**《计算机网络》**

**实验报告**

**题目： 实验二：HTTP协议**

**探索和分析**

**专业： 软 件 工 程**

**班级： 5班**

**学号： 201924100436**

**姓名： 宋 章 耀**

**郑州大学信息工程学院**

# 实验二：HTTP协议探索和分析

## 【实验目的】

1、熟悉HTTP协议的请求和响应格式；

2、掌握分析HTTP协议数据流的方法。

## 【实验步骤与结果记录】

**要求：根据实验指导书中的实验内容和步骤，认真完成实验。采取截图、拍照等形式记录自己的实验步骤和结果。（可根据需要加页）**

#### 步骤1:从主机上启动浏览器访问http://www.zzu.edu.cn,同时利用Wireshark软件抓包,保存抓包结果并分析。

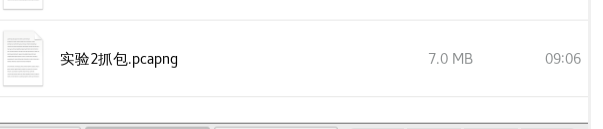
1. 在 Vmware中的Linux主机上启动 Wireshark软件，选择连接互联网的网络接口,启动抓包



1. 在Linux主机上打开浏览器,访问http://www.zzu.edu.cn，等待网页完全显示出来后关闭浏览器

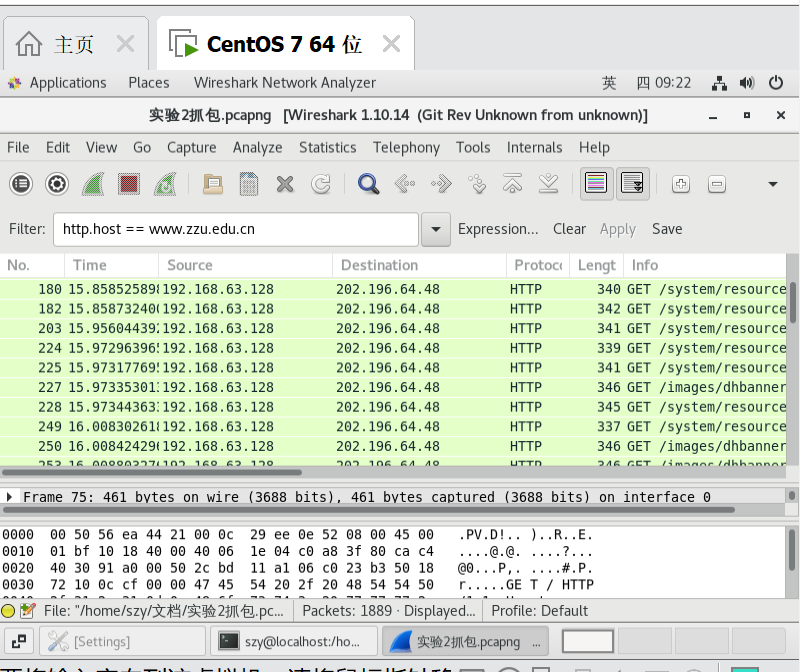


1. 在 Wireshark中停止抓包，并保存抓包结果文件



#### **步骤2:从抓包结果中,过滤出浏览器和Web服务器之间的通信,分析HTTP协议的请求和响应格式。**

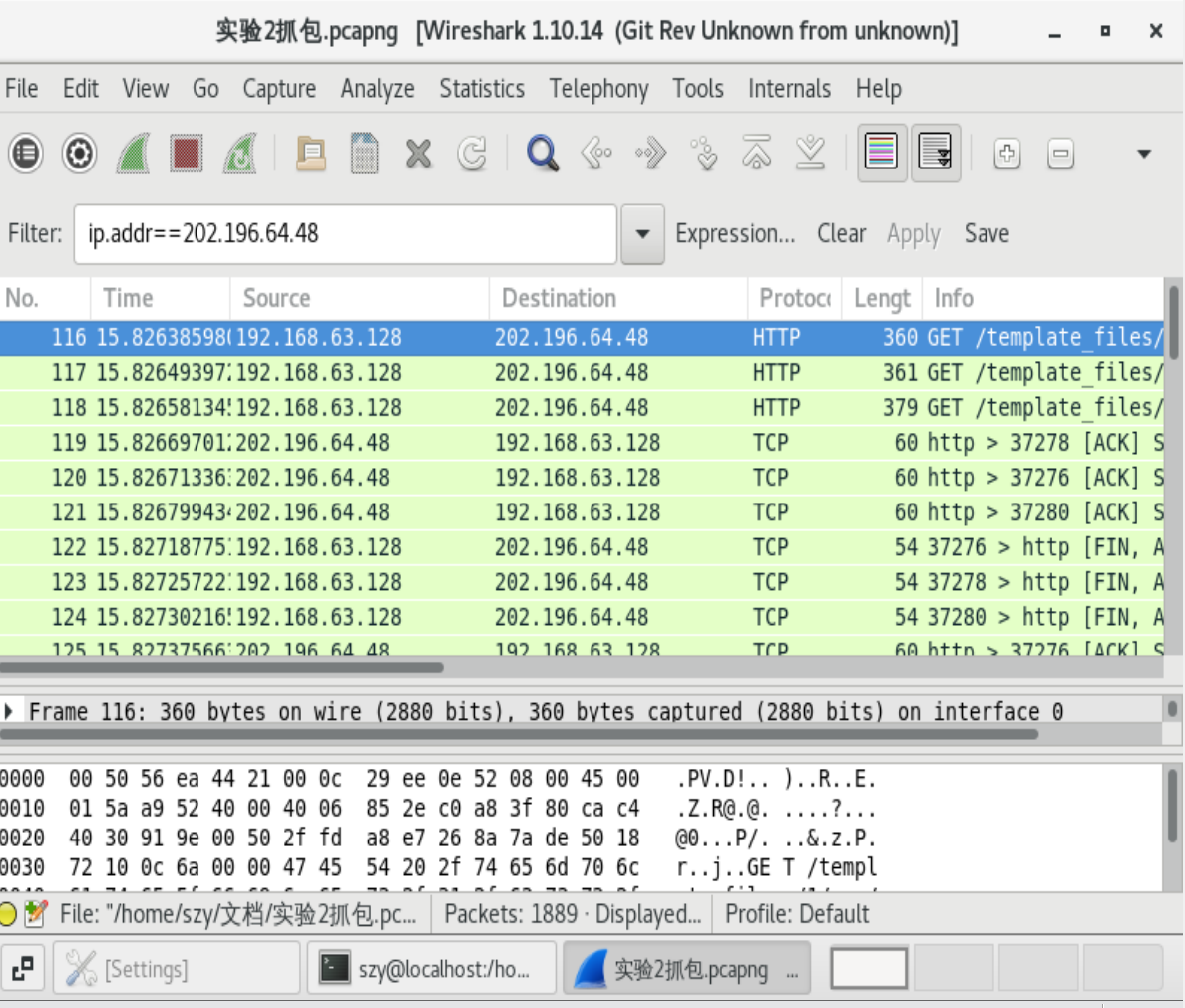
1. 在Wireshark软件的显示过滤器中输入httphost==www.zzu.edu.cn。使Wireshark仅显示HTTP协议报文中包含首部行“Host:www.zzu.edu.cn”的报文,从中分析出服务器www.zzu.edu.cn的IP地址,记作IP\_zzu



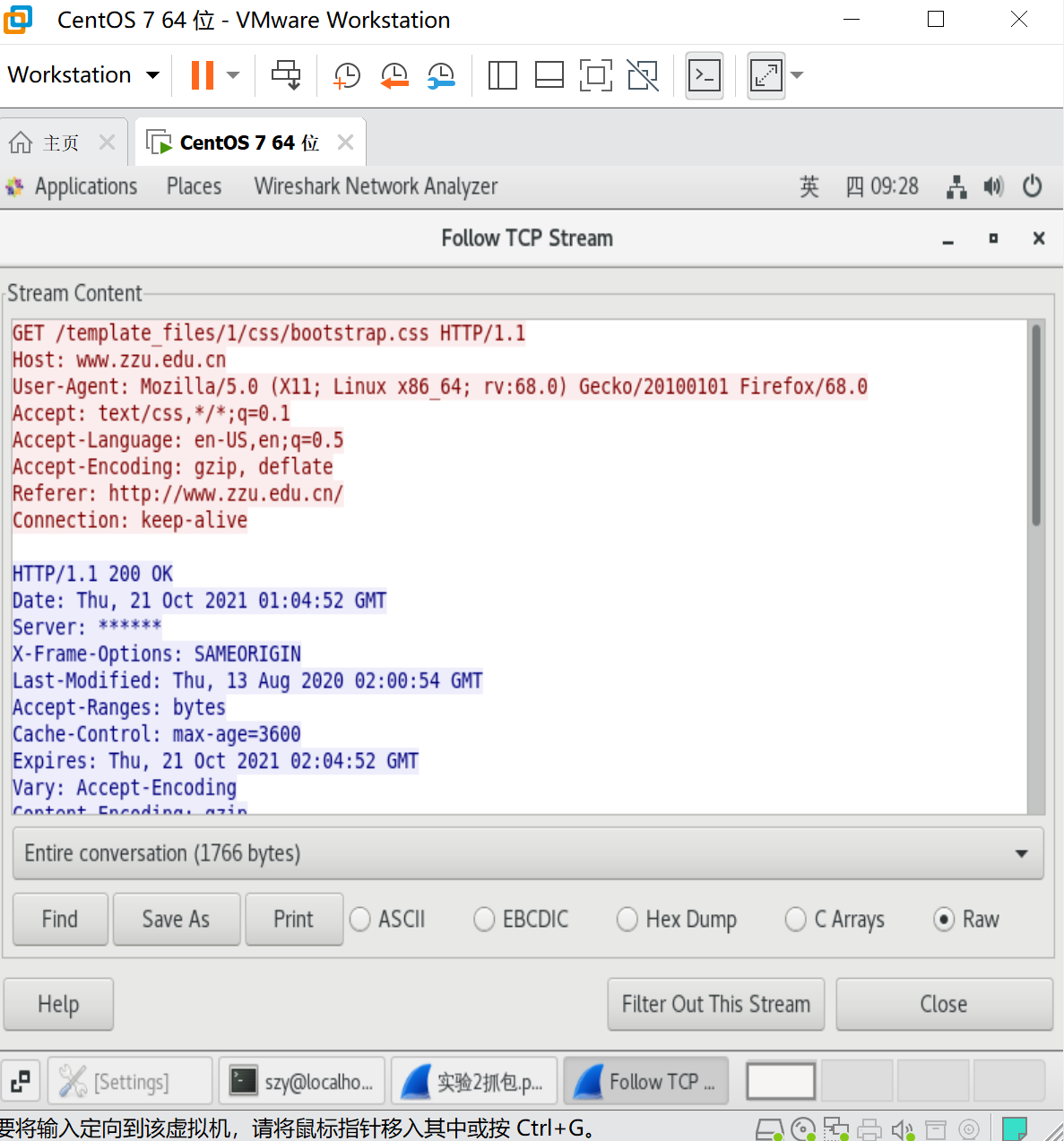
IP\_zzu=202.196.64.48

1. 在 Wireshark软件的显示过滤器中输入“ip.addr=IP\_zzu”,使 Wireshark

显示Web服务器参与的所有通信数据

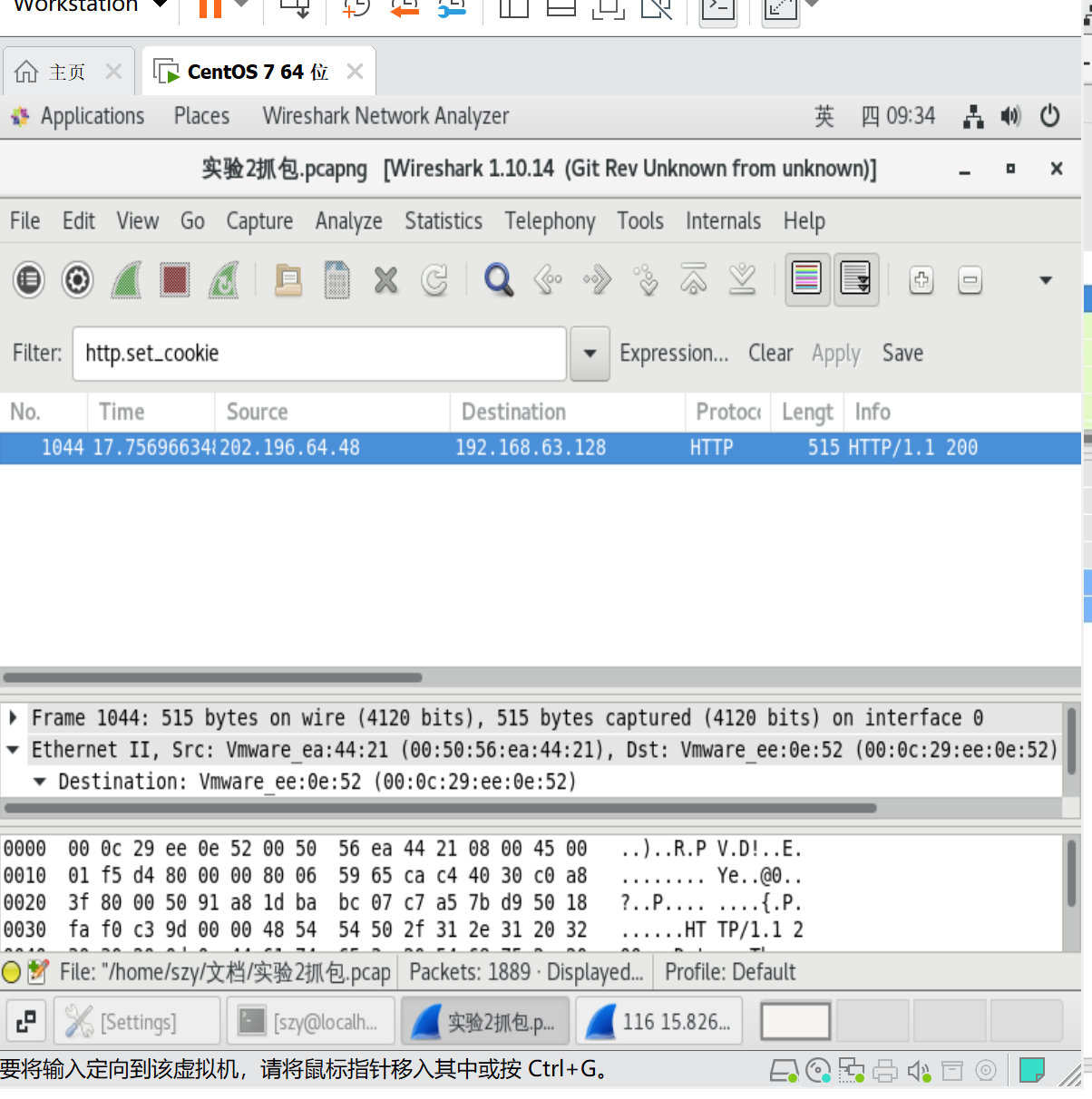


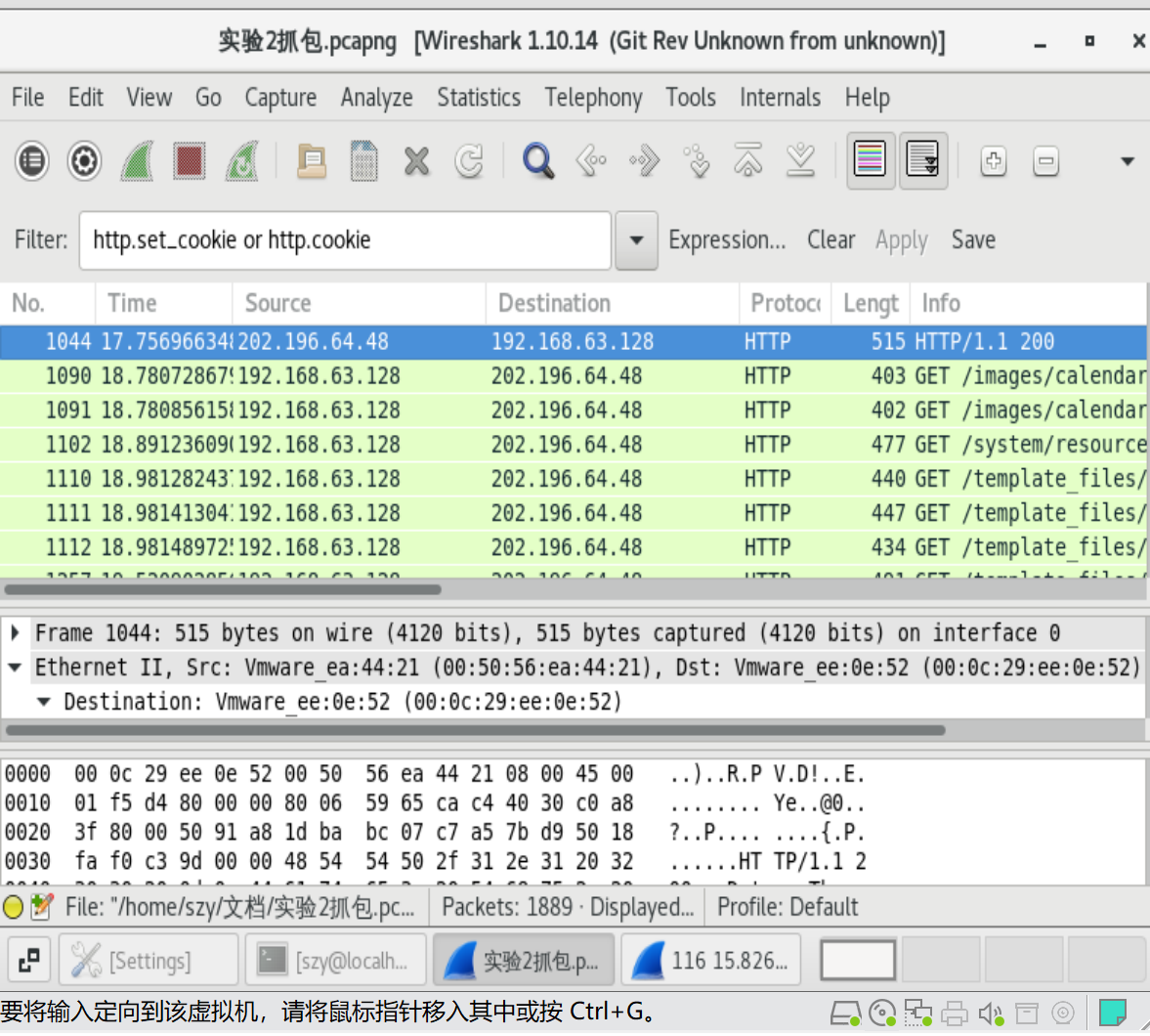
1. 任意选择一个HTTP报文,点击Analyze菜单→Followtcpstream子菜单.跟踪TCP流，选择其中仼意一对HTTP请求和响应,分析HTTP请求和响应的格式



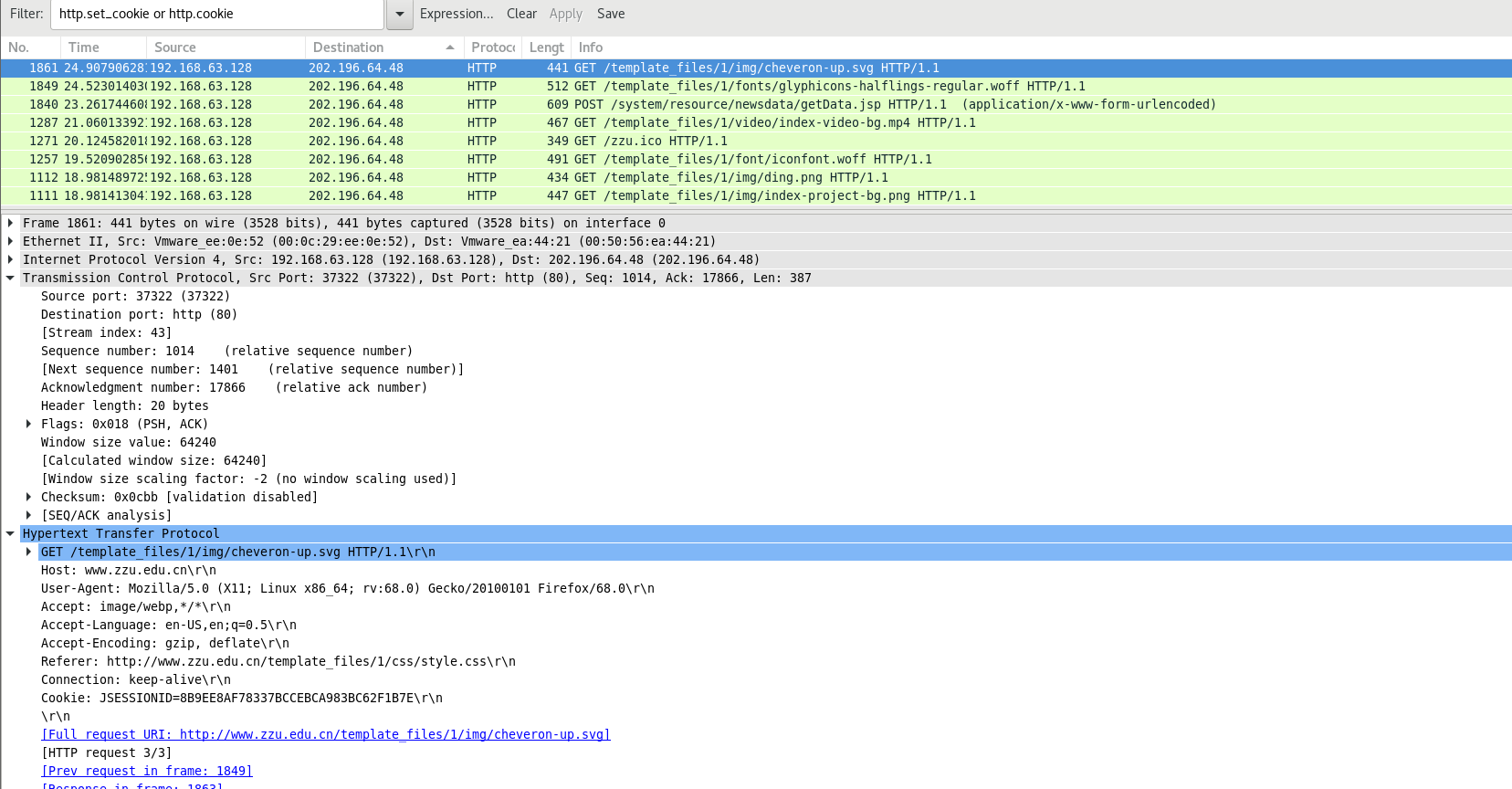
#### **步骤3:从抓包结果中,分析 cookie的格式,理解 cookie的作用**

1. 在Wireshark软件的显示过滤器中输入http.set-cookie OR http.cookie。使Wireshark显示包含set-cookie的HTTP响应和包含cookie的HTP请求，分析cookie的格式和作用





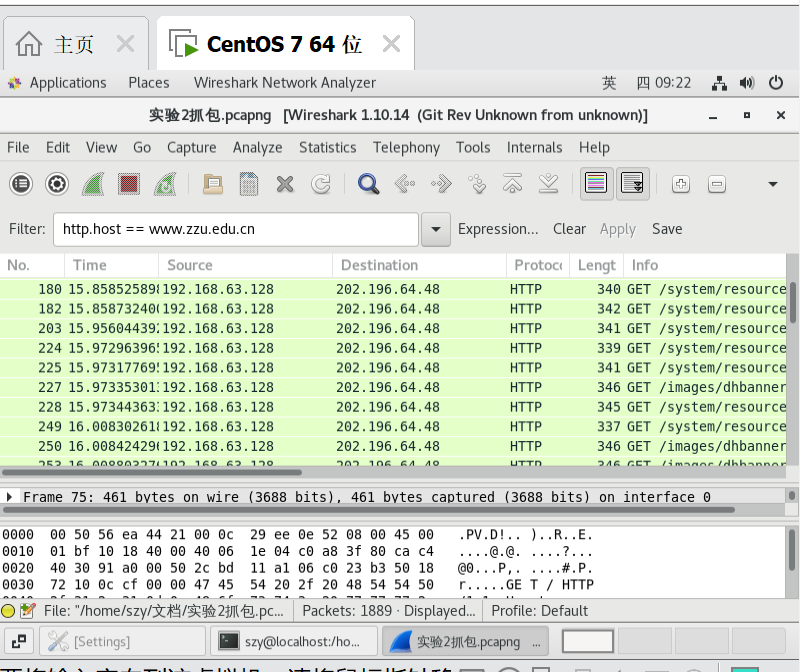
1个setcookie





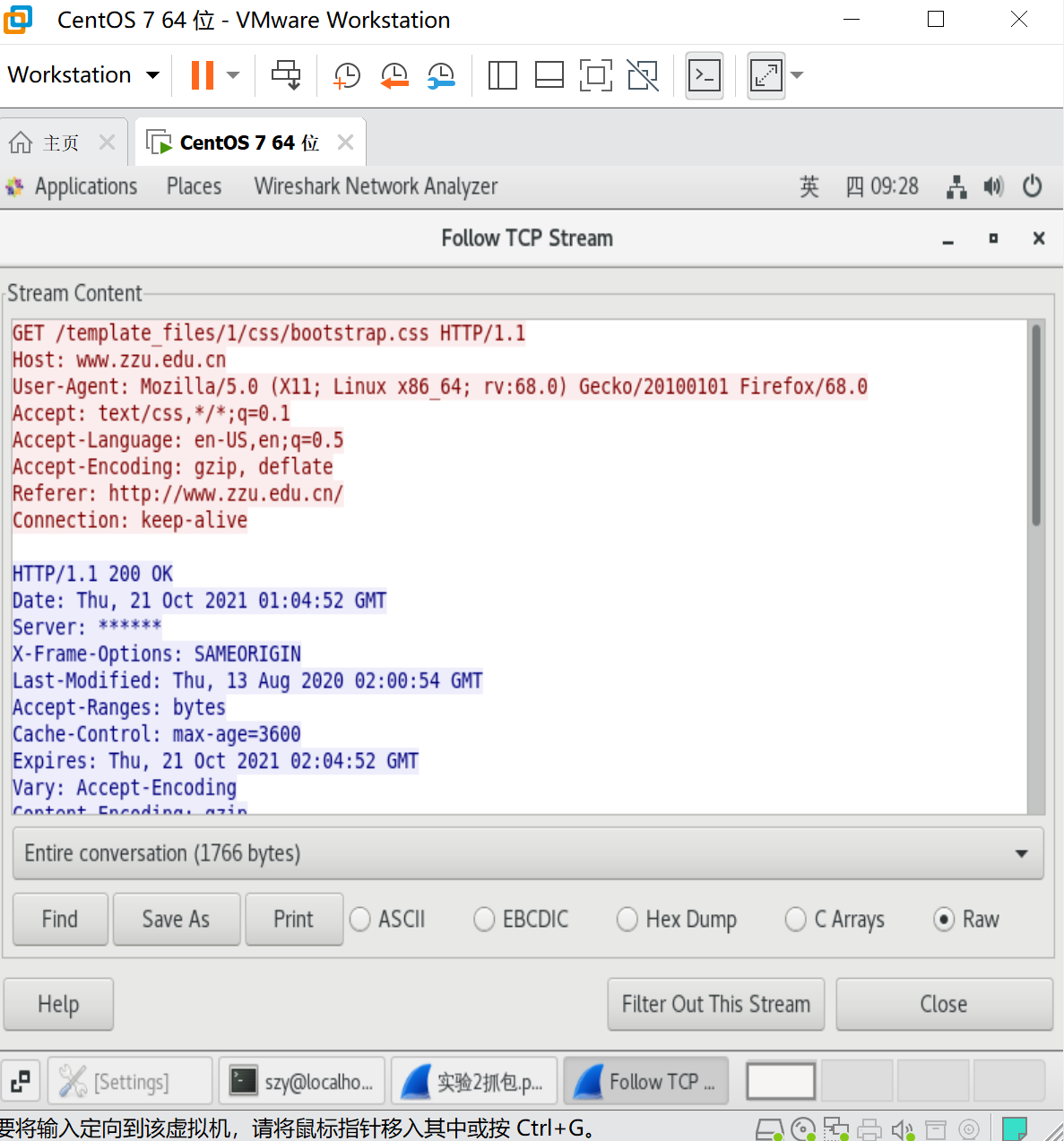
## 【问题与分析】

1、从你的抓包结果中分析出的www.zzu.edu.cn的IP地址是什么？截图说明你的分析过程。



IP\_zzu=202.196.64.48

1. 在步骤2中，从你的抓包结果中，选出任意一对HTTP请求和响应，分析截获的数据，截图说明分析过程并填写表2.1和表2.2。



|  |  |
| --- | --- |
| 表2.1 HTTP请求中的数据 | |
| 请求方法： | Get |
| URL： | /system/resource/code/datainput.jsp?owner=1653154221&e=1&w=956&h=890&treeid=1001&refer=&pagename=L2luZGV4LmpzcA%3D%3D&newsid=-1 |
| 版本： | HTTP/1.1 |
| 是否采用持续连接： | 是 |
| 从本HTTP请求中，任选5个首部行，将其首部字段名和值填入以下5行中 | |
| Host | www.zzu.edu.cn |
| User-Agent | Mozilla/5.0 (X11; Linux x86\_64; rv:68.0) Gecko/20100101 Firefox/68.0 |
| Accept | image/webp,\*/\* |
| Accept-Lanuage | en-US,en;q=0.5 |
| Referer | http://www.zzu.edu.cn |

|  |  |
| --- | --- |
| 表2.2 HTTP请求中的数据 | |
| 版本： | HTTP/1.1 |
| 状态码： | 200 |
| 短语： | OK |
| 从本HTTP响应中，任选5个首部行，将其首部字段名和值填入以下5行中 | |
| Date | Thu,21 Oct2021 01:64:52 GMT |
| X-Frame-Options: | SAMEORIGIN |
| Cache-Control | no-store |
| Pragma | no-cache |
| Content-Type | image/gif;charset=UTF-8 |

3、在步骤3中，你一共截获了几个包含set-cookie首部行和cookie首部行的数据帧？其中，包含几个cookie？。这几个cookie的内容字段的值是什么？截图说明你的分析过程。

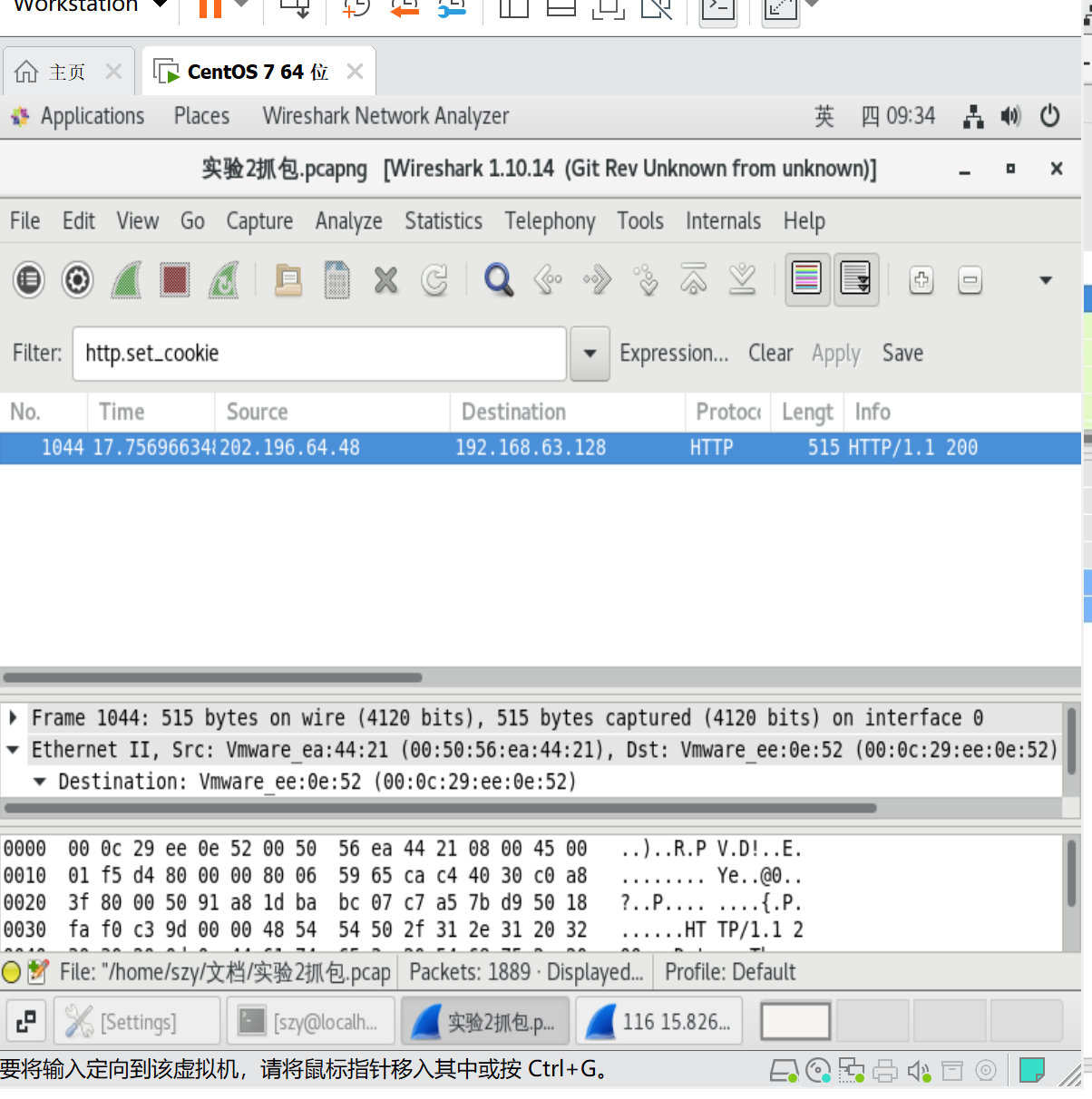
10个包含set-cookie首部行和cookie首部行的数据帧

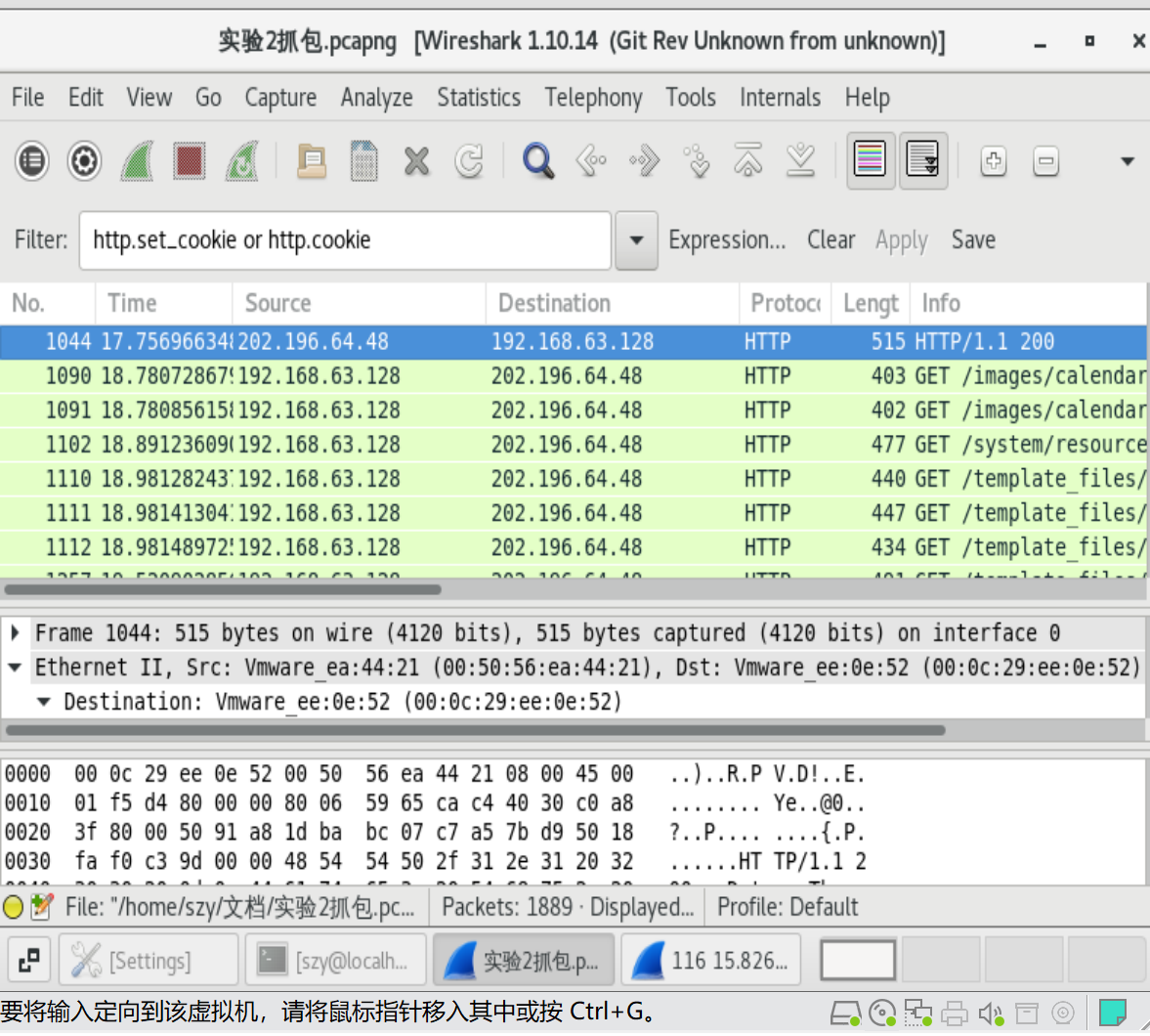
1个包含cookie



剩下的字段







1. 【选做】分析你截获的HTTP数据，浏览器与web服务器之间建立了几条TCP连接？为什么这样做？

三条

在建立TCP连接的过程中需要三次握手

第一次握手：浏览器发送请求数据包，SYN=1，序号x=1

第二次握手：服务器收到浏览器的报文，向浏览器发送一个SYN和ACK都置为1的TCP报文

第三次握手：浏览器收到服务器发来的包后检查确认后，再次发送确认包，服务器收到后确认建立成功。

建立TCP连接的过程中需要三次握手

第一次握手：浏览器发送请求数据包，SYN=1，序号x=1

第二次握手：服务器收到浏览器的报文，向浏览器发送一个SYN和ACK都置为1的TCP报文

第三次握手：浏览器收到服务器发来的包后检查确认后，再次发送确认包，服务器收到后确认建立成功。