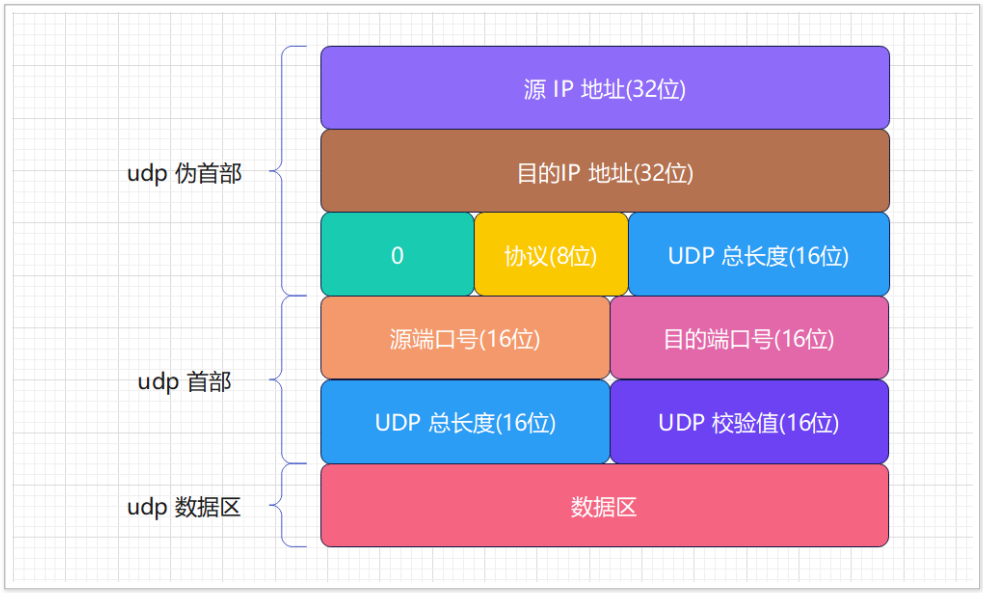
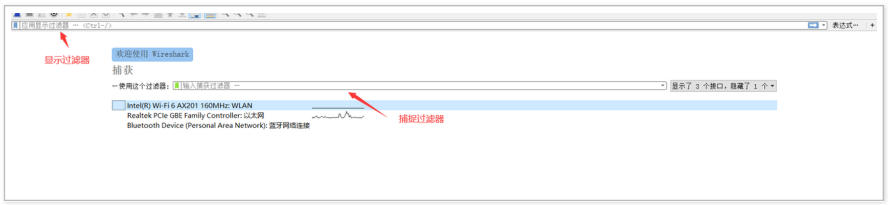
# 5.1 udp 协议与 wireshark 抓包分析_物联网 / 嵌入式工程师 - 慕课网

> 慕课网慕课教程 5.1 udp 协议与 wireshark 抓包分析涵盖海量编程基础技术教程，以图文图表的形式，把晦涩难懂的编程专业用语，以通俗易懂的方式呈现给用户。




- udp 协议由 伪首部、首部、数据区构成
  - 伪首部:
    - 伪首部不是 UDP 的真正首部，只在计算校验和时用到
    - 伪首部为 12 字节
    - 伪首部既不向下传送也不向上递交，只是为了计算校验和
  - 首部:
    - 源端口号：发送端的端口号
    - 目的端口号：接收端的端口号
    - udp 总长度：udp 协议头 与 数据长度
    - udp 校验值：udp 伪首部、首部与数据来计算 校验和
  - 数据区
    - udp 数据区域
- wireshark 过滤器:
  - **捕捉过滤器**：从网卡中捕捉符合过滤规则的数据包
  - **显示过滤器**：会捕捉所有的数据包，只显示符合过滤规则的数据包



显示过滤器常用语法规则

ip.addr == 10.226.42.58 显示 源 ip 或者目的 ip 为 10.226.42.58 的数据包

ip.src == 10.226.42.58 显示 源 ip 为 10.226.42.58 的数据包

ip.dst == 10.226.42.58 显示目的 ip 为 10.226.42.58 的数据包

udp.srcport == 8888 显示 udp 源端口号为 8888 的数据包

udp.dstport == 8888 显示 udp 目的端口号为 8888 的数据包

udp.port == 8888 显示 udp 源端口号或者目的端口号为 8888 的数据包

tcp.srcport == 8888 显示 tcp 源端口号为 8888 的数据包

tcp.dstport == 8888 显示 tcp 目的端口号为 8888 的数据包

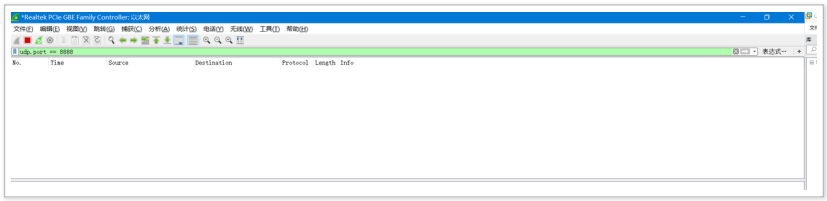
tcp.port == 8888 显示 tcp 源端口号或者目的端口号为 8888 的数据包

ip.addr == 10.226.42.58 && tcp.port == 8888 显示 源 ip 或者目的 ip 为 10.226.42.58 **并且** tcp 源端口号或者目的端口号为 8888 的数据包

ip.addr == 10.226.42.58 || tcp.port == 8888 显示 源 ip 或者目的 ip 为 10.226.42.58 **或者** tcp 源端口号或者目的端口号为 8888 的数据包

!ip.addr == 10.226.42.58 显示源 ip 或者目的 ip 不是 10.226.42.58 的数据包

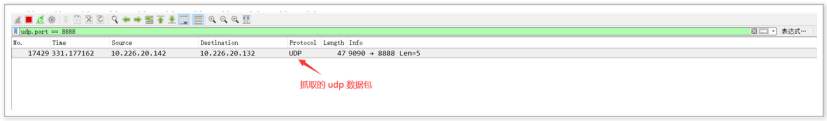
- 使用 wireshark 抓取 udp 数据包的步骤如下:
  - step 1：选择网卡，双击进入到抓包界面
  - 

  - step 2：设置显示过滤器，设定 udp 服务器的端口号为 8888，可以设置显示 udp 端口号为 8888 的数据包，**按回车生效**
  - 
  - step 3：运行 udp 服务器

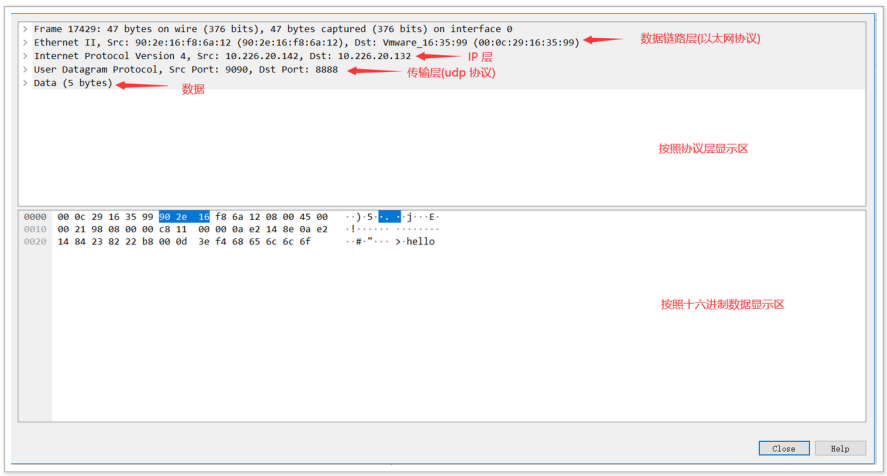
```
ben@ubuntu:~/class/week15/codes/part5/A01udp$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.226.20.132  netmask 255.255.255.0  broadcast 10.226.20.255
        inet6 fe80::f0f9:daec:7c3b:83c3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:16:35:99  txqueuelen 1000  (Ethernet)
        RX packets 1108928  bytes 1292666480 (1.2 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 432513  bytes 39393733 (39.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3959314  bytes 1962211230 (1.9 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3959314  bytes 1962211230 (1.9 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ben@ubuntu:~/class/week15/codes/part5/A01udp$ ./server 10.226.20.132 8888
```

  - step 4：运行 udp 客户端，这里直接使用 网络调试助手

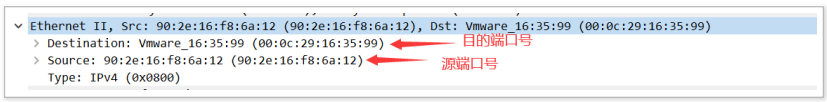

- step 5：发送数据，并查看 wireshark 抓包界面




- 在 wireshark 中双击抓取的数据包，可以看到详细信息

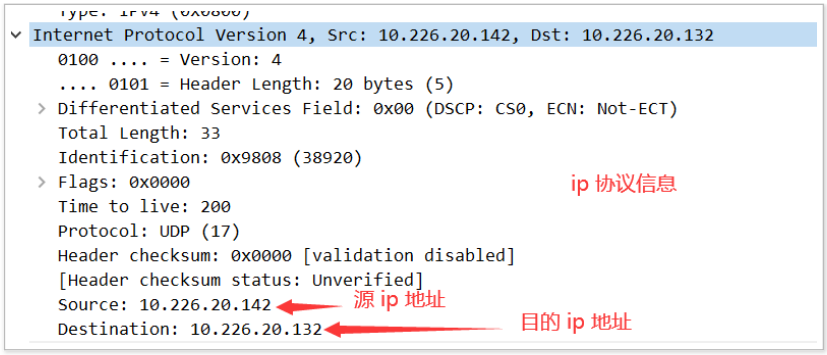



- 以太网协议信息



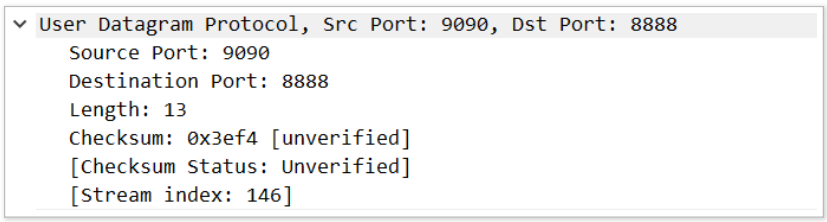

  - 主要信息为 源 MAC 地址与目的 MAC 地址

- ip 层信息




- 主要信息为 源 IP 地址 与 目的 IP 地址

- 传输层信息




- 主要信息为:
  - Source Port : 源端口号
  - Destination Port : 目的端口号
  - Length : udp 协议头长度
  - Checksum : 校验和
  -

- 数据区


1. 熟悉 wireshark 过滤规则,
2. 使用 wireshark 软件来抓取数据包, 并分析 udp 协议的信息

全文完