实验内容

- Ubuntu18.10安装`wireshark`
- 运行wireshark并且进行抓包

实验步骤

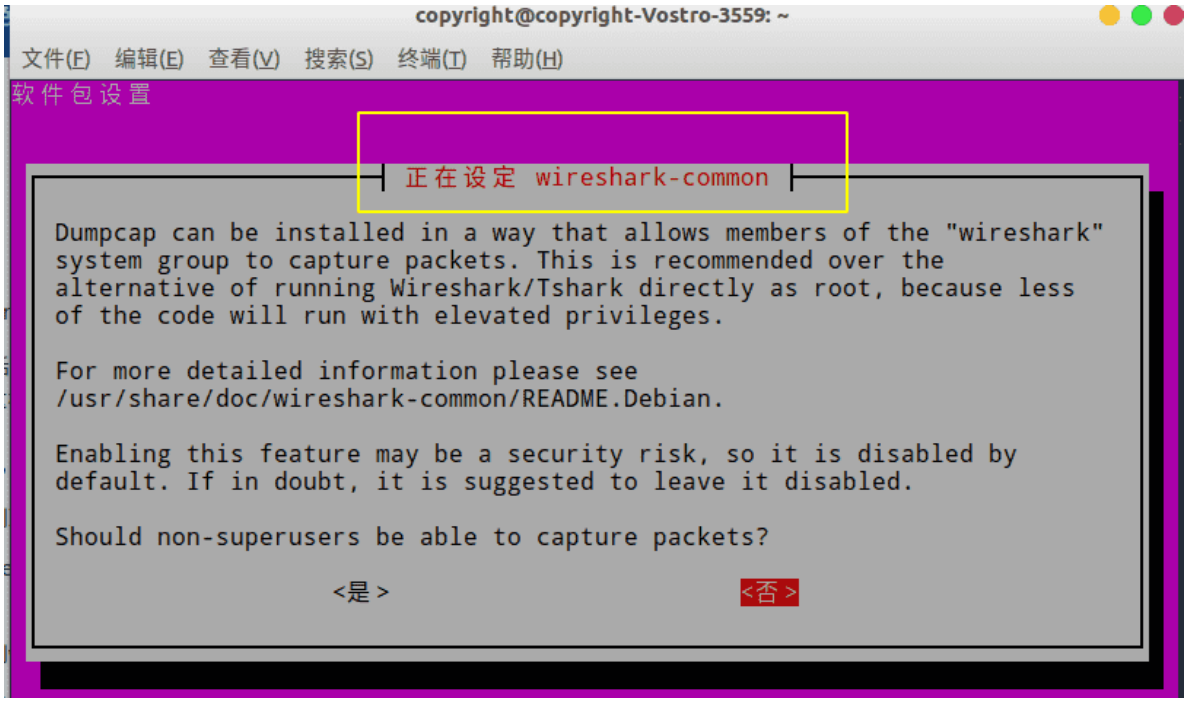
安装wireshark

- 环境：Ubuntu18.10
- 版本：Stable Wireshark
- 参考：链接

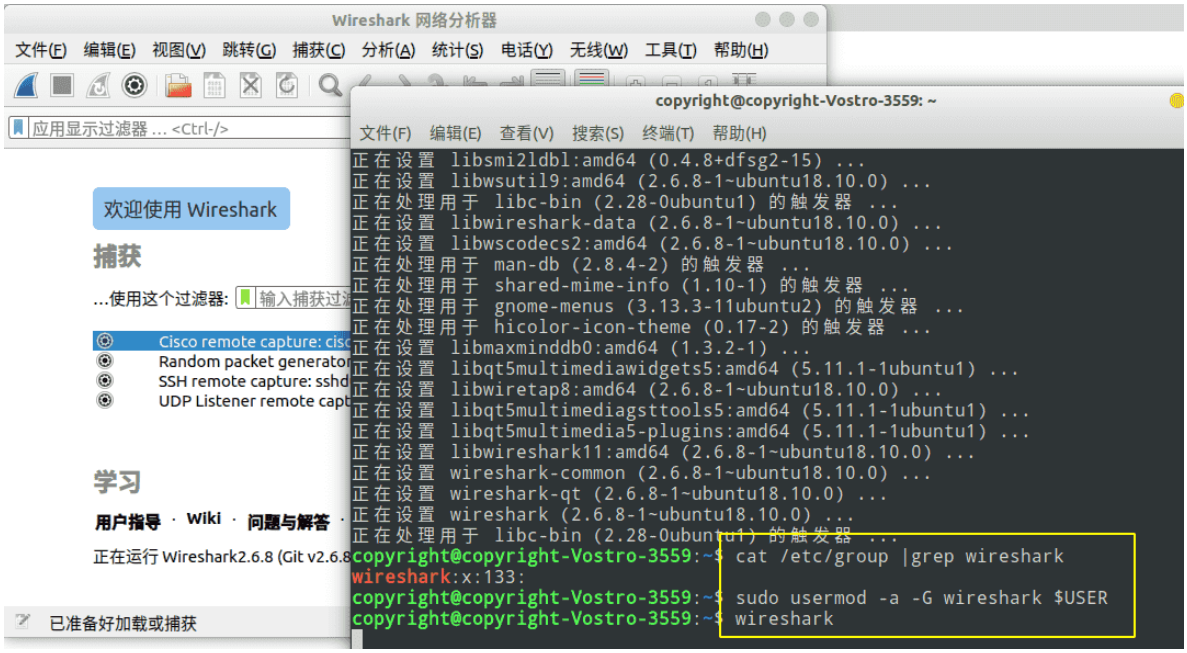
命令行安装

```
copyright@copyright-Vostro-3559:~$ sudo apt install wireshark
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  dwz libarchive-cpio-perl libfile-stripnondeterminism-perl
  libmail-sendmail-perl libsys-hostname-long-perl po-debconf
使用'sudo apt autoremove'来卸载它(它们)。
将会同时安装下列软件：
  libmaxminddb0 libnl-route-3-200 libqt5multimedia5 libqt5multimedia5-plug
```

安装`wireshark-common`选择`yes`

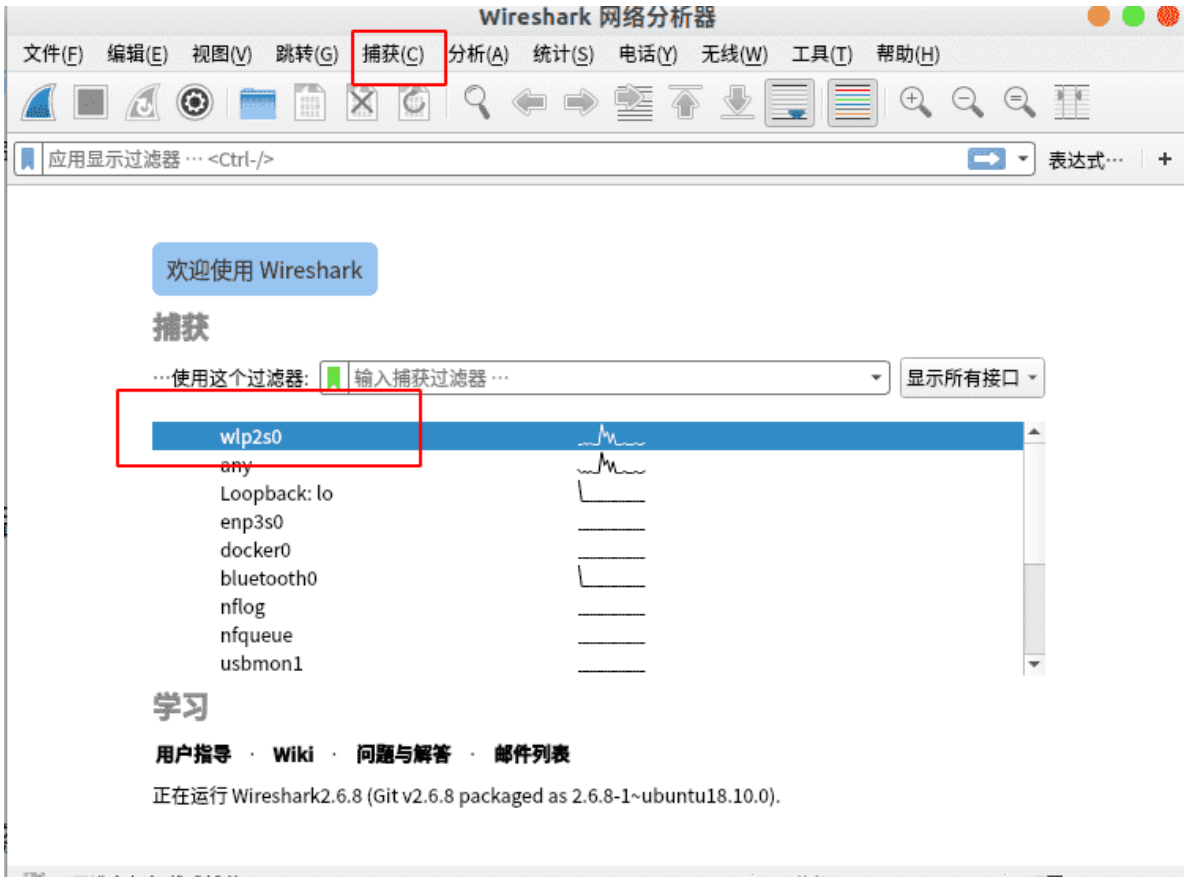


添加到`$USER`变量，以后运行时不用加`sudo`权限

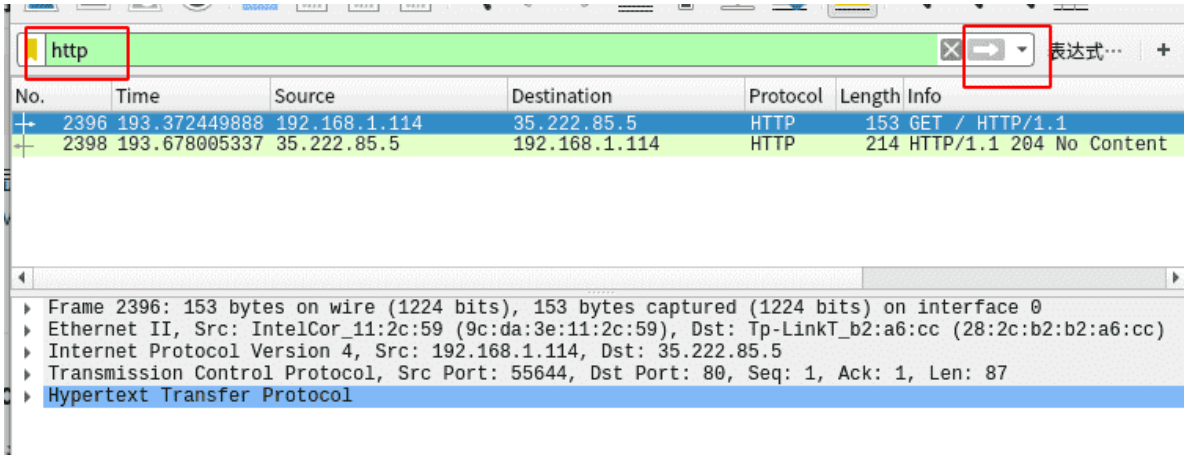


运行wireshark

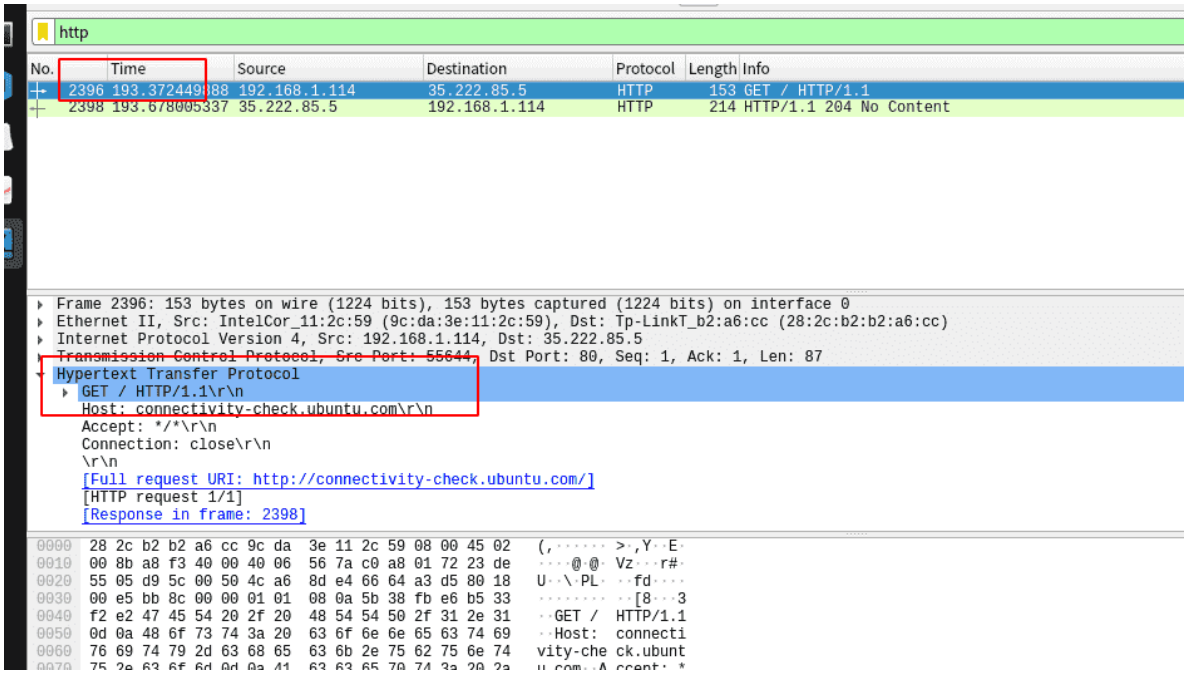
命令行启动软件，因为现在是WiFi环境，选择无线网卡`wlps20`，点击捕获->开始。



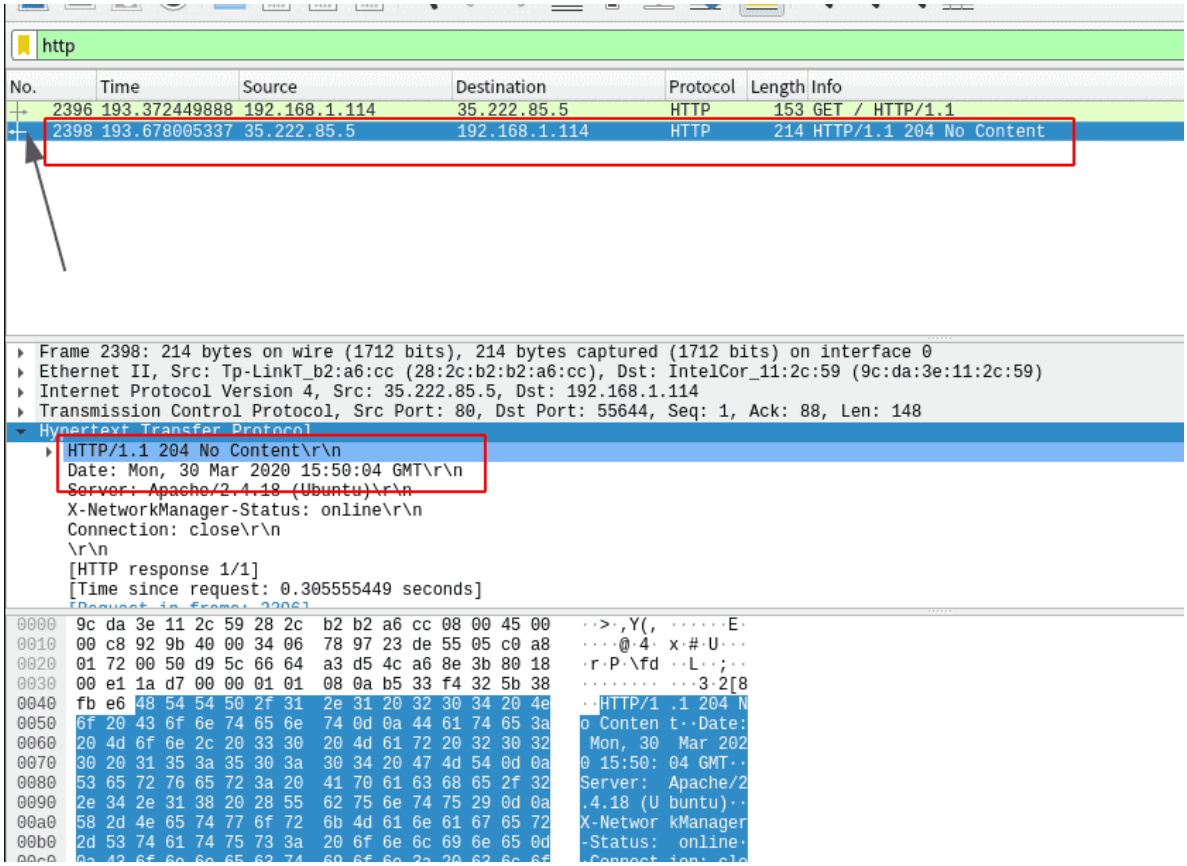
在浏览器输入一个`HTTP`协议的网页（最好是之前没浏览过的，好像本地缓存过的地址不会被wireshark抓到？）。输入完成后，点击`wireshark`中的捕获->停止，在过滤器列表输入`http`(小写)，并点击右边的箭头。



捕获的 HTTP 的请求消息



捕获的 HTTP 响应消息（紫色箭头的方向可以区分是请求消息还是响应消息）



图中的响应状态码是204

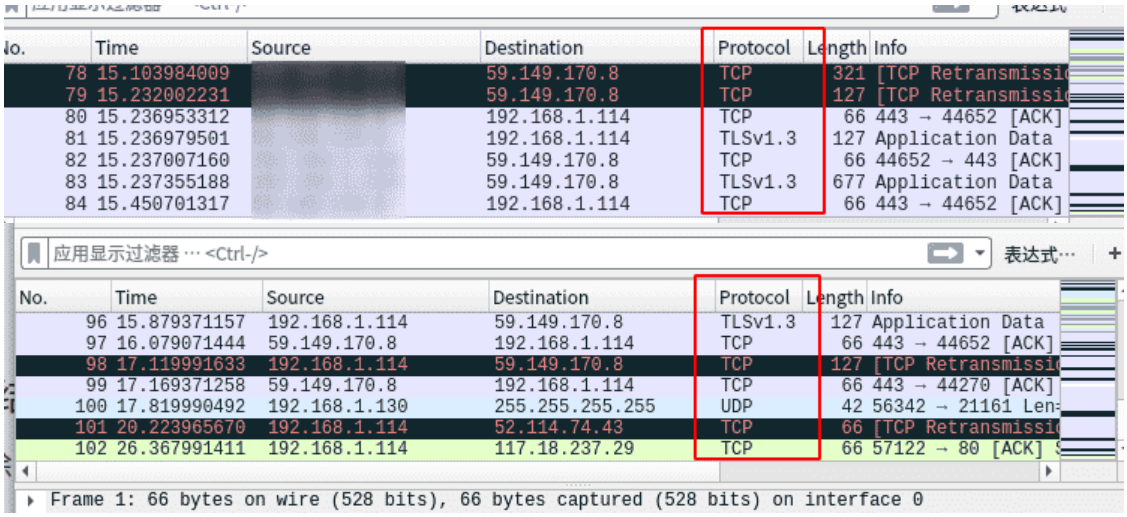
204 No Content

服务器成功处理了请求，但不需要返回任何实体内容，并且希望返回更新了的元信息。响应可能通过实体头部的形式，返回新的或更新后的元信息。如果存在这些头部信息，则应当与所请求的变量相呼应。如果客户端是浏览器的话，那么用户浏览器应保留发送了该请求的页面，而不产生任何文档视图上的变化，即使按照规范新的或更新后的元信息应当被应用到用户浏览器活动视图中的文档。由于204响应被禁止包含任何消息体，因此它始终以消息头后的第一个空行结尾。

实验结果

- 列出上述出现在未过滤的分组列表窗口的协议列中的3种不同的协议。

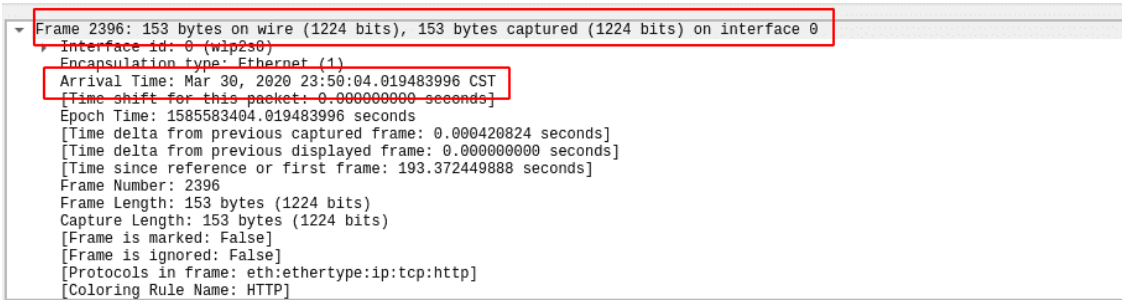
  在捕获的过程中还出现 TCP ， UDP ， TLSV1.2 ， TLSV1.3 这几种协议



- 从HTTP GET消息发送到HTTP OK回复需要多长时间?

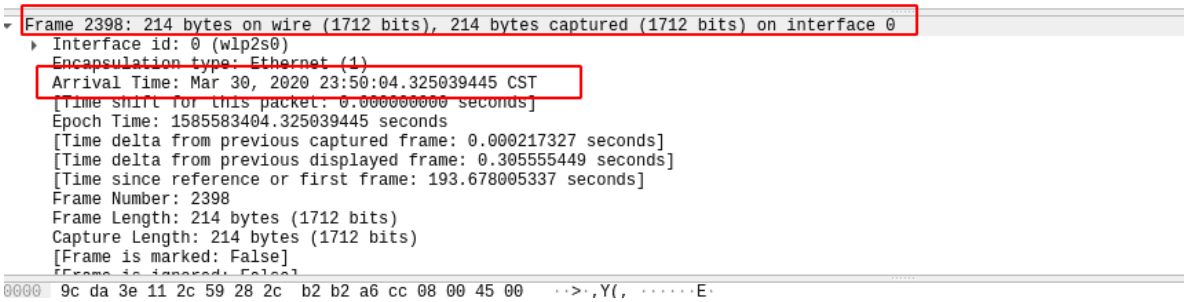
  `GET` 消息发送时间

  > Arrival Time: Mar 30, 2020 23:50:04.019483996 CST



这次实验收到的是 `204 No Content` 响应状态码

> Arrival Time: Mar 30, 2020 23:50:04.325039445 CST



所以从 `HTTP GET` 消息发送到 `HTTP No Content` 回复需要的时间为 `0.3055555449`

参考资料

- 安装wireshark
- 实验文档翻译