NetAnalyzer

使用说明书

 作者：冯天文

http://twzy.sinaapp.com

日期：2017-11-28

DIRECTORY
目录

01

初识NetAnalyzer

1 .简介

2 .界面介绍

3 .功能概览

1.1 .简介

转眼之间，距离第一个NetAnalyzer发布版本已经7年了，我们在叹息时光易逝的时候，NetAnalyzer也从当初一个玩具似地小工具，变为一个可以帮助使用者解决实际问题的好帮手。看着一个软件一点点的成长，感慨颇多，在此有无数个周末与夜晚，都是在编码中度过的，时间花费了不少，最终除了赚几声喝彩，成果了了。自己很清楚这本身就是一条没有结果的路，在功利很重的今天这无异于不务正业……算了，不说废话了，本身就是出于爱好才去做的，何必计较。

NetAnalyzer作为目前最新版的协议分析工具，使用了当下流行的Ribbon界面，并且为了软件兼容性和易用性，新版的协议分析工具做了大量处理工作；包括NetAnalyzer整体架构的改造，以适应不断增加的功能点，优化代码结构，简化使用方法，还有对于Winpcap驱动，则单独提取相关的文件出来，在安装时自动安装，这样就可以避免安装完软件之后还要安装驱动的尴尬情景。除此之外还包括功能扩展、稳定性增强等多种方面的改善。

配置要求

系统：WinXP/Win7/Win8/Win8.1/Win10 （x86 和 x64）

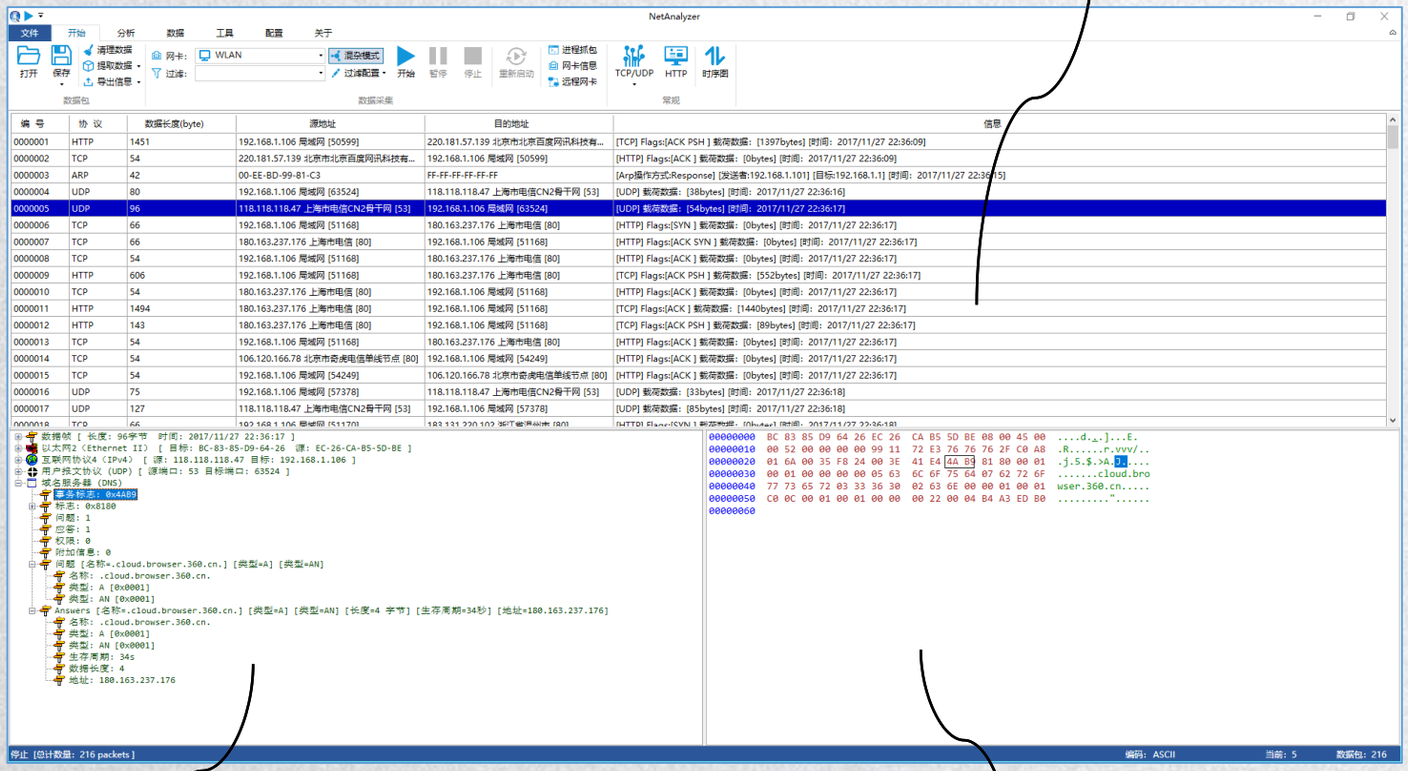
平台：NET Framework4.0

驱动：Winpcap4.1.3

浏览器：Internet Explorer7.0以上版本

扩展开发：Visual Studio 2010 以及以上版本

1.2 .界面

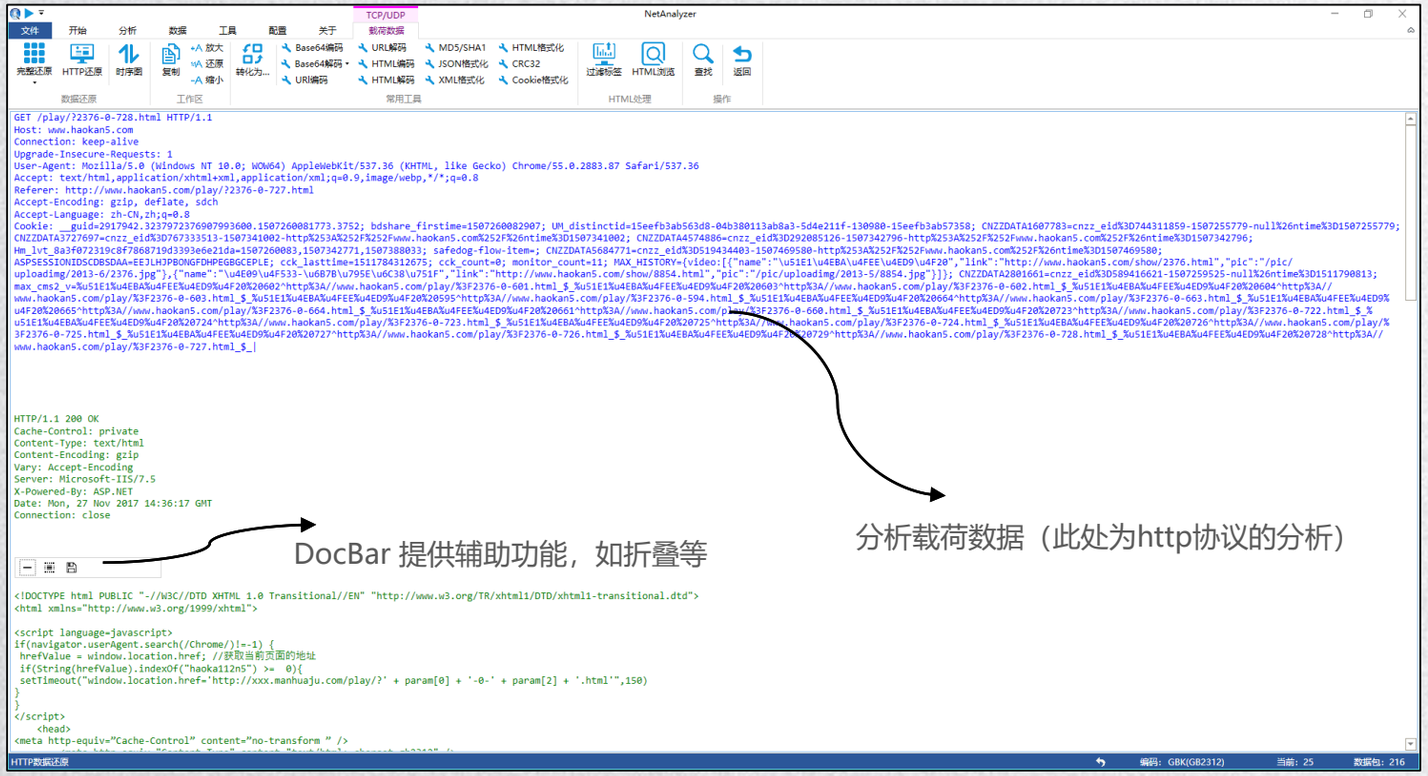


NetAnalyzer是一款集网络数据采集、报文协议分析、统计、网络流量监控于一体的网络管理工具软件，用户可以通过该软件采集网络数据，并对相关的数据进行分析，对于网络管理人员或从事网络软件开发的人是一个不错的工具。系统提供多种辅助工具方便用户更加深入的对原始数据进行还原。目前该系统已经支持80多种协议，覆盖TCP/IP、IPX等协议模型各层，支持EthernetII、PPP、Cisco HDLC、Linux SLL等多种底层网络，并且提供TCP、UDP载荷数据查看，为符合国内用户软件还提供了多种中文编码方式，方便查看中文数据。另外还提供了远程抓包功能，方便对远程机器进行监控。

NetAnalyzer工具栏部分使用最新的Ribbon界面，大大简化操作方式，而在工作区域继承原来的设计风格，在进行融合之后既具有主流软件的设计感，又具备操作上的易用性。

01 - 初识NetAnalyzer

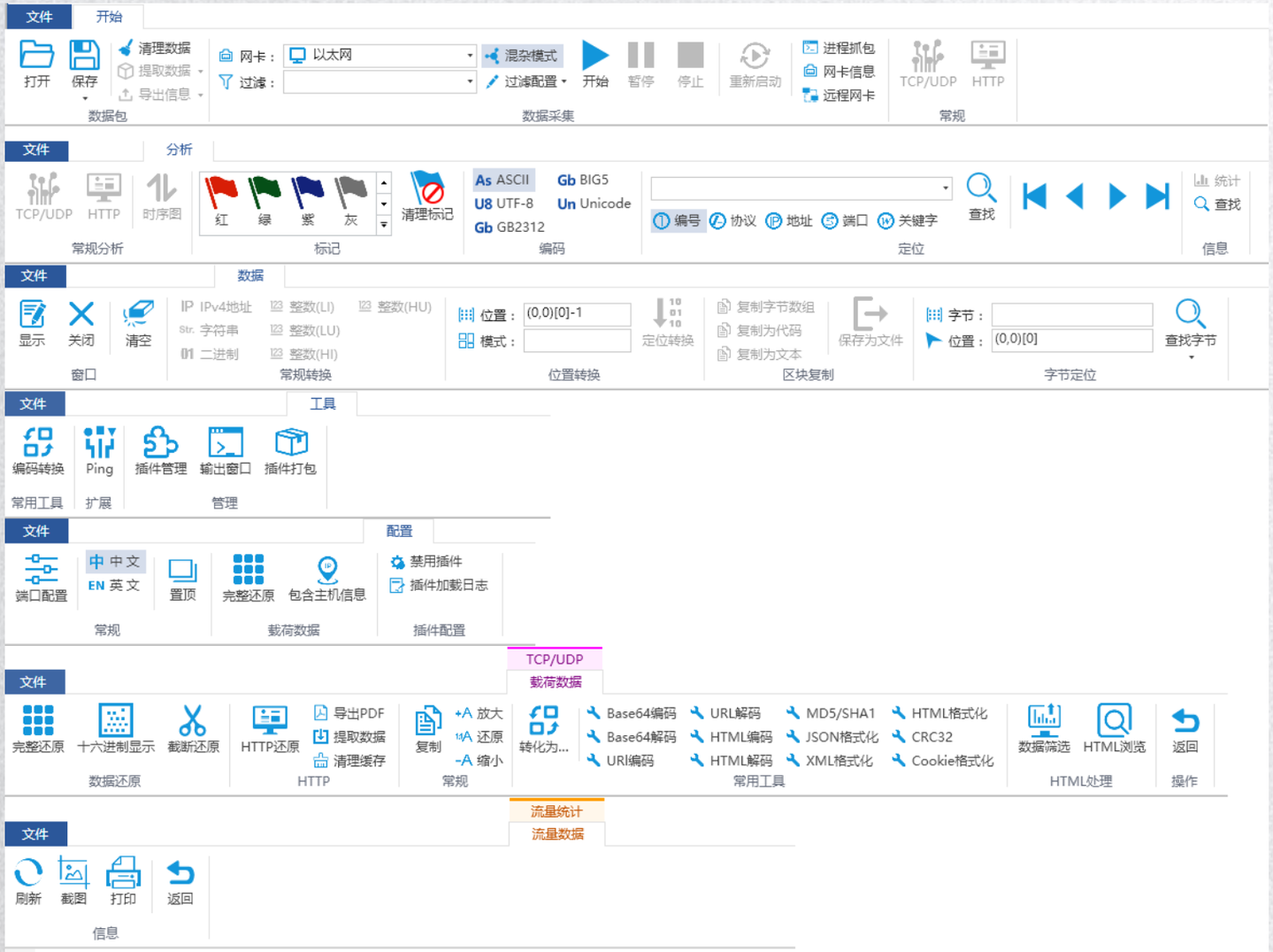
NetAnalyzer使用说明书



对于TCP/UDP载荷数据的分析，一直以来是NetAnalyzer的重要功能。

对于载荷数据分析，尤其是对于HTTP协议的内容还原一直是作为NetAnalyzer核心功能在开发。在该版本中载荷数据分析功能被极大的增强，不但加强了载荷数据分析的稳定、准确性，更提供了大量的分析功能，和数据转换工具。

1.3 .功能概览



NetAnalyzer主要分为7个标签页，涵盖从网络包抓取到数据分析统计。

02

NetAnalyzer使用方法

1 .快速开始

2 .数据获取

3 .数据分析

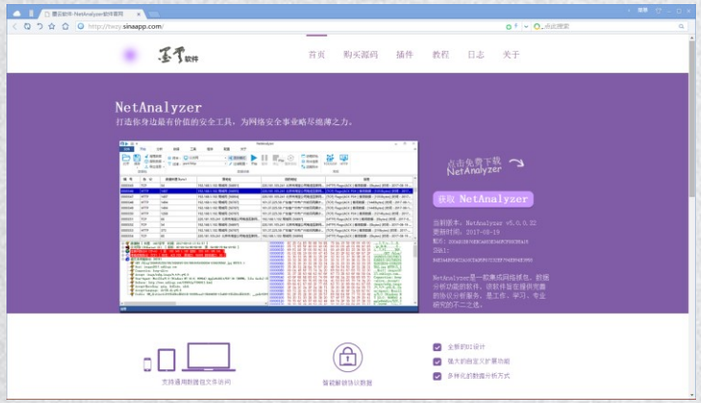
4 .辅助功能

02 – NetAnalyzer使用方法

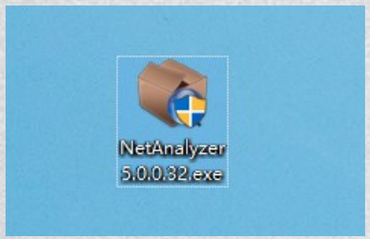
NetAnalyzer使用说明书

1. 快速开始

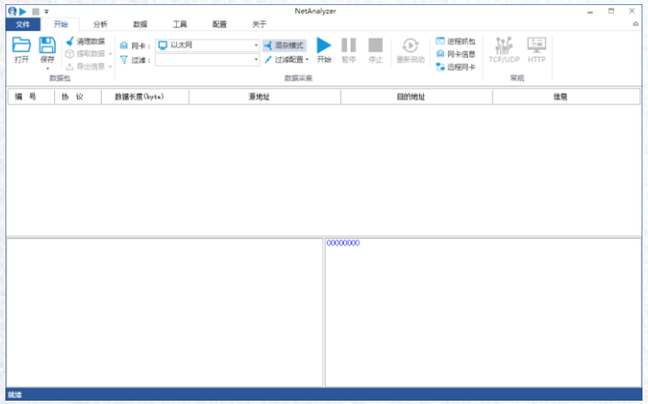
1. 首先从墨云软件官网（http://twzy.sinaapp.com/）下载NetAnalyzer。



2. 安装NetAnalyzer，安装常规的Windows安装流程，完成对NetAnalyzer的安装即可，该安装包已经集成了.Net Frameword 和Winpcap 安装，如果会自行检测安装。



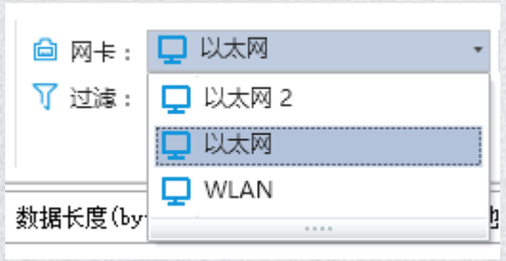
3. 安装完成后，会在桌面自动创建NetAnalyzer程序的图标，双击启动。



4. 在【开始】标签中选择当前系统连接网络的网卡，然后点击开始，开始抓包。至此，完成NetAnalyzer最基本的使用方法。

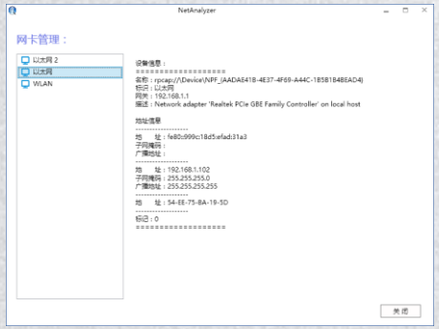
2. 数据获取

网卡信息，数据获取分为两种，从网卡直接获取和从文件读取，这里先说从网卡获取，点　击【网卡】下拉列表，即可列出当前系统已启用的网卡(包含虚拟网卡)



当我们选择了一个网卡，接下来就是对这个网卡进行操作，如开启抓包，停止抓包等等。

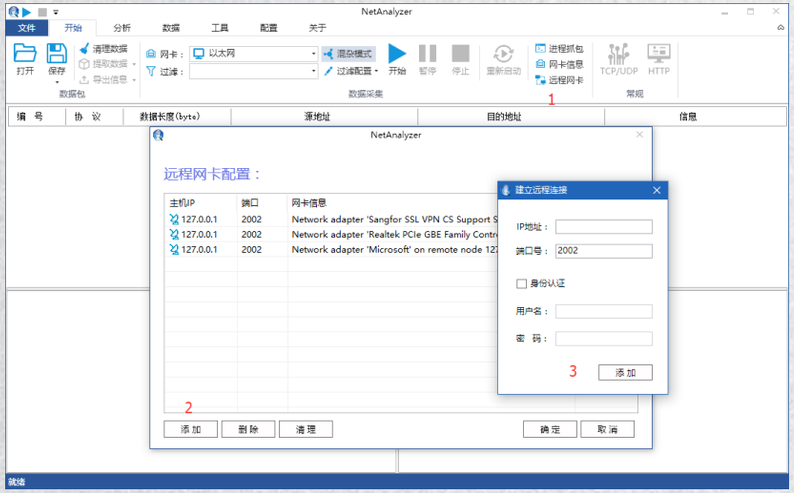
在这里我们只看到了网卡的系统给定的名称，有时候我们想要看看这块网卡具体的的配置信息，如IP地址、MAC地址之类的信息是，只需要点击 网卡信息 便可以看到我们需要的内容。

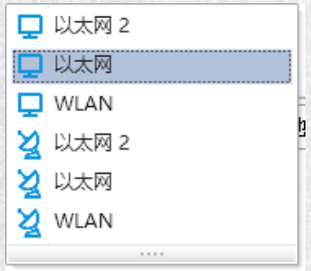


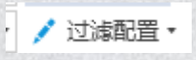
我们从这里只可以看到本机的一些网卡，但是有时候我们需要看看远程电脑的网卡那该怎么操作呢，首先在远程电脑上安装Winpcap，然后运行C:\Program Files (x86)\Winpcap\rpcapd.exe，具体使用方法如下：

2. 数据获取

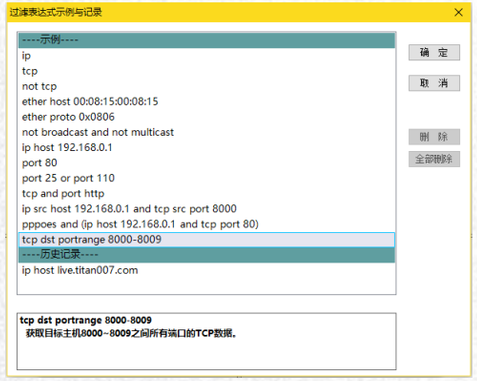
具体操作步骤如下，最后点击确定按钮，完成对远程网卡的添加（本次模拟添加当前系统的网卡）

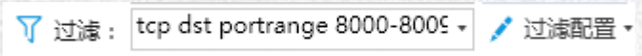




过滤表达式，对于过滤表达式，依托于Winpcap，只要使用符合Winpcap内核的过滤表达即可，在此处不会过多的讨论表达式的编写，这里会介绍一些基本的使用方法和一些抓包的特殊技巧。点击 **开始** 标签页 

进行过滤表达式配置，当然也可以直接在过滤配置前面的输入框中设置过滤表达式。



可以通过**主机**输入IP或域名地址，然后在**端口**输入端口地址，配置器会自动生成简单的过滤表达。同时，配置窗口还提供了一些示例，可以通过**示例与记录**查看。设置结果如图 

接下来就是过滤表达式的一些使用技巧，该技巧同样适用于Wireshark软件

2. 数据获取

技巧 一 抓取环回地址(127.0.0.1)的数据包

通过 `route add` 添加本地IP地址跳转，是数据经过指定的网管然后再传输到本机，通过 `route delete` 移除跳转，以减少不必要的跳转，影响系统网络效率

示例：

192.168.1.110 为本机IP地址192.168.1.1 为网管地址

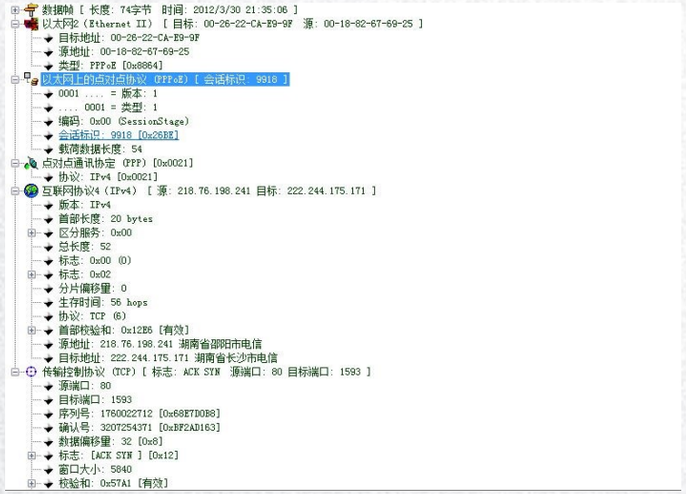
子网掩码视情况而定，若不清楚具体的iP地址，可以在DOS中 通过 ipconfig 查看

代码如下：

```
route add 192.168.1.110 mask 255.255.255.255 192.168.1.1 metric 1
route delete 192.168.1.110 mask 255.255.255.255 172.21.1.254 metric 1
```

技巧 二 抓取ASDL数据包

在一些个别地方还在使用拨号上网（ASDL）,我们在抓包时，设置了TCP或UDP端口的过滤表达式，往往不起作用，事实上，因为拨号上网在IP层上封装了PPP协议，然后再通过 PPPoE 封装PPP协议，如下图所示



对于该种，协议Winpcap所使用的过滤表达式会与一般的方式不同，对于这部分抓包需要使用 pppoes and (XXX) 方式

示例：

```
pppoes and (ip host 192.168.0.1 and tcp port 80)
```

2. 数据获取

技巧 三 抓取一段端口

有时候需要监控一段端口比如要监控目标地址的8000~80099端口之间的所有Tcp数据包，那么设置如下表达式如下表达式：

```
tcp dst portrange 8000-8009
```

网络抓包，网卡是数据源，过滤表达式为筛选条件，有了这两个准备我们就可以进行数据抓包了。

首先选择网卡：我们选择**以太网**，因为我现在使用的是网线连接，所以此处选在以太网作为我们将要监控的网卡。

接下来就是设置过滤表达式：我们设置了 `port http` 所以接下来我们只抓http协议的数据包，然后点击开始，就可以抓包了

状态栏会实时显示抓包信息

在抓包过程中我们可以随时暂停或停止抓包，当然也可以重新启动重新开始抓包。

暂停抓包：当点击**暂停**仅仅停止网卡监控，NetAnalyzer中的分析线程等还在继续工作，如果点击开始，软件不会进行初始化操作，而是在此基础上继续进行抓包。

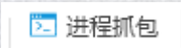
停止抓包：当点击**停止**时软件会完全停止所有的操作，包括数据采集和数据分析，并且取消界面中的功能限制。当在此点击开始时，会销毁当前采集到的数据。

重新启动：当点击**重新启动**时，软件会自动终止当前的抓包分析等操作并且销毁当前抓到的数据，然后自动启动重新进行抓包。

（*注 在销毁抓取到的数据的时候会有是否保存的提示）

2. 数据获取

除了刚才常规的抓包方式，NetAnalyzer还提供了基于进程的抓包方式。对基于进程的抓包本质上来说其实就是自动生成过滤表达式抓包，获取系统打开端口的所有进程，并获取进程所开启的端口、IP地址以及使用的协议等信息，生成对应的过滤表达式，然后给NetAnalyzer设置该过滤表达式，最后开始抓包。

点击**开始**标签页中的 

勾选需要监控的进程，点击开始抓包，进行基于进程的抓包操作。

数据包保存于打开 和传统软件类似，NetAnalyzer也提供了数据包的保存和打开操作。

保存的文件类型为 *.pcap文件，兼容市面上绝大部分的协议分析软件。

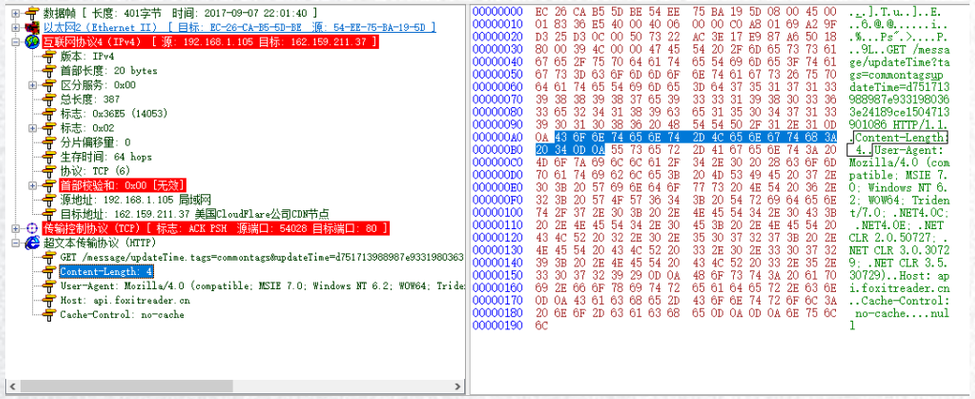
3. 数据分析

完成了数据的抓取，那么接下来就是NetAnalyzer的重点部分了，协议分析是整个软件的核心，在这里分为单个数据包分析，传输协议（TCP/UDP）协议分析，还有特意针对HTTP协议分析，以及最后的数据统计四个部分。对于协议分析，需要了解相关的网络知识或是有相关专业背景支持。

单数据包分析，在获取到数据包后，软件工作界面数据包列表框中会显示所获取的所用数据包，并且对这次数据做了一些简单的分析，我们可以凭借这些数据简单判断所对应的的数据包类型。

编　号	协　议	数据长度(byte)	源地址	目的地址	信息
0000001	TCP	119	192.168.1.105 局域网 [49852]	111.221.29.80 新加坡Microsoft分公司 [443]	[Unknown] Flags:[ACK PSH] 载荷数据：[53bytes] [时间：2017-09-07 22:01:39]
0000002	TCP	204	111.221.29.80 新加坡Microsoft分公司 [443]	192.168.1.105 局域网 [49852]	[Unknown] Flags:[ACK PSH] 载荷数据：[138bytes] [时间：2017-09-07 22:01:39]
0000003	TCP	66	192.168.1.105 局域网 [49852]	111.221.29.80 新加坡Microsoft分公司 [443]	[Unknown] Flags:[ACK] 载荷数据：[0bytes] [时间：2017-09-07 22:01:39]
0000004	TCP	54	192.168.1.105 局域网 [54024]	180.149.131.35 北京市百度网讯科技电信节...	[HTTP] Flags:[ACK FIN] 载荷数据：[0bytes] [时间：2017-09-07 22:01:40]
0000005	TCP	54	192.168.1.105 局域网 [54003]	220.181.112.244 北京市北京百度网讯科技有...	[Unknown] Flags:[ACK FIN] 载荷数据：[0bytes] [时间：2017-09-07 22:01:40]
0000006	TCP	74	192.168.1.105 局域网 [54028]	162.159.211.37 美国CloudFlare公司CDN节...	[HTTP] Flags:[SYN] 载荷数据：[0bytes] [时间：2017-09-07 22:01:40]
0000007	TCP	66	162.159.211.37 美国CloudFlare公司CDN节...	192.168.1.105 局域网 [54028]	[HTTP] Flags:[ACK SYN] 载荷数据：[0bytes] [时间：2017-09-07 22:01:40]
0000008	TCP	54	192.168.1.105 局域网 [54028]	162.159.211.37 美国CloudFlare公司CDN节...	[HTTP] Flags:[ACK] 载荷数据：[0bytes] [时间：2017-09-07 22:01:40]
0000009	HTTP	401	192.168.1.105 局域网 [54028]	162.159.211.37 美国CloudFlare公司CDN节...	[TCP] Flags:[ACK PSH] 载荷数据：[347bytes] [时间：2017-09-07 22:01:40]

当我们选中一行，即选中一个数据包，我们可以看到对该数据包详细的数据分析信息，并一树状结构树呈现出来，并在右侧显示该数据包原始信息。

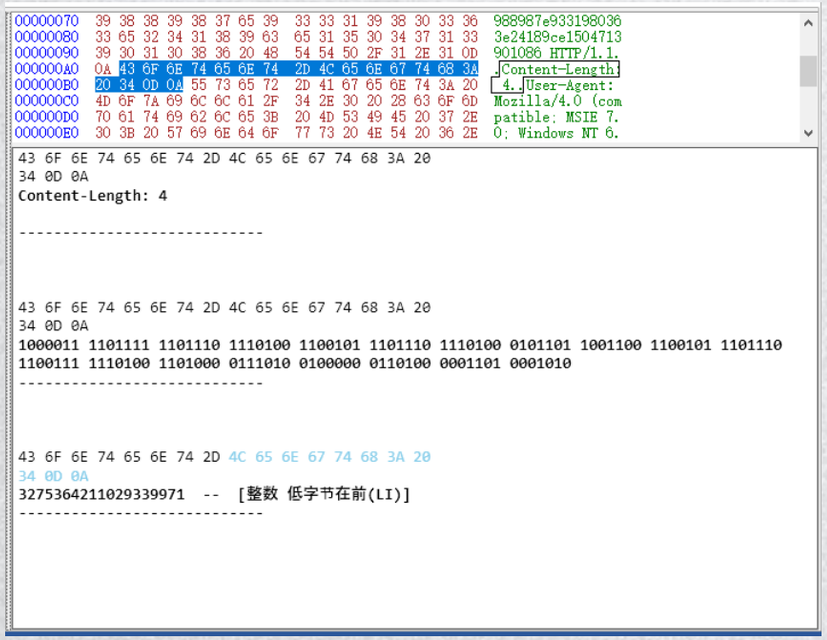


当我们选中具体的某个字段，右侧会自动选中当前字段在原始数据中的位置和具体字节。

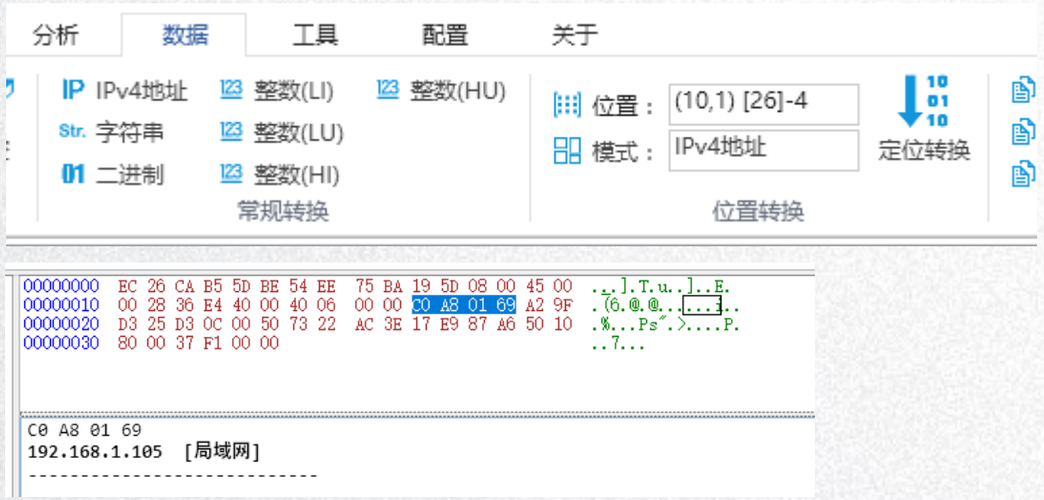
在**数据**标签页点击 **显示** 按钮 就可以打开数据转换窗口，当热也可以在常规转换中点击任意功能可以打开转换窗口

3. 数据分析

该转换功能作为NetAnalyzer软件的辅助功能，用于对二进制数据进行进一步的提取与个性化分析。



通过该就可以通过常规转换提供的功能完成对一些选定的字节进行转换。
关闭按钮为关闭转换窗口，清空则是清空当前窗口内的数据。



定位转换功能需要配合常规转换进行使用，有时候我们确定某个字节会在一个确定的位置出现，比如IP地址字段，我们选中该位置，位置字段就会出现一串代码 `(10,1) [26]-4`

(x,y) [offset] – length

x： 十六进制编辑器水平方向的偏移量

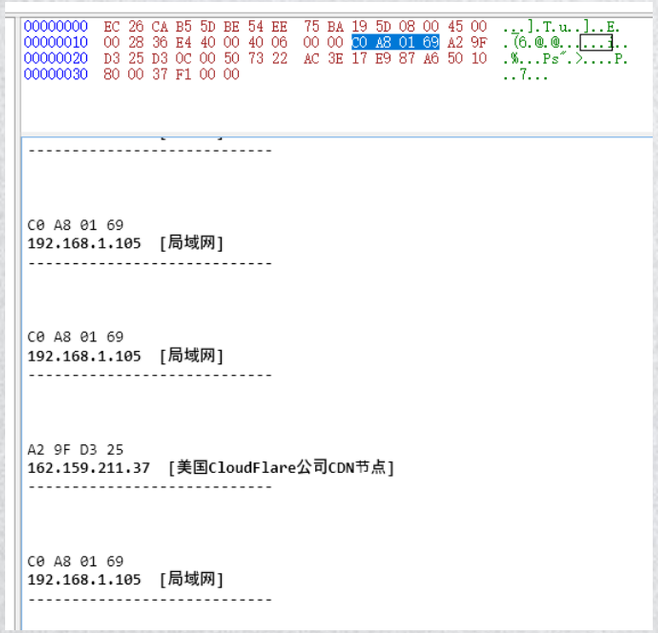
y ： 十六进制编辑器垂直方向的偏移量

offset ： 字节偏移量，offset = y * 16 + x

length ： 当前选择的数据长度

3. 数据分析

所以代码 `(10,1) [26]-4` 确定了当前IP地址的位置，此时点击 **常规转换** -> **IPv4 地址** 则会在**模式**中记录当前的转换模式，然后点击**定位转换**，就会在这个这个位置一直执行这个操作，寻找所需要的数据。



区块复制，主要是对一些已经选中的字节进行复制转为代码，字节数组，以及保存的功能，此处不再详细介绍。

字节定位，用来在数据包列表中查找相同位置出现相同字节序列的数据包。

分析，分析标签下个功能依托于数据包列表，分别有载荷数据提取，数据包标记，编码转换，数据查找，统计等相关功能，下面将会着重对一下功能进行说明。

3. 数据分析

TCP/UDP协议分析 前面介绍的都是基于单包的数据分析，而在协议分析中，我们大部分分析的数据都是依托于TCP/UDP的长连接数据，这部分数据的特点就是有多个数据包通过tcp或udp相关协议完成数据重组后才可以使用（基于udp的连接数据可能不是很严格）。

NetAnalyzer 除了提供基于单包的数据分析，更提供了基于连接数据的分析，而分析出来的数据不仅仅是在窗口上呈现一堆乱码，更可以通过DocBar将获取的数据提取出来进行使用。

在**开始** 标签最后一部分就是基于长连接的分析。点击**TCP/UDP** 按钮

此时NetAnalyzer便会切换到**载荷数据模式**(该过程可以通过配置，使用独立窗口打开)。在该模式下会打开专有的载荷数据菜单，数据区域也会变为对于载荷数据的分析，这里先介绍一个NetAnalyzer中的DocBar工具，如下图

在文本模式下，分析载荷数据会显示该工具条，该工具条会提供针对当前数据块的各种操作，当然在不动情况下，显示的工具和数量，都有所不同，下面是对当前各个功能的说明。

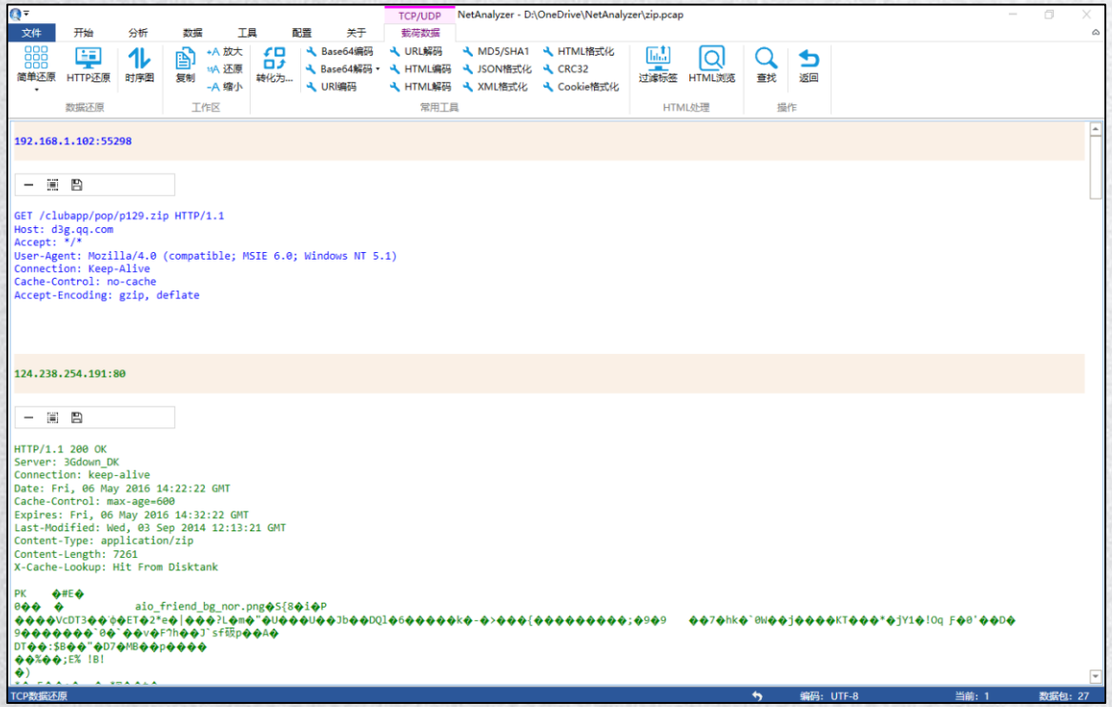
- 对当前数据块进行折叠
- 选中当前的分析数据
- 保存当前原始数据

对于其他情况下的工具在这里不会一一介绍，但是碰到的时候会有说明

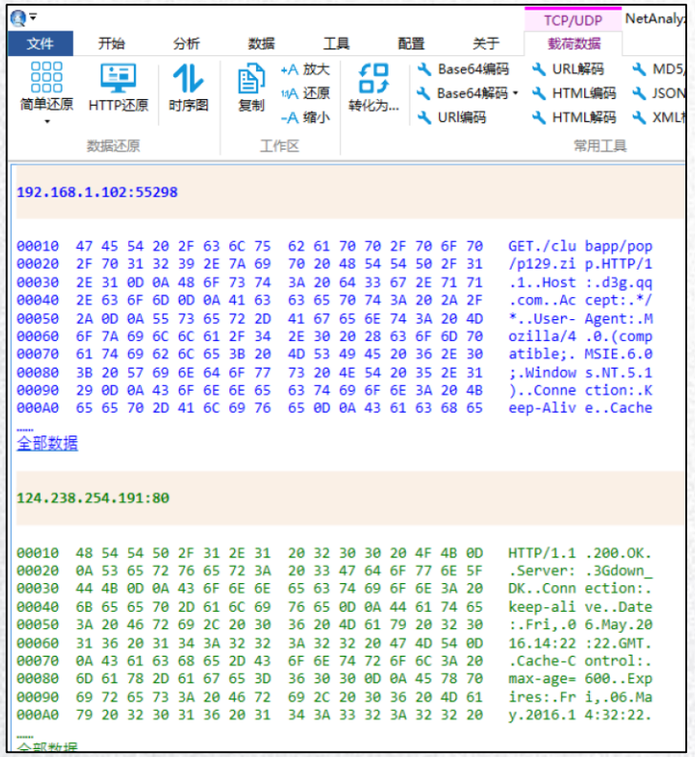
对于tcp/udp 的分析分为 **文本模式**和 **原始模式** ，文本模式主要是用于分析载荷数据为文本的数据，我们可以通过下面两种方式更改文本编码方式，分析数据。

3. 数据分析

文本模式下，呈现方式如下：

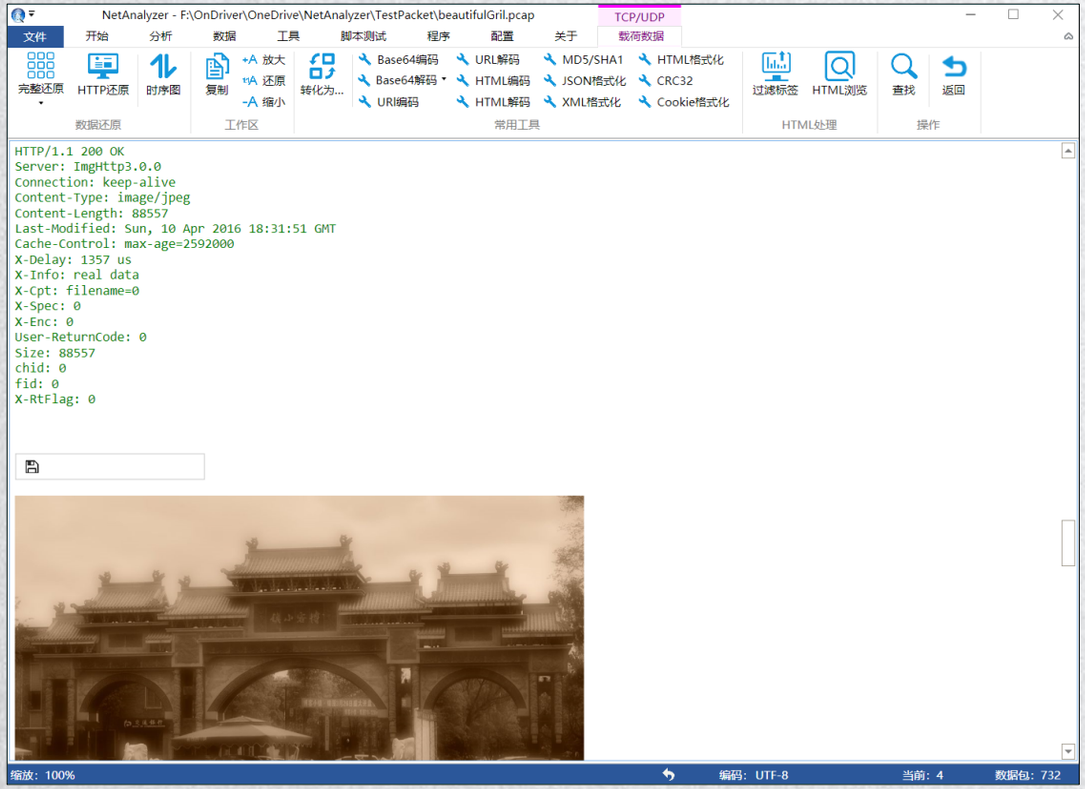


原始模式分析如下，可用通过**TCP/UDP**的下拉菜单命令 字节数据 切换为原始数据

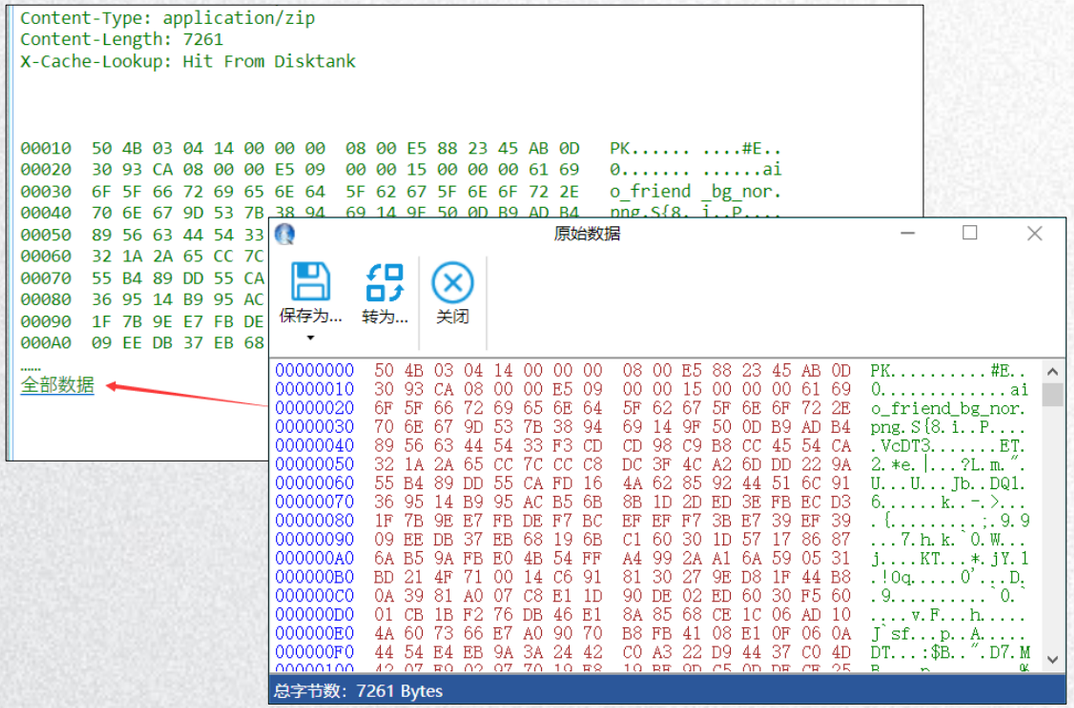


3. 数据分析

HTTP数据分析 http作为最有网络代表意义的协议，NetAnalyzer提供了更加完善的分析，http基于tcp协议，所以数据还原等都建立在tcp数据还原的基础之上。通过http分析，我们可以还原很多有意义的数据。比如下面通过http协议分析得到的图片。

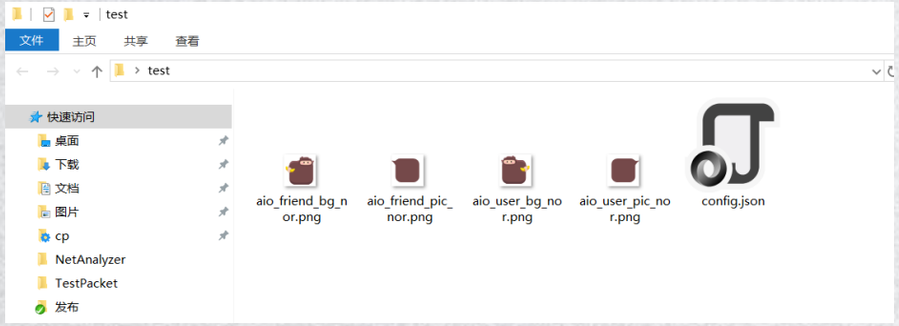


有时候通过HTTP协议还原部分二进制数据，如下面还原ZIP文件，文档会以二进制数据呈现，而我们可以通过**0x50 0x4B(PK)**推断出该文件很有可能是zip文件，所以我们点击**全部数据**，打开原始数据窗口，这部分数据正好是zip的全部数据。

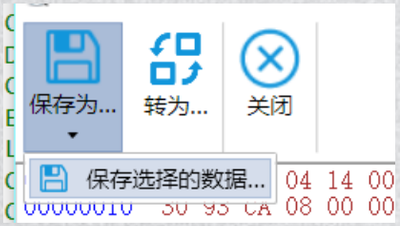


3. 数据分析

此时点击将当前数据保存为zip文件。减压就可以看到对应的文件内容。

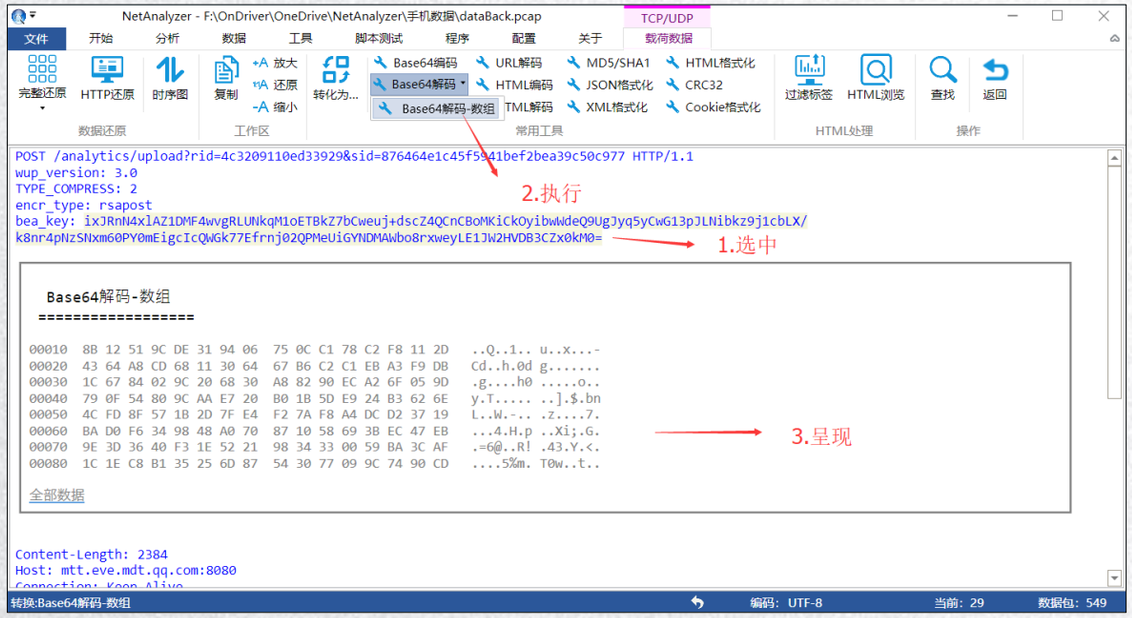


有时候数据可能存在偏差，或者我们需要提取选定的数据保存为文件，可以通过下拉**保存选定的数据**进行保存。



通过**转为...**功能我们可以打开，针对于字符串专门涉及的编码工具进行进一步处理，该部分功能的内容我们会在后面单独进行说明。

对于文本模式，针对于字符串的多种处理方式，通过如下方式，我们可以对数据进行进一步的处理。因为涉及到功能众多，这里不再一一介绍。



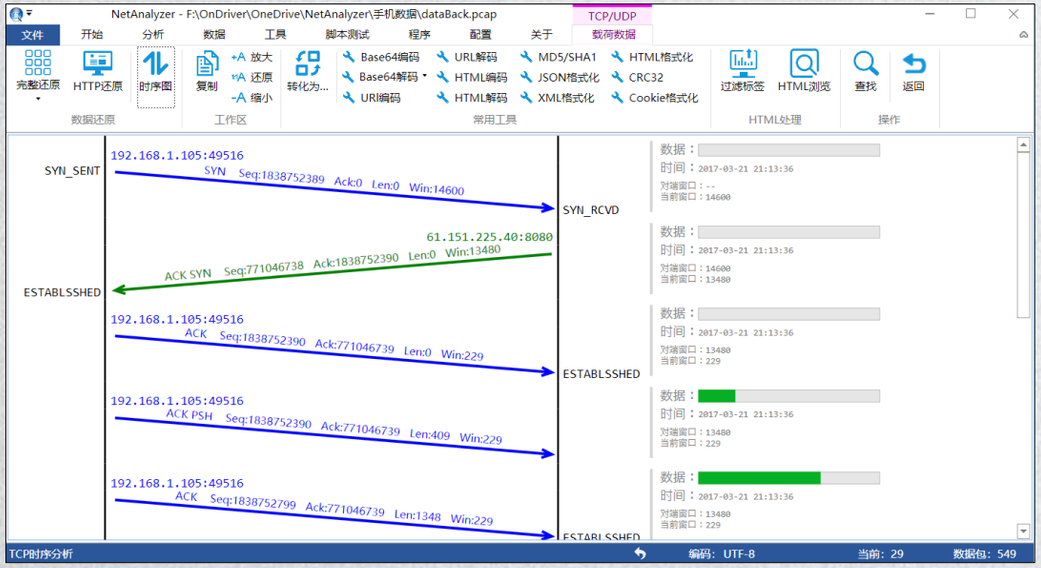
3. 数据分析

时序图 在数据分析中，除了对于数据本身的分析之外，有时候我们还要去评测一些数据质量等方面的内容。并且可以通过图像化的方式表现出来。

时序图可以作为对当前分析数据从另外一个方面的反馈，更具有参考意义。

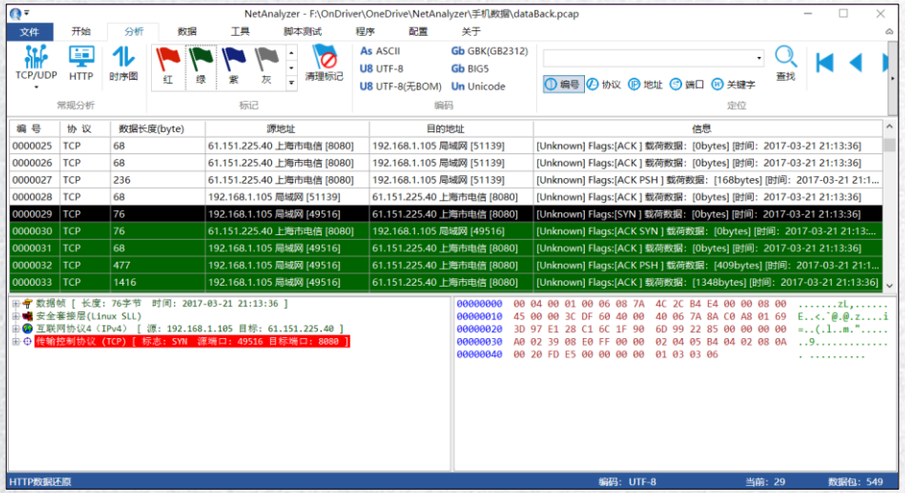
点击

就可以看到针对于当前tcp/udp 数据交互的说明



在分析标签下面，有**标记**功能，实现对当前采集会话数据连接的进行快速识别。

NetAnalyzer提供了四中颜色对数据包连接进行区分。

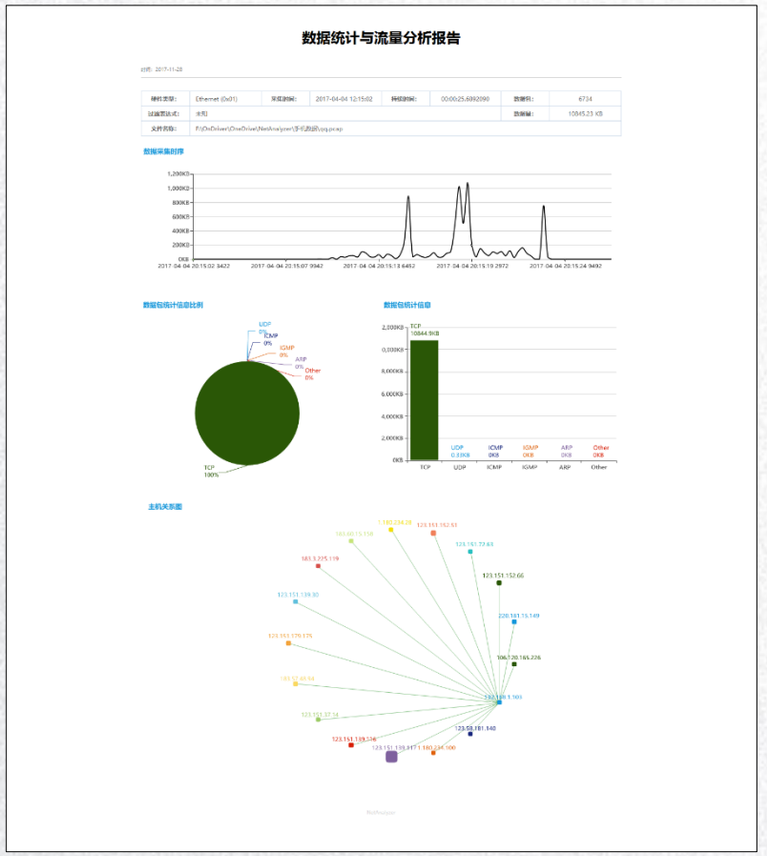


注* ctrl+鼠标左键 可以实现对数据会话的快速标记 颜色为红色

3. 数据分析

数据包查找 该功能主要是实现快速查找数据包的功能，可以通过编号，协议，地址(mac/ip)，端口，关键字等五种方式查找数据包。还可以通过数据列表导航按钮进行数据包列表浏览。

统计 对当前捕获的数据表中的数据进行统计与归类。呈现方式如有图所示。包含一些基本信息，数据量与时间直线图，数据量占比，关系图等信息



针对于协议分析相关功能，到这里基本结束了，而事实上因为篇幅的限制和作者自身文案功底太差的原因，还有很多细节的地方需并没有讲到，这需要使用者自己去体会，也随时欢迎交流。

4. 辅助功能

工具标签提供了很多辅助工具，和相关的扩展功能，因为环境不一样，该部分功能截图可能与实际情况有所出入。

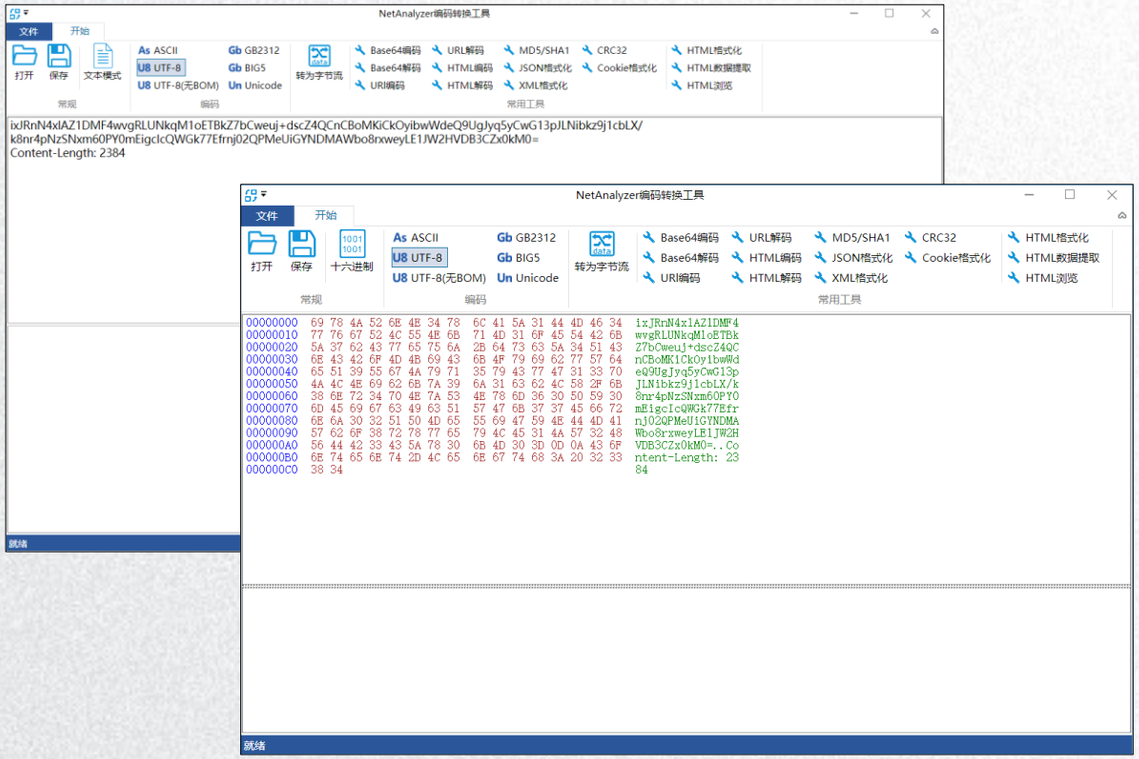
该标签下面的工具分为三组。

常用工具： NetAnalyzer内置的工具，

扩展：插件常规方式引入的功能模块

管理：对插件的管理功能。

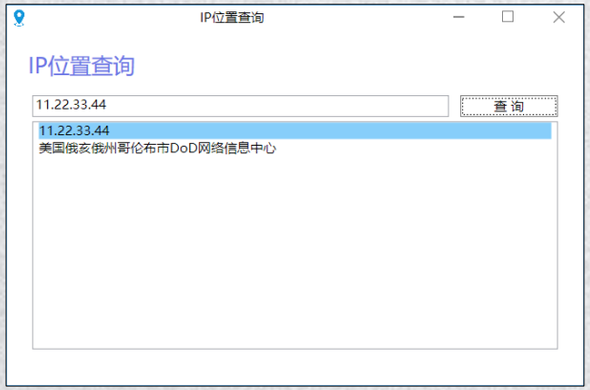
在前面做文本分析，我们发现有个**转换为...**的功能蛋就是我们将要说明的编码转换功能。

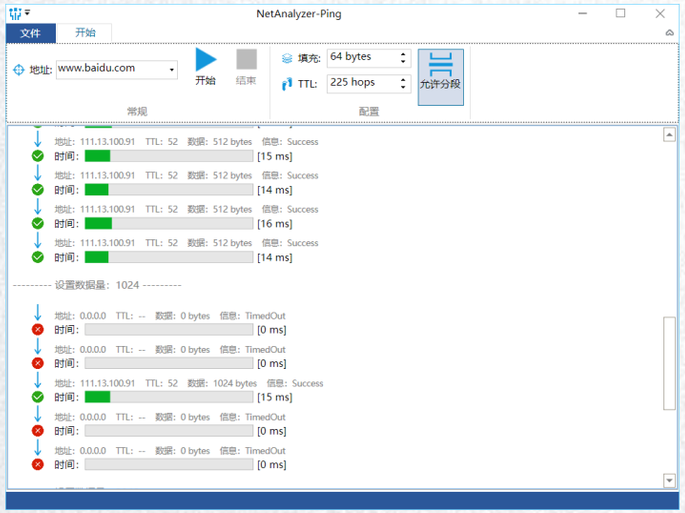


该编码转换工具可以独立使用，提供了大部分的编码转换方式。该工具也分为文本模式和原始数据模式，

4. 辅助功能

IP位置，提供通过IP地址查询地理位置的功能





接下来介绍扩展部分的两个工具

Ping ping工具区别与传统工具，可以通过自动增加数据量对目前主机进行网络性能测试。

资料查询 提供ASCII，Http状态，Mime相关内容查询

4. 辅助功能

插件管理，NetAnalyzer提供了插件机制，通过插件可以对NetAnalyzer进行扩展。

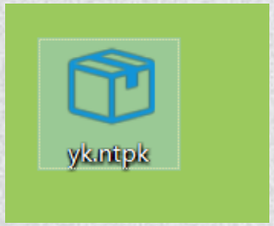
插件位置：**<安装目录>\Mods**

D:\Program Files (x86)\Twzy\NetAnalyzer\Mods

该目录下面，会针对每个插件有一个独立的文件夹

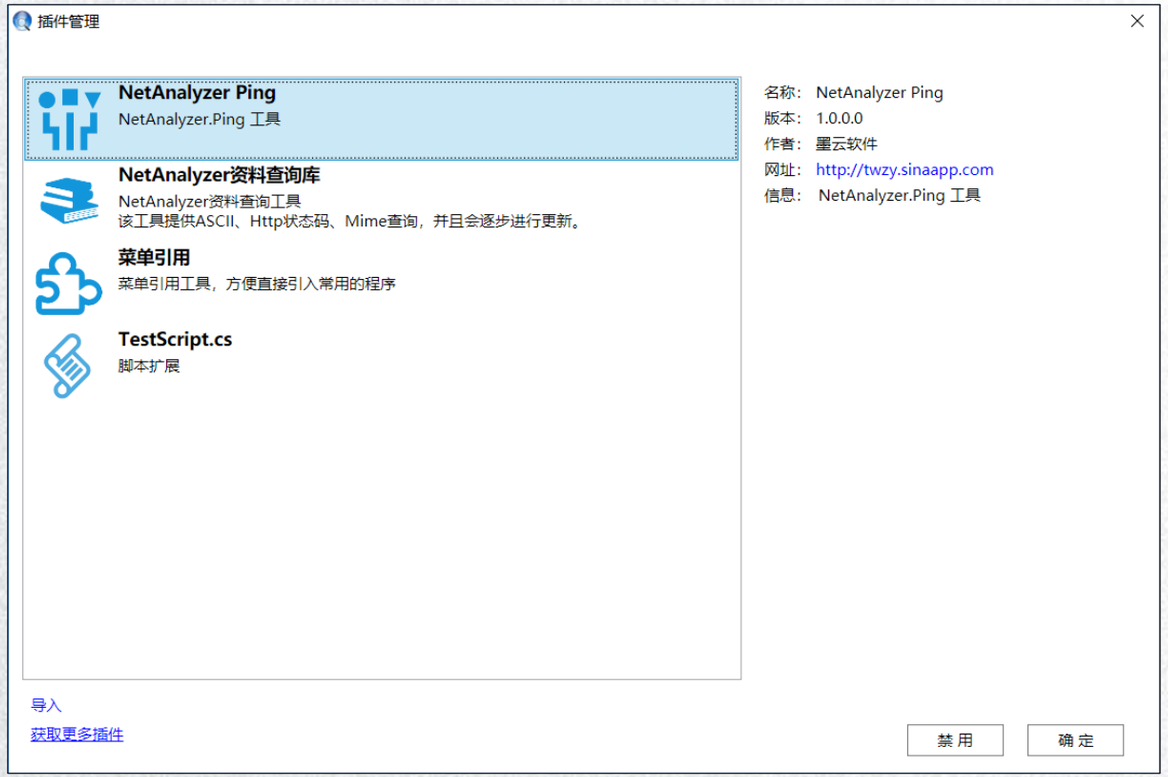
插件类型：NetAnalyzer使用两种插件方式，生成的DLL方式，脚本方式

该两种方式开发方式将会在下个章节中详细说明。



我们可以通过手动加入和通过ntpk安装包，安装插件中方法使用插件。墨云会不定期在官网增加新的插件，大家可以通过 访问官网获取对应的插件包。

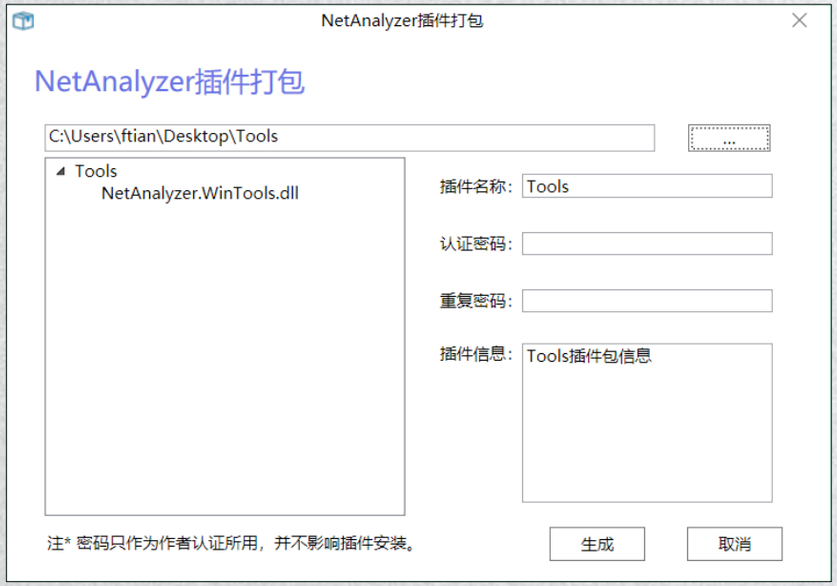
插件控制：选定一个插件后，可以通过禁用和启用插件既可以实现对插件功能呢的控制。



4. 辅助功能

输出窗口，该部分主要为调试插件而用，通过调用相关接口，就可以数据对应的数据。

插件打包，该功能主要是为打包*.ntpk 插件包用



输出窗口，该部分主要为调试插件而用，通过调用相关接口，就可以数据对应的数据。

插件打包，该功能主要是为打包*.ntpk 插件包用

03

其他

1 .声明信息

2 .资料引用

3 .其他信息

1. 声明信息

NetAnalyzer协议分析软件声明

1. 请使用本软件的用户自觉遵守国家相关法律，不得利用本软件从事任何违法犯罪活动，因使用本软件而造成的一切违反法律法规的责任与软件作者无关。
2. 非经作者许可不得对软件中的任何内容进行修改、删除、进行反向工程等操作。
3. NetAnalyzer使用了部分开源代码、组件、图表、图标以及图片，该部分开源代码、组件、图表、图标以及图片版权归对应的作者和机构所有。
4. 使用者可以对本软件提供的非第三方的代码组件进行非商业用途的调用或二次开发，对于开源代码、组件、图表、图标以及图片请在遵循对应授权条件下使用。
5. 该软件可免费用于学习研究，但非经作者同意不得用于商业用途。
6. 使用者可以在非商业用途的情况下，自由复制、传播、分发本软件；从事商业用途必须经过作者同意。
7. 作者对本软件不提供任何保证，不对任何用户因本软件所遭遇到的任何理论上的或实际上的损失承担责任，不对用户使用本软件造成的任何后果承担责任。
8. 本软件相关资料来源于互联网，并不会涉及使用者隐私，因此不会侵害使用者的隐私。
9. 软件中使用了纯真IP地址数据库，纯真IP地址数据库归纯真网络所有。
10. 软件中使用了ECharts.js图表库，版权归百度 ECharts 团队所有。
11. 除第3、第8、第9条所涉及的开源代码、组件、图表、图标以及图片外，本软件作者保留该软件的所有代码权利。
12. NetAnalyzer使用了插件技术，对于所使用的插件安全性当由用户自行甄别，对于用户因为使用恶意插件而造成的任何后果与软件作者无关。
13. 作者保留对NetAnalyzer程序、《NetAnalyzer协议分析软件声明》的最终解释权利。

2. 资料引用

这里推荐一些常用的网络协议分析网站，最后三个可以下载数据包

Wikipedia http://en.wikipedia.org/wiki/Communications_protocol

RFCSourcebook http://www.networksorcery.com/enp/default1101.htm

中国协议分析网 http://www.cnpaf.net/

Packet Captures - Packet Life http://packetlife.net/captures/

SampleCaptures - The Wireshark Wiki http://wiki.wireshark.org/SampleCaptures

Protocols | pcapr http://www.pcapr.net/browse/protos

3. 其他信息

这里面的协议是NetAnalyzer可以完整分析的协议，共80多个协议，并且正在不断更新中。

该文档为使用手册，后续会有**开发手册**放出。

NetAnalyzer 可分析协议列表
应用层
HTTP，DNS，DHCPv4，FTP，Gopher，NNTP，POP2，POP3，SMTP，Telnet，SSDP，BGP，RIPv1，RIPv2，RIPng，Echo，IPP，AODV，ESMTP，COPS，DCAP，QQ，IMAP，HSRP，MGCP，RTSP，GDOI、SIP、Kismet、MSNMS
传输层
TCP，UDP，OSPFv2，OSPFv3，GREv0，GREv1，UDP-Lite，AH，ESP，CBT，DCCP，SCTP，EGP，GGP，DSR，IFMP，PIM，PGM
网络层
IPv4，IPv6，ARP，PARP，ICMPv4，ICMPv6，IGMPv1，IGMPv2，RGMP， PPPoES，PPPoED，IPCP，IPv6CP，CCP，BVCP，IPIP、IPX、AARP
数据链路层
Ethernet II， PPP，Cisco HDLC，Linux SLL，LCP，Cisco SLARP，EAP，CHAP，LLDP，WOL，ECP、IEEE802.3/802.2、Novell Ethernet、LLC、SNAP

NetAnalyzer可分析协议

NetAnalyzer

墨云软件

 作者：冯天文

http://twzy.sinaapp.com

日期：2017-11-28