学生实验实习报告册

学年学期：2018-2019 学年 □春☑秋学期

课程名称：计算机网络

学生学院：软件工程学院

专业班级：13001603班

学生学号：2016214052

学生姓名：姜文泽

联系电话：17783101834

重庆邮电大学教务处制

实验一：802.3 协议分析和以太网

一、实验目的

1. 分析 802.3 协议；
2. 熟悉以太网帧的格式；
3. 熟悉 ARP 报文的格式。

二、实验内容

通过练习使用分组分析器 Wireshark 来分析协议。

Wireshark 是一种可以运行在 Windows, UNIX, Linux 等操作系统上的分组分析器。Wireshark 的界面主要有五个组成部分：

（1） 命令菜单（command menus）：命令菜单位于窗口的最顶部，是标准的下拉式菜单。最常用菜单命令有两个：File、Capture。File 菜单允许你保存捕获的分组数据或打开一个已被保存的捕获分组数据文件或退出 Wireshark 程序。Capture 菜单允许你开始捕获分组。

（2） 捕获分组列表（listing of captured packets）：按行显示已被捕获的分组内容，其中包括：Wireshark 赋予的分组序号、捕获时间、分组的源地址和目的地址、协议类型、分组中所包含的协议说明信息。单击某一列的列名，可以使分组按指定列进行排序。在该列表中，所显示的协议类型是发送或接收分组的最高层协议的类型。

（3） 分组头部明细（details of selected packet header）：显示捕获分组列表窗口中被选中分组的头部详细信息。包括：与以太网帧有关的信息，与包含在该分组中的 IP 数据报有关的信息。单击以太网帧或 IP 数据报所在行左边的向右或向下的箭头可以展开或最小化相关信息。另外，如果利用 TCP 或 UDP 承载分组，Wireshark 也会显示 TCP 或 UDP 协议头部信息。最后，分组最高层协议的头部字段也会显示在此窗口中。

（4） 分组内容窗口（packet content）：以 ASCII 码和十六进制两种格式显示被捕获帧的完整内容。

（5） 显示筛选规则（display filter specification）：在该字段中，可以填写协议的名称或其他信息，根据此内容可以对分组列表窗口中的分组进行过

滤。

三、实验环境

操作系统：Windows 10 专业版 1803

工具软件：Wireshark 2.6.4

浏览器软件：Google Chrome

网络环境：

以太网适配器 以太网:

连接特定的 DNS 后缀 . . . . . : cqupt.edu.cn

本地链接 IPv6 地址. . . . . : fe80::2c7f:943c:931b:d417%22

IPv4 地址 . . . . . : 172.18.109.83

子网掩码 . . . . . : 255.255.252.0

默认网关. . . . . : 172.18.108.1

PPP 适配器 Netkeeper:

连接特定的 DNS 后缀 . . . . . :

IPv4 地址 . . . . . : 113.251.216.160

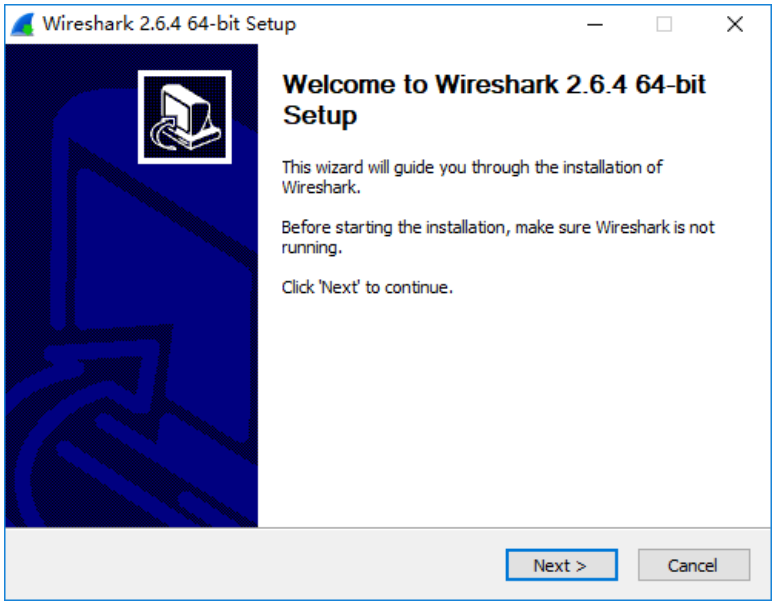
子网掩码 . . . . . : 255.255.255.255

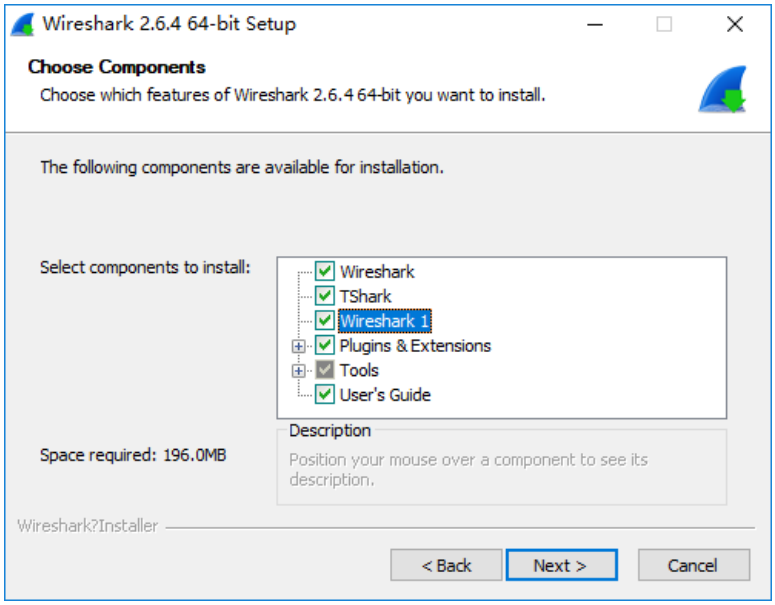
默认网关. . . . . : 0.0.0.0

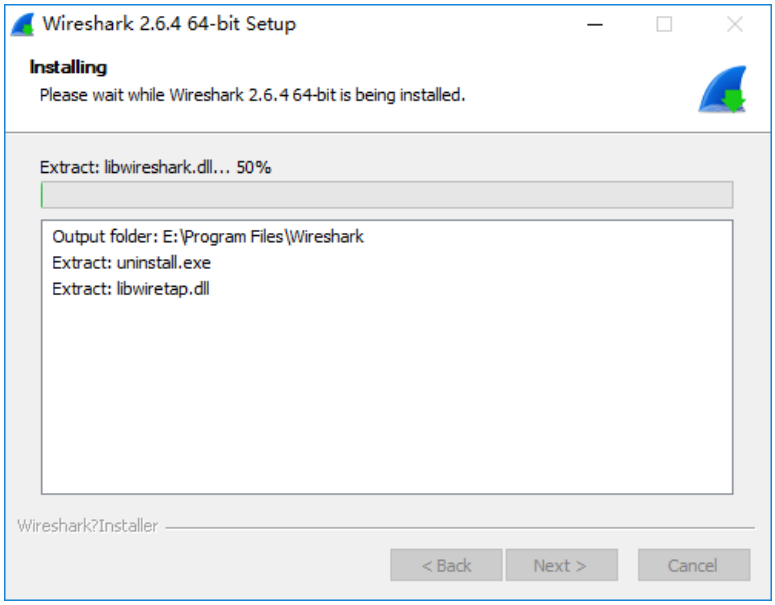
四、实验步骤

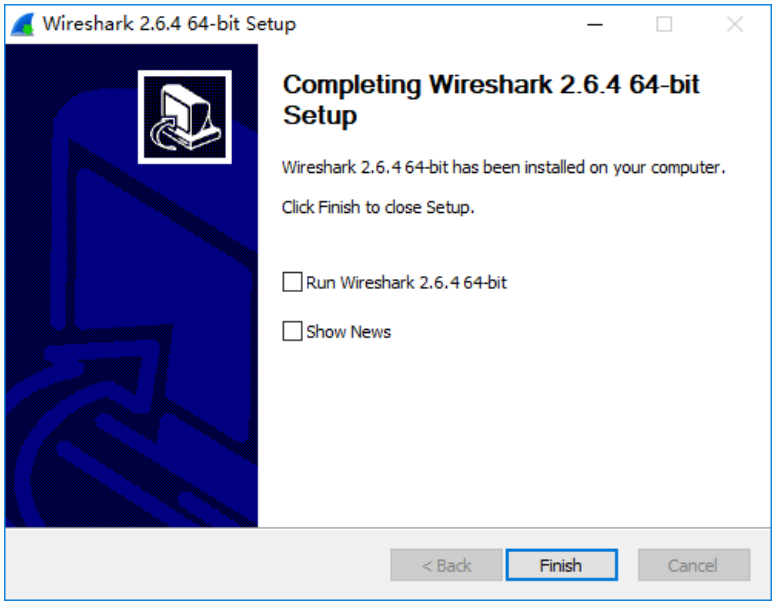
1. 安装 Wireshark

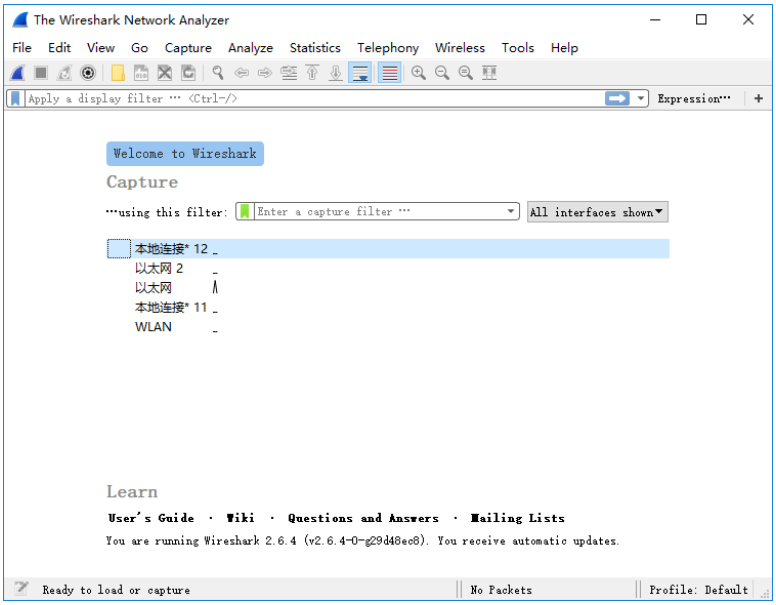
本次实验 Wireshark 使用的是 2.6.4 英文版本。安装过程及软件开始界面如下：




Wireshark 2.6.4 64-bit Setup
Choose Components
Choose which features of Wireshark 2.6.4 64-bit you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
Wireshark 1
Plugins & Extensions
Tools
User's Guide
Description
Position your mouse over a component to see its description.
Space required: 196.0MB
Wireshark?Installer
< Back
Next >
Cancel

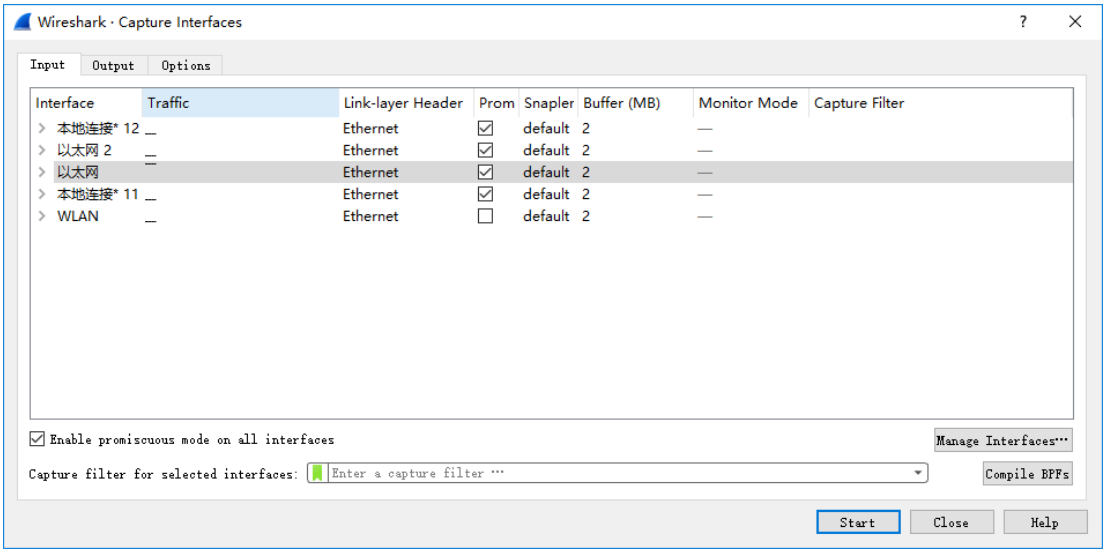

Wireshark 2.6.4 64-bit Setup
Installing
Please wait while Wireshark 2.6.4 64-bit is being installed.
Extract: libwireshark.dll... 50%
Output folder: E:\Program Files\Wireshark
Extract: uninstall.exe
Extract: libwiretap.dll
Wireshark?Installer
< Back
Next >
Cancel


Wireshark 2.6.4 64-bit Setup
Completing Wireshark 2.6.4 64-bit Setup
Wireshark 2.6.4 64-bit has been installed on your computer.
Click Finish to close Setup.
Run Wireshark 2.6.4 64-bit
Show News
< Back
Finish
Cancel



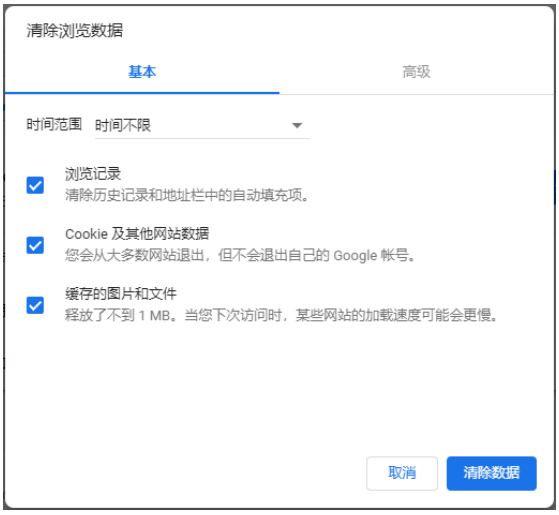
2. 使用 Wireshark

启动界面后，点击命令菜单中的“Options”命令，可进行分组捕获设置。设置完成后即可点击 Start 开始进行分组捕获。



3. 使用 Wireshark 捕获并分析以太帧

（1） 清空浏览器缓存（在 IE 窗口中，选择“工具/Internet 选项/删除文件”命令）；

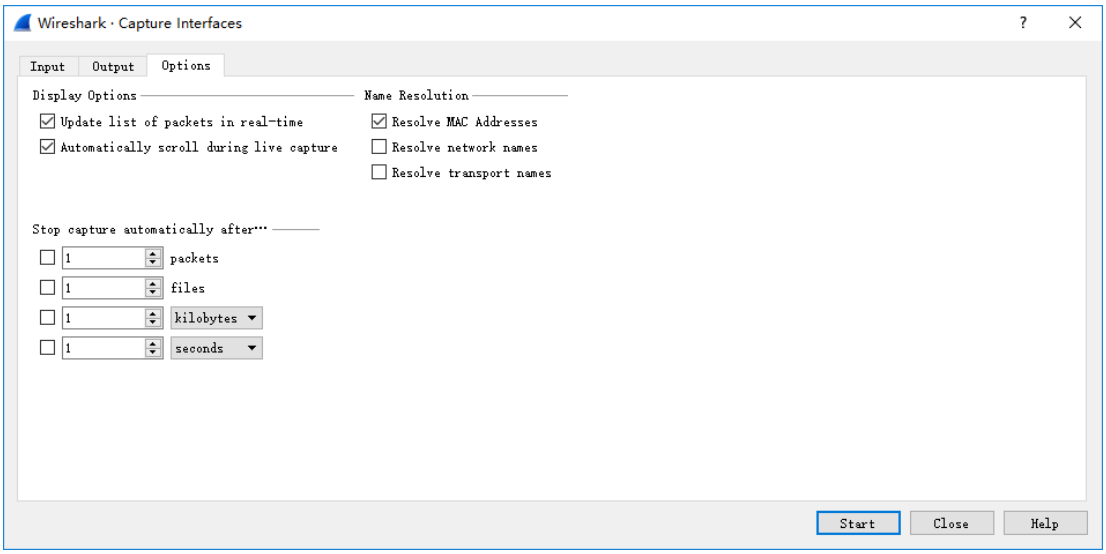


（2） 启动 Wireshark，开始分组捕获；

（3） 启动主机上的 web 浏览器。

（4） 启动 Wireshark。窗口中没有任何分组列表。

（5） 开始分组捕获：选择“capture”下拉菜单中的“Options”命令，会出现如图所示的“Wireshark: Capture Options”窗口，可以设置分组捕获的选项。

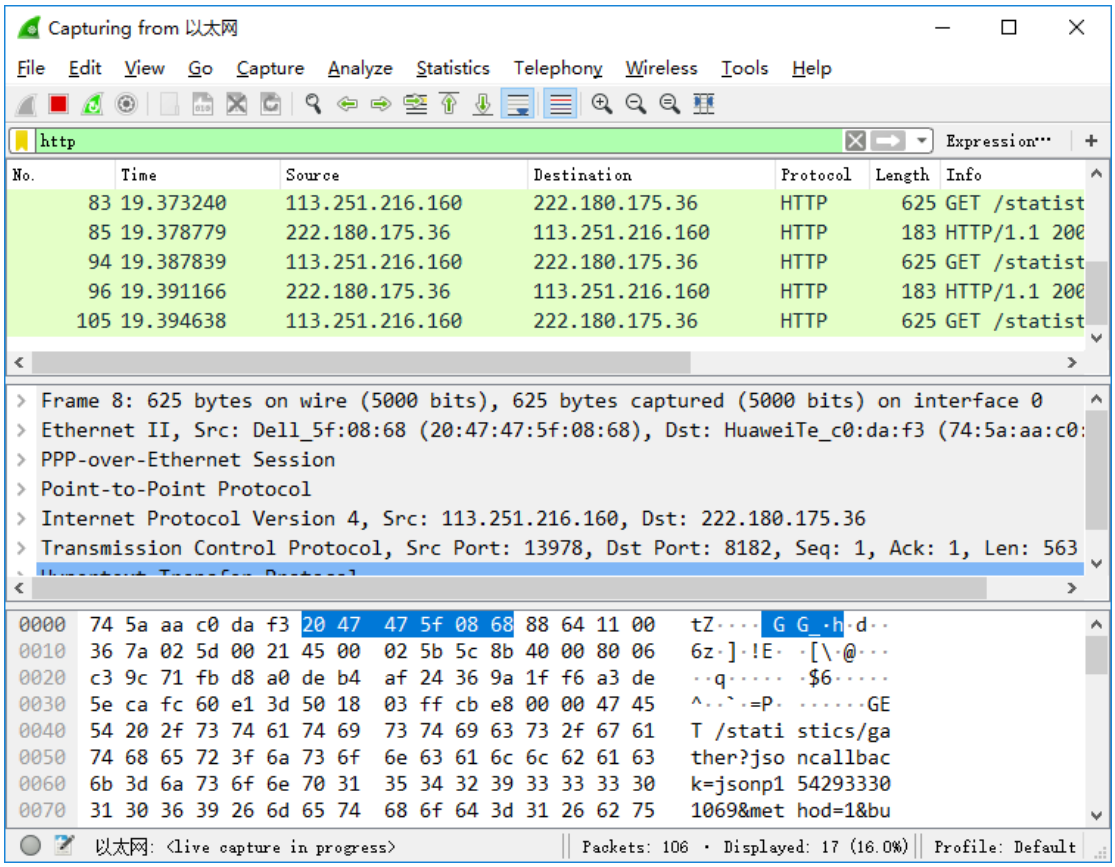


（6） 在实验中，可以使用窗口中显示的默认值。在“Wireshark: Capture Options”窗口的最上面有一个“interface”下拉菜单，其中显示计算机中所安装的网络接口（即网卡）。当计算机具有多个活动网卡（装有多块网卡，并且均正常工作）时，需要选择其 中一个用来发送或接收分组的网络接口（如某个有线接口）。

（7） 随后，单击“Start”开始进行分组捕获，所有由选定网卡发送和接收的分组都将被捕获。

（8） 开始分组捕获后，会出现分组捕获统计窗口。该窗口统计显示各类已捕获分组的数量。在该窗口中有一个“stop”按钮，可以停止分组的捕获。

（9） 在运行分组捕获的同时，在浏览器地址栏中输入某网页的 URL，如：www.baidu.com。为显示该网页，浏览器需要连接 www.baidu.com 的服务器，并与之交换 HTTP 消息，以下载该网页。包含这些 HTTP 消息的以太网帧(Frame)将被 Wireshark 捕获。



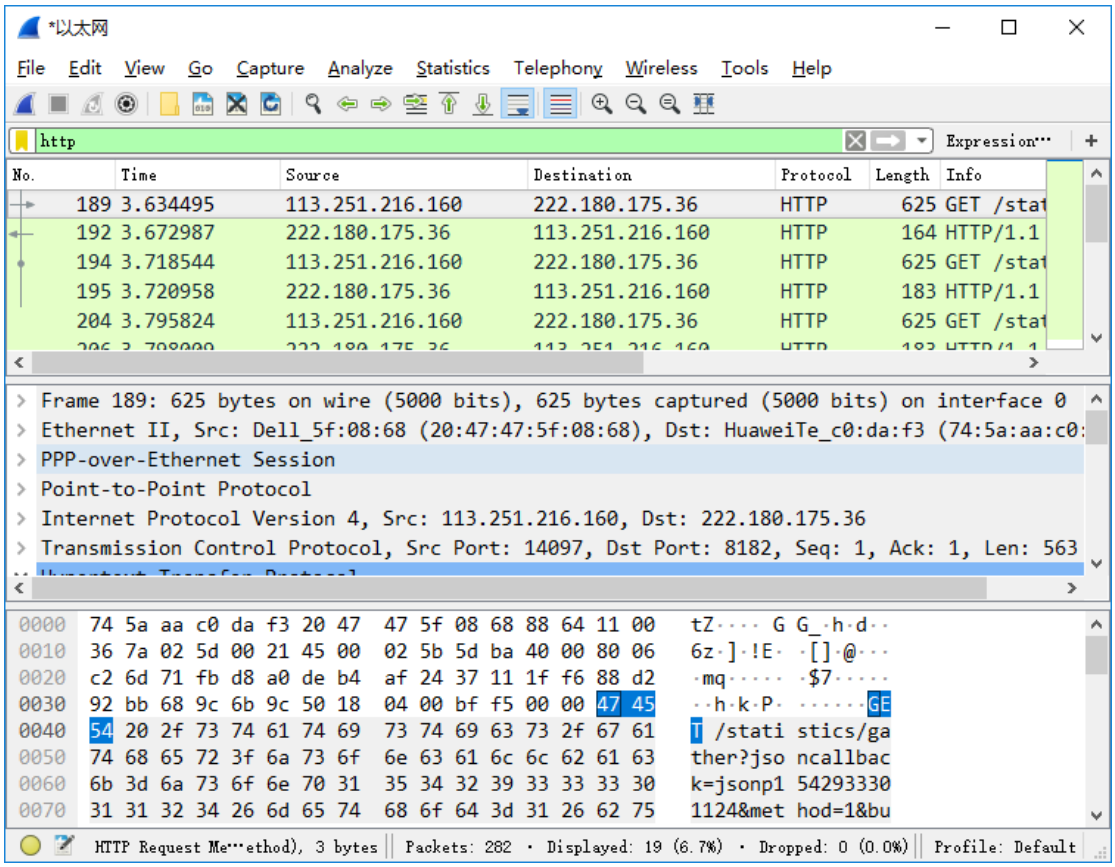
（10） Wireshark 主窗口显示已捕获的你的计算机与其他网络实体交换的所有协议报文，其中一部分就是与 www.baidu.com 服务器交换的 HTTP 消息。

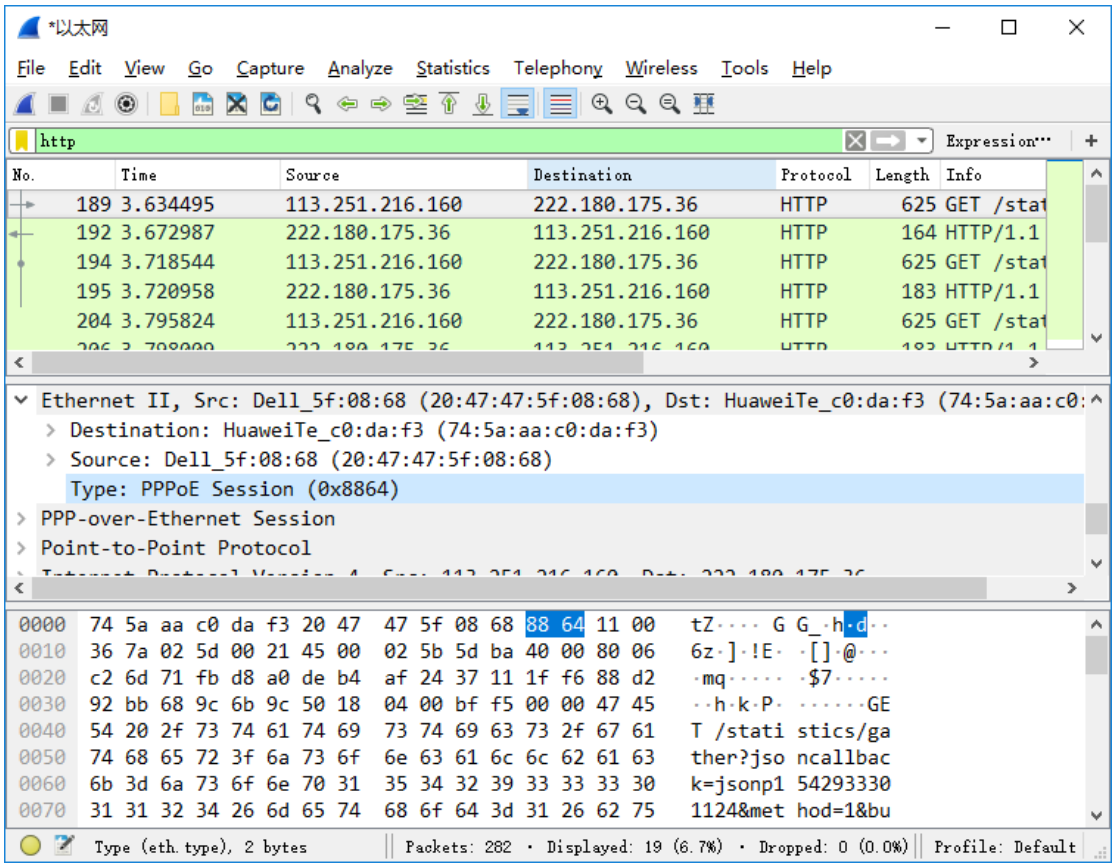
（11） 在显示筛选编辑框中输入“http”，单击“apply”，分组列表窗口将只显示 HTTP 消息。

（12） 选择分组列表窗口中的第一条 HTTP 消息。它应该是你的计算机发向 www.baidu.com 服务器的 HTTP GET（HTTP 定义的用于获取/查询资源信息的方法）消息。

（13） 选择“Analyze->Enabled Protocols”，取消对 IP 复选框的选择，单击 OK。当你选择该消息后，以太网帧、IP 数据报、TCP 报文段、以及 HTTP 消息首部信息都将显示在分组首部子窗口中。单击分组首部详细信息子窗口中向右和向下箭头，可以最小化帧、以太网、IP、TCP 信息显示量，可以最大化 HTTP 协议相关信息的显示量。

（14） 选择包含 HTTP GET 消息的以太网帧，在分组详细信息窗口中，展开 Ethernet II 部分。根据操作，回答“五、实验报告内容”中的 1-4 题；

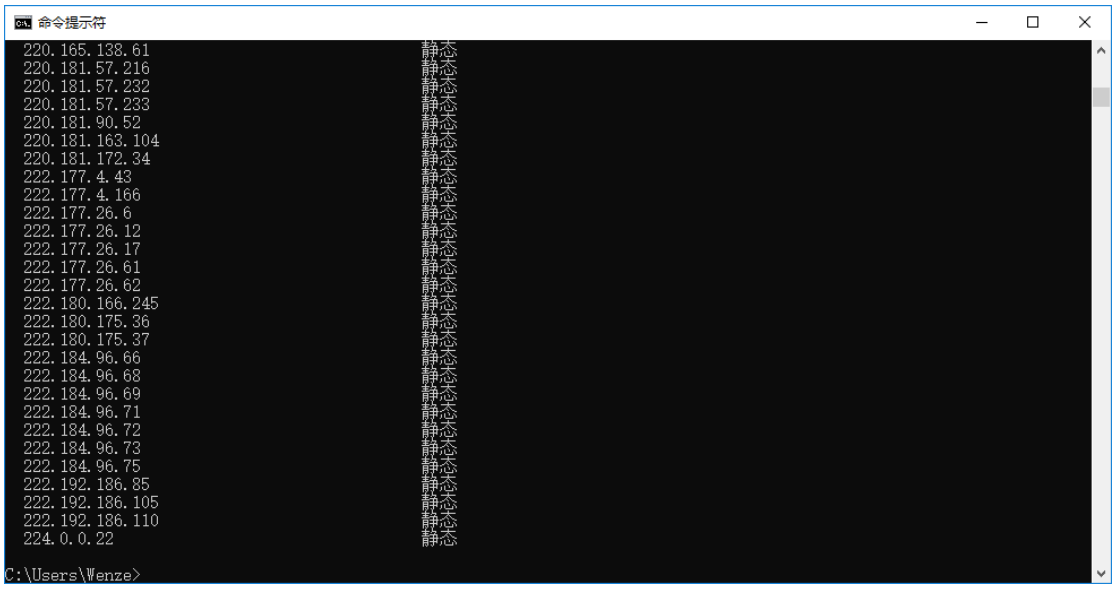




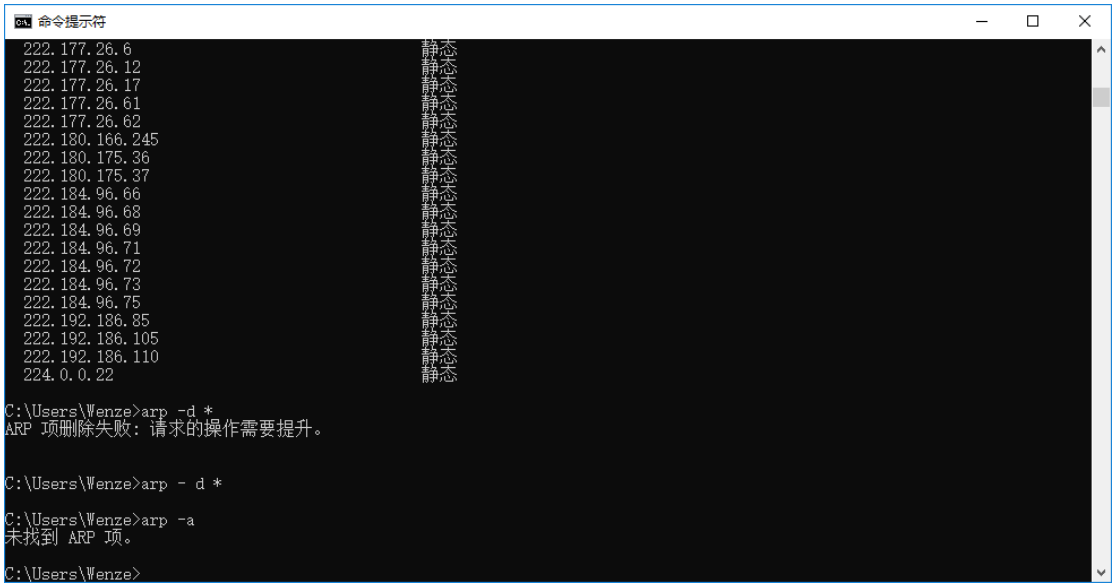
（15） 选择包含 HTTP 响应消息第一个字节的以太网帧。

4. 查看主机 ARP 缓存

（1） 利用 MS-DOS 命令：arp -a 查看主机上 ARP 缓存的内容。



（2） 利用 MS-DOS 命令：arp -d * 以清除主机中 ARP 缓存的内容。



5. 实验结果

（1） 你的主机的 48 位以太网地址(MAC 地址)是多少？

20-47-47-5F-08-68

（2） 目标 MAC 地址是 www.baidu.com 服务器的 MAC 地址吗？如果不是，该地址是什么设备的 MAC 地址？

该地址是连接该服务器的路由器的 MAC 地址（HuaweiTe_c0:da:f3 (74:5a:aa:c0:da:f3)）

（3） 给出 Frame 头部 Type 字段(2 字节)的十六进制值。

0x8864

（4） 在包含“HTTP GET”的以太网帧中，字符“G”的位置(是第几个字节，假设 Frame 头部第一个字节的顺序为 1)？

3F（16 进制） 63（10 进制）

五、实验结论

收获 1. 在 Wireshark 的抓包细节中,具体字节排序序号是以 16 进制来显示的。如下图所示。

问题 1. arp -d * 删除时报错 ARP 项删除失败: 请求的操作需要提升？

解决 1. 可以使用命令为 arp - d *，也可使用管理员权限打开 cmd 进行执行。