# 网络协议分析软件用户手册

## 1. 软件概述

### 1.1 软件简介

网络协议分析软件是一款功能强大的网络数据包捕获和分析工具，支持实时数据包捕获、协议识别、数据包解码、统计分析等功能。软件提供命令行和图形界面两种交互方式，适合网络管理员、安全分析师、开发人员等各类用户使用。

### 1.2 主要功能

- 实时网络数据包捕获
- 支持 BPF 过滤规则
- 自动协议识别（TCP、UDP、HTTP、DNS、ICMP 等）
- 详细的数据包解码
- 协议统计与可视化
- PCAP 文件导入/导出
- 支持浅色/深色主题切换
- 友好的图形用户界面
- 灵活的命令行接口

### 1.3 应用场景

- 网络故障排查
- 网络性能分析
- 安全威胁检测
- 协议开发与调试
- 网络流量监控
- 教学与研究

## 2. 系统要求

### 2.1 硬件要求

- CPU：双核处理器或更高

- 内存：2GB RAM 或更高
- 硬盘：100MB 可用空间
- 网络接口：至少一个可用的网络接口

### 2.2 软件要求

- 操作系统：Windows 7/8/10/11
- Python 版本：Python 3.8 或更高
- 依赖库：Scapy, PyQt5 等（详见 requirements.txt）

## 3. 使用方法

### 3.1 命令行界面使用

#### 3.1.1 基本语法

```
python main.py [选项] [参数]
```

#### 3.1.2 主要选项

| 选项 | 说明 | 示例 |
| --- | --- | --- |
| `-i, --interface` | 指定网络接口 | `-i "Ethernet 2"` |
| `-c, --count` | 捕获数据包数量 | `-c 100` |
| `-f, --filter` | BPF 过滤规则 | `-f "tcp port 80"` |
| `-o, --output` | 输出 PCAP 文件路径 | `-o capture.pcap` |
| `-r, --read` | 读取 PCAP 文件进行分析 | `-r capture.pcap` |
| `--help` | 显示帮助信息 | `--help` |

表 1 选项

#### 3.1.3 使用示例

**示例 1：列出可用网络接口**

```
python main.py
```

**示例 2：捕获指定数量的数据包**

```
python main.py -i "Ethernet 2" -c 100
```

**示例 3：使用 BPF 过滤规则捕获 TCP 数据包**

```
python main.py -i "Ethernet 2" -c 50 -f "tcp port 80"
```

**示例 4：捕获并保存数据包到 PCAP 文件**

```
python main.py -i "Ethernet 2" -c 100 -o capture.pcap
```

**示例 5：分析已有的 PCAP 文件**

```
python main.py -r capture.pcap
```

### 3.2 图形界面使用

#### 3.2.1 启动图形界面

```
python qt_gui.py
```

#### 3.2.2 主界面介绍

图形界面主要包括以下几个部分：

1. 菜单栏：包含文件、捕获、分析、视图、帮助等菜单
2. 工具栏：提供常用操作的快捷按钮
3. 控制面板：用于配置捕获参数
4. 数据包列表：显示捕获的数据包摘要信息
5. 数据包详情：显示选中数据包的详细解码信息
6. 统计视图：显示协议分布统计信息
7. 接口状态：显示网络接口状态信息

#### 3.2.3 基本操作流程

**步骤 1：选择网络接口**

1. 在控制面板中，从"网络接口"下拉菜单中选择一个可用的网络接口
2. 如果接口列表为空，点击"刷新接口"按钮

**步骤 2：配置捕获参数**

1. 设置"捕获数量"（可选，默认为 100）
2. 输入 BPF 过滤规则（可选）
3. 选择是否保存到 PCAP 文件（可选）

**步骤 3：开始捕获**

1. 点击"开始捕获"按钮

2. 查看数据包列表中的实时捕获结果

**步骤 4：查看数据包详情**

1. 在数据包列表中点击任意数据包
2. 在下方"数据包详情"区域查看详细的解码信息

**步骤 5：查看统计信息**

1. 切换到"统计视图"标签页
2. 查看协议分布统计图表

**步骤 6：停止捕获**

1. 点击"停止捕获"按钮
2. 捕获过程结束，可继续分析已捕获的数据包

### 3.2.4 高级功能

**PCAP 文件导入/导出**

- 导入 PCAP 文件：

1. 点击菜单栏"文件" → "打开 PCAP 文件"
2. 选择要导入的 PCAP 文件
3. 查看导入的数据包

- 导出 PCAP 文件：

1. 捕获数据包或导入 PCAP 文件
2. 点击菜单栏"文件" → "保存 PCAP 文件"
3. 选择保存路径和文件名

**主题切换**

1. 点击菜单栏"视图" → "切换主题"
2. 软件将在浅色主题和深色主题之间切换

**数据包过滤**

1. 在数据包列表上方的搜索框中输入过滤条件

2. 按回车键或点击搜索按钮

3. 数据包列表将只显示符合条件的数据包

## 4. 功能特点

### 4.1 实时捕获功能

- 支持从多个网络接口同时捕获
- 可配置捕获数量和超时时间
- 实时显示捕获的数据包
- 支持后台捕获模式

### 4.2 协议识别功能

- 自动识别多种网络协议
- 支持分层协议识别（数据链路层到应用层）
- 高准确率的应用层协议识别
- 可扩展的协议识别框架

### 4.3 数据包解码功能

- 详细的协议字段解码
- 支持嵌套协议解码
- 格式化的解码输出
- 支持原始数据查看

### 4.4 统计分析功能

- 实时协议统计
- 可视化的统计图表
- 支持导出统计报告
- 协议分布分析
- 流量趋势分析

### 4.5 用户界面功能

- 直观的图形界面
- 支持拖拽操作
- 可定制的界面布局
- 支持快捷键操作
- 友好的错误提示

# 5. 协议支持

## 5.1 支持的协议列表

| 协议层级 | 支持的协议 |
| --- | --- |
| 数据链路层 | Ethernet |
| 网络层 | IP, IPv6, ARP, ICMP |
| 传输层 | TCP, UDP |
| 应用层 | HTTP, DNS, DHCP, FTP, SMTP, POP3, IMAP, SSH, TLS/SSL |

**表 2 支持的协议**

## 5.2 协议识别特征

| 协议 | 识别特征 |
| --- | --- |
| HTTP | TCP 端口 80 或 443，数据载荷包含 HTTP 方法或状态码 |
| DNS | UDP 或 TCP 端口 53，数据载荷符合 DNS 报文格式 |
| DHCP | UDP 端口 67 或 68，数据载荷符合 DHCP 报文格式 |
| FTP | TCP 端口 21，数据载荷包含 FTP 命令或响应 |
| SMTP | TCP 端口 25，数据载荷包含 SMTP 命令或响应 |
| SSH | TCP 端口 22，数据载荷符合 SSH 协议格式 |

**表 3 协议识别特征**

# 6. 常见问题与解决方法

## 6.1 捕获相关问题

| 问题 | 解决方法 |
| --- | --- |
| 无法找到网络接口 | 以管理员身份运行软件，或检查网络接口是否正常工作 |
| 捕获到的数据包为 0 | 检查过滤规则是否正确，或网络接口是否有流量 |
| 捕获过程中程序崩溃 | 减少捕获数量，或优化系统资源使用 |
| 权限不足导致捕获失败 | 使用管理员权限运行软件，或添加用户到相应组（Linux/macOS） |

**表 4 捕获功能相关问题**

## 6.2 其他问题

| 问题 | 解决方法 |
| --- | --- |
| 软件无法启动 | 检查 Python 版本和依赖库是否符合要求 |
| PCAP 文件无法打开 | 检查文件格式是否正确，或文件是否损坏 |

**表 5 其他问题**

# 7. 免责声明

1. 本软件仅供合法用途使用，请勿用于非法活动
2. 使用本软件捕获和分析网络流量时，请遵守相关法律法规
3. 本软件不保证 100%的协议识别准确率
4. 本软件不承担因使用不当造成的任何损失
5. 请在使用前仔细阅读并理解本免责声明

# 8. 附录

## 8.1 BPF 过滤规则示例

| 过滤规则 | 说明 |
| --- | --- |
| `tcp` | 仅捕获 TCP 数据包 |
| `udp` | 仅捕获 UDP 数据包 |
| `icmp` | 仅捕获 ICMP 数据包 |
| `tcp port 80` | 仅捕获 TCP 端口 80 的数据包（HTTP） |
| `udp port 53` | 仅捕获 UDP 端口 53 的数据包（DNS） |
| `host 192.168.1.1` | 仅捕获与 192.168.1.1 相关的数据包 |
| `src host 192.168.1.1` | 仅捕获源地址为 192.168.1.1 的数据包 |
| `dst host 192.168.1.1` | 仅捕获目标地址为 192.168.1.1 的数据包 |
| `net 192.168.1.0/24` | 仅捕获 192.168.1.0/24 网段的数据包 |
| `tcp and port 80 and host 192.168.1.1` | 仅捕获与 192.168.1.1 相关的 TCP 端口 80 数据包 |

**表 6 BPF 过滤规则**

## 8.2 快捷键列表

| 快捷键 | 功能 |
| --- | --- |
| `Ctrl+O` | 打开 PCAP 文件 |
| `Ctrl+S` | 保存 PCAP 文件 |
| `Ctrl+R` | 开始/停止捕获 |
| `Ctrl+T` | 切换主题 |
| `Ctrl+F` | 查找数据包 |
| `Ctrl+L` | 清除数据包列表 |

| 快捷键 | 功能 |
| --- | --- |
| `Ctrl+Q` | 退出软件 |
| `F5` | 刷新网络接口列表 |
| `F1` | 打开帮助文档 |

**表 7 快捷键列表**

## 8.3 术语表

| 术语 | 解释 |
| --- | --- |
| BPF | Berkeley Packet Filter，伯克利数据包过滤器 |
| PCAP | Packet Capture，数据包捕获文件格式 |
| Scapy | 一个强大的 Python 网络数据包处理库 |
| PyQt5 | Python 的 Qt5 绑定库，用于开发图形界面 |
| DNS | Domain Name System，域名系统 |
| HTTP | Hypertext Transfer Protocol，超文本传输协议 |
| TCP | Transmission Control Protocol，传输控制协议 |
| UDP | User Datagram Protocol，用户数据报协议 |
| IP | Internet Protocol，互联网协议 |
| ARP | Address Resolution Protocol，地址解析协议 |
| ICMP | Internet Control Message Protocol，互联网控制消息协议 |

**表 8 术语**

---

感谢您使用网络协议分析软件！希望本用户手册能帮助您快速掌握软件的使用。