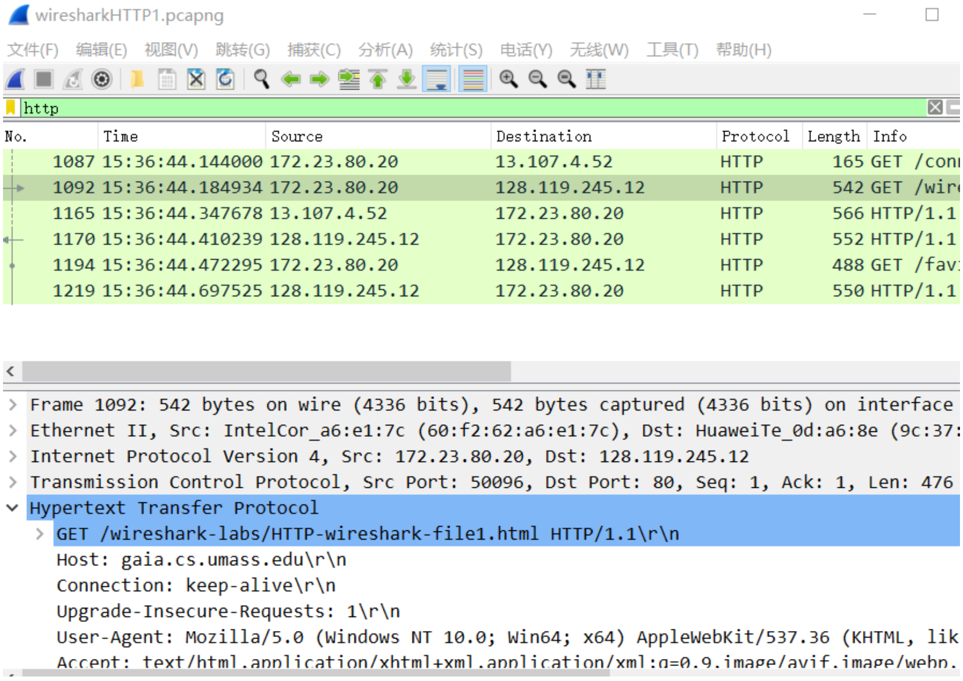
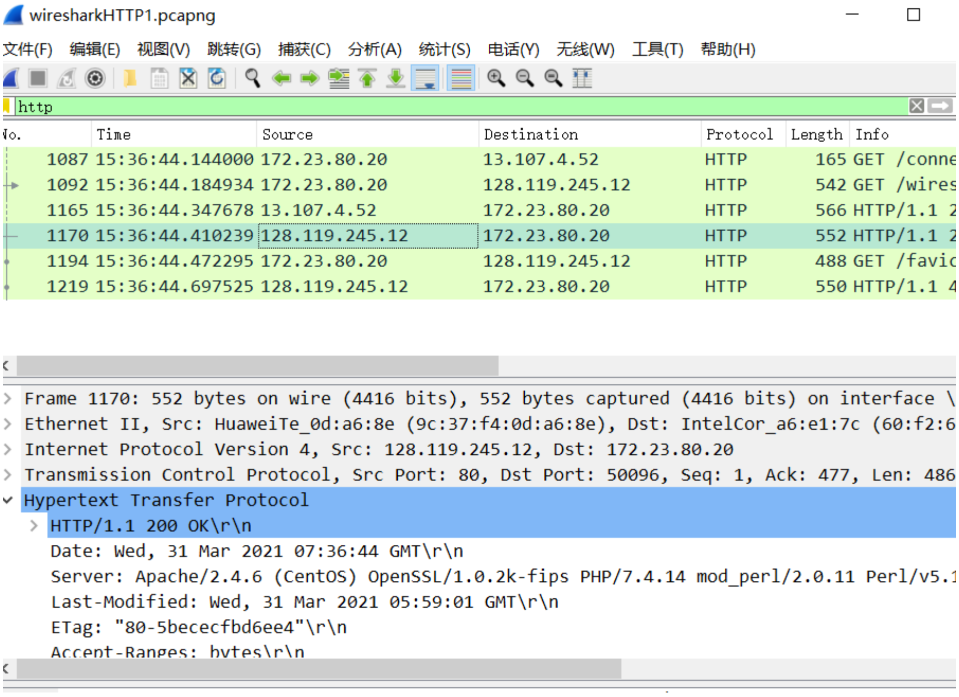
一、基本的 HTTP 获取/响应交互

1、我的浏览器运行的 HTTP 版本为 1.1，服务器运行的 HTTP 版本为 1.1


wiresharkHTTP1.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
No.  Time             Source          Destination      Protocol Length Info
1087 15:36:44.144000 172.23.80.20    13.107.4.52      HTTP     165 GET /con
1092 15:36:44.184934 172.23.80.20    128.119.245.12   HTTP     542 GET /wir
1165 15:36:44.347678 13.107.4.52     172.23.80.20     HTTP     566 HTTP/1.1
1170 15:36:44.410239 128.119.245.12  172.23.80.20     HTTP     552 HTTP/1.1
1194 15:36:44.472295 172.23.80.20    128.119.245.12   HTTP     488 GET /fav
1219 15:36:44.697525 128.119.245.12  172.23.80.20     HTTP     550 HTTP/1.1
```

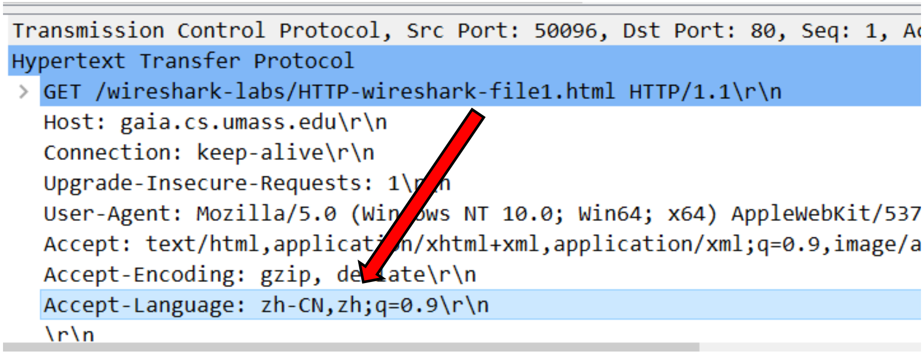
```
> Frame 1092: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface
> Ethernet II, Src: IntelCor_a6:e1:7c (60:f2:62:a6:e1:7c), Dst: HuaweiTe_0d:a6:8e (9c:37:
> Internet Protocol Version 4, Src: 172.23.80.20, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50096, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
v 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, lik
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
```


wiresharkHTTP1.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
No.  Time             Source          Destination      Protocol Length Info
1087 15:36:44.144000 172.23.80.20    13.107.4.52      HTTP     165 GET /conne
1092 15:36:44.184934 172.23.80.20    128.119.245.12   HTTP     542 GET /wires
1165 15:36:44.347678 13.107.4.52     172.23.80.20     HTTP     566 HTTP/1.1 2
1170 15:36:44.410239 128.119.245.12  172.23.80.20     HTTP     552 HTTP/1.1 2
1194 15:36:44.472295 172.23.80.20    128.119.245.12   HTTP     488 GET /favic
1219 15:36:44.697525 128.119.245.12  172.23.80.20     HTTP     550 HTTP/1.1 4
```

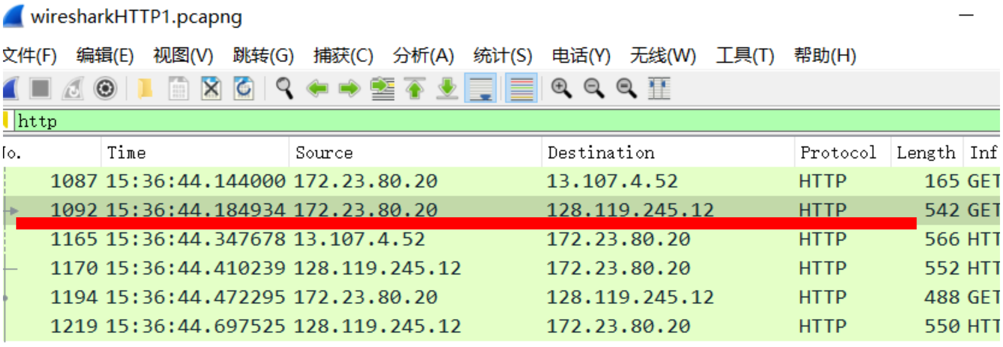
```
> Frame 1170: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface \
> Ethernet II, Src: HuaweiTe_0d:a6:8e (9c:37:f4:0d:a6:8e), Dst: IntelCor_a6:e1:7c (60:f2:6
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.23.80.20
> Transmission Control Protocol, Src Port: 80, Dst Port: 50096, Seq: 1, Ack: 477, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 31 Mar 2021 07:36:44 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.1
    Last-Modified: Wed, 31 Mar 2021 05:59:01 GMT\r\n
    ETag: "80-5bececfbd6ee4"\r\n
    Accept-Ranges: bytes\r\n
```

2、我的浏览器指示服务器可以接受 zh-CN、zh



```
Transmission Control Protocol, Src Port: 50096, Dst Port: 80, Seq: 1, Ac
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
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/a
   Accept-Encoding: gzip, deflate\r\n
   Accept-Language: zh-CN,zh;q=0.9\r\n
   \r\n
```

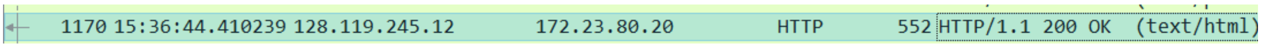
3、my computer：172.23.80.20，gaia.cs.umass.edu：128.119.245.12


wiresharkHTTP1.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http

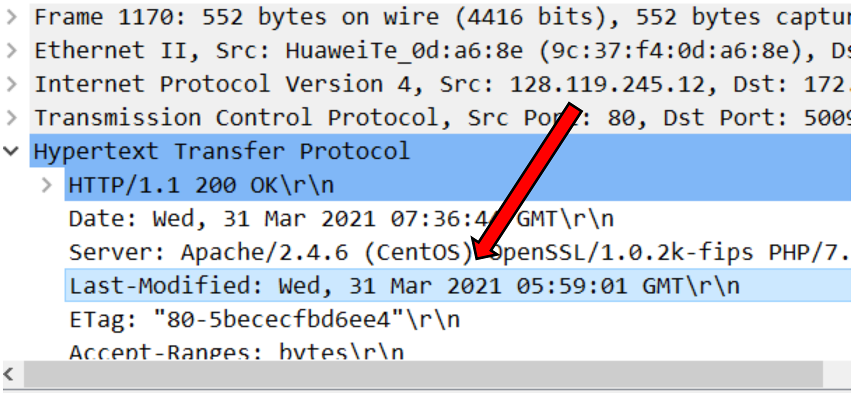
lo.	Time	Source	Destination	Protocol	Length	Inf
1087	15:36:44.144000	172.23.80.20	13.107.4.52	HTTP	165	GET
1092	15:36:44.184934	172.23.80.20	128.119.245.12	HTTP	542	GET
1165	15:36:44.347678	13.107.4.52	172.23.80.20	HTTP	566	HTT
1170	15:36:44.410239	128.119.245.12	172.23.80.20	HTTP	552	HTT
1194	15:36:44.472295	172.23.80.20	128.119.245.12	HTTP	488	GET
1219	15:36:44.697525	128.119.245.12	172.23.80.20	HTTP	550	HTT

4、status code: 200 OK



```
1170 15:36:44.410239 128.119.245.12    172.23.80.20    HTTP    552 HTTP/1.1 200 OK  (text/html)
```

5 Last-Modified: Wed, 31 Mar 2021 07:36:44 GMT



```
> Frame 1170: 552 bytes on wire (4416 bits), 552 bytes captu
> Ethernet II, Src: HuaweiTe_0d:a6:8e (9c:37:f4:0d:a6:8e), D
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.
> Transmission Control Protocol, Src Port: 80, Dst Port: 500
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 31 Mar 2021 07:36:44 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.
    Last-Modified: Wed, 31 Mar 2021 05:59:01 GMT\r\n
    ETag: "80-5bececfbd6ee4"\r\n
    Accept-Ranges: bytes\r\n
```

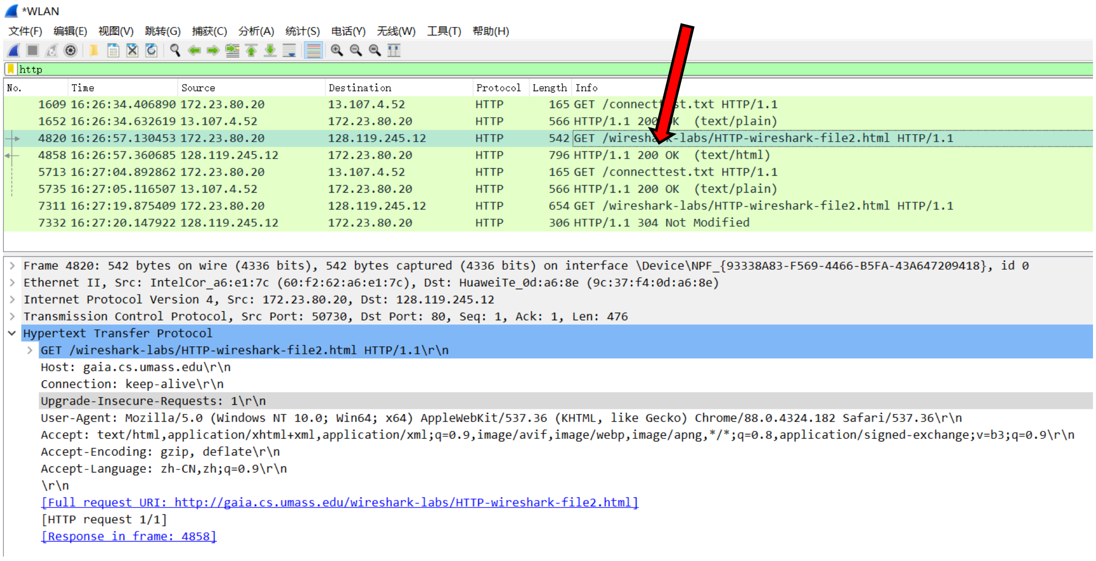
6、128bytes

7、Host

二、HTTP 条件获取/响应交互

8、没有

9、是，因为返回的 status code 为 200


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

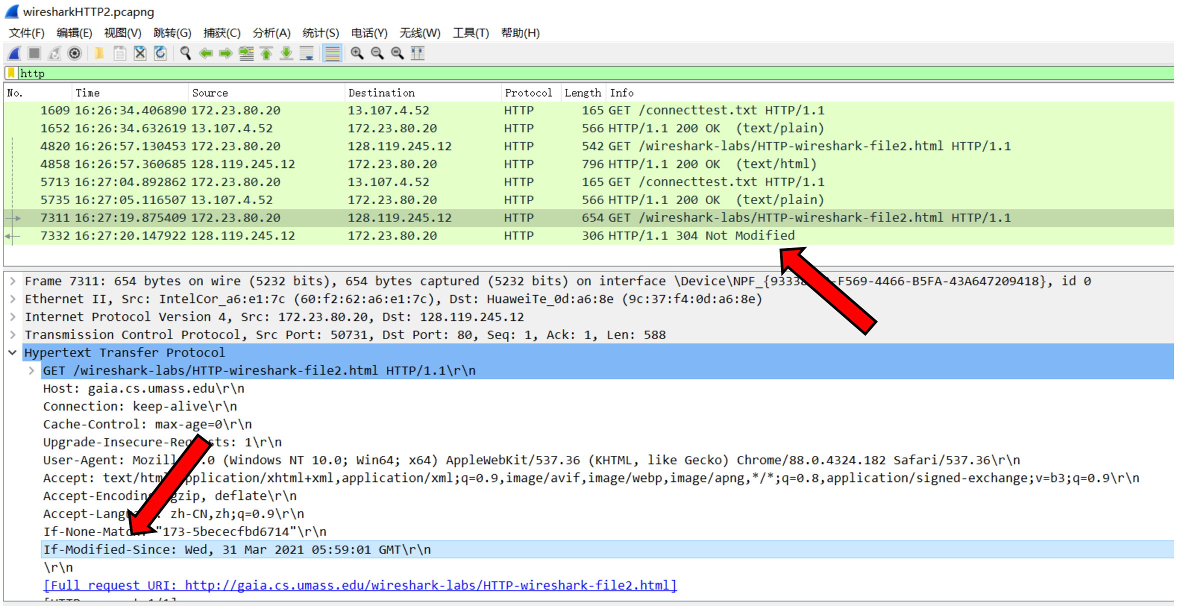
```
http
No.     Time            Source          Destination     Protocol Length Info
   1609 16:26:34.406890 172.23.80.20    13.107.4.52     HTTP     165 GET /connecttest.txt HTTP/1.1
   1652 16:26:34.632619 13.107.4.52     172.23.80.20    HTTP     566 HTTP/1.1 200 OK  (text/plain)
   4820 16:26:57.130453 172.23.80.20    128.119.245.12  HTTP     542 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   4858 16:26:57.360685 128.119.245.12  172.23.80.20    HTTP     796 HTTP/1.1 200 OK  (text/html)
   5713 16:27:04.892862 172.23.80.20    13.107.4.52     HTTP     165 GET /connecttest.txt HTTP/1.1
   5735 16:27:05.116507 13.107.4.52     172.23.80.20    HTTP     566 HTTP/1.1 200 OK  (text/plain)
   7311 16:27:19.875409 172.23.80.20    128.119.245.12  HTTP     654 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   7332 16:27:20.147922 128.119.245.12  172.23.80.20    HTTP     306 HTTP/1.1 304 Not Modified

> Frame 4820: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface \Device\NPF_{93338A83-F569-4466-B5FA-43A647209418}, id 0
> Ethernet II, Src: IntelCor_a6:e1:7c (60:f2:62:a6:e1:7c), Dst: HuaweiTe_0d:a6:8e (9c:37:f4:0d:a6:8e)
> Internet Protocol Version 4, Src: 172.23.80.20, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50730, Dst Port: 80, Seq: 1, Ack: 1, Len: 476
v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 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
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 4858]
```

10、是

11、status code and phrase: 304 Not Modified

服务器没有显式返回文件的内容

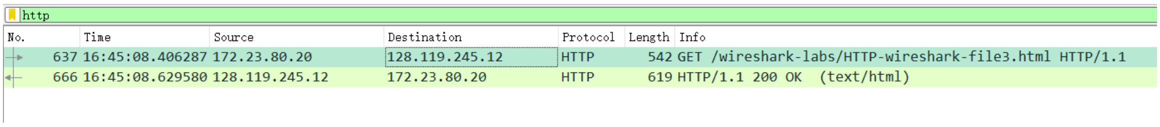

wiresharkHTTP2.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
http
No.     Time            Source          Destination     Protocol Length Info
   1609 16:26:34.406890 172.23.80.20    13.107.4.52     HTTP     165 GET /connecttest.txt HTTP/1.1
   1652 16:26:34.632619 13.107.4.52     172.23.80.20    HTTP     566 HTTP/1.1 200 OK  (text/plain)
   4820 16:26:57.130453 172.23.80.20    128.119.245.12  HTTP     542 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   4858 16:26:57.360685 128.119.245.12  172.23.80.20    HTTP     796 HTTP/1.1 200 OK  (text/html)
   5713 16:27:04.892862 172.23.80.20    13.107.4.52     HTTP     165 GET /connecttest.txt HTTP/1.1
   5735 16:27:05.116507 13.107.4.52     172.23.80.20    HTTP     566 HTTP/1.1 200 OK  (text/plain)
   7311 16:27:19.875409 172.23.80.20    128.119.245.12  HTTP     654 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   7332 16:27:20.147922 128.119.245.12  172.23.80.20    HTTP     306 HTTP/1.1 304 Not Modified

> Frame 7311: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface \Device\NPF_{93338A83-F569-4466-B5FA-43A647209418}, id 0
> Ethernet II, Src: IntelCor_a6:e1:7c (60:f2:62:a6:e1:7c), Dst: HuaweiTe_0d:a6:8e (9c:37:f4:0d:a6:8e)
> Internet Protocol Version 4, Src: 172.23.80.20, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50731, Dst Port: 80, Seq: 1, Ack: 1, Len: 588
v 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, like Gecko) Chrome/88.0.4324.182 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
    If-None-Match: "173-5bececfbd6714"\r\n
    If-Modified-Since: Wed, 31 Mar 2021 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

三、长文档检索

12、只发送了一个 HTTP GET 请求信息，其中 637 号 HTTP GET 请求数据包包含对于美国权利法案的请求

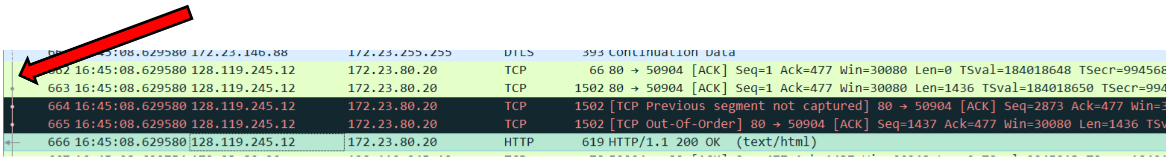


```
http
No.     Time            Source          Destination     Protocol Length Info
    637 16:45:08.406287 172.23.80.20    128.119.245.12  HTTP     542 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
    666 16:45:08.629580 128.119.245.12  172.23.80.20    HTTP     619 HTTP/1.1 200 OK  (text/html)
```

13、

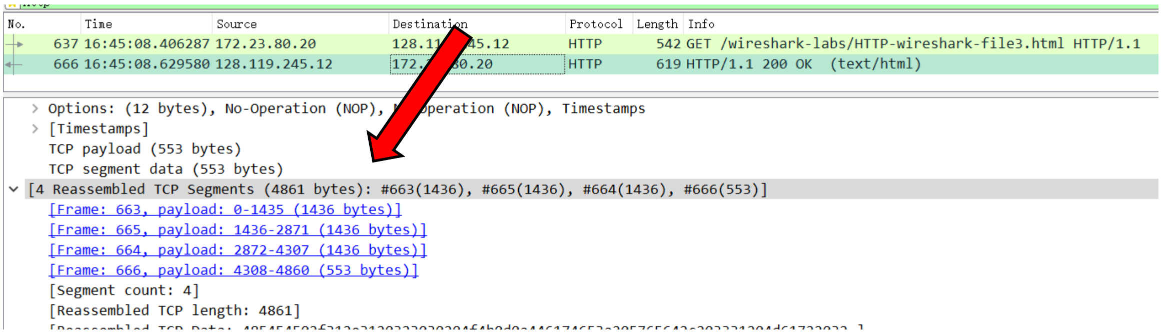
663 号数据包包含有 HTTP GET 请求的响应的状态码和描述短语

14、响应中的状态码和描述短语分别是 200 和 OK



```
    5:08.629580 172.23.146.88   172.23.255.255   DTLS    393 Continuation Data
662 16:45:08.629580 128.119.245.12  172.23.80.20  TCP     66 80 → 50904 [ACK] Seq=1 Ack=477 Win=30080 Len=0 TSval=184018648 TSecr=994568
663 16:45:08.629580 128.119.245.12  172.23.80.20  TCP   1502 80 → 50904 [ACK] Seq=1 Ack=477 Win=30080 Len=1436 TSval=184018650 TSecr=994
664 16:45:08.629580 128.119.245.12  172.23.80.20  TCP   1502 [TCP Previous segment not captured] 80 → 50904 [ACK] Seq=2873 Ack=477 Win=3
665 16:45:08.629580 128.119.245.12  172.23.80.20  TCP   1502 [TCP Out-Of-Order] 80 → 50904 [ACK] Seq=1437 Ack=477 Win=30080 Len=1436 TSv
666 16:45:08.629580 128.119.245.12  172.23.80.20  HTTP   619 HTTP/1.1 200 OK  (text/html)
```

15、需要 4 个包含数据的 TCP 段来传输单个 HTTP 响应和权利法案文本



```
No.  Time            Source          Destination     Protocol Length Info
637 16:45:08.406287 172.23.80.20    128.119.245.12  HTTP      542 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
666 16:45:08.629580 128.119.245.12  172.23.80.20    HTTP      619 HTTP/1.1 200 OK  (text/html)

  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
    TCP payload (553 bytes)
    TCP segment data (553 bytes)
v [4 Reassembled TCP Segments (4861 bytes): #663(1436), #665(1436), #664(1436), #666(553)]
    [Frame: 663, payload: 0-1435 (1436 bytes)]
    [Frame: 665, payload: 1436-2871 (1436 bytes)]
    [Frame: 664, payload: 2872-4307 (1436 bytes)]
    [Frame: 666, payload: 4308-4860 (553 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
```