

**实 验 报 告**

（2019 / 2020 学年 第 二 学期）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 课程名称 | 计算机网络 | | | | | |
| 实验名称 | 网络协议数据报捕获与分析实验 | | | | | |
| 实验时间 | 2020 | 年 | 6 | 月 | 10 | 日 |
| 指导单位 | 自动化学院、人工智能学院 | | | | | |
| 指导教师 | 范保杰 | | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 学生姓名 | 陈力 | 班级学号 | B17050322 |
| 学院(系) | 自动化、人工智能学院 | 专 业 | 自动化 |

网络协议数据包捕获与分析实验

一、实验目的

1. 了解网络协议数据包捕获软件的使用方法。

2. 加深对计算机网络结构以及数据封装方式。

二、实验环境

1. 软件环境：Microsoft Windows 操作系统，Wireshark网络协议分析软件。

2. 硬件环境：配置网卡的计算机，有网络连接。

三、实验步骤

1.下载wireshark网络数据捕获分析软件，安装该软件，安装完成后，运行该软件。

2.设置过滤器为icmp，捕获并分析icmp报文。

3. 开始捕获报文，选择捕获菜单下，开始选项。

4. 在CMD中使用ping命令，ping任意一个IP地址。

5. 选中捕获的数据包，分别：

1）对照书本中MAC帧的格式，查看数据包的MAC帧首部，如图2.3所示（抓包软件抓到的是去掉前导同步码、帧开始分界符、FCS之外的数据）。

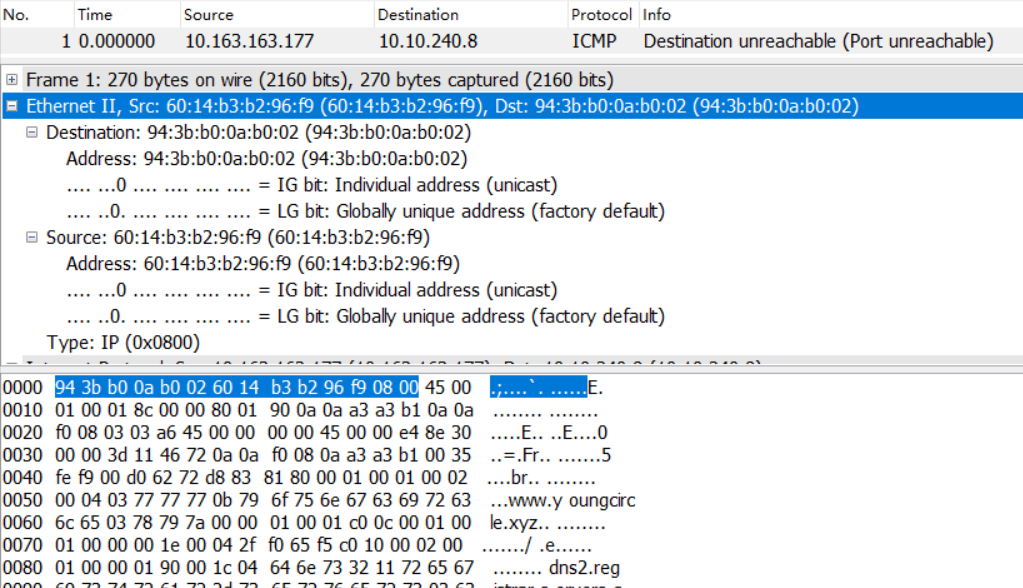


图2.1 MAC首部（蓝色部分）

**MAC帧首部组成**：

* 目的地址：94:3b:b0:0a:b0:02
* 源地址：60:14:b3:b2:96:f9
* 类型字段：0x0800

2） 对照课本IP数据报的格式，查看数据包的IP首部，如图2.4所示。

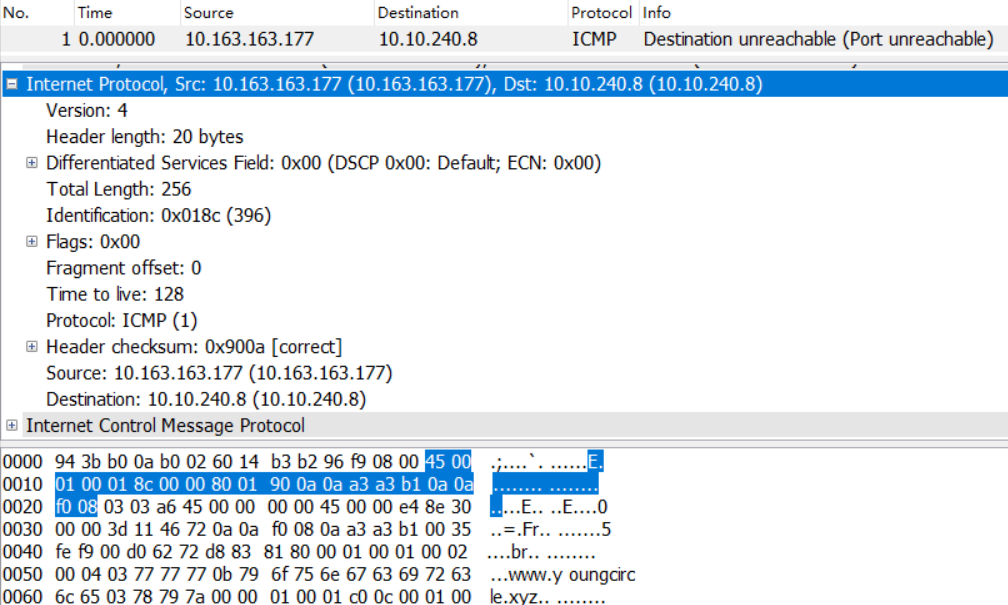


图2.2 IP首部（蓝色部分）

**IP数据报的首部**

* 版本：IPv4
* 首段长度：20bytes
* 区分服务：0x00
* 总长度：256
* 标识：0x018c (396)
* 片偏移：0x00
* 生存时间：128
* 协议：ICMP
* 首段检验和：0x900a[correct]

3）对照书上ICMP报文格式，查看ICMP报文内容。

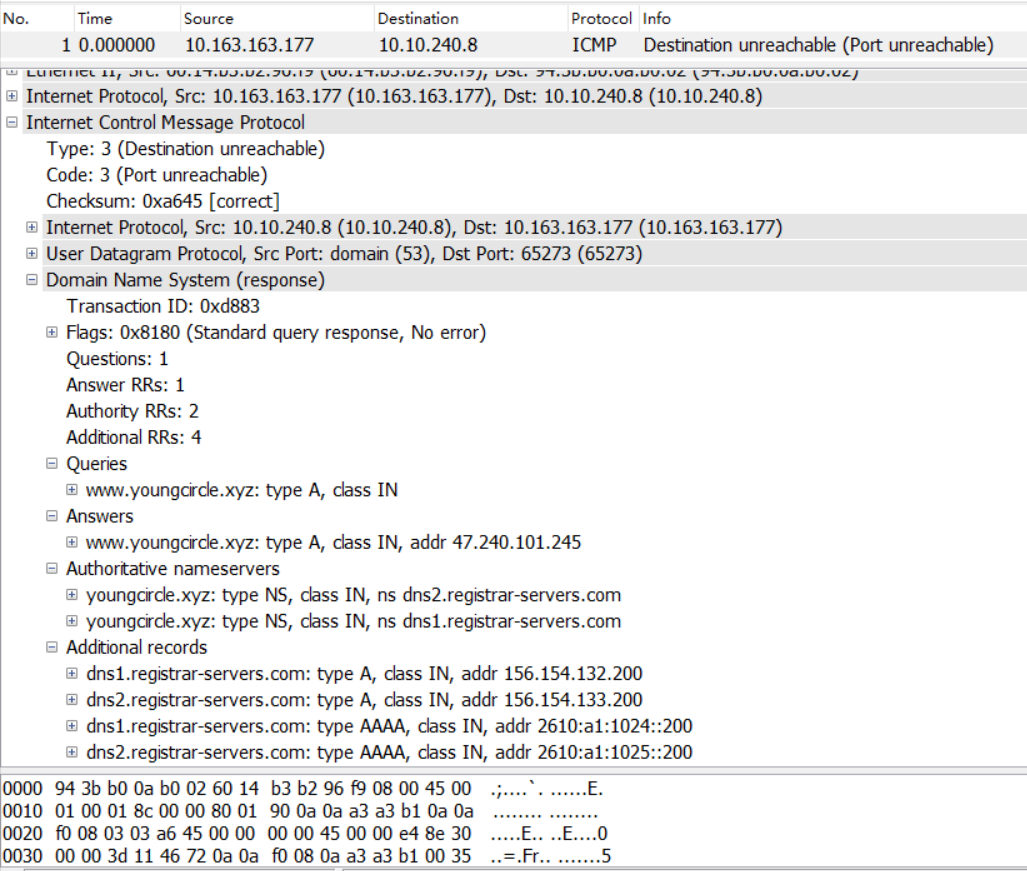


图2.3 ICMP报文

**ICMP报文首部：**

* 类型：3（Destination unreachable）
* 代码：3（Port unreachable）
* 检验和：0xa645[correct]

**ICMP的数据部分：**

* IP数据报首部:
* UDP：DNS的目的端口是65273
* DNS：
  + Transaction ID：标识字段，用于辨别DNS应答报文是哪个请求报文的响应
  + Flag：
  + Questions： 1
  + Answer RRs：1
  + Authority RRs：2
  + Additional RRs：4
  + Queries：
    - www.youngcircle.xyz: type A, class IN
  + Answers
    - www.youngcircle.xyz: type A, class IN
  + Authoritative nameservers：
    - youngcircle.xyz: type NS, class IN, ns dns2.registrar-servers.com
    - youngcircle.xyz: type NS, class IN, ns dns1.registrar-servers.com
  + Additional records：
    - dns1.registrar-servers.com: type A, class IN, addr 156.154.132.200
    - dns2.registrar-servers.com: type A, class IN, addr 156.154.133.200
    - dns1.registrar-servers.com: type AAAA, class IN, addr 2610:a1:1024:: 200
    - dns2.registrar-servers.com: type AAAA, class IN, addr 2610:a1:1025:: 200

**分析：**

ICMP数据报除了最基本的首部以外，主体部分主要是DNS。DNS中的Questions、Answer RRs、Authority RRs、Additional RRs这几个标志后面所跟的数字都与后面的解析结果数量有关。解析结果中的每一项包含了Name、Type、Class、TTL、Date length和Addr中的几项或全部。Addr中存放的IP地址就是我们最后想要的资源IP地址。

6. 捕获并分析ARP报文数据，具体步骤如下：

1）设置过滤器为arp，开始捕获数据

2）CMD中输入arp–a查看ARP缓存表

3）ping一个arp缓存表中没有的IP地址

4）分析捕获的数据包中的内容,如图2.5所示。

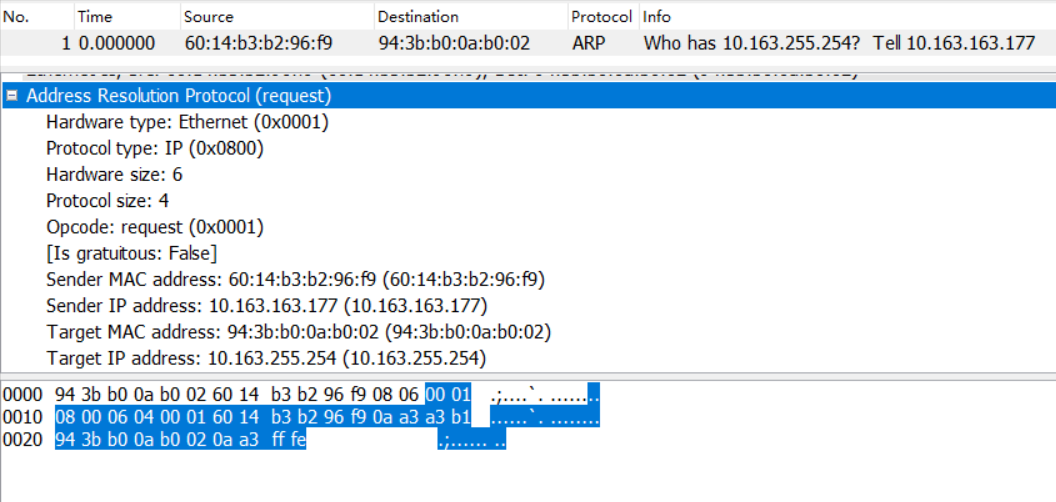


图2.4 捕获的arp报文

ARP帧格式：

* 硬件类型：Ethernet (0x0001)
* 上层协议类型：IP (0x0800)
* MAC地址长度：6
* IP地址长度：4
* 操作类型：request (0x0001)
* 源MAC地址：60:14:b3:b2:96:f9 (60:14:b3:b2:96:f9)
* 源IP地址：10.163.163.177 (10.163.163.177)
* 目的MAC地址：94:3b:b0:0a:b0:02 (94:3b:b0:0a:b0:02)
* 目的IP地址：10.163.255.254 (10.163.255.254)

**分析：**

根据书上的ARP帧格式与抓包结果相比较，发现，上图所抓的包帧格式与书上格式完全吻合。

7. 捕获并分析http报文。

1）将过滤器设置为http，开始捕捉数据包。

2）在浏览器中输入<http://www.baidu.com/>或者其他网址

3）分别查看并分析捕捉到的数据包中的应用层（http），运输层，网络层，数据链路层首部。

由于http请求较多, 不易分辨Get获得<http://www.baidu.com/的数据>, 因此我以访问baidu时带有特征性的图片来研究整个http请求过程。

通过chrome开发者工具抓包，可以观察到在加载baidu界面时，也请求了图片资源。%E5%94%AF%E5%93%81%E4%BC%9A解码后为苏宁易购。

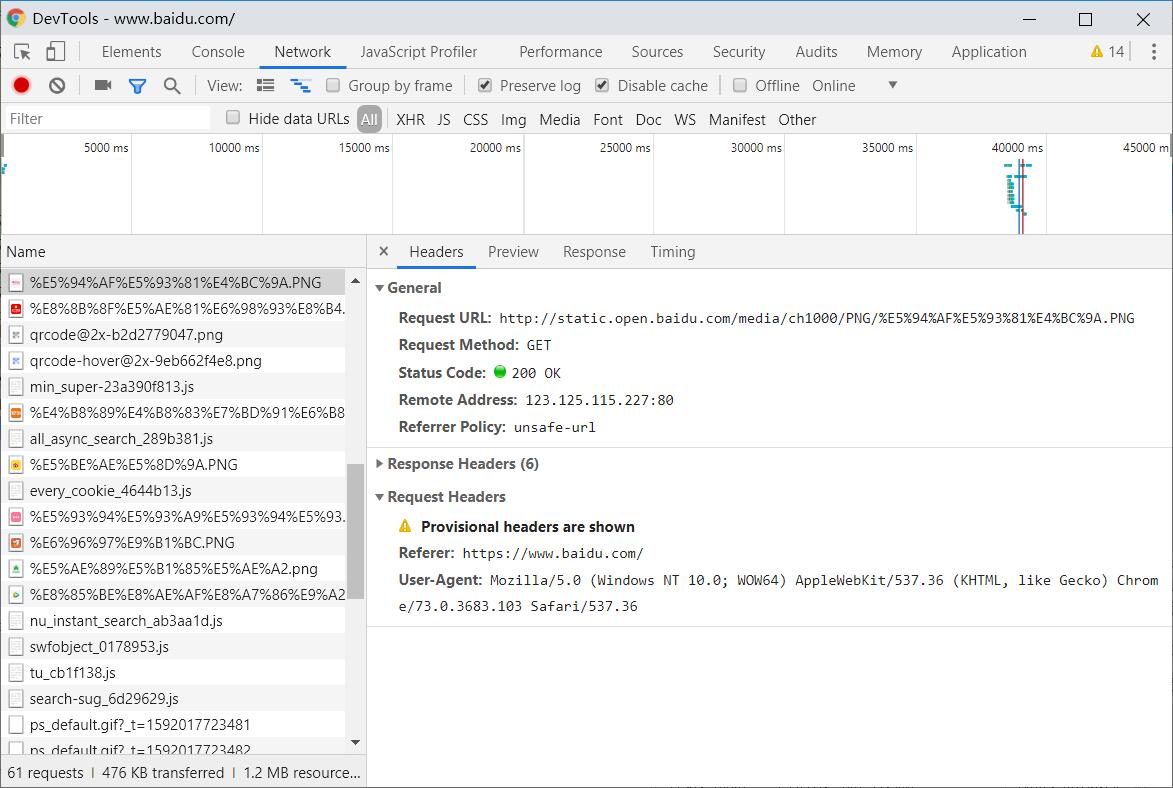


图2.5 确定研究对象-苏宁易购图片

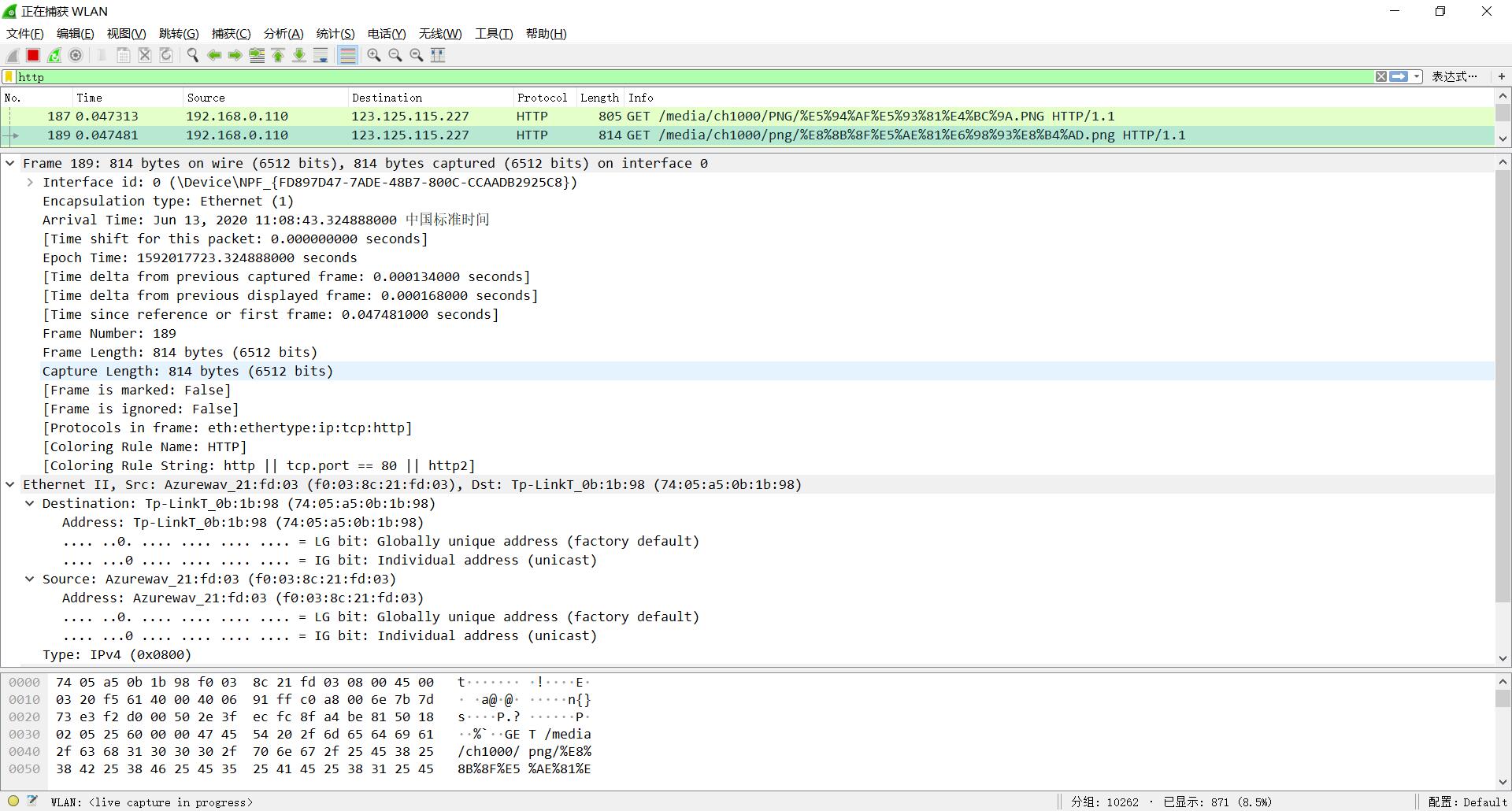


图2.6 物理层(frame)、数据链路层(EthernetII)

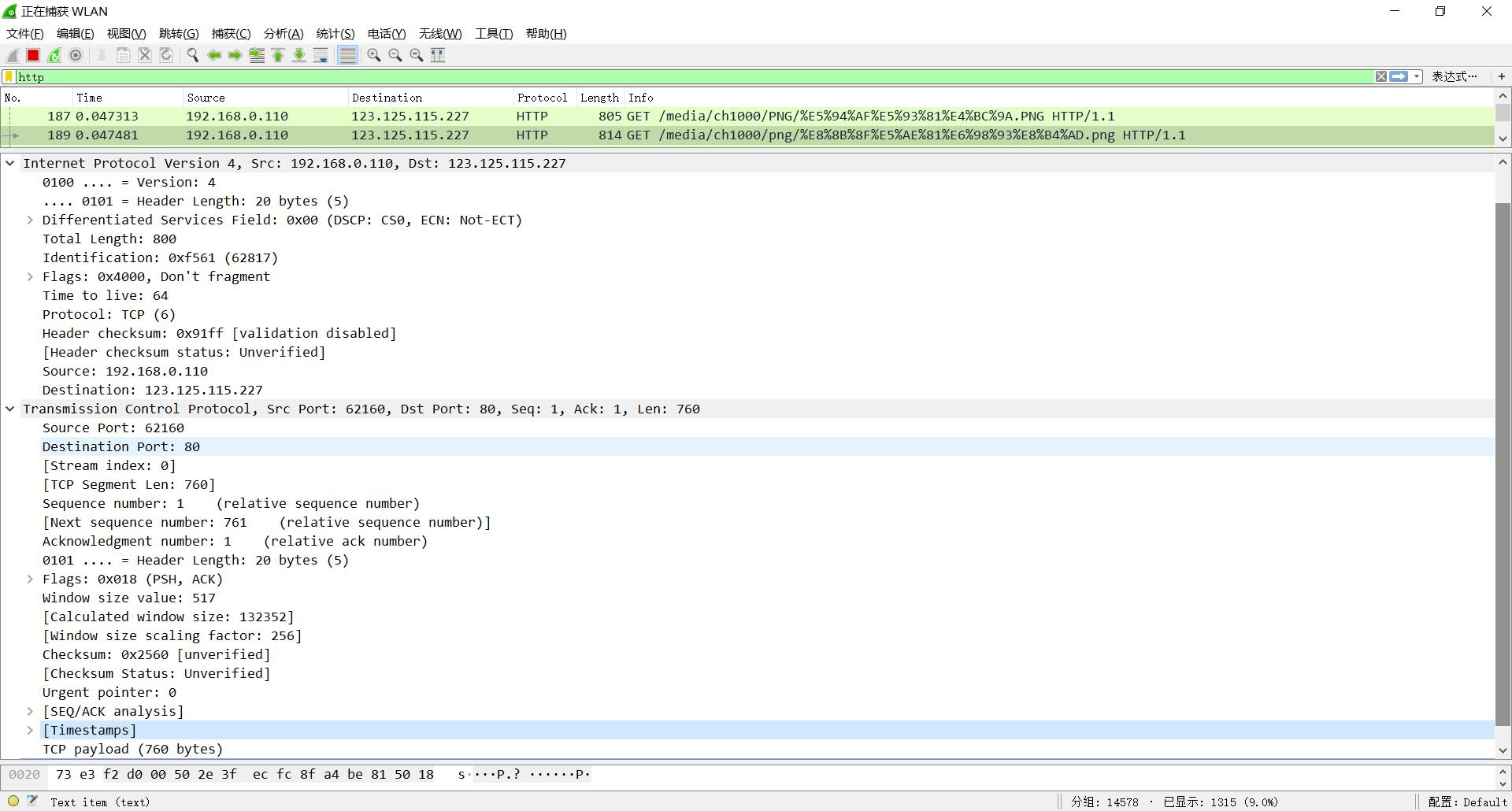


图2.7 网络层(Internet Protocol)、传输层(Transmission Control Protocol)

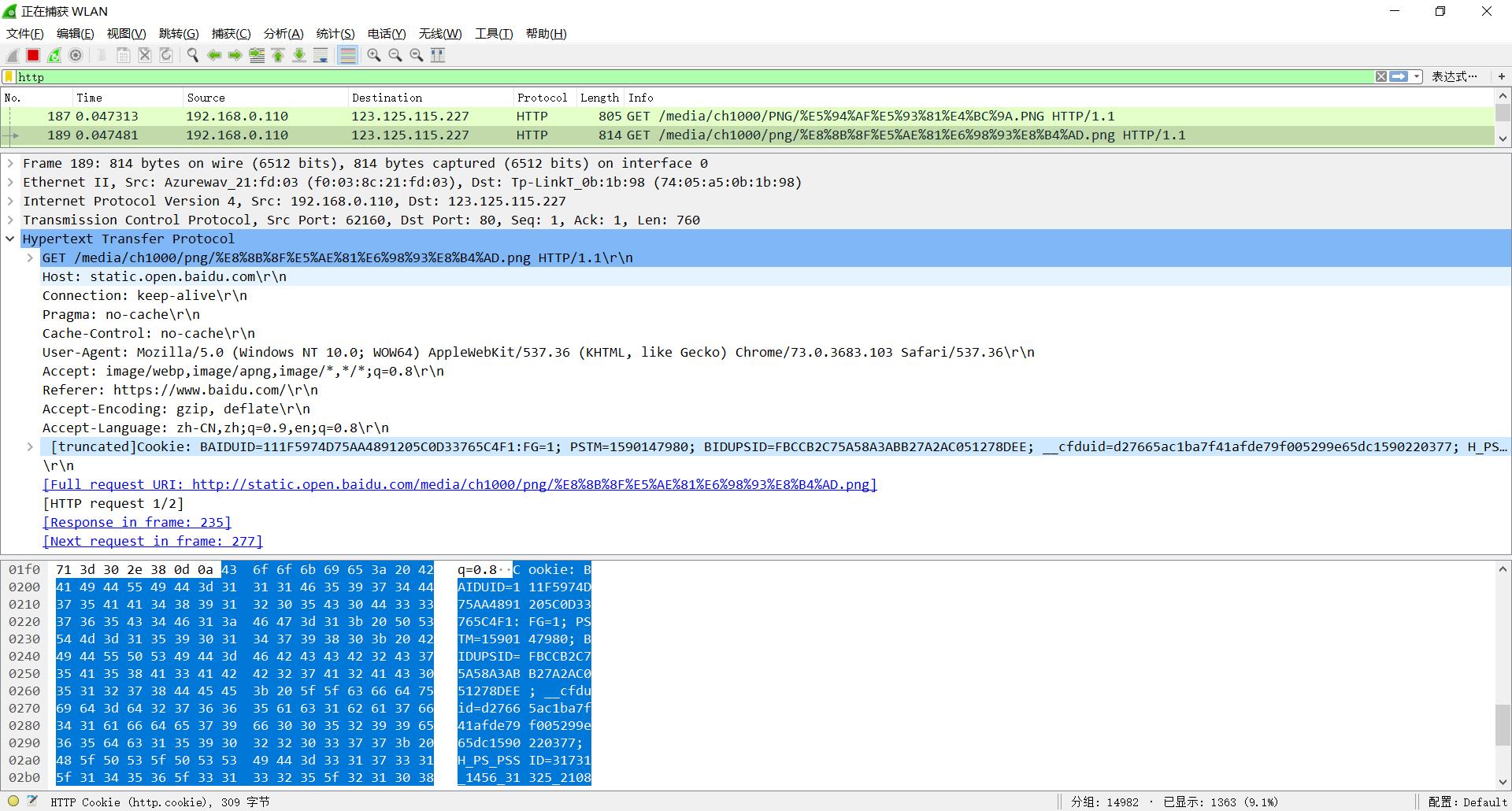


图2.8 应用层(Hypertext Transfer Protocol-http)

**分析：**

http报文中包含了从应用层、运输层、网络层、数据链路层和物理层各层的首部信息，符合教材上所写的五层体系结构。

四、实验小结

本次实验对网络协议的数据包进行了捕获，同时也对里面几个经典的报文进行了分析，与教材上的内容进行了对照，所得的结果与书上所写一致。通过这次实验，巩固了我们在课上所学的知识，加深了对报文知识与计算机网络结构的理解。