小实验 1 实验指导书

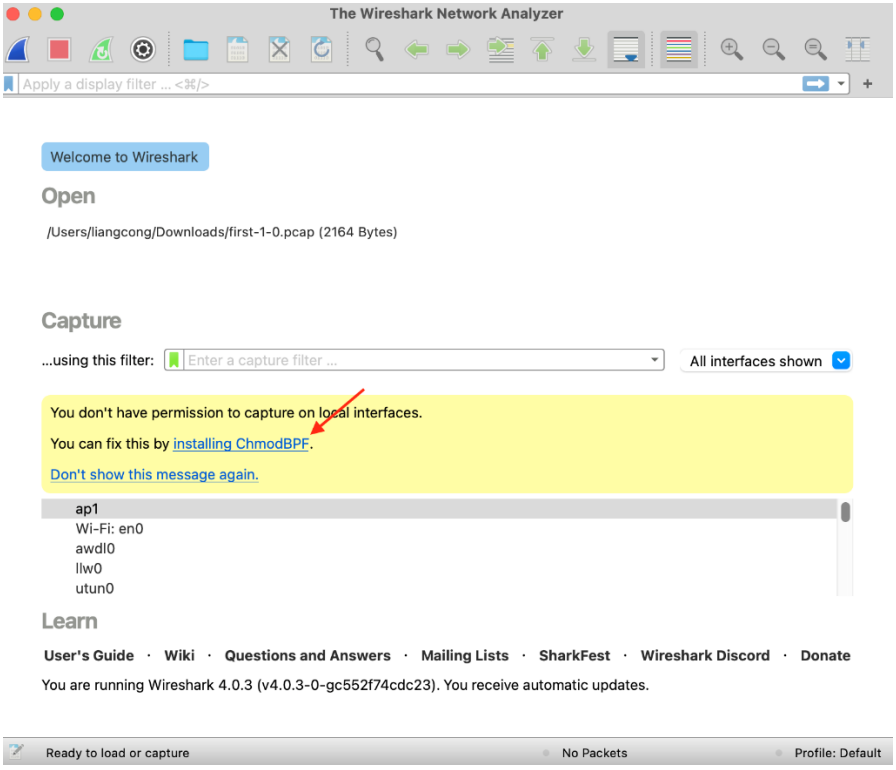
0、Wireshark 简易教程

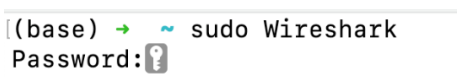
(1)下载并安装 Wireshark

官方网址：https://www.wireshark.org/#download/

助教测试版本：Wireshark 4.0.3 (windows 64bit & macOS)

注：macOS 请按照提示安装 chmodBPF；安装后若仍无法抓包，需要在命令行以 root 权限打开（命令为 sudo Wireshark）

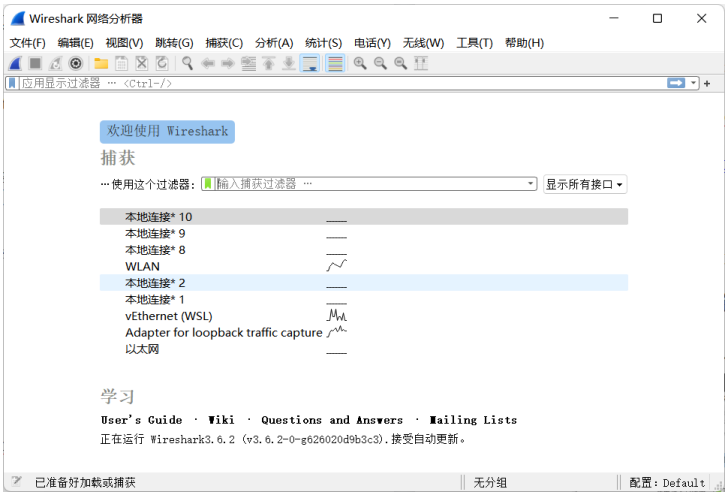




(2)Wireshark 抓包示例

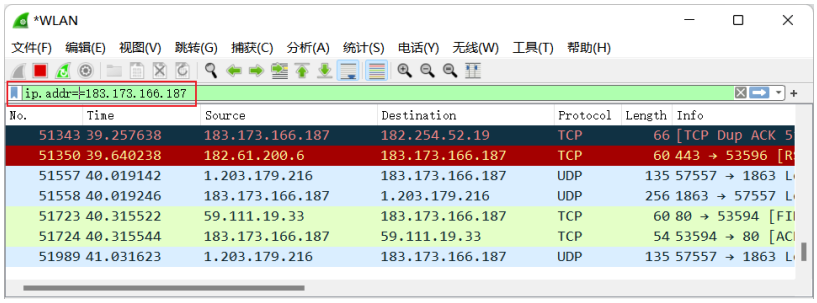
STEP 1:选择抓包接口

以无线连接为例，启动后选择 WLAN 接口开始抓包。



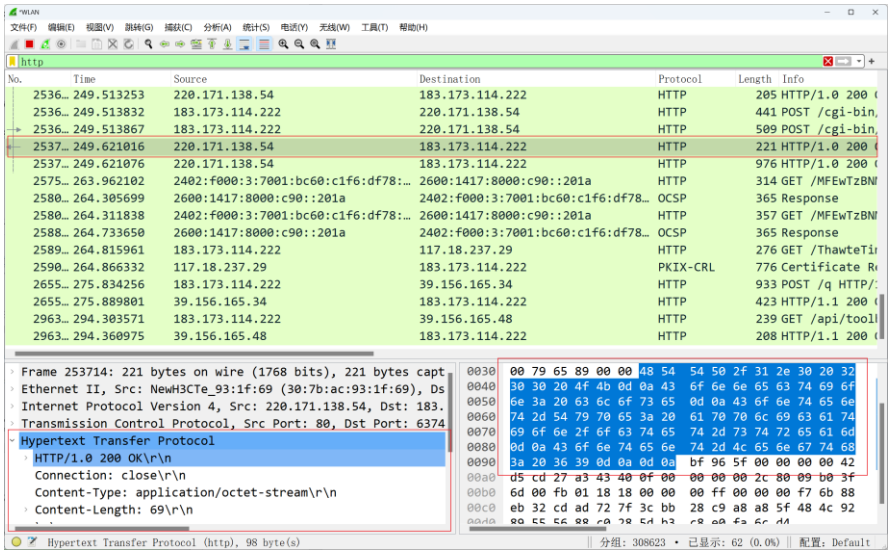
STEP 2:输入过滤条件

例：观察源或目的 IP 为 183.173.166.187 的数据包



STEP 3:观察实验结果

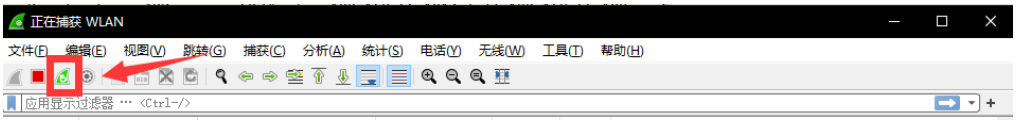
点击需要观察的报文。左下侧为 Wireshark 解析后信息，右下侧为原始报文十六进制信息。



(3)助教的 tips

A. 观察现象前重启捕获

为了能更容易找到抓包现象，做实验操作前（ping，访问网页等）先重启捕获，清空抓包缓存。



B. 利用过滤器降低干扰

组合使用 IP 过滤，协议过滤，端口过滤等条件，锁定需要观察的数据包。(无线网络场景，强烈建议使用本机地址过滤)

例如观察 HTTP 流量的实验，我们可以考虑使用本机 IP && 对端 IP && HTTP 协议作为过滤规则过滤。（例：本机地址 1.0.0.0，服务器地址 2.0.0.0，用 http 的流量：(ip.addr == 1.0.0.0 && ip.addr == 2.0.0.0) && http）

C. 常用条件：

IP 过滤： ip.addr == <IPv4>(保留源或目的 IP 为<IPv4>)

ipv6.addr == <IPv6>(保留源或目的 IP 为<IPv6>)

协议过滤： arp,icmp,tls,http(保留对应协议数据包)

端口过滤： tcp.port == 443(保留端口为 443)

组合方法：!<cond>（取反）,<cond1> && <cond2>（且）

<cond1> || <cond2>（或）

1、实验要求

本次小实验由 4 个抓包观察实验(第二部分)和 1 个简述题(第三部分)构成。所有抓包实验都需要给出简短的实验报告，内容包括：

(1)文字回答：回答指导书中提出的问题。要求简短，每个实验回答总计不宜超过 100 字。有参考答案的题目可不做文字回答。

(2)过程截图：展示关键实验过程，也可作为文字回答的补充。若无特别要求，则每个实验至少一张截图，展示实验过程。若有具体截图要求([]为要求)，则按照[]中要求给出对应截图。

注意 1：本次小实验中，抓包实验 1 有样例过程。这是为了给回答格式，回答字数做参考，同样是作业的一部分，需要再做一遍

注意 2：本次小实验中，抓包实验 4 为选做实验。不完成不扣分，完成也没有额外的加分

2、实验题目及指导

抓包实验 1：利用 Wireshark 观察 ping 流量（样例）

在控制台中使用 ping 功能，ping 百度(www.baidu.com)。

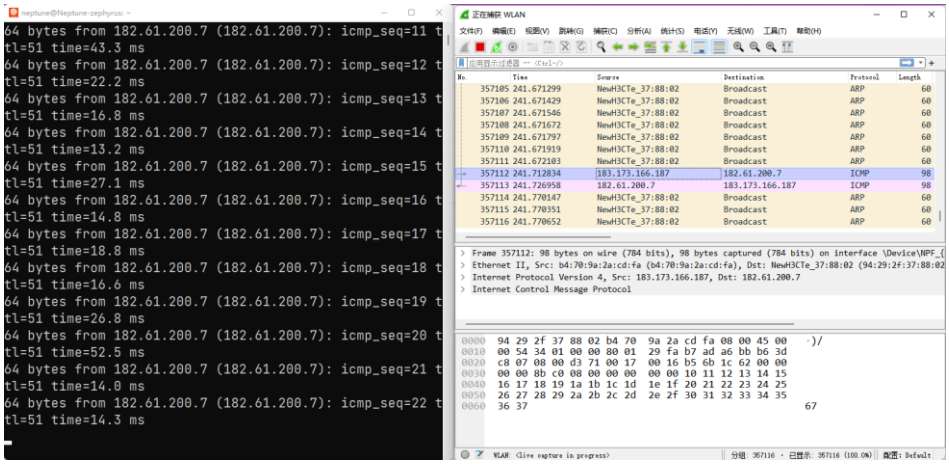
观察 Wireshark 中捕获的数据包，并回答以下问题。

（1）ping 功能使用的是什么协议？

（2）描述使用 ping 功能时，计算机与远端服务器的交互。

解题思路：

首先我们开启 Wireshark 抓包，同时在控制台启用 ping。

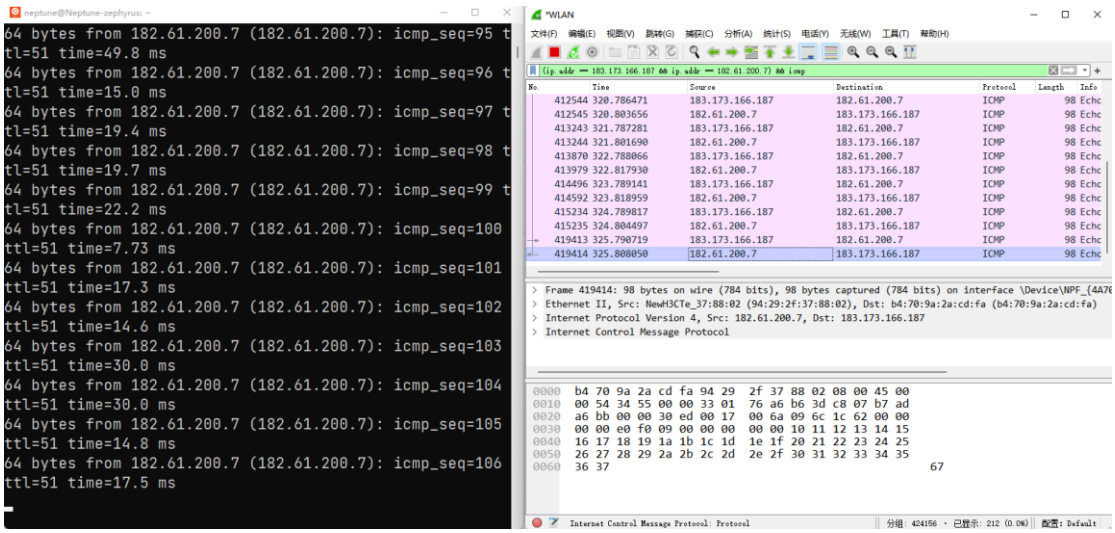


观察到随着控制台返回 ping 的结果，Wireshark 捕获到了有规律 ICMP 报文，并且对应的记录中出现了控制台所示的百度 IP 地址和自己的 IP 地址。由此我们可以推断 ping 使用的是 ICMP 协议。

接下来使用过滤器进一步过滤。利用源端 IP 地址(本机)，目的 IP 地址(百度)和协议(ICMP)三个参数来设置我们的过滤器。

- 本机地址 183.173.166.187
- 目标地址 182.61.200.7
- 目标协议 ICMP

组合成过滤规则为：(ip.addr == 183.173.166.187 || ip.addr == 182.61.200.7) && icmp



观察结果并分析。交互流程主要由一个 request 和一个 reply 构成，交互过程中网卡会记录前后延时，也就是我们在控制台上看到的 ping 延时。(Linux 系统在长度足够时，会使用 data 字段传输时间戳以实现更好的时延测量)。一组 request 和 reply 报文构成关键过程截图内容。

推荐的答题格式：

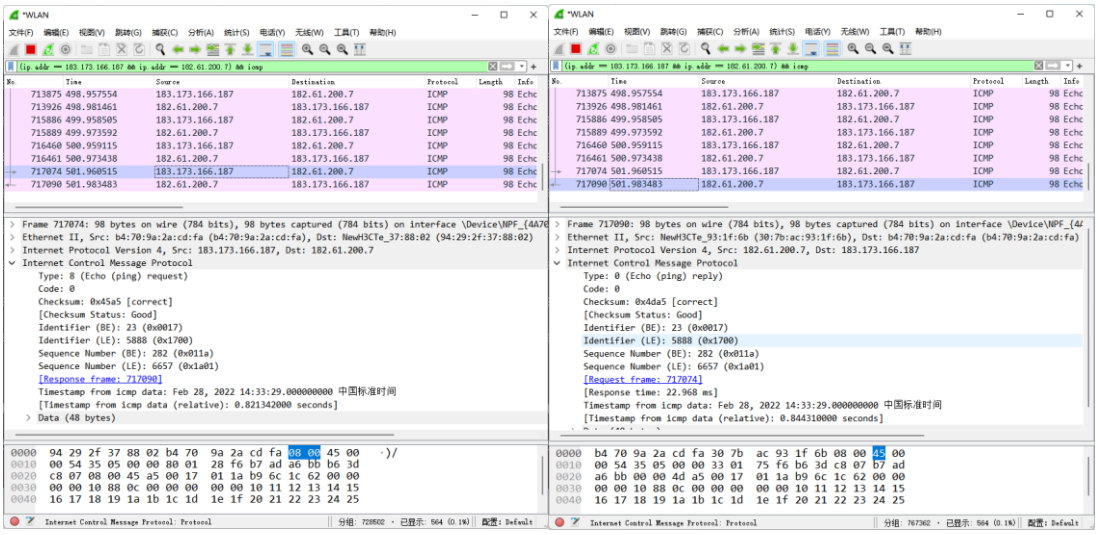
1、回答思考题

（1）ICMP 协议

（2）交互流程主要由一个 request 和一个 reply 构成，交互过程中网卡会记录前后延时，也就是我们在控制台上看到的 ping 延时。

（注意所有思考题不设标准答案，描述你的发现即可，不必追求细致，答案仅供参考）

2、附上关键实验过程截图



抓包实验 2：利用 Wireshark 观察 http&https 流量

启动浏览器，打开中国政府网（http://www.gov.cn/），观察 Wireshark 中捕获的数据包。

启动浏览器，打开清华官网（https://www.tsinghua.edu.cn/），观察 Wireshark 中捕获的数据包。

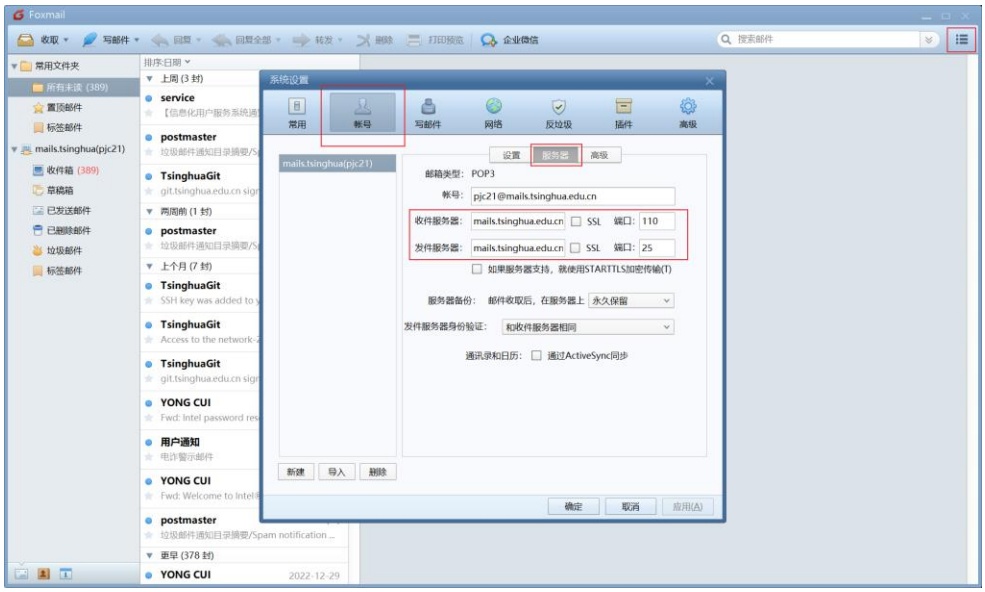
综合以上实验的结果，回答以下问题。

（1）观察浏览中国政府网过程中捕获的数据包，你是否能看到网页源代码的内容？**[截图展示数据包中的 HTML 网页源代码。(有中文文字内容为佳)]**

（2）观察浏览清华官网的过程中捕获的数据包，你是否能看到网页源代码的内容？

注 1：Safari 浏览器可能强制 HTTPS，可用 Chrome 浏览器进行实验

抓包实验 3：利用 Wireshark 观察 SMTP 流量



下载安装软件 Foxmail(https://www.foxmail.com/)，并登录自己的清华邮箱。在设置--账号--服务器中，取消收件和发件的服务器的 SSL 选项。编辑邮件并发送至任意邮箱，观察捕获的数据包。(建议内容为“Network Class”，方便观察正文信息)

（1）观察邮件收发的数据包，你是否能够看到刚才发送的邮件信息？**[截图展示数据包中的邮件正文信息]**

（2）尝试利用捕获的数据包内容，获得你邮箱的用户名和密码。对你有什么启示？**[截图展示数据包中用户密码，请将具体数值涂黑]**

参考资料：Base64 编解码网址(https://base64.us/)

注 1：完成实验后恢复 SSL 选项，避免信息泄露。

注 2：部分邮箱设置第三方登录要求手机二次验证生成动态授权码，此时抓包观察到的密码是动态授权码而非账户密码。因此建议使用清华邮箱实验，效果较为明显。

抓包实验 4：利用 Wireshark 观察 QQ 流量（选做）

启动电脑端 QQ，观察 Wireshark 中捕获的数据包。

（由于本实验在 macOS 和 windows 上的难度差距较大，故作为选做实验。推荐使用 windows 环境做实验，效果更明显）

（1）在你的平台上，QQ 使用什么传输层协议，什么应用层协议？

（2）对于 windows 用户，你是否能从 Wireshark 解析后信息中，得知 QQ 正在进行的操作？

3、简述题

数据从应用下发到网络的过程中，经过层层封装（如下图）。请你结合本次实验，说明 Ping（ICMP 协议）、http 协议、邮件协议，分别使用了哪些协议进行逐层封装，才最终将数据发送出去？（力求简短，总计不宜超过 200 字）