1. **实验目的：**

1、熟悉掌握Wireshark的使用方法；

2、理解ARP原理与IP报文的报头结构。

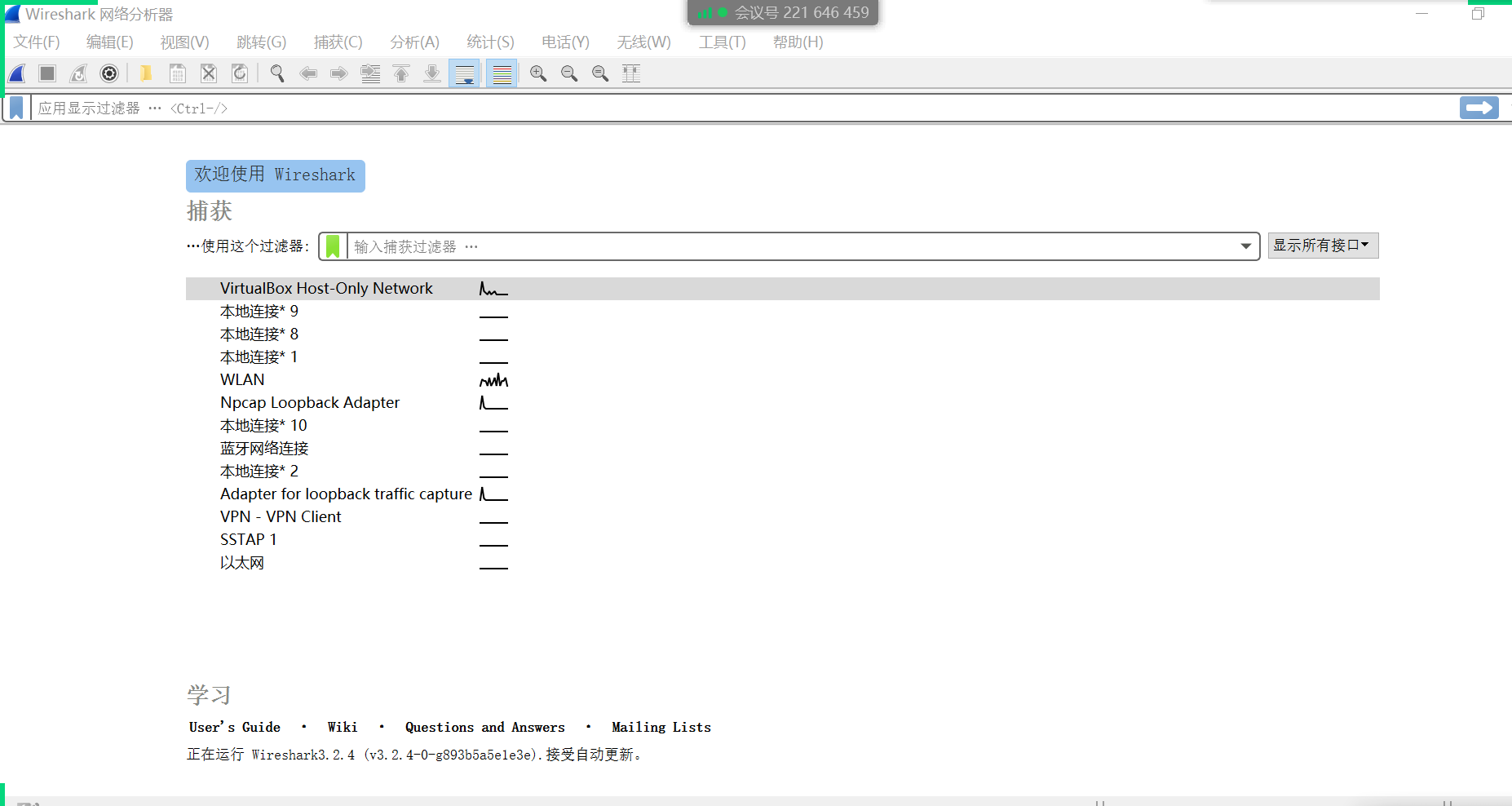
1. **实验配置**

与因特网连接的计算机；

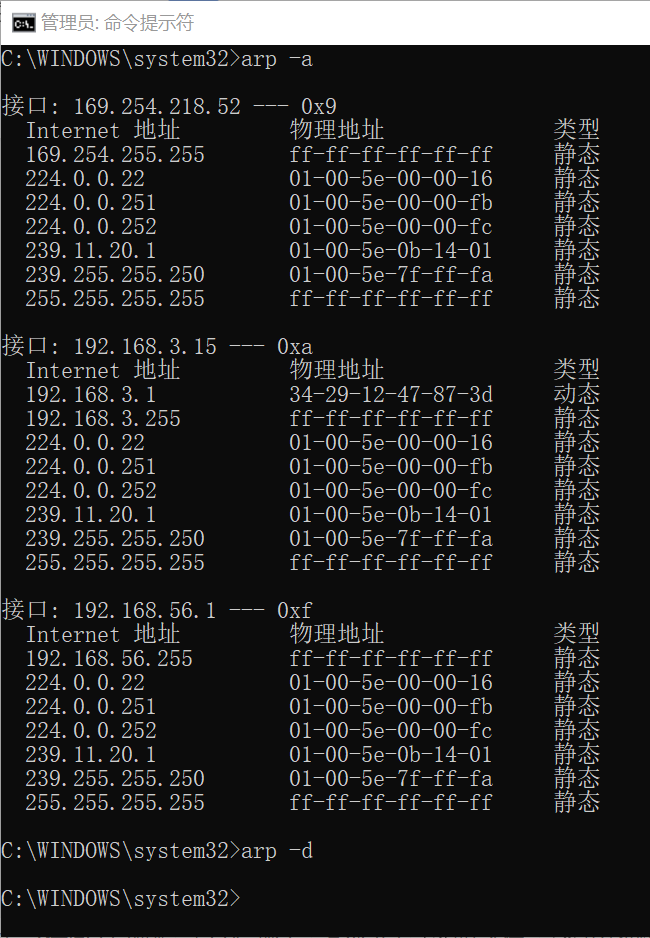
主机操作系统为windows；

Wireshark、IE等软件。

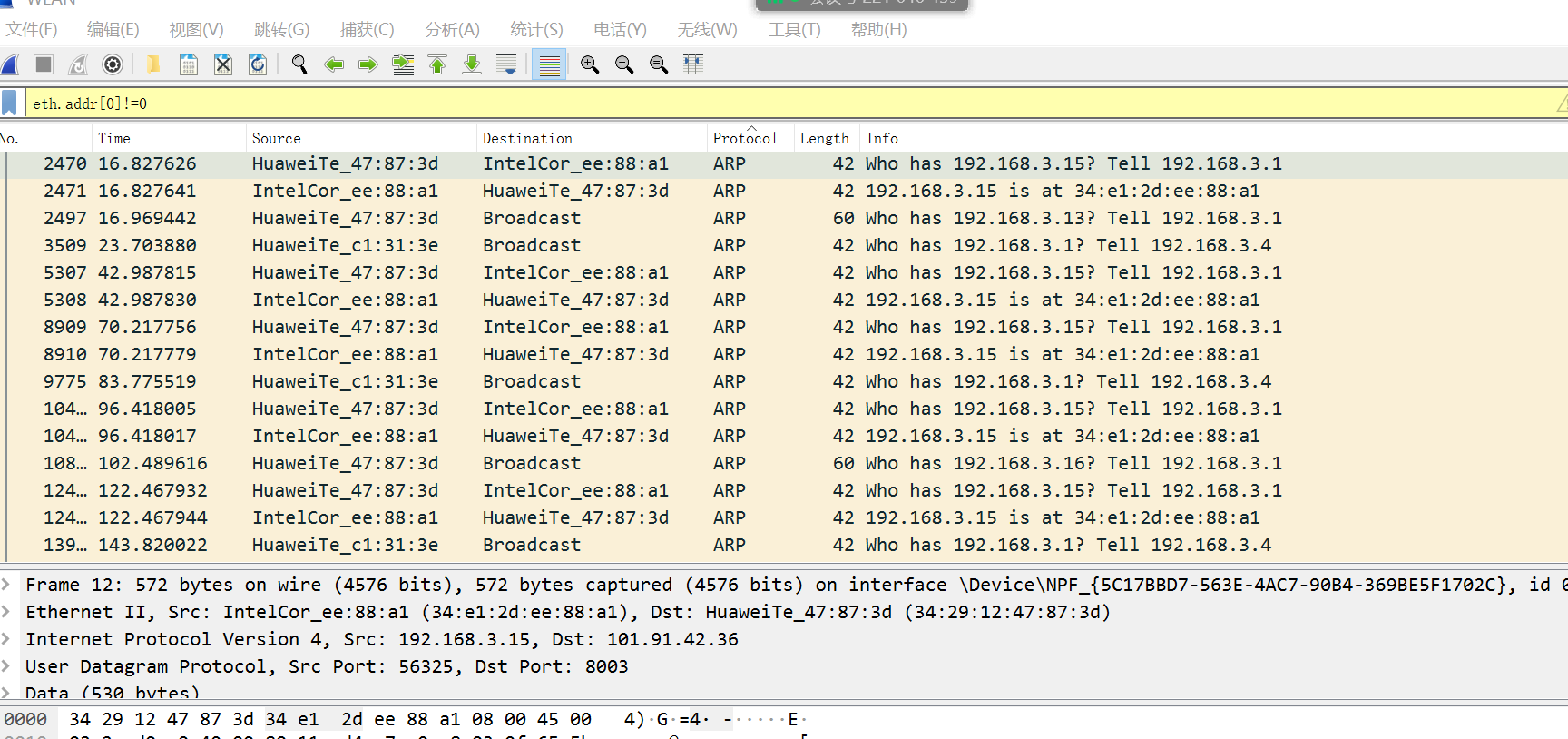
1. **实验步骤：**
2. 启动Wireshark，开始抓包；



1. 在命令提示符中清除ARP缓存；

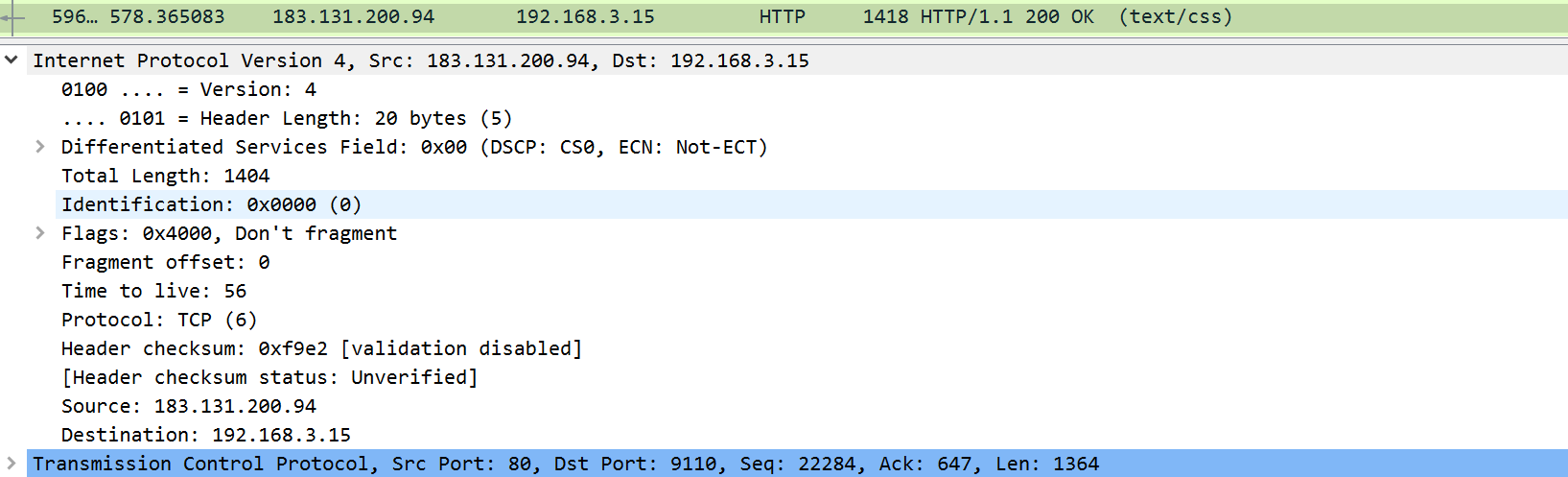
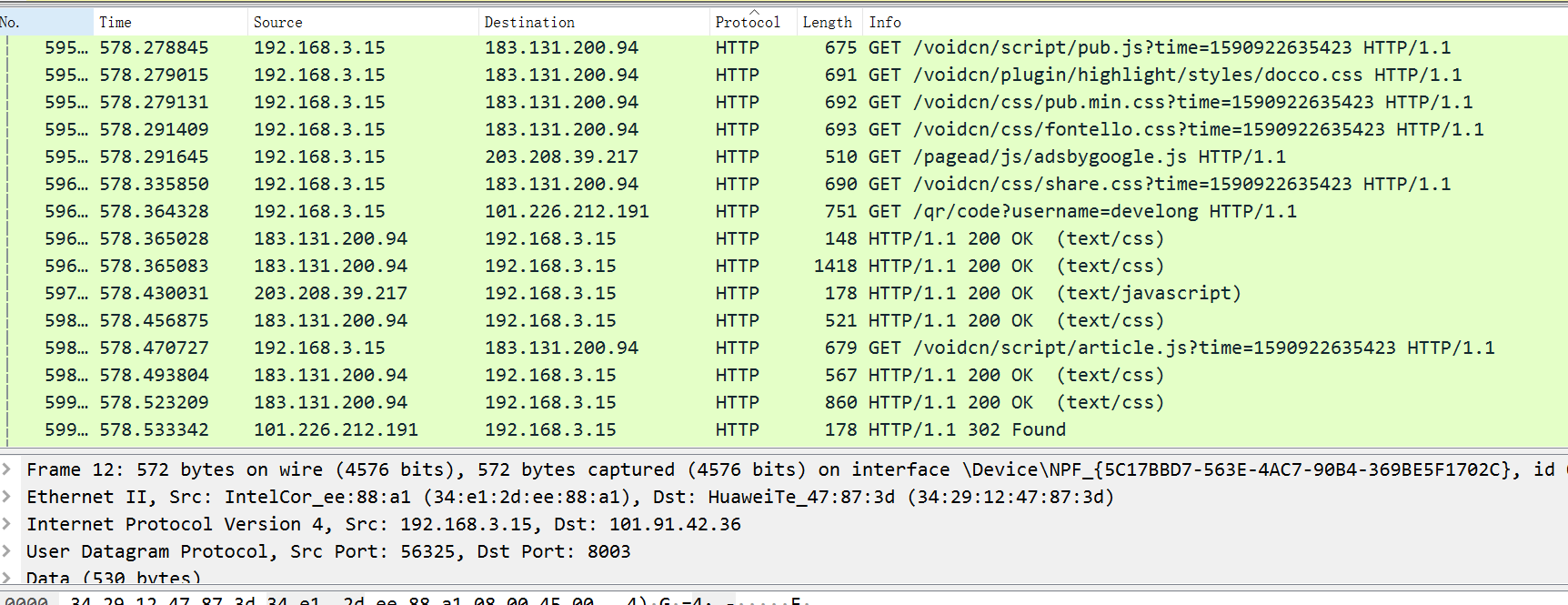


1. **实验报告内容：**
2. **找到一个ARP请求分组，和对它的响应分组，观察ARP包的封装层次，是否所有的ARP请求都是广播包？**



[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA/455151" \t "https://baike.baidu.com/item/ARP/_blank)发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，因此ARP请求消息都是以广播包发送的。

1. **找到一个IP包，观察IP层首部，分析IP首部各字段值，并说明其含义，例如该IP协议版本号是多少？首部长度是几个字节？整个IP数据报长度是多少字节？源IP地址和目的IP地址各是什么？等等,尽量全面。**



该IP协议版本号：Version 4，IPv4

首部长度：20 bytes

Differentiated Services Field为区分服务字段

整个IP数据报长度：1404

标识：0x0000

标志：0x4000

片偏移：0

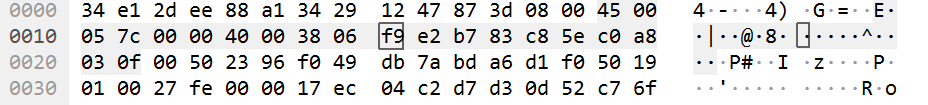
协议：TCP

首部校验和为：0xf9e2

源IP地址：183.131.200.94

目的IP地址：192.168.3.15

1. **根据抓到的IP Header内容，计算校验和，并验证**



计算校验和：

4500+057c+0000+4000+3806+f9e2+b783+c85e+c0a8+030f=3FFFC

0003+FFFC=FFFF

~FFFF=0000

1. **停止捕获**



参考资料：

1. <https://blog.csdn.net/luokh327/article/details/50801190>
2. <https://blog.csdn.net/hebbely/article/details/54424823>