IP网络工具使用

Andrew Huang< bluedrum@163.com>

课程内容:

- 网络检测软件
  - ping ,traceroute, netstat, route, ifconfig(Linux), ipconfig(Windows)
- 网络截包软件
  - tcpdump , Sniffer pro ,EtherPeek NX, Ethreal

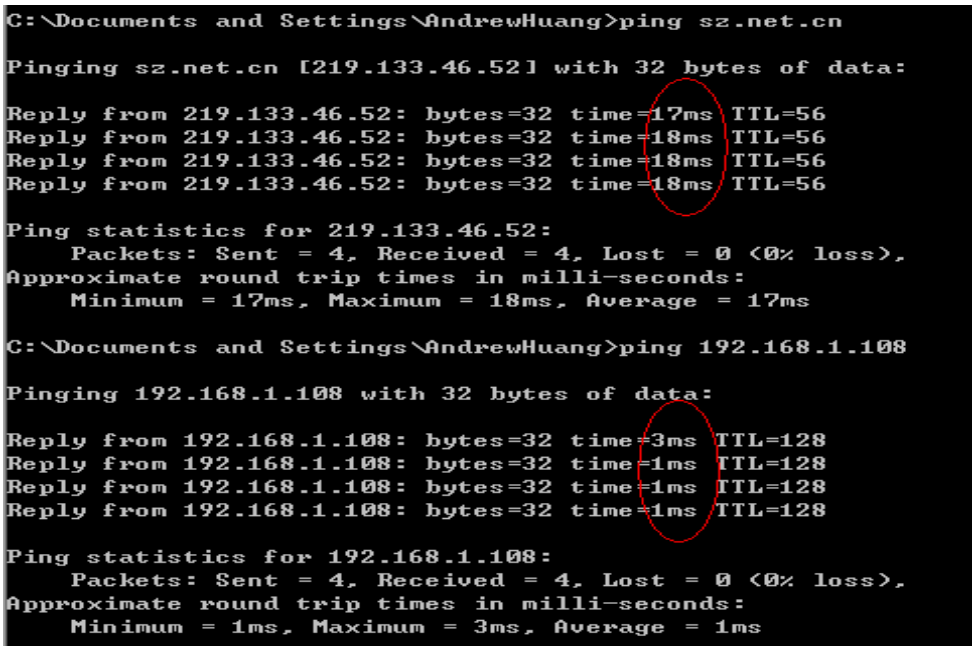
网络检测软件

ping

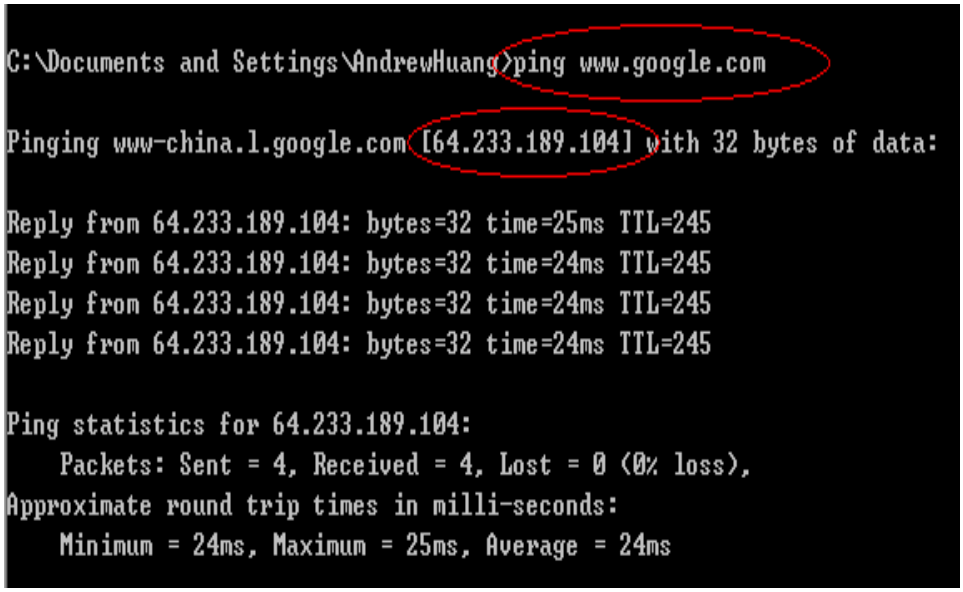
- 使用 ping可以测试计算机名和计算机的 ip 地址,验证与远程计算机的连接,通过将 icmp 回显数据包发送到计算机并侦听回显回复数据包来验证与一台或多台远程计算机的连接
- Ping的主要功能
  - 检测本机与被测主机之间网络是否相通
  - 检测本机与被测主机之间网络的网速
  - 测试域名解析(DNS)是否有效

- Linux ping 命令参数
  - Linux ping命令详解.htm
- Windows ping 命令参数
  - Windows ping命令详解.htm
- 测试是否连通

- 简单测试网速



- 测试域名解析是否有效



Tracert (Windows)

- 用于检测本机与某个站点之间路由的路径
  - 是否连接
  - 每一跳的速度,一跳指经过一个边界路由器

```
C:\Documents and Settings\AndrewHuang>tracert www.csdn.net

Tracing route to www.csdn.net [211.100.26.121]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13    51 ms    52 ms    51 ms  211.100.26.121

Trace complete.
```

Traceroute (Linux)

```
[root@TecherHost root]# traceroute 192.168.0.1
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 38 byte packets
 1  192.168.0.1 (192.168.0.1)  0.533 ms  0.198 ms  0.123 ms
[root@TecherHost root]#
```

netstat

- Netstat用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。
- 是一个检测网络状况极为有用的工具
- 使用 netstat 控制台命令来输出网络连接、路由表、接口统计、伪装连接和组播成员。
  netstat 具有多个命令行开关来控制其功能。下面是其中一些常用的开关：
  - netstat -p 显示每个套接字所属的程序的 PID 或名称
  - netstat -a 同时显示侦听和非侦听套接字
  - netstat -t 显示 TCP 连接
  - netstat -u 显示 UDP 连接
  - netstat -e 显示附加信息；使用这个选项两次，可以获得最详细的信息

ipconfig(Windows)

- ipconfig 显示网络基本信息
- ipconfig /all 显示网络详细信息
- ipconfig /release [adapter] 将指定网卡的上的DHCP信息清空,(即把IP地址失效)
  - ipconfig /release v* 把所有v打头的网卡IP信息清空
- ipconfig /renew [adapter] 重新向DHCP服务器申请IP地址
  - Ipconfig /renew v*

网络截包软件

网络截包软件

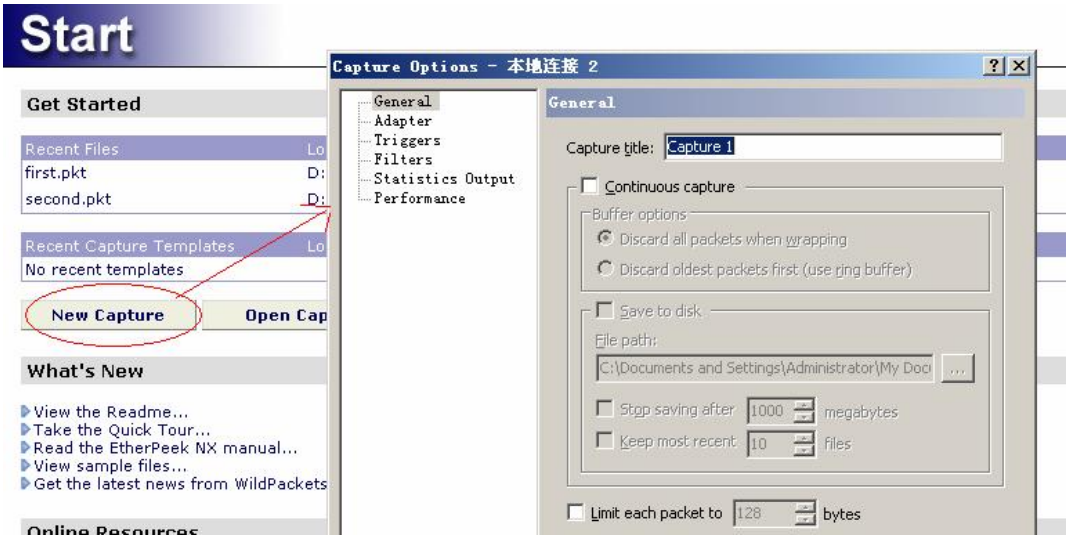
- 网络截包软件是分析协议,监控工具强有力的工具
- Windows 下截包软件
  - Sniffer pro
  - EtherPeek NX
  - Ethreal
- Linux 下截包软件
  - Ethreal for Linux
  - TCPDump

截包条件

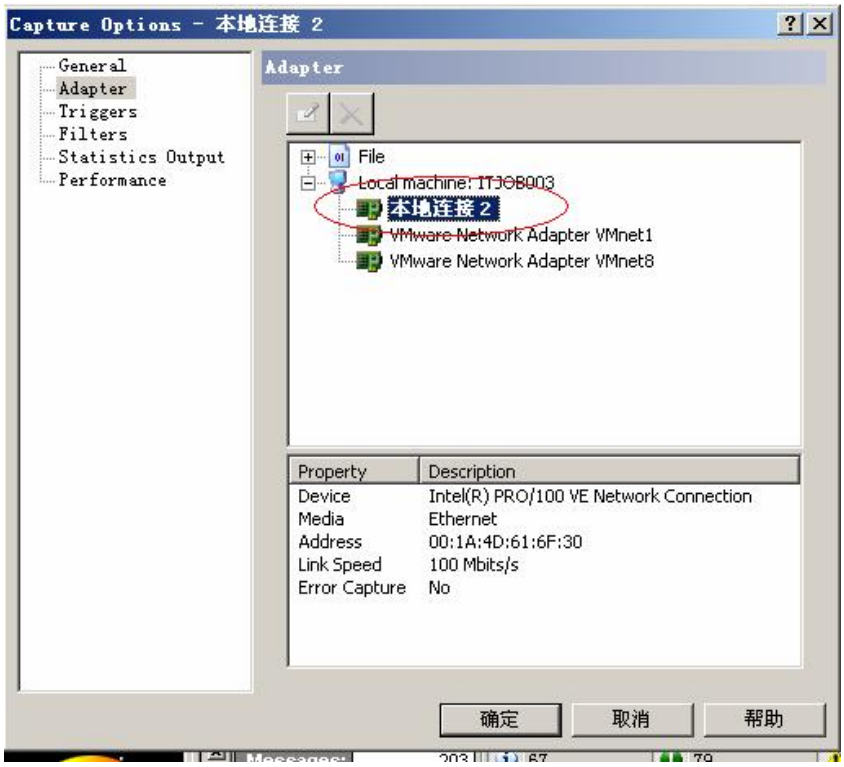
- 如果是发送和接本机的包,一般需要打开网卡的杂凑模式.
- 截包软件不能截取发往本机的包(如127.0.0.1)的包
- 如果截取不经过本身的包,需要交换设备具有包转发功能
  - 交换机的管理端口
  - HUB

EtherPeek NX使用指南

- 第一步:创建一个捕获

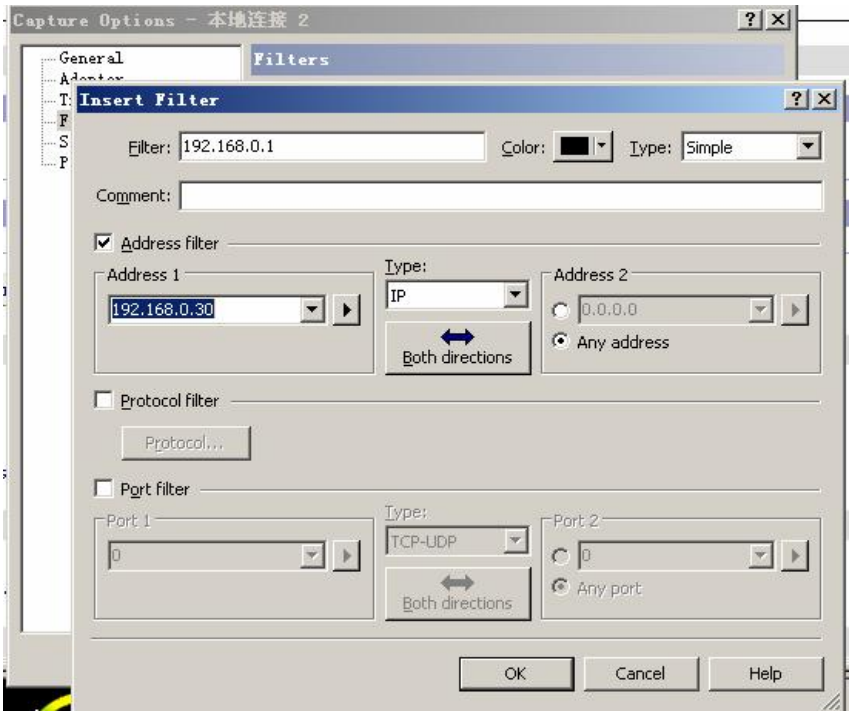


- 第二步,选择捕获的网卡



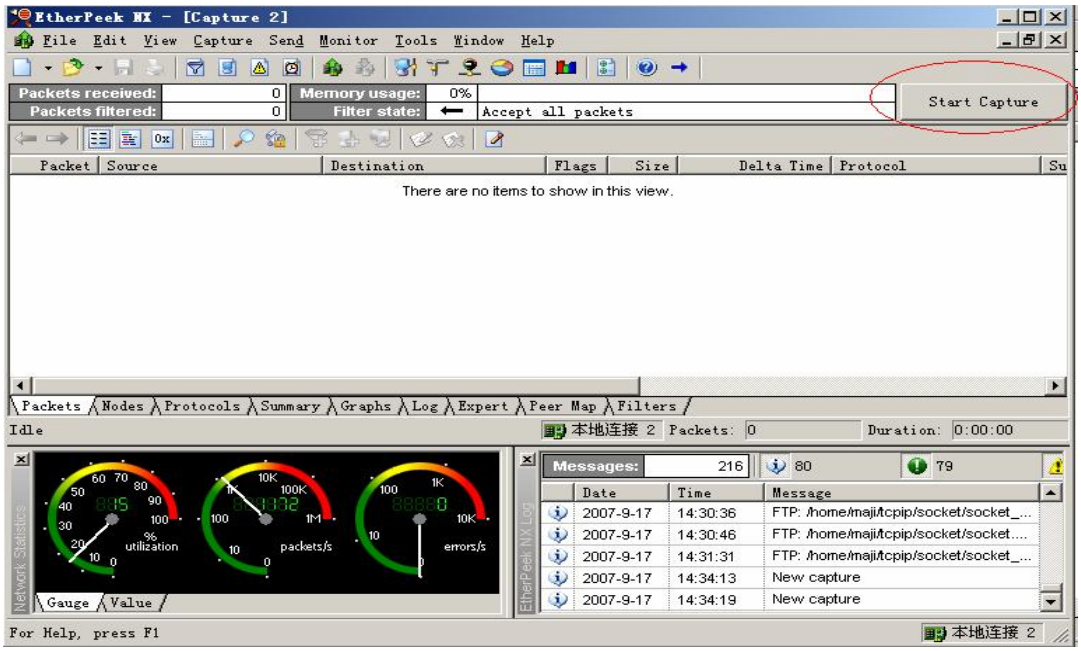
- 第三步,选择捕获的协议

- 第四步,可以针对特殊条件进行捕获

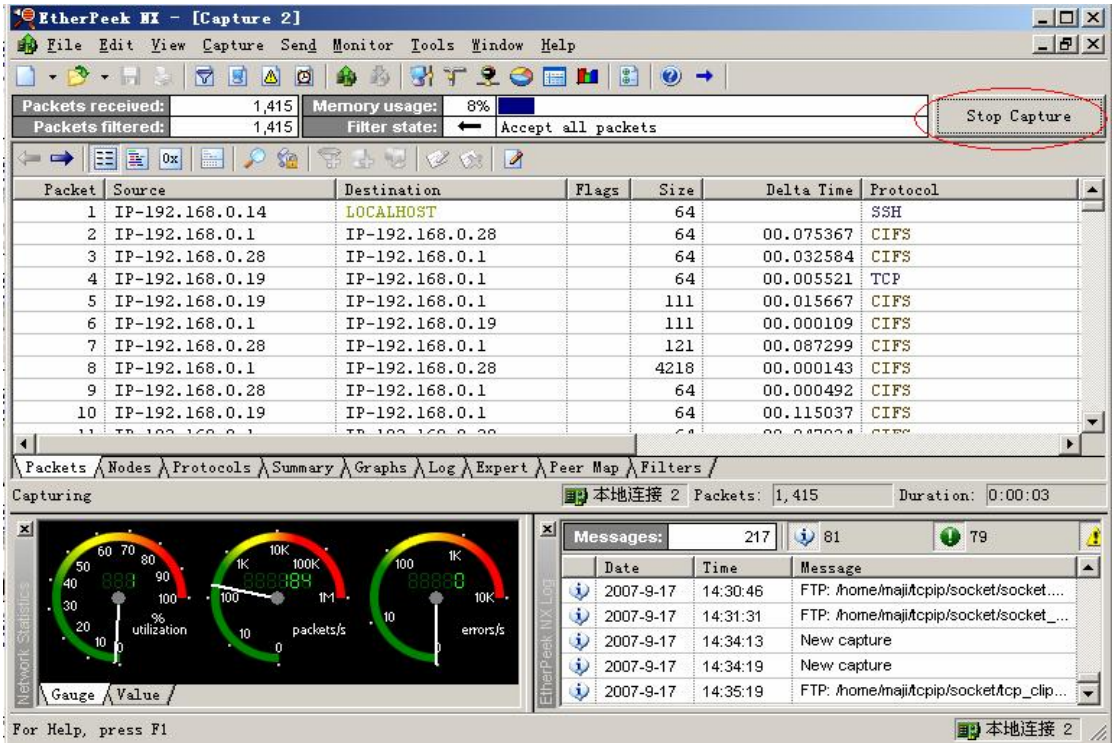


– 在捕获协议的右键菜单选择Insert
– 过滤条件
  - 针对IP
  - Port
  - Mac 地址

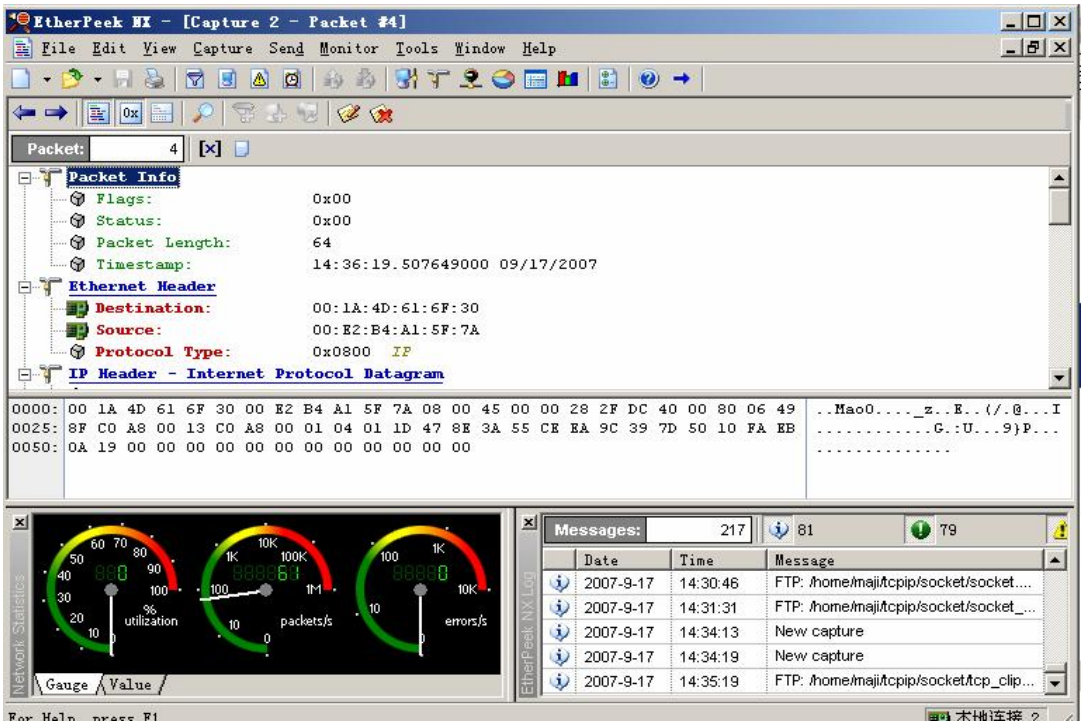
- 第五步,按start 开始捕获



- 第六步, 捕获结束后,按stop 停止,进行保存或分析

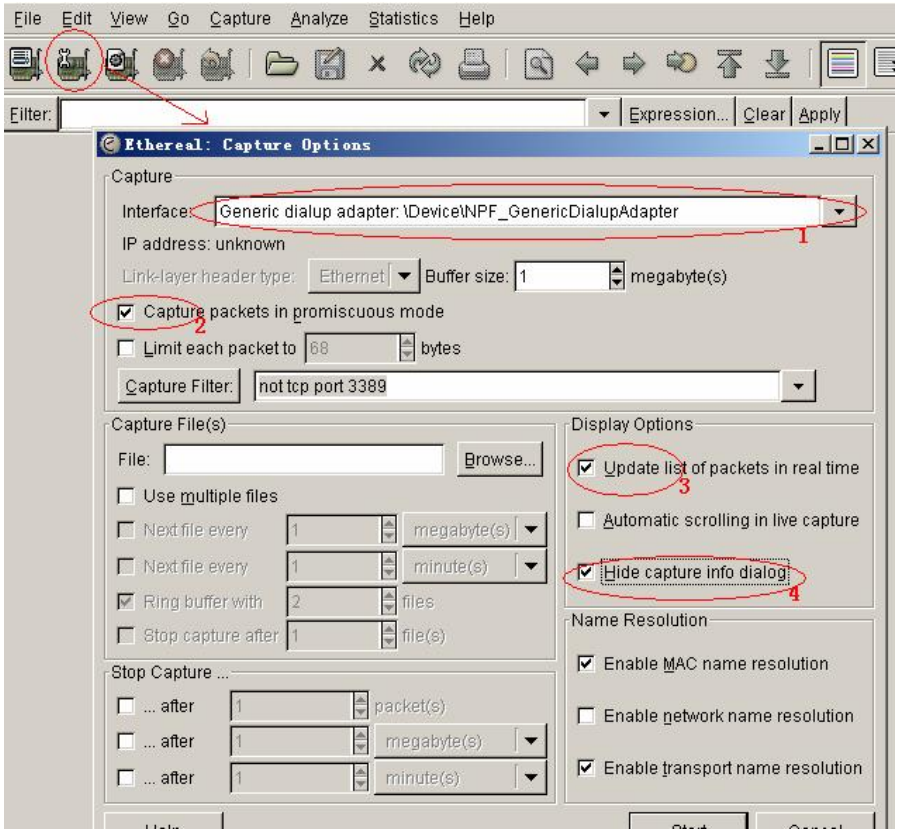


- 第七步:双击后对包进行分析



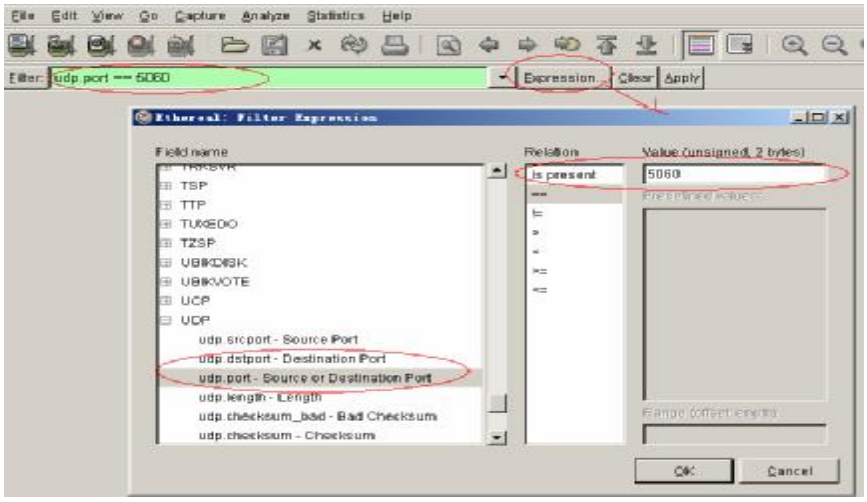
ethereal 快速使用手册

- 抓包前的设置工作

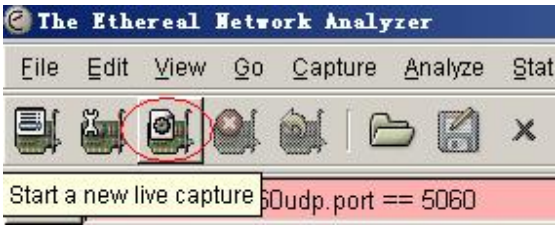


- 1.选择捕获的网卡
- 2.选择杂凑模式,(不选只能抓本机收发的包)
- 3.选择抓包进可以实时更新列表
- 4.选择抓包时不显示信息窗口

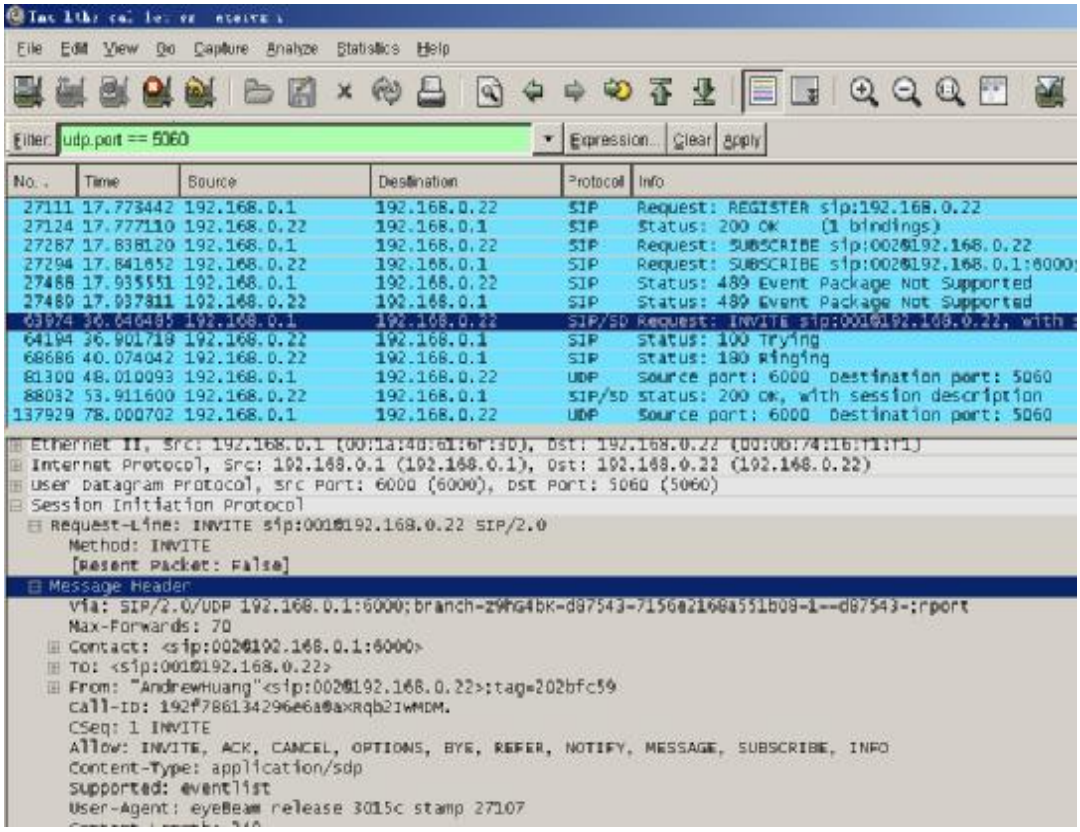
- 设置抓包的过滤模式



- Ethereal 支持强大的表达式(Expression)过滤.并支持复合表达式

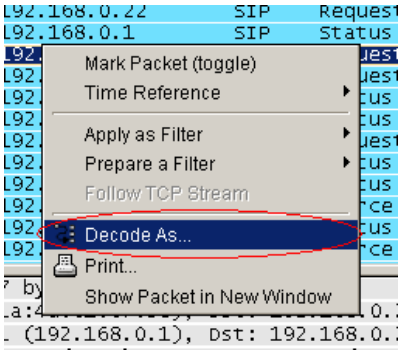
- Ethereal可以在表达式窗直接输入表达式,
- 也能用Filter Expression窗口对某一协议某一参数进行设置
  - 前图即是捕获**UDP**收发端口为**5060**的包**,**即**SIP**包
  - 

- 按捕获设置窗口(Caption Optins)中start按钮,或工具条的star按钮,即可开始抓包工作对SIP的捕获结果



Ethereal增强功能

- 1直接打开EtherPeek 的捕获文件
- 2.可以将非标准端口的包强行作为某一些协议进行解析
  - EtherPeek通常只对标准端口进行协议解析,如只把5060端口的包作为SIP协议解析,但如果采用5080端口则无法解析.在实际开发中,大量用到非标准端口,这样非常不方便
  - Ethereal支持强制解析功能,如上例,只要在5080的包上选择”Decode As…”后选择解析协议即可



TCPDump

- TCPDump 是一个Linux 字符界的捕获包工具
- 直接在shell 下运行tcpdump 即可运行捕获包
- Tcpdump 有较多的参数进行捕获.
  - -a 将网络地址和广播地址转变成名字；
  - -d 将匹配信息包的代码以人们能够理解的汇编格式给出；
  - -dd 将匹配信息包的代码以c语言程序段的格式给出；
  - -ddd 将匹配信息包的代码以十进制的形式给出；
  - -e 在输出行打印出数据链路层的头部信息；
  - -f 将外部的Internet地址以数字的形式打印出来；
  - -l 使标准输出变为缓冲行形式；
  - -n 不把网络地址转换成名字；
  - -t 在输出的每一行不打印时间戳；
  - -v 输出一个稍微详细的信息，例如在ip包中可以包括ttl和服务类型的信息；
  - -vv 输出详细的报文信息；
  - -c 在收到指定的包的数目后，tcpdump就会停止；
  - -F 从指定的文件中读取表达式,忽略其它的表达式；
  - -i 指定监听的网络接口；
  - -r 从指定的文件中读取包(这些包一般通过-w选项产生)；
  - -w 直接将包写入文件中，并不分析和打印出来；
  - -T 将监听到的包直接解释为指定的类型的报文，常见的类型有rpc（远程过程调用）和snmp（简单网络管理协议；）
- tcpdump 支持正则表达式捕获.可以设置复杂的表达式进行捕获.
- 第一类参数host，net，port
  - tcpdump host 210.27.48.1
    - 捕获所有经过ip地址210.27.48.1的包
  - tcpdump net 202.0.0.0
    - 捕获所有是子网202.0.0.0的包
  - tcpdum port 23
    - 捕获所有经过端口23的包
- 第二类指定传输方向的参数, src , dst ,dst or src, dst and src 与第一类配合使用
  - tcpdump src 192.168.0.30 捕获源地址为192.168.0.30的IP包
  - Tcpdump dst net 202.0.0.0 捕获目标网络为 202.0.0.0的包

- 缺省是dst or src 两者均可的意思
- 第三种是协议的关键字,主要包括**fddi,ip ,arp,rarp,tcp,udp**等类型
- 一些逻辑处理符,and (并且) or(或者) !(否)
  - tcpdump host 210.27.48.1 and \ (210.27.48.2 or 210.27.48.3 \)
    - 想要截获主机210.27.48.1 和主机210.27.48.2 或210.27.48.3的捕获,(,)需要\来打头
  - tcpdump ip host 210.27.48.1 and ! 210.27.48.2
    - 如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包
  - tcpdump tcp port 23 host 210.27.48.1
    - 如果想要获取主机210.27.48.1接收或发出的telnet包
- Tcpdump常用参数
  - Tcpdump –w dump.txt 把结果输出到dump.txt中
  - Tcpdump –e 输出以太网信息.
  - Tcpdump –c 200 捕获200个包后停止
  - Tcpdump –i eth0 只捕获流经eth0网卡上的包
- 非root用户使用tcpdump需要使用sudo命令,临时采用root权限
  - sudo /usr/sbin/tcpdump
  - 然后输出自己的密码,即可运行
  - 要实现这一功能,需要root编辑/etc/sudoers 把tcpdump权限发布给指定组
    - %student ALL=/usr/sbin/tcpdump

课堂练习

- 请使用etherPeek NX,捕获如下协议,并保存下来分析,用参考文档对比观察协议的组成
  - 运行一个FTP命令捕获FTP协议
  - 可运行一个BOA程序,捕获HTTP协议
  - 运行PUTTY 观察,SSH协议的使用
  - 用SMBA访问一个Linux主机,捕获Smba的协议
  - 运行ping命令,捕获ICMP协议
  - 在Windows运行3Deamon,在Linux下运行tftp 捕获TFTP协议
  - 如有ARM板,可运行mount –o nolock 192.168.0.146:/home/nfs /mnt 观察NFS协议的
  - 用ipconfig /release 和 ipconfig/renew 来捕获DHCP的协议