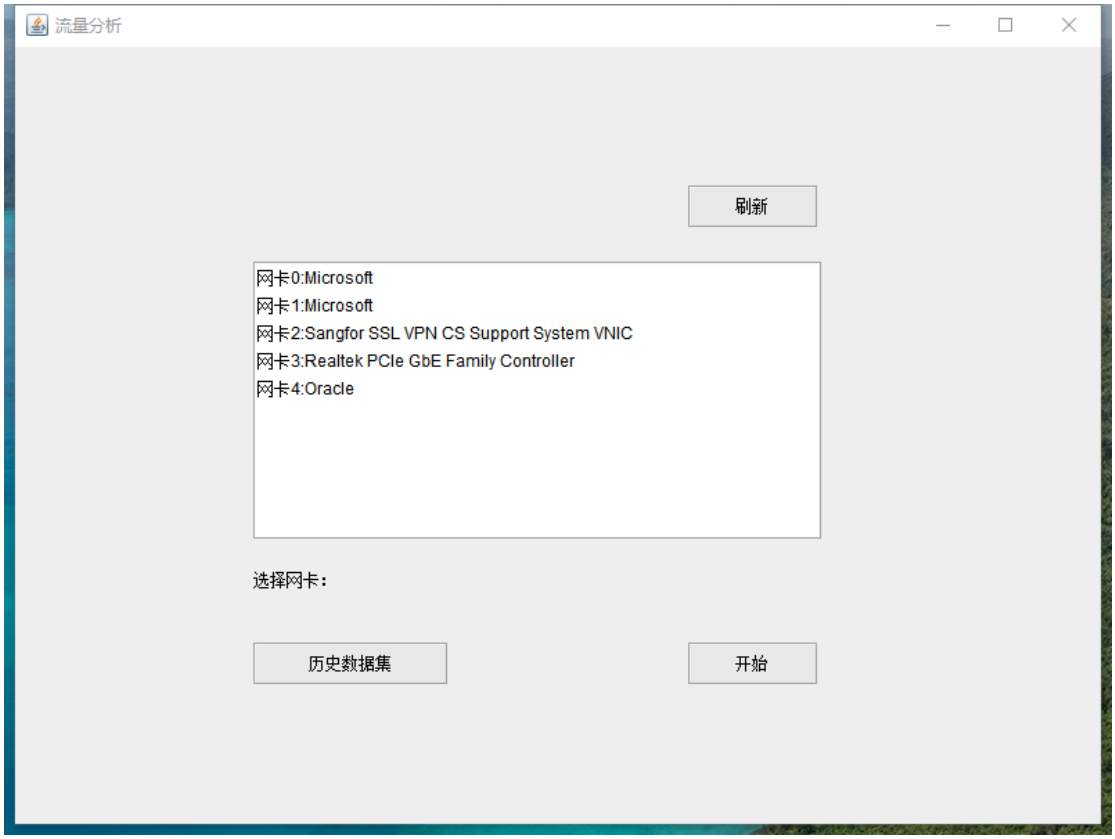
# 流量分析软件使用说明

**环境配置：**
Jdk 或 jre 等 java 运行环境，以及系统要安装 winpcap

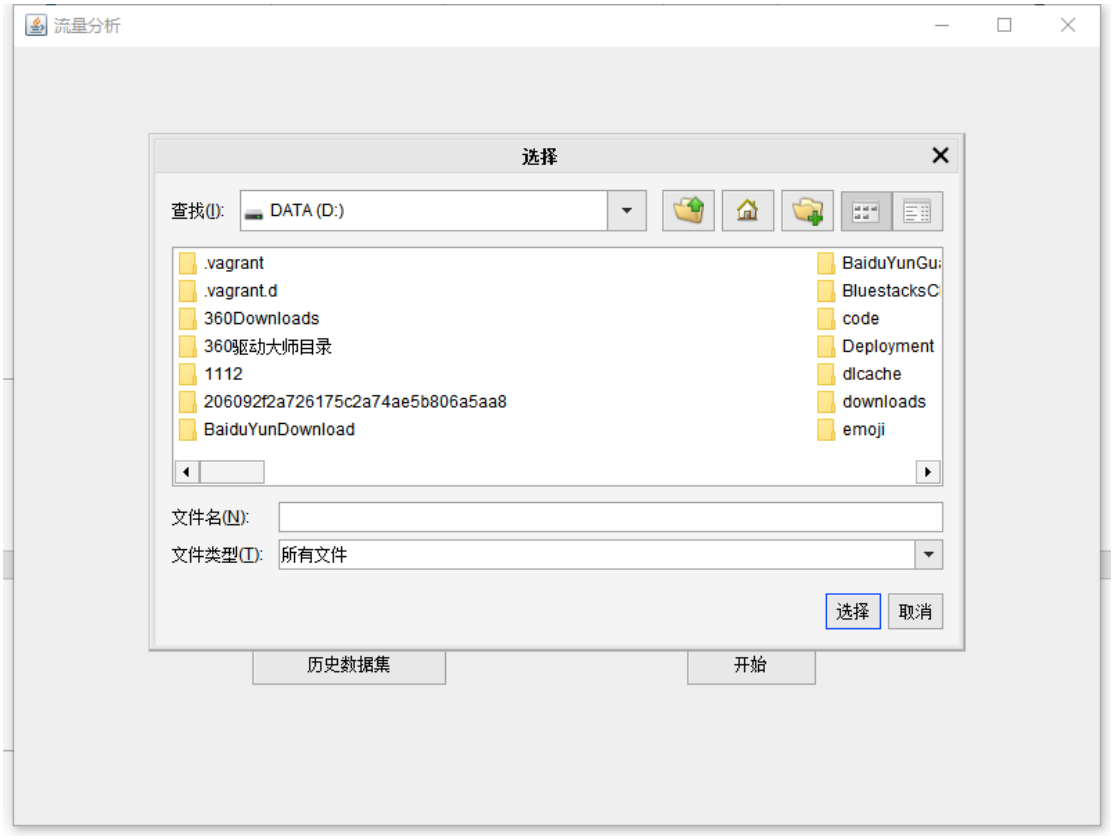
**请一定在 jdk 的 jre/bin 目录下添加 Jpcap.dll,否则软件无法正常工作!!!**
Jpcap.dll 可在 BIN 目录下找到。

**引用的 jar：**
jpcap.jar,jcommon.jar,gnujaxp.jar,jfreechart.jar,JTattoo.jar
其中 jpcap.jar 与获取数据包有关
jcommon.jar,gnujaxp.jar,jfreechart.jar 与绘图有关
JTattoo.jar 与主题有关

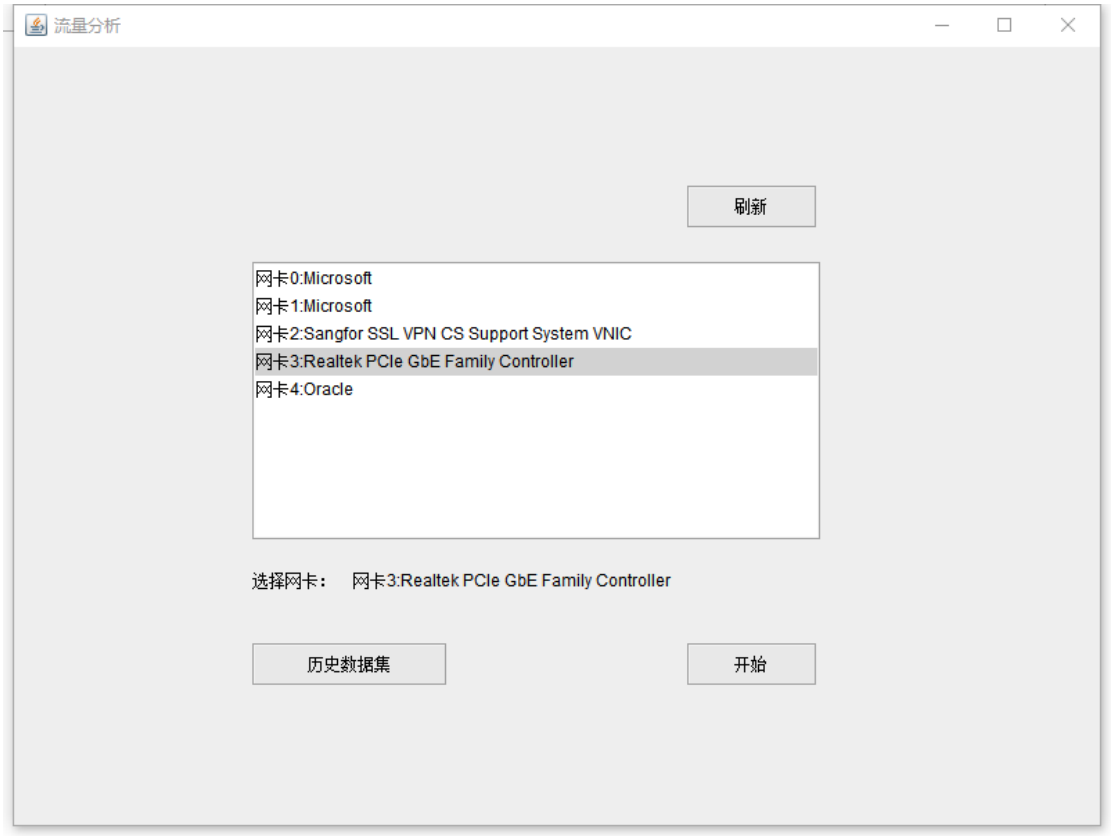
**使用方法：**
点击"流量分析.jar"，即可运行软件，进入主界面：
**主界面：**
软件会检测电脑的网卡，并显示在列表中，点击相应网卡即可选定。
点击刷新按钮会重新获取网卡。




“历史数据集“按钮是可以打开文件浏览窗口，并选择保存的数据集。


流量分析
选择
查找(I):
DATA (D:)
.vagrant
.vagrant.d
360Downloads
360驱动大师目录
1112
206092f2a726175c2a74ae5b806a5aa8
BaiduYunDownload
BaiduYunGu
BluestacksC
code
Deployment
dlcache
downloads
emoji
文件名(N):
文件类型(T):
所有文件
选择
取消
历史数据集
开始

点击选择一个网卡:


流量分析
刷新
网卡0:Microsoft
网卡1:Microsoft
网卡2:Sangfor SSL VPN CS Support System VNIC
网卡3:Realtek PCIe GbE Family Controller
网卡4:Oracle
选择网卡: 网卡3:Realtek PCIe GbE Family Controller
历史数据集
开始

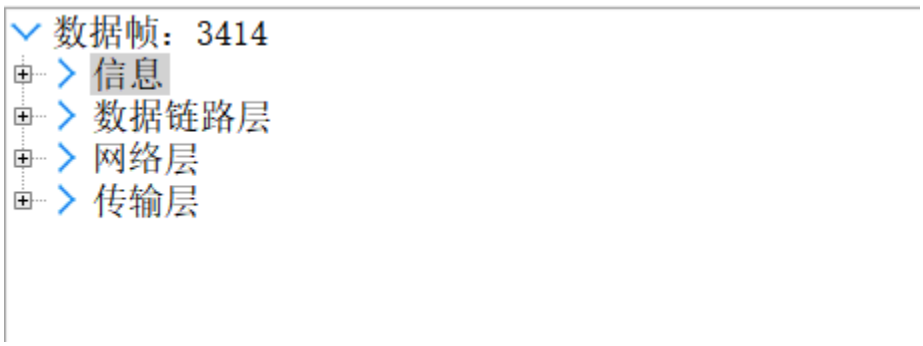
点击“开始”按钮，进入数据包展示界面

**数据包展示界面：**

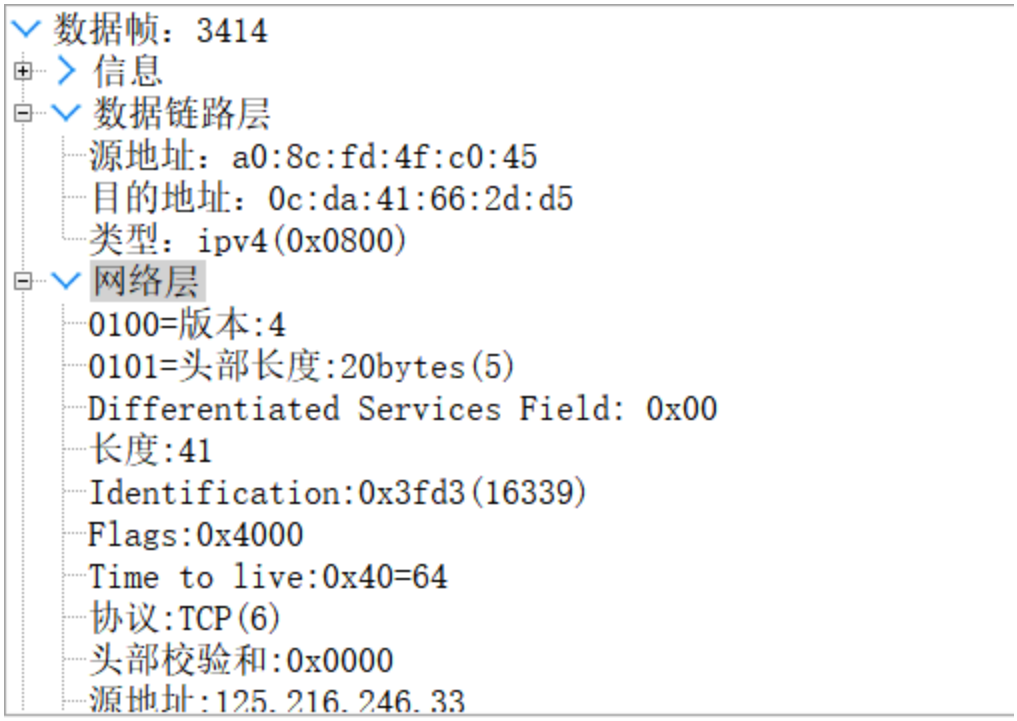

中间区域可以看到各种数据包，其中数据包种类与颜色的对应关系是：
TCP 数据包——绿色
UDP 数据包——黄色
ARP 数据包——橙色
ICMP 数据包——红色
Ipv4 数据包——蓝色
Ipv6 数据包——粉红色
其他类型数据包——灰色

单个数据包在表格上每一列分别代表：
数据包编号、数据包到达时间、数据包源地址、数据包源端口、数据包目的地址，数据包目的端口、数据包协议、数据包长度

点击单个数据包时，对数据包的分层解析与数据包的头部及数据内容会显示在下方：
**分层解析：**



点击树形标签可展开:




**数据展示**:
左方是 16 进制的数据，右方是对应的 ascll 码字符

```
header:
0cda41662dd5a08cf       ....Af-......
fd4fc045080045000       ..O..E....E..
00293fd3400040060       ..)?..@..@..
00007dd8f62108245       ....}....!..$
50d7d5f201bba736c       P.............6
c23b88a0368b50100       ..;....6..P..
0100cd100000    ............
data:
00      ..
```

在功能栏中，有“停止“按钮，可以停止获取数据包，并可以选择继续获取数据包或者保存数据集。

还有过滤框和过滤按钮，可以对已获取的数据包进行过滤显示，支持在获取数据包时过滤（动态过滤）与在停止时或打开历史记录时过滤（静态过滤）
其中过滤规则如下:

**过滤规则：**

**1.基本过滤规则**

非时间规则由<关键字>+<关系运算符>+<参数>组成;

时间规则由<关键字>(<时间>)组成;

**2.关键字有以下几种：**

num----number

作用：用于通过包的序号过滤;

用法：num<关系运算符><参数>，关系运算符包括>、<、>=、<=、==、!=，如 num<52;

a----after

作用：用于过滤参数时间之后的包;

用法：a(<参数>)，参数为 yyyy-MM-dd HH:mm:ss 格式的时间，如 a(2018-10-10 12:12:12);

b----before

作用：用于过滤参数时间之前的包;

用法：b(<参数>)，参数为 yyyy-MM-dd HH:mm:ss 格式的时间，如 b(2018-10-10 12:12:12);

src----source address

作用：用于过滤源地址与参数一样的包;

用法：src==<参数>，如 src=="192.168.10.12";

dst----destination address

作用：用于过滤目的地址与参数一样的包;

用法：dst==<参数>，如 dst=="192.168.10.12";

sp----source port

作用：用于过滤源端口与参数一样的包;

用法：sp==<参数>，如 sp=="1900";

dp----destination port

作用：用于过滤目的端口与参数一样的包;

用法：dp==<参数>，如 dp=="1900";

pro----protocol

作用：用于过滤协议与参数一样的包;

用法：pro==<参数>，如 pro=="ARP"

len----length

作用：用于过滤符合长度的包;

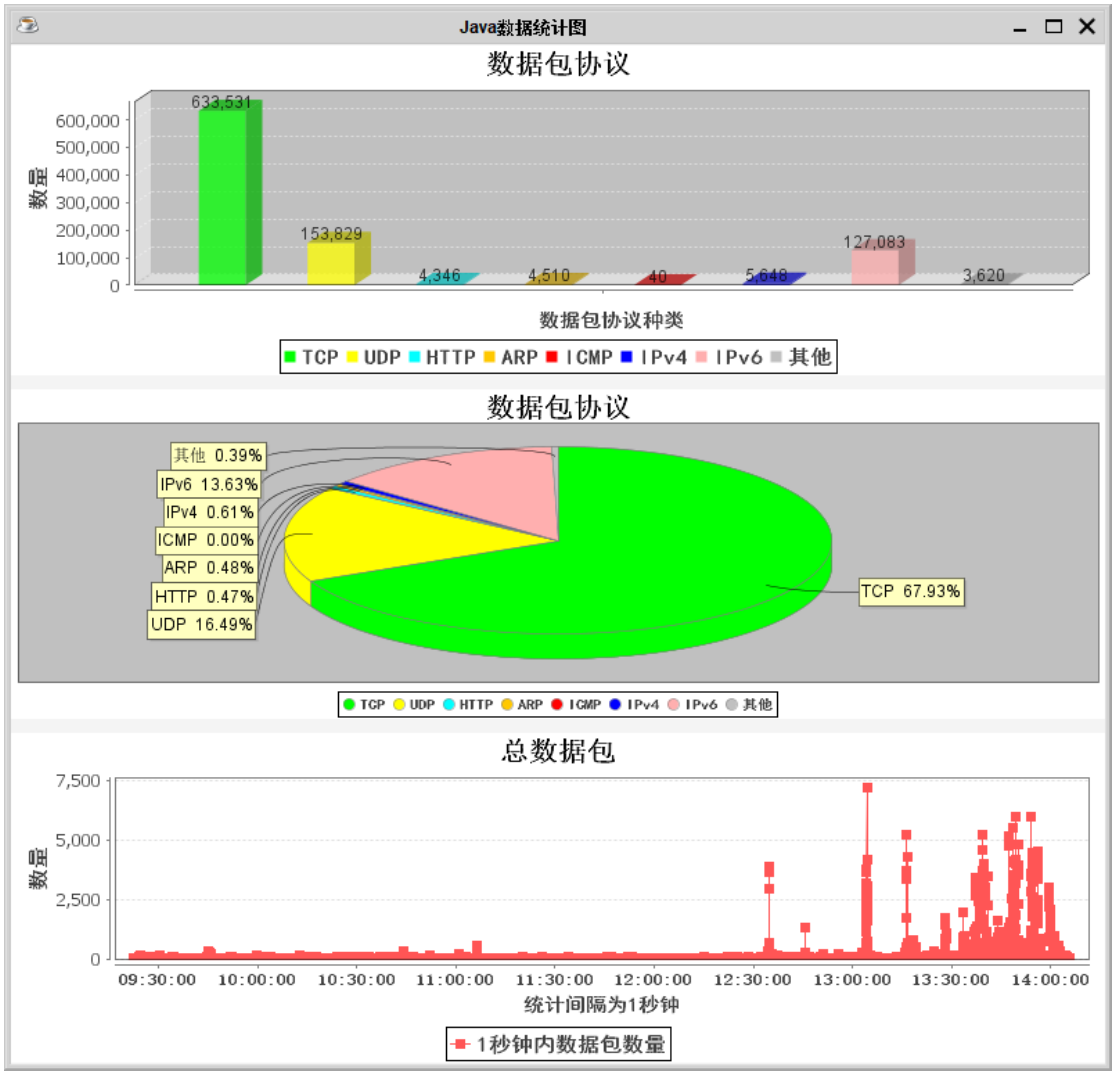
用法：len<关系运算符><参数>，关系运算符包括>、<、>=、<=、==、!=，如 len<200;

**3.过滤规则由多条基本规则组成**

多条规则通过逻辑运算符（&&、||、!）连接，组成总的过滤规则，如 num<65&&(src=="192.168.10.3"||dst=="192.168.10.3");

另外还有“统计数据集“按钮，点击后会出现图形化的统计界面。在抓取网络中的数据报文的同时统计各种数据报文的数量，各种数据包的占比，以及直观地看出网络数据报文传输的速率,根据统计每秒中的数据包的数量来反映该参数。对历史数据集进行数据报文的三项统计。前者完成的是动态统计，后者完成的是静态统计。

**统计界面：**




另外还有“历史数据集”按钮，同样是打开已保存的数据集文件。

**关于保存数据集的说明：**

保存文件和选择文件的窗口默认会导航至 D 盘，当然可以自己去选择其他盘。保存时会默认根据当前系统时间生成一个文件名，当然也是可以自己修改的。保存的文件为后缀为“.hll”的二进制文件，在 BIN 文件夹内有一个“test.hll”可以用来测试，使用该软件中“历史数据集”按钮进入文件选择即可读取。