

## 使用 Ethereal 软件分析 IP 流

硬件要求：奔腾 II 300 以上电脑配置 10M 以上网卡；  
10MBase/T 集线器（HUB），不能使用 10/100 交换机，交换机是 2 层交换，口和口之间不广播。

## 一、下载软件

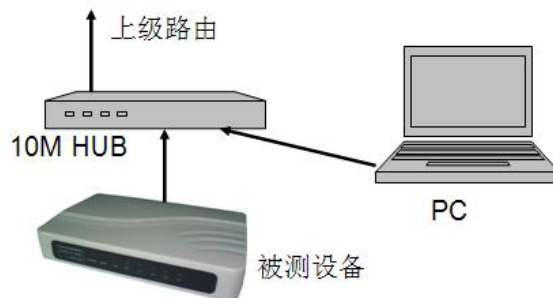
按这个连接，下载官方发布的 Ethereal 安装程序

<http://www.ethereal.com/distribution/win32/ethereal-setup-0.99.0.exe>

下载完毕以后直接运行，安装程序。

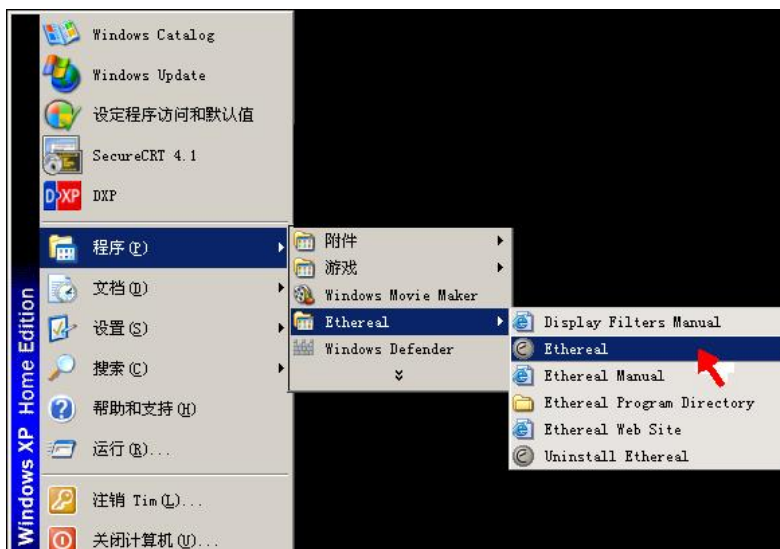
## 二、连接

以下是连接方式



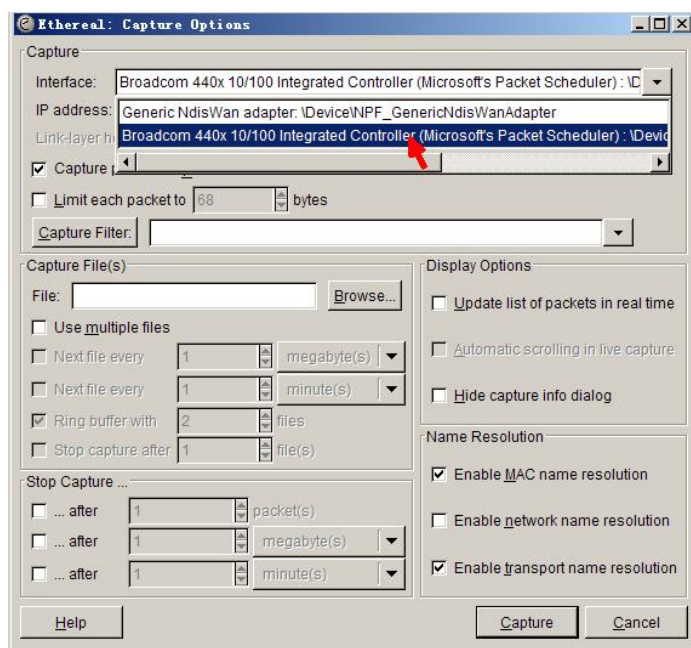
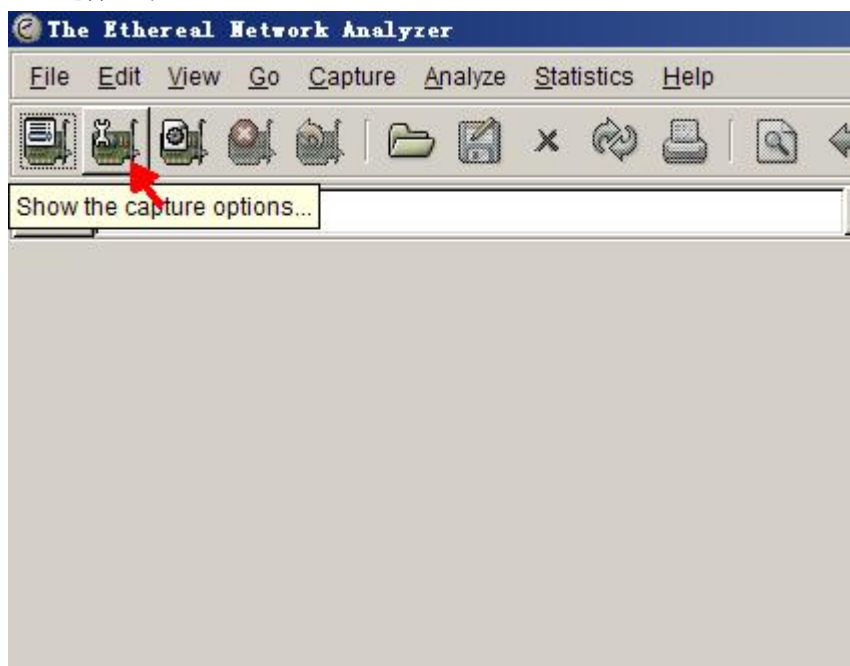
## 三、运行程序

在程序组里运行 Ethereal



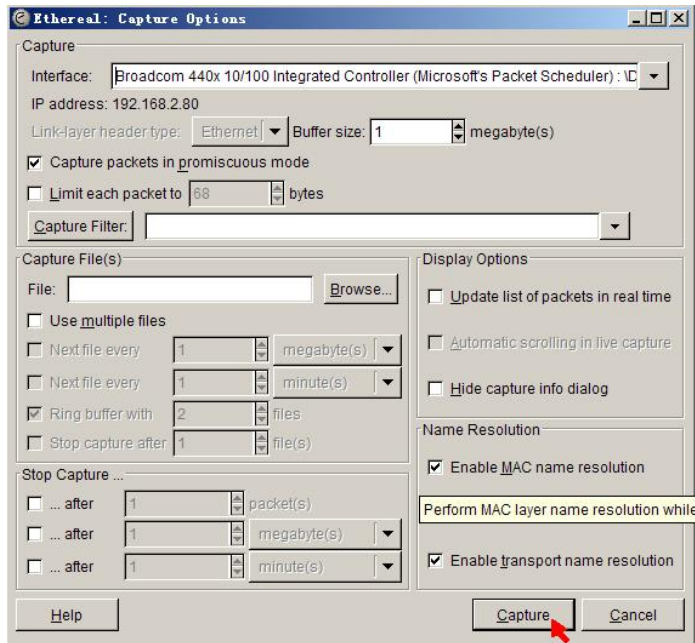
#### 四、开始抓包

##### 1、选择网卡

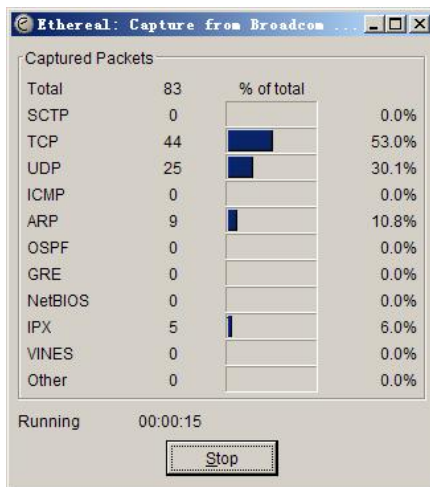


按 Interface 选项右面的下选按键，选择您电脑上安装的网卡型号

## 2、开始



按 Capture 按键开始 IP 包的捕获开始了：



注意，分析网络包要先开始“捕获”再进行网络动作。例如 IP 电话得分析就要先开始捕获然后发起呼叫（打电话），直到接通就可以停止捕获了。如果需要分析断线等情况，就要从开始呼叫到断线全程捕获。

## 3、停止：按 Stop 键停止捕获

### 五、分析

停止捕获以后软件会进行自动分析，其内容解析入下：

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.217	220.246.4.210	UDP	Source port: 21514 Destination
2	0.576854	192.168.2.210	192.168.2.255	NBNS	Name query NB D91TQP1X<20>
3	0.576920	192.168.2.80	Broadcast	ARP	who has 192.168.2.210? Tell
4	0.577225	192.168.2.210	192.168.2.80	ARP	192.168.2.210 is at 00:0a:eb:
5	0.577230	192.168.2.80	192.168.2.210	NBNS	Name query response NB 192.16
6	0.577751	192.168.2.210	192.168.2.80	TCP	1187 > netbios-ssn [SYN] Seq=
7	0.577784	192.168.2.80	192.168.2.210	TCP	netbios-ssn > 1187 [SYN, ACK]
8	0.578203	192.168.2.210	192.168.2.80	NBSS	Session request, to D91TQP1X<
9	0.578236	192.168.2.80	192.168.2.210	NBSS	Positive session response
10	0.578893	192.168.2.210	192.168.2.80	SMB	Negotiate Protocol Request
11	0.582923	192.168.2.80	192.168.2.210	SMB	Negotiate Protocol Response
12	0.584253	192.168.2.210	192.168.2.80	SMB	Session Setup AndX Request, N
13	0.584415	192.168.2.80	192.168.2.210	SMB	Session Setup AndX Response, N
14	0.585729	192.168.2.210	192.168.2.80	SMB	Session Setup AndX Request, N
15	0.588579	192.168.2.80	192.168.2.210	SMB	Session Setup AndX Response
16	0.589302	192.168.2.210	192.168.2.80	SMB	Tree Connect AndX Request, Pa
17	0.589368	192.168.2.80	192.168.2.210	SMB	Tree Connect AndX Response
18	0.590044	192.168.2.210	192.168.2.80	LANMAN	NetServerEnum2 Request, works
19	0.590284	192.168.2.80	192.168.2.210	LANMAN	NetServerEnum2 Response

选定包的十六进制码

```

0000 00 11 43 75 be 58 00 0a eb 23 cb 75 08 06 00 01 ..Cu.X...#.u....
0010 08 00 06 04 00 02 00 0a eb 23 cb 75 c0 a8 02 d2 .....#.u....
0020 00 11 43 75 be 58 c0 a8 02 50 00 00 00 00 00 00 ..Cu.X...P.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

No. → 包的序列号      Time → 时间顺序      Source → 源地址  
 Destination → 目标地址      Protocol → 应用协议      Info → 包内文描述

### 六、IP 流存档

当你所捕获的 IP 流需要备份或交给其他人分析就要先把 IP 流进行存档，操作如下：

按保存键：

No. .	Time	Source	Destination
1	0.000000	192.168.2.217	220.246.4.210
2	0.576854	192.168.2.210	192.168.2.255
3	0.576920	192.168.2.80	Broadcast
4	0.577225	192.168.2.210	192.168.2.80
5	0.577230	192.168.2.80	192.168.2.210
6	0.577751	192.168.2.210	192.168.2.80
7	0.577784	192.168.2.80	192.168.2.210

填写文件名，选择保存目录以后按“Save”键完成保存

