IPv4流量分析程序报告

学号：2120250723

姓名：于成俊

一、编程环境

- 操作系统：Windows 11
- 需**使用管理员权限**启动 Python 解释器（否则无法启用 RCVALL）
- Python 版本：**3.7~3.12** 均可
- 必要库（全部为 Python 标准库，无需安装第三方）
    - `socket`：创建原始套接字、绑定、本地抓包
    - `struct`：解析二进制 IPv4/TCP/UDP/ICMP 头部
    - `threading`：抓包线程，避免阻塞 GUI
    - `tkinter`：图形用户界面 GUI
    - `datetime`：时间戳、报告生成
    - `csv`：将流量分析导出为 CSV
    - `sys`：显示平台信息、退出程序等
    - `binascii`：十六进制转换，用于显示 HexDump

二、关键问题说明

- **Windows 原始套接字的限制：**Windows 不允许像 Linux 那样使用原始套接字对任意网卡进行"混杂模式"抓包，只能捕获 **发往本地 IP 的流量**（非全部网卡混杂流量）
- **多线程与 GUI 冲突：**抓包是阻塞操作，必须使用：
    - `threading.Thread`
    - 使用 `root.after(0, ...)` 将更新任务安全地投递回主线程

  否则 GUI 会卡死。
- **IPv4/TCP/UDP/ICMP 逐层解析：**程序需要手工解析：
    - IPv4 20 字节头部
    - TCP 20 字节 + 可变头部
    - UDP 8 字节
    - ICMP 4 字节

  并根据端口或负载进行启发式协议识别（HTTP/DNS/DHCP）
- **捕获过滤条件：**用户输入过滤条件格式支持：

```
单个 IP：   192.168.1.8
双方 IP：   192.168.1.8,192.168.1.3
```

并用于过滤：

  - 单端过滤（src==IP 或 dst==IP）
  - 双向过滤（src–dst 成对）

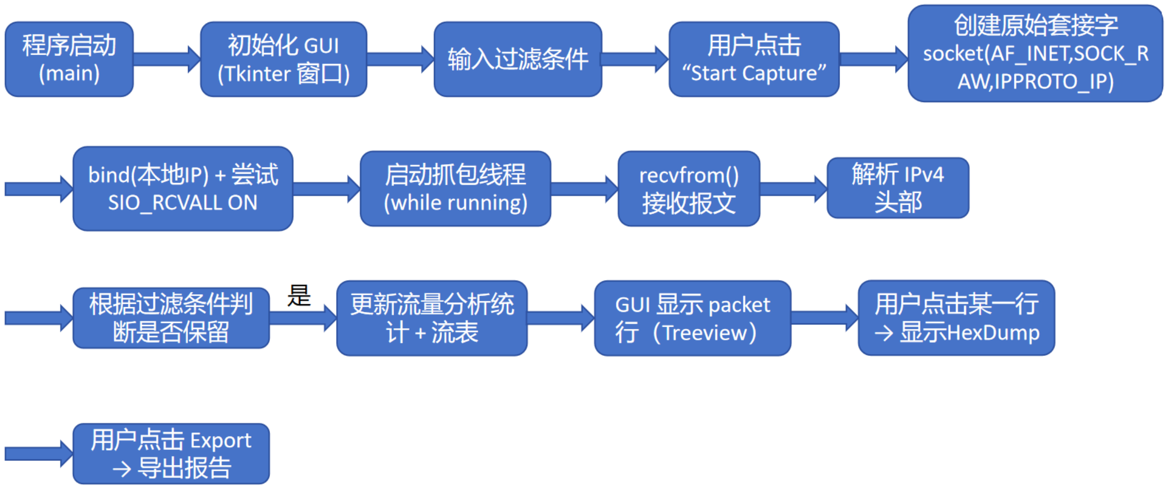
- **流量分析：**统计内容包括：
  - IPv4 总包数
  - TCP/UDP/ICMP/OTHER 计数
  - 高层协议计数（HTTP/DNS/DHCP）
  - 流表（src,dst,proto → packet_count）

  可导出 TXT 或 CSV 报告。

- **定义“关闭窗口按钮”的行为（右上角 X 按钮）**：

  当用户点击关闭时，程序要停止抓包线程、关闭 raw socket、停止 RCVALL，以避免程序退出时 socket 没关闭导致程序挂死或残留系统资源。

三、程序流程图

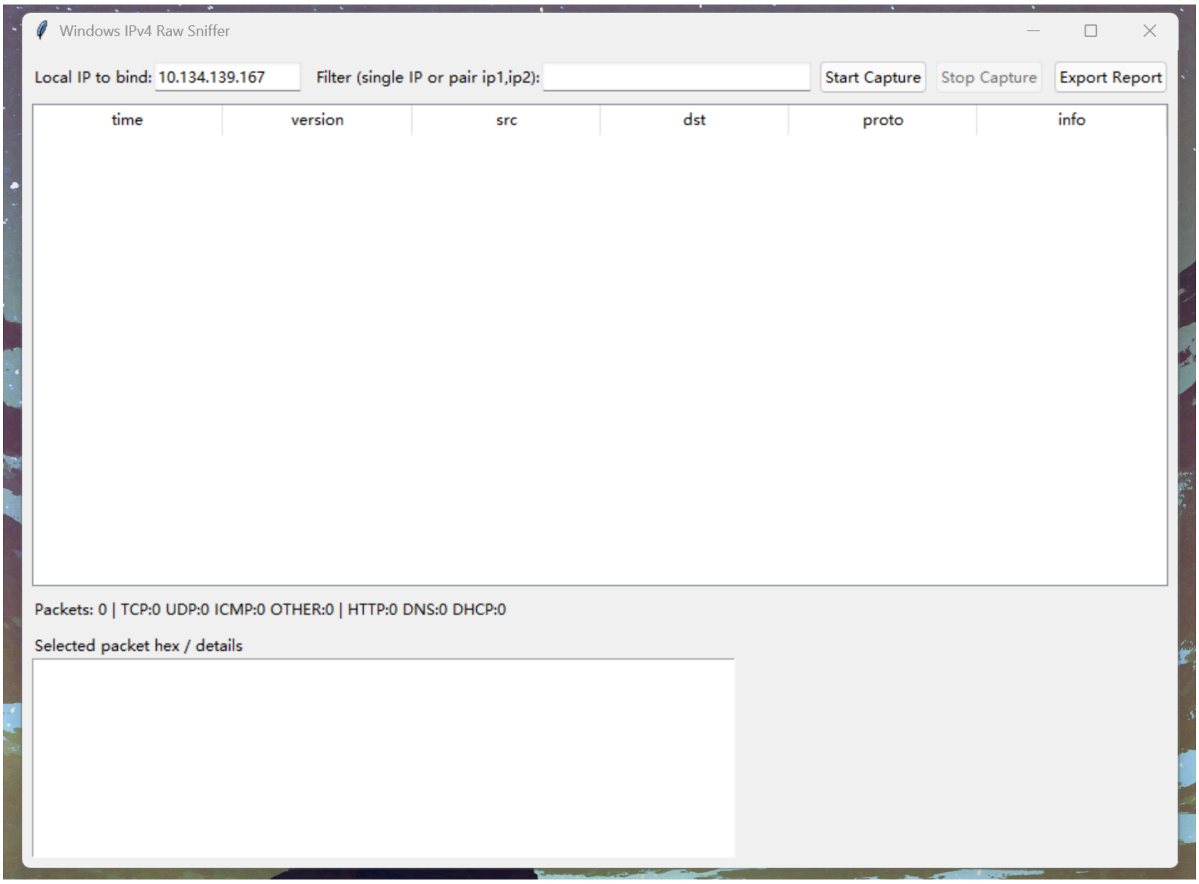


四、测试截图

1.程序启动界面

主要模块：

- Local IP to bind 输入框：输入本地IP地址，进行绑定
- Filter(single IP or pair ip1,ip2）输入框：过滤条件
- Start Capture 按钮：开始捕获包
- Stop Capture 按钮：停止捕获包
- Export Report 按钮：导出报告
- Select packet hex / details：显示所选包的详细信息



Local IP to bind: 10.134.139.167

Filter (single IP or pair ip1,ip2):

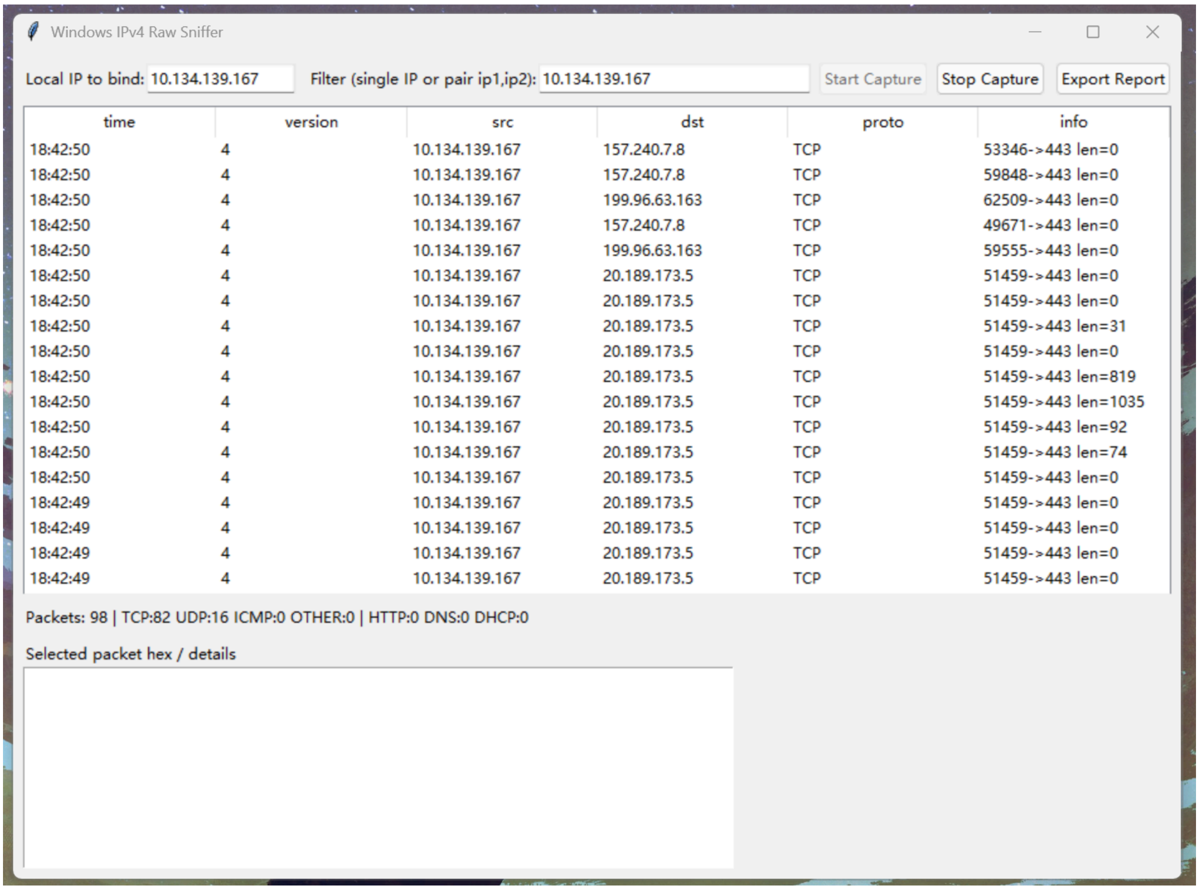
time	version	src	dst	proto	info

Packets: 0 | TCP:0 UDP:0 ICMP:0 OTHER:0 | HTTP:0 DNS:0 DHCP:0

Selected packet hex / details

2.输入捕获条件进行捕获

- 单端过滤：



Local IP to bind: 10.134.139.167

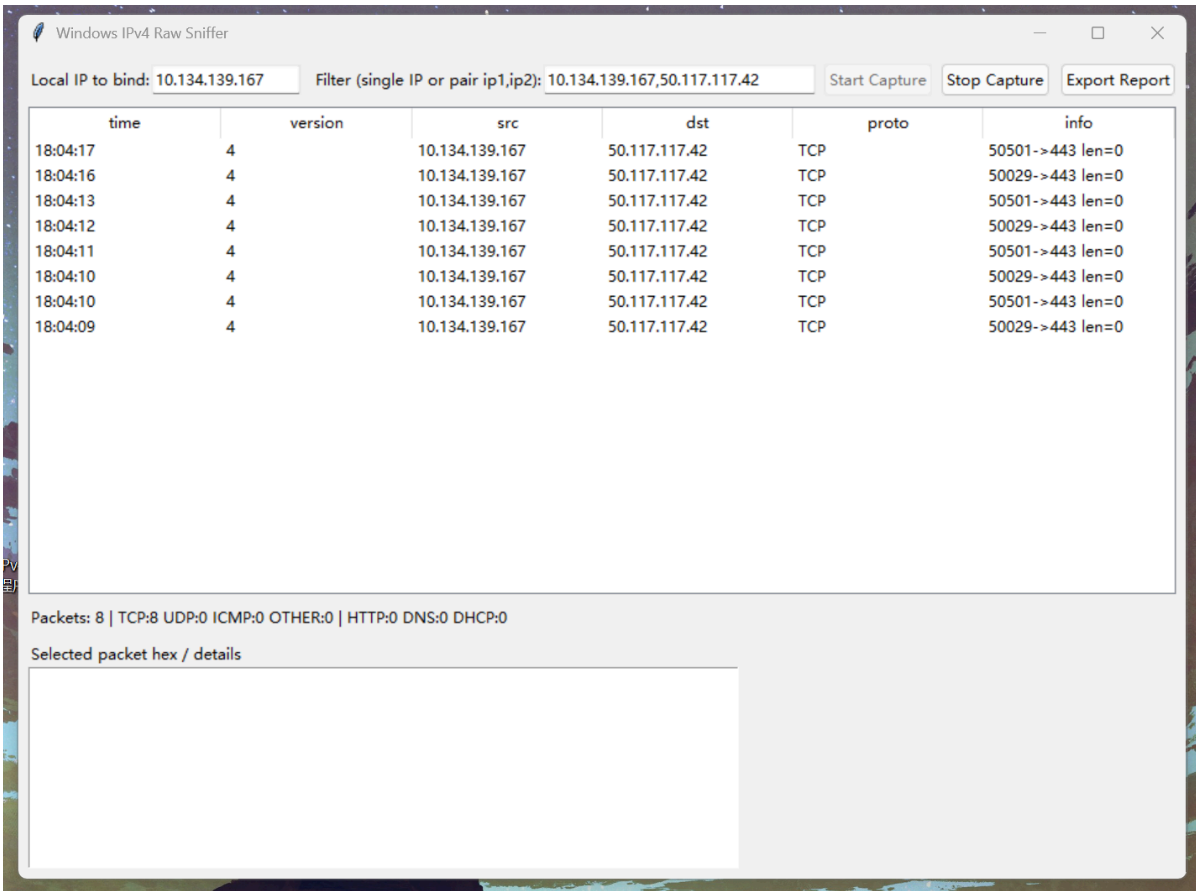
Filter (single IP or pair ip1,ip2): 10.134.139.167

time	version	src	dst	proto	info
18:42:50	4	10.134.139.167	157.240.7.8	TCP	53346->443 len=0
18:42:50	4	10.134.139.167	157.240.7.8	TCP	59848->443 len=0
18:42:50	4	10.134.139.167	199.96.63.163	TCP	62509->443 len=0
18:42:50	4	10.134.139.167	157.240.7.8	TCP	49671->443 len=0
18:42:50	4	10.134.139.167	199.96.63.163	TCP	59555->443 len=0
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=31
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=819
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=1035
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=92
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=74
18:42:50	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:49	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:49	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:49	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0
18:42:49	4	10.134.139.167	20.189.173.5	TCP	51459->443 len=0

Packets: 98 | TCP:82 UDP:16 ICMP:0 OTHER:0 | HTTP:0 DNS:0 DHCP:0

Selected packet hex / details

- 双向过滤：



Local IP to bind: 10.134.139.167

Filter (single IP or pair ip1,ip2): 10.134.139.167,50.117.117.42

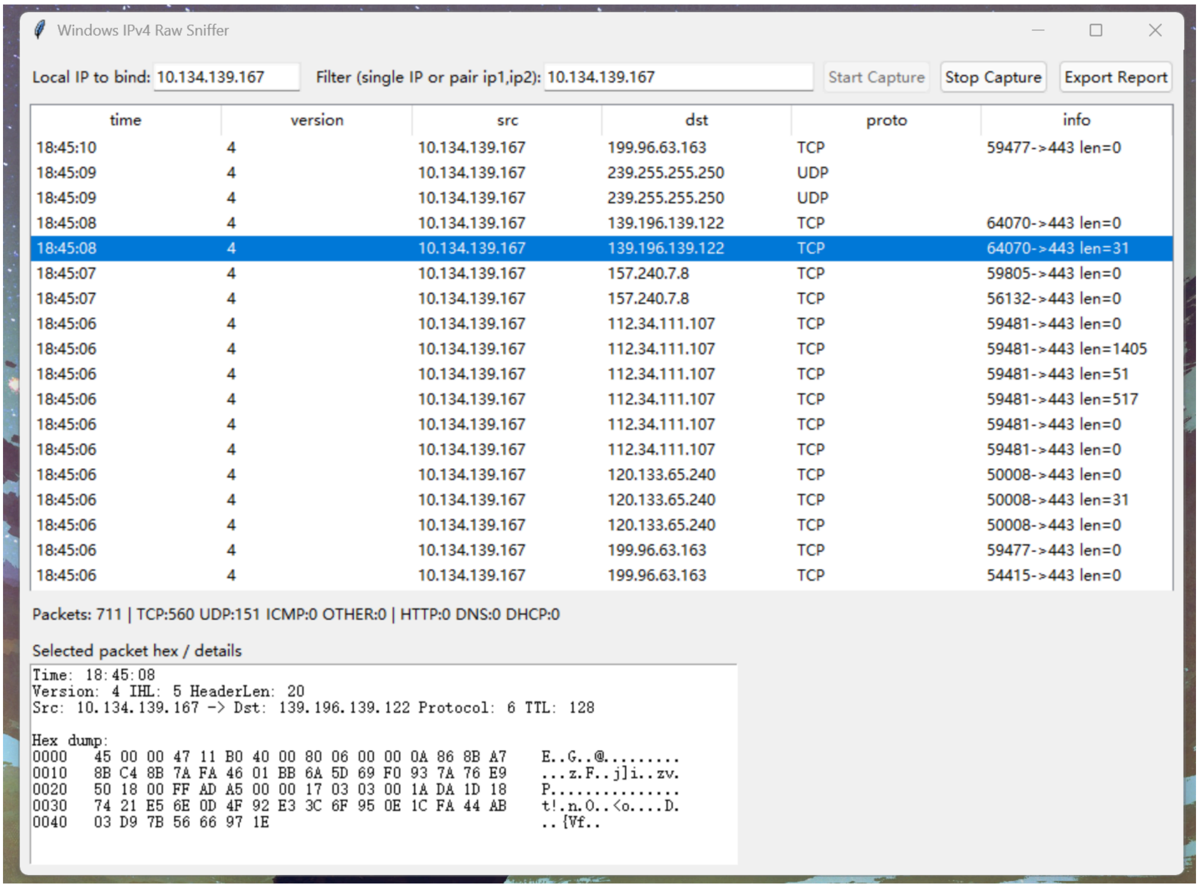
time	version	src	dst	proto	info
18:04:17	4	10.134.139.167	50.117.117.42	TCP	50501->443 len=0
18:04:16	4	10.134.139.167	50.117.117.42	TCP	50029->443 len=0
18:04:13	4	10.134.139.167	50.117.117.42	TCP	50501->443 len=0
18:04:12	4	10.134.139.167	50.117.117.42	TCP	50029->443 len=0
18:04:11	4	10.134.139.167	50.117.117.42	TCP	50501->443 len=0
18:04:10	4	10.134.139.167	50.117.117.42	TCP	50029->443 len=0
18:04:10	4	10.134.139.167	50.117.117.42	TCP	50501->443 len=0
18:04:09	4	10.134.139.167	50.117.117.42	TCP	50029->443 len=0

Packets: 8 | TCP:8 UDP:0 ICMP:0 OTHER:0 | HTTP:0 DNS:0 DHCP:0

Selected packet hex / details

3.点击某包显示十六进制

点击一个捕获的包，可在`Selected packet hex/details`中显示详细信息：



Local IP to bind: 10.134.139.167

Filter (single IP or pair ip1,ip2): 10.134.139.167

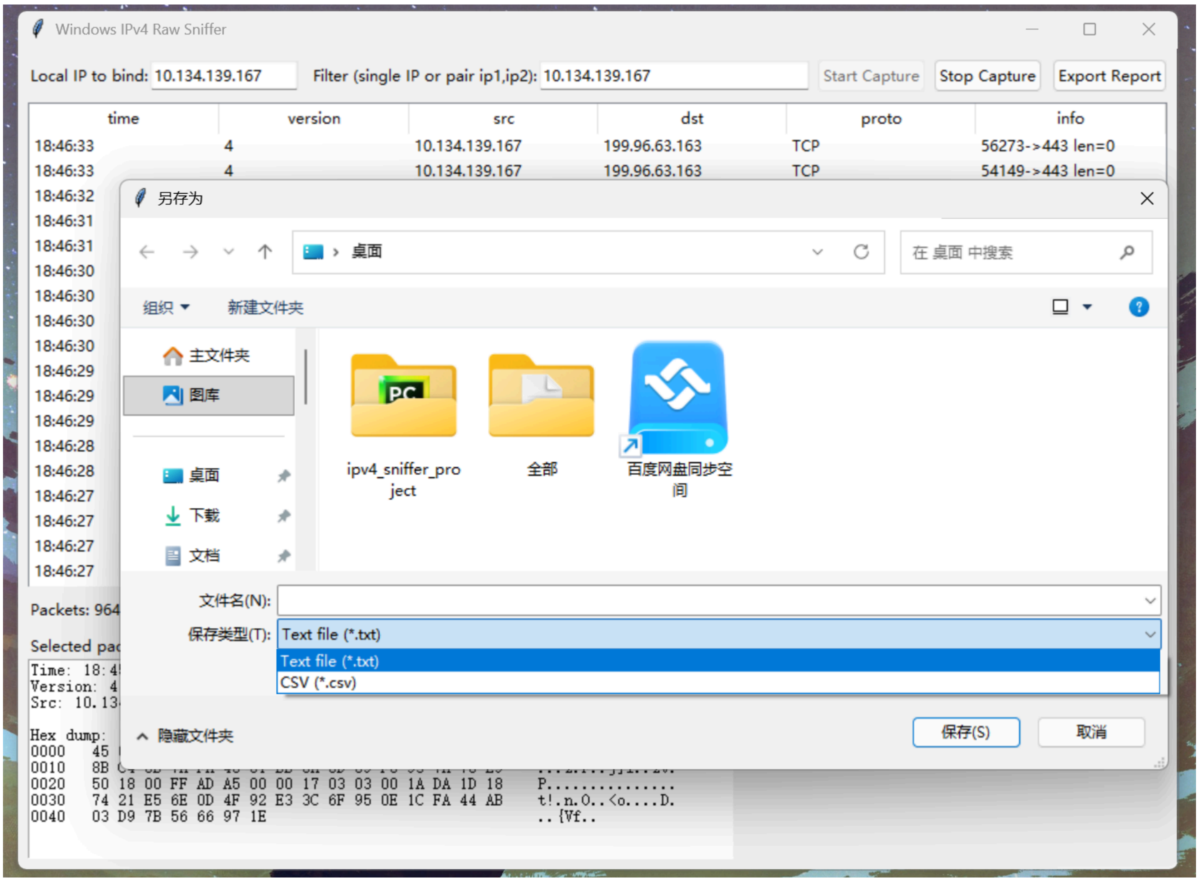
time	version	src	dst	proto	info
18:45:10	4	10.134.139.167	199.96.63.163	TCP	59477->443 len=0
18:45:09	4	10.134.139.167	239.255.255.250	UDP	
18:45:09	4	10.134.139.167	239.255.255.250	UDP	
18:45:08	4	10.134.139.167	139.196.139.122	TCP	64070->443 len=0
18:45:08	4	10.134.139.167	139.196.139.122	TCP	64070->443 len=31
18:45:07	4	10.134.139.167	157.240.7.8	TCP	59805->443 len=0
18:45:07	4	10.134.139.167	157.240.7.8	TCP	56132->443 len=0
18:45:06	4	10.134.139.167	112.34.111.107	TCP	59481->443 len=0
18:45:06	4	10.134.139.167	112.34.111.107	TCP	59481->443 len=1405
18:45:06	4	10.134.139.167	112.34.111.107	TCP	59481->443 len=51
18:45:06	4	10.134.139.167	112.34.111.107	TCP	59481->443 len=517
18:45:06	4	10.134.139.167	112.34.111.107	TCP	59481->443 len=0
18:45:06	4	10.134.139.167	112.34.111.107	TCP	59481->443 len=0
18:45:06	4	10.134.139.167	120.133.65.240	TCP	50008->443 len=0
18:45:06	4	10.134.139.167	120.133.65.240	TCP	50008->443 len=31
18:45:06	4	10.134.139.167	120.133.65.240	TCP	50008->443 len=0
18:45:06	4	10.134.139.167	199.96.63.163	TCP	59477->443 len=0
18:45:06	4	10.134.139.167	199.96.63.163	TCP	54415->443 len=0

Packets: 711 | TCP:560 UDP:151 ICMP:0 OTHER:0 | HTTP:0 DNS:0 DHCP:0

Selected packet hex / details

```
Time: 18:45:08
Version: 4 IHL: 5 HeaderLen: 20
Src: 10.134.139.167 -> Dst: 139.196.139.122 Protocol: 6 TTL: 128

Hex dump:
0000   45 00 00 47 11 B0 40 00 80 06 00 00 0A 86 8B A7    E..G..@.........
0010   8B C4 8B 7A FA 46 01 BB 6A 5D 69 F0 93 7A 76 E9    ...z.F..j]i..zv.
0020   50 18 00 FF AD A5 00 00 17 03 03 00 1A DA 1D 18    P...............
0030   74 21 E5 6E 0D 4F 92 E3 3C 6F 95 0E 1C FA 44 AB    t!.n.O..<o....D.
0040   03 D9 7B 56 66 97 1E                               ..{Vf..
```

4.导出报告



Local IP to bind: 10.134.139.167

Filter (single IP or pair ip1,ip2): 10.134.139.167

time	version	src	dst	proto	info
18:46:33	4	10.134.139.167	199.96.63.163	TCP	56273->443 len=0
18:46:33	4	10.134.139.167	199.96.63.163	TCP	54149->443 len=0
18:46:32					
18:46:31					
18:46:31					
18:46:30					
18:46:30					
18:46:30					
18:46:30					
18:46:29					
18:46:29					
18:46:29					
18:46:28					
18:46:28					
18:46:27					
18:46:27					
18:46:27					
18:46:27					

Packets: 964

Selected pa

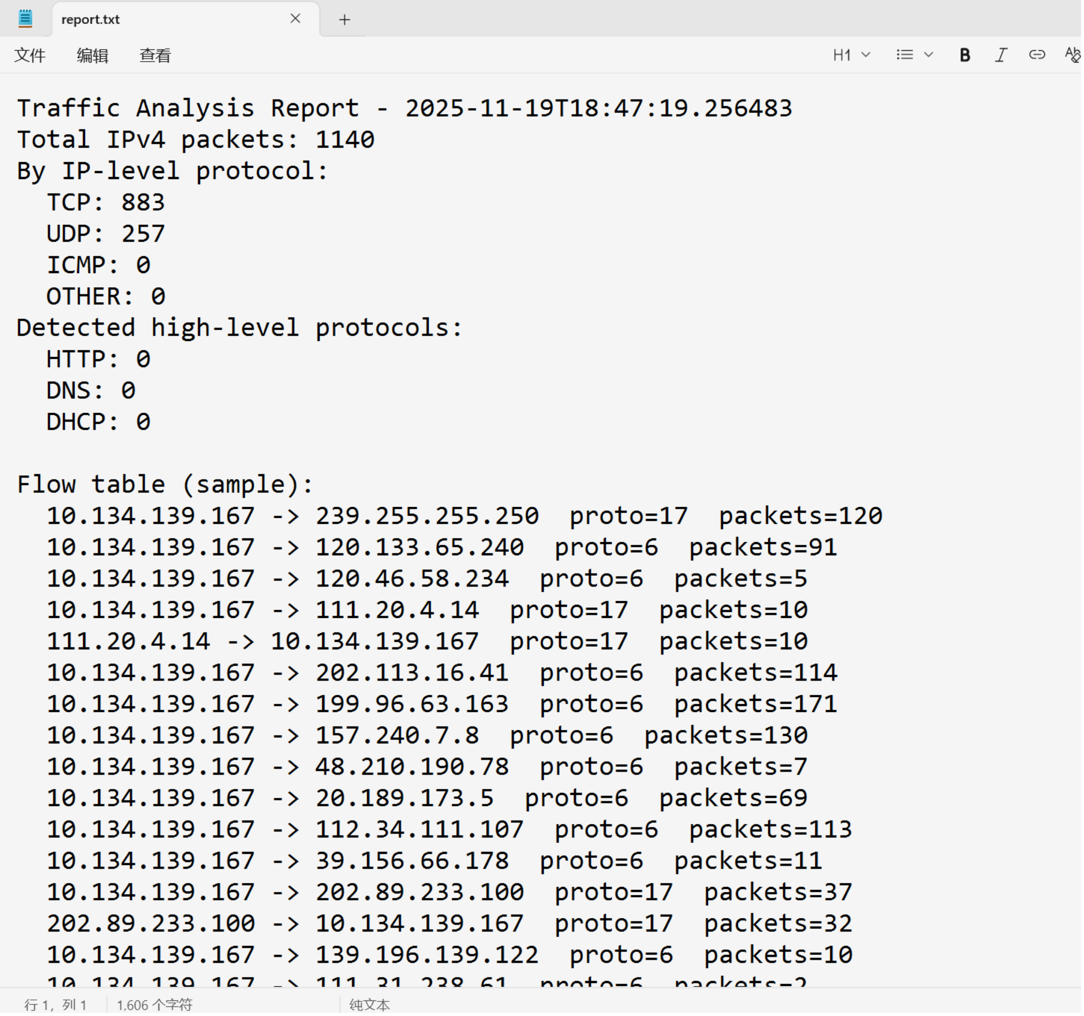
```
Time:  18:4
Version:  4
Src:  10.13

Hex  dump:
0000    45
0010    8B
0020    50 18 00 FF AD A5 00 00 17 03 03 00 1A DA 1D 18    P...............
0030    74 21 E5 6E 0D 4F 92 E3 3C 6F 95 0E 1C FA 44 AB    t!.n.O..<o....D.
0040    03 D9 7B 56 66 97 1E                                ..{Vf..
```

文件名(N):

保存类型(T): Text file (*.txt)

Text file (*.txt)
CSV (*.csv)

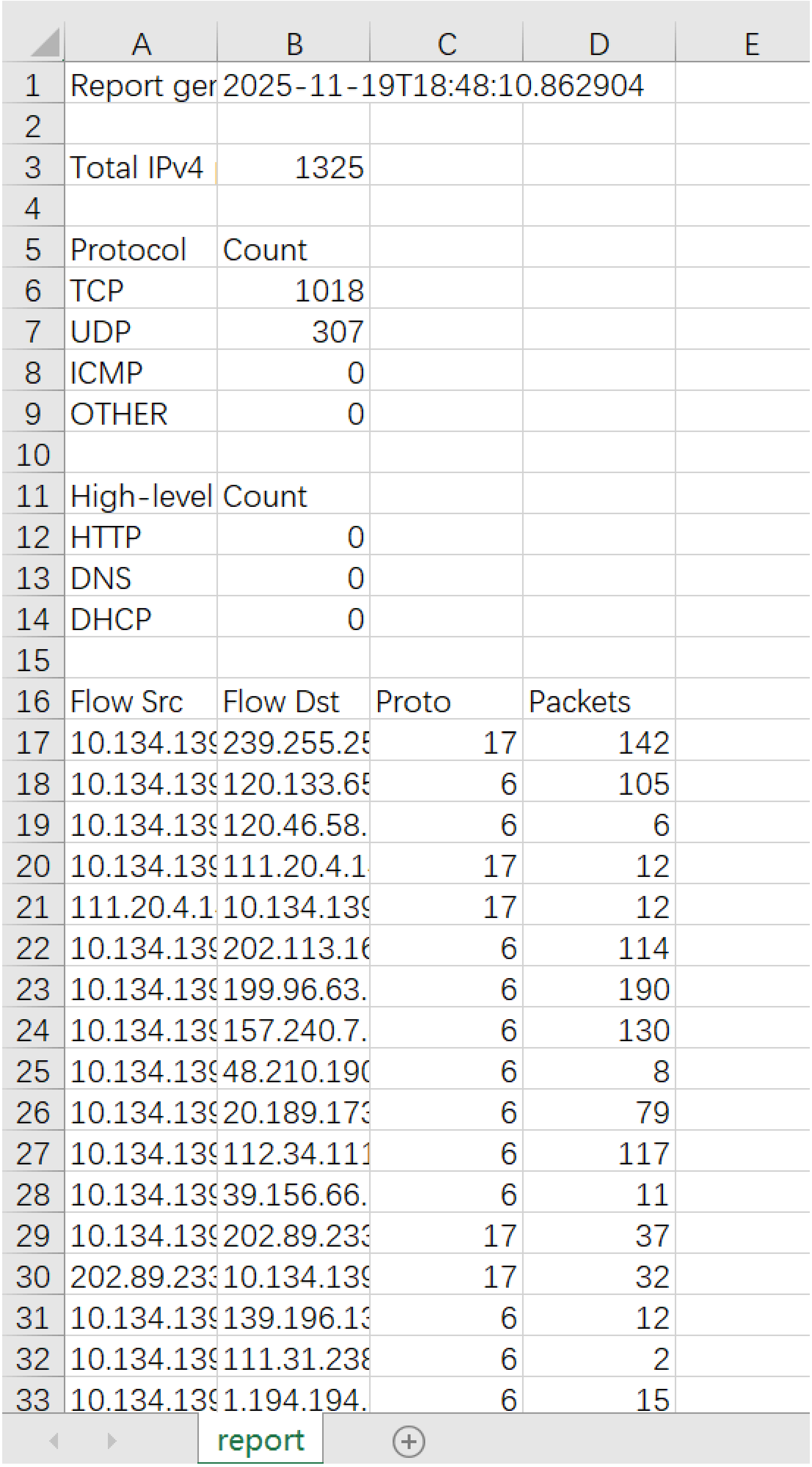
- 导出txt报告：



```
Traffic Analysis Report - 2025-11-19T18:47:19.256483
Total IPv4 packets: 1140
By IP-level protocol:
  TCP: 883
  UDP: 257
  ICMP: 0
  OTHER: 0
Detected high-level protocols:
  HTTP: 0
  DNS: 0
  DHCP: 0

Flow table (sample):
  10.134.139.167 -> 239.255.255.250  proto=17  packets=120
  10.134.139.167 -> 120.133.65.240  proto=6  packets=91
  10.134.139.167 -> 120.46.58.234  proto=6  packets=5
  10.134.139.167 -> 111.20.4.14  proto=17  packets=10
  111.20.4.14 -> 10.134.139.167  proto=17  packets=10
  10.134.139.167 -> 202.113.16.41  proto=6  packets=114
  10.134.139.167 -> 199.96.63.163  proto=6  packets=171
  10.134.139.167 -> 157.240.7.8  proto=6  packets=130
  10.134.139.167 -> 48.210.190.78  proto=6  packets=7
  10.134.139.167 -> 20.189.173.5  proto=6  packets=69
  10.134.139.167 -> 112.34.111.107  proto=6  packets=113
  10.134.139.167 -> 39.156.66.178  proto=6  packets=11
  10.134.139.167 -> 202.89.233.100  proto=17  packets=37
  202.89.233.100 -> 10.134.139.167  proto=17  packets=32
  10.134.139.167 -> 139.196.139.122  proto=6  packets=10
  10.134.139.167 -> 111.31.238.61  proto=6  packets=2
```

行 1，列 1　1,606 个字符　纯文本

- 导出csv报告：



	A	B	C	D	E
1	Report ger	2025-11-19T18:48:10.862904			
2					
3	Total IPv4	1325			
4					
5	Protocol	Count			
6	TCP	1018			
7	UDP	307			
8	ICMP	0			
9	OTHER	0			
10					
11	High-level	Count			
12	HTTP	0			
13	DNS	0			
14	DHCP	0			
15					
16	Flow Src	Flow Dst	Proto	Packets	
17	10.134.139	239.255.25	17	142	
18	10.134.139	120.133.65	6	105	
19	10.134.139	120.46.58.	6	6	
20	10.134.139	111.20.4.1	17	12	
21	111.20.4.1	10.134.139	17	12	
22	10.134.139	202.113.16	6	114	
23	10.134.139	199.96.63.	6	190	
24	10.134.139	157.240.7.	6	130	
25	10.134.139	48.210.190	6	8	
26	10.134.139	20.189.173	6	79	
27	10.134.139	112.34.111	6	117	
28	10.134.139	39.156.66.	6	11	
29	10.134.139	202.89.233	17	37	
30	202.89.233	10.134.139	17	32	
31	10.134.139	139.196.13	6	12	
32	10.134.139	111.31.238	6	2	
33	10.134.139	1.194.194.	6	15	