一、前言

曾写过《<u>用协议分析工具学习 TCP/IP</u>》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 <u>www.baidu.com</u>或 <u>www.google.com</u>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 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 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 Kops, KB, Mops 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)





2 Host table(主机列表)

如图 3所示,点击图 3中 所指的图标,出现图中显示的界面,选择图中 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 所示单击 该地址出现图 4界面。

Sniffer - Local, Ethernet (Lin	e speed at	10 Mbps)						
Monitor Capture Display	Iools Data	ibase Windi	ow Help					
▶ 11 = Ma 例 必 D	efault	•						
			20	8				
Host Table: 22 stations							<u> </u>	
IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes	Broad	Mul	Update Time	
Image: 2000 constraints 218.65.110.52 Image: 2000 constraints 211.90.139.83 Image: 2000 constraints 210.192.98.39 Image: 2000 constraints 202.114.122.194 Image: 2000 constraints 202.106.185.73 Image: 2000 constraints 2000 constraints Image: 2000 constraints 2000 con	34 1,536 47 73 30 10 17 16 28 23 23 23 23 23	32 2,790 47 85 8 37 10 17 18 28 28 0 2	2,940 101,460 3,008 10,671 467 2,658 1,146 1,370 3,300 2,202 2,971 160	19,234 3,987KB 3,008 101,693 1,038 46,726 1,410 1,302 4,224 9,699 0 254	000000000000000000000000000000000000000	000000000000000000000000000000000000000	2003-09-29 09:28:39.470.52 2003-09-29 09:24:49.506.45 2003-09-29 09:20:45.231.76 2003-09-29 09:20:45.231.76 2003-09-29 09:20:45.231.76 2003-09-29 09:20:15.226.15 2003-09-29 09:20:15.226.15 2003-09-29 09:30:23.874.83 2003-09-29 09:30:23.874.83 2003-09-29 09:30:23.874.83 2003-09-29 09:30:23.873.36 2003-09-29 09:30:25.133.66	20 37 37 35 55 44) 56 88 88
192168.113.208 192168.113.111 192168.113.88 192168.113.22 162.105.203.115 162.105.203.115	12 33 271 3,325 75	19 41 251 1,971 89	1,693 9,690 202KB 4,557KB 7,350	2,518 4,246 35,202 132KB 85,932	0 0 0 0	000000000000000000000000000000000000000	2003-09-29 09:26:57 623.66 2003-09-29 09:30:18 105.65 2003-09-29 09:30:24.746.76 2003-09-29 09:30:35.619.26 2003-09-29 09:28:31.109.35	8 -

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。



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	
	192.168.100.1	1	79	0	0	
	192.168.113.88	9	2,036	9	730	
DNIC	192.168.113.111	36	13,713	37	2,879	
DNS	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	
ETD CH	202.114.122.194	7	467	8	1,038	
FIP_Cm	192.168.113.22	8	1,038	7	467	
	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	
HTTP	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	
	102 100 112 00	04	11 200	22	9,510	1

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。



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。



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 选择这台机器。点击 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。

S5r	hiffer - Local, Ethernet (Line s	speed at 10 Mb	ps) - [Host Tab
题 E	ile Monitor ⊆apture Display	<u>T</u> ools Data <u>b</u> a	se <u>W</u> indow <u>H</u> e
	II 🖬 🊧 🌋 Defa	ault	.
2		• 🗾 🕥 🙆	🔼 🙇 🔮
	IP Addr	In Pkts	Out Pkts 1
一般	昌 192.168.113.250	0	3
Q	📮 192.168.113.211	498	809
	🖳 192.168.113.208 🔪	8,761	8,219
	🖪 192.168.113.118	11,730	9,959
	昌 192.168.113.111 🔨	105K	114K
	🖪 192.168.113.88 🛛 👌 🏹	100K	117K
	🖪 192.168.113.81 🛛 🕓	56,867	35,818
\mathcal{P}_{\bullet}		378	322
1	E 192.168.113.22(2)	42,813	24,359
-21	国 192.168.100.1	44	0

冬



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。



步骤 2: 抓包

按 F10键出现图 15界面,开始抓包。

Sniffer - Local, Ethe	rnet (Line speed a	t 10 Mbps)	
jie Monitor ⊆apture	Display Tools Dat	ta <u>b</u> ase <u>W</u> indow	Help
▶ II = 🗠 🖗	🔊 Default	¥.	
FI 5 5 4	9 3 4 2	🌫 🖾 🍙	
Expert .			
Layer +	First Time	Duration	
			Sum
			ler,
Service			
			8
			jeo
Diagnoses			d d
Symptoms			
Objects	-		
- 194			§

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

<u>File Monitor Capture Display Tools Database Window Help</u>



INo	Statul Source Address	Dest Address	Summanu	112
115 115 16 17 18 20 21 22 23 24 25 26 27 30 31 32	192 168 113 208 113 <td>[192.168.113.50] [192.168.113.50]</td> <td>Telnet: C PORT=2059 q Telnet: C PORT=2059 t Telnet: C PORT=2059 t Telnet: C PORT=2059 i Telnet: C PORT=2059 (08) Telnet: C PORT=2059 (08) Telnet: C PORT=2059 (08) Telnet: C PORT=2060 t Telnet: C PORT=2060 t Telnet: C PORT=2060 t Telnet: C PORT=2060 t Telnet: C PORT=2060 1 Telnet: C PORT=2060 1 Telnet: C PORT=2060 1 Telnet: C PORT=2060 4 Telnet: C PORT=2060 4 Telnet: C PORT=2060 4 Telnet: C PORT=2060 5 Telnet: C POR</td> <td></td>	[192.168.113.50] [192.168.113.50]	Telnet: C PORT=2059 q Telnet: C PORT=2059 t Telnet: C PORT=2059 t Telnet: C PORT=2059 i Telnet: C PORT=2059 (08) Telnet: C PORT=2059 (08) Telnet: C PORT=2059 (08) Telnet: C PORT=2060 t Telnet: C PORT=2060 t Telnet: C PORT=2060 t Telnet: C PORT=2060 t Telnet: C PORT=2060 1 Telnet: C PORT=2060 1 Telnet: C PORT=2060 1 Telnet: C PORT=2060 4 Telnet: C PORT=2060 4 Telnet: C PORT=2060 4 Telnet: C PORT=2060 5 Telnet: C POR	
•1				
 ■ ■	LC: Ethertype=0800, siz P D=[192.168.113.50] CP D=23 S=2060 ACK elnet: C PORT=2060 t	e=60 bytes S=[192 168 113 208 =859603127 SEQ=3480] LEN=21 ID=24583 8832343 LEN=1 WIN=17412	

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/TOP/FTP,将 Packet Size设置为 In Between 63 -71, Packet Type 设置为 Nomal,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 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。



marre bddra	Data Pattern	Advanced Buff		
nmary Addre	ss baca raccan	wayancea barr	.er	Default
AND				New1 New2
add and/o <u>r</u>	Toggle AND/OR	Toggle NOT	Add NOT	
Add AND/O <u>R</u> idd Pattern	<u>I</u> oggle AND/OR <u>E</u> dit Pattern	Toggle NOT	Add NOT Evaluate	

Jata <u>R</u> eset <u>F</u>	rom: P	acke	et]	• •	r <u>m</u> at	: He	x	•	I	Qf:	fset	2 F	\rightarrow			
1 18	7	2	3	4	5	6	7	8	9	a	b	C	d	е	f	
ICF: 1	11ags 3	-10 no s	sel	ecte	d f	rame	÷.							<u>s</u> Pkt	et Da	ta
														•	<u>P</u> revi Ne <u>x</u>	ou et
			3. 			-					- 7			-		Ī

efine Filter			ilie a la companya da comp		?>
Summary Addre	ss Data Pattern flags =18 TCP:flags =18 New Not Op	Advanced Buf	Eer	Settings For: Default New1 New2	
Add AND/O <u>R</u>	Toggle AND/OR Edit Pattern	Toggle MOT	Add N <u>o</u> . E <u>v</u> aluate	-1	
	·2 _{确定}		Profiles]	



ſ	0	1	2	3	4	5	6	7	8	9	-	Ь			f
-(10		~	•	100.00			132		•	a				
	~														
Th Th	ere	is	no	sele	ecte	d f	rame	•.						5	et Da
B) Th	ere	is	no	sele	ecte	d f	rame).					_	<u>S</u> Pkt	et Da
Th	ere	is	no	sele	ecte	d f	rame	1.						S Pkt	et Da <u>P</u> revi

= <mark>AND</mark> TCP	:flags =18 AND (NO TCP:flags =18 NOT TP: serviers)T IP: serviers s = 10	= 10)	Default New1 New2	
	<mark>PAT</mark> IP: servier	s = 10			
add and/o <u>r</u>	Toggle AND/OR	Toggle NOT	Add NOT		

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,Od 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。CFFset、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, CFFset指的是数据包中某位数据的位置, 方格内填的是值。

1.0	1	2	3	4	5	6	7	8	9	a	h	C	h	e	f
		-				•		-		•		•			-
100	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
DLC: IP: -	Eth:	erty - IP	pe= He	0800 ader), s :	ize=	=65	byt	25						et
DLC: IP: -] IP] IP	Eth : : Ve	erty - IP ersi	pe= He on :	0800 ader = 4,), s : he:	ize: ader	=65 : le:	byt:	25	20 1	oyte	5		<u> </u>	et :1
DLC: IP: - IP: - IP IP IP	Eth : : Ve : Ty	erty - IF ersi pe	pe= He on :	0800 ader = 4, serv), s : he: ice	ize= ader = 0	=65 : le:	byte ngth	25	20 I	oyte	s		<u> </u>	et :1

图 26

	0	1	2	3	4	5	6	7	8	9	а	b	C	d	е	f
	18	1	1	Î	1	1	Î	Î	9	8	Î		ĵ.	1	1	Î
1		Ĩ		Ĩ.	Ĩ.	Ĩ	Ĩ.	Ĩ	Ĩ.	Ĩ.	2		ŝ.	Ĩ.		2
	TCP: 1	Flag P: S D- N	s lequi	ence	e nu	mber ed 9	: c	= 18	=	: 38	0460	0795				et
	TCP: 1 TCI	Flag P: S P: N	s lequ lext	ence exp	e nu	mber ed S	: č šeq	= 18 numl	= ber=	- 38 - 38	0460	0795		•	<u></u>	et .
me.].) TCI) TCI) TCI) TCI	Flag P: S P: N P: A	s (equ lext lckn	ence exp owle	e nu pect	mber ed S ent	: c Seq num	= 18 numl ber	= ber=	= 38 = 38 = 39	0460 0460 6343	0795 0806 5589	0	•	<u>S</u>	et i
	TCP: 1 TCI TCI TCI	Flag P: S P: N P: A P: D	s lequ lext lckn ata	ence exp owle of:	e nu pect edgm fset	mber ed S ent	: Seq num	= 18 numl ber	= ber= =	= 38 = 38 = 39 = 20	0460 0460 6349 byt)795)806 5589 :es	0		<u> </u>	et 1
	TCP: 1 TCI TCI TCI TCI	Flag P:S P:N P:A P:D P:F	s (equ lext .ckn (ata (lag:	ence exp owle of: s	e nu pect edgm fset	mber ed S ent	: r Seq num	= 18 numl ber	= ber= =	= 38 = 38 = 39 = 20 = 18	0460 0460 6349 byt)795)806 5589 :es	0		 Pkt:	et 1 Pre
	TCP: 1 TCI TCI TCI TCI TCI	Flag P: S P: N P: A P: D P: F	s (equ Jext (ckn) (ata (lag)	ence exp owle of: s	e nu pect edgm fset	mber ed S ent	: Seq num	= 18 numl ber	= ber= = =	= 38 = 38 = 39 = 20 = 18 = (N	0460 0460 6345 byt o ur)795)806 5589 :es	0 t p		Pkt:	et 1 Ere

图 27

-	Snif2: D	ecode	, 2/2 Ethe	ernet Fra	nes									_ [] ×
100	No.	Statu	Source Ad	dress		Dest Add	ess		Summary					Len
g	1	М	[192.1	68.113	.208]	[192.1	68.113	3.50]	FTF: C	PORT=19	149 1	ISER to	est	65
Ц	2		[192.1	68.113	. 208]	1192.1	.68.113	5.50]	FIP: C	PORT=1	949 E	A55 1	23456789	/0
						_								<u> </u>
8	200	TCP: TCP: TCP:	Acknow Data c Flags	ledgme offset	nt nu	ber	= 3963 = 20 E = 18	45592 oytes	3					<u>_</u>
	8	TCP :			0		= (No = Ackr	novied	t pointer gment)				_
	- D	TCP :			14.400	1	- Fush	1						-
000000000000000000000000000000000000000	000000 000010 000020 000030 000030	0: 00 0: 00 0: 71 0: 44 0: 36	50 ba 38 26 32 07 00 64 37 38	19 58 22 40 9d 00 7e 00 39 0d	d0 00 00 80 15 16 00 50 0a	02 1e 06 00 ad 5f 41 53	f8 31 00 c0 06 ec 53 20	72 01 a8 7 3d 8 31 3	8 00 45 0 L d0 5 a 5 5 50 1 2 33 34 3	0 .P?X? 8 .8&*@ g2.?. 5 D.d~. 6789.	.?r. 1. 括 璁.?地 PASS 1	E. P. 2345		2
E)	opert) D	ecode	Matrix A	Host Tabl	e A Proto	col Dist.	Statistics	1						

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。



E	OR T	Address Data Fattern Advanced Buffer DR TCP: Flags = 18 OR TCP: Destin									Settings For:						
	F	PAT PAT	ICP:	Fla; Des	gs tina ⁴	tion	por	t		= 18 = 80	3 D (W1	የጸ-ዧ	TTP	NN	ew2 ew3		
t Pal	ttern																?
ata					_		-		1000	r.		53	_	_			
Keset From: Packet 💌 'ormat: Hex 💌 Offset 24												fset	24				
	1.000	1	2	3	4	5	6	7	8	9	a	b	C	d	е	f	
	0	and the second second second		SS 33	SS - 3S	84 - XS	83 - X8	23 - 28 	Si 23	SS - 38					84 - 38 		
1	00	50	1				1 C							1	1		1
1	00	50							1				1	1			

步骤 2: 抓包

按 F10 键开始抓包。

步骤 3: 访问 <u>www.ccidnet.com</u>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。

Logia Snif8: Decode, 589/890 Ethernet Frames												
No. Statu Source Address Dest Address Summary	Len (Bytes)	Rel Time										
589 [192.168.113.208] [202.108.252.140] HTTP: C Port=3126 POST /cgi/163/login_ [202.108.252.140] [192.168.113.208] HTTP: R Port=3126 HTML Data	¢ 455 1078	0:00:35.										
[192.168.113.208] [202.108.252.140] TCP D=80 S=3126 ACK=1294001618 WI	N 60	0:00:35.										
1 1 202.100.252.140/11192.100.113.2001 Infile & Port-Size Graduites Data	922	0.00.35.										
TO DIC: Ethertune=0800 size=455 hutes												
3 IP D=[202 108.252 140] S=[192 168.113 208] LEN=421 ID=22523												
TCP: D=80 S=3126 ACK=1293999570 SEQ=1442795719 LEN=401 WIN=16968												
🖻 💑 HTTP: C Port=3126 POST /cgi/163/login_pro.cgi HTTP/1.1												
00000040: 31 36 33 21 6c 61 67 69 6e 51 70 72 61 2e 63 67 163/login_pro.cg												
00000050: 69 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63 63 65 i HTTP/1 1. Acce												
00000000 30 /4 3a 20 2a 21 2a 00 0a 52 05 06 57 2 55 /2 pt. ***. Reference												
00000080: 2e 63 6f 6d 2f 0d 0a 41 63 63 65 70 74 2d 4c 61 .com/.Accept-La												
00000090: 6e 67 75 61 67 65 3a 20 7a 68 2d 63 6e 0d 0a 43 nguage: zh-cn. C												
000000b0 6 6 6 6 6 7 6 7 6 6 6 6 2 f 7 8 2 d 7 7 7 7 7 2 d 6 licent-type app												
000000c0: 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a orm-urlencoded												
000000001 41 53 55 70 74 20 45 56 53 51 57 36 57 38 Accept-Encoding												
00000010: 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Agent: Mozi												
00000100: 6c 6c 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 11a/4.0 (compati												
00000110: 62 6c 65 3b 20 4d 53 49 45 20 36 2e 30 3b 20 57 ble; MSIE 6.0; 0												
00000120 by de f 73 74 3a 20 62 6a 77 65 62 2e 31 36 33 2e Host birds hit 5 0												
00000140: 6e 65 74 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e net. Content-Les HIF 4												
00000150: 67 74 68 3a 20 35 39 0d 0a 43 6f 6e 6e 65 63 74 gth: 59. Connect												
00000160: 63 61 65 63 42 40 65 65 70 20 41 65 65 76 65 96 101 101: Keep-Alaye.												
00000180 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a 74 79 70 65 no-cache type												
00000190: 3d 30 26 73 74 79 6c 65 3d 31 30 26 75 73 65 72 = <u>D&style=_O&</u> user												
000001a0: 3d 71 69 61 6e 67 6b 6e 39 39 37 26 70 61 73 73 = grangkn9974 page												
000001c0: 72 61 66 53 65 34 31												
Expert Decode (Matrix Host Table) Protocol Dist.) Statistics /												

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。