**电子科技大学信息与软件工程学院**

**标 准 实 验 报 告**

**（实验）课程名称 网络安全技术**

**电子科技大学教务处制表**

**电 子 科 技 大 学**

**实 验 报 告**

**学生姓名：陆圣珩 学 号： 2017221302009 指导教师：赵洋**

**实验地点：信软学院楼西303 实验时间：11-12**

**一、实验室名称：**

**二、实验项目名称：网络侦听实验**

**三、实验学时： 4 学时**

**（一）实验目的**

通过使用Sniffer（嗅探）工具，实现捕捉ARP、ICMP、FTP等协议的数据包，以理解TCP/IP协议栈中多种协议的数据结构、会话连接建立和终止的过程、TCP序列号、应答序号的变化规律。并且通过实验了解FTP、HTTP等协议明文传输的特性，以建立安全意识，防止FTP、HTTP等协议由于传输明文密码造成的泄密。

**（二）实验内容**

1. 地址解析协议（ARP）实验
2. 网络路径跟踪（TRACE）实验
3. TCP连接实验

**四、实验原理：**

1. **地址解析协议（ARP）实验**

本实验中，所有计算机位于一个物理网络中：所有计算机通过以太网交换机连接在一个以太网中。该物理网络中没有连接路由器。同时，所有计算机也位于同一个IP网络中。

IP分组在以太网中发送时，除了要有接收站的IP地址（IP分组中的目的IP地址）外，还需要接收站的MAC地址（以太网帧中的目的MAC地址）。ARP协议将IP地址（逻辑地址）动态映射为MAC地址（物理地址）。

实验中两人一组，在“**未知**”（使用命令***arp -d \**** 清空ARP缓存表）和“**已知**”IP网络内通信时所需地址映射（目的IP地址，目的MAC地址）这两种情况下，先后使用计算机上的通信测试命令（***ping***）发起一次通信过程，并通过使用Sniffer软件捕获通信过程中通信双方的交互信息。比较两次通信过程中所捕获的分组数量、分组类型和分组内容，分析ARP协议的工作原理，包括：ARP分组（ARP请求分组和ARP应答分组）的产生条件、具体内容和传输方式。

每个实验者使用计算机上的ARP缓存表查看命令（***arp -a***），查看本小组的ARP协议操作结果和ARP缓存表内容，了解ARP缓存表的形成及其在ARP协议操作过程中的作用。

1. **网络路径跟踪（TRACE）实验**

本实验中，每个实验小组中的计算机分别连接在两个以太网中，每个以太网被配置为一个IP子网。

ICMP协议作为IP协议的辅助协议，提供差错报告和查询机制。

实验者在计算机上使用路径跟踪命令（***tracert***）查看子网A和子网B之间的通信路径，理解并掌握命令的用途和使用方法，结合IP协议、ICMP协议分析命令的工作原理。

实验者通过更改***tracert***命令参数，结合Sniffer软件所捕获的数据报文和ICMP的差错报告机制，考察IP分组生存时间（TTL）的含义及其对网络间IP分组交付的影响，了解并体会***tracert***命令的工作原理。

1. **TCP连接实验**

本实验中，所有计算机位于一个物理网络中：所有计算机通过以太网交换机连接在一个以太网中。该物理网络中没有连接路由器，有一台FTP服务器。所有计算机和FTP服务器位于同一个IP网络中。

TCP协议是一个面向连接的、可靠的运输层协议，通过连接建立和连接终止这两个过程完成面向连接的传输。

FTP协议是一个用于文件传输的应用层协议，采用客户/服务器模式实现文件传输功能，使用TCP协议提供的面向连接的可靠传输服务。FTP客户和服务器之间需要建立两条FTP连接：控制连接（端口21）和数据连接（端口20）。

实验者的计算机作为FTP客户，通过***ftp***命令与FTP服务器进行一次FTP会话活动。使用Sniffer软件捕获通信双方的交互信息，考察TCP协议的连接建立过程和连接终止过程。

分析TCP连接建立和连接终止过程中所捕获的TCP报文段，掌握TCP报文段首部中的端口地址、序号、确认号和各个码元比特的含义和作用。结合FTP操作，体会网络应用程序间的交互模式——客户/服务器（C/S）模式。

**五、实验器材（设备、元器件）**

* 1. 实验人数50～80人，每人1台计算机；2人一组配合完成本实验。
  2. 拓扑：（A、B范围中的主机分别简称为A主机和B主机）



**A**

**B**

* 1. 设备：以太网交换机2～4台；计算机50～80台
  2. 软件：Sniffer软件（捕获网络上传输的数据报文）

**六、实验步骤**

**（一）地址解析协议（ARP）实验**

1. 在A、B主机上运行Sniffer软件，设置捕获条件：

Address：Type = Hardware，Mode = Include，

Station 1 = <本机MAC地址>，Station 2 = any：

Advanced：Protocol = ARP，ICMP

1. 清空A、B主机上的ARP缓存表（命令：***arp -d \****）。
2. 在A、B主机上启动Sniffer的捕获过程。首先由A主机PING B主机。PING结束以后，停止A、B主机的Sniffer捕获过程，保存捕获数据。
3. 查看A、B主机上的ARP缓存表（命令：***arp -a***）。
4. 在A、B主机上再次启动Sniffer的捕获过程，由B主机PING A主机。PING结束以后，停止A、B主机的Sniffer捕获过程，保存捕获数据。
5. 查看A、B主机上的ARP缓存表（命令：***arp -a***）。
6. 查看并比较步骤3和步骤5中A、B主机上Sniffer软件所捕获的数据报文数量和类型。

**（二）网络路径跟踪（TRACE）实验**

1. 根据实验拓扑要求设置主机上的TCP/IP协议配置参数。运行Sniffer软件，设置捕获条件：

Address：Type = IP，Mode = Include，

Station 1 = <本机IP地址>，Station 2 = any：

Advanced：Protocol = ICMP

1. 计算子网A、B的子网地址和子网广播地址。
2. 路径跟踪——TRACE
3. 在主机的cmd窗口键入“***tracert***”命令，查看并分析选项***-d***、***-h***的含义和作用。
4. 启动Sniffer捕获过程，子网A、B中的主机TRACE对方子网中的1个主机IP地址。TRACE结束以后，停止Sniffer的捕获过程，保存捕获数据，查看并解释本主机上显示的通信结果。
5. 启动Sniffer捕获过程，使用***-d***选项TRACE步骤3-2中的目的主机。TRACE结束后，停止Sniffer的捕获过程，保存捕获数据，查看本主机上显示的通信结果，并与步骤3-2的结果相比较。
6. 启动Sniffer捕获过程，使用***-d***和***-h***选项重新TRACE步骤3-2中的目的主机，***-h***选项取值分别为***1***、***2***、***3***。TRACE结束以后，停止Sniffer的捕获过程，保存捕获数据，查看本主机上显示的通信结果。
7. 启动Sniffer捕获过程，使用***-d***和***-h***选项TRACE对方子网中1个不存在的主机IP地址，***-h***选项取值为***6***。TRACE结束以后，停止Sniffer的捕获过程，保存捕获数据，查看本主机上所显示的通信结果。

**（三）TCP连接实验**

* 1. 在主机上运行Sniffer软件，设置捕获条件：

Address：Type = IP，Mode = Include，

Station 1 = <本机IP地址>，Station 2 = 192.168.3.254：

Advanced：Protocol = FTP

* 1. 启动Sniffer的捕获过程，并在主机的cmd窗口中以命令行的方式启动FTP客户进程，过程如下：

（***黑斜体***表示输入内容，其它为系统显示信息）

C:\> ***ftp 192.168.4.254（或ftp 192.168.3.254）***

Connected to 192.168.4.254.

220 Serv-U FTP Server v4.0 for WinSock ready…

User (192.168.3.254:(none)): ***ftp***

331 User name okay, please send complete E-mail address as password.

Password: ***ftp@***

230 User logged in, proceed.

ftp> ***quit***

221 Goodbye!

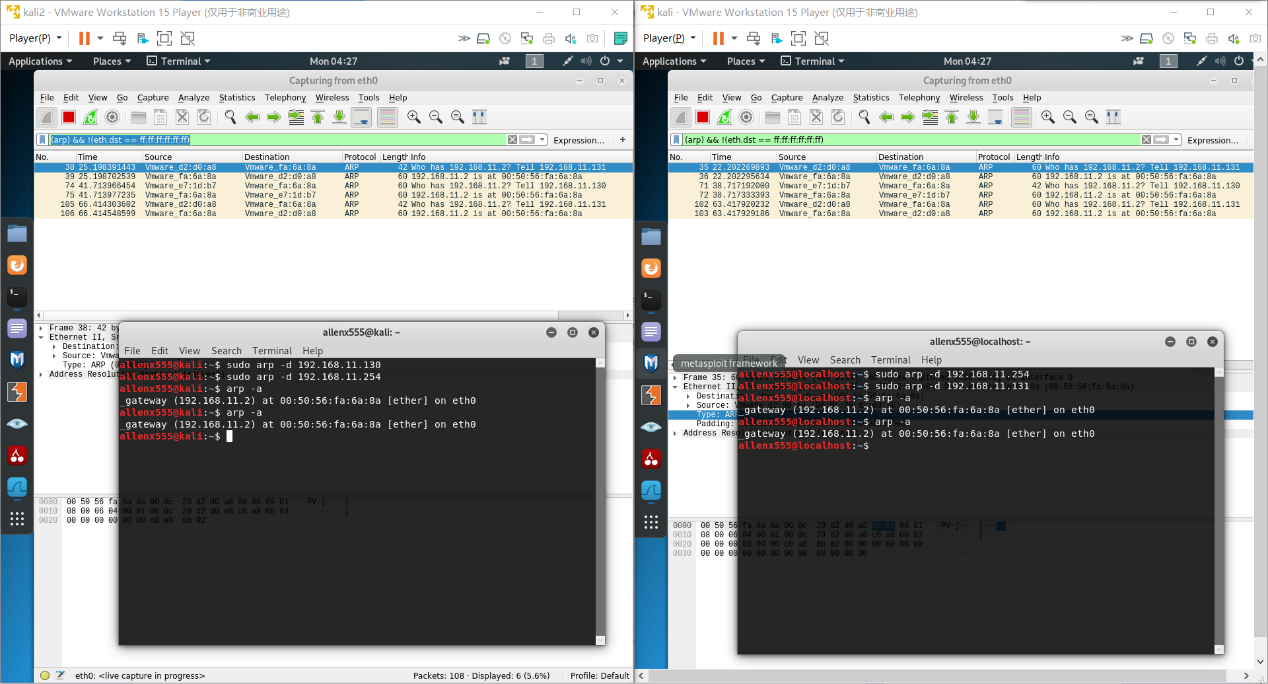
* 1. 停止Sniffer的捕获过程，保存捕获数据。
  2. 查看捕获报文中的本机FTP进程端口号、FTP服务器进程端口号、本机TCP初始序号和服务器TCP初始序号。
  3. 重复步骤2和3，查看捕获报文中的本机FTP进程端口号、FTP服务器进程端口号、本机TCP初始序号和服务器TCP初始序号，并与步骤4的查看结果相比较。

**七、实验数据及结果分析**

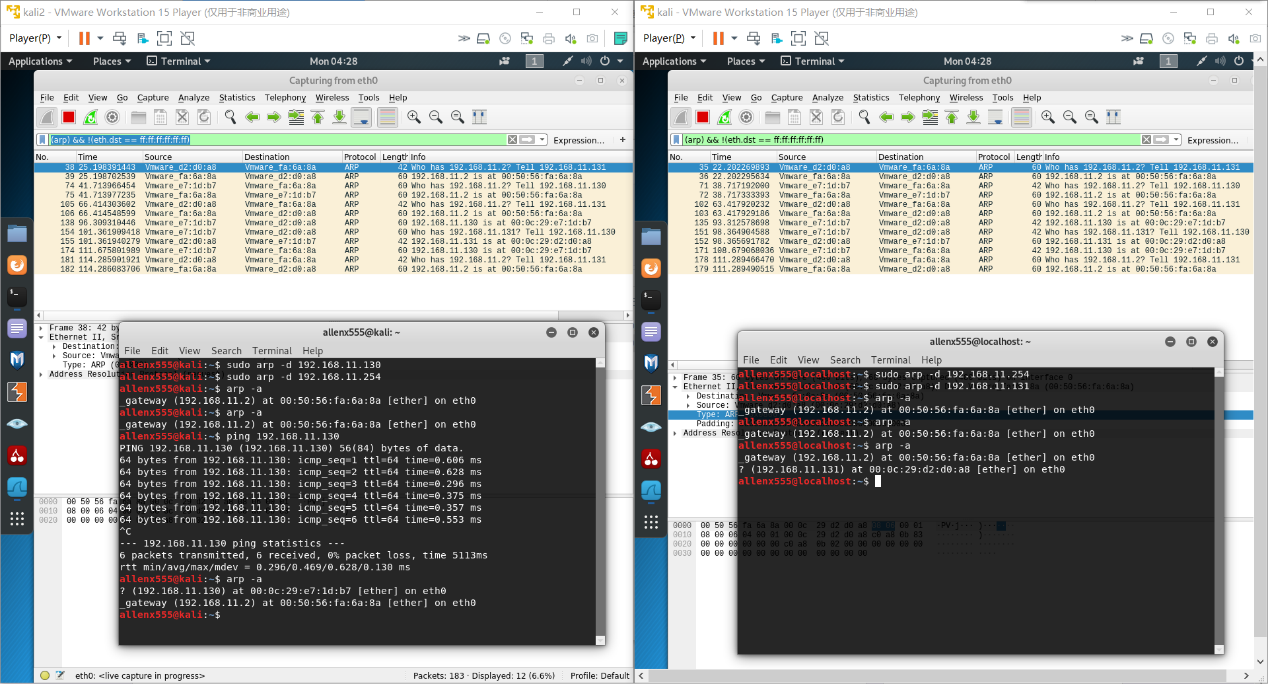
**（一）地址解析协议（ARP）实验**

因网络原因，选择自建两个虚拟机，网络选择 NAT 模式，使其在同一网关下进行实验。

清空arp 表及第一次ping：



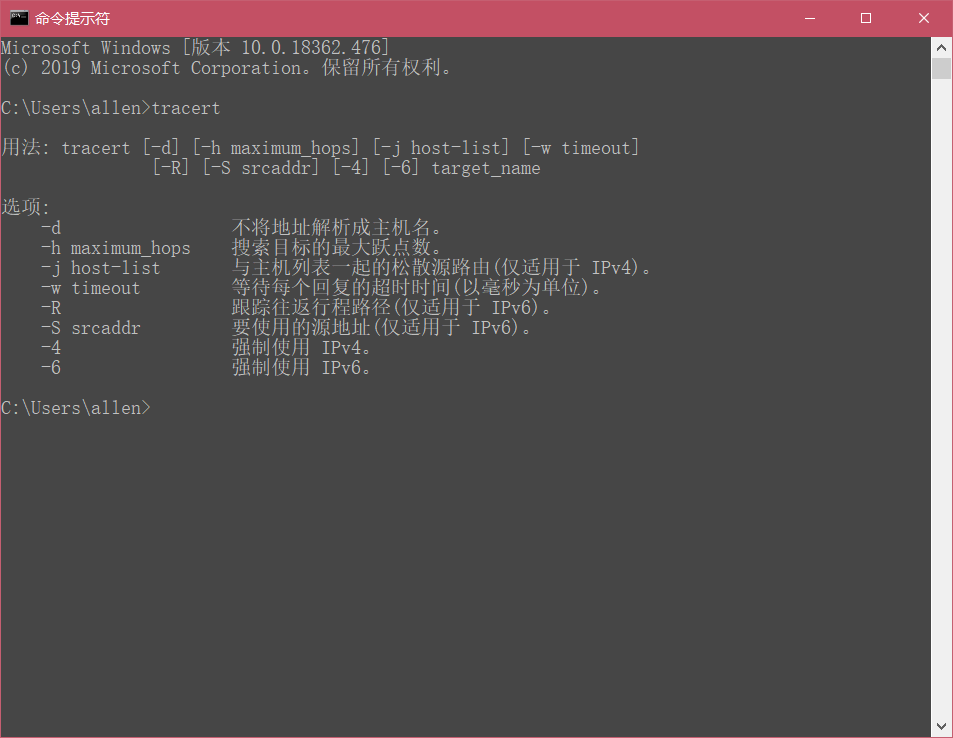
第二次ping：



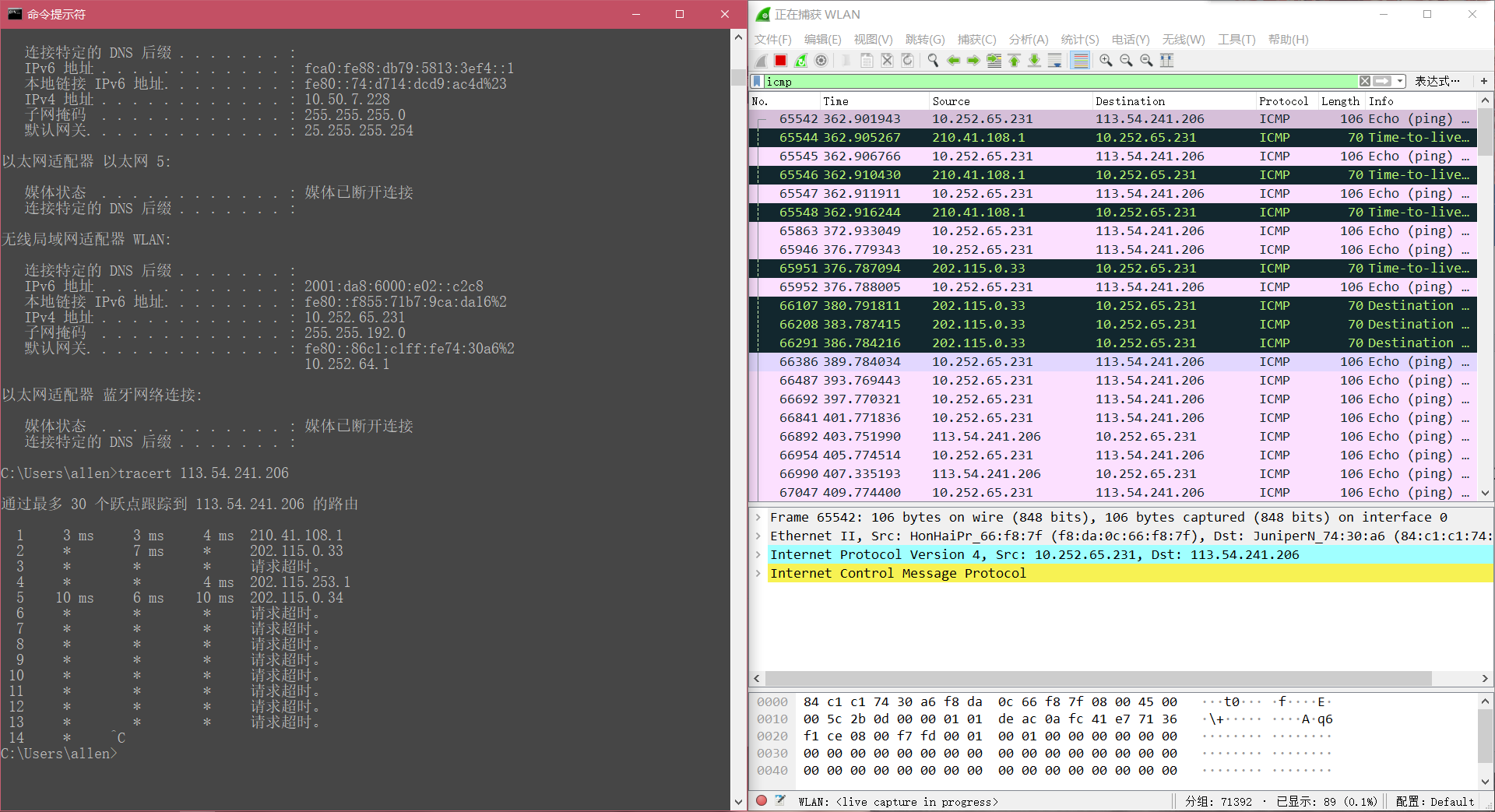
**（二）网络路径跟踪（TRACE）实验**

此实验与小组同学，一人在 UESTC-WIFI 下，一人在UESTC-WIFI-GUEST下。

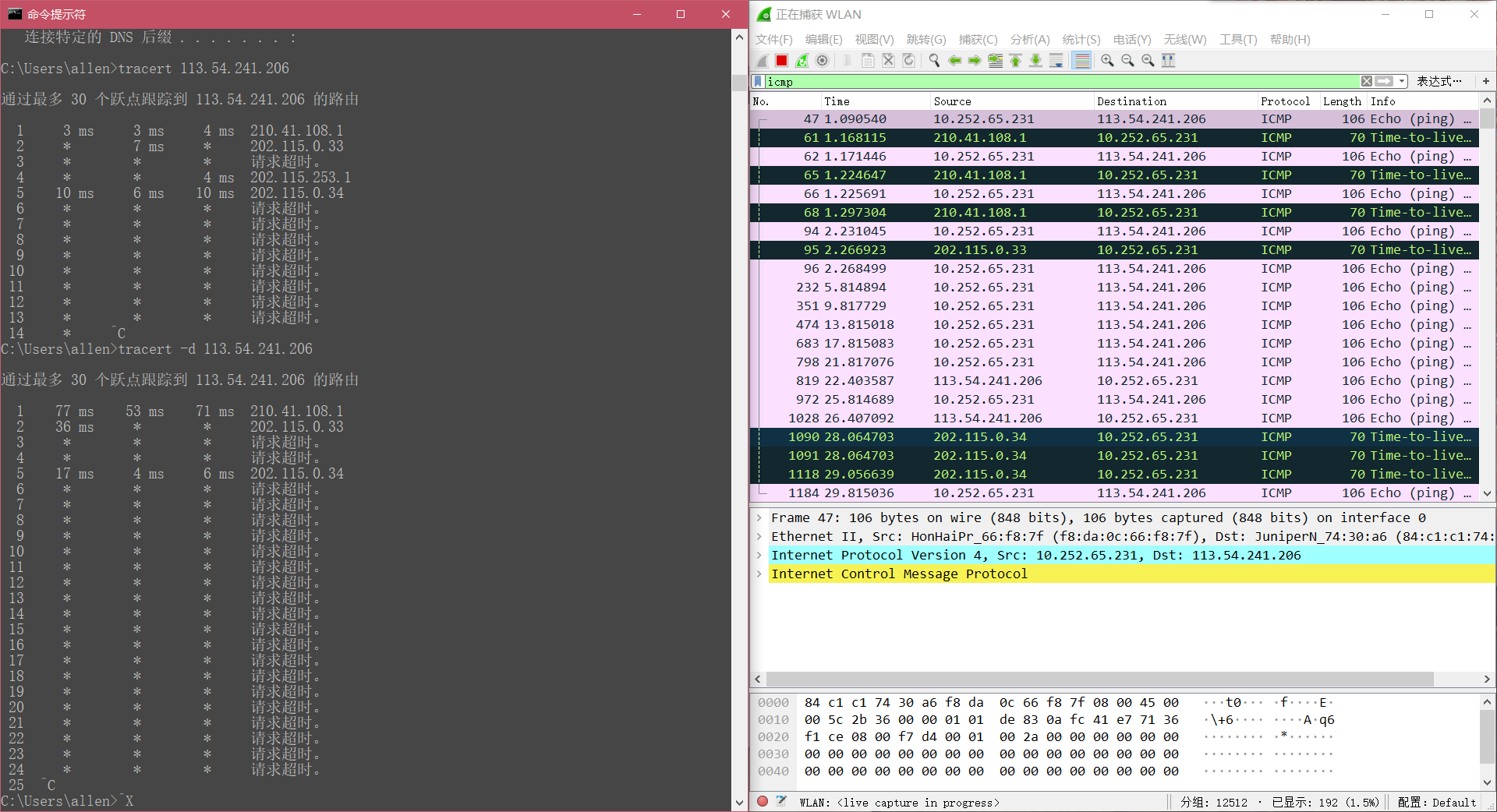
查看 tracert：



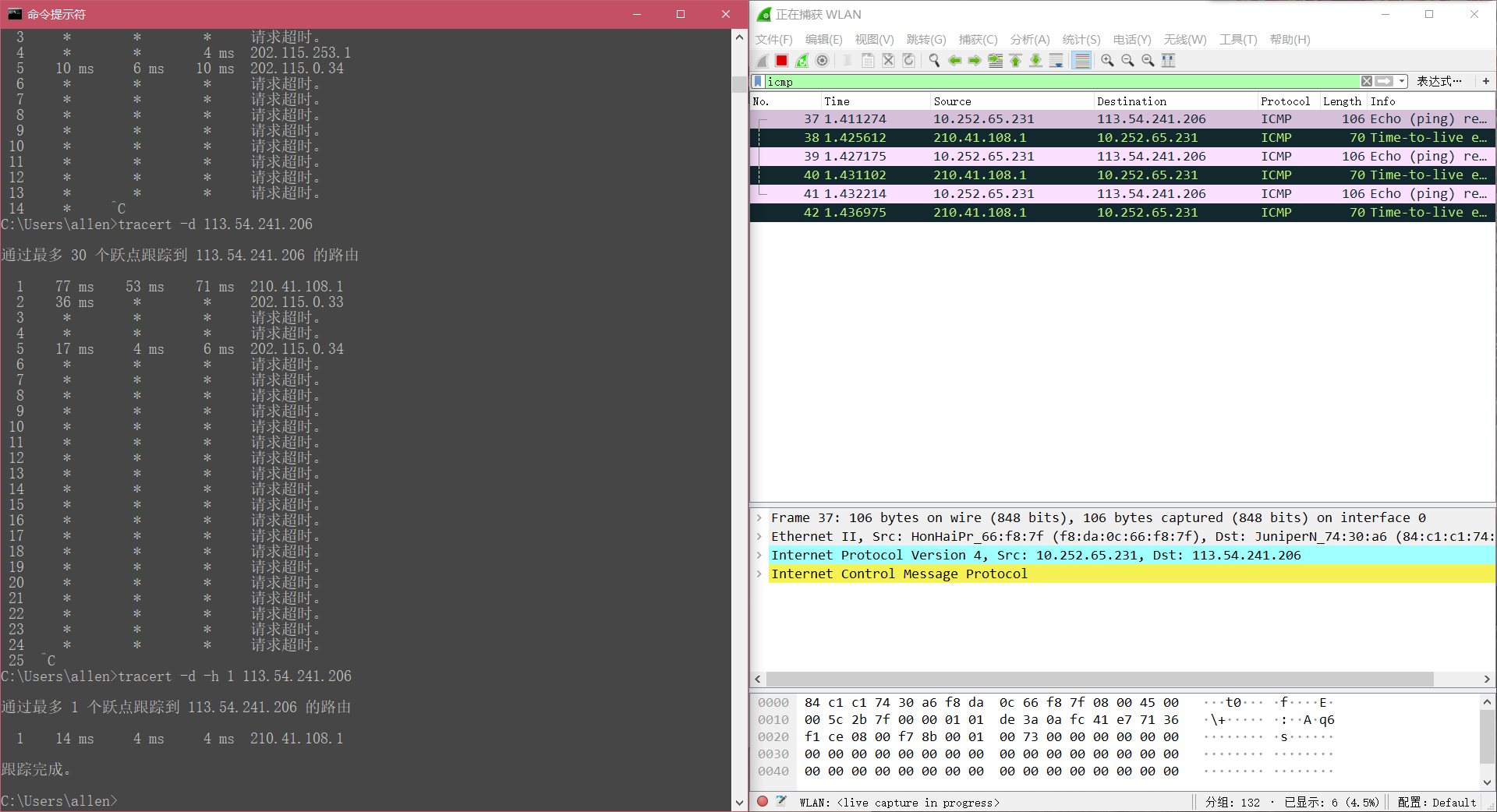
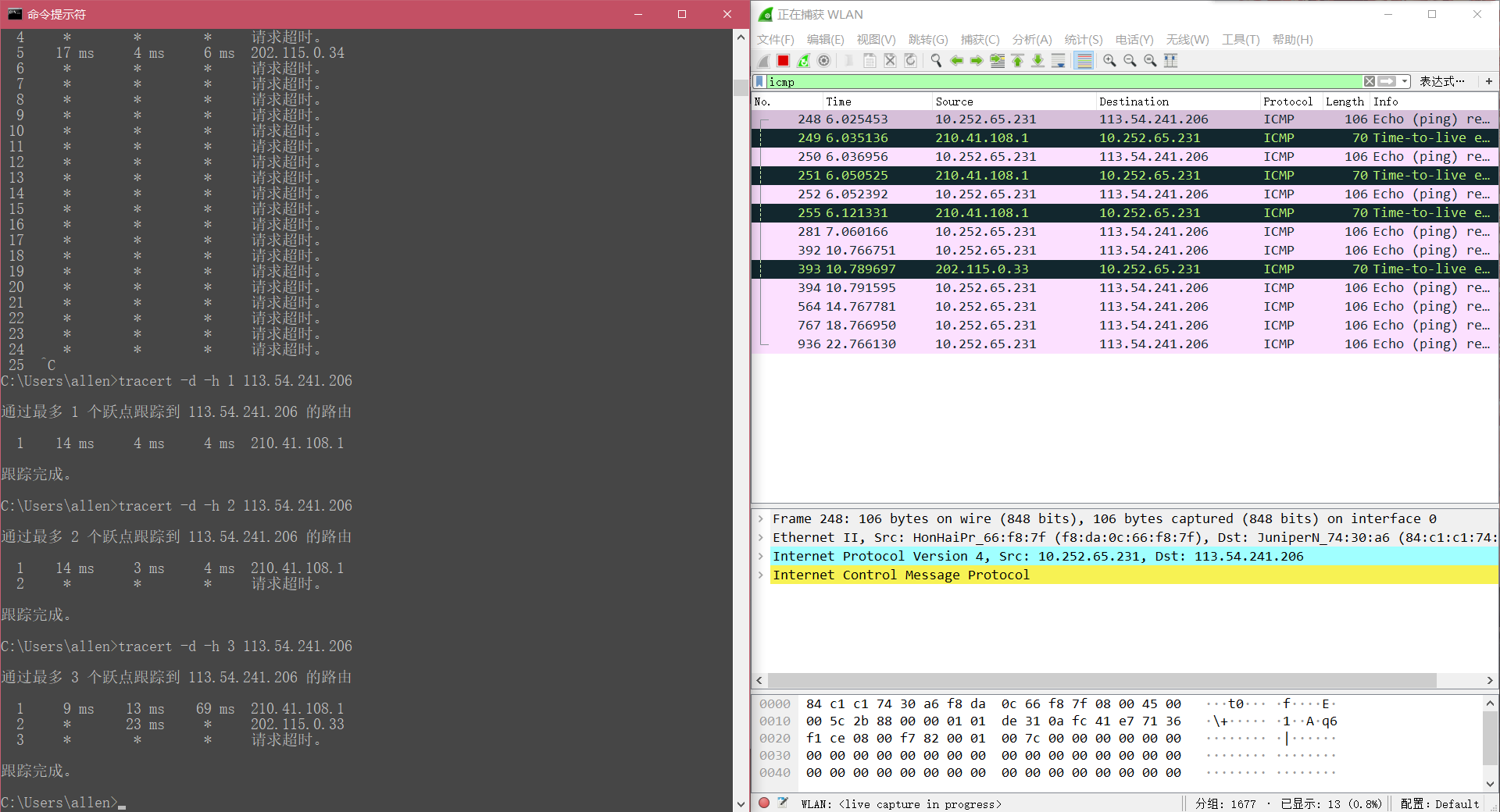
无参数：



-d：

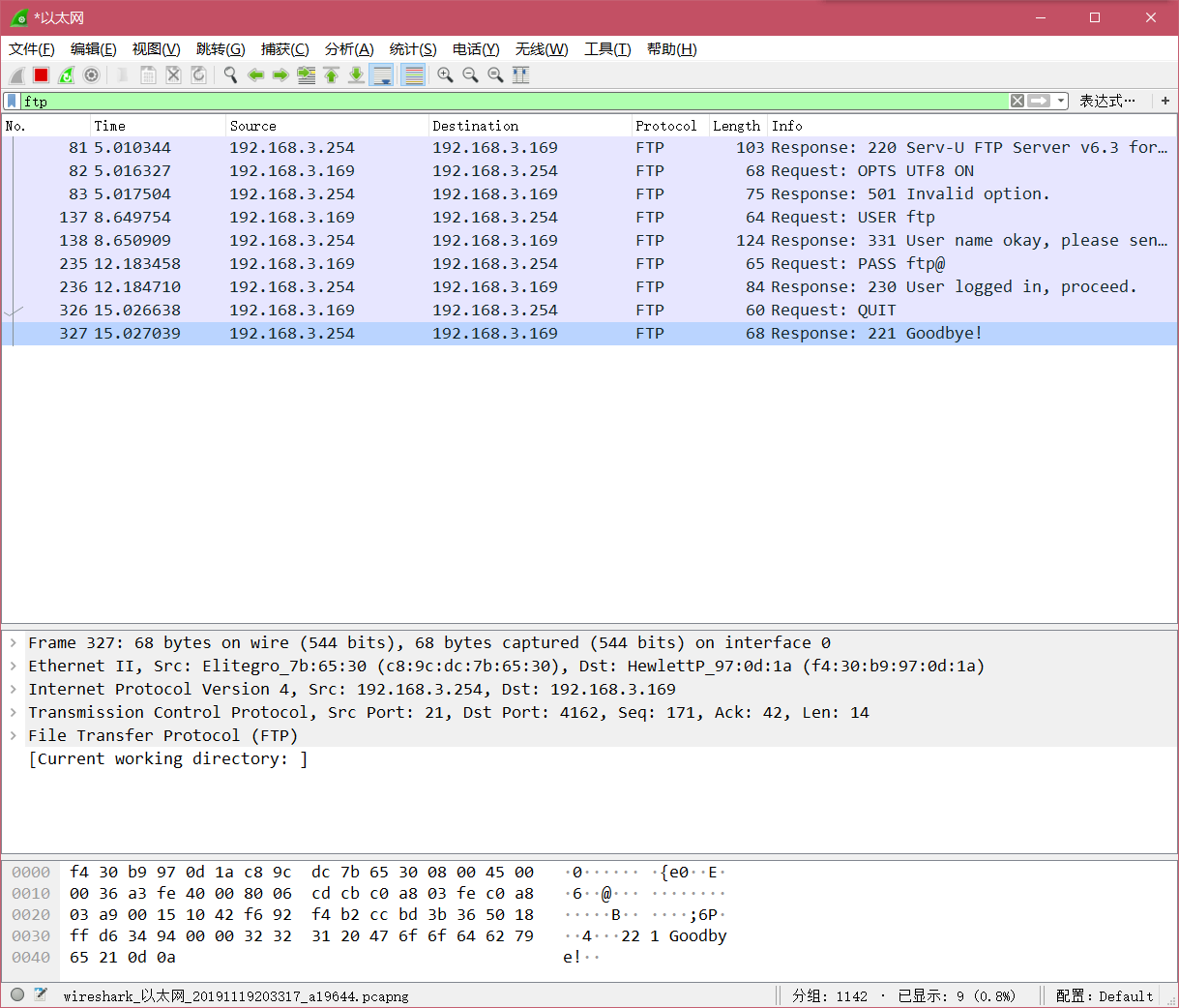
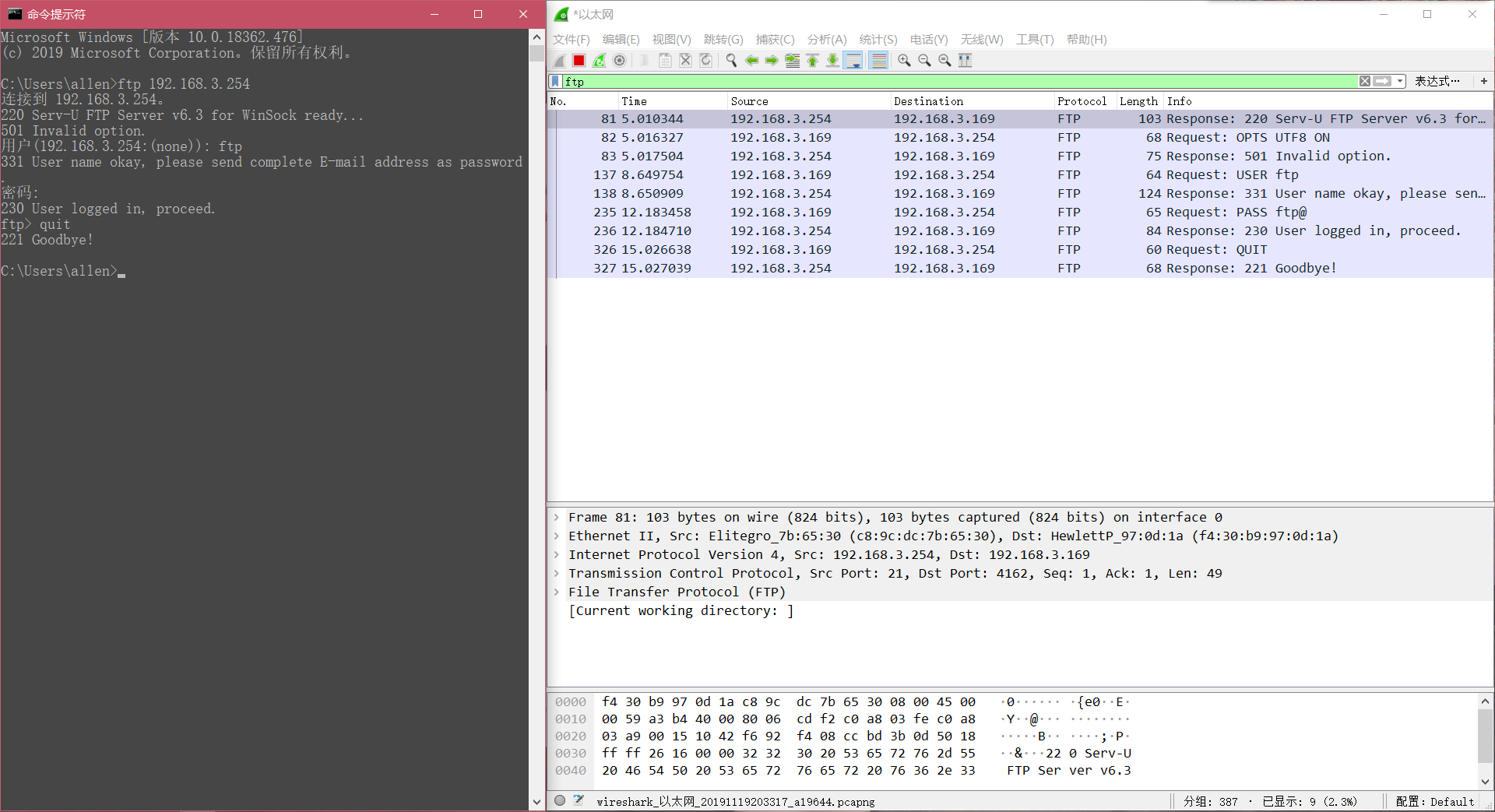


-h：

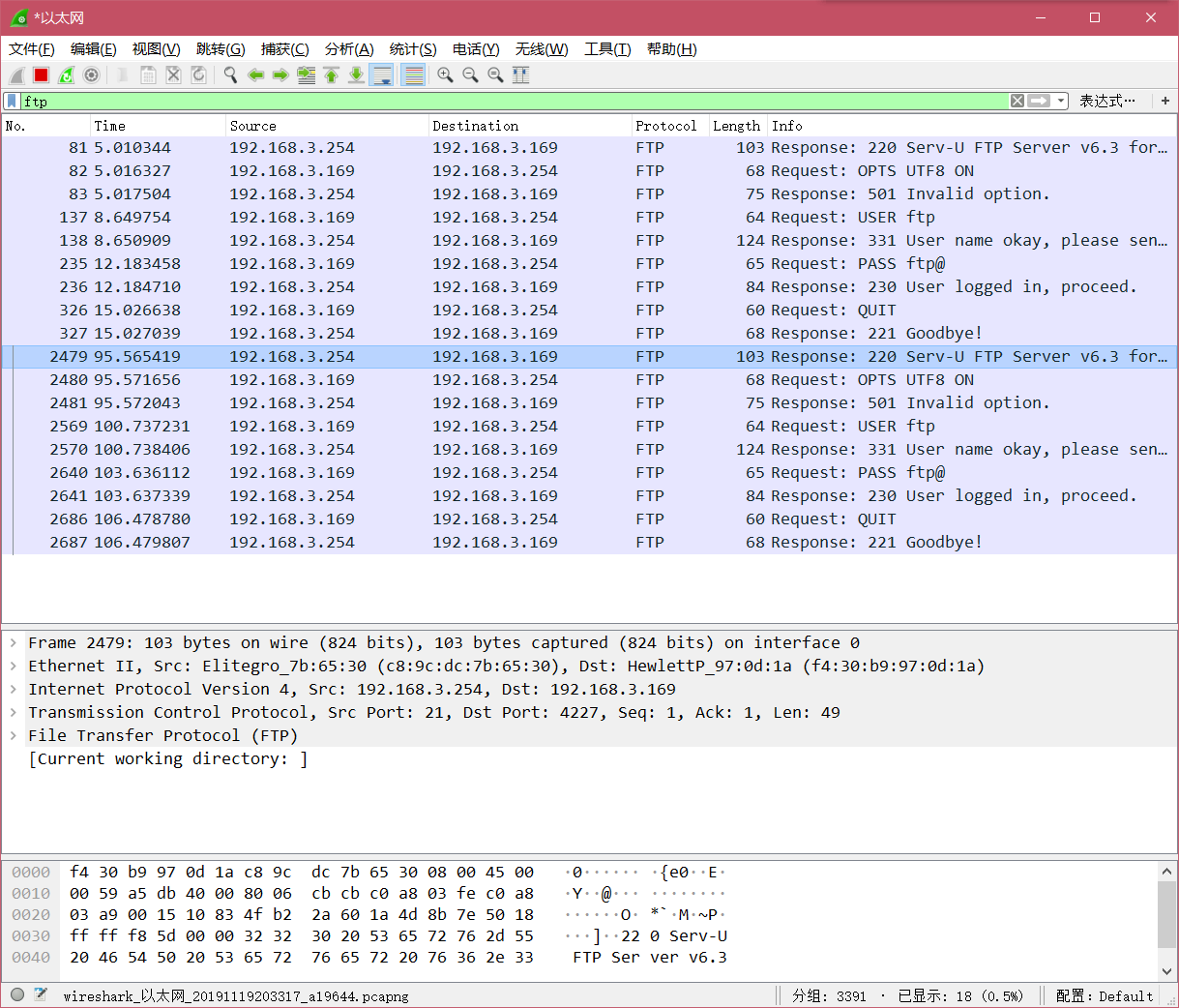
 

**（三）TCP连接实验**

第一次：



第二次：



**八、实验结论、心得体会**

**（一）地址解析协议（ARP）实验**

1. 计算机在通信过程中，什么情况下要发送ARP请求分组？什么情况下不发送ARP请求分组？

当 目的IP（若向子网外的主机发送，则为网关IP，或下一跳设备的IP）的MAC地址在ARP缓存表里没有时，则需要发送ARP请求分组查询该IP对应的MAC地址。但是ARP只能用来查询同一子网中的IP对应的MAC地址。

1. 如果步骤4或步骤6中显示A主机或B主机上有多余一条的ARP映射表项，请根据实验中的数据报文捕获结果，解释为什么会获得这些ARP映射表项？

没有显示

1. 请分析本实验中关于Sniffer软件捕获条件的设置问题：
2. Address Type捕获条件是否能设置成为***IP***？为什么？

不能，arp包无ip协议

1. 如果Station2的地址设置成为对方主机的地址，对实验的捕获操作会有什么影响？

会少结果

1. 如果Station1和Station2的地址均设置成为***any***，对实验的捕获操作会有什么影响？

会有大量干扰项

**（二）网络路径跟踪（TRACE）实验**

1. TRACE的功能是什么？有哪些可能的响应？产生这些响应的原因是什么？

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

1. 分析步骤3中捕获的TRACE报文，阐述TRACE的工作原理。

向目标发送不同 IP 生存时间 (TTL) 值的“Internet 控制消息协议 (ICMP)”回应数据包,Tracert诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时,路由器应该将“ICMP 已超时”的消息发回源系统。 Tracert 先发送 TTL 为 1 的回应数据包,并随后的每次发送过程将 TTL 递增 1,直到目标响应或 TTL 达到最大值,从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包,这在 Tracert 实用程序中看不到。 Tracert 命令按顺序打印出返回“ICMP 已超时”消息的路径中的近端路由器

**（3）TCP连接实验**

1. 一条TCP连接需要用哪些参数来标识？实验步骤2和实验步骤5中的TCP连接是否是同一条连接？请根据实验记录分别写出其连接标识。

seq，ack

不是

seq=1,ack=1

1. 本实验中用来建立TCP连接的3个TCP报文段的详细作用分别是什么？每个报文段中包含了哪些用于连接建立的信息？

确认tcp链接、要求用户名、要求密码

Response、request、src port、src dst、seq、ack

1. 利用步骤3中保存的捕获数据，画出主机与FTP服务器之间的TCP连接建立过程和TCP连接终止过程的时序交互图，并在图中注明每个TCP报文段的类型、序号和确认号。

**九、对本实验过程及方法、手段的改进建议**

无

**报告评分：**

**指导教师签字：**