WireKunpeng数据包抓取分析软件 V1.0

- 使用说明

1 简介

1.1 编写目的

本文档为使用说明文档，为产品的使用与维护提供信息基础。

1.2 使用对象

本文档的使用对象主要为产品测试与使用人员。

1.3 软件功能

主要功能为侦听、解析数据包。扩展功能有流量监测和简单的攻击检测。本软件目前支持解析 IP、IPv6、ARP、TCP、UDP、ICMP、ICMPv6、SSDP、HTTP、TLS、SSL、DNS 等协议的数据包。

1.4 软件运行环境

- Python 环境依赖

  本软件运行在 Python 3.8.0 环境下，且需要以下第三方模块支持：psutil==5.7.2；scapy==2.4.4；matplotlib==3.2.2；PySide2==5.15.0；WMI==1.5.1；pywin32==228；numpy==1.19.1。

- 计算机需安装有 Npcap V0.9994 及以上版本。

2 模块描述

- capture_core.py

该模块主要功能是对抓取到的数据包进行协议分类；统计计算机网卡收发数据包的速率；解析数据包在数据链路层、网络层、传输层及应用层中的报文格式及各种标志信息。例如，解析捕获到的数据包的大小、目的地址、目的端口、使用协议等等。

- flow_monitor.py

该模块主要功能是提供流量监测系统的底层实现方法，如获取正在运行的进程列表及各进程使用的端口号；计算各进程的指定类型数据包收发速率等等。

- main_ui.py

该模块主要功能是创建前端图形化窗口界面，用于展示捕获到的数据包的各种信息，可方便用户使用本软件。

- monitor_system.py

  该模块主要功能是实现本软件的流量监测功能，提供流量监测功能的图形化界面。

- tools.py

  该模块主要功能是提供本软件的各种基础功能实现方法，如获取计算机网卡列表、以标准格式显示时间和数据包收发速率及搜集数据包收发速率信息等等。

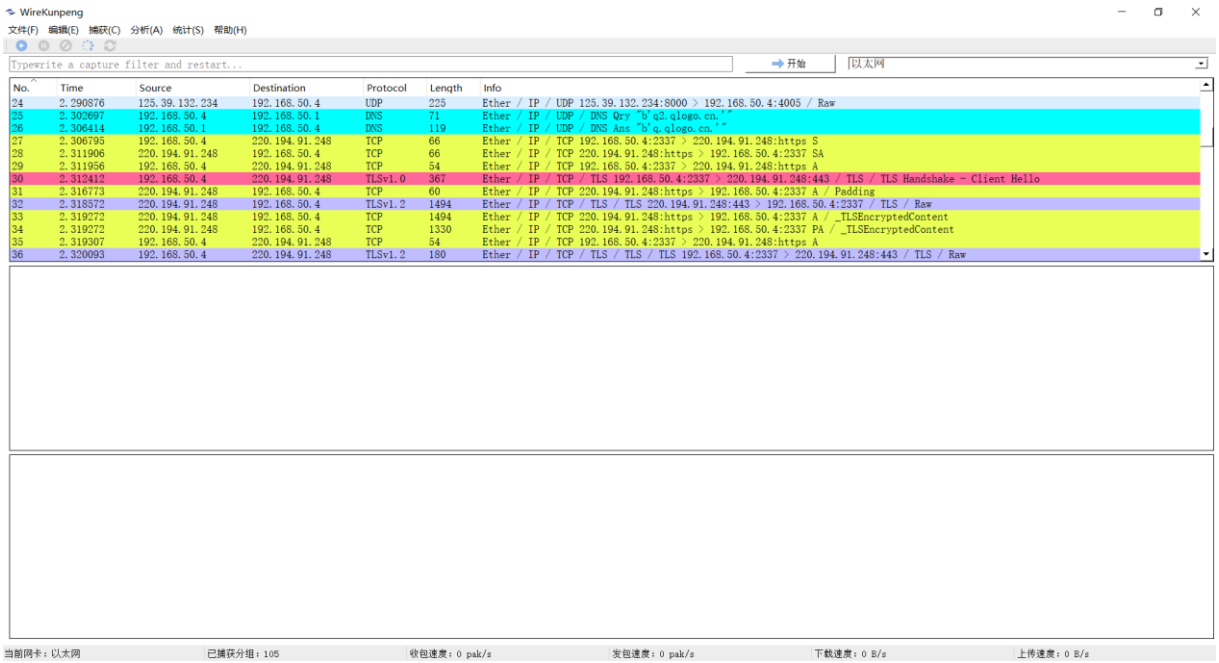
- WireKunpeng.py 模块主要功能是提供运行本软件的方法。

3　使用说明

3.1　抓取数据包说明

1） 用户在网卡选择框选取指定计算机网卡用以侦听此网卡流经的所有数据包。

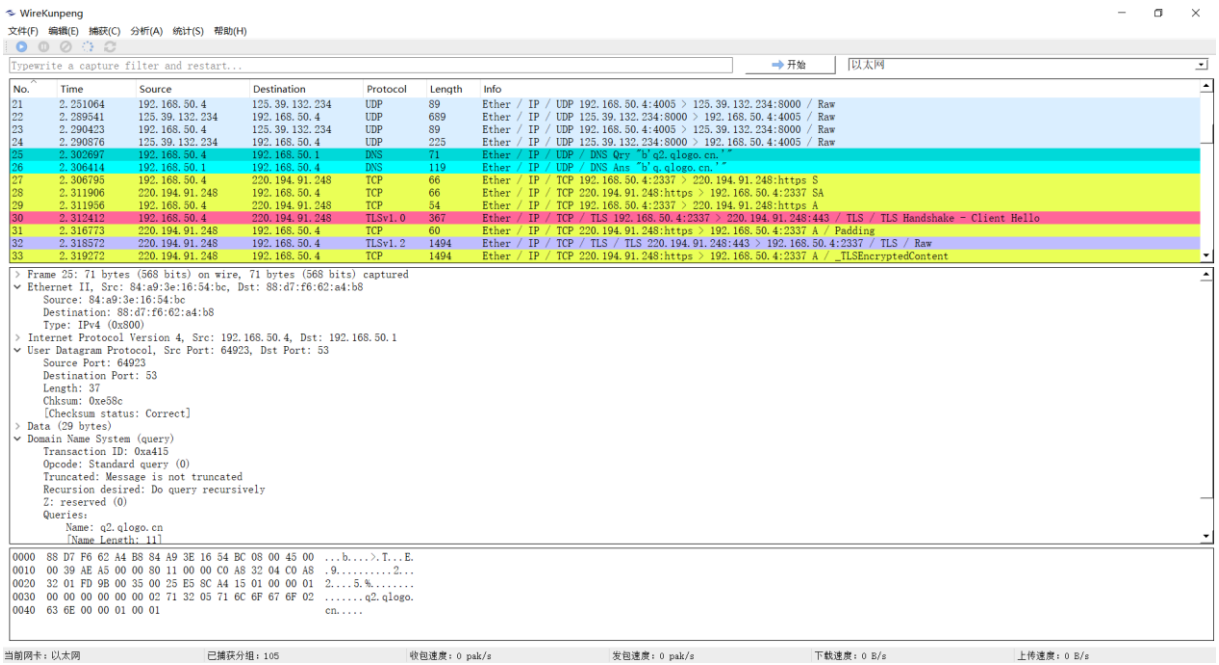
2） 点击开始按钮后，本软件开始抓取数据包并在窗口界面中罗列出数据包的简略信息。



3.2　解析数据包说明

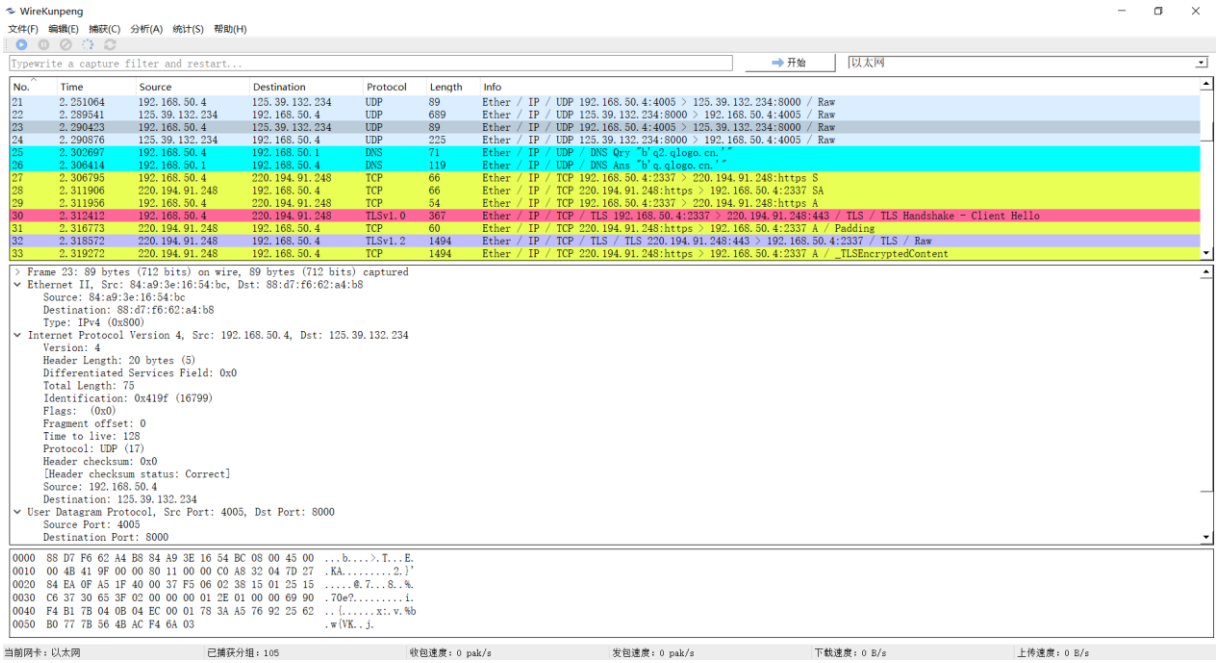
点击任意数据包即可查看该数据包详细结构及内容信息。

1） DNS 协议数据包示例：



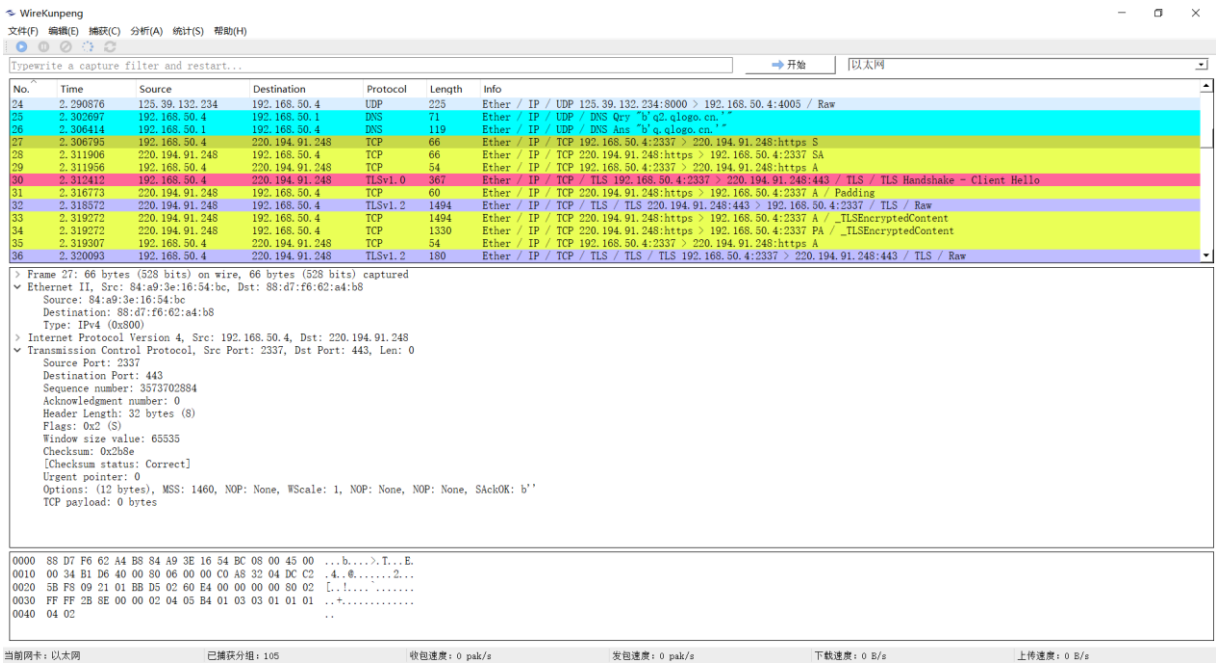
在 DNS 协议数据包中详细解析了 DNS 协议层的报文结构及数据内容，包括 DNS 查询请求或 DNS 查询响应数据包的事务 ID、标志、查询问题区域或者回答问题区域等等。

2） UDP 协议数据包示例：



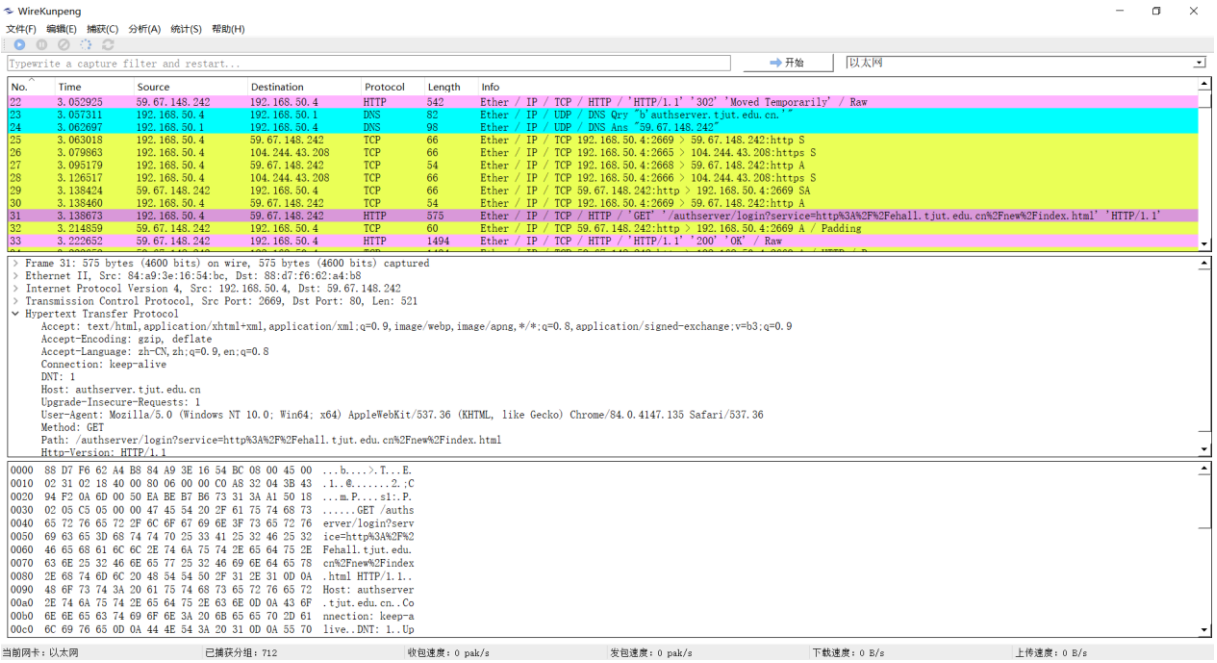
在 UDP 协议数据包中详细解析了 UDP 协议层的报文结构及数据内容，包括该 UDP 数据包源端口与目的端口、UDP 数据报长度以及校验值等信息。

3） TCP 协议数据包示例：



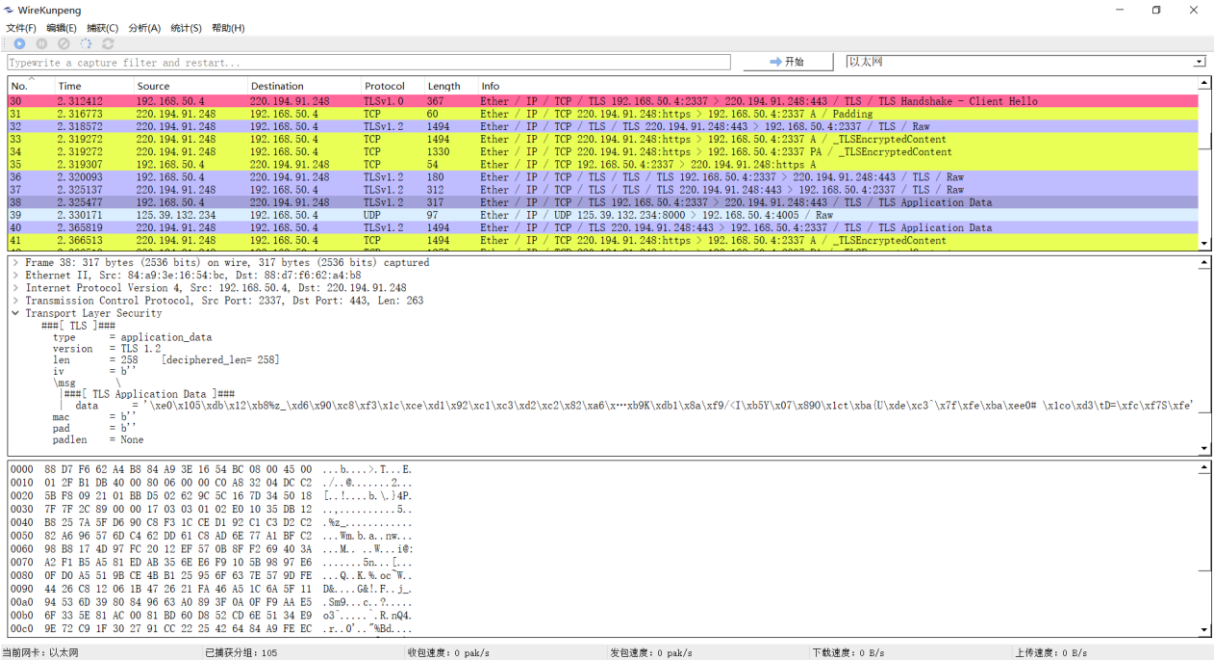
在 TCP 协议数据包中详细解析了 TCP 协议层的报文结构及数据内容，包括该 TCP 数据包的源端口和目的端口、TCP 协议序列号及确认序号、头部字节长度、标志、校验和、窗口大小等等。

4） HTTP 协议数据包示例：



在 HTTP 协议数据包中详细解析了 HTTP 协议层的报文结构及数据内容，包括 HTTP 请求报文的请求方法、URL、HTTP 协议版本、请求头部及请求数据等信息；HTTP 响应报文的 HTTP 版本号、状态码、状态值、响应头及响应数据（如 HTML 文本）等信息。

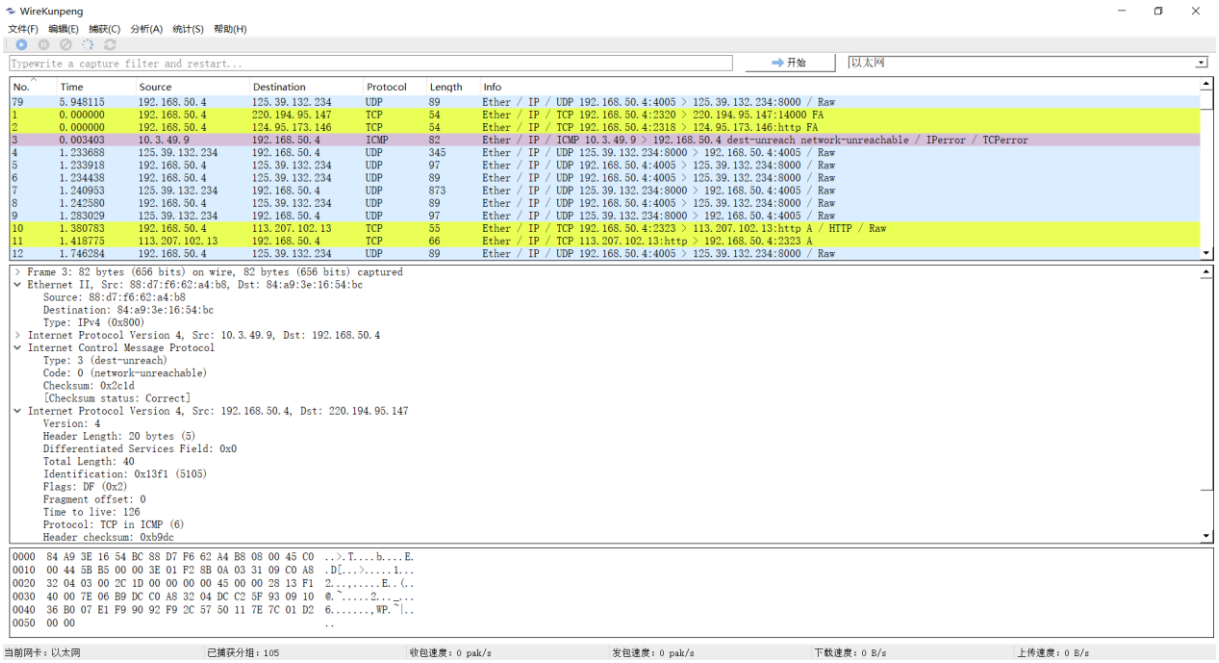
5） TLS 协议数据包示例：



在 TLS 协议数据包中详细解析了 TLS 协议层的报文结构，包括数据包的 TLS 协议版本号、TLS 协议类型（如握手协议、记录协议等）等标志信息，且尝试解密 TLS 传输的应用数据内容。

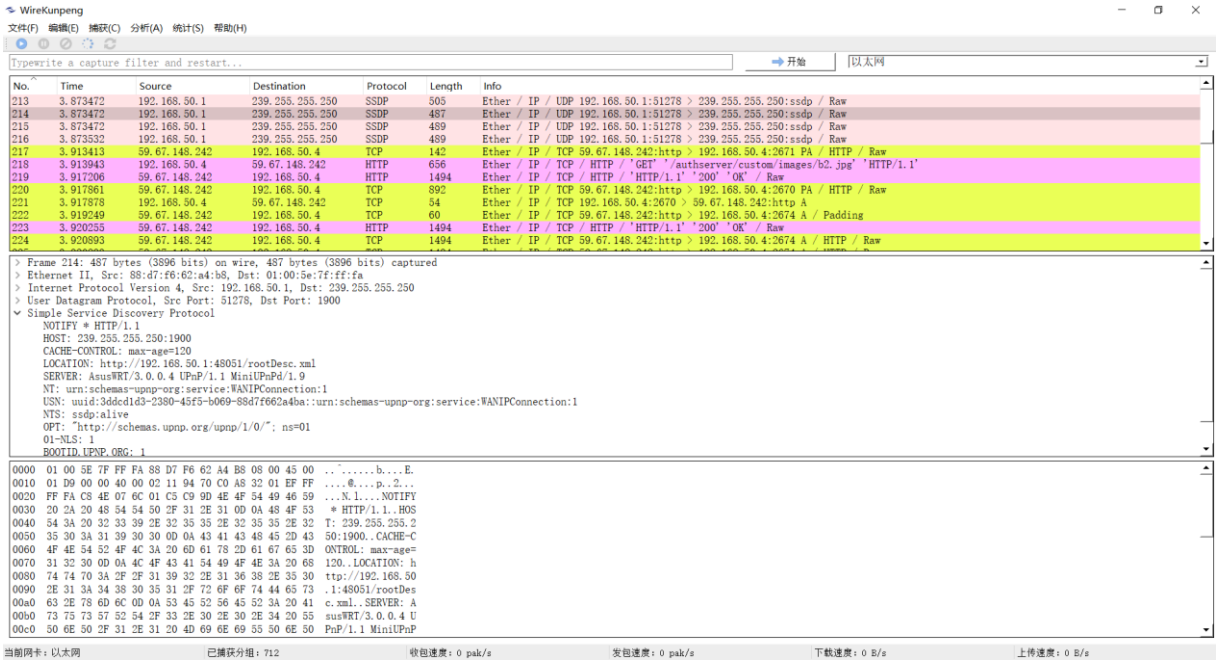
6） ICMP 协议数据包示例：

在 ICMP 协议数据包中详细解析了 ICMP 协议层的报文结构，包括数据包的 ICMP 报文类型、标识对应 ICMP 报文的代码及校验和等信息。



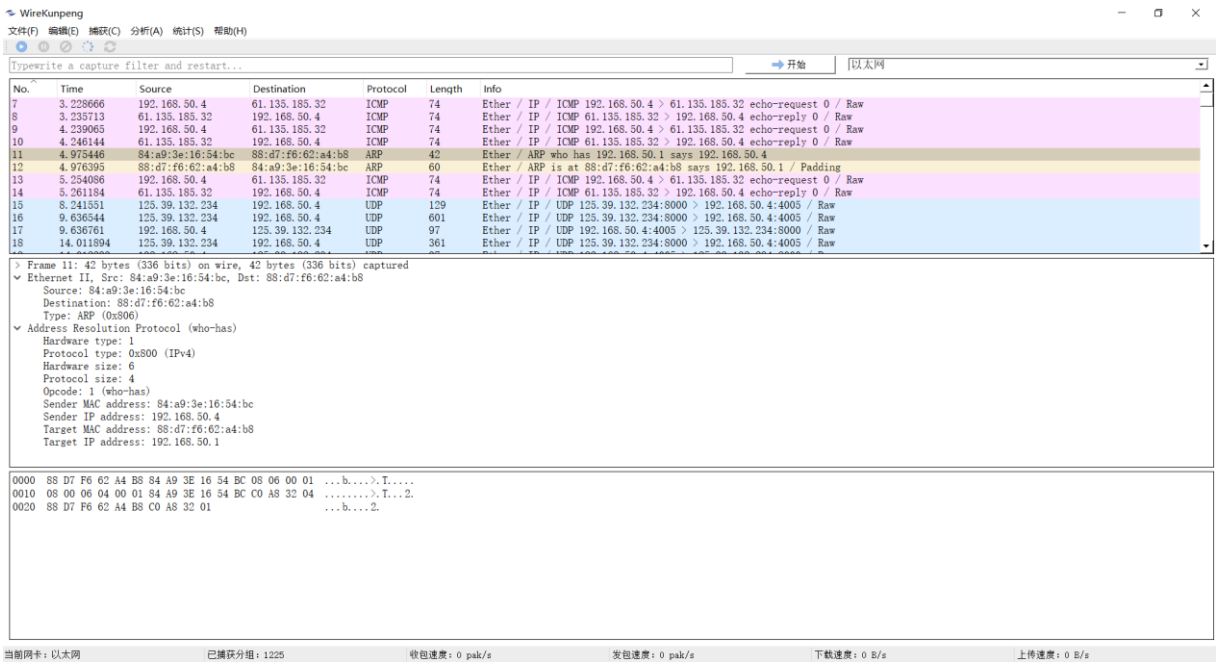
7） SSDP 协议数据包示例：

在 SSDP 协议数据包中详细解析了 SSDP 协议层的报文结构及数据内容，包括多播地址和端口、协议查询类型、设备响应最长等待时间、服务查询目标等信息。



8） ARP 协议数据包示例：

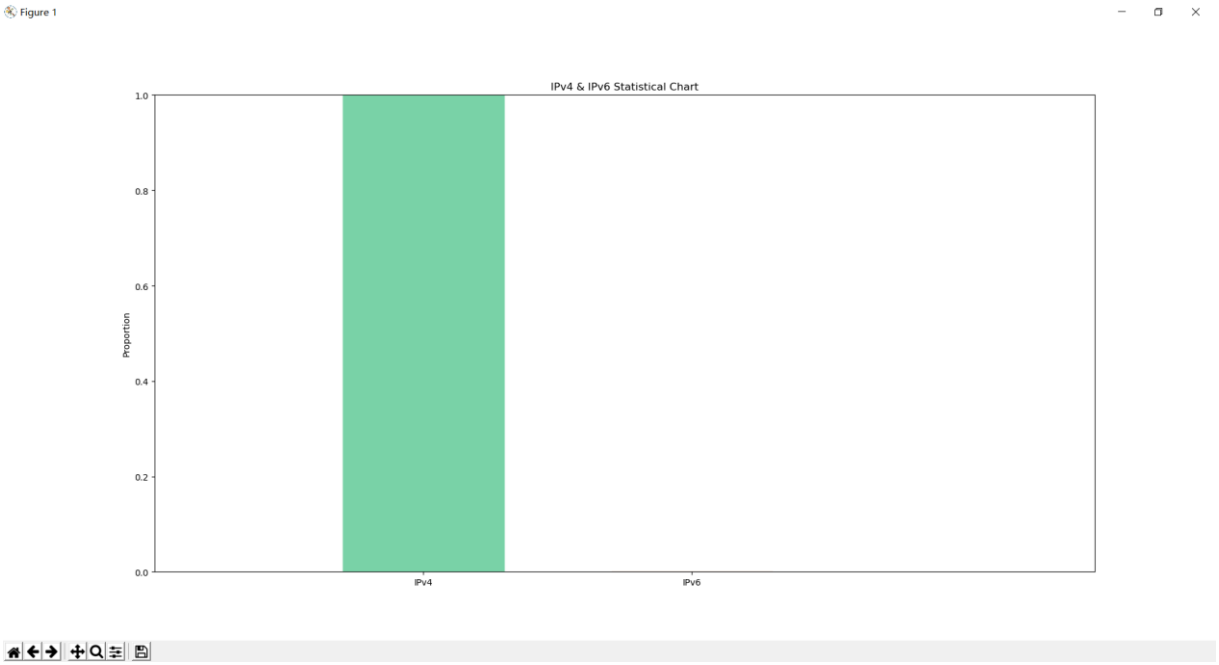
在 ARP 协议数据包中详细解析了 ARP 协议层的报文结构及数据内容，包括硬件类型、协议类型、硬件地址长度、协议长度、操作类型、发送方 MAC 地址、发送方 IP 地址、目标 MAC 地址、目标 IP 地址等信息。



3.3　数据包统计功能说明

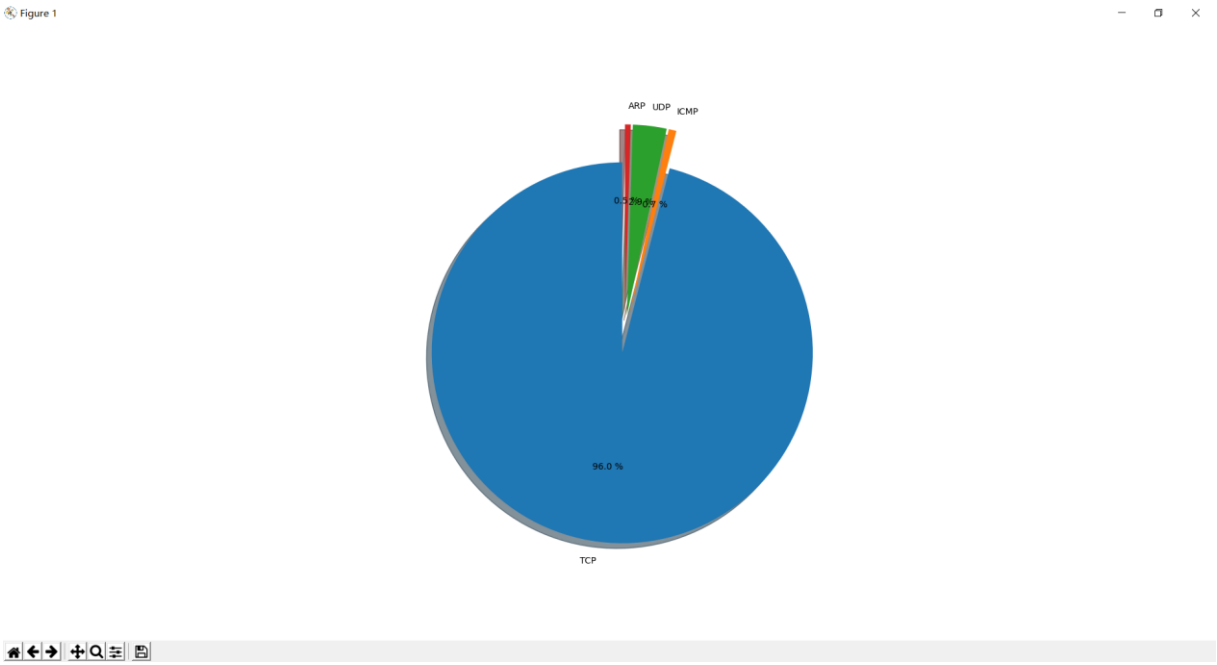
- IP 地址类型统计

  统计捕获到的数据包中 IPv4 和 Ipv6 协议占比



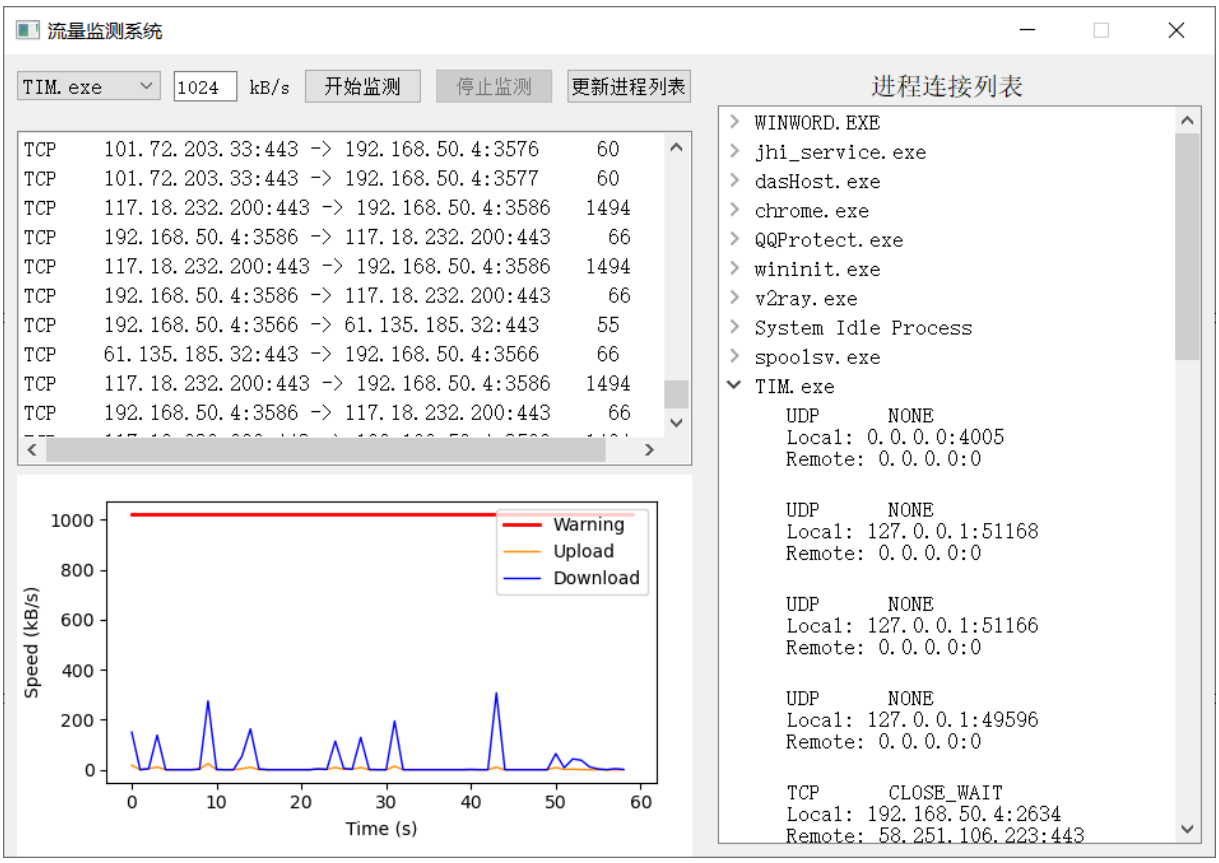
- 报文类型统计

  统计捕获到的数据包中各协议占比情况



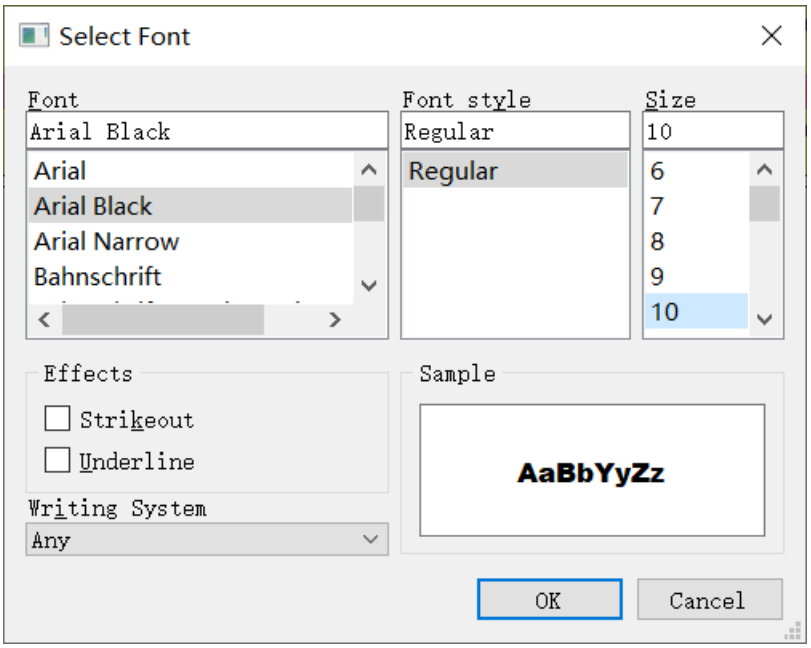
3.4　流量监测功能说明

本软件实现了流量监测功能，可对正在运行且具有网络连接的进程实施网络速率监测，以速率图的方式实时显现某一进程的网络连接活动，监测其连接速率。还可设置速率预警线，若指定进程的网络连接速率超过预警线则发出警告信息提醒用户。

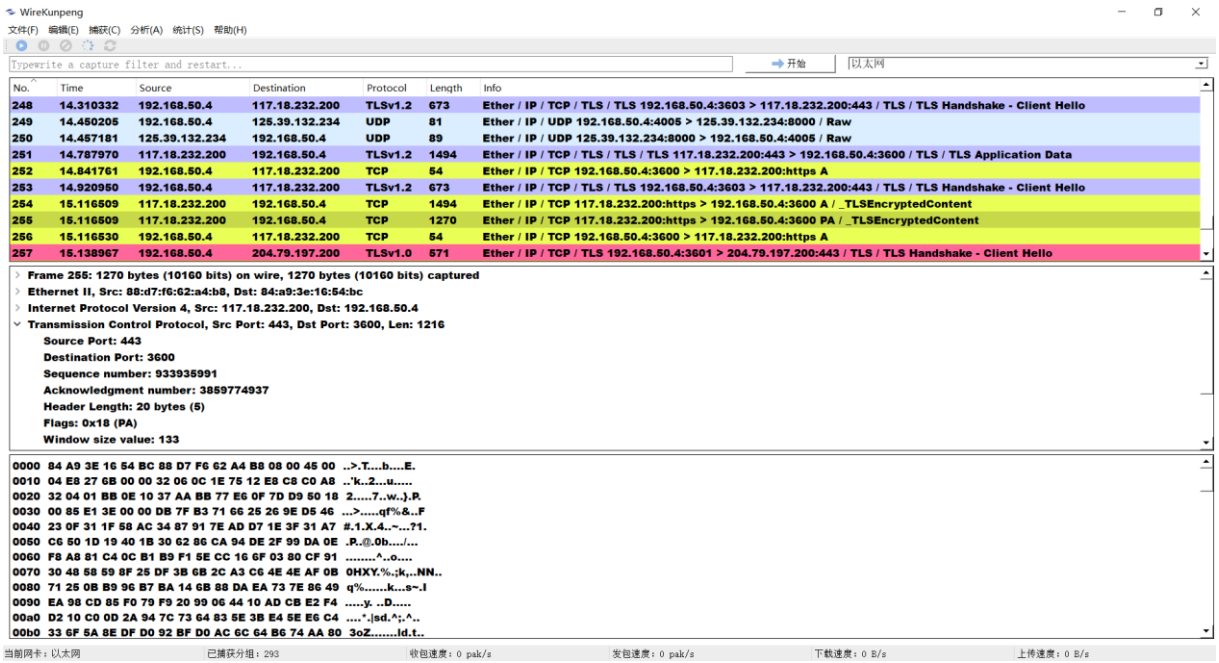


3.5　更改界面字体功能说明

本软件可根据用户需要手动更改软件界面字体以方便用户使用。

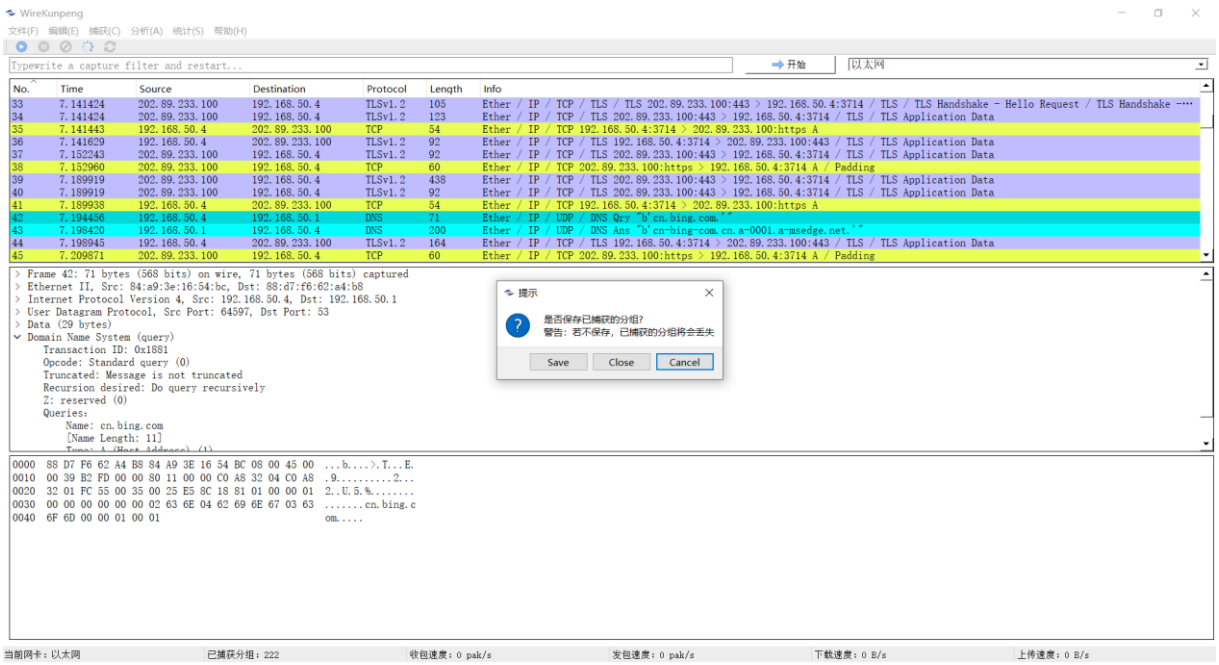


效果展示如下：



3.6　保存及打开 pcap 文件功能说明

本软件可将捕获到的数据包另存为 pcap 文件；也可打开 pcap 文件进行数据包解析。



3.7　过滤器功能说明

过滤器使用 BPF（Berkeley Packet Filter）语法。需要先行填写正确过滤语法后再开始抓包。

如：port 53