

科来数据包生成器快速入门指南

什么是数据包生成器

科来数据包生成器是一个用于网络测试的网络数据生成工具，它可以生成各种的数据包，或 directly 对网络中捕获的数据包进行数据值编辑，目前是**目前最强**的数据包编辑器。用它可以：

网络测试：

生成 64 到 1518 字节的数据包，循环发送，来测试网络或关键设备对流量的承载能力。

错误或攻击测试：

生成错误的数据包，或从网络中采集攻击数据包，模拟故障网络，来调整网络安全策略。

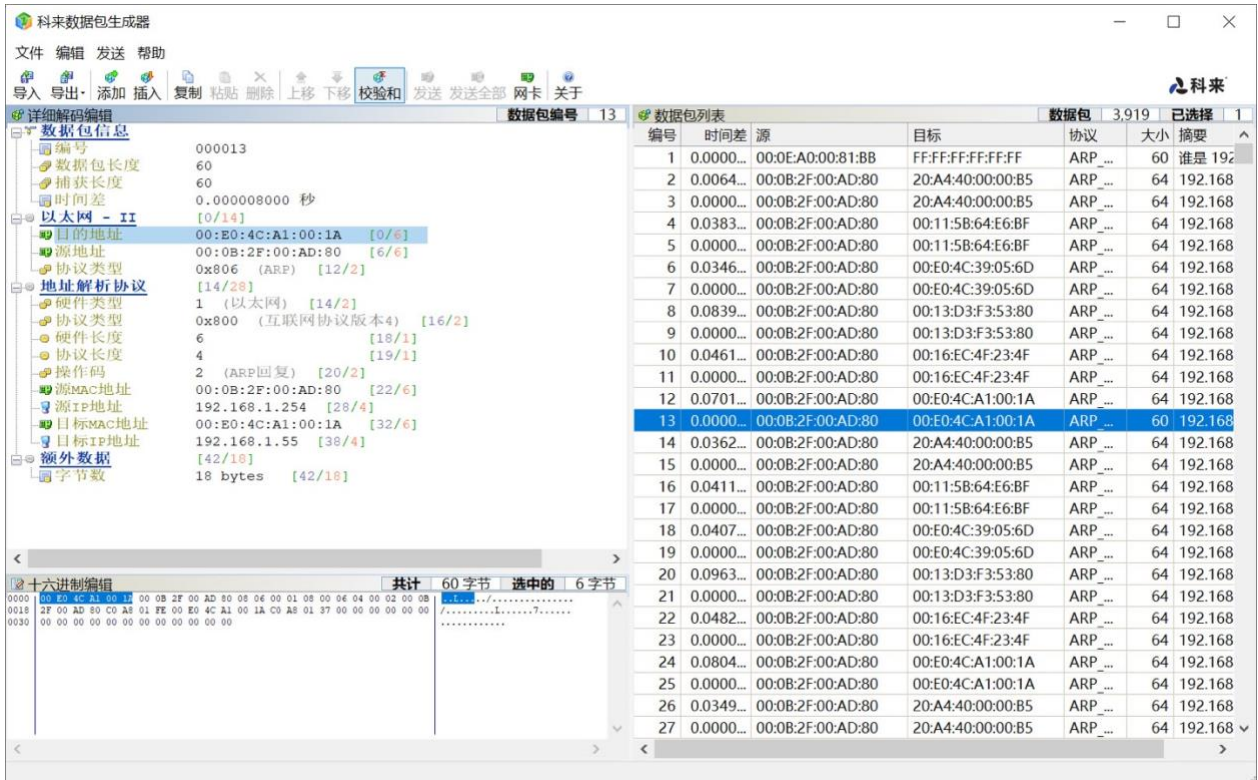
应用模拟：

可以截取网络中的各种应用进行回放，如上网操作，邮件发送，FTP 传输等。

教学和演示：

结合科来网络分析系统，用于 TCP/IP 网络教学和网络传输过程的演示。

下载地址：<http://www.colasoft.com.cn/download/capsa.php>



快速使用数据包生成器

科来数据包生成器是科来网络分析系统 6.3 免费提供的-一个数据包构造工具，它可以对科来网络分析系统捕获的数据包进行编辑以及构造新的数据包文件。用户通过使用数据包生成器，可以构造出各种特殊的数据包来测试网络的性能等问题。

科来数据包播放器的启动方法有以下三种：

- 科来网络分析系统程序菜单->科来网络分析系统工具集->科来数据包生成器；
- 科来网络分析系统工具菜单->数据包生成器；
- 开始->运行->输入“pktbuilder”命令并回车。

启动数据包生成器后，其界面如下图所示。

使用界面由 3 部分构成：

- 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

下面 2 个编辑窗口依附于数据包列表窗口，用户可以选择一个或多个数据包文件通过下面两个编辑窗口进行详细的编辑。用户也可以根据需要使用鼠标任意调整三个窗口之间的位置。

在科来数据包生成器中，你能添加数据包、编辑数据包以及发送数据包：

1. 添加数据包

用户可以在数据包列表窗口导入已捕获的数据包，也可以使用数据包生成器提供的模板构造新数据包（目前提供了 4 种数据包模板：ARP、IP、TCP、UDP）。

用户可以通过工具栏或右键菜单中的“添加”和“插入”在数据包列表窗口中添加新的数据包。

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 2 个选项：

- **选择模板：**科来数据包生成器为用户提供了 ARP、IP、TCP、UDP 四种常见的数据包模板，用户可以在新建数据包时进行选择。
- **时间差：**用户可以为新添加的数据包设定时间差。

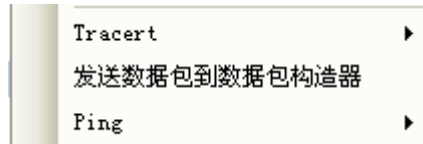
除了使用数据包模板添加新的数据包以外，用户还可以向数据包生成器直接导入已捕获的数据包。

数据包生成器可以导入外部的数据包文件，其支持导入的数据包文件格式如下：

- *.cscpkt（科来网络分析系统数据包文件）
- *.cpf（科来网络分析系统 4.0 数据包文件）
- *.cap（Network Associates Sniffer 数据包文件）
- *.pkt（EtherPeek/TokenPeek/AiroPeek 数据包文件）
- *.pkt（Etherpeek Packet File V7）

- *.pkt (Omnipeek Packet File V9)
- *.rawpkt (Raw 数据包文件)
- *.cap (Libpcap Tcpdump, Ethereal, 等通用数据包文件)
- *.cap (Microsoft Network Monitor 2. x)

用户也可以在科来网络分析系统的数据包视图中将捕获的数据包文件直接导入到数据包生成器中，如下图。



另外，用户可以在数据包生成器中随意调动数据包之间的位置。

2. 编辑数据包

在科来数据包生成器中，用户可以在详细解码编辑窗口和十六进制编辑窗口中编辑数据包。

- 详细解码编辑窗口

在详细解码编辑窗口，科来数据包生成器已经将所选数据包文件进行详细解码，用户可以很方便的在字段解码窗口中直接编辑，如下图。

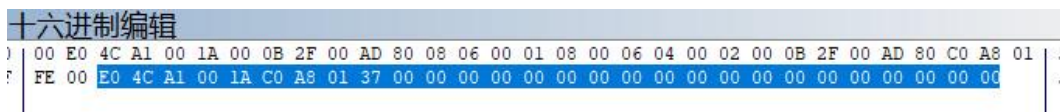



注意：用户在字段解码窗口编辑数据包时，必须根据数据包中字段的的标准来编辑，若输入错误的值，可使用 Esc 键取消，否则该字段编辑无效，并且提示如下信息，如下图。



- 十六进制编辑窗口

在十六进制编辑窗口中，用户可以直接对十六进制和 ASCII 码进行编辑，但是用户需要对协议结构非常熟悉并且懂的数据包的手动解码，如下图。



在编辑数据包时，科来数据包生成器默认启用了“自动计算校验和”的功能，若使用该功能系统自动计算并填入正确的校验和值。用户可以通过工具栏中按钮取消，若取消该功能，用户在编辑数据包时需手动填入系统自动计算出的校验和值，如下图。

窗口:	65535	[48/2]
校验和:	0xF079	(错误,应该是 0x0BFF) [50/2]
紧急指针:	0	[52/2]

3. 发送数据包

在数据包生成器中，用户可以将数据包列表窗口中的部分或者所有数据包通过指定的网卡发送到网络中。

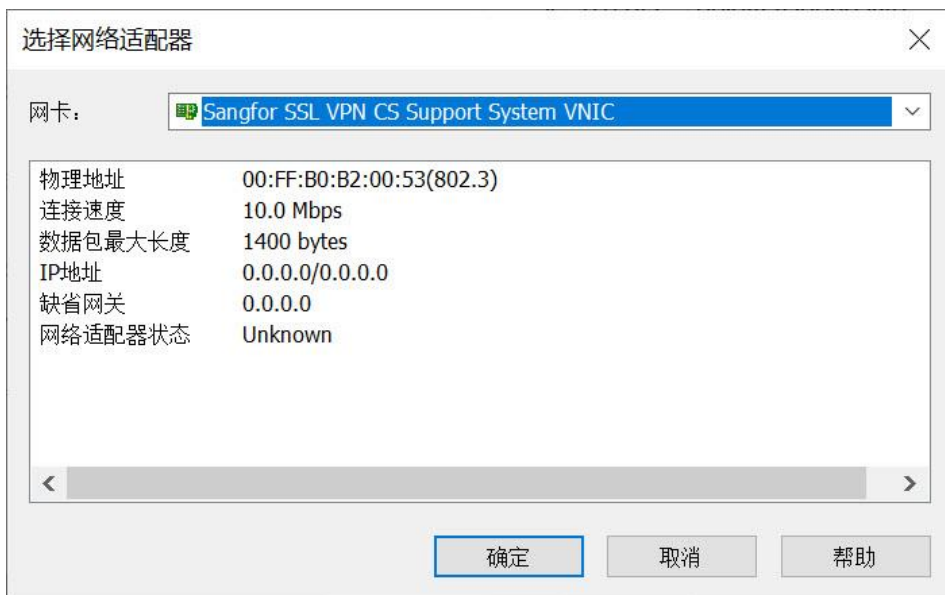
选择发送数据包按钮，系统将弹出发送数据包的设置对话框，如下图。



在图中的上方为设置选项信息：

- 选择网卡

第一使用数据包生成器发送数据包时，系统默认是没有选择网卡，用户需要手动选择发送的网卡，以后每次使用都会沿用上一次选用的网卡，选择网卡对话框对话框，如下图。



- 连续模式

在发送数据包时会忽略数据包之间的时间差，实现快速发送，系统默认没有启用。

- **循环发送**

用户可以设置发送数据的循环次数以及每次循环之间的时间间隔，系统默认没有启用。

循环次数： 设置所选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 范围内设置，设置 0 表示无限循环；

循环间隔： 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 范围内设置。

另外，在发送数据包设置对话框的下方，用户可以清楚的了解发送数据包的信息，比如总共的数据包数，已发送数据包数以及发送进度，如下图。



- 总共的数据包数：表示总共有 480 个数据包，8*40 表示 8 个数据包循环发送 60 次。
- 已发送数据包数：表示已发送 55 个数据包。
- 发送进度：形象的显示数据包的发送进度。

另外，科来数据包生成器可以将编辑好的数据包文件导出保存，目前只支持导出 (*.cscpkt) 格式的数据包。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统 (UPM)
- 科来网络回溯分析系统 (RAS)
- 科来网络分析系统 (CSNAS)

科来网络安全分析解决方案

- 科来网络全流量安全分析系统 (TSA)
- 科来APT攻击检测系统 (IDP)

CSNA 网络分析认证培训

科来网络流量分析技术资料

科来网络通讯协议图

科来网络攻击与防范图谱

CSNA 网络分析经典实战案例

科来网络故障诊断图

学习资料（视频教程、案例分析、数据包样本、文档资料）

术语表

科来网络流量分析产品下载(免费版)

科来网络分析系统

科来 Ping 工具

科来 MAC 地址扫描器

科来数据包播放器

科来数据包生成器

网络分析过滤器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。根据全球著名咨询与分析公司 Gartner 的评选，2018-2019 年，科来蝉联 Gartner NPMD 魔力象限“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影

响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

科来是最早研究木马数据流行为特征的厂家之一，在木马研究领域取得了丰硕的成果，承接了多项前瞻性科研项目。由于科来公司在网络安全领域的技术优势，受邀为“中国海军成立 70 周年阅兵”、“中非合作论坛”北京峰会、青岛“上合峰会”、“两会”、“十九大”、“G20 峰会”、“九三阅兵”、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 科来的技术服务于世界 110 个国家和地区
- 为全球 10000 余家商业客户提供网络分析解决方案
- 108 家世界 500 强企业选择科来

本文档所有内容均为科来公司独立完成，未经科来公司做出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、修改、存储、引入检索系统或者传播。

© 2003-2019 科来 保留所有权利 非商业应用

咨询电话：400-6869-069

官方网站：<http://www.colasoft.com.cn>

邮件地址：support@colasoft.com.cn