门手册
· Ethereal协议分析系统介绍
· SuperScan3.0使用详解

+ 热点文章 +

打印本页 回到顶部 报告错误 关闭窗口

· 没有硝烟的战争：网络禁用与突
· “Worm.Win32.Viking.i”病毒分
· MSN登陆问题(MSN不能登陆的N种
· CnsMinKP.sys文件损坏导致系统
· Ethereal使用入门

+ 原创文章 +

· “Worm.Win32.Viking.i”病毒分
· 信息安全产业三部曲之“敦刻尔
· Dvbbs7.1 sp1 SQL版savepost.a
· 针对西京大学网站的一次安全性
· phpBB 2.0.12非法获取管理员权

关于站点 | 免责申明 | 版权隐私 | 业务合作 | 提供捐助 | 联系我们