

重庆大学大数据与软件学院

上机报告

上机名称

利用 wireshark 分析协议 HTTP

课程名称

计算机网络

开课实验室：DS-1501

2025 年 3 月 16 日

姓 名		学号		成 绩	
上机（项目）名称		利用 wireshark 分析协议 HTTP		指导教师	高旻
教师评语	<div>教师签名：高旻</div> <div>年 月 日</div>				

一、实验目的

分析 HTTP 协议

二、实验内容

利用 Wireshark 俘获 HTTP 分组/ HTTP GET/response 交互/ HTTP 条件 GET/response 交互/获取长文件/嵌有对象的 HTML 文档

三、使用的软件、硬件

与因特网连接的计算机，操作系统为 Windows，安装有 Wireshark、IE 等软件

四、实验步骤及实验过程原始记录(数据、图表、计算等，需要有截图和简要说明)

Q1:HTTP/1.1

```

  ▾ Hypertext Transfer Protocol
    ▾ GET / HTTP/1.1\r\n
      > [Expert Info (Chat/Sequence): GET / HTTP/
        Request Method: GET
        Request URI: /
        Request Version: HTTP/1.1
        Host: www.sce.pku.edu.cn\r\n
        Connection: keep-alive\r\n
    > [86 Reassembled TCP Segments (106020 byte)
  ▾ Hypertext Transfer Protocol
    ▾ HTTP/1.1 200 OK\r\n
      Content-Encoding: gzip\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      Cxv all: +ccd6f133cb1502cbceb4680f379981

```

Q2:优先接受简体中文

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

Q3:

我的 ip: 172.20.10.14

服务器 ip: 220.181.33.105

2710	7.417455	172.20.10.14	220.181.33.105	HTTP	874 GET /cpro/ui/mads.php?c...
2721	7.418527	172.20.10.14	220.181.33.105	HTTP	886 GET /cpro/ui/mads.php?c...

Q4:

2299	7.292308	240e:954:0:1e::7521...	240e:430:121a:206d:...	HTTP	1371 HTTP/1.1 200 OK (JPEG ...
2317	7.292313	240e:954:0:1e::7521...	240e:430:121a:206d:...	HTTP	925 HTTP/1.1 200 OK (JPEG ...
2346	7.292542	240e:954:0:1e::7521...	240e:430:121a:206d:...	HTTP	529 HTTP/1.1 200 OK (JPEG ...

Q5:2018/4/9/11: 26: 26 周一

```
Connection: keep-alive\r\n
Expires: Wed, 19 Mar 2025 02:28:55 GMT\r\n
Last-Modified: Mon, 09 Apr 2018 11:26:26 GMT\r\n
ETag: "cc8bfa63f63504856eccd17dea30b40f"\r\n
```

Q6:806 字节

```
Server: nginx\r\n
Date: Sun, 16 Mar 2025 08:19:07 GMT\r\n
Content-Type: image/png\r\n
> Content-Length: 806\r\n
Connection: keep-alive\r\n
Content-Length: 806\r\n
Connection: keep-alive\r\n
```

Q7:

没有

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Host: gaiã.cs.umass.edu\r\n
Connection: keep-alive\r\n
```

Q8: 是，在 Line_based text data 中

```
> Hypertext Transfer Protocol
> Line-based text data: text/html
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

Q9:在第三个 get 请求中有，表示页面最后修改的时间

```

Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
If-None-Match: "173-6306f5e506857"\r\n
If-Modified-Since: Sun, 16 Mar 2025 05:59:02 GMT\r\n
\r\n

```

Q10:

状态码： 304。 服务器没有明确返回文件内容。因为返回 304 状态码，意思是不返回文件内容。具体原因：浏览器端缓存页面最后修改时间与服务器端时间一致，返回 304 状态码，客户端接到之后，就直接把本地缓存文件显示到浏览器中。

10794	37.431866	172.20.10.14	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-...
10810	37.767516	128.119.245.12	172.20.10.14	HTTP	294	HTTP/1.1 304 Not Modified

```

> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 52646 (52646), Seq: 1, Ack: 632, Len: 240
Hypertext Transfer Protocol
> HTTP/1.1 304 Not Modified\r\n
Date: Sun, 16 Mar 2025 08:42:41 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-6306f5e506857"\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.335650000 seconds]
[Request in frame: 10794]
[Next request in frame: 10818]

```

Q11:一个

No.	Time	Source	Destination	Protocol	Length	Info
2486	2.771337	172.20.10.14	128.119.245.12	HTTP	519	GET /favicon.ico HTTP/1.1
2777	3.026886	128.119.245.12	172.20.10.14	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Q12:404 NOT FOUND

2777	3.026886	128.119.245.12	172.20.10.14	HTTP	539	HTTP/1.1 404 Not Found (text/html)
------	----------	----------------	--------------	------	-----	------------------------------------

Q13:三个 GET 请求，

Ip 分别是：128.119.245.12 128.119.245.12 178.79.137.164

No.	Time	Source	Destination	Protocol	Length	Info
102	3.117590	172.20.10.14	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wi...
142	3.404754	128.119.245.12	172.20.10.14	HTTP	1355	HTTP/1.1 200 OK (text/html)
160	3.435830	172.20.10.14	128.119.245.12	HTTP	519	GET /pearson.png HTTP/1.1
255	3.694042	128.119.245.12	172.20.10.14	TCP	1414	[TCP segment of a reassembl...
273	4.057231	172.20.10.14	178.79.137.164	HTTP	486	GET /8E_cover_small.jpg HTT...
281	4.335999	178.79.137.164	172.20.10.14	HTTP	225	HTTP/1.1 301 Moved Permanen...

Q14:

并行，因为两个图片是连续请求，不需要等第一个请求得到回复后才继续第二次请求。有时候不同网络环境下，可能抓到的包是在对应请求得到回应后才继续第二次的请求，有时候是不需要等第一个请求得到回复后才继续第二次请求。可以多抓几次试试。只有存在不需要等第一个请求得到回复后才继续第二次请求的情况，就说明是并行的