

HTTP 实验报告

PB20111689 蓝俊玮

Basic Interaction

1. 通过请求报文 HTTP GET 中的请求行 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n 中的 HTTP 版本字段可以看出，我的浏览器运行的是 **HTTP 1.1**，同理，通过响应报文 HTTP OK 中可以看出，服务器使用的也是 **HTTP 1.1**。

```

  ▾ Hypertext Transfer Protocol
    ▾ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      ▾ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.html
        Request Version: HTTP/1.1
      ▾ Hypertext Transfer Protocol
        ▾ HTTP/1.1 200 OK\r\n
          ▾ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
            Response Version: HTTP/1.1
            Status Code: 200
            [Status Code Description: OK]
            Response Phrase: OK

```

2. 从请求报文 HTTP GET 的 Accept-Language 字段可以看到，可以接受：**中文(zh)**，**大陆中文(zh-CN)**，**美国英语(en-US)**，**英语(en)**，**英国英语(en-GB)**。

```

  ▾ Hypertext Transfer Protocol
    ▾ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/80.0.4012.101 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,en-GB;q=0.6\r\n

```

3. 从每个报文的 Source Address 可以看出我电脑下 WLAN 的 IP 地址为 **114.214.190.205**，而从 Destination Address 可以看到服务器的 IP 地址为 **128.119.245.12**。

```

  ▾ Internet Protocol Version 4, Src: 114.214.190.205, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 723
      Identification: 0xb987 (47495)
    > Flags: 0x40, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 128
      Protocol: TCP (6)
      Header Checksum: 0x9775 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 114.214.190.205
      Destination Address: 128.119.245.12

```

4. 从响应报文 HTTP OK 中的 Status code 字段可以看出结果是 **200**。

```

  ▾ Hypertext Transfer Protocol
    ▾ HTTP/1.1 200 OK\r\n
      ▾ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK

```

5. 从响应报文 HTTP OK 中的 Last-Modified 字段可以看出，时间是 **Thu, 15 Sep 2022 05:59:02 GMT**，即北京时间 **2022年9月15日13:59:02 星期四**

```
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 16 Sep 2022 00:12:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 15 Sep 2022 05:59:02 GMT\r\n
    ETag: "80-5e8b0f136f83a"\r\n
    Accept-Ranges: bytes\r\n
```

6. 从 Frame 中可以查看获取了 **540 bytes** 的内容

```
▼ Frame 103: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{78348DFD-6104-46FE-923D-EF83B9D90DB2}
  > Interface id: 0 (\Device\NPF_{78348DFD-6104-46FE-923D-EF83B9D90DB2})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 16, 2022 08:12:26.684556000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1663287146.684556000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.245705000 seconds]
    [Time since reference or first frame: 4.249318000 seconds]
    Frame Number: 103
    Frame Length: 540 bytes (4320 bits)
    Capture Length: 540 bytes (4320 bits)
```

7. 有很多，实际上 packet-listing window 只有少量内容，而 packet-content window 还有许多详细内容包括：Date, Server, Last-Modified, ETag 等等。

Conditional Interaction

8. 在第一次请求报文 HTTP GET 中没有 If-Modified-Since 字段

```
▼ Hypertext Transfer Protocol
  ▼ 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
      Upgrade-Insecure-Requests: 1\r\n
      User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,en-GB;q=0.6\r\n
    > Cookie: _gcl_au=1.1.60676089.1662773803; _ga_21RLS0L7EB=GS1.1.1662773803.1.0.1662773803.0.0.0; _ga=GA1.
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
      [HTTP request 1/2]
      [Response in frame: 111]
      [Next request in frame: 149]
```

9. 在响应报文 HTTP OK 中有 Line-based text data，能够直接看到服务器明确地返回了网页的内容

```
> Content-Length: 371\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: 0.274475000 seconds]
  [Request in frame: 93]
  [Next request in frame: 149]
  [Next response in frame: 154]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
▼ Line-based text data: text/html (10 lines)
  \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
```

10. 可以看到，并且 If-Modified-Since 后面跟着一个时间

11. 在第二次响应报文 HTTP OK 中的 Status Code 是 **304**, Phrase 是 **Not Modified**。服务器并没有显式地返回文件内容。原因在于服务器返回的状态码信息是 304, 意味着文件在近期并没有被修改过, 它会告诉浏览器从代理缓存中获取该对象副本。所以浏览器会从缓存中获取文件内容, 因此不会显示地返回文件内容。

Retrieving Long Documents

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File (F), Edit (E), View (V), Jump (G), Capture (C), Analyze (A), Statistics (S), Telephony (Y), Wireless (W), Tools (T), and Help (H). Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is titled 'http' and shows a list of captured packets. The first packet is selected, showing details of an HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
87	3.095373	114.214.192.187	128.119.245.12	HTTP	737	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
108	3.309704	128.119.245.12	114.214.192.187	HTTP	535	HTTP/1.1 200 OK (text/html)
118	3.577093	114.214.192.187	128.119.245.12	HTTP	683	GET /favicon.ico HTTP/1.1
124	3.817398	128.119.245.12	114.214.192.187	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
> Frame 108: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe_17:ac:42 (80:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.192.187
> Transmission Control Protocol, Src Port: 80, Dst Port: 61021, Seq: 4381, Ack: 684, L
> [4 Reassembled TCP Segments (4861 bytes): #105(1460), #106(1460), #107(1460), #108(4
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Fri, 16 Sep 2022 07:43:59 GMT\r\n
```

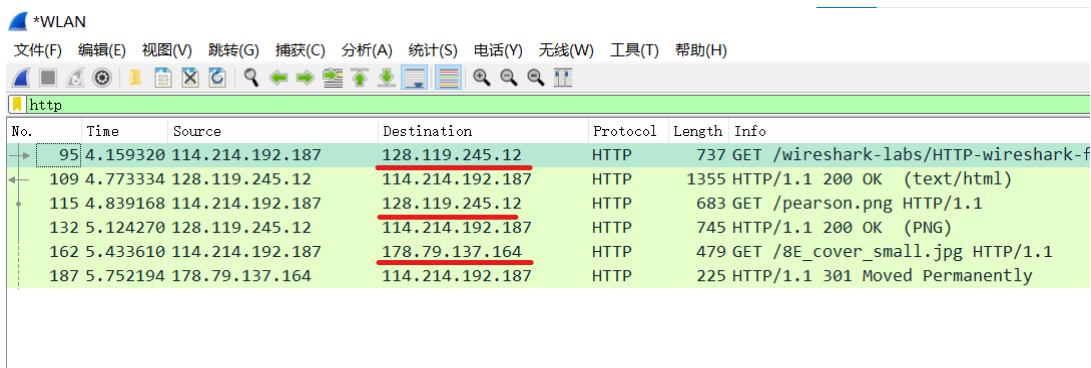
```
> Frame 108: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe_17:ac:42 (80:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.192.187
> Transmission Control Protocol, Src Port: 80, Dst Port: 61021, Seq: 4381, Ack: 684, L
> [4 Reassembled TCP Segments (4861 bytes): #105(1460), #106(1460), #107(1460), #108(4
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Fri, 16 Sep 2022 07:43:59 GMT\r\n
```

15. 为了传输一次 HTTP 响应和 Bill of Rights 文章，需要 4 个 TCP 报文段。

```
> Frame 108: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF{...}
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe_17:ac:42 (80:30:42:17:ac:42)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.192.187
> Transmission Control Protocol, Src Port: 80, Dst Port: 61021, Seq: 4381, Ack: 684, Len: 4861
✖ [4 Reassembled TCP Segments (4861 bytes): #105(1460), #106(1460), #107(1460), #108(481)]
  [Frame: 105, payload: 0-1459 (1460 bytes)]
  [Frame: 106, payload: 1460-2919 (1460 bytes)]
  [Frame: 107, payload: 2920-4379 (1460 bytes)]
  [Frame: 108, payload: 4380-4860 (481 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a204672692c2031362053]
✖ Hypertext Transfer Protocol
```

HTML Documents with Embedded Objects

16. 我的浏览器一共发送了 3 次请求报文，其中 3 次的目的 IP 地址分别为 128.119.245.12, 128.119.245.12, 178.79.137.164。



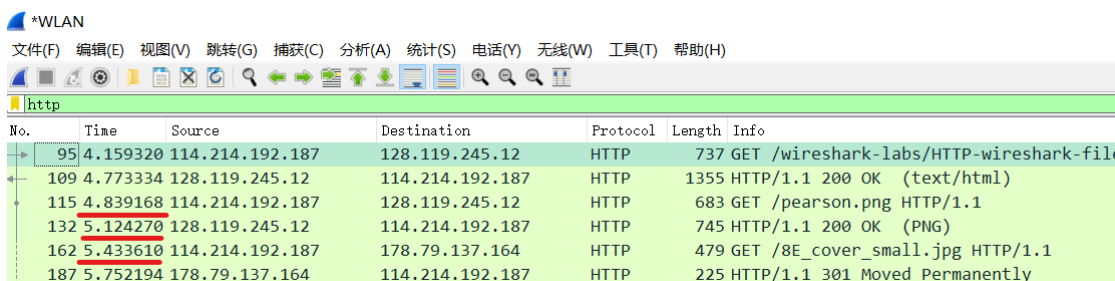
No.	Time	Source	Destination	Protocol	Length	Info
95	4.159320	114.214.192.187	128.119.245.12	HTTP	737	GET /wireshark-labs/HTTP-wireshark-f
109	4.773334	128.119.245.12	114.214.192.187	HTTP	1355	HTTP/1.1 200 OK (text/html)
115	4.839168	114.214.192.187	128.119.245.12	HTTP	683	GET /pearson.png HTTP/1.1
132	5.124270	128.119.245.12	114.214.192.187	HTTP	745	HTTP/1.1 200 OK (PNG)
162	5.433610	114.214.192.187	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
187	5.752194	178.79.137.164	114.214.192.187	HTTP	225	HTTP/1.1 301 Moved Permanently

这里在最后一个响应报文中的状态码和相应短语为 301 Moved Permanently 的原因：所请求的这个图片对象已经被永久转移了，新的 URL 定义为：

```
✖ Hypertext Transfer Protocol
> HTTP/1.1 301 Moved Permanently\r\n
  Location: https://kurose.cslash.net/8E_cover_small.jpg\r\n
> Content-Length: 0\r\n
  Date: Mon, 19 Sep 2022 00:33:59 GMT\r\n
  Server: lighttpd/1.4.47\r\n
  \r\n
[HTTP response 1/1]
[Time since request: 0.290702000 seconds]
```

同时根据这个现象，我们访问这个两个对应 URL [pearson.png \(253×199\) \(umass.edu\)](https://kurose.cslash.net/pearson.png) 和 [404 Not Found \(umass.edu\)](https://kurose.cslash.net/404_Not_Found) 也可以发现其响应报文为何不同。

17. 浏览器下载两个图片是有先后顺序的，通过请求时间和响应时间就可以看出来（第一个图片的响应报文比第二个图片的请求报文发生时间更早）。同时根据实践体验，当访问这个网站时，第二个图片总是显示得非常慢，甚至不显示。



No.	Time	Source	Destination	Protocol	Length	Info
95	4.159320	114.214.192.187	128.119.245.12	HTTP	737	GET /wireshark-labs/HTTP-wireshark-fil
109	4.773334	128.119.245.12	114.214.192.187	HTTP	1355	HTTP/1.1 200 OK (text/html)
115	4.839168	114.214.192.187	128.119.245.12	HTTP	683	GET /pearson.png HTTP/1.1
132	5.124270	128.119.245.12	114.214.192.187	HTTP	745	HTTP/1.1 200 OK (PNG)
162	5.433610	114.214.192.187	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
187	5.752194	178.79.137.164	114.214.192.187	HTTP	225	HTTP/1.1 301 Moved Permanently

HTTP Authentication

18. 在第一次 HTTP GET 之后服务器返回的响应报文信息（状态码和响应短语）分别是 401 和 Unauthorized

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 61411, Seq: 1
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 401 Unauthorized\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Fri, 16 Sep 2022 08:08:19 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_

```

19. 对比浏览器发出的两次请求报文中，第二次请求报文中增加了 **Cache-Control** 字段和 **Authorization** 字段，其中比较重要的应该是 **Authorization** 字段，其给出了重要的认证信息。

```

Hypertext Transfer Protocol
> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\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/webp,image/
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,en-GB;q=0.6\r\n
  Cookie: _gcl_au=1.1.60676089.1662773803; _ga_21RLS0L7EB=GS1.1.1662773803.1.0.16
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP
Hypertext Transfer Protocol
> GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like C
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,en-GB;q=0.6\r\n
  > Cookie: _gcl_au=1.1.60676089.1662773803; _ga_21RLS0L7EB=GS1.1.1662773803.1.0.1662773803

```