科来

科来数据包生成器

快速入门指南

科来
电话：400-6869-069
网址：http://www.colasoft.com.cn
邮箱：support@colasoft.com.cn

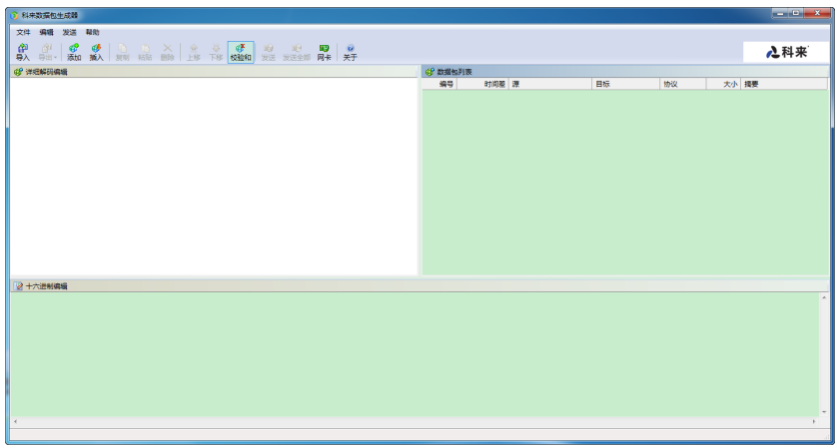
1 快速启动

科来数据包生成器是科来网络分析系统免费提供的网络数据包生成工具。它能够构造各种数据包，或直接对网络中捕获的数据包进行数据值编辑。用户使用科来数据包构造器可以构造出各种特殊的数据包，可用于网络性能测试、应用模拟或演示教学等等。

科来数据包生成器的启动方法有以下三种：

- 开始->科来网络分析系统程序菜单->科来网络分析系统工具集->数据包生成器；
- 启动科来网络分析系统->开始分析->工具->数据包生成器；
- 开始->运行->输入“pktbuilder”命令并确认。

数据包生成器启动后的初始界面如下图所示：



如上图所示，科来数据包生成器的使用界面由数据包列表窗口、详细解码编辑窗口、十六进制解码编辑窗口三部分构成。其中详细解码编辑窗口、十六进制解码编辑窗口都依附于数据包列表窗口，用户可以在数据包列表窗口选择数据包文件后，通过其它两个编辑窗口进行数据包的编辑。科来数据包生成器支持用户使用鼠标拖拽的方式，任意调整三个窗口之间的位置。

在科来数据包生成器中您可以添加数据包、编辑数据包、发送数据包、导出数据包。

2 添加数据包

科来数据包生成器提供了以下 3 种添加数据包的方式，具体使用方法如下：

- 新建数据包

新建数据包是指使用科来数据包生成器提供的模板，进行数据包的添加。您可以通过工具栏或数据包列表窗口右键菜单中“添加”或“插入”的进行数据包的新建。

使用“添加”新建的数据包会出现在数据表列表的最后位置，而使用“插入”新建的数据包会出现在当前所选数据包的前一位置。

选择“添加”和“插入”都会弹出一个对话框，如下图：

该对话框中有个 2 个选项：

选择模板：科来数据包生成器提供了 ARP、IP、TCP、UDP 四种常见的数据包模板，您可以在新建数据包时进行选择。

时间差：设置数据包回放时，两个数据包之间的时间间隔。

两个选项都选择完毕后，按下“确定”键，数据包就新建成功了。此时，数据包列表窗口中将增加一条数据包记录。

- 导入数据包

科来数据包生成器支持导入外部的数据包文件。您可以通过工具栏的进行外部数据包的导入。 目前科来数据包的导入格式支持以下 12 种：

Accellent 5View Packet File(*.5vw)

Colasoft Packet File (*.rapkt;*.cscpkt;*rawpkt;*cscproj)

EthePeek Packet File(V7/V9) (*.pkt)

HP Uinx Nettl Packet File (*.TRCO;TRC1)

libpcap(Wireshark,Ethereal,Tcpdump,etc.) (*.cap;*.pcap)

Wireshark(Wireshark,etc.) (*.pcapng;*.pcapng.gz;*.ntar;*.ntar.gz)

Microsoft Network Mintor 1.x,2.x (*.cap)

Novell LANalyzer (*.tr1)

Network Instruments Observer V9.0 (*.bfr)

NetXRay2.0 and Windows Sniffer (*.cap)

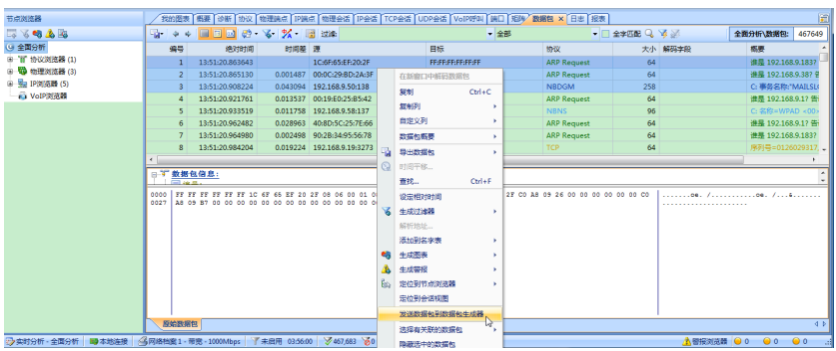
Sun_Snoop (*.snoop)

Visual Network Traffic Capture (*.cap)

- 接收科来网络分析系统发送的数据包

如果您正在运行科来网络分析系统，并希望将部分数据包添加到科来数据包生成器。则可以切换到科来网络分析系统的数据包视图，选中需要发送的数据后，点击鼠标右键，在右键菜单中选择“发送数据包到数据包生成器”。科来数据包生成器会被自动开启，并把选中的数据包添加到科来数据包生成器。

如下图：



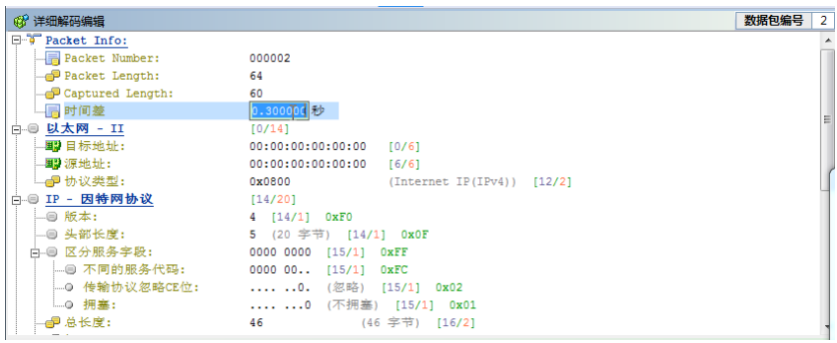
数据包添加完成后，您可以通过工具栏中的上移、下移对已添加的数据包进行位置调整；也可以通过数据包列表窗口的右键菜单，进行数据包位置的移动、列表展示字段的自定义、删除数据包等。

3 编辑数据包

数据包添加成功后，选中需要编辑的数据包，科来数据包生成器会将所选数据包文件进行解码，您可以在详细解码编辑或十六进制解码编辑窗口进行数据包的编辑。

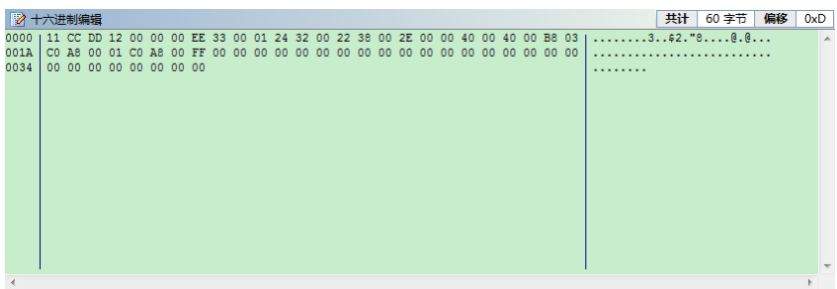
- 详细解码编辑窗口

在详细解码窗口中，科来数据包生成器已经将所选数据包文件进行详细解码，您可以选中数据包中需要编辑的字段信息（如：时间差、目标地址、区分服务字段等），按需要进行编辑。但是编辑数据包时，您需要根据数据包中该字段的标准格式来编辑，否则系统将不会保存输入的信息。编辑窗口如下图：



- 十六进制解码编辑窗口

在十六进制解码编辑窗口中，您可以直接对数据包的十六进制解码和ASCII 码进行编辑，但是这种编辑方法，需要您对协议结构和数据包的手动解码非常熟悉。编辑窗口如下图：

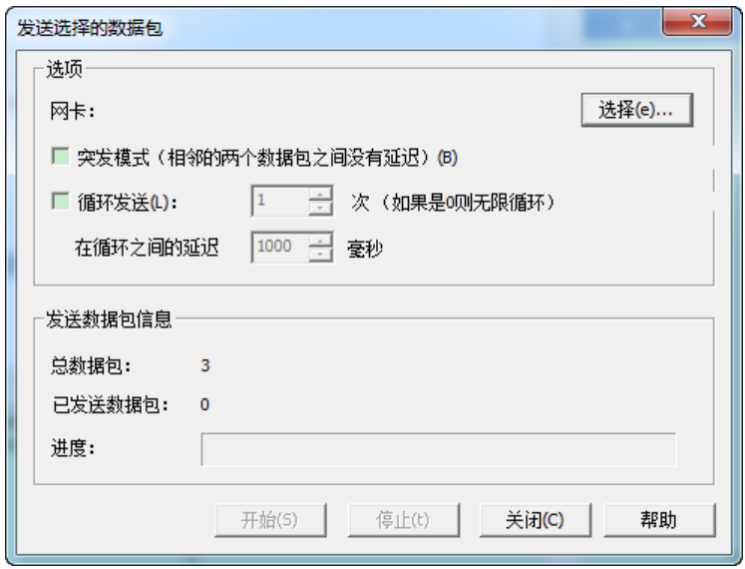


4 发送数据包

数据包生成器中,您可以在数据包列表窗口选择部分或者全部数据包通过指定的网卡发送到网络。需要发送数据包时,您可以使用工具栏中的“发送”或“全部发送”按钮。

使用“发送”时,仅发送选中的数据包;使用“全部发送”时,发送所有数据包。

选择“发送”或“全部发送”后,都会弹出发送数据包的设置对话框,如下图:



在以上的设置对话框中,分为选项和发送数据包信息两部分。

- 选项

数据包发送前,对发送数据包的网卡、数据包的发送方式等进行设置;

网卡:科来数据包生成器,提供了发送数据包网卡的选择功能。点击上图设置对话框中,“网卡”最右边的“选择”按钮,会弹出选择网卡的对话框,如下图:

您的主机有多张网卡时，可以通过对话框中的下拉菜单，选择不同的网卡。页面中显示的网卡详细信息，会根据选择的网卡自动切换。

突发模式: 系统默认没有启用，启用突发模式后，发送数据包时会忽略数据包之间的时间延迟，实现快速发送。

循环发送:

循环次数 :设置数据包循环发送的次数 ,系统默认设置为 1 次 ,用户可在 0～10000 次范围内设置，设置 0 表示无限循环；

在循环之间的延迟：设置每次循环发送之间的时间间隔，系统默认设置为 1000 毫秒，用户可在 0～600000 毫秒范围内设置

- 发送数据包信息

“发送数据包信息”是在数据包发送时显示数据包的发送情况。通过“发送数据包信息”您可以更清晰的了解数据包的发送情况，比如总数据包，已发送数据包以及发送进度，如下图：

以上图中的发送数据包为例：

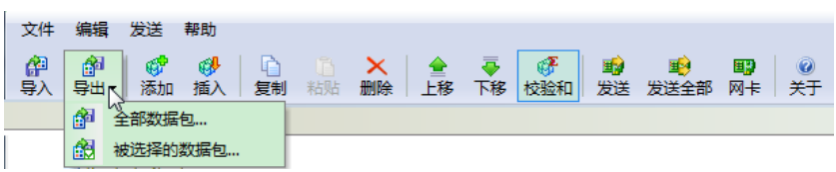
总数据包：总数据包的表示方式为：8*1000=8000。8*1000 表示 8 个数据包循环发送 1000 次，总共有 8000 个数据包，

已发送数据包：显示已发送的数据包个数及等待循环的时间。

进度：形象的显示数据包的发送进度。

5 导出数据包

科来数据包生成器支持对编辑后的数据导出到本地保存。需要导出数据包时，您可以点击工具栏中的“导出”按钮。点击后，将会弹出子菜单，如下图：



全部数据包：导出数据包列表窗口中的所有数据包；

被选择的数据包：导出数据包列表窗口中被选中的数据包；

选择“全部数据包”或“被选择的数据包”后，可以进行数据包的保存。目前科来数据包的导出格式支持以下14 种：

libpcap(Wireshark,Ethereal,Tcpdump,etc.) (*.cap;*.pcap)

Accellent 5View Packet File(*.5vw)

Colasoft Packet File(V3) (*.rapkt)

Colasoft Packet File (*.cscpkt)

Colasoft Raw Packet File (*rawpkt)

Colasoft Raw Packet File(v2) (*rawpkt)

EthePeek Packet File(V9) (*.pkt)

HP Uinx Nettl Packet File (*.TRCO;TRC1)

Wireshark(Wireshark,etc.) (*.pcapng;*.pcapng.gz;*.ntar;*.ntar.gz)

Microsoft Network Mintor 1.x,2.x (*.cap)

Novell LANalyzer (*.tr1)

NetXRay2.0 and Windows Sniffer (*.cap)

Sun_Snoop (*.snoop)

Visual Network Traffic Capture (*.cap)