Packetless 网络协议分析器

用户使用说明书

目录

运行环境

本程序依赖于 WinPcap 工作，在使用本程序前请确保您的计算机已经安装了 Winpcap。
您可以在此处获取最新版的 Winpcap 安装程序。

界面介绍

程序的主界面如图 1 所示。各界面元素的说明如下：

① 菜单栏。菜单栏包含了程序的各种命令。
② 工具栏。工具栏上列出了常用的命令。
③ 过滤器栏。用户可以应用或清除捕获过滤器。
④ 数据包概要信息面板。这里列出了捕获到的数据包。点击某一数据包条目您可以在其他两个面板上看到更多关于该数据包的信息。
⑤ 数据包详细信息面板。这里展示了所选数据包各层协议的信息。
⑥ 数据包字节面板。这里十六进制和 Ascii 格式展示了所选数据包的数据内容。
⑦ 统计信息。这里展示了捕获到的数据包总数和各协议类型数据包的数量。

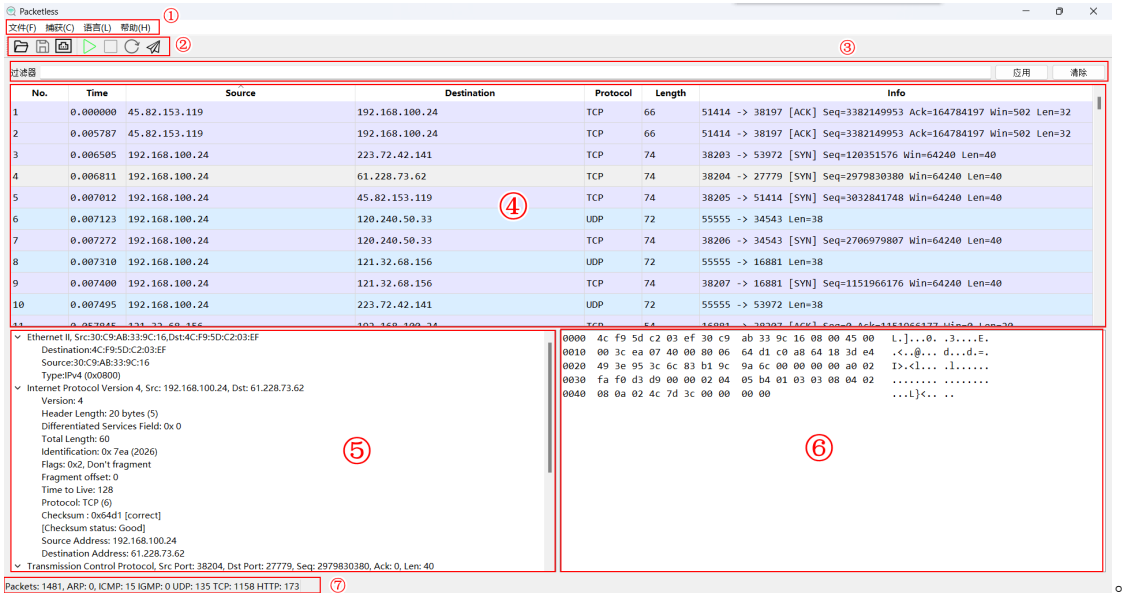


图 1 程序主界面

菜单栏

在文件菜单下，可以打开、保存捕获文件，退出程序。
在捕获菜单下，可以开始捕获、停止捕获和重新开始捕获。
在语言菜单下，可以切换界面的语言。
在帮助菜单下，可以了解有关该软件的信息。

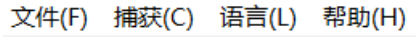


图 2 菜单栏

工具栏

工具栏的按钮从左到右为：打开捕获文件，保存捕获文件，选择网络接口，开始捕获，停止捕获，重新开始捕获，发送数据包。

图 3 工具栏

过滤器栏

在输入框内输入过滤表达式后按回车键或点击“**应用**”按钮应用过滤器。如果过滤表达式应用成功，输入框将变为绿色。应用的过滤器将在下一次捕获时生效。如果过滤表达式语法错误或应用失败，输入框会变成红色，同时弹出错误对话框提示。

在已经应用过滤器时，点击“**清除**”按钮会清除过滤器，输入框内容会变成白色并清空。

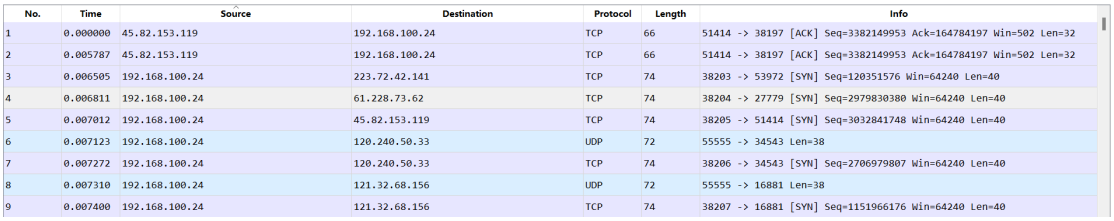
有关过滤表达式的语法请参见 Filtering expression syntax。

图 4 过滤器栏

数据包概要信息面板

这里以表格形式列出了每个数据包的概要信息。表格有七列，分别为：序号、时间、源地址、目的地址、协议类型、数据包长度、数据包信息。

右键点击某一条目可以复制此数据包的信息。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	45.82.153.119	192.168.100.24	TCP	66	51414 -> 38197 [ACK] Seq=3382149953 Ack=164784197 Win=502 Len=32
2	0.005787	45.82.153.119	192.168.100.24	TCP	66	51414 -> 38197 [ACK] Seq=3382149953 Ack=164784197 Win=502 Len=32
3	0.006505	192.168.100.24	223.72.42.141	TCP	74	38203 -> 53972 [SYN] Seq=120351576 Win=64240 Len=40
4	0.006811	192.168.100.24	61.228.73.62	TCP	74	38204 -> 27779 [SYN] Seq=2979830380 Win=64240 Len=40
5	0.007012	192.168.100.24	45.82.153.119	TCP	74	38205 -> 51414 [SYN] Seq=3032841748 Win=64240 Len=40
6	0.007123	192.168.100.24	120.240.50.33	UDP	72	55555 -> 34543 Len=38
7	0.007272	192.168.100.24	120.240.50.33	TCP	74	38206 -> 34543 [SYN] Seq=2706979807 Win=64240 Len=40
8	0.007310	192.168.100.24	121.32.68.156	UDP	72	55555 -> 16881 Len=38
9	0.007400	192.168.100.24	121.32.68.156	TCP	74	38207 -> 16881 [SYN] Seq=1151966176 Win=64240 Len=40

图 5 概要信息面板

数据包详细信息面板

这里以树状结构展示了数据包按协议分层的解析结果。

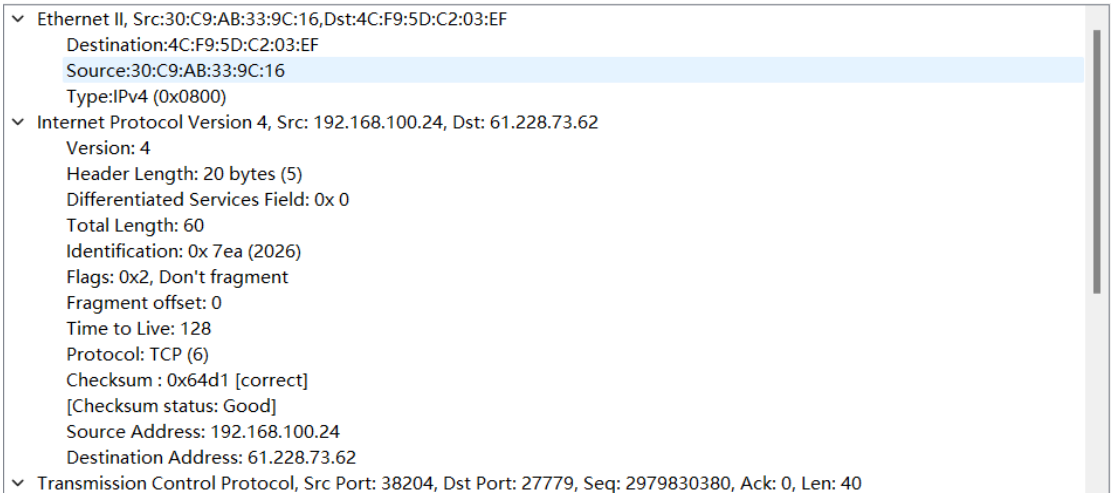


图 6 数据包详细信息面板

数据包字节面板

这里以列出了数据包的具体内容。最左侧是行号，每行有十六字节的内容。中间是十六进制表示的信息。右侧是 Ascii 码表示的信息，不在 Ascii 码表中的字节使用“.”表示。

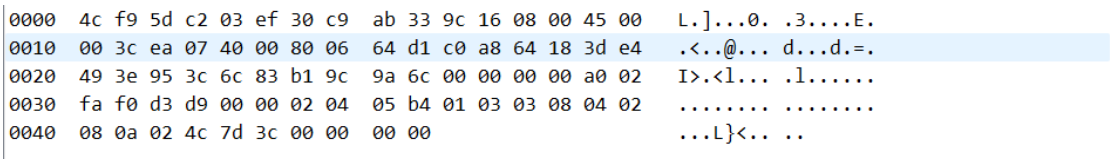


图 7 数据包字节面板

统计信息

这里展示了已捕获的数据包的相关统计信息。Packets 后的数字代表已捕获的数据包总数，ARP 后的数字代表捕获到的 ARP 数据包数量，以此类推。

图 8 统计信息

开始使用

打开应用程序会显示**主界面**和**选择捕获接口界面**（图 9）。

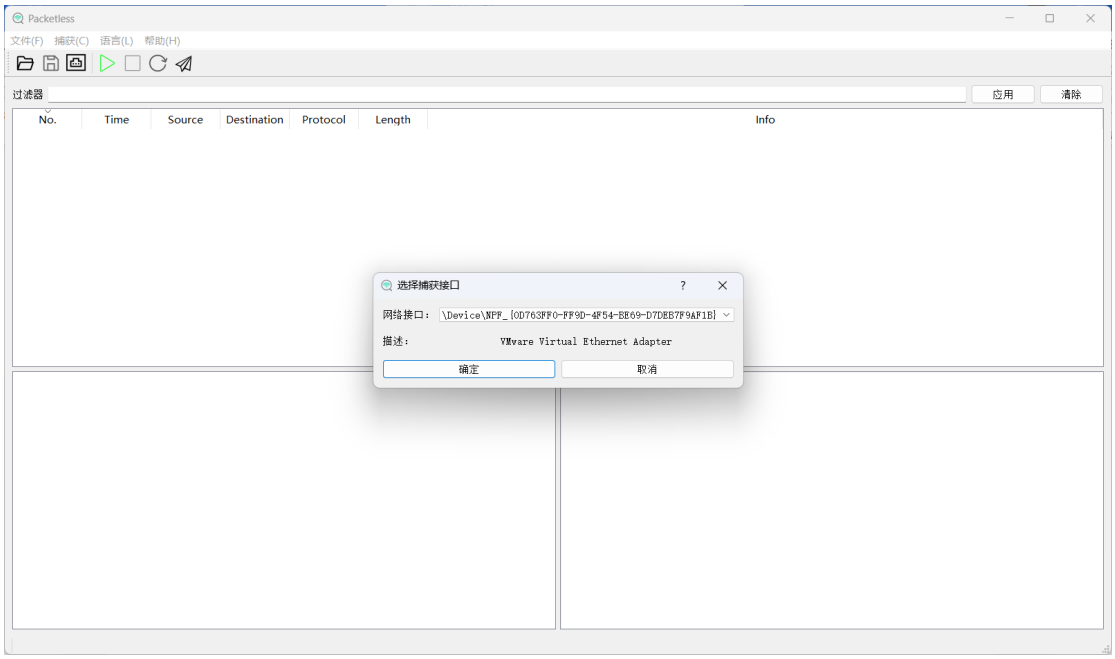


图 9 主界面和捕获接口界面

点击“**网络接口”下拉框**选择要在哪个接口上进行捕获。“**描述**”标签显示了对所选网络接口的描述。点击“**确认**”按钮，选定该接口。点击“**取消**”按钮，不对捕获接口进行更改。

打开捕获文件

1. 点击菜单栏的“**文件-打开**”或点击工具栏的“**打开捕获文件**”按钮，会弹出文件对话框（图 10）
2. 在文件对话框中选择你要打开的文件，点击“**打开**”按钮
3. 程序读取完毕后，数据包会显示在主界面中。

可能出现的问题：如果打开的文件并不是.pcap 捕获文件或捕获文件已经损坏，程序会弹出错误对话框（图 11）

捕获数据包

1. 点击菜单栏的“**捕获-开始**”或点击工具栏的“**开始捕获**”按钮启动数据包捕获
2. 程序会按照您设定的过滤规则（如果有的话）捕获网络中的数据包
3. 在捕获过程中，概要信息面板中的条目会不断变多。您可以随时点击某一条目查看其详细信息和数据内容
4. 如果要停止捕获，请点击菜单栏的“**捕获-停止**”或点击工具栏的“**停止捕获**”按钮
5. 您也可以选择重新开始捕获，此时程序会询问您是否要保存所捕获到的数据包，在您完成选择后，程序会开始新一轮的捕获。

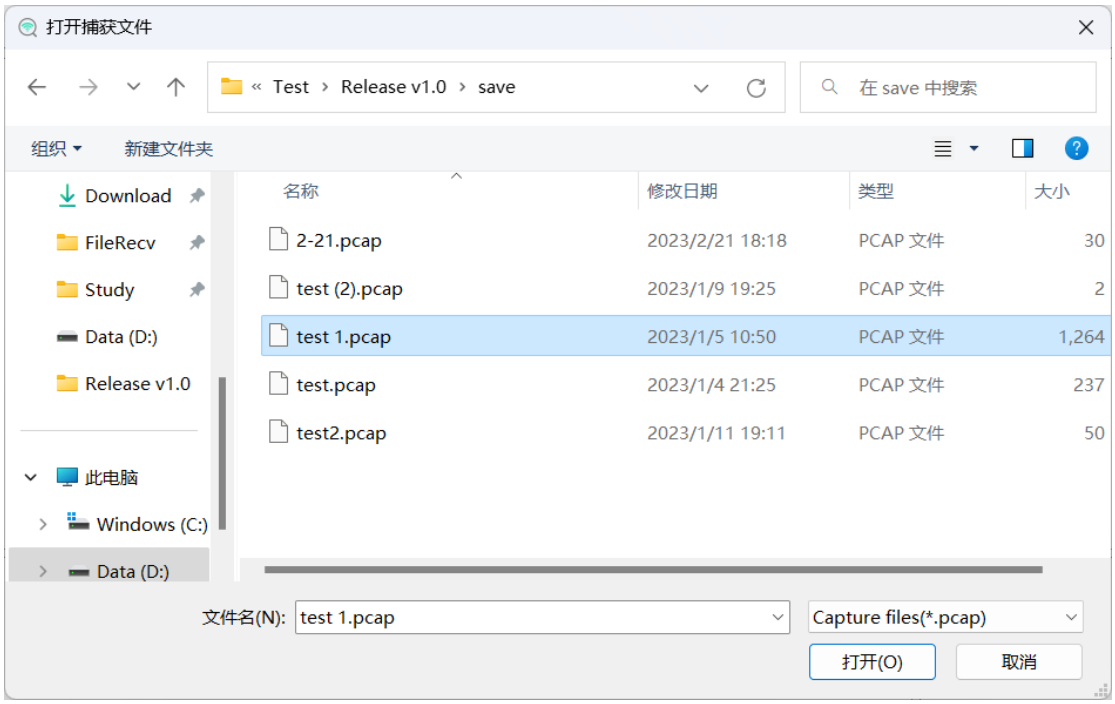


图 10 打开文件对话框

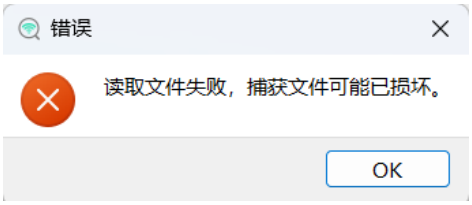


图 11 打开文件错误

保存数据包

1. 当捕获停止后，点击菜单栏的“**文件-保存**”或点击工具栏的“**保存捕获文件**”按钮，会弹出文件对话框（图 12）
2. 在文件对话框选择保存路径并输入保存文件名，点击“**保存**”按钮
3. 捕获文件将会被保存到选择的路径。如果保存路径中有同名的文件，您可以选择替换该文件或修改保存的文件名。

可能出现的问题：如果被替换的文件被其他程序占用，程序会弹出错误对话框。

切换捕获接口

1. 点击工具栏上的“**选择捕获接口**”按钮，打开“**选择捕获接口**”对话框
2. 点击“**网络接口**”**下拉框**选择要使用的网络接口
3. 点击“**确定**”按钮应用更改。

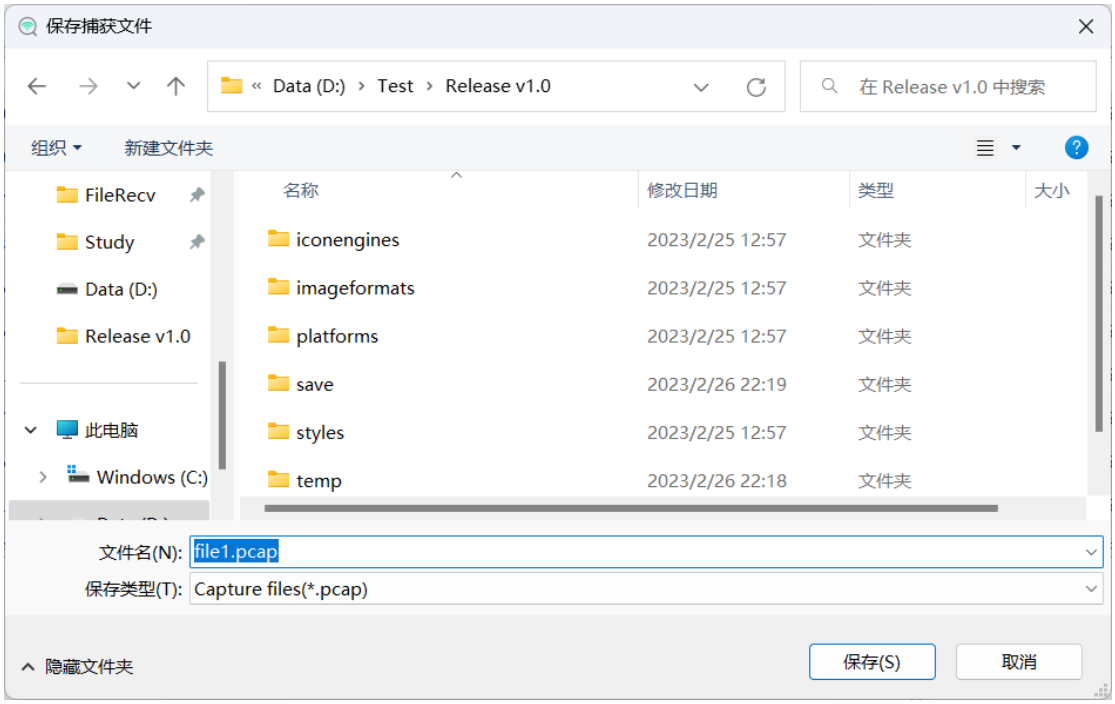


图 12 保存文件对话框

发送数据包

1. 点击工具栏上的“**发送数据包**”按钮，打开“**发送数据包**”对话框（图 13）
2. 在协议类型处选择要发送的协议类型。选择不同的协议类型，启用的数据输入框也不同
3. 根据要发送的数据包填写各数据输入框。鼠标在输入框上方悬浮可以获取输入提示。**注意：不满足规则的输入不会被输入框接受**
4. 在发送次数输入框中设置报文要发送的次数
5. 填写完所有数据后点击“**发送**”按钮。如果数据包发送成功，会弹出“报文发送成功”的提示对话框。如果有部分数据填写不符合要求，会弹出错误提示，同时错误的输入框会变红。（图 14）

从文件发送数据包

1. 点击工具栏上的“**发送数据包**”按钮，打开“**发送数据包**”对话框（图 13）
2. 点击“**发送文件**”按钮，弹出选择文件对话框
3. 选择要发送的文件，点击“**打开**”按钮，发送文件
4. 如果数据包发送成功，会弹出“报文发送成功”的提示对话框。

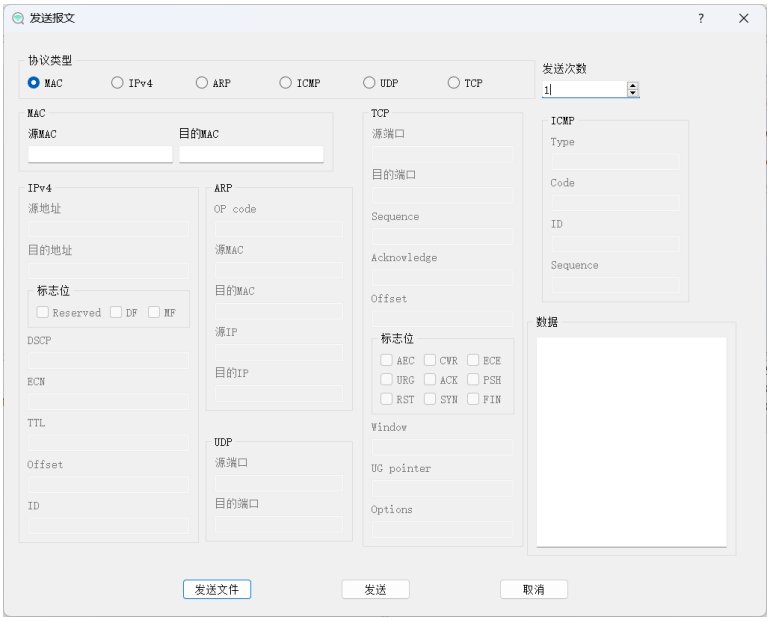


图 13 发送数据包对话框

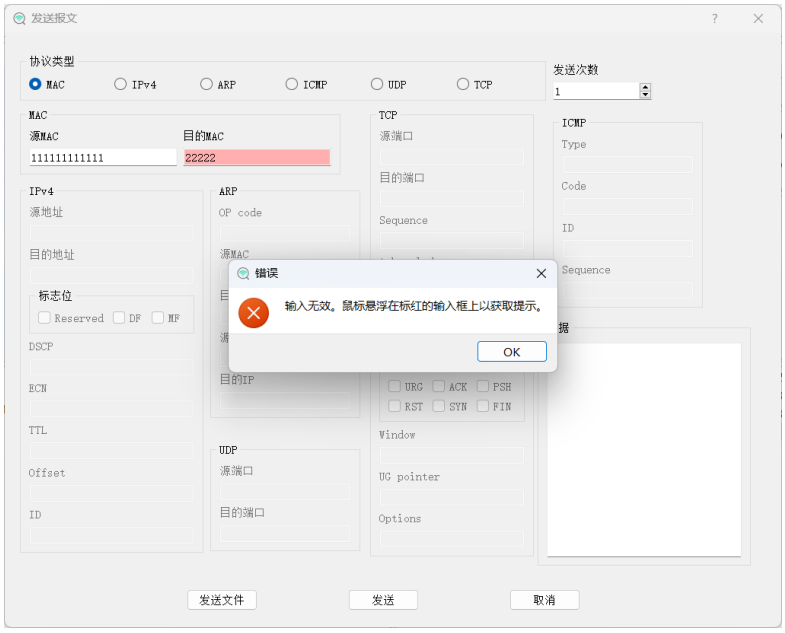


图 14 数据输入错误

保存提示

当您有未保存的捕获文件时进行以下操作之一（打开、开始捕获、重新开始捕获、退出程序），程序会询问您是否需要保存数据包。您可以根据您的需要选择保存或不保存，之后程序会继续执行您的操作。

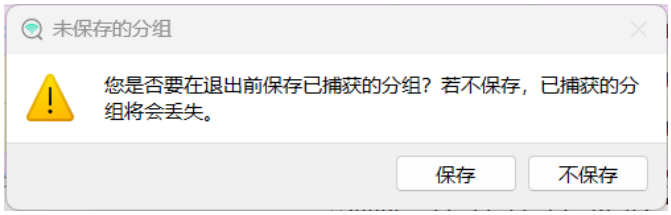


图 15 退出前提示是否保存数据包

复制数据包信息

在概要信息面板中右键单击某一数据包，可以复制该数据包的概要信息（图 16）。
在数据包字节面板中右键单击，可以复制当前数据包的数据内容（图 17）。

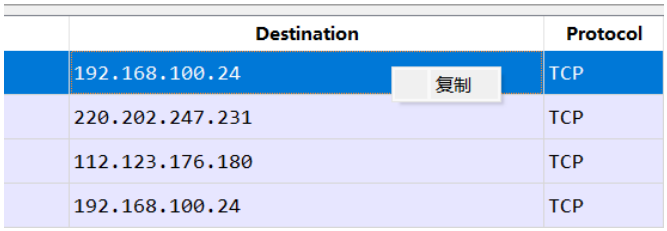


图 16 复制概要信息

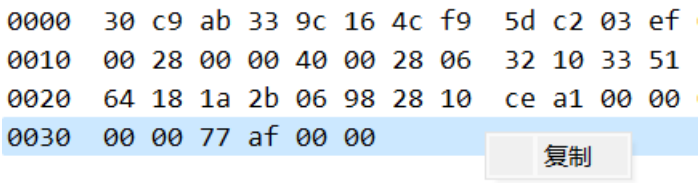


图 17 复制数据内容