CN Lab-2

1. The Basic HTTP GET/response interaction

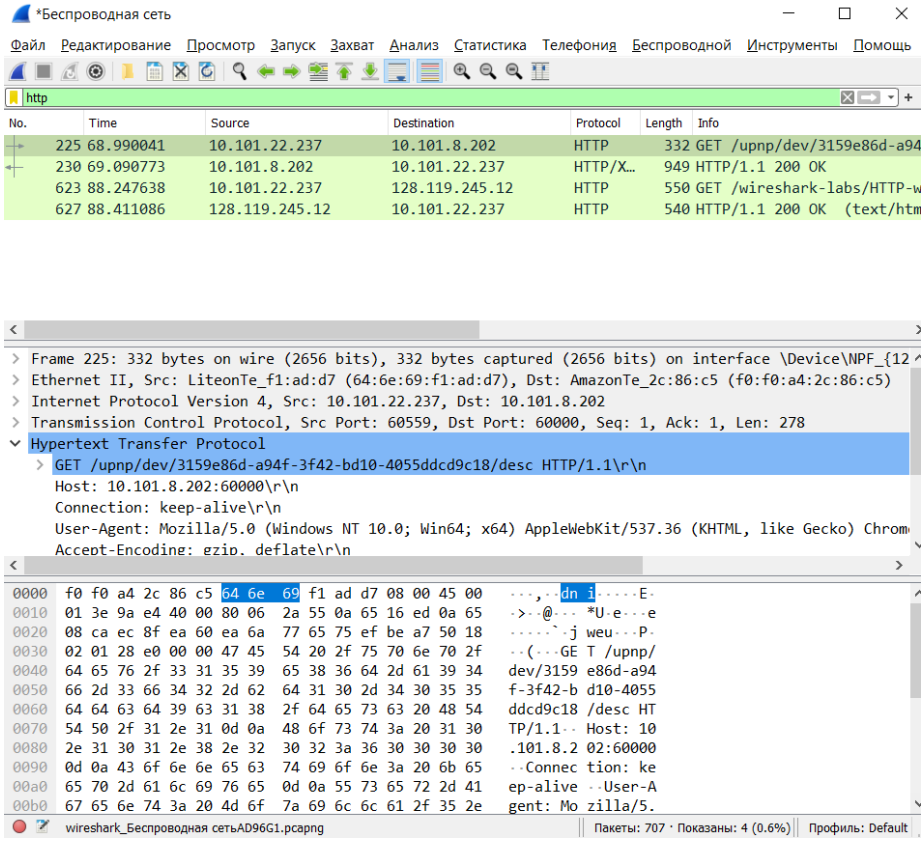


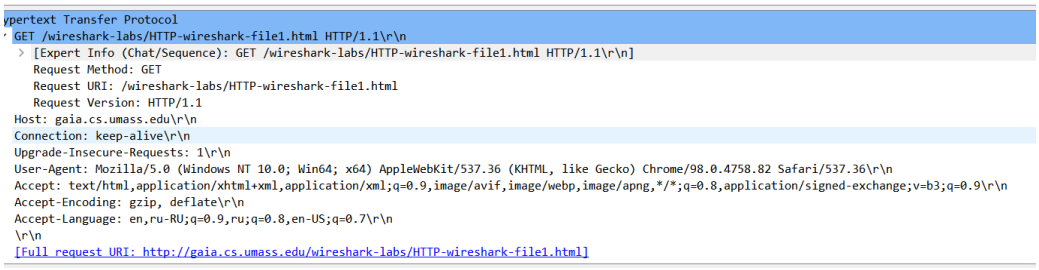
Figure 1.

1.Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer: HTTP 1.1

2.What languages (if any) does your browser indicate that it can accept to the server?

Answer: en, ru-RU, en-US.



3.What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer: My computer's IP address 10.101.22.237 and the destination is 128.119.245.12

4.What is the status code returned from the server to your browser?

Answer: 200 OK

5. When was the HTML file that you are retrieving last modified at the server?
Answer: Mon, 14 Feb 2022 06:59:01 (Figure 2)

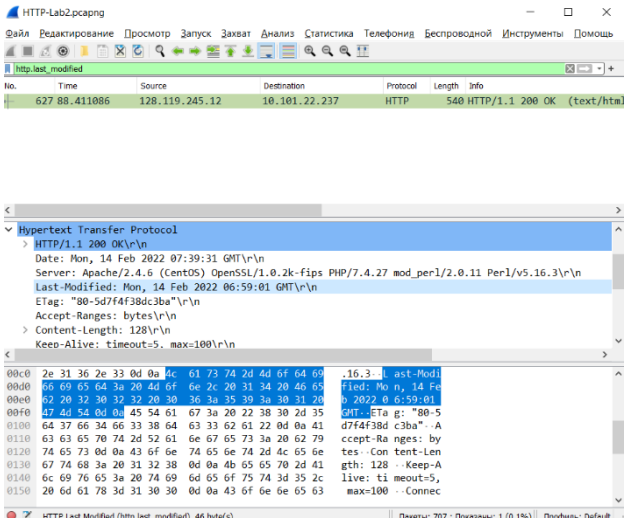


Figure 2.

6.How many bytes of content are being returned to your browser?
Answer: 895 bytes (Figure 3)

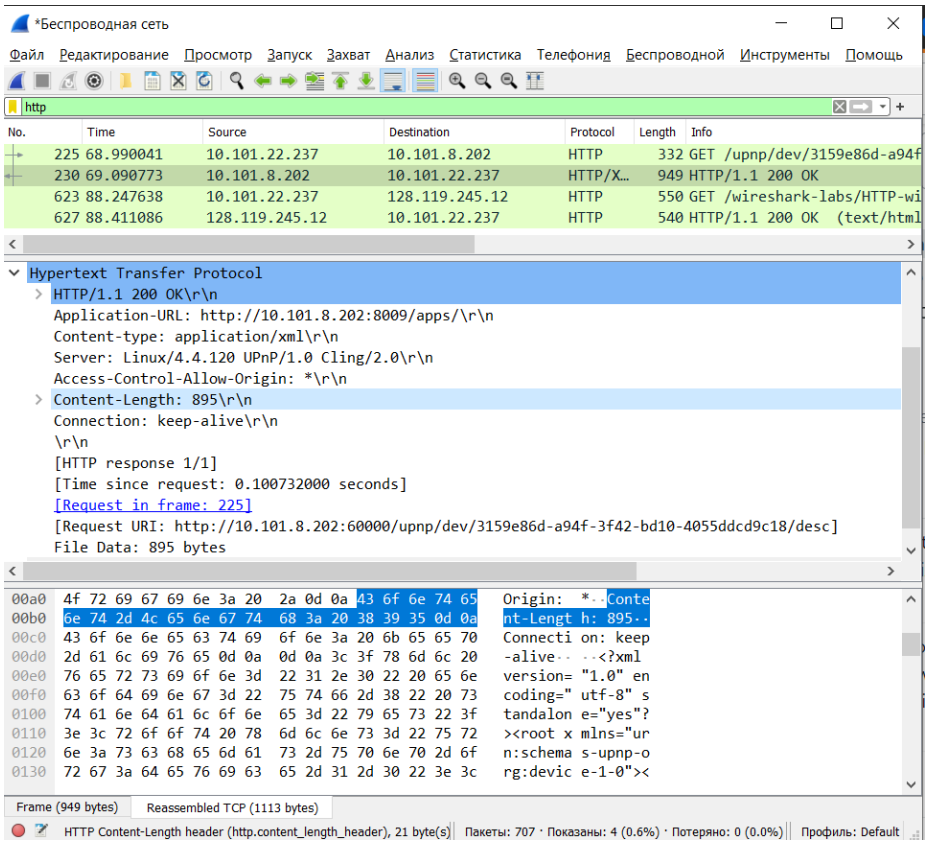


Figure 3.

7.By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Answer: No

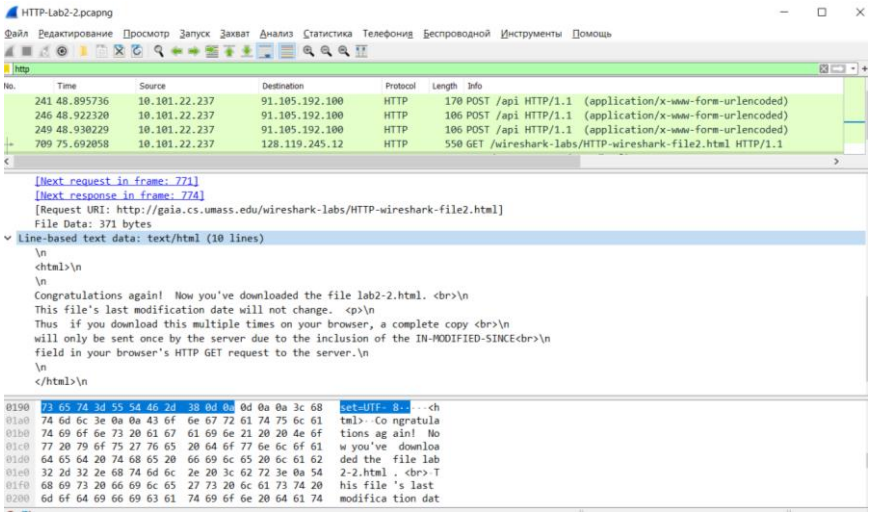
2. The HTTP CONDITIONAL GET/response interaction

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer: No

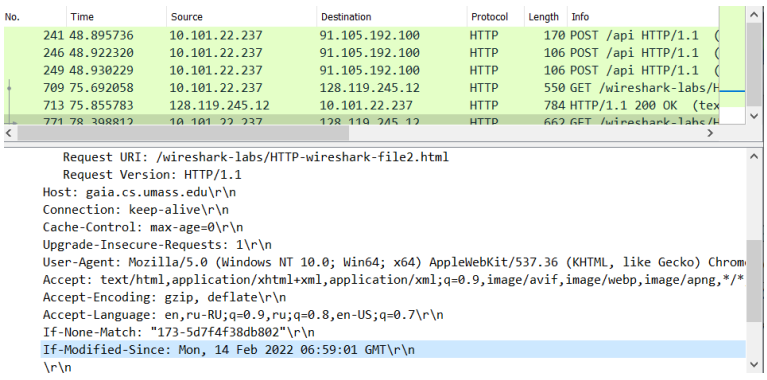
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: The server explicitly returns the contents of the file. If we expand Line-based text data, it shows the contents of the hmtl file.



10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Answer: Mon, 14 Feb 2022 06:59:01



11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain

Answer: No

3. Retrieving Long Documents

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Answer: 1 HTTP GET request messages; packet #2266 in the trace contains the GET message for the Bill or Rights.

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

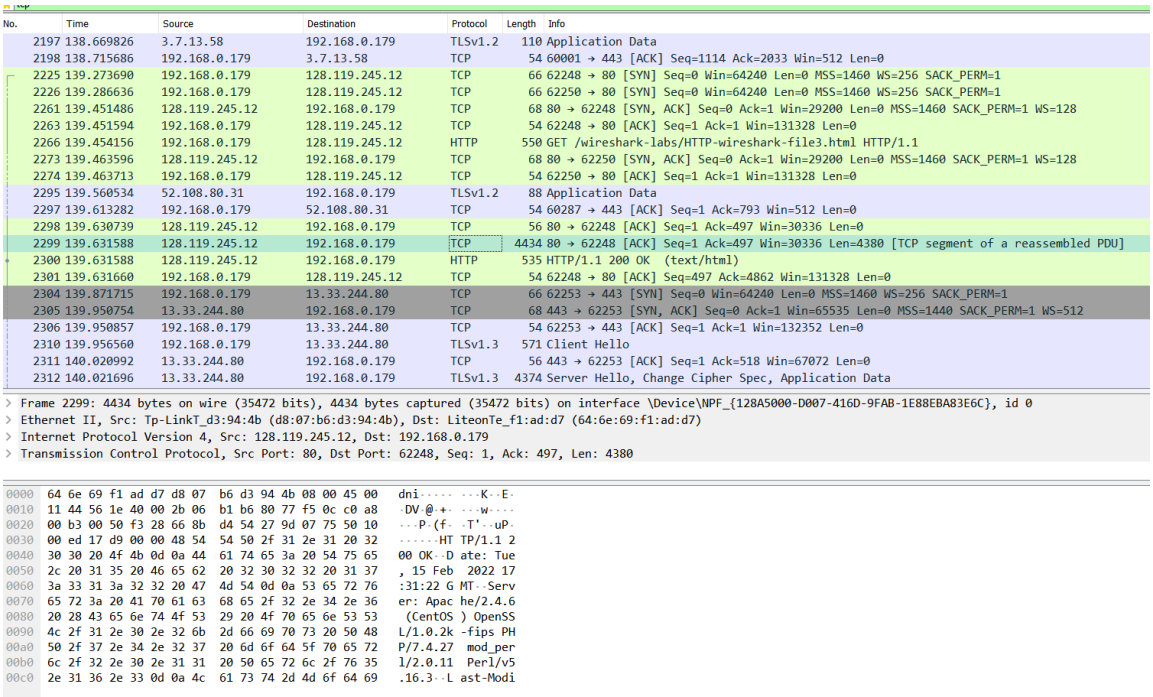
Answer: packet number 2263.

14. What is the status code and phrase in the response?

Answer: 200 OK

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answer: three data-containing TCP segments were needed: 2273, 2298, and 2299.



No.	Time	Source	Destination	Protocol	Length	Info
2197	138.669826	3.7.13.58	192.168.0.179	TLSv1.2	110	Application Data
2198	138.715686	192.168.0.179	3.7.13.58	TCP	54	60001 → 443 [ACK] Seq=1114 Ack=2033 Win=512 Len=0
2225	139.273690	192.168.0.179	128.119.245.12	TCP	66	62248 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2226	139.286636	192.168.0.179	128.119.245.12	TCP	66	62250 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2261	139.451486	128.119.245.12	192.168.0.179	TCP	68	80 → 62248 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2263	139.451594	192.168.0.179	128.119.245.12	TCP	54	62248 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
2266	139.454156	192.168.0.179	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2273	139.463596	128.119.245.12	192.168.0.179	TCP	68	80 → 62250 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
2274	139.463713	192.168.0.179	128.119.245.12	TCP	54	62250 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
2295	139.560534	52.108.80.31	192.168.0.179	TLSv1.2	88	Application Data
2297	139.613282	192.168.0.179	52.108.80.31	TCP	54	60287 → 443 [ACK] Seq=1 Ack=793 Win=512 Len=0
2298	139.630739	128.119.245.12	192.168.0.179	TCP	56	80 → 62248 [ACK] Seq=1 Ack=497 Win=30336 Len=0
2299	139.631588	128.119.245.12	192.168.0.179	TCP	4434	80 → 62248 [ACK] Seq=1 Ack=497 Win=30336 Len=4380 [TCP segment of a reassembled PDU]
2300	139.631588	128.119.245.12	192.168.0.179	HTTP	535	HTTP/1.1 200 OK (text/html)
2301	139.631660	192.168.0.179	128.119.245.12	TCP	54	62248 → 80 [ACK] Seq=497 Ack=4862 Win=131328 Len=0
2304	139.871715	192.168.0.179	13.33.244.80	TCP	66	62253 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2305	139.950754	13.33.244.80	192.168.0.179	TCP	68	443 → 62253 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM=1 WS=512
2306	139.950857	192.168.0.179	13.33.244.80	TCP	54	62253 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
2310	139.956560	192.168.0.179	13.33.244.80	TLSv1.3	571	Client Hello
2311	140.020992	13.33.244.80	192.168.0.179	TCP	56	443 → 62253 [ACK] Seq=1 Ack=518 Win=67072 Len=0
2312	140.021696	13.33.244.80	192.168.0.179	TLSv1.3	4374	Server Hello, Change Cipher Spec, Application Data

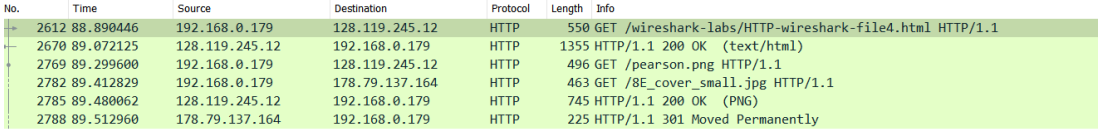
```
> Frame 2299: 4434 bytes on wire (35472 bits), 4434 bytes captured (35472 bits) on interface \Device\NPF_{128A5000-D007-416D-9FAB-1E88EBA83E6C}, id 0
> Ethernet II, Src: Tp-LinkT_d3:94:4b (d8:07:b6:d3:94:4b), Dst: LiteonTe_f1:ad:d7 (64:6e:69:f1:ad:d7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 62248, Seq: 1, Ack: 497, Len: 4380
```

```
0000  64 6e 69 f1 ad d7 d8 07  b6 d3 94 4b 08 00 45 00   dni····· ···K··E·
0010  11 44 56 1e 40 00 2b 06  b1 b6 80 77 f5 0c c0 a8   ·DV·@·+· ···w····
0020  00 b3 00 50 f3 28 66 8b  d4 54 27 9d 07 75 50 10   ···P·(f· ·T'··uP·
0030  00 ed 17 d9 00 00 48 54  54 50 2f 31 2e 31 20 32   ·····HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54 75 65   00 OK··D ate: Tue
0050  2c 20 31 35 20 46 65 62  20 32 30 32 32 20 31 37   , 15 Feb  2022 17
0060  3a 33 31 3a 32 32 20 47  4d 54 0d 0a 53 65 72 76   :31:22 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 32 37  20 6d 6f 64 5f 70 65 72   P/7.4.27  mod_per
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f 76 35   l/2.0.11  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
```

4. HTML Documents with Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: Browser sent 3 HTTP GET request messages: #2612 sent to 128.119.245.12, #2769 sent to 128.119.245.12, and #2782 sent to 178.79.137.164



No.	Time	Source	Destination	Protocol	Length	Info
2612	88.890446	192.168.0.179	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2670	89.072125	128.119.245.12	192.168.0.179	HTTP	1355	HTTP/1.1 200 OK (text/html)
2769	89.299600	192.168.0.179	128.119.245.12	HTTP	496	GET /pearson.png HTTP/1.1
2782	89.412829	192.168.0.179	178.79.137.164	HTTP	463	GET /8E_cover_small.jpg HTTP/1.1
2785	89.480062	128.119.245.12	192.168.0.179	HTTP	745	HTTP/1.1 200 OK (PNG)
2788	89.512960	178.79.137.164	192.168.0.179	HTTP	225	HTTP/1.1 301 Moved Permanently

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
Answer: They were downloaded in parallel. First image started in 2769 and ended 2785, while the second image started in 2782 and ended in 2788 packets. It shows that the second image started downloading before the first one has been downloaded.