网络编程基础

如何使用 WireShark 抓包分析

目录

RT-Thread

背景介绍

背景介绍

- 网络世界的数据实际上都是封装成一个个的数据包，你发给我一个数据包，我传给你一个数据包。

- 因此，在网络编程的过程中，经常需要利用抓包工具对开发板发出或接收到的数据包进行抓包分析。

- wireshark 是一个非常好用的抓包工具，使用 wireshark 工具抓包分析，是学习网络编程必不可少的一项技能。

程序安装

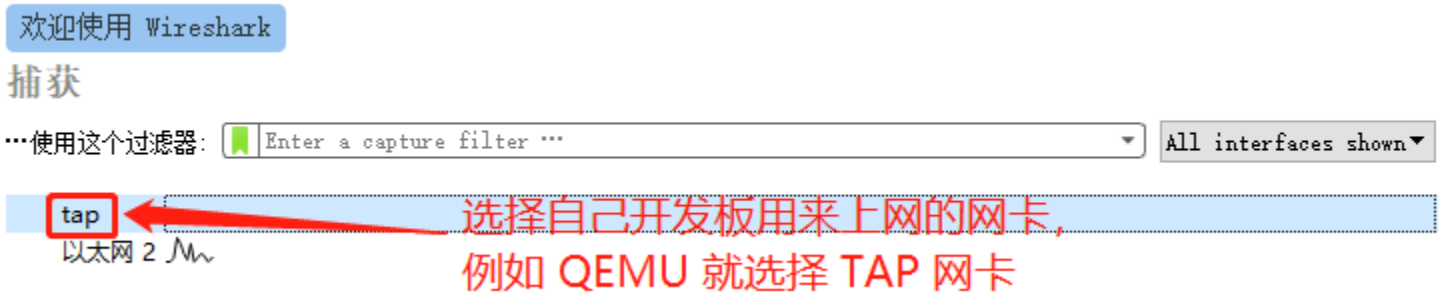
安装 wireshark

- 下载路径：https://www.wireshark.org/
- 下载完 wireshark，一路默认安装就行。
- 安装完软件之后，双击打开 wireshark 软件。

程序使用

选择与开发板相对应的网卡

- 打开 wireshark 之后，会给出你的所有网卡信息，让你选择一个要抓包的网卡
- 如下图所示，选择自己开发板用来上网的网卡，双击就开始抓包了。



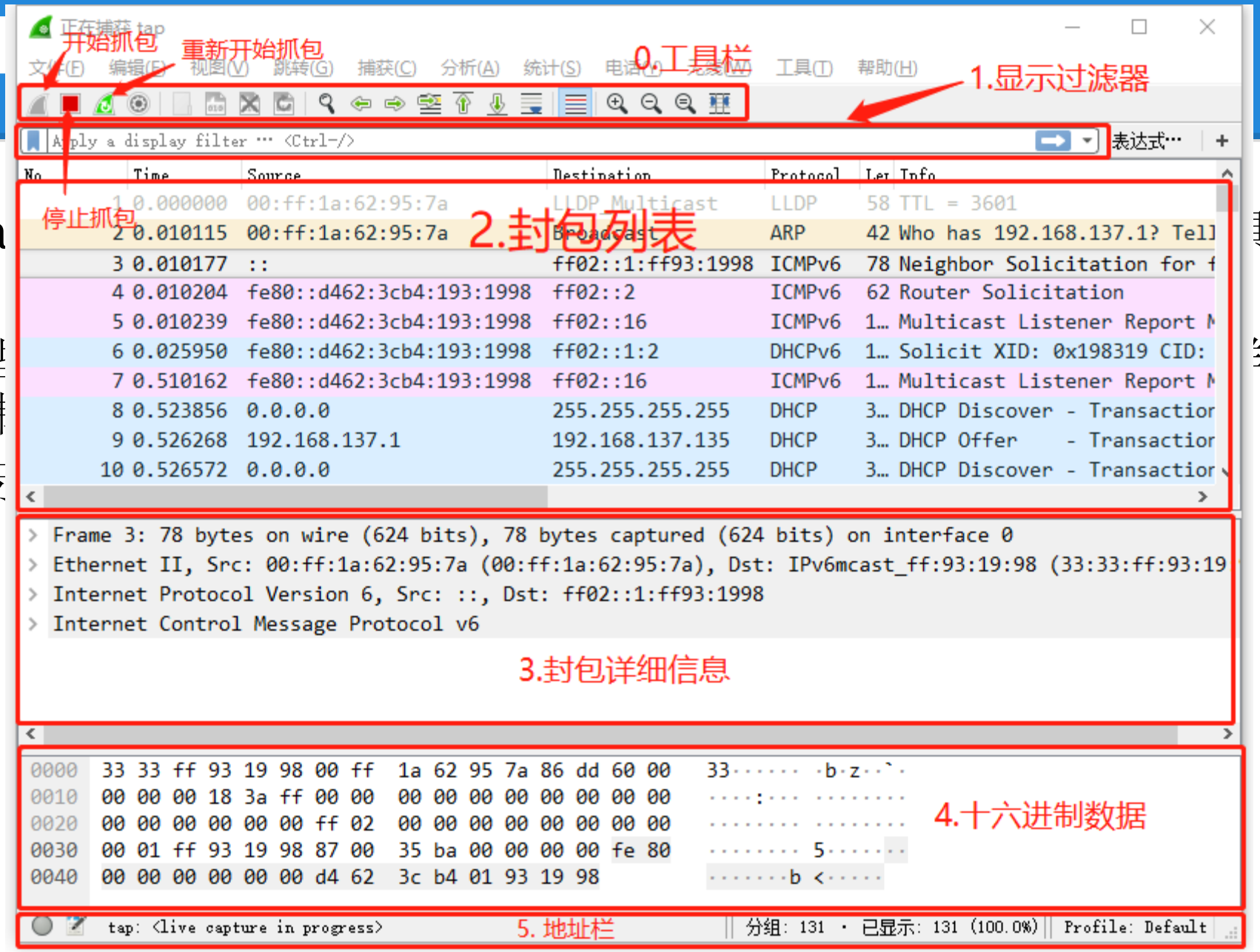
RT-Thread

wireshark 主界面介绍

- wireshark 的主界面和一般的 Windows 软件很像，也有菜单栏，工具栏，地址栏等。
- 还有一些它自己特有的窗口，比如：显示过滤器、封包列表、封包详细信息、十六进制数据显示区等。
- 如图所示，选择完网卡之后其实就已经开始抓包了。

wiresh

- wiresha 栏，地址栏等。
- 还有一些 细信息、十六进制
- 如图所示



RT-Thread

显示过滤器的使用

- 合理的使用显示过滤器，有助于我们从下面的封包列表里快速找到我们要关注网络包。
- 假如我们的开发板获取到的 IP 地址为 192.168.137.135 ，这样在显示过滤器里输入 ip.src == 192.168.137.135 or ip.dst == 192.168.137.135 然后点击右边的那个小箭头就会执行这个过滤条件。
- 过滤之后，剩下的都是和我们限定的 IP 相关的包。

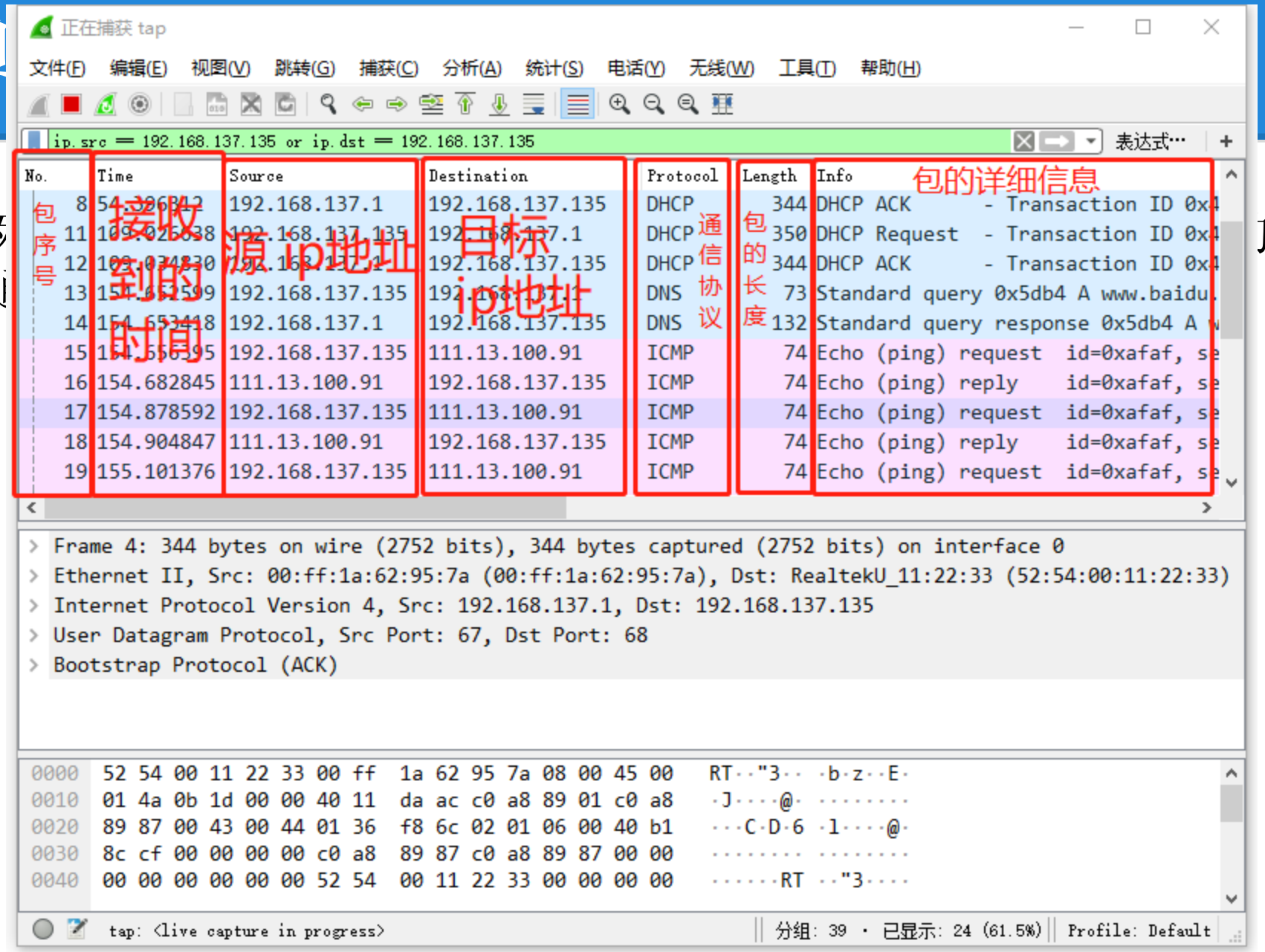
- 当然也有一些其他的过滤条件，比如：
  - 按 mac 地址过滤 eth.addr == 52:54:00:11:22:33
  - 只显示 TCP 协议的数据包 tcp
  - 只显示 UDP 协议的数据包 udp

封包列表介绍

- 从封包列表里我们也可以看到一些跟封包相关的信息，例如：来源的 ip，还有用到的通信协议等。

封包列

- 从封包列 ip，还有
用到的



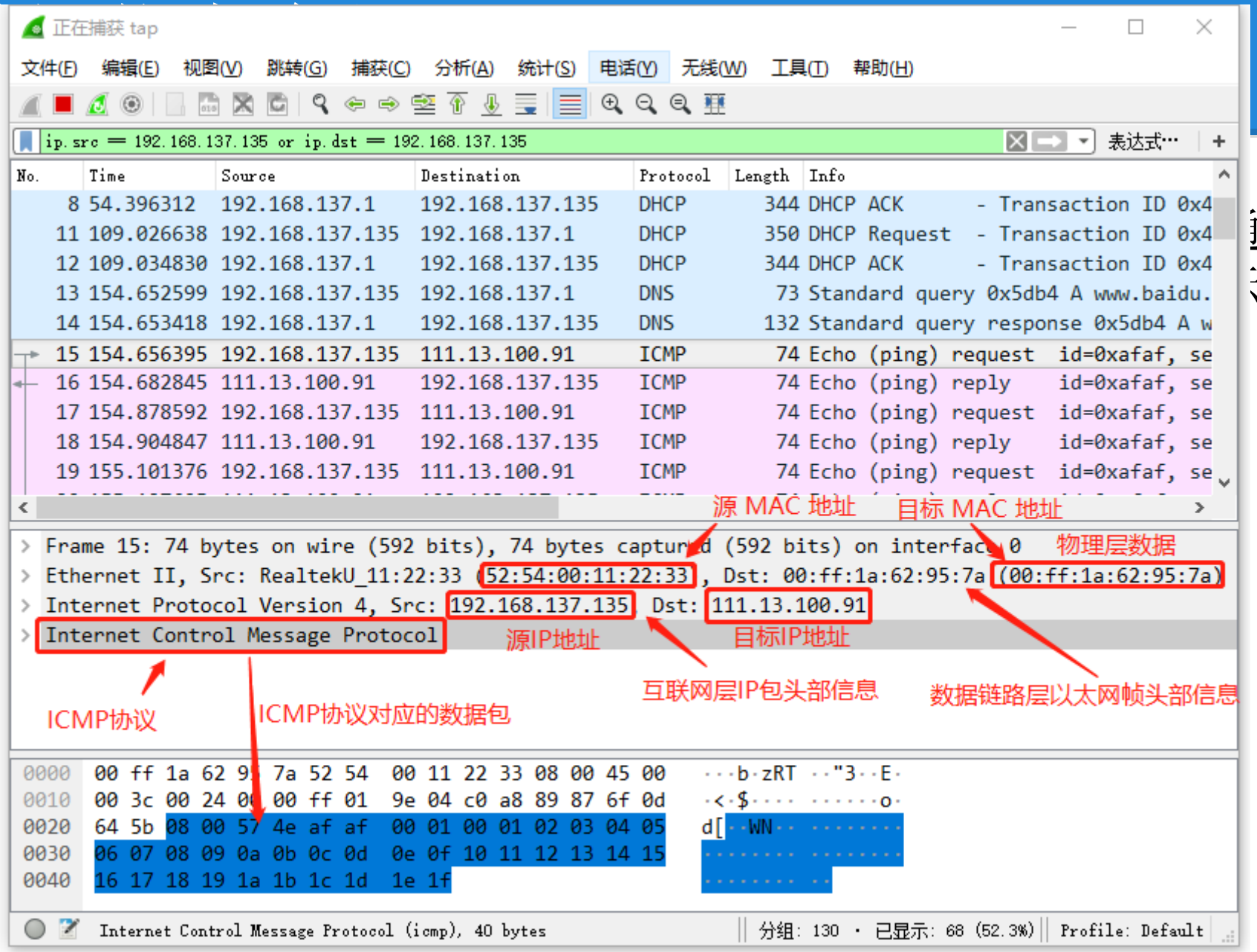
RT-Thread

封包详细信息介绍

- 下面介绍一下封包详细信息那一栏，它和底下的十六进制数据是相通的。封包的详细信息就是从底下的实际数据解包显示出来的。下面这张图展示了封包的一些详细信息。

封包详

- 下面介绍 的。封包的详细 了封包的一些详细



RT-Thread