利用协议分析工具 SNIFF PRO学习 TCP/IP

一、前言

曾写过《用协议分析工具学习 TCP/IP》一文，有幸受到一些人的关注，该文中用的工具是 Iris，其实 Sniffer Pro是非常优秀的协议分析软件，许多下载网站说它是最好的网络协议分析软件。做为一名合格的网管肯定需要有这么一套好的网络协议分析软件，它对分析网络故障等极为有用。 Sniffer Pro同时又是非常优秀的嗅探器，也就是说它可以捕捉到网络中其它机器的帐号和密码。本文介绍它的基本功能和用几个例子来演示捕捉密码的过程，也算是对学习 TCP/IP的一些补充。介绍嗅探（Sniffer）原理的文章非常多，本文就不啰嗦了。

二、运行环境及安装

Sniffer Pro可运行在局域网的任何一台机器上，如果是练习使用，网络连接最好用 Hub且在一个子网，这样能抓到连到 Hub上每台机器传输的包。

本文用的版本是 4.6，Sniffer Pro软件的获取可在 www.baidu.com或 www.google.com中输入 Sniffer Pro 4.6，查找相应的下载站点来下载。 该版本是不要序列号的。

安装非常简单， setup后一路确定即可，第一次运行时需要选择你的网卡。

最好在 win2000下运行，在 win2003下运行网络流量表有问题。

三、常用功能介绍

1、 Dashboard （网络流量表）

点击图 1中①所指的图标，出现三个表，第一个表显示的是网络的使用率（Utilization），第二个表显示的是网络的每秒钟通过的包数量（Packets），第三个表显示的是网络的每秒错误率（Errors）。通过这三个表可以直观的观察到网络的使用情况，红色部分显示的是根据网络要求设置的上限。

选择图 1中②所指的选项将显示如图 2所示的更为详细的网络相关数据的曲线图。每个子项的含义无需多言，下面介绍一下测试网络速度中的几个常用单位。

在 TCP/IP协议中，数据被分成若干个包（Packets）进行传输，包的大小跟操作系统和网络带宽都有关系，一般为 64、128、256、512、1024、1460等，包的单位是字节。

很多初学者对 Kbps、KB、Mbps等单位不太明白，B和 b分别代表 Bytes(字节）和 bits(比特)，1比特就是 0或 1。1 Byte = 8 bits。

1Mbps (megabits per second兆比特每秒），亦即 1 x 1024 / 8 = 128KB/sec（字节/秒），我们常用的 ADSL下行 512K指的是每秒 512K比特 (Kb)， 也就是每秒 512/8=64K字节（KB）

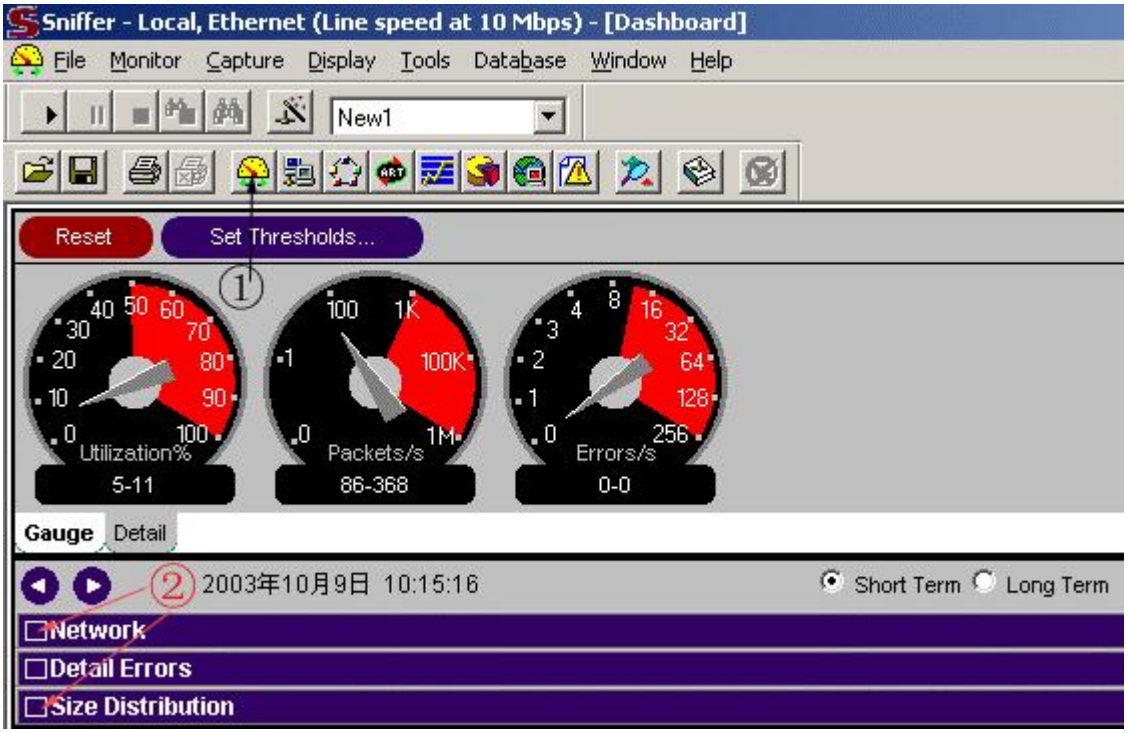


图 1

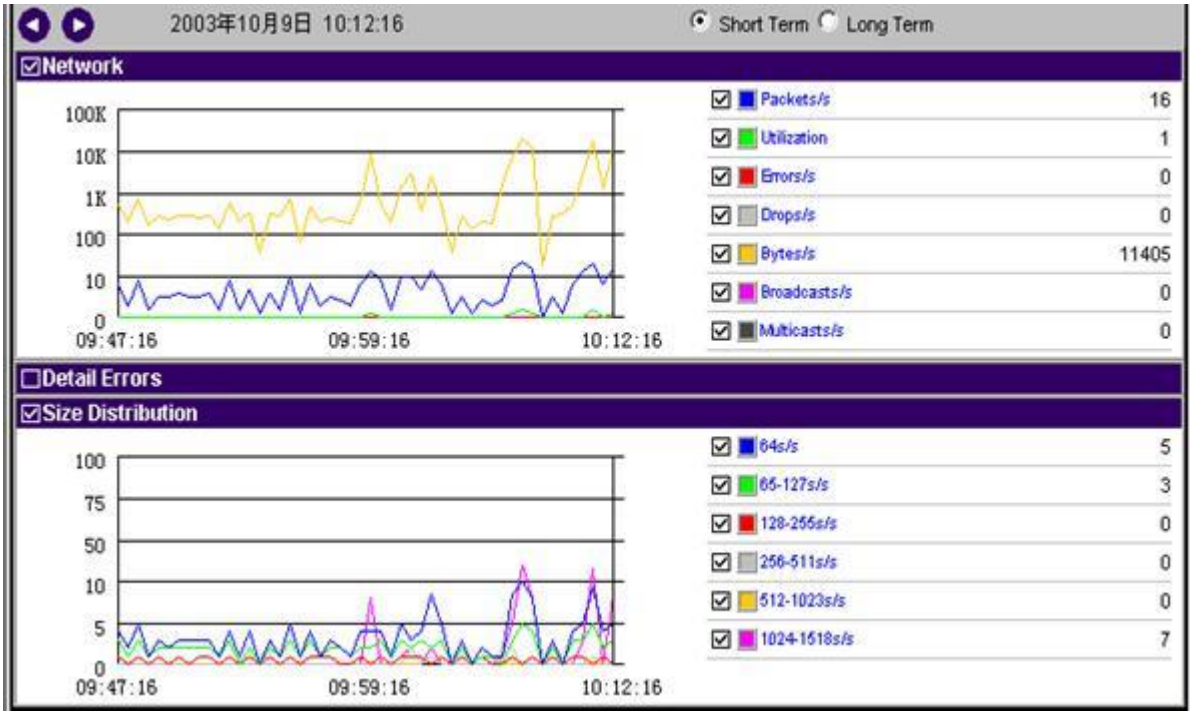
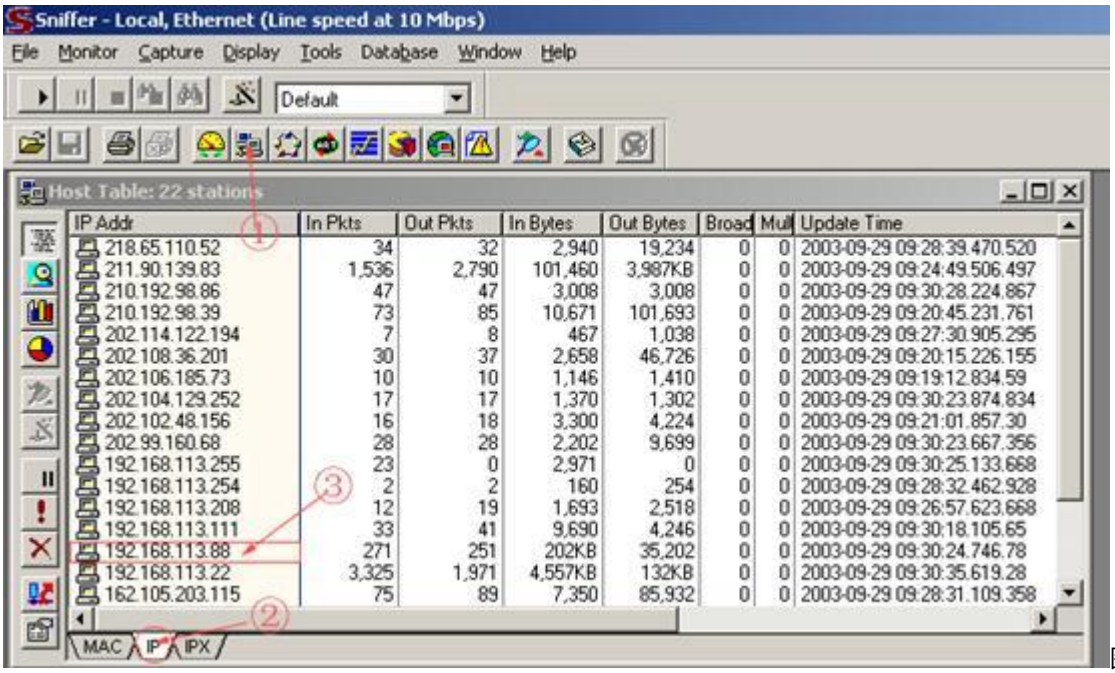


图 2

2、Host table（主机列表）

如图 3所示，点击图 3中①所指的图标，出现图中显示的界面，选择图中②所指的 IP选项，界面中出现的是所有在线的本网主机地址及连到外网的外网服务器地址，此时想看看 192.168.113.88这台机器的上网情况，只需如图中③所示单击该地址出现图 4界面。



IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broad	Mul	Update Time
218.65.110.52	34	32	2,940	19,234	0	0	2003-09-29 09:28:39.470.520
211.90.139.83	1,536	2,790	101,460	3,987KB	0	0	2003-09-29 09:24:49.506.497
210.192.98.86	47	47	3,008	3,008	0	0	2003-09-29 09:30:28.224.867
210.192.98.39	73	85	10,671	101,693	0	0	2003-09-29 09:20:45.231.761
202.114.122.194	7	8	467	1,038	0	0	2003-09-29 09:27:30.905.295
202.108.36.201	30	37	2,658	46,726	0	0	2003-09-29 09:20:15.226.155
202.106.185.73	10	10	1,146	1,410	0	0	2003-09-29 09:19:12.834.59
202.104.129.252	17	17	1,370	1,302	0	0	2003-09-29 09:30:23.874.834
202.102.48.156	16	18	3,300	4,224	0	0	2003-09-29 09:21:01.857.30
202.99.160.68	28	28	2,202	9,699	0	0	2003-09-29 09:30:23.667.356
192.168.113.255	23	0	2,971	0	0	0	2003-09-29 09:30:25.133.668
192.168.113.254	2	2	160	254	0	0	2003-09-29 09:28:32.462.928
192.168.113.208	12	19	1,693	2,518	0	0	2003-09-29 09:26:57.623.668
192.168.113.111	33	41	9,690	4,246	0	0	2003-09-29 09:30:18.105.65
192.168.113.88	271	251	202KB	35,202	0	0	2003-09-29 09:30:24.746.78
192.168.113.22	3,325	1,971	4,557KB	132KB	0	0	2003-09-29 09:30:35.619.28
162.105.203.115	75	89	7,350	85,932	0	0	2003-09-29 09:28:31.109.358

图 3

图 4中清楚地显示出该机器连接的地址。点击左栏中其它的图标都会弹出该机器连接情况的相关数据的界面。

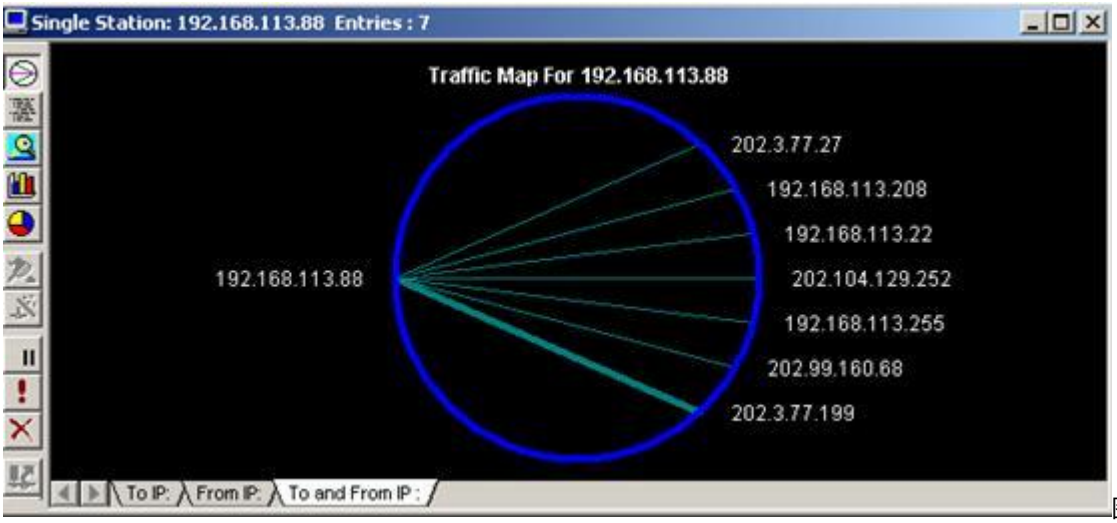
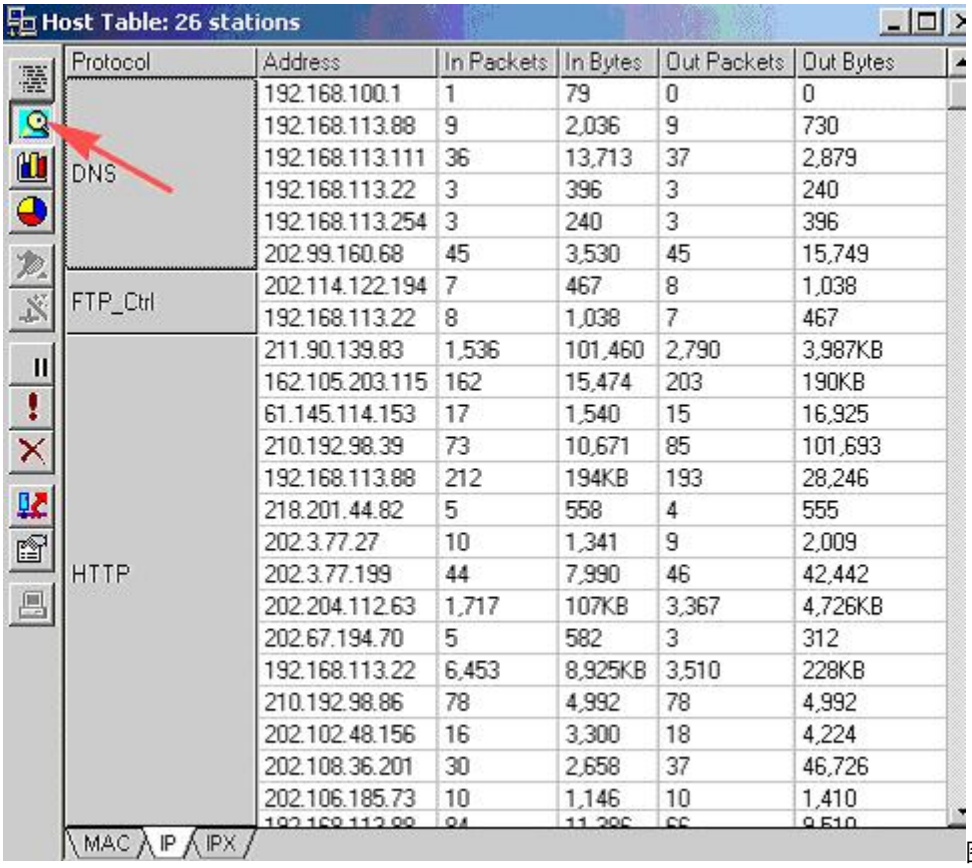


图 4

3、Detail（协议列表）

点击图 5所示的 Detail 图标，图中显示的是整个网络中的协议分布情况，可清楚地看出哪台机器运行了那些协议。注意，此时是在图 3的界面上点击的，如果在图 4的界面上点击显示的是那台机器的情况。



Protocol	Address	In Packets	In Bytes	Out Packets	Out Bytes
DNS	192.168.100.1	1	79	0	0
	192.168.113.88	9	2,036	9	730
	192.168.113.111	36	13,713	37	2,879
	192.168.113.22	3	396	3	240
	192.168.113.254	3	240	3	396
	202.99.160.68	45	3,530	45	15,749
FTP_Ctrl	202.114.122.194	7	467	8	1,038
	192.168.113.22	8	1,038	7	467
HTTP	211.90.139.83	1,536	101,460	2,790	3,987KB
	162.105.203.115	162	15,474	203	190KB
	61.145.114.153	17	1,540	15	16,925
	210.192.98.39	73	10,671	85	101,693
	192.168.113.88	212	194KB	193	28,246
	218.201.44.82	5	558	4	555
	202.3.77.27	10	1,341	9	2,009
	202.3.77.199	44	7,990	46	42,442
	202.204.112.63	1,717	107KB	3,367	4,726KB
	202.67.194.70	5	582	3	312
	192.168.113.22	6,453	8,925KB	3,510	228KB
	210.192.98.86	78	4,992	78	4,992
	202.102.48.156	16	3,300	18	4,224
	202.108.36.201	30	2,658	37	46,726
	202.106.185.73	10	1,146	10	1,410

图 5

4、Bar（流量列表）

点击图 6所示的 Bar 图标，图中显示的是整个网络中的机器所用带宽前 10名的情况。显示方式是柱状图，图 7显示的内容与图 6相同，只是显示方式是饼图。

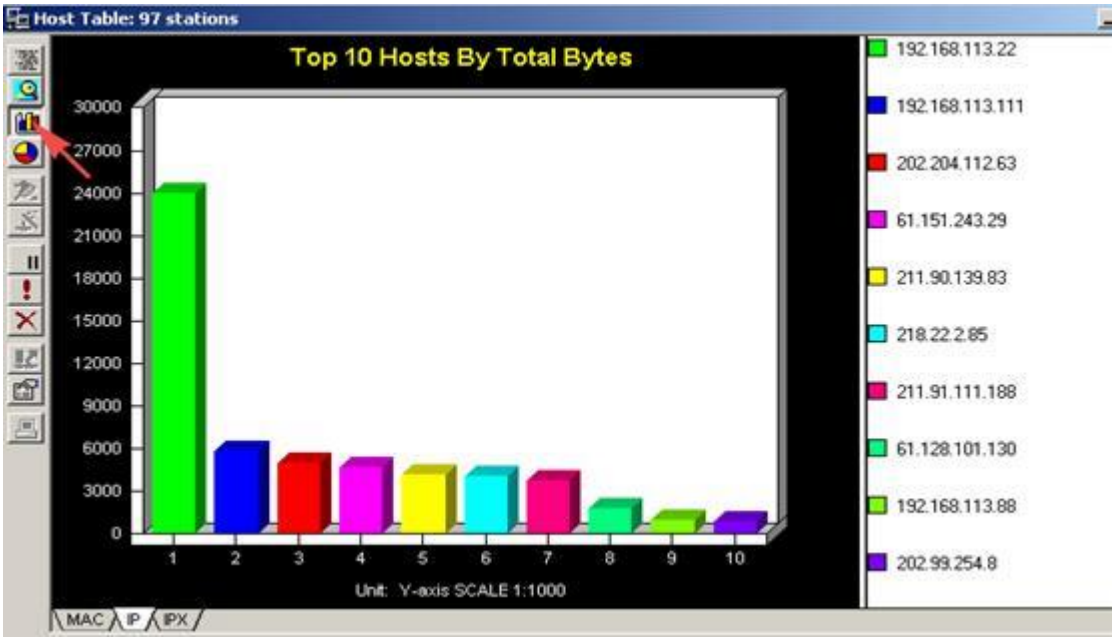


图 6

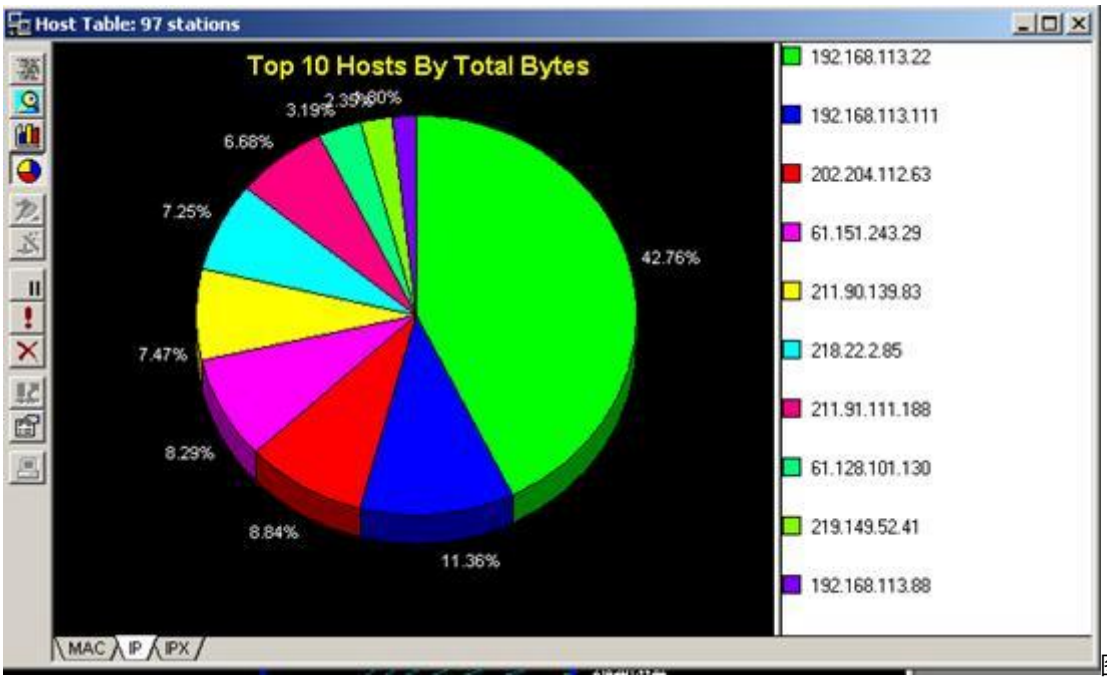


图 7

5、Matrix （网络连接）

点击图 8中箭头所指的图标，出现全网的连接示意图，图中绿线表示正在发生的网络连接，蓝线表示过去发生的连接。将鼠标放到线上可以看出连接情况。鼠标右键在弹出的菜单中可选择放大（zoom）此图。

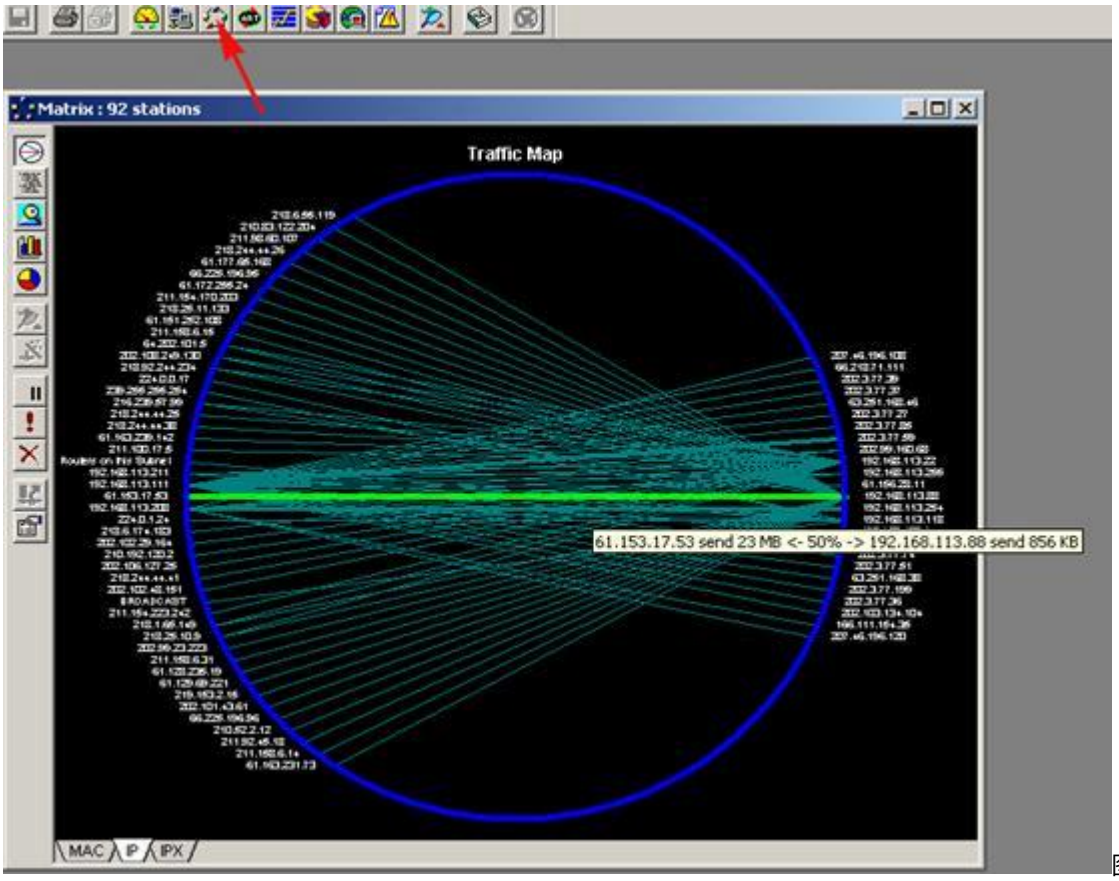


图 8

四、抓包实例

1、抓某台机器的所有数据包

如图 9所示，本例要抓 192.168.113.208这台机器的所有数据包，如图中①选择这台机器。点击②所指图标，出现图 10界面，等到图 10中箭头所指的望远镜图标变红时，表示已捕捉到数据，点击该图标出现图 11界面，选择箭头所指的 Decode 选项即可看到捕捉到的所有包。

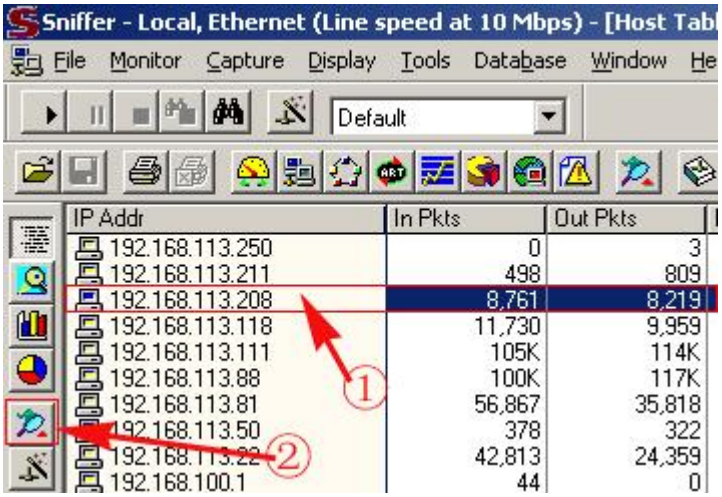


图 9

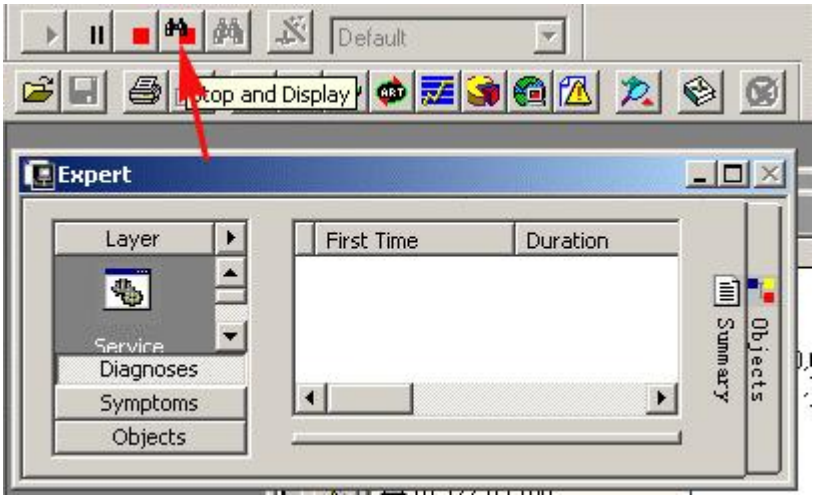


图 10

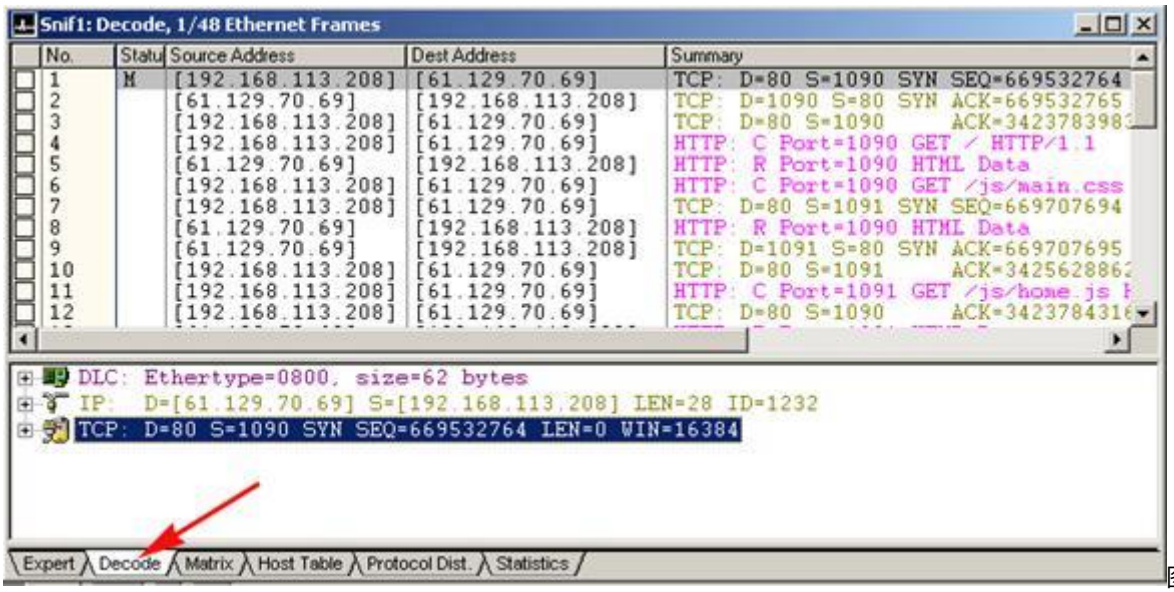


图 11

2、抓 Telnet密码

本例从 192.168.113.208 这台机器 telnet到 192.168.113.50，用 Sniff Pro抓到用户名和密码。

步骤 1：设置规则

如图 12所示，选择 Capture菜单中的 Defind Filter，出现图 13界面，选择图 13中的 ADDress项，在 station1和 2中分别填写两台机器的 IP地址，如图 14所示选择 Advanced选项，选择选 IP/TCP/Telnet ,将 Packet Size设置为 Equal 55， Packet Type 设置为 Normal。

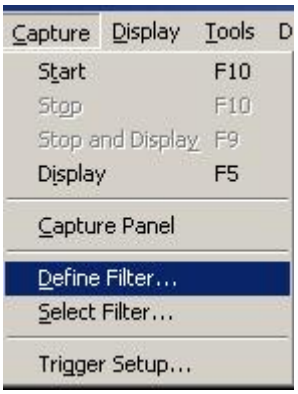
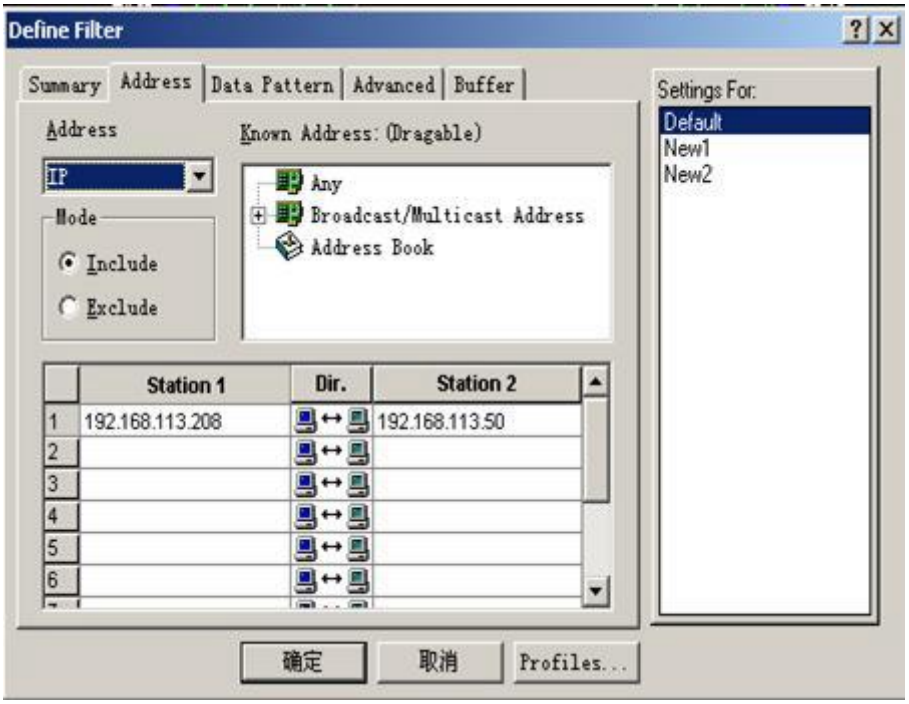


图 12



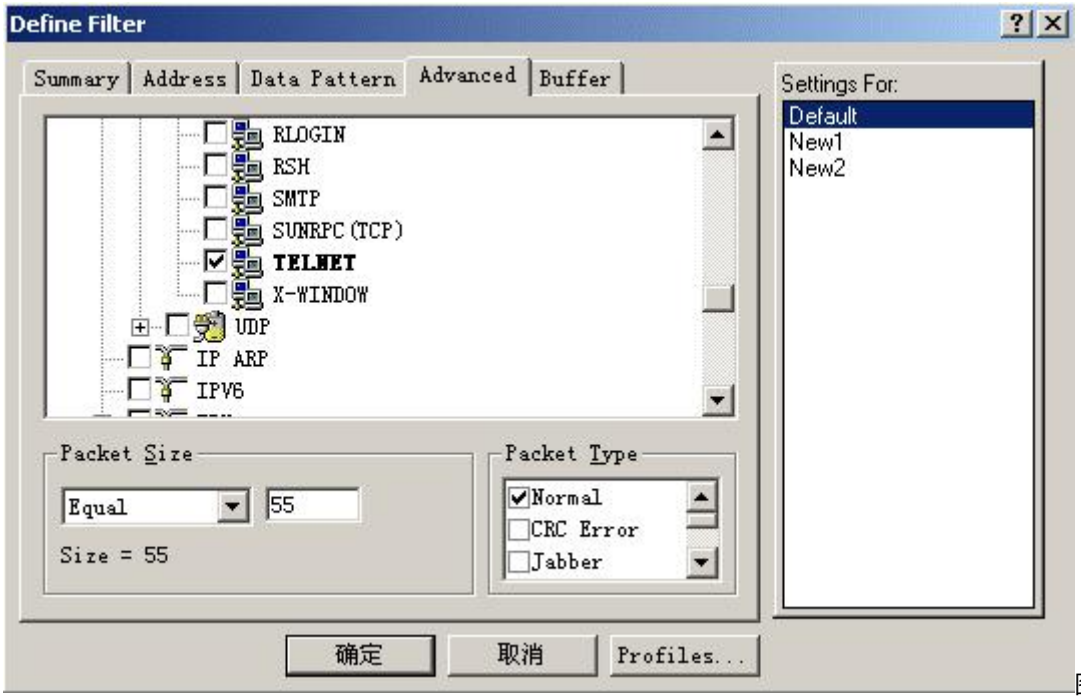


图 13

图 14

步骤 2：抓包

按 F10键出现图 15界面，开始抓包。

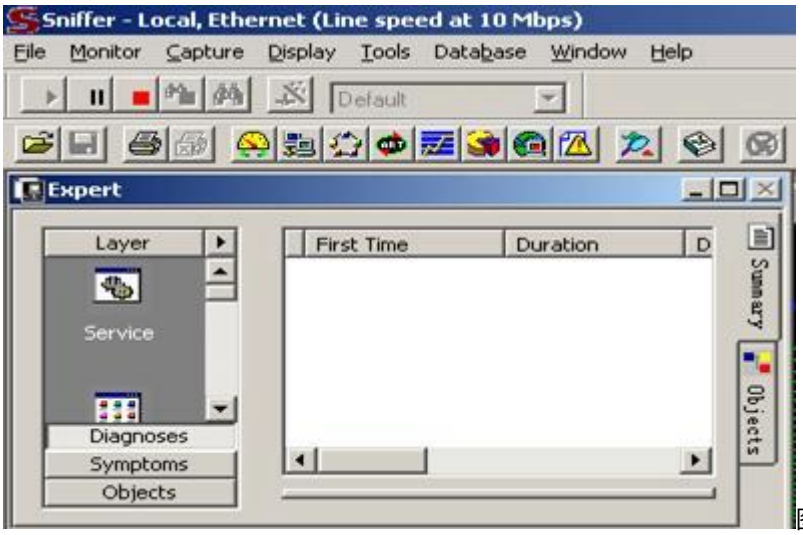


图 15

步骤 3：运行 telnet命令

本例使 telnet到一台开有 telnet服务的 Linux机器上。

telnet 192.168.113.50

login: test

Password:

步骤 4：察看结果

图 16中箭头所指的望远镜图标变红时，表示已捕捉到数据，点击该图标出现图 17界面，选择箭头所指的 Decode选项即可看到捕捉到的所有包。可以清楚地看出用户名为 test密码为 123456。

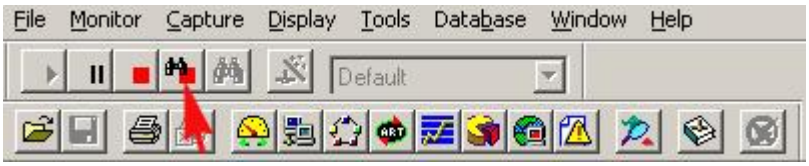


图 16

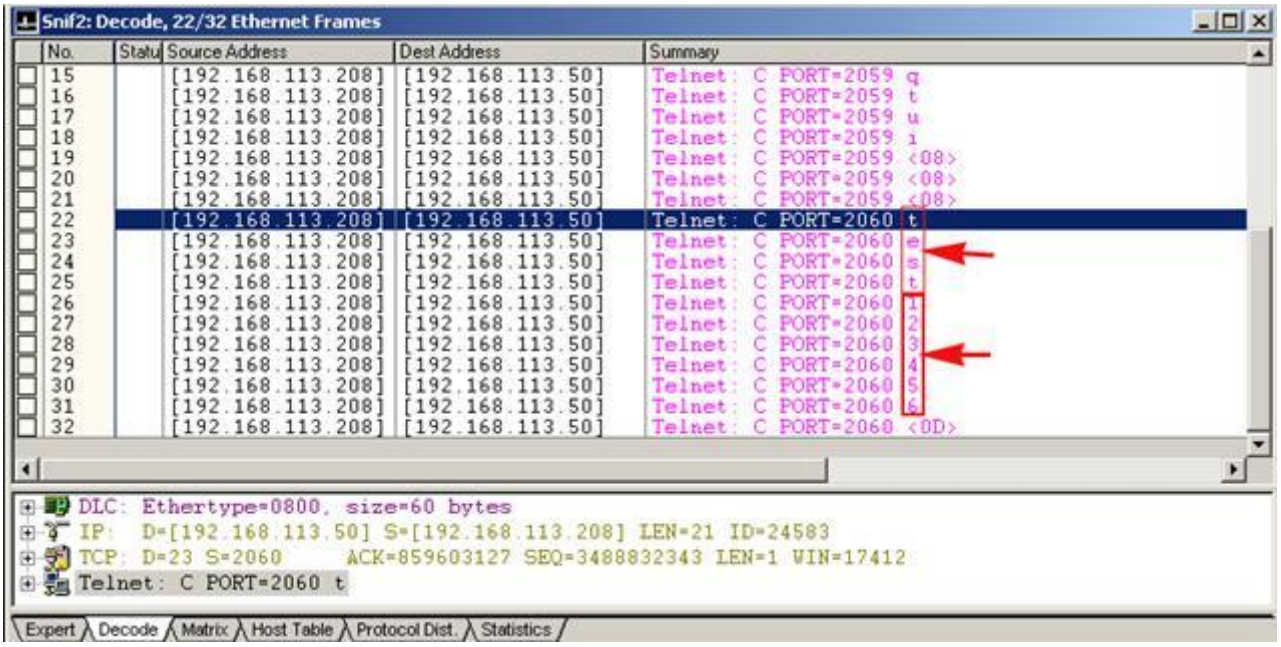


图 17

解释：

虽然把密码抓到了，但大家也许对包大小（Packet Size）设为 55不理解，网上的数据传送是把数据分成若干个包来传送，根据协议的不同包的大小也不相同，从图 18可以看出当客户端 telnet到服务端时一次只传送一个字节的数据，由

于协议的头长度是一定的，所以 telnet的数据包大小=DLC(14字节)+IP(20字节)+TCP(20字节)+数据（一个字节）=55字节，这样将 Packet Size设为 55正好能抓到用户名和密码，否则将抓到许多不相关的包。

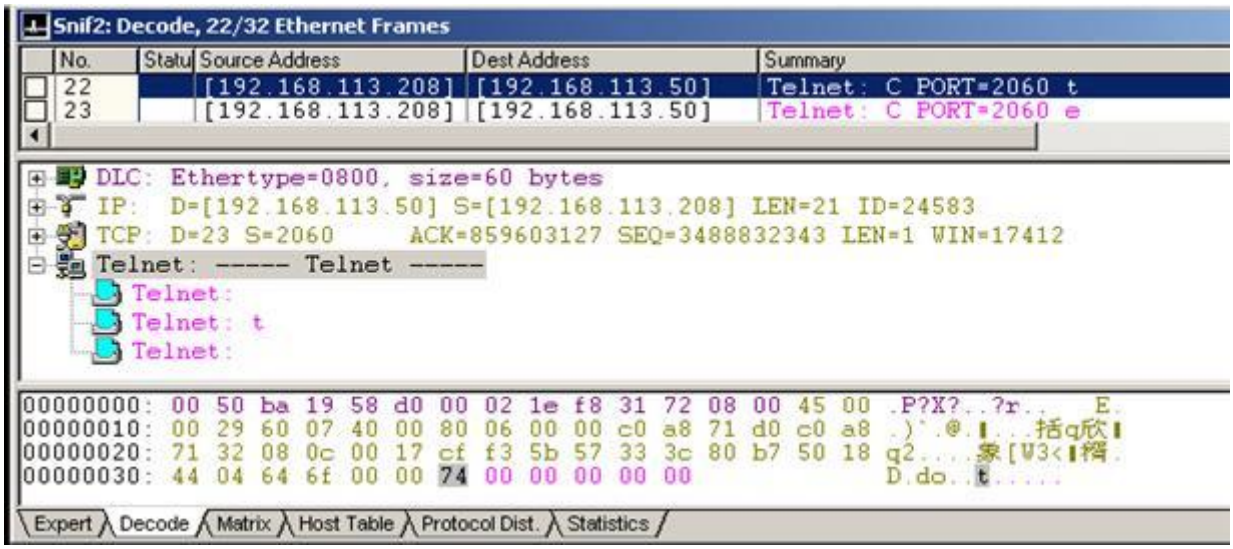


图 18

3、抓 FTP密码

本例从 192.168.113.208这台机器 ftp到 192.168.113.50，用 Sniff Pro抓到用户名和密码。

步骤 1：设置规则

如图 12所示，选择 Capture菜单中的 Defind Filter出现图 19界面，选择图 19中的 ADDress项，在 station1和 2中分别填写两台机器的 IP地址，选择 Advanced选项，选择选 IP/TCP/FTP，将 Packet Size设置为 In Between 63 -71，Packet Type 设置为 Normal。如图 20所示，选择 Data Pattern项，点击箭头所指的 Add Pattern按钮，出现图 21界面，按图设置 OFFset为 2F，方格内填入 18，name可任意起。确定后如图 22点击 Add NOT按钮，再点击 Add Pattern按钮增加第二条规则，按图 23所示设置好规则，确定后如图 24所示。

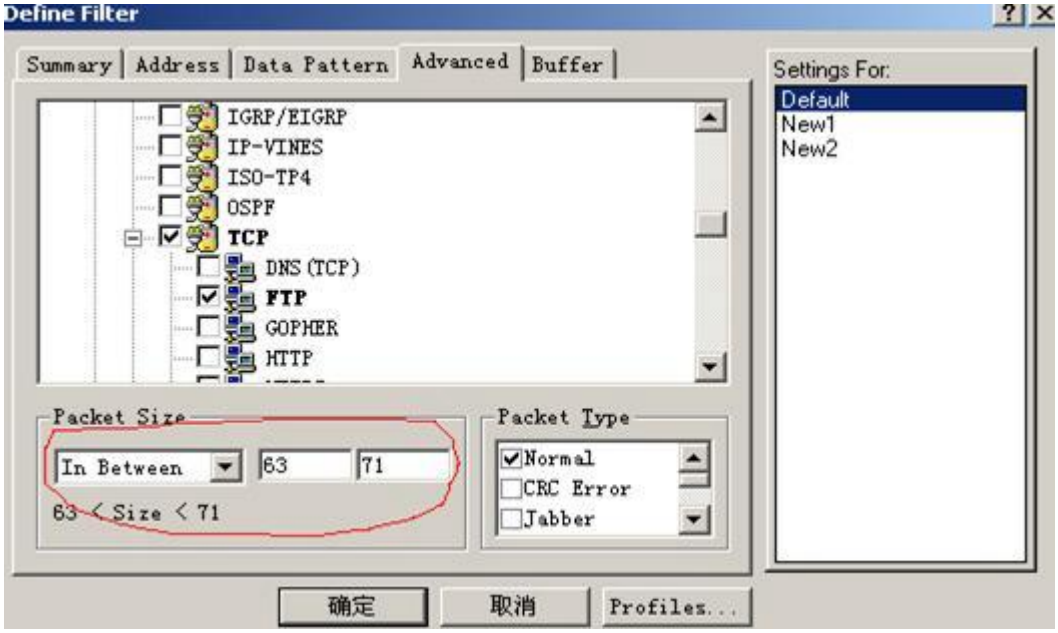


图 19

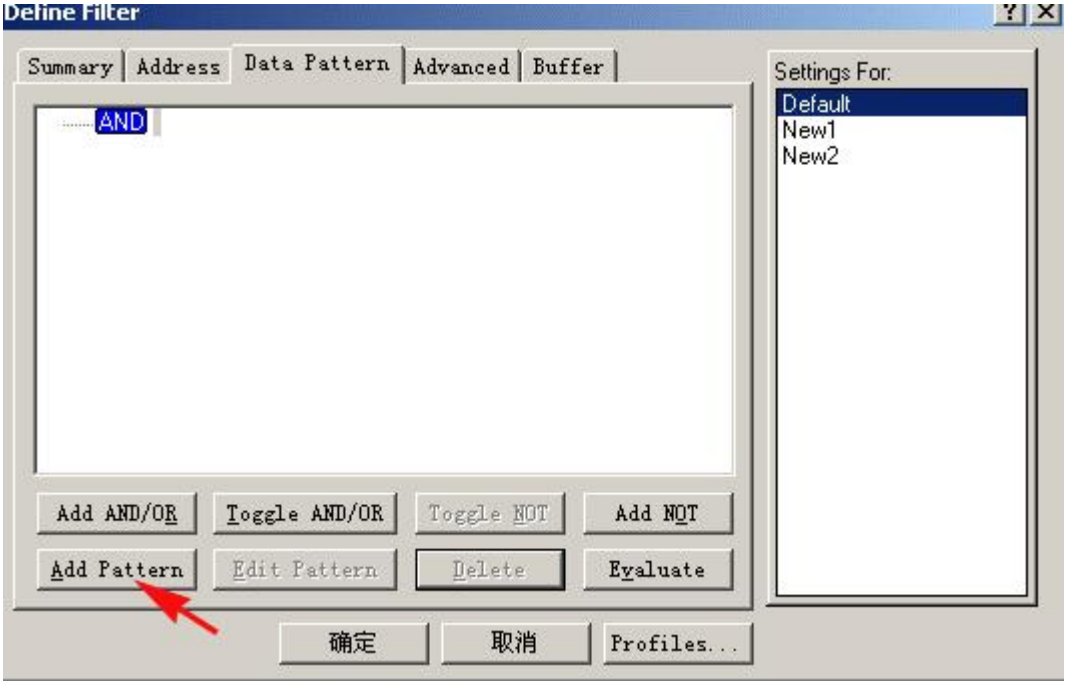

Define Filter
Summary
Address
Data Pattern
Advanced
Buffer
AND
Settings For:
Default
New1
New2
Add AND/OR
Toggle AND/OR
Toggle NOT
Add NOT
Add Pattern
Edit Pattern
Delete
Evaluate
确定
取消
Profiles...

图 20

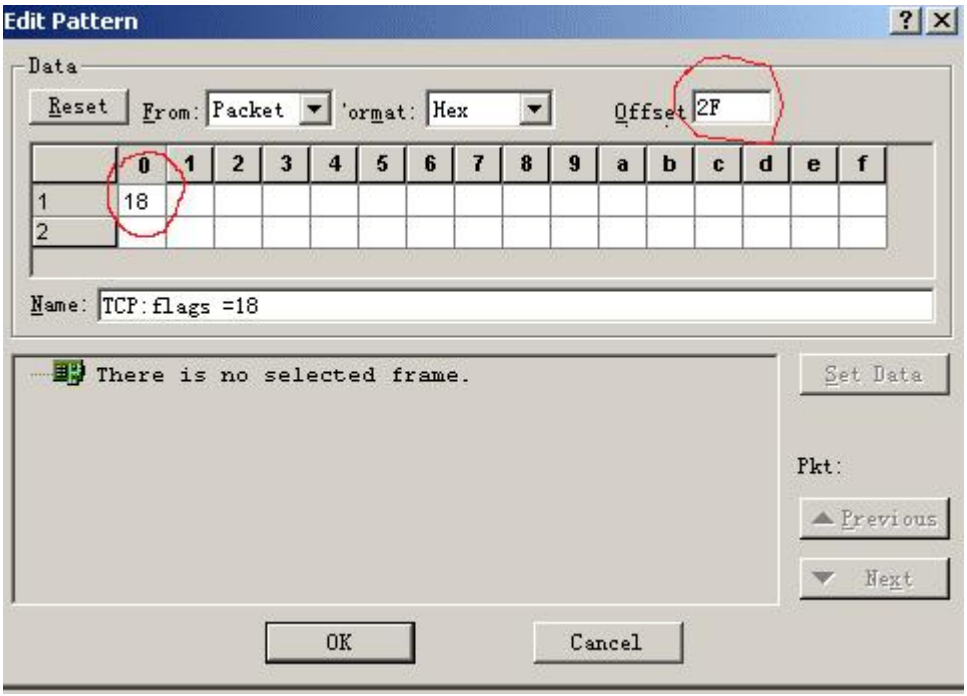

Edit Pattern
Data
Reset
From:
Packet
Format:
Hex
Offset
2F
0 1 2 3 4 5 6 7 8 9 a b c d e f
1 18
2
Name:
TCP:flags =18
There is no selected frame.
Set Data
Pkt:
Previous
Next
OK
Cancel

图 21

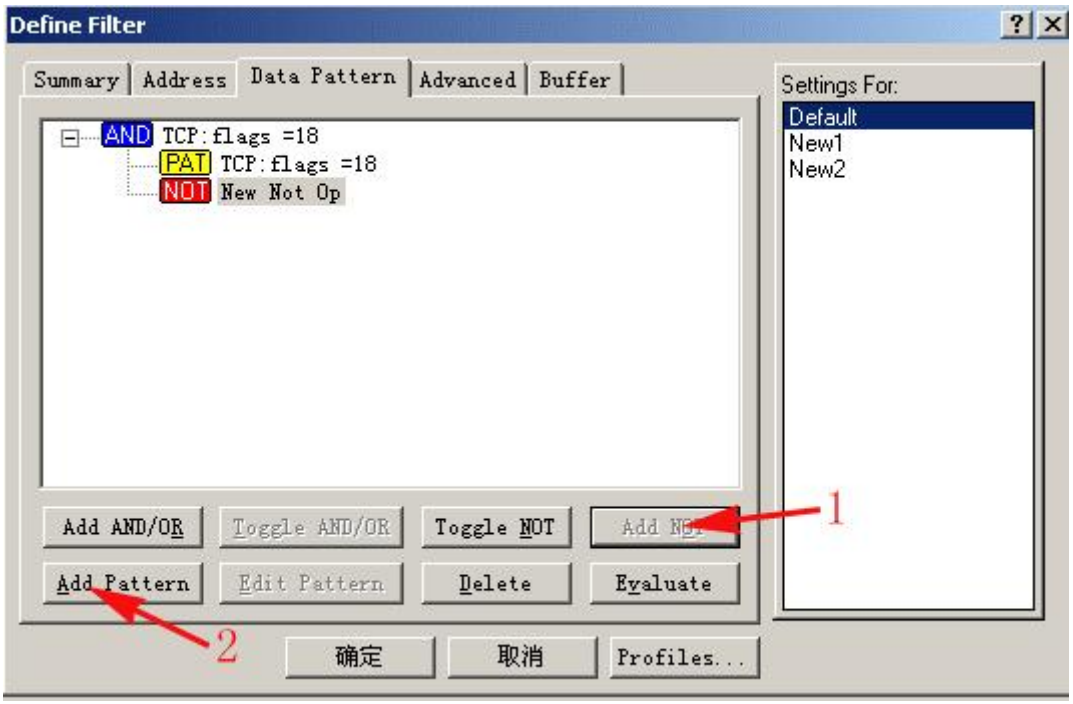

Define Filter
Summary
Address
Data Pattern
Advanced
Buffer
AND TCP:flags =18
PAT TCP:flags =18
NOT New Not Op
Settings For:
Default
New1
New2
Add AND/OR
Toggle AND/OR
Toggle NOT
Add NOT
Add Pattern
Edit Pattern
Delete
Evaluate
1
2
确定
取消
Profiles...

图 22

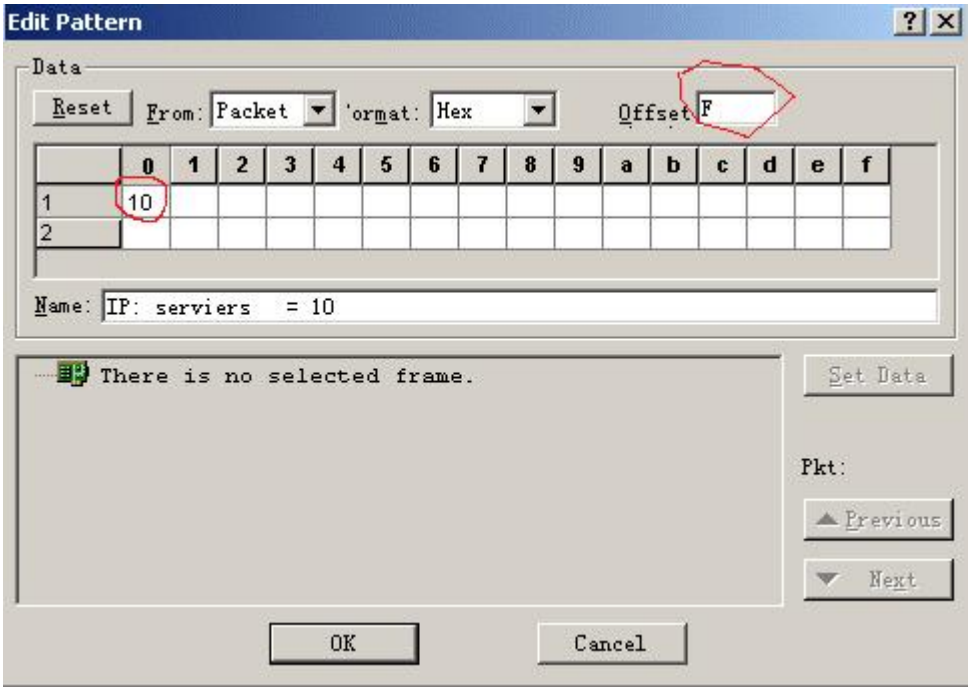

Edit Pattern
Data
Reset
From: Packet
Format: Hex
Offset F
0 1 2 3 4 5 6 7 8 9 a b c d e f
1 10
2
Name: IP: serviers = 10
There is no selected frame.
Set Data
Pkt:
Previous
Next
OK
Cancel

图 23

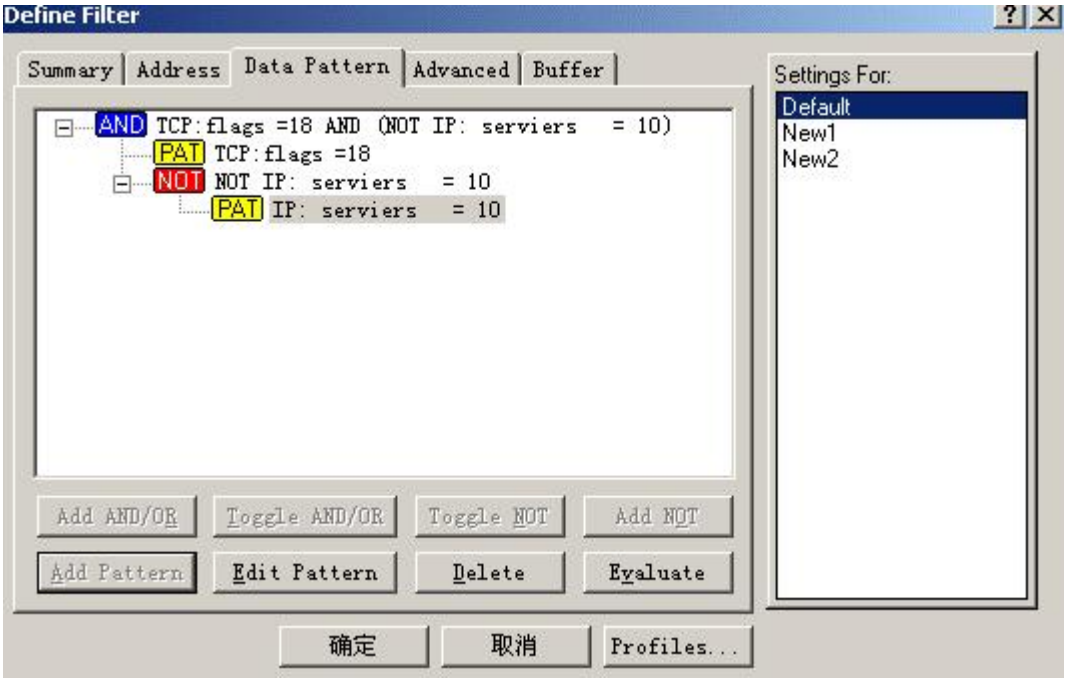


图 24

步骤 2：抓包

按 F10键出现图 15界面，开始抓包。

步骤 3：运行 FTP命令

本例使 FTP到一台开有 FTP服务的 Linux机器上

D:\>ftp 192.168.113.50

Connected to 192.168.113.50.

220 test1 FTP server (Version wu-2.6.1(1) Wed Aug 9 05:54:50 EDT 2000) ready.

User (192.168.113.50:(none)): test

331 Password required for test.

Password:

步骤 4：察看结果

图 16中箭头所指的望远镜图标变红时，表示已捕捉到数据，点击该图标出现图 25界面，选择箭头所指的 Decode选项即可看到捕捉到的所有包。可以清楚地看出用户名为 test密码为 123456789。

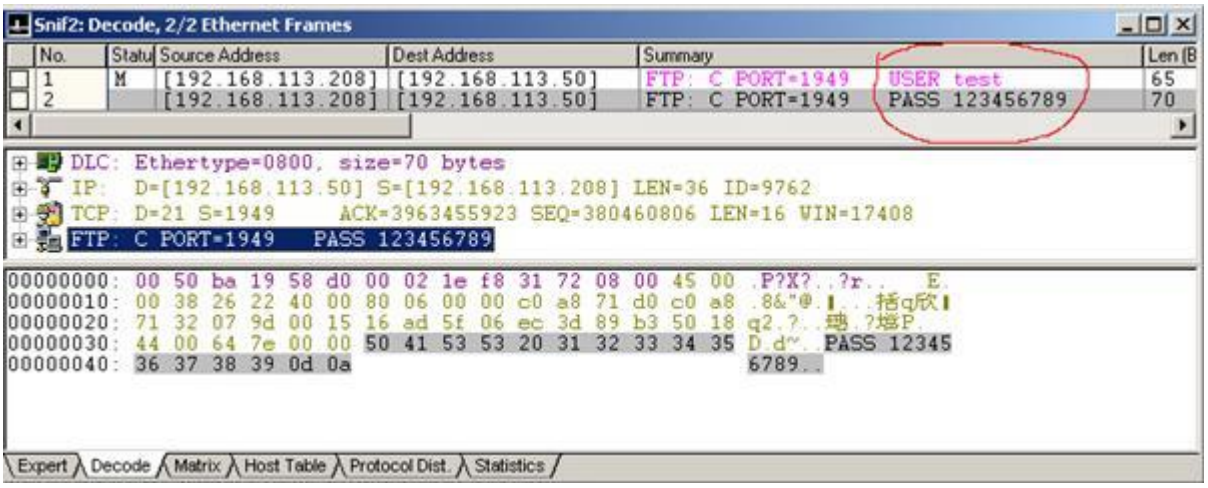


图 25

解释：

虽然把密码抓到了，但大家也许设不理解，将图 19中 Packet Size设置为 63 -71是根据用户名和口令的包大小来

设置的，图 25可以看出口令的数据包长度为 70字节，其中协议头长度为：14+20+20=54，与 telnet的头长度相同。Ftp的数据长度为 16，其中关键字 PASS占 4个字节，空格占 1个字节，密码占 9个字节，0d 0a(回车 换行)占 2个字节，包长度 =54+16=70。如果用户名和密码比较长那么 Packet Size的值也要相应的增长。

Data Pattern中的设置是根据用户名和密码中包的特有规则设定的，为了更好的说明这个问题，请在开着图 15的情况下选择 Capture菜单中的 Defind Filter，如图 20所示，选择 Data Pattern项，点击箭头所指的 Add Pattern按钮，出现图 26界面，选择图中 1所指然后点击 2所指的 Set Data按钮。OFFset、方格内、Name将填上相应的值。同理图 27中也是如此。

这些规则的设置都是根据你要抓的包的相应特征来设置的，这些都需要对 TCP/IP协议的深入了解，从图 28中可以看出网上传输的都是一位一位的比特流，操作系统将比特流转换为二进制，Sniffer这类的软件又把二进制换算为 16进制，然后又为这些数赋予相应的意思，图中的 18指的是 TCP协议中的标志位是 18。OFFset指的是数据包中某位数据的位置，方格内填的是值。

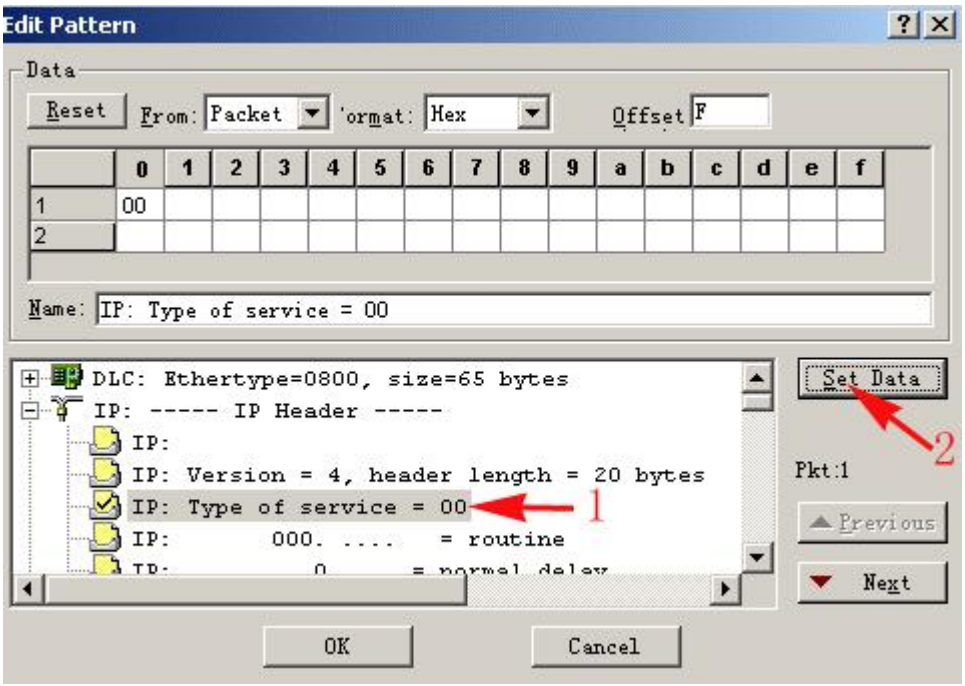


图 26

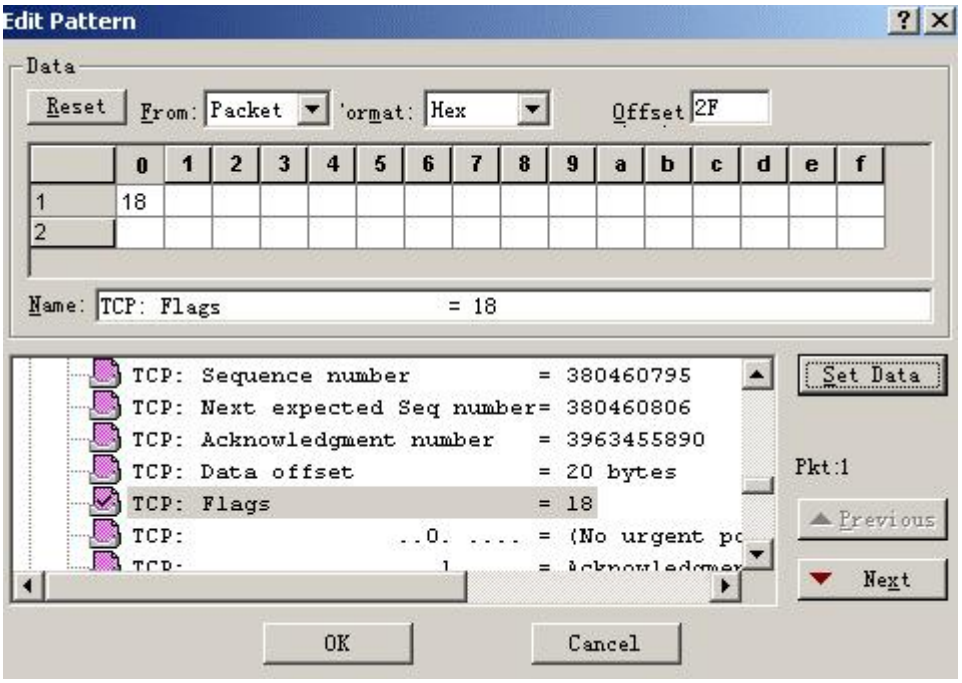


图 27

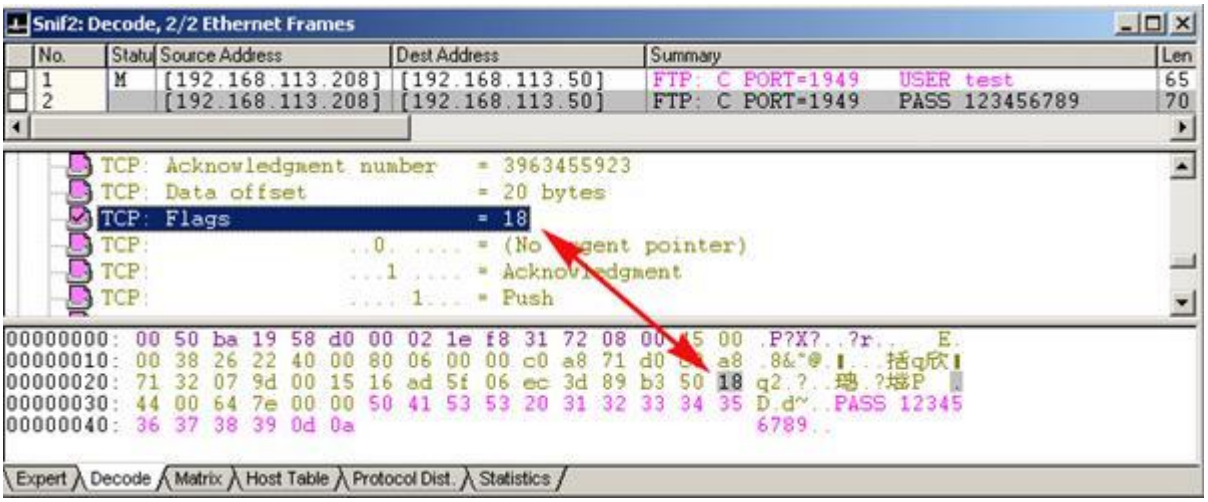


图 28

4、抓 HTTP密码

步骤 1：设置规则

按照下图 29、30进行设置规则，设置方法同上。

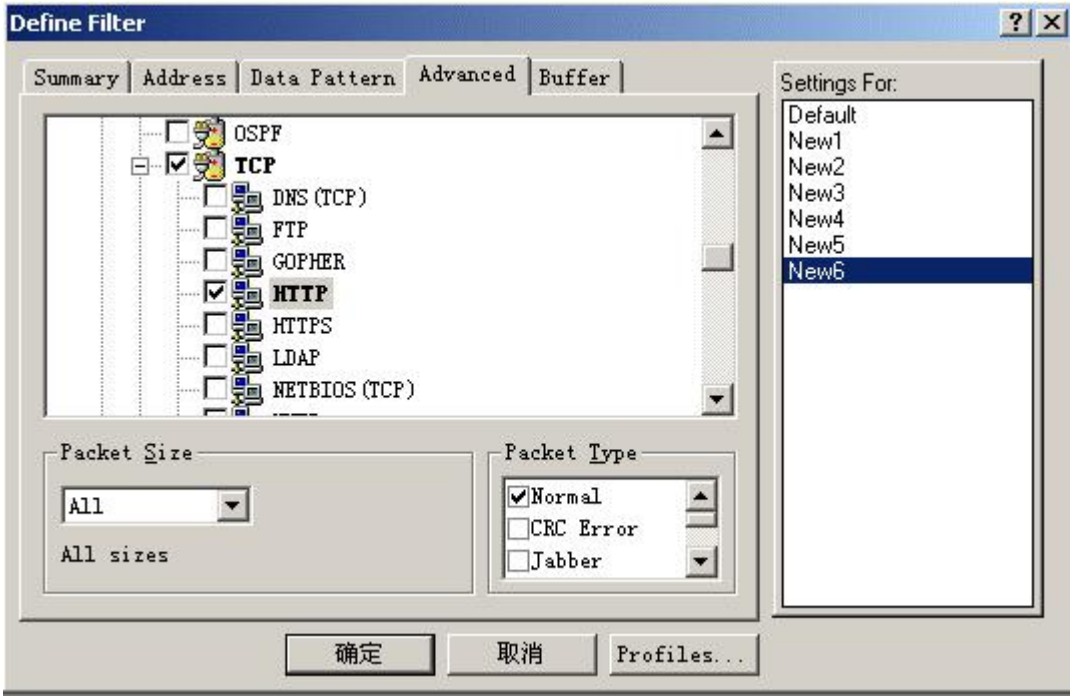


图 29

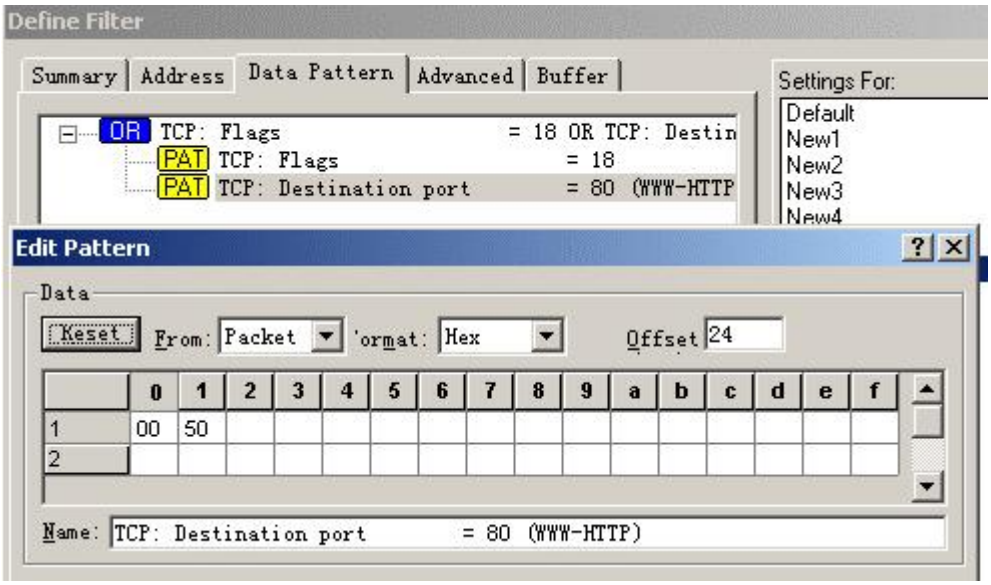


图 30

步骤 2：抓包

按 F10 键开始抓包。

步骤 3：访问 www.ccidnet.com网站

步骤 4：察看结果

图 16中箭头所 指的望远镜图标变红时，表示已捕捉到数据，点击该图标出现图 31界面，选择箭头所指的 Decode选项即可看到捕捉到的所有包。在 Summary中找到含有 POST关键字的包，可以清楚地看出用户名为 qiangkn997，密码为 ?，这可是我邮箱的真实密码！当然不能告诉你，不过欢迎来信进行交流。

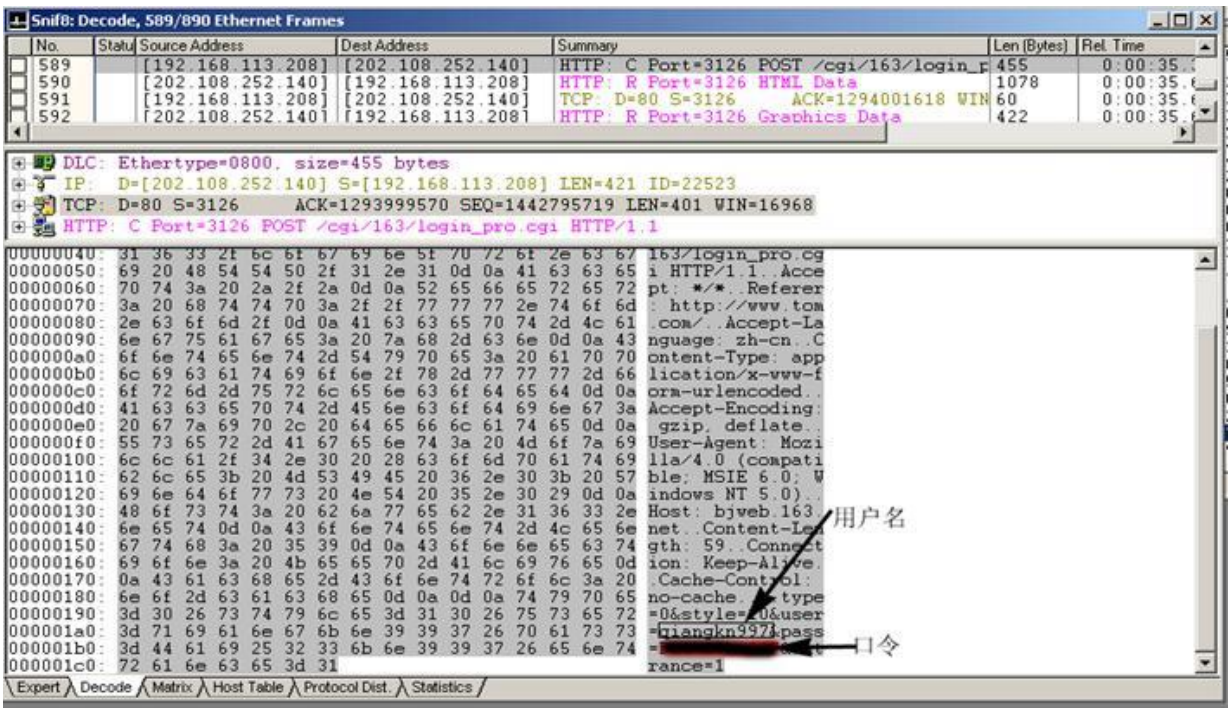


图 31

五、后记

本文中的例子是网内试验，若捕捉全网机器的有关数据请将图 13中的 station设置为 any<->any，作为学习研究可以，可别做坏事！如果要用好 Sniff Pro必须有扎实的网络基础知识特别是 TCP/IP协议的知识，其实 Sniff Pro本身也是学习这些知识的好工具。