中国科学技术大学计算机学院
《计算机网络》实验报告

实验题目：lab1 WireShark_Intro

学生姓名：张舒恒

学生学号：PB19030888

专业：计算机科学与技术

授课老师：华蓓

完成日期：2021 年 9 月 12 日

实验目的

1. 学习 Wireshark 网络分析工具的使用
2. 捕获，观察并分析 HTTP 报文结构
3. 回答本次实验指导书中的问题

实验原理

本次实验使用 WireShark 工具。其中用于观察执行协议实体之间交换的消息的基本工具称为分组嗅探器(packet sniffer)。顾名思义，分组嗅探器捕获从计算机发送/接收的消息;它还将存储并显示这些捕获的消息中各种协议字段的内容。分组嗅探器本身是被动的。它只是观察有计算机上运行的应用程序和协议发送和接收的消息，但本身不会发送分组。类似地，接收的分组也不会直接到达分组嗅探器。相反，分组嗅探器接收一份从您的机器中的应用程序和协议发送/接收的分组的副本。

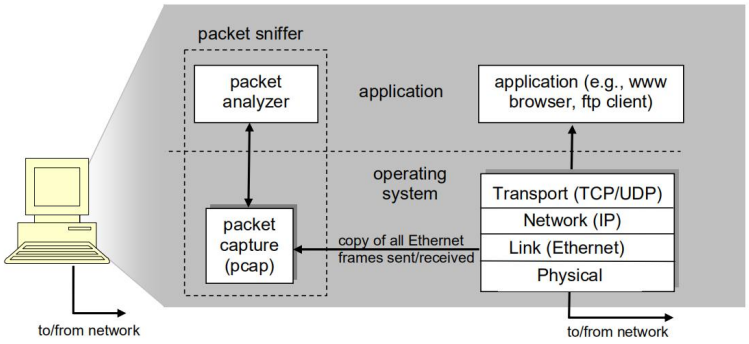


图 1（引自实验指导书）

分组嗅探器的结构如图 1 所示。在图 1 的右边是运行在计算机上的协议和应用。分组嗅探器(图中画虚线框部分)是计算机中的附加软件(区别于上述协议和应用)，它包含两个部

分。分组捕获库获取每一个链路层接收/发送的帧。第二部分是分组分析器，其中显示了协议所有字段的内容。为了实现这一目的，分组分析器必须理解所有协议所交换的信息的结构。比如，我们对图 1 中 HTTP 协议的各个字段信息感兴趣。分组分析器理解以太网帧的格式，所以可以从以太网帧中区分出 IP 数据报。同时，它还理解 IP 数据报格式，所以它能从 IP 数据报分离出 TCP 报文段。最后，它还理解 TCP 报文段格式，从中分离出 HTTP 报文。又因它理解 HTTP 协议，所以能在实现 WireShark 中显示 HTTP 协议各字段信息的功能。

实验环境

1.PC 一台

2. Windows 操作系统

3. WireShark 网络分析工具包

4. Google 浏览器

实验过程

（1）WireShark 的安装

1.前往 http://www.wireshark.org/download.html 下载并安装 WireShark

2.简要阅读 WireShark 用户指南

（2）运行 WireShark

1.启动 WireShark，结合实验指导书，了解 WireShark 各个界面(命令菜单，显示过滤器，分组列表，分组详细信息)的功能。

2.根据实验指导书，对 WireShark 工具进行一系列设置。

3.开始运行 WireShark 的捕获功能，打开链接

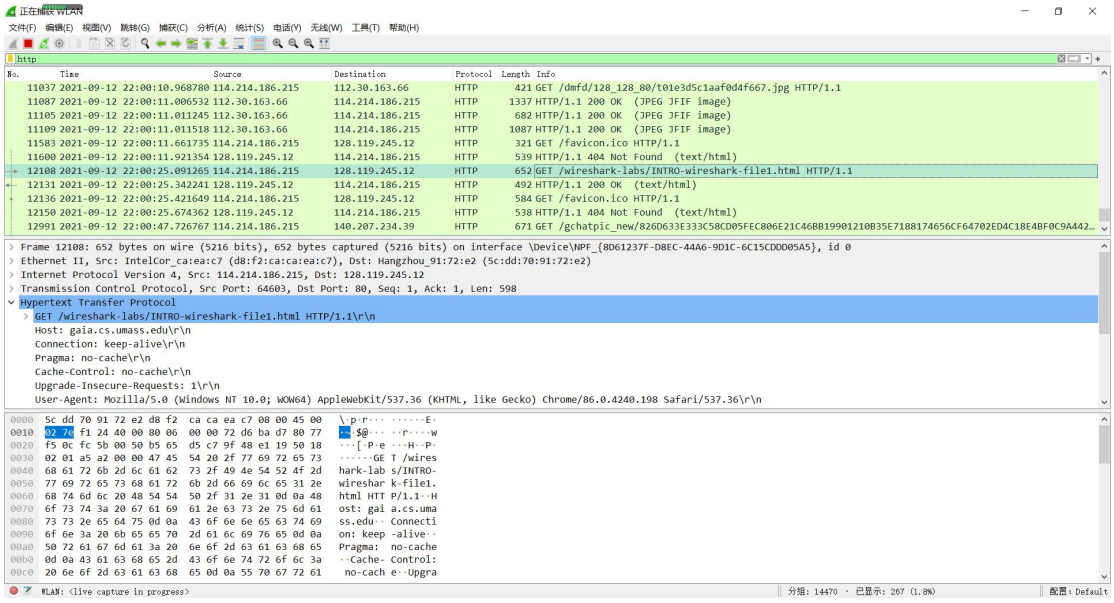
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

4.捕获完成后，在捕获窗口中停止 WireShark 捕获分组，利用“http”规则筛选出 HTTP 协议条目

5.分析 HTTP 报文结构并进行打印

6.退出 WireShark

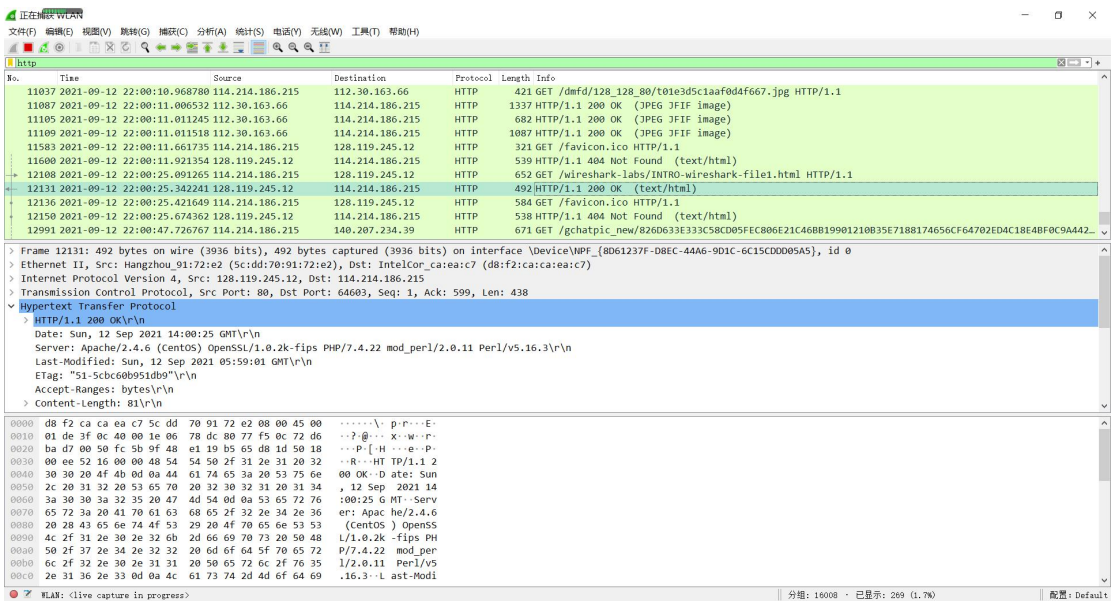
请求报文分析



如图所示，第一部分是请求行，说明请求类型为 GET，要访问的 URL 字段为 /wireshark-labs/INTRO-wir eshark-file1.html，所用的 HTTP 版本为 1.1 版本。

第二部分是请求头部。Host 指明了对象所在的主机(gaia.cs.umass.edu)。Connection: keep-alive 表示使用持续连接。Upgrade-Insecure-Requests: 1 告诉服务器浏览器可以处理 https 协议。User-Agent 用来指明用户代理，即向服务器发送请求的浏览器类型。这里浏览器类型是 Chrome/86.0.4240。

响应报文分析



如图所示，第一部分为状态行，有协议版本字段、状态码和相应状态信息。这里表示服务器正在使用 HTTP/1.1，并且处于正常状态。

第二部分为首部行。Date 指示服务器产生并发送该响应报文的日期和时间。Server 指示该报文是由 Apache Web 服务器产生的。Last-Modified 指示对象创建或最后修改的日期和时间。ETag:指示对象的标记，主要是为了解决一些 Last-Modified 无法解决的问题。Accept-Ranges 标识自身支持范围请求。Content-Length 指示被发送对象中的字节数。

问题回答

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

TCP，UDP，NBNS

2.How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?

如发送报文和响应报文，0.342241-0.091265=0.250976 秒

3.What is the Internet address of the gaia.cs.umass.edu (also known as www.net.cs.umass.edu)? What is the Internet address of your computer?

gaia.cs.umass.edu 的因特网地址是 128.119.245.12。我的计算机的因特网地址是 114.214.186.215。

4.Print the two HTTP messages (GET and OK) referred to in question 2 above.

```
No.     Time                           Source                Destination           Protocol Length Info
  12108 2021-09-12 22:00:25.091265    114.214.186.215       128.119.245.12        HTTP     652    GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 12108: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{8D61237F-
D8EC-44A6-9D1C-6C15CDDD05A5}, id 0
Ethernet II, Src: IntelCor_ca:ea:c7 (d8:f2:ca:ca:ea:c7), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
Internet Protocol Version 4, Src: 114.214.186.215, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64603, Dst Port: 80, Seq: 1, Ack: 1, Len: 598
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/
537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    Cookie: __guid=256026397.3328607658669036000.1631447539519.0063; monitor_count=27\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 12131]
    [Next request in frame: 12136]
```

```
No.     Time                           Source                Destination           Protocol Length Info
  12131 2021-09-12 22:00:25.342241    128.119.245.12        114.214.186.215       HTTP     492    HTTP/1.1 200 OK  (text/
html)
Frame 12131: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{8D61237F-
D8EC-44A6-9D1C-6C15CDDD05A5}, id 0
Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_ca:ea:c7 (d8:f2:ca:ca:ea:c7)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.186.215
Transmission Control Protocol, Src Port: 80, Dst Port: 64603, Seq: 1, Ack: 599, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 12 Sep 2021 14:00:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.22 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 12 Sep 2021 05:59:01 GMT\r\n
    ETag: "51-5cbc60b951db9"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.250976000 seconds]
    [Request in frame: 12108]
    [Next request in frame: 12136]
    [Next response in frame: 12150]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

总结

本次实验通过 WireShark 分组嗅探器捕获并分析 HTTP 报文，了解了 HTTP 请求报文、响应报文的结构，对报文中的内容有了一定的理解，将为今后的实验打下坚实的基础。