

目录

主页模块.....1

离线检测模块.....2

设置模块.....3

在线检测模块.....4

客户端与服务器的交互.....5

主页模块

Skynet 主页包含三个部分：接口选择、实时上传速度及下载速度、实时流量

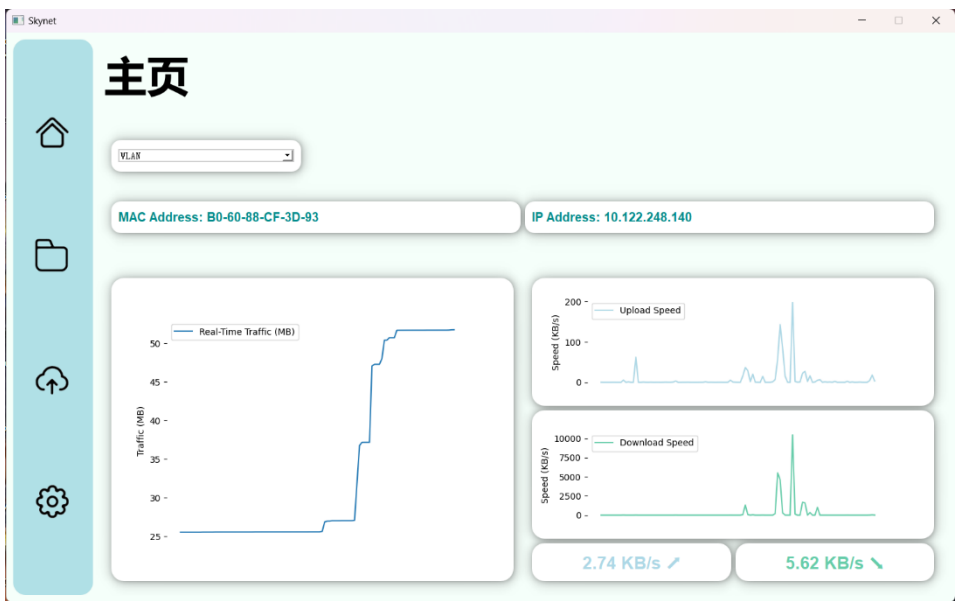


图 1：主页

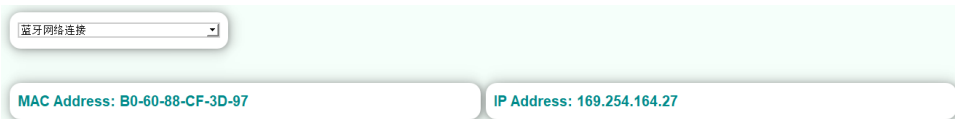


图 2：接口选择

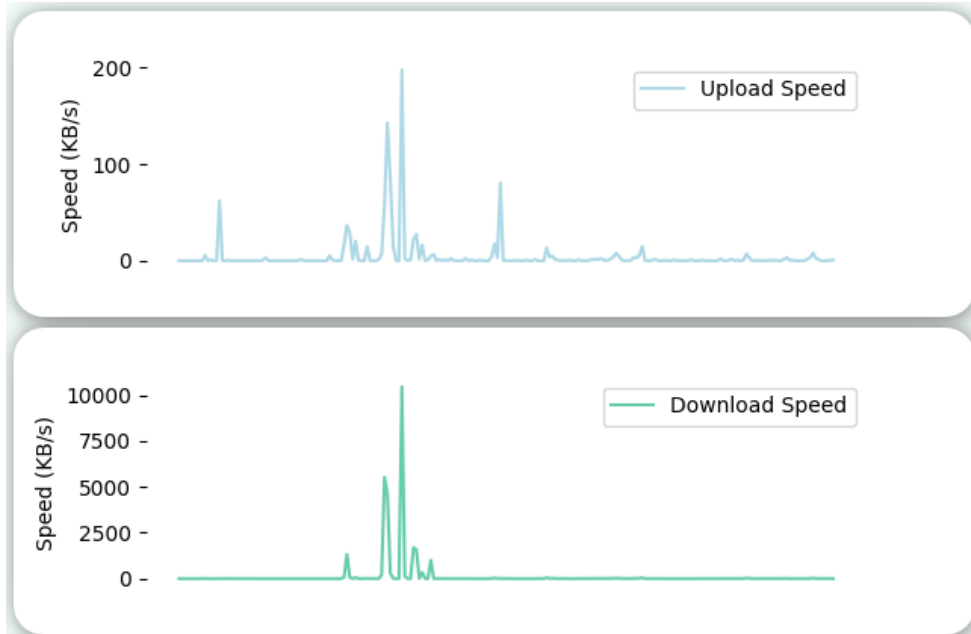


图 3：实时上传速度及下载速度

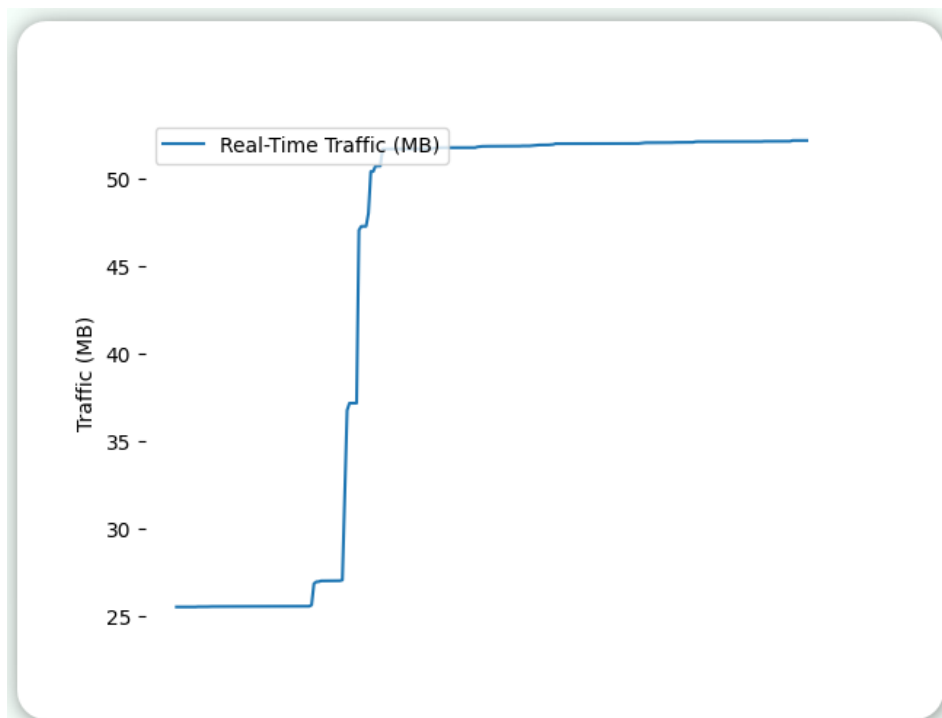


图 4：实时流量

离线检测模块

Skynet 的离线检测模块支持用户上传本地的 pcap 包进行异常检测，服务器端将返回结果图。



图 5：离线检测界面

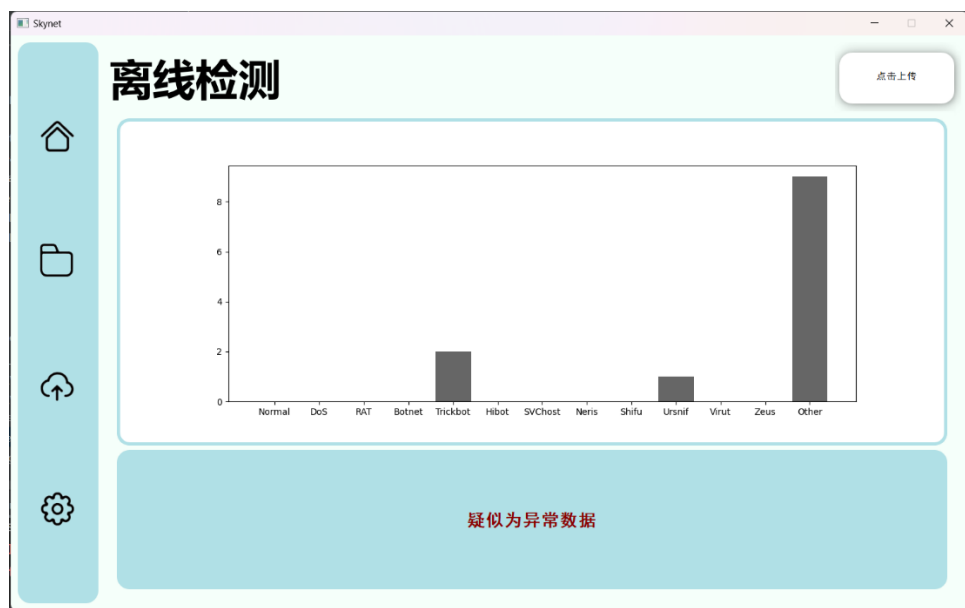


图 6：返回的离线检测结果

设置模块

Skynet 的设置模块用于设置保存文件夹路径。在线检测模块抓取的 pcap 包将存储在这个文件夹中。

注意：必须先设置路径，才能进行实时的抓包和检测

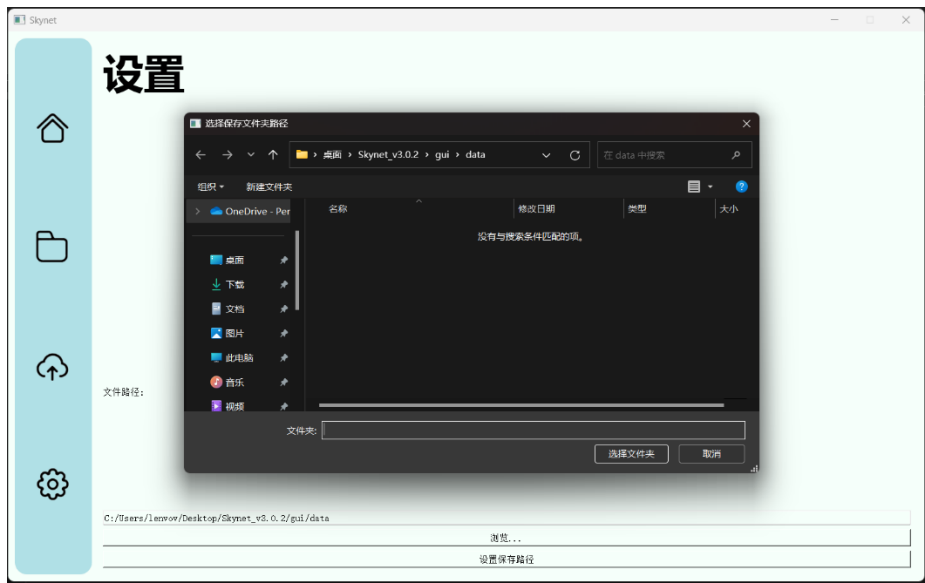


图 7：设置界面

在线检测模块

Skynet 的在线检测模块支持用户进行实时的抓包和异常检测,服务器端将返回结果图。



图 8：在线检测界面

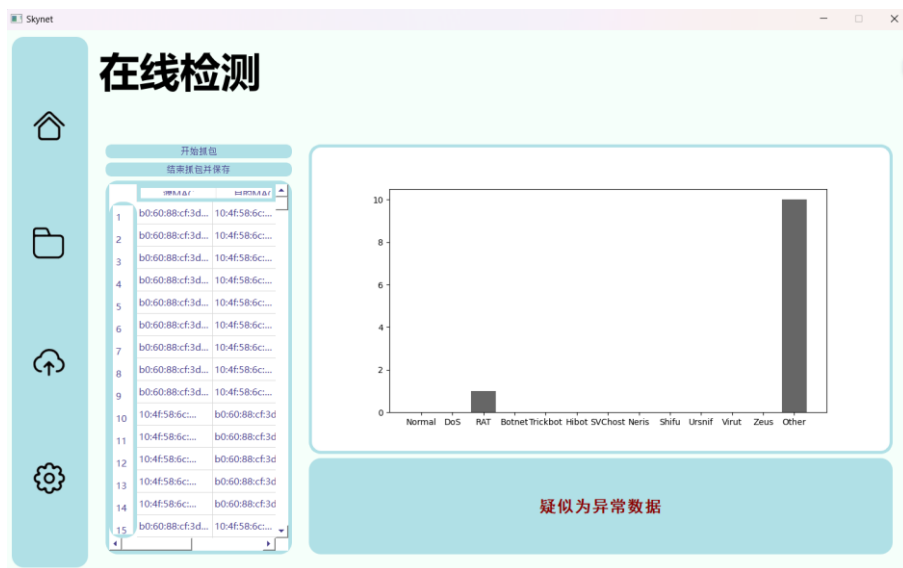


图 9：返回的在线检测结果

客户端与服务器的交互

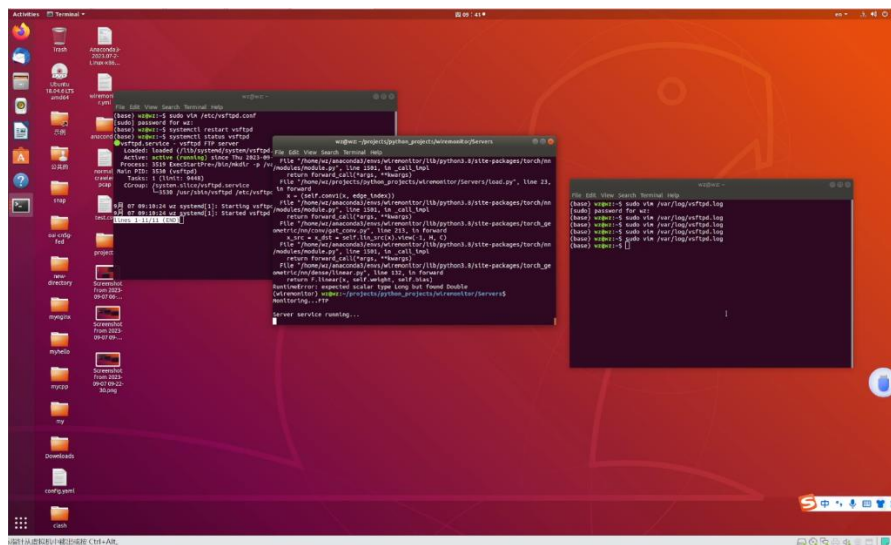
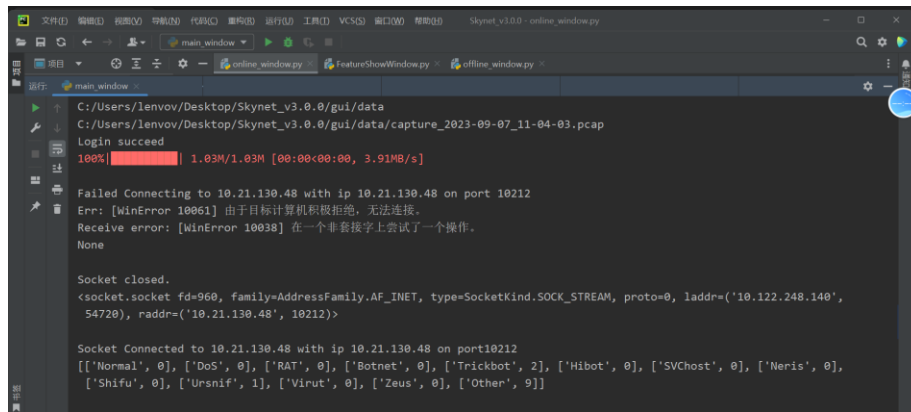


图 10：服务器监听响应



```

C:/Users/lenov/Desktop/Skynet_v3.0.0/gui/data
C:/Users/lenov/Desktop/Skynet_v3.0.0/gui/data/capture_2023-09-07_11-04-03.pcap
Login succeed
100%|██████████| 1.03M/1.03M [00:00<00:00, 3.91MB/s]

Failed Connecting to 10.21.130.48 with ip 10.21.130.48 on port 10212
Err: [WinError 10061] 由于目标计算机积极拒绝，无法连接。
Receive error: [WinError 10038] 在一个非套接字上尝试了一个操作。
None

Socket closed.
<socket.socket fd=960, family=AddressFamily.AF_INET, type=SocketKind.SOCK_STREAM, proto=0, laddr=('10.122.248.140', 54720), raddr=('10.21.130.48', 10212)>

Socket Connected to 10.21.130.48 with ip 10.21.130.48 on port10212
[['Normal', 0], ['DoS', 0], ['RAT', 0], ['Botnet', 0], ['Trickbot', 2], ['Hibot', 0], ['SVChost', 0], ['Neris', 0],
['Shifu', 0], ['Ursnif', 1], ['Virut', 0], ['Zeus', 0], ['Other', 9]]

```

图 11: 客户端收到服务器的回显