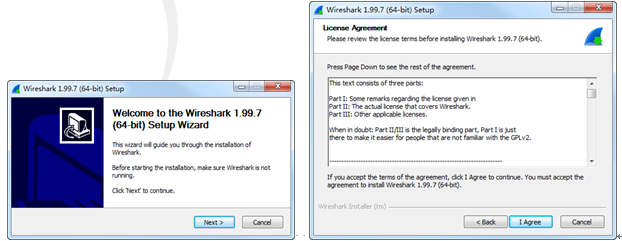
## 一、工作内容

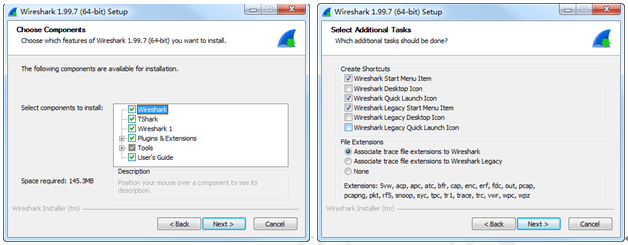
所有互联网主机设备每3小时进行1次人工流量分析，确认流量异常是否攻击行为，如确认攻击有效，立即通知系统处置组下线处置，整改后才能再上线。

## 1）Windows安装wireshark与使用

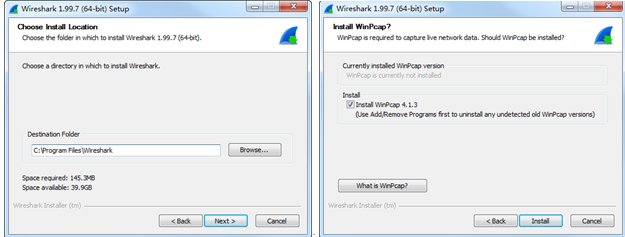
1. 打开wireshark官网下载的wireshark软件，该界面显示了Wireshark的基本信息。此时单击Next按钮，将弹出许可协议对话框，单击I Agree按钮，将弹出选择组件对话框

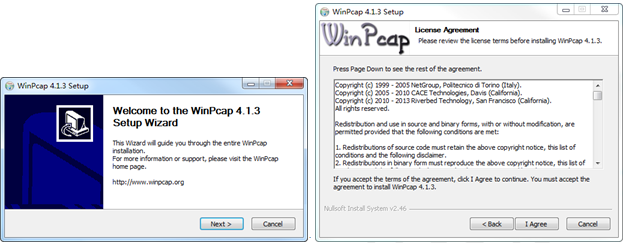


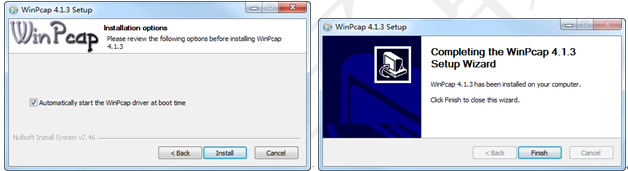
1. 该界面选择希望安装的Wireshark组件，这里使用默认的设置。然后单击Next按钮，将弹出Select Additional Tasks对话框. 该界面用来设置创建快捷方式的位置和关联文件扩展名。设置完后，单击Next按钮，将显示安装位置对话框



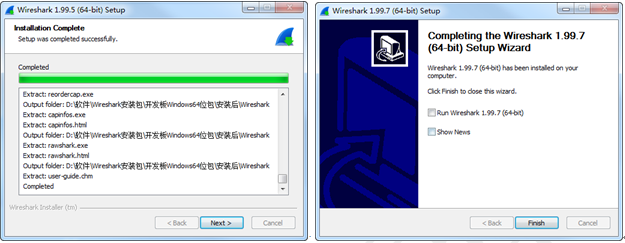
1. 在该界面选择Wireshark的安装位置。然后单击Next按钮，将显示安装WinPcap对话框。如果要使用Wireshark捕获数据，必须要安装WinPcap。所以这里必须将Install WinPcap 4.1.3复选框勾上。然后单击Install按钮，Wireshark将开始安装。



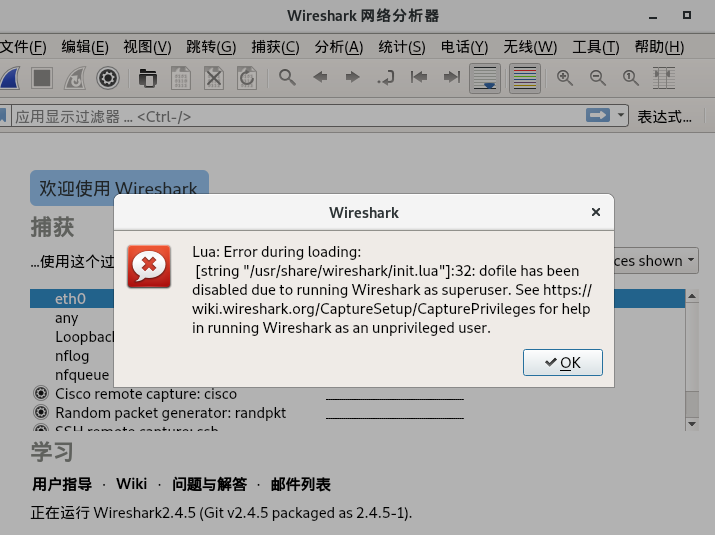
1. 该界面显示了WinPcap基本信息。此时单击Next按钮，将显示WinPcap许可证条款对话框，
2. 该界面显示了WinPcap许可证条款信息。此时单击I Agree按钮，将显示安装选项，然后单击Install按钮



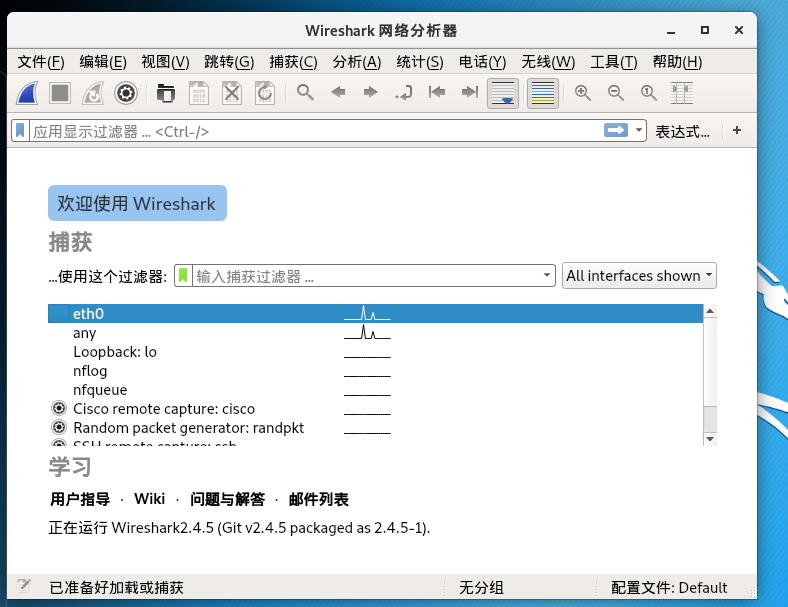
1. 从该界面可以看到WinPcap已安装完成。此时单击Finish按钮，将继续安装Wireshark。可以看到Wireshark已经安装完成。此时单击Next按钮，可以看见完成界面



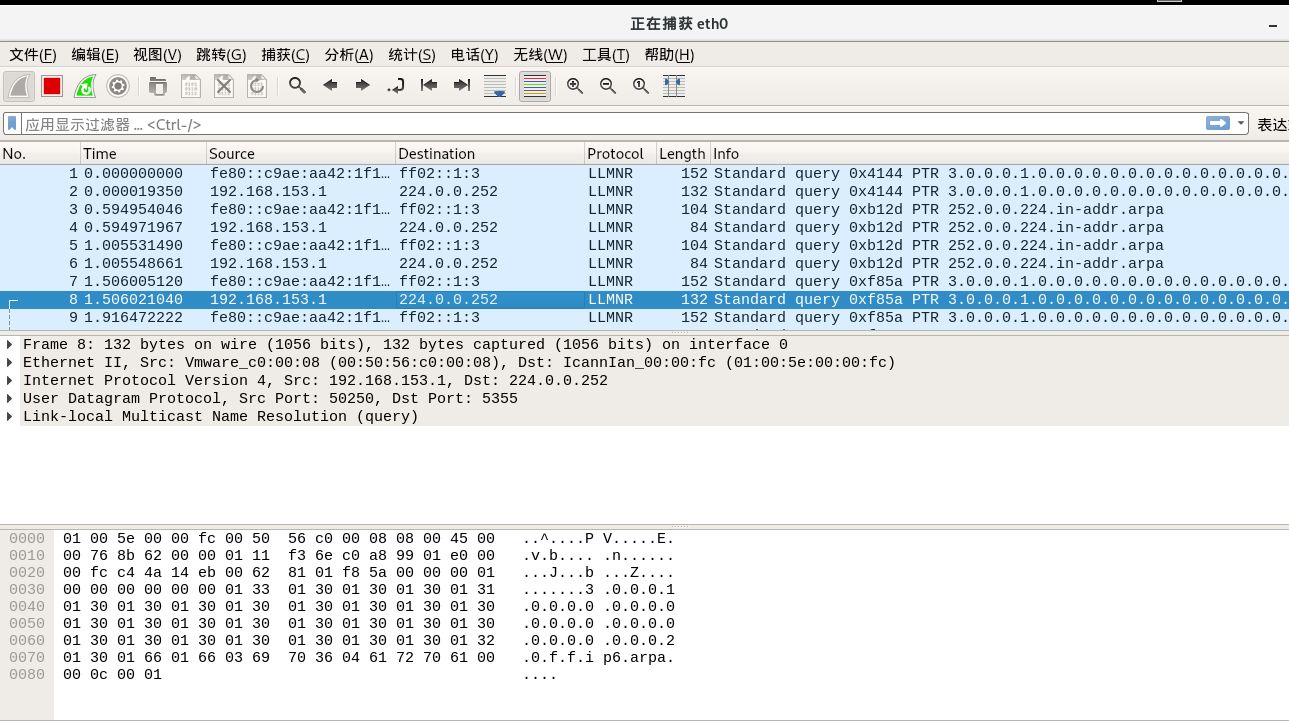
1. 启用wireshark，会有一个警告提示，选OK



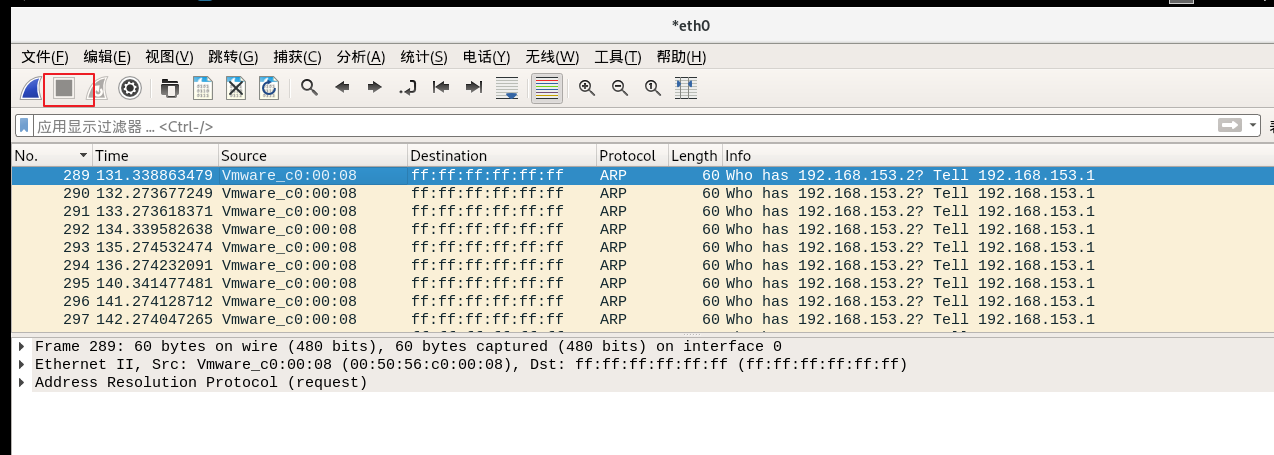
1. 然后打开了界面，选择一个流量网卡进行监控



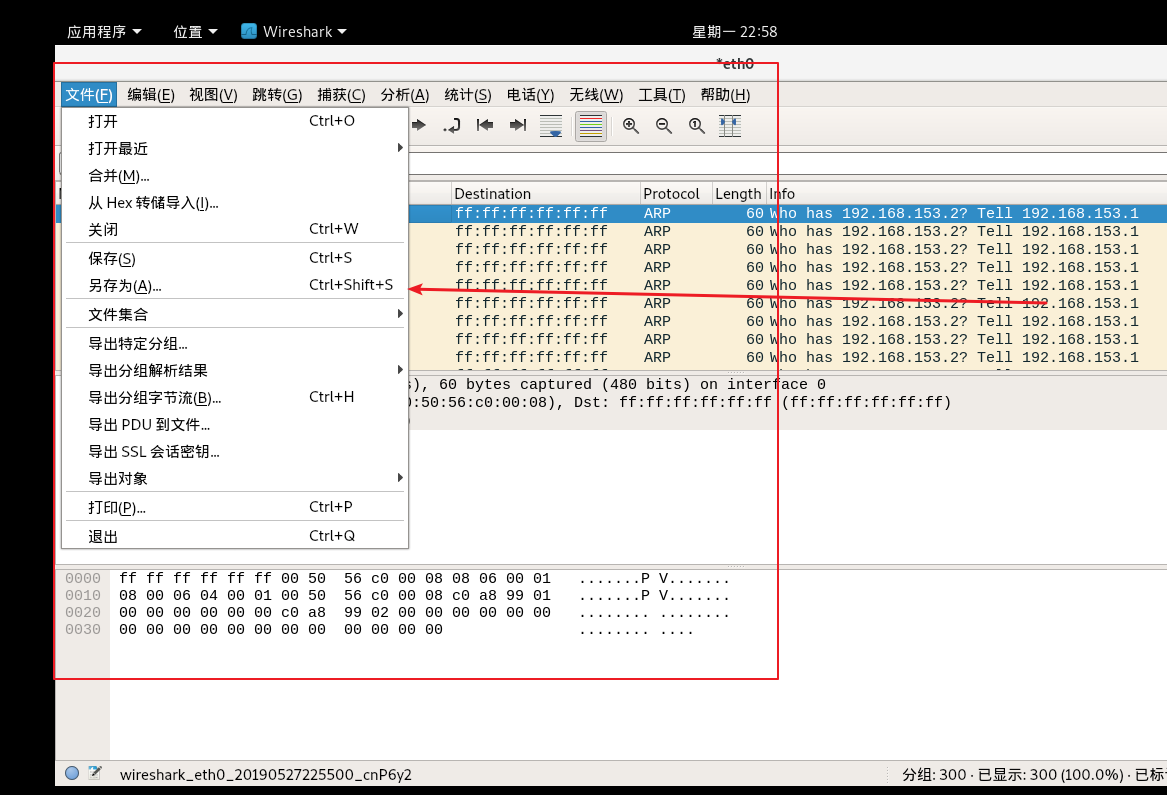
1. 点击流量网卡，就进入了监控界面



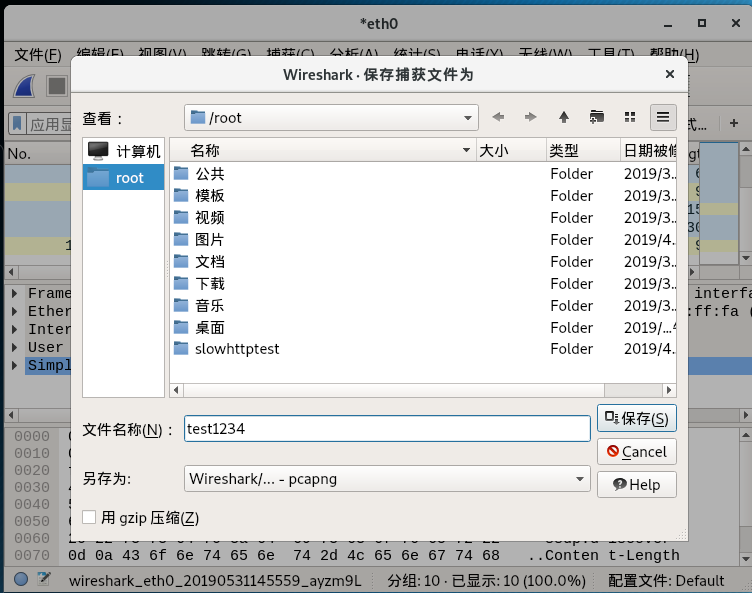
1. 点击红色按钮进行暂停后即可导出文件



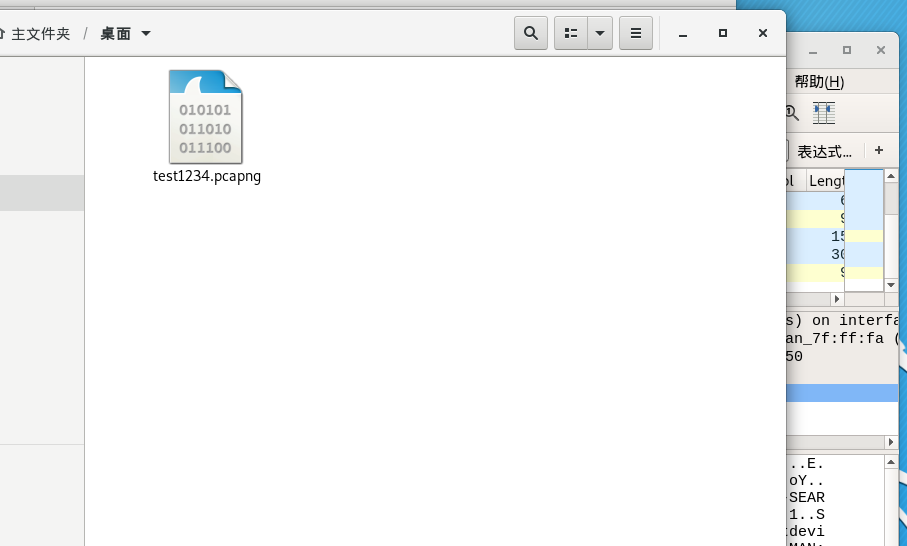
1. 点击文件，选择另存为



1. 将其另存为文件即可，这里命名规则为 系统名\_ip\_时间.pcap  
   eg:门户\_10.12.22.22\_201905311827.pcap

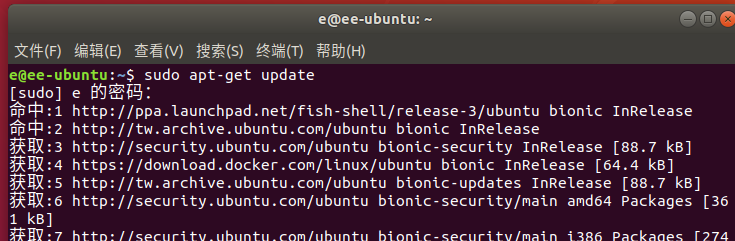


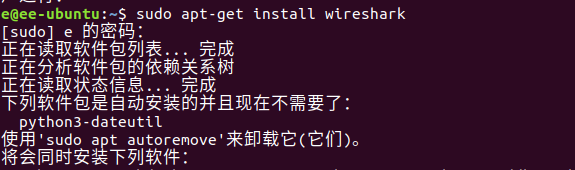
1. 点击保存后在桌面即可看到保存的文件了

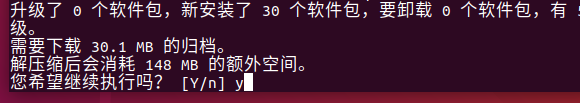


## 2）Linux安装wireshark与使用

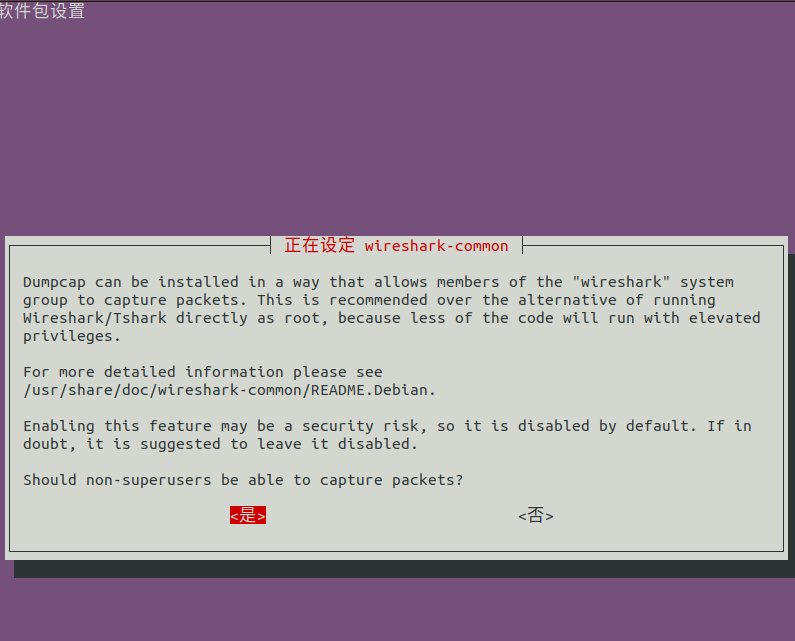
1> 这里以Ubuntu为例，输入命令：sudo apt-get update 和 sudo apt-get install wireshark 进行安装wireshark软件



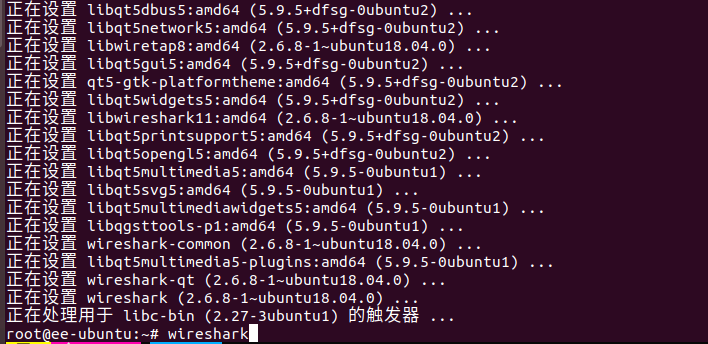




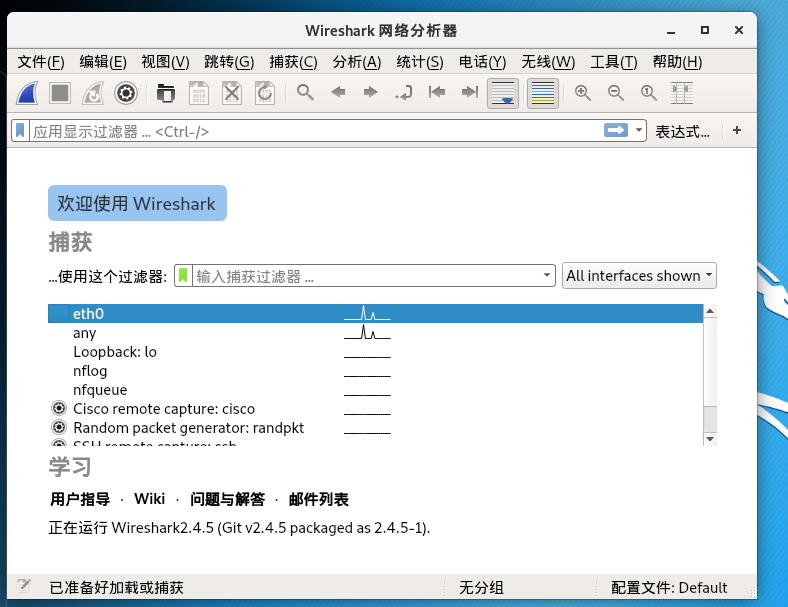
1. 会有一个提示，我们选yes



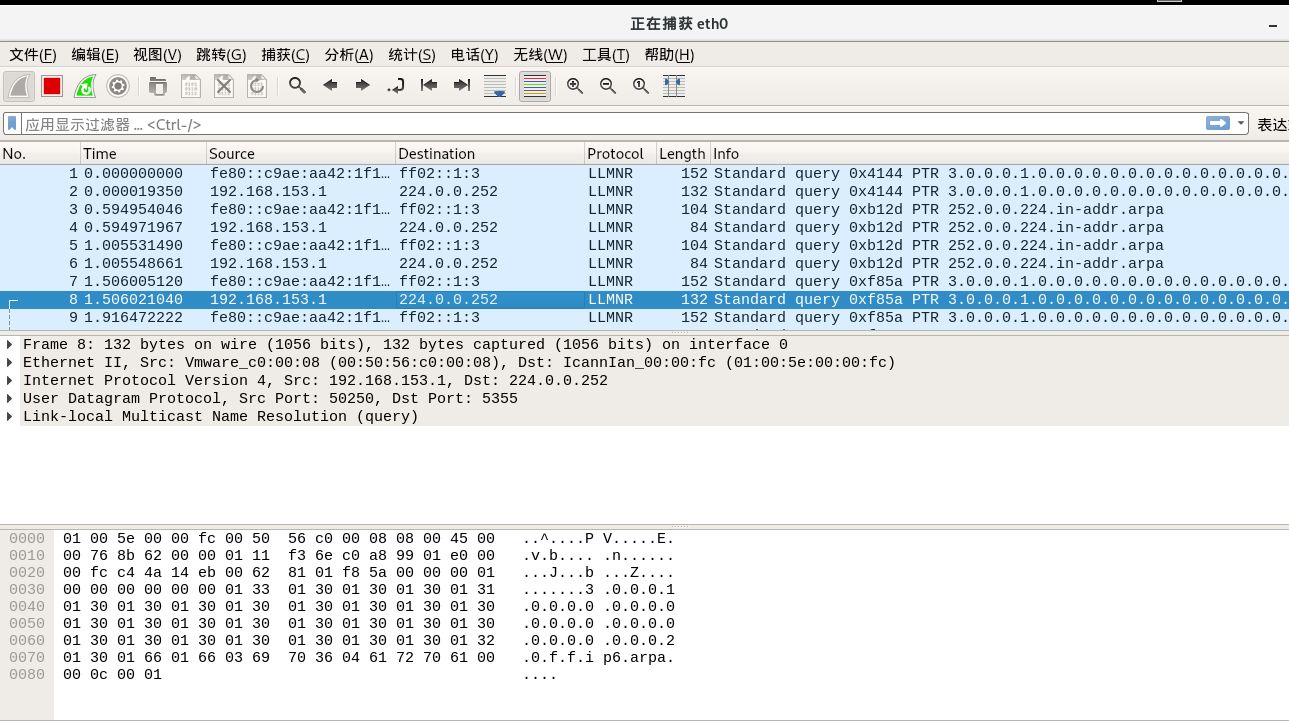
1. 安装好以后，我们输入wireshark就可以运行软件了



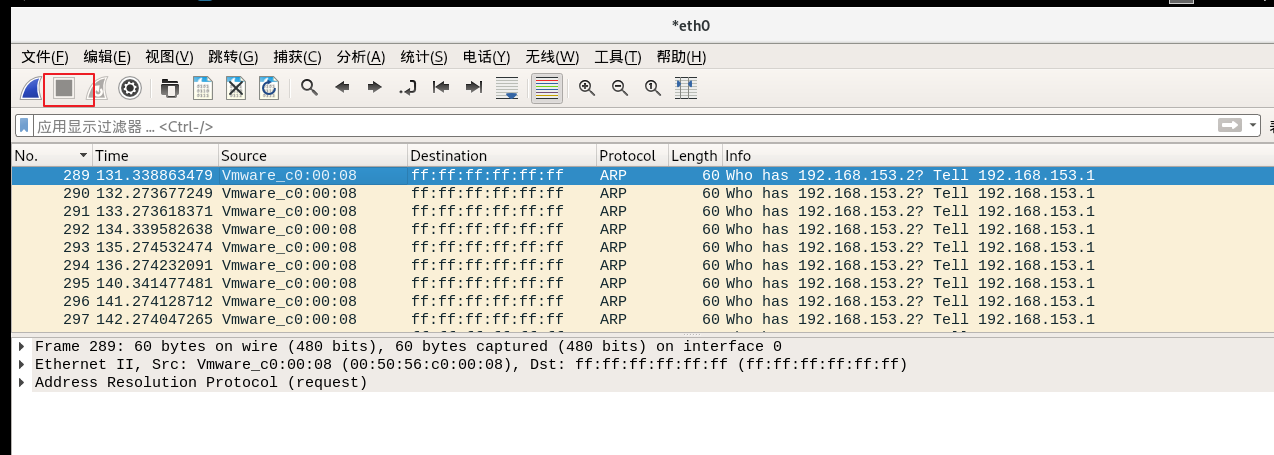
1. 然后打开了界面，选择一个流量网卡进行监控



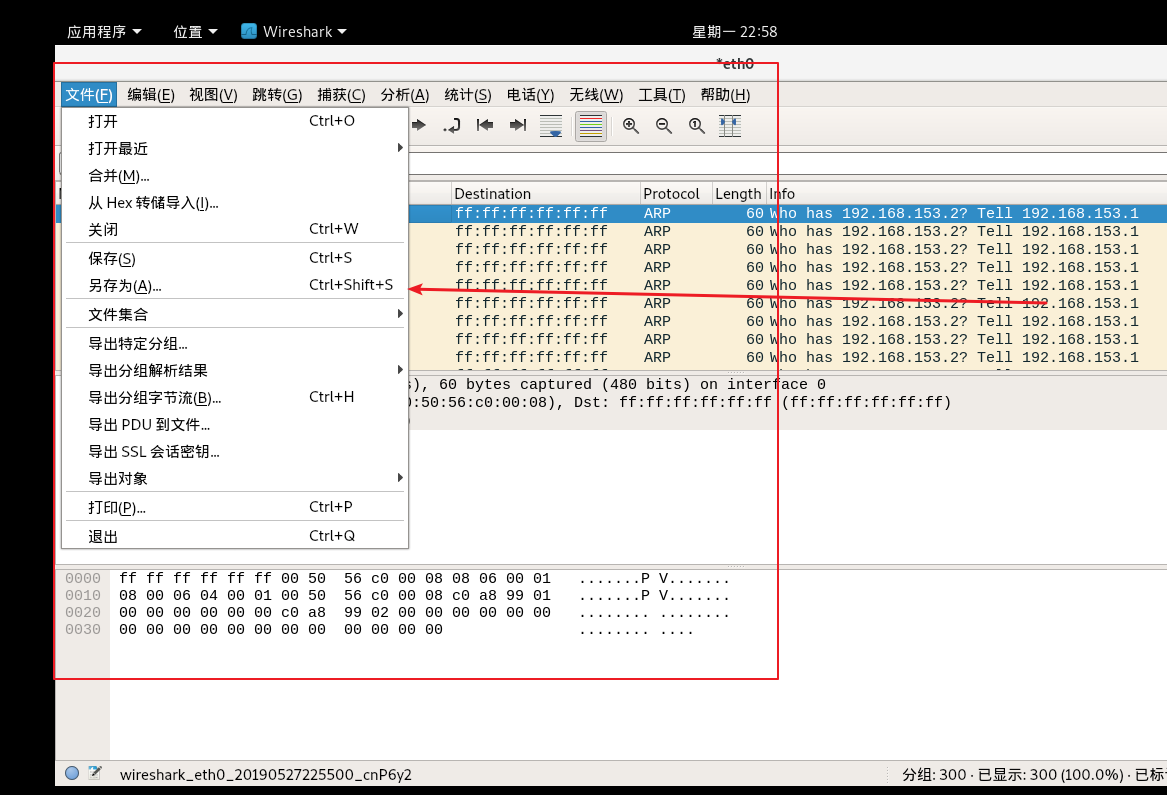
1. 点击流量网卡，就进入了监控界面



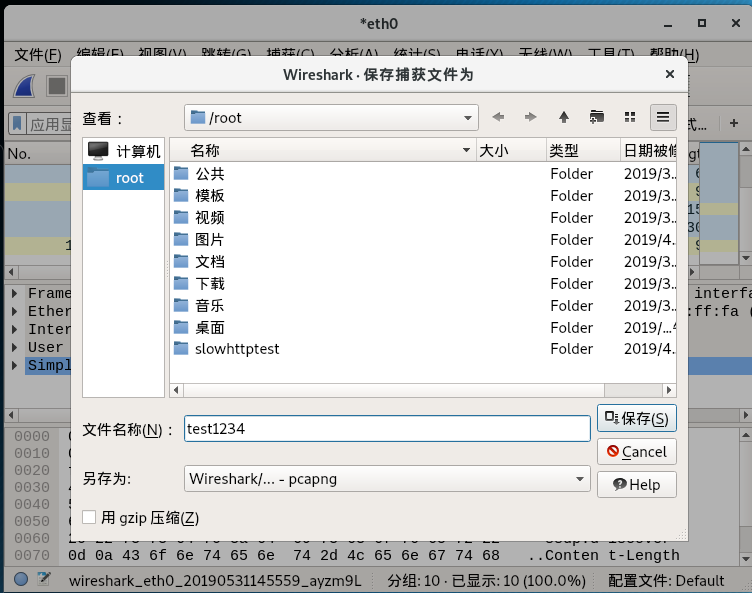
1. 点击红色按钮进行暂停后即可导出文件



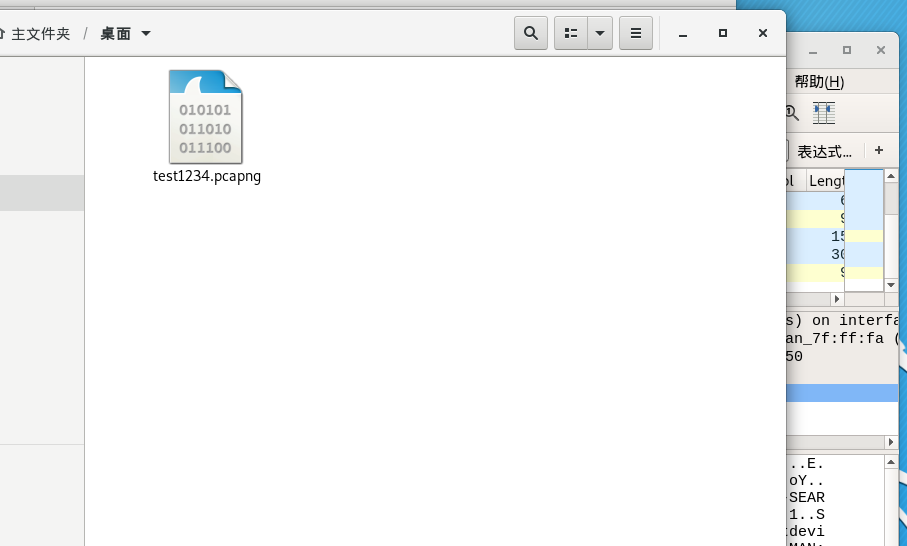
1. 点击文件，选择另存为



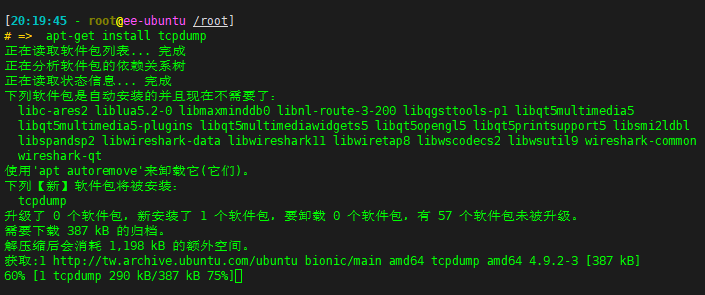
1. 将其另存为文件即可，这里命名规则为 系统名\_ip\_时间.pcap  
   eg:门户\_10.12.22.22\_201905311827.pcap



1. 点击保存后在桌面即可看到保存的文件了

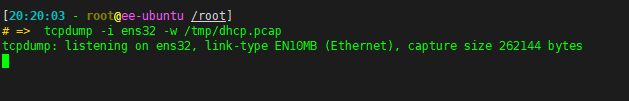


## 3）命令行下Linux的抓包

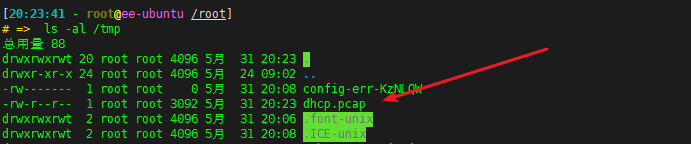
1> 这里以Ubuntu为例，输入命令：sudo apt-get update 和 sudo apt-get install tcpdump进行安装tcpdump工具

1. 安装好以后，我们输入tcpdump -i 指定网卡-w 保存的路径.pcap，这里我们使用tcpdump -i ens32 -w /tmp/dhcp.pcap

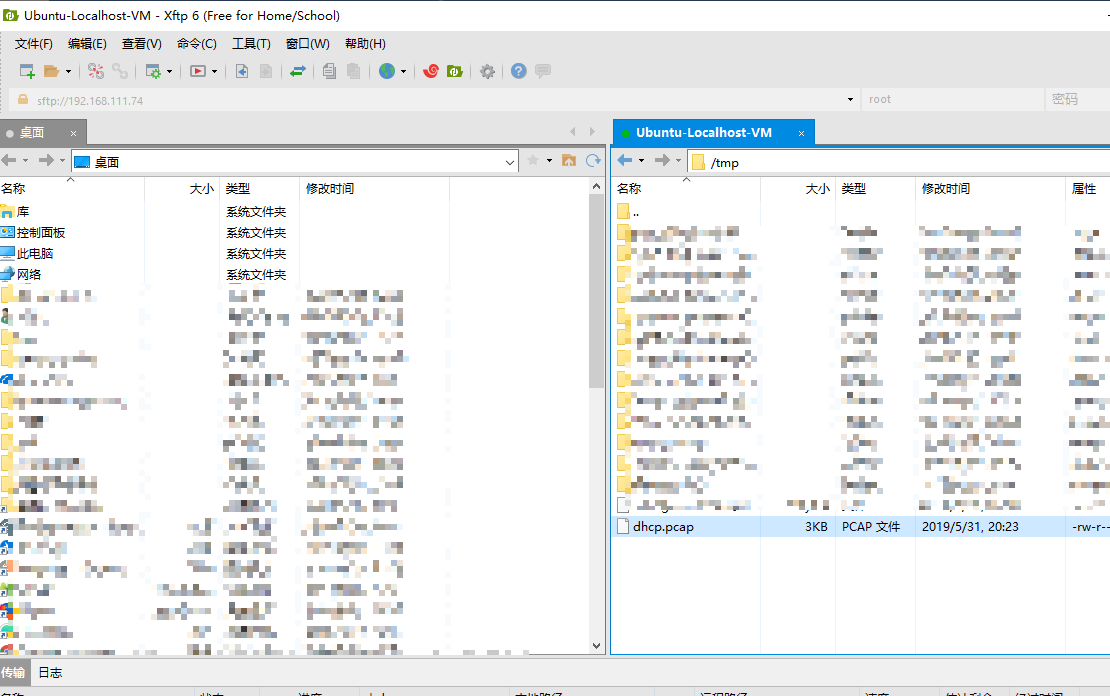
文件命名规则：系统名\_ip\_时间.pcap  
eg:门户\_10.12.2.22\_201905311827.pcap



1. 我们可以看到/tmp目录下有dhcp.pcap这个文件



1. 我们将这个文件通过xftp导回本地即可



1. 直接拖拽复制导回本地即可

