# wireshark使用方法

## 一、下载安装：

wireshark是一款抓包工具，可以捕捉网络中的数据包用于分析

官网网站下载驱动：<https://www.wireshark.org/>

## 二、初始界面：

图片包含 屏幕截图

描述已自动生成

选择监测哪块网卡

图片包含 屏幕截图

描述已自动生成图片包含 屏幕截图

描述已自动生成

捕捉过滤规则

显示过滤规则

## 三、（capture filter）与（Display filter）

capture filter作用：捕捉规则 - 只捕捉符合过滤规则的包

Display filter 作用：显示规则 - 在捕捉结果中只显示符合过滤规则的包

捕捉过滤规则举例：

tcp port 80 （端口80数据包）

tcp port 3306 （端口3306数据包）

host www.baidu.com（只抓取访问百度网络包数据）

显示过滤规则举例

ip.src == 192.168.3.11 ip源地址为192.168.3.11

ip.dst == 192.168.3.12 ip目的地址为192.168.3.12

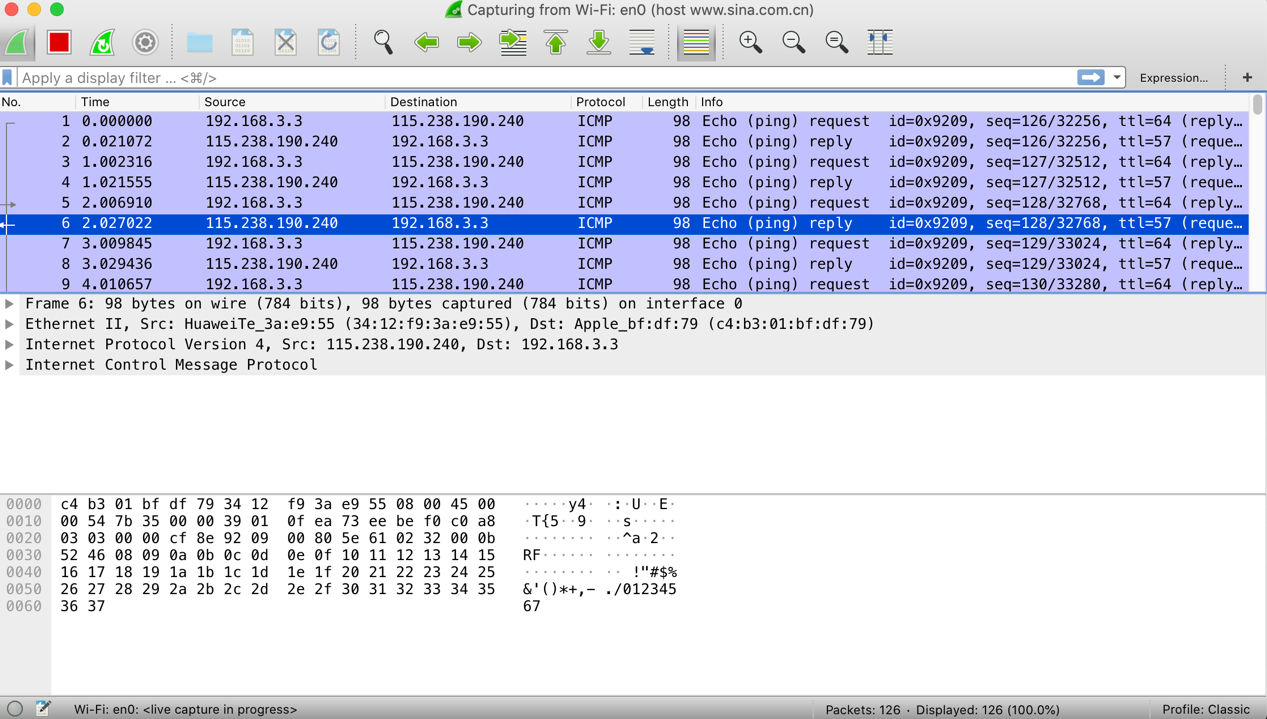
tcp.port == 80 tcp传输， 端口80

tcp.srcport == 10021 tcp传输， 端口为10021

tcp.dstport == 3306 tcp传输， 端口为3306

过滤规则可以使用and与or组合

## 四、抓包结果



选中某一行，既可以显示该数据包详细信息