



# Iris 使用详解—基础篇

作者：劲刀狂舞 (webmaster@heihoo.com)

相关网站：黑狐网络 (<http://www.heihoo.com>)

eEye Digital Security (<http://www.eeye.com/iris/>)

大家都知道嗅探器吧。嗅探器的英文写法是Sniff，可以理解为一个安装在计算机上的窃听设备它可以用来窃听计算机在网络上所产生的众多的信息。简单一点解释：一部电话的窃听装置，可以用来窃听双方通话的内容，而计算机网络嗅探器则可以窃听计算机程序在网络上发送和接收到的数据。早在Win95时代就有一个叫做Netxary的嗅探器，不过这个拥有这个软件网络管理员（或是黑客）可以对经过自己计算机网络数据包进行接听或者编辑。不过这个软件有个缺陷，就是不再支持Win2K系统。许多原来用Netxary嗅探器的朋友就在网上询问什么软件可以做Windows的嗅探器。下面我给大家介绍一个叫做Iris的sniff软件。

## 一. 安装Iris

### 系统要求：

笔者使用的是IRIS 3.6版，以下也是参照这个版本而写。大家可以在<http://www.xfocus.net/download.php?id=275>得到，或者到软件的网站上下载 (<http://www.eeye.com/iris/>)，大小3.7mb。

### 软件环境：

Windows 95/98/NT/2000

Internet Explorer 4.x AND comctl32.dll version 5.00 或者更高

或者

Internet Explorer 5.x.

### 最小安装：

Pentium 166, 32MB RAM, 1GB HDD

### 推荐安装

Pentium 400, 128MB, 10 GB HDD

### 额外推荐：

系统使用最新的service packs，补丁程序和Internet Explorer。

拥有一块支持以太网络的网络配置器。

### 在网络的什么位置可以安装Iris：

1. 在你的网络边缘，例如交换机和路由器之间。
2. 你不可在交换机组成的网络安装。因为交换式网络对于sniffer有一定的免疫，所以你不会得到任何其他主机的数据。不过有些特殊端口的数据将会被所有主机得到，在这种情况下你可以进行嗅探。
3. 安装在你的防火墙上。安装两个Iris在你的防火墙的前段和后端，随时监视数据包的情况，可以保护你的防火墙。

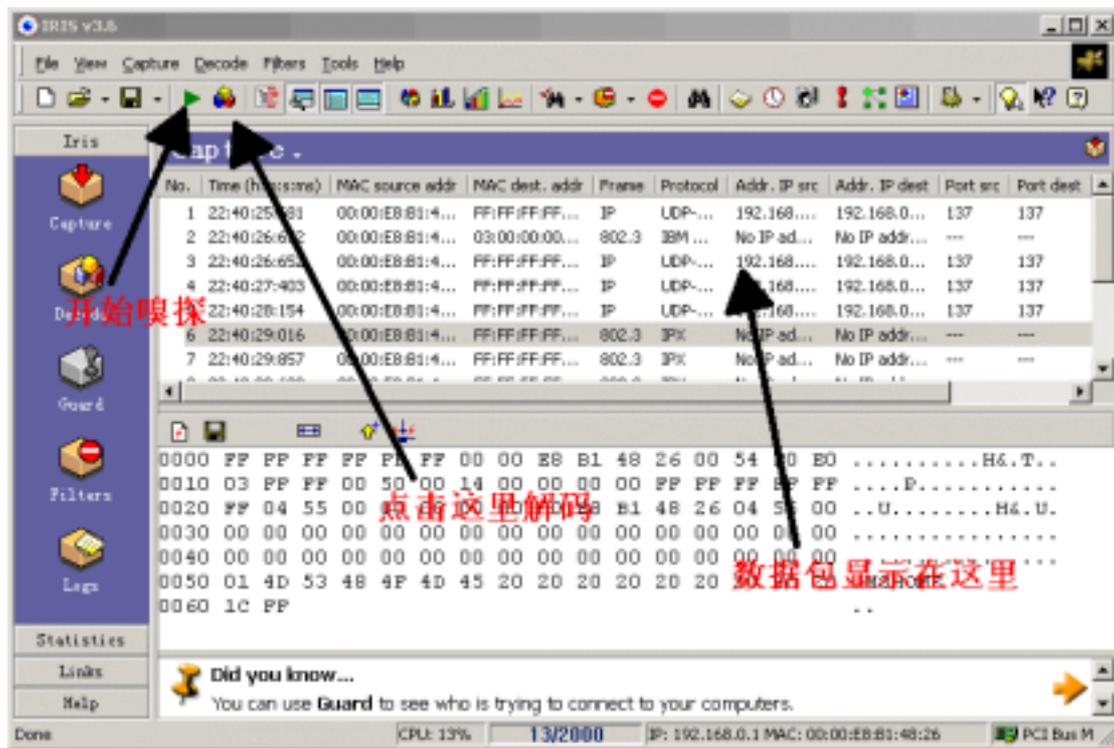
4. 安装在共享式集线器组成的网络中。这个是传统的安装地点，例如你有三个网络端口，其中你的主机安装了Iris，另外的两个端口的信息你就可以用Iris得到。

### 执行安装：

由于这个软件不是免费版本，所以我们需要得到注册码。到官方网站上去注册，或者通过别的途径都可以得到注册码。我们一路回车就可完成安装。

## 二. 使用Iris监视网络

我们假设是默认安装，点击开始>程序>Iris，选择点击Capture > Start (Ctrl-A)。我们开始截获我们网络中的数据包。如图一所示：



图一

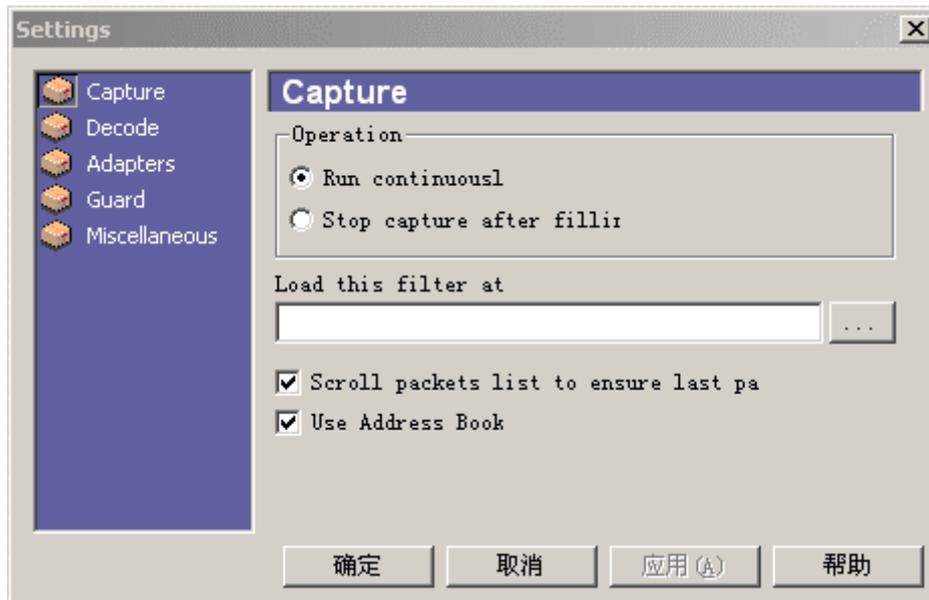
### 一.配置Iris

在Iris中有很多的需要用户配置，众多的选项的配置主要的目的就是使得用户得到自己想要的数帧，过滤掉不想要的协议和关键字。

下面我们讲一讲怎样整体配置IRIS。打开tools> Settings, 选择指定模式进行配置。当你配置完成，点击ok进行确定。

#### 1. Capture (捕获)

如图二所示：



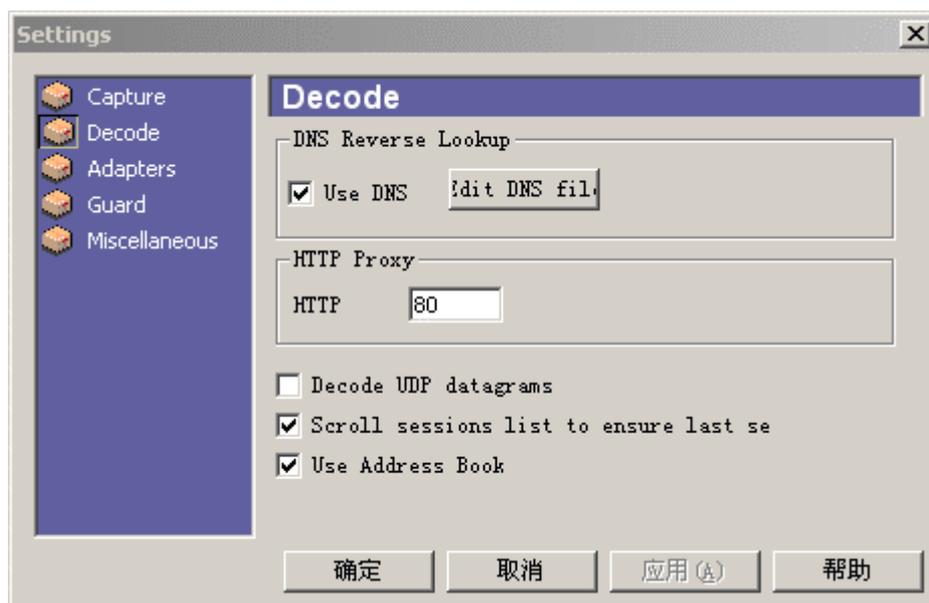
图二

选项	功能描述
Run continuously	当缓冲区溢出时，Iris将覆盖原来的数据包。
Stop capture after filling buffer	当缓冲区溢出时，Iris将停止进行数据包截获，并停止纪录。
Load this filter at startup	导入过滤文件并应用，这样我们可以看到命令行方式的调试。
Scroll packets list to ensure last packet visible	一般选中，使用这种模式可以使新的数据包截获后，软件会记住以前的数据包并显示不删除。
Use Address Book	Iris将会使用Address Book来保存mac地址，软件会记住mac地址和网络主机名。Ip会被解释成netbios名字。

表1

## 2 . Decode ( 解码 )

如图三所示



图三

选项	功能描述
Use DNS	使用域名解析
Edit DNS file	使得域名解析本地化，使用这个选项可以编辑本地解析文件。
HTTP proxy	使用http使用代理服务器，编辑端口号。默认为80端口
Decode UDP Datagrams	使得解码器支持UDP协议
Scroll sessions list to ensure last session visible	选择这个选项使得最新截获的数据帧显示在捕获窗口的最上。
Use Address Book	同Capture中的Use Address Book

表 2

### 3 . Adapters (网络配置器)

如图4所示：

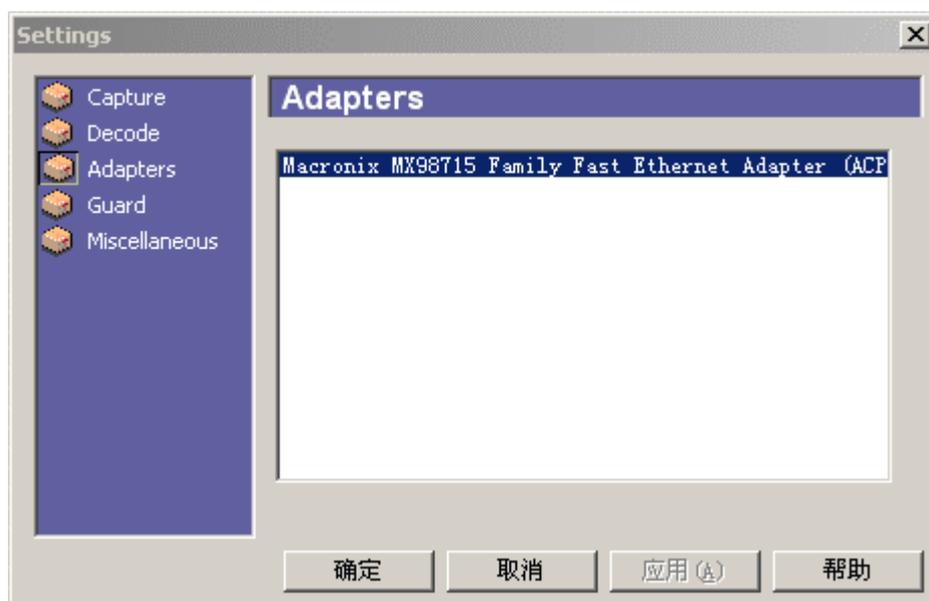


图4

选择你想从哪个网络配置器中截获数据，如果你有其他的网络设备可以在被选框中选择。例如图4中就是笔者的tp-link网卡。

#### 4 . Guard ( 警报和日志选项 )

如图5所示：



图5

选项	功能描述
Enable alarm sound	当发现合乎规则的数据包发出警报声音
Play this wave file	选择警报声音路径，声音格式是wav文件
Log to file	启动日志文件。如果选中后，当符合规则的数据包被截获后将被纪录并保存。
Ignore all local connections	Iris会通过本地的ip地址和子网掩码识别地址是否是本地的地址。这个选项指对Guard时有效，以后我们会提到。当这个选项被不选中后，Iris会接受所有的数据包，不管数据是否来自本地。如果选中，将不接受本地网络的数据包。
Ignore connections on these ports	忽略指定端口(port)，在列表中可以选择不。
Use software filter	当此处被选中后，软件过滤方案会生效。当没有被选中后，软件将会接受所有的数据。值得注意的是：只有当Apply filter to incoming packets 被选中后Use software filter才能使用，以后我们将介绍。

表3

#### 5 . Miscellaneous ( 杂项功能 )

如图6所示：



图6

选项	功能描述
Packet buffer size	在缓冲区可以保存的包裹数量（默认值是2000个）
Stop when free disk space drops bellow	当磁盘空间低于指定值时,Iris将会停止捕获和记录数据。这个选项可以很有效的防止恶意用户进行对Iris的拒绝服务攻击。不过值得注意的是当decode选项打开时,Iris会建立一个临时文件夹进行纪录。当我们退出软件后,文件才会删除。
Enable CPU overload protection	当Cpu的占用率连续4秒钟达到100%时,后软件将对计算机进行保护,即停止运行。等到恢复正常后才开始纪录。
Start automatically with Windows	点击这里可以把Iris加入到启动组中。

表4

## 二. 使用日志列表

如图7所示：

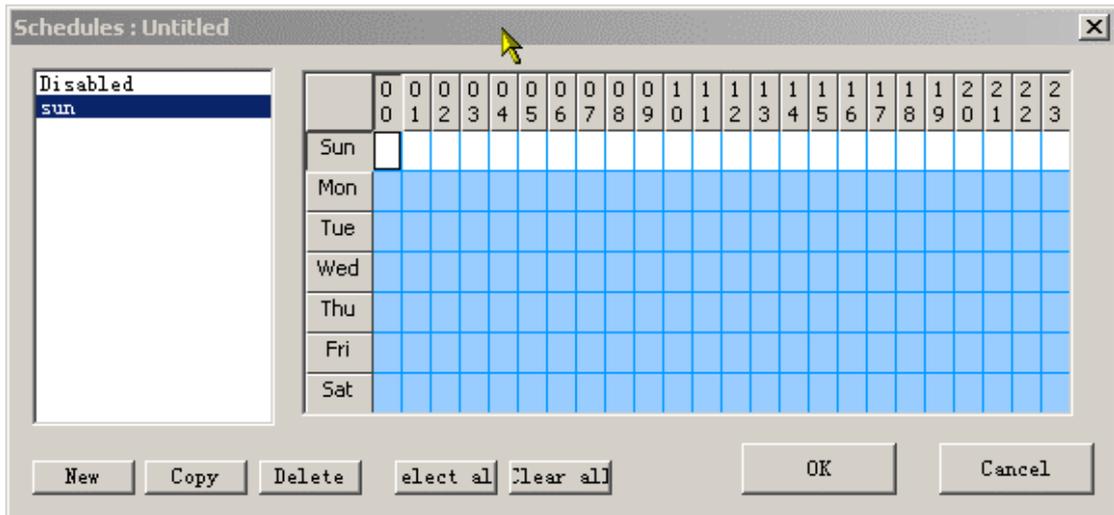


图7

使用这个功能可以配置Iris指定的时间捕获数据包,蓝色代表捕获,白色代表停止捕获。在上边的例子中我们可以清楚地看到,管理员指定Iris除了星期日,其他的时间里都处于捕获运行状态。

### 三. 使用数据包的截获功能

在数据包编辑区内,显示着完整的数据包。窗口分两部分组成,左边的数据是以十六进制数字显示,右边则对应着ASCII。点击十六进制码的任何部分,右边都会显示出相应的ASCII代码,这个以便于我们进行分析。十六进制码是允许用户进行编辑再生的,你可以重写已经存在的的数据包。新的数据包可以被发送,或者保存到磁盘中。

如图8所示

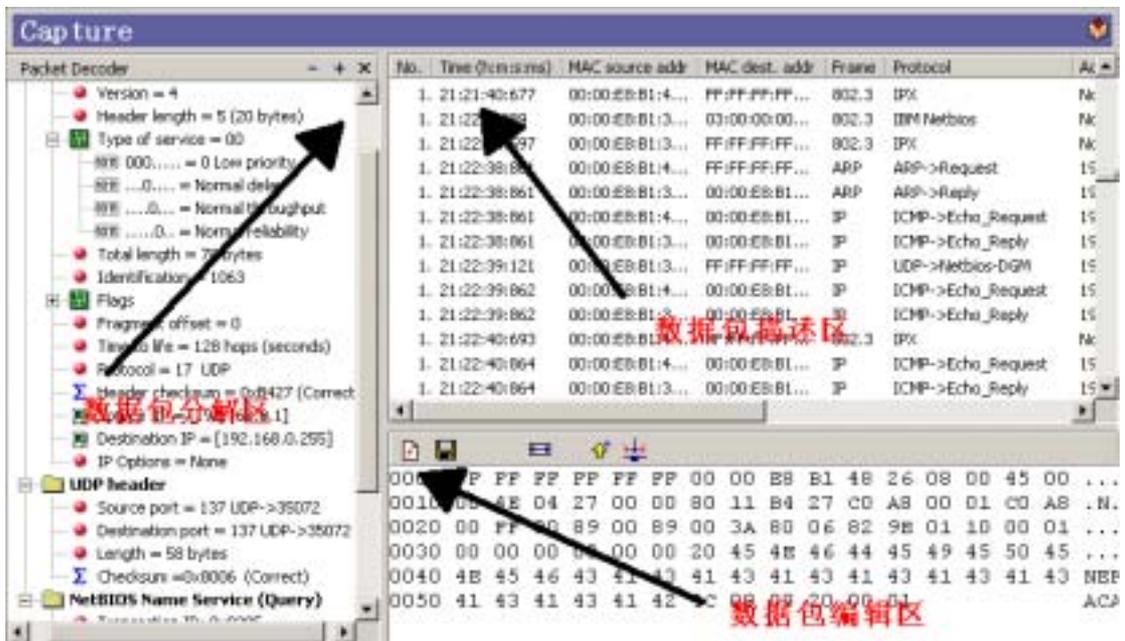


图8

#### 1. 数据包解码(Packet Decoder)

请看上图中的数据包分解区,在这里数据包根据OSI七层模型被分解成个若千的部分。每一个数据包的包头(MAC, IP, ICMP, TCP, and UDP)将会在这里显示出来。(如图9所示)

如果数据包编辑区也显示出来，数据包分解区将会和数据包编辑区合作，进行数据相关联。其中被选择的部分将会被红色标亮，以便区分。如果你想了解更多有关数据包的结构，请参看有关的书籍。如果此区域被隐藏，请点击 **Capture**，选中其中的钉书钉就可以显示出来。

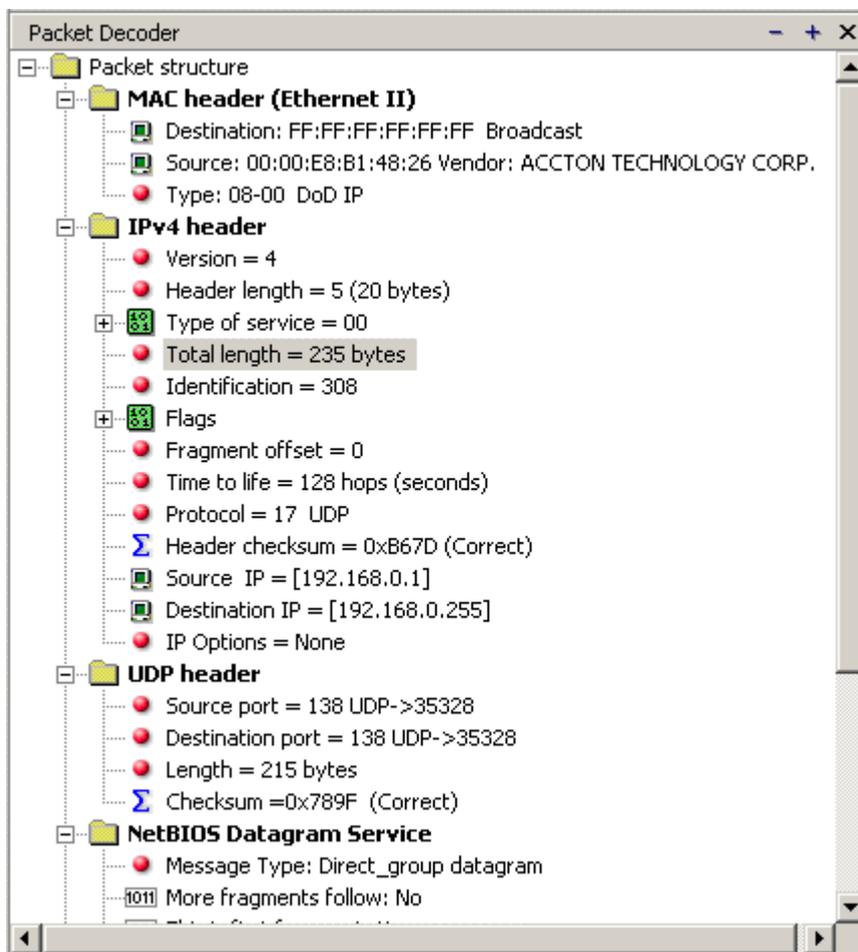


图9

## 2. 捕获数据描述区 ( Capture Window )

这个区域可以描述出你所截获的数据包的收发地址，端口，协议等。你能选择每一个数据包点击右键来执行不同的命令。我们可以进行脱放，修改，删除，做标记等。如图10所示：

No.	Time (h:m:s.ms)	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP src	Addr. IP dest
3.	14:13:31:406	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
3.	14:13:32:287	ACCTON-b14826	FF:FF:FF:FF...	802.3	IPX	No IP address	No IP address
3.	14:13:33:129	ACCTON-b14826	FF:FF:FF:FF...	802.3	IPX	No IP address	No IP address
3.	14:13:33:970	ACCTON-b14826	FF:FF:FF:FF...	802.3	IPX	No IP address	No IP address
3.	14:13:34:811	ACCTON-b14826	03:00:00:00...	802.3	IBM Netbios	No IP address	No IP address
4.	14:13:34:811	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
✓ 4.	14:13:35:562	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
4.	14:13:36:313	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
4.	14:13:39:167	ACCTON-b14826	03:00:00:00...	802.3	IBM Netbios	No IP address	No IP address
4.	14:13:39:167	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
4.	14:13:39:918	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
4.	14:13:40:669	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255
4.	14:13:41:521	ACCTON-b14826	03:00:00:00...	802.3	IBM Netbios	No IP address	No IP address
4.	14:13:46:047	ACCTON-b14826	FF:FF:FF:FF...	IP	UDP->Netbios-NS	heihoo	192.168.0.255

图10

我们用鼠标右键单击区域一，还可以调整捕获数据描述区的各类选项属性。

### 3.数据包编辑区 (Packet Editor)

这个区域可以在Capture > Show Packet Editor点击显示出来。我们选择一块区域点击右键，除了正常的c&p操作外还有一个 Copy to C style 的选项，这个可以使得十六进制的编码转化成c语言的形式，例如：E8 B1 48 26 08 Copy to C style 后得到 \xE8\xB1\x48\x26\x08，这个有利于我们进行网络编程时使用。

在此区域的工具条上还有几个选项，其中是数据包空生成和删除的选项。利用工具条的其他选项可以进行数据包的保存，更改，加入到列表和发送等操作。例如黑客想生成一个TCP数据包，首先点击生成一个空数据包，参照RFC792的数据包格式，使得每一部分都用十六进制表示法来表示。理解一下这个结构，我们机建立了一个包假设它由100个字节的长度（我们假设一下，20 个字节是IP信息，20个字节是TCP信息，还有60个字节为传送的数据）。现在把这个包发给以太网，放14个字节在目地MAC地址之前，源MAC地址，还要置一个0x0800的标记，他指示出了TCP/IP栈后的数据结构。同时，也附加了4个字节用于做CRC校验（CRC校验用来检查传输数据的正确性），其余的用00补齐。如图11所示：

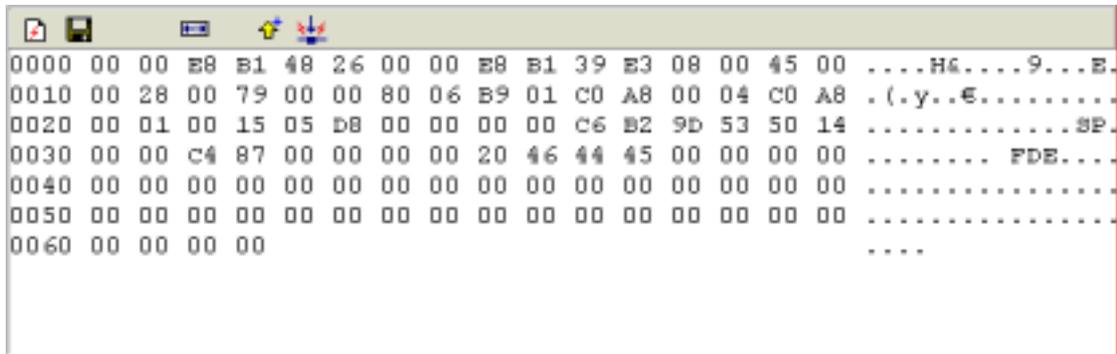


图11

之后我们点击发送按钮IRIS会出现如图12所示的窗口：

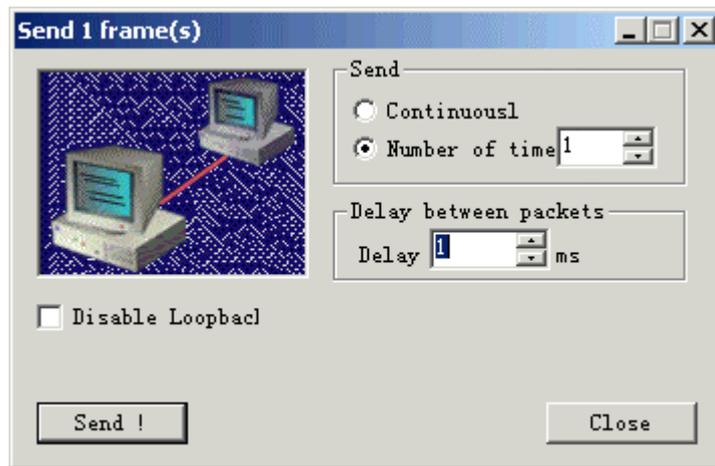


图12

功能如表5所示：

选项	功能描述
Send Continuously	发送器会一直发送你所选择的数据包直到你点击Stop
Send Number of Times	选择你想发送的次数

Delay between packets	设置连续连个数据包的相隔时间，单位是毫秒（ms），如果这个选项设置成0，那么IRIS会用最快的速度发送。
Disable Loopback	不接收你自己计算机发送的数据包
Send和Stop	发送和停止选项

表5

## 三.解码、重新构建捕获数据

看过这个部分我们可以做到，把数据帧进行解码可以很直观的看清楚截获的每一个会话（主要是HTTP），就好像使用自己会话一样。

### 1. 解码概况

众所周知TCP提供一种面向连接的、可靠的字节流服务。也就是说一个普通的会话形式（例如，下载网页），整个过程之前一定是建立了一个连接，会话结束在销毁这个连接。当两个主机建立了一连接之后，互相之间才可以发送数据，直到连接中断。丢失或受损的数据包都被重传。如有必要，进来的数据包被重组，以便与原来的传输顺序匹配。顺序是按每个数据包中的序列号(sequence number)来维系的。每个被发送的字节，以及开放和关闭请求，均被单独标上不同的序列号。传统的Sniffer只是可以提供一个数据包序列号和信息的截获信息的描述，给管理员一个关于这个会话的判断。而IRIS则远远超出了这一层次，软件可以重新组织HTTP协议中的数据，进行填充、着色使得数据被还原成网页。当然这种功能也可以用在其他的方面，例如重新构造Email的附件等。

### 2. 对截获的数据进行解码

设置DECODE选项，如果你不熟悉请仔细看看上面的文字。下面启动DECODE选项，只有我们打开Decode > Enable Code Output时，才能使解码进行。

这里主要是由三个窗口组成：主机行为窗口（Host Activity）、查看会话窗口（Session Data）和会话列表窗口（Sessions View）。

#### 1. 主机行为窗口（Host Activity）

如图13所示：

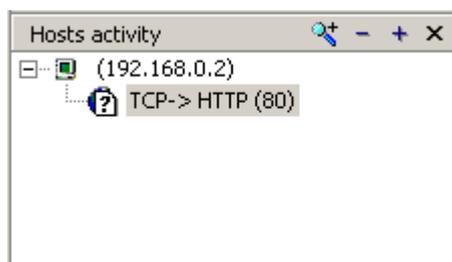


图13

这个窗口把会话以树形排列，每一个小项代表一个服务（通常是使用同一个端口的协议）。当我们在这个窗口选择了一个服务（如图13），在数据列表窗口就会相应的显示出服务器和客户端的会话。

#### 2. 查看会话窗口（Session Data）

如图14所示：

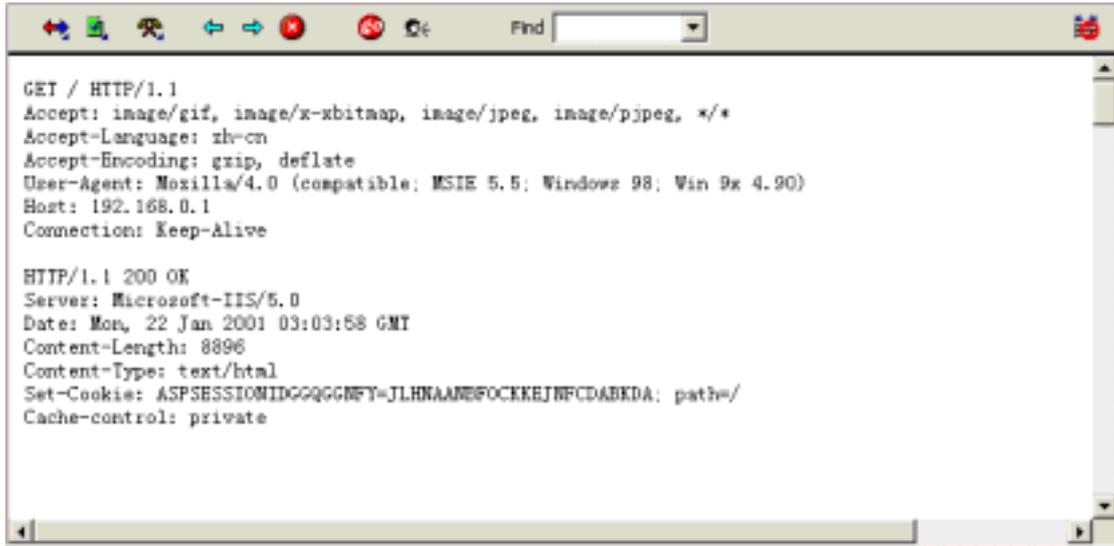


图14

这个窗口显示我们截获的每一会话的具体信息。在我们上面的图中，IRIS截获了一个HTTP的会话。你可以看到客户端发出的浏览请求和WEB服务器的回应。

下面我们介绍一下这个窗口主要的工具条选项的作用：

选项	功能描述
	你在这个选项下，可以单纯选择一个会话的客户端或服务端的数据。默认是双向的。
	可以使得会话以各种编码显示，可选择HTML，ASCII，Packets三种。其中HTML适合显示WEB相关的会话，是默认格式。ASCII是8 Bit的编码，不适合显示HTML的文档，适合显示HTML标签。Packets显示成数据包原来的形式。合理使用编码转换会使得我们更直观的理解数据包的内容，例如，当我们截获一个发送ai l的数据包，当我们用HTML显示时MAIL FROM:和RCPT TO就不会被看见，当我们转换了编码ASCII后就可以正常显示了。
	得到会话的相关资源

表6

其它的功能很容易理解，例如查找指定字符等，读者可以自行操作。

### 3. 会话列表窗口 (Sessions View)

这个区域可以描述出你所截获会话的收发地址，端口，协议等。形式和截获数据包的窗口差不多在这里不做赘述。

我们截获了数据经过以上步骤就可以使得数据包由抽象变得形象了。

## 四.监测连接状态

我们首先要在Click Tools > Guard > Guard Settings配置，在文章的前面可以找到相关配置。IRIS还可以充当入侵监测装置，我们打开Tools>Guard>enable Guard使其生效。打开Tools>Guard>Show Guard windows开启监视窗口。如图15所示：

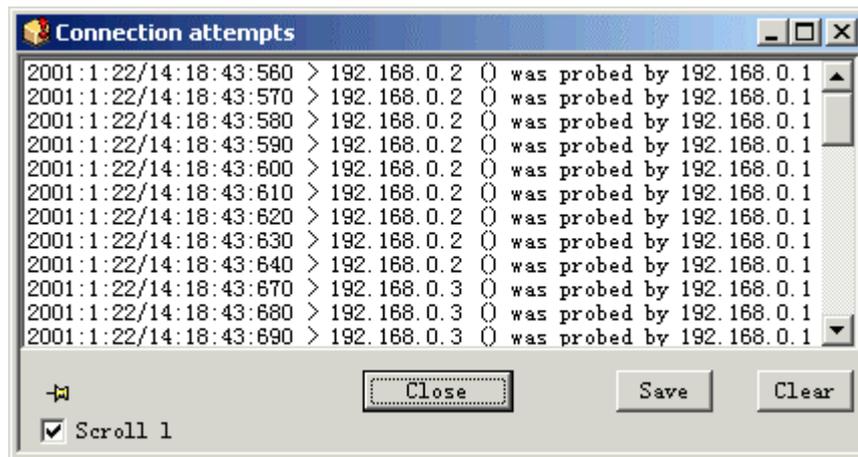


图15

主机192.168.0.2和192.168.0.3被192.168.0.1进行了端口扫描。

以上我们介绍了IRIS的基本使用方法，主要还是介绍用户的基本操作，不过IRIS的功能还有很多，我们将在《Iris使用详解—提高篇》中介绍。