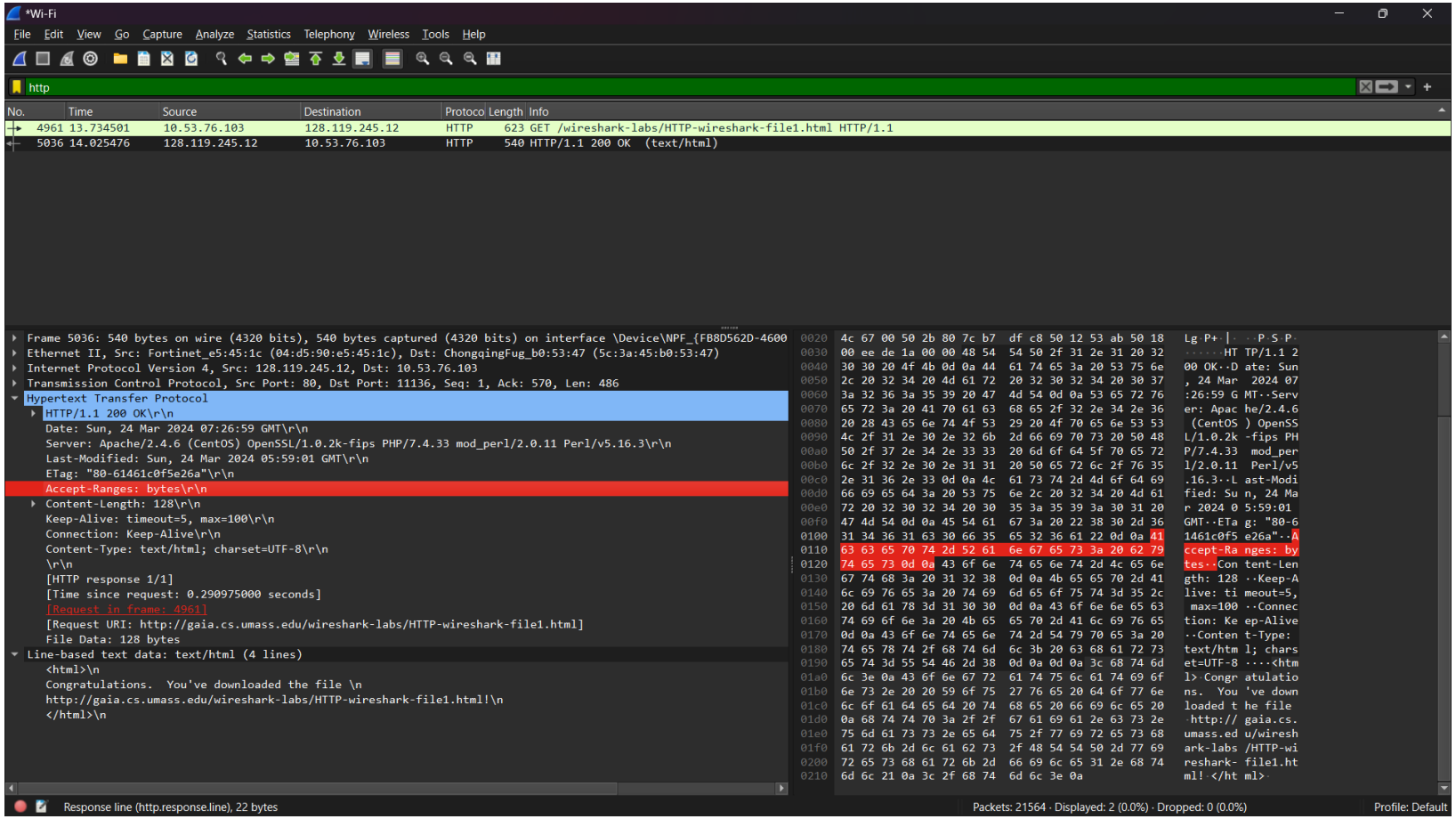
1. The Basic HTTP GET/response interaction

Yogesh P
201EE138

Figure 1: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/ HTTPwireshark-file1.html has been retrieved by your browser



1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

A: 1.1

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

A: Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n

English us, English gb

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

A: 10.53.76.103 , 128.119.245.12

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

A: 200

5. When was the HTML file that you are retrieving last modified at the server?

A: Last-Modified: Sun, 24 Mar 2024 05:59:01 GMT\r\n

6. How many bytes of content are being returned to your browser?

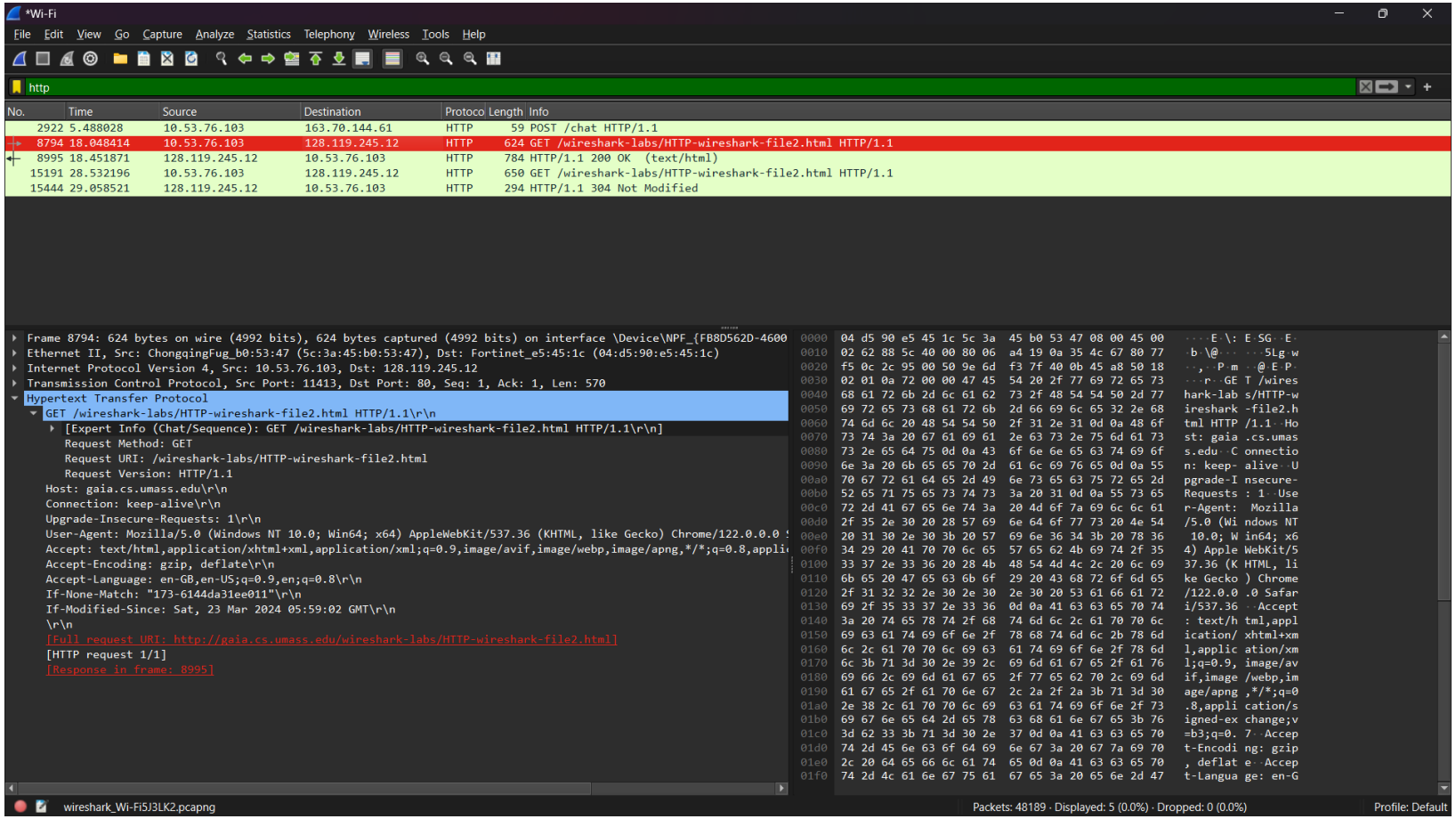
A: len:486

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.

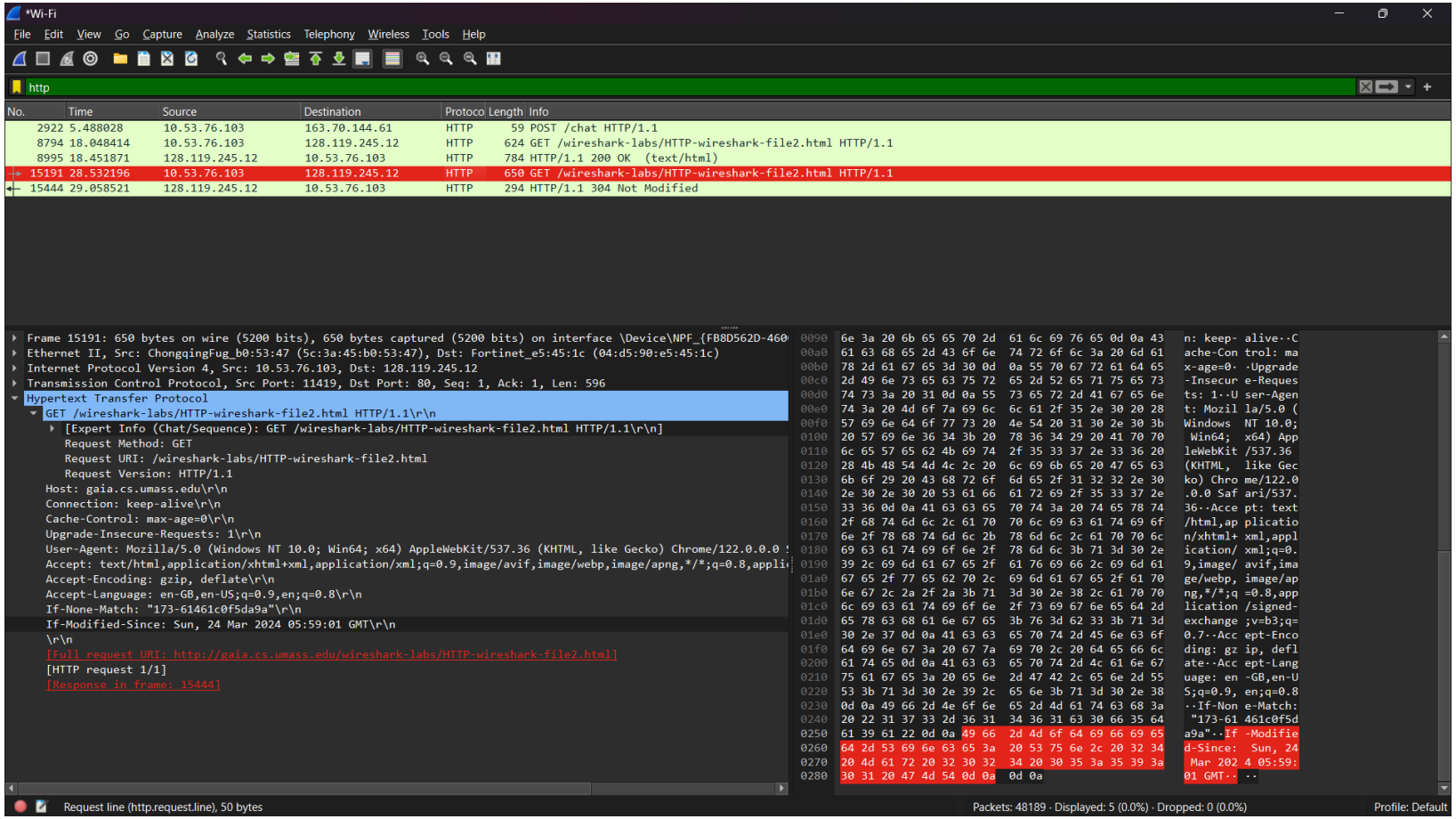
A: All headers are displayed

2. The HTTP CONDITIONAL GET/response interaction

First get

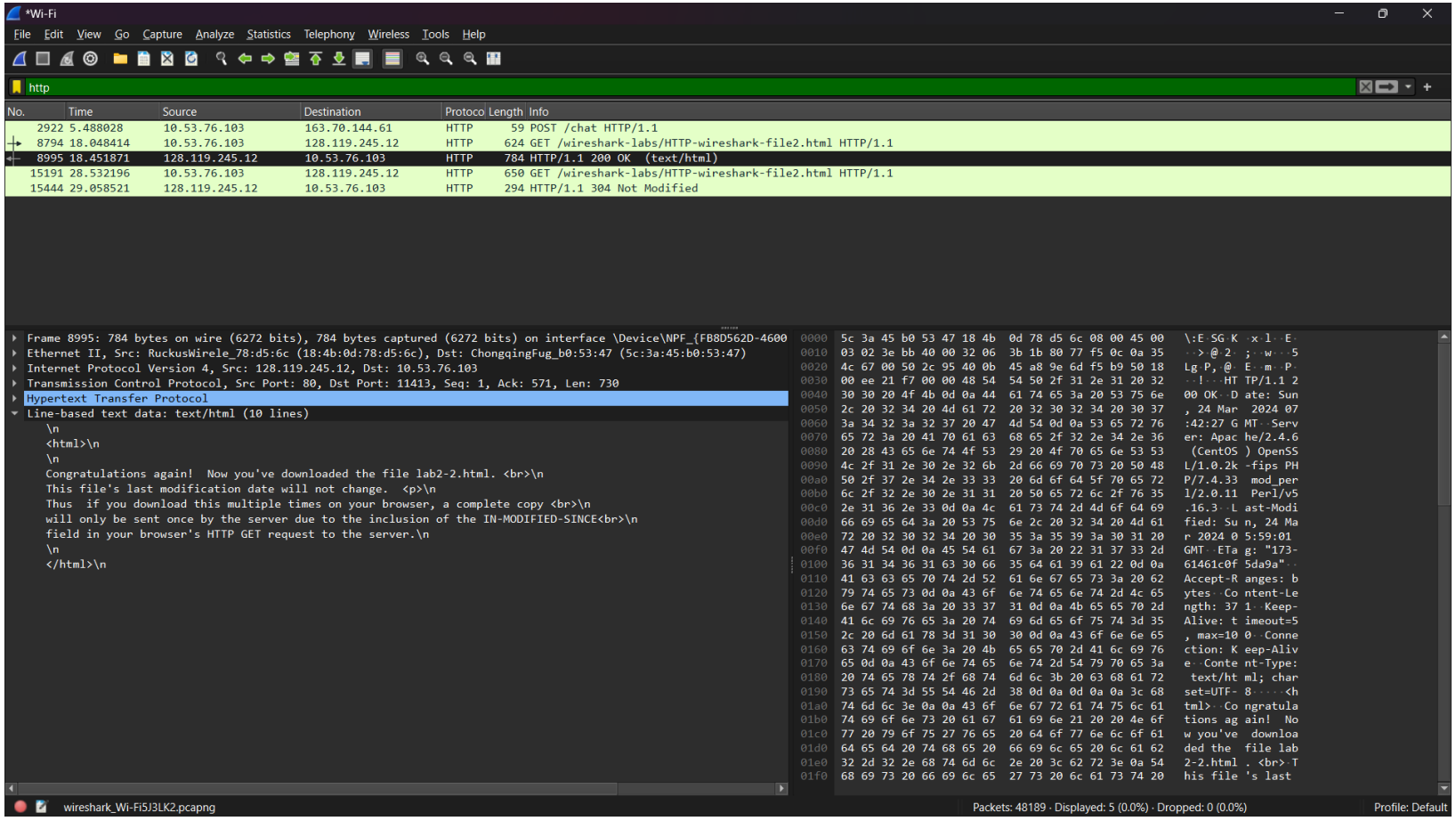

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Length Info
2922 5.488028 10.53.76.103 163.70.144.61 HTTP 59 POST /chat HTTP/1.1
8794 18.048414 10.53.76.103 128.119.245.12 HTTP 624 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
8995 18.451871 128.119.245.12 10.53.76.103 HTTP 784 HTTP/1.1 200 OK (text/html)
15191 28.532196 10.53.76.103 128.119.245.12 HTTP 650 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
15444 29.058521 128.119.245.12 10.53.76.103 HTTP 294 HTTP/1.1 304 Not Modified
Frame 8794: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits) on interface \Device\NPF_{FB8D562D-4600
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 11413, Dst Port: 80, Seq: 1, Ack: 1, Len: 570
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]
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/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
If-None-Match: "173-6144da31ee011"\r\n
If-Modified-Since: Sat, 23 Mar 2024 05:59:02 GMT\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: 8995]
0000 04 d5 90 e5 45 1c 5c 3a 45 b0 53 47 08 00 45 00 ····E·\: E·SG··E·
0010 02 62 88 5c 40 00 80 06 a4 19 0a 35 4c 67 80 77 ·b·\@··· ···5Lg·w
0020 f5 0c 2c 95 00 50 9e 6d f3 7f 40 0b 45 a8 50 18 ··,··P·m ··@·E·P·
0030 02 01 0a 72 00 00 47 45 54 20 2f 77 69 72 65 73 ···r··GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 32 2e 68 ireshark -file2.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1··Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu··C onnectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive··U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1··Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6
00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
0120 2f 31 32 32 2e 30 2e 30 2e 30 20 53 61 66 61 72 /122.0.0 .0 Safar
0130 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 i/537.36 ··Accept
0140 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl
0150 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/ xhtml+xm
0160 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,applic ation/xm
0170 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 l;q=0.9, image/av
0180 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d if,image /webp,im
0190 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 age/apng ,*/*;q=0
01a0 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 .8,appli cation/s
01b0 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 igned-ex change;v
01c0 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 63 65 70 =b3;q=0. 7··Accep
01d0 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encodi ng: gzip
01e0 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 , deflat e··Accep
01f0 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 47 t-Langua ge: en-G
wireshark_Wi-Fi5J3LK2.pcapng
Packets: 48189 · Displayed: 5 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

Second get


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
2922 5.488028 10.53.76.103 163.70.144.61 HTTP 59 POST /chat HTTP/1.1
8794 18.048414 10.53.76.103 128.119.245.12 HTTP 624 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
8995 18.451871 128.119.245.12 10.53.76.103 HTTP 784 HTTP/1.1 200 OK (text/html)
15191 28.532196 10.53.76.103 128.119.245.12 HTTP 650 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
15444 29.058521 128.119.245.12 10.53.76.103 HTTP 294 HTTP/1.1 304 Not Modified
Frame 15191: 650 bytes on wire (5200 bits), 650 bytes captured (5200 bits) on interface \Device\NPF_{FB8D562D-460
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 11419, Dst Port: 80, Seq: 1, Ack: 1, Len: 596
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]
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
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/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
If-None-Match: "173-61461c0f5da9a"\r\n
If-Modified-Since: Sun, 24 Mar 2024 05:59:01 GMT\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: 15444]
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 n: keep- alive··C
00a0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Con trol: ma
00b0 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65 x-age=0· ·Upgrade
00c0 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecur e-Reques
00d0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e ts: 1··U ser-Agen
00e0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00f0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
0100 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64; x64) App
0110 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit /537.36
0120 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec
0130 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 32 32 2e 30 ko) Chro me/122.0
0140 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e .0.0 Saf ari/537.
0150 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 36··Acce pt: text
0160 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
0170 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
0180 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
0190 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 9,image/ avif,ima
01a0 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 ge/webp, image/ap
01b0 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 ng,*/*;q =0.8,app
01c0 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d lication /signed-
01d0 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d exchange ;v=b3;q=
01e0 30 2e 37 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 0.7··Acc ept-Enco
01f0 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
0200 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 ate··Acc ept-Lang
0210 75 61 67 65 3a 20 65 6e 2d 47 42 2c 65 6e 2d 55 uage: en -GB,en-U
0220 53 3b 71 3d 30 2e 39 2c 65 6e 3b 71 3d 30 2e 38 S;q=0.9, en;q=0.8
0230 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a ··If-Non e-Match:
0240 20 22 31 37 33 2d 36 31 34 36 31 63 30 66 35 64 "173-61 461c0f5d
0250 61 39 61 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 a9a"··If -Modifie
0260 64 2d 53 69 6e 63 65 3a 20 53 75 6e 2c 20 32 34 d-Since: Sun, 24
0270 20 4d 61 72 20 32 30 32 34 20 30 35 3a 35 39 3a Mar 202 4 05:59:
0280 30 31 20 47 4d 54 0d 0a 0d 0a 01 GMT·· ··
Request line (http.request.line), 50 bytes
Packets: 48189 · Displayed: 5 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

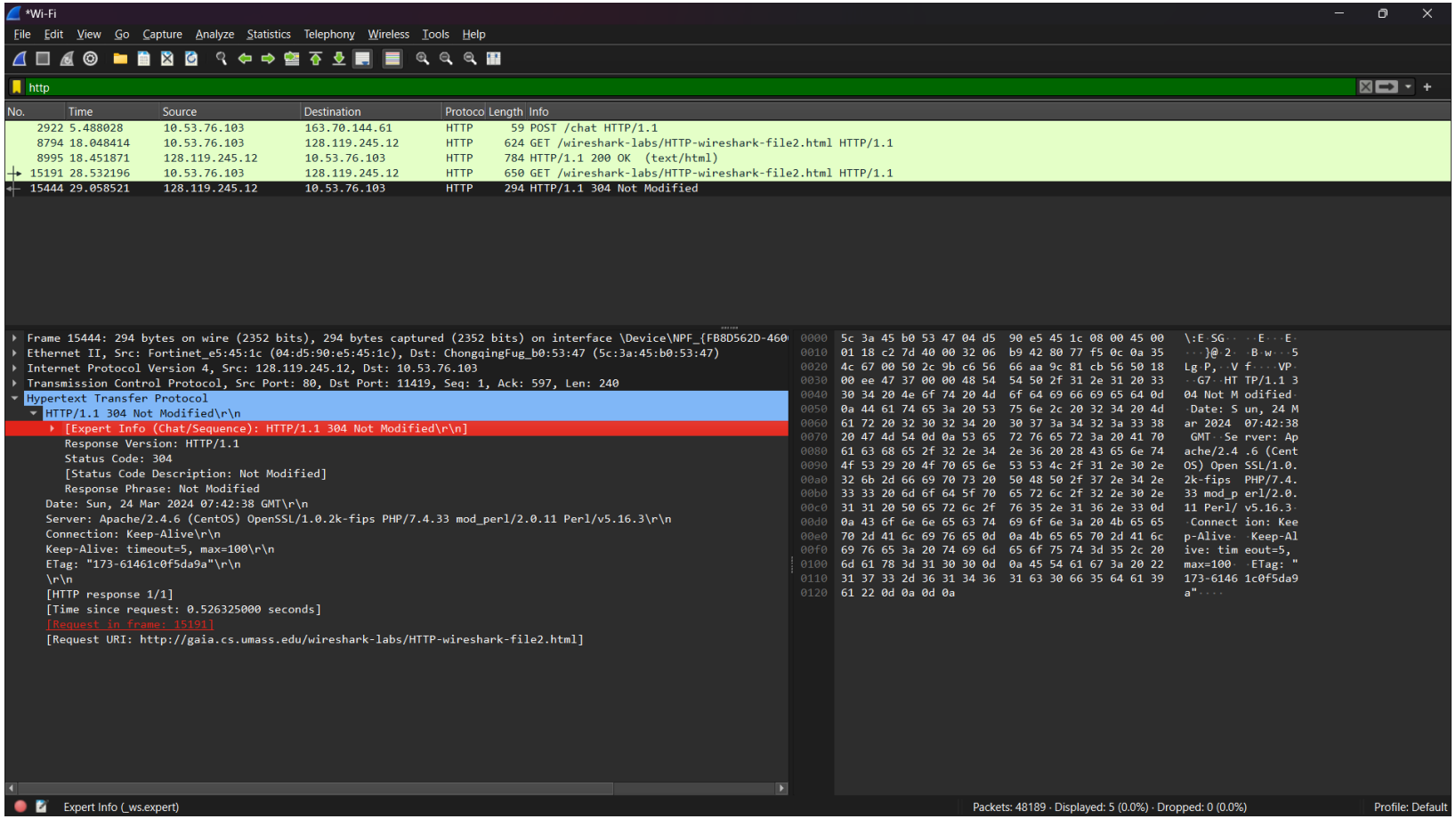
First response contents

Figure 2: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/ HTTPwireshark-file2.html has been retrieved by your browser



Second response contents

Figure 3: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/ HTTPwireshark-file2.html has been refreshed again



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?

A: No

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

A: Yes, Line-based text data: text/html (10 lines), shown before

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 GET6 ? If so, what information follows the “IF-MODIFIED-SINCE:” header?

A:Yes, If-Modified-Since: Sun, 24 Mar 2024 05:59:01 GMT\r\n

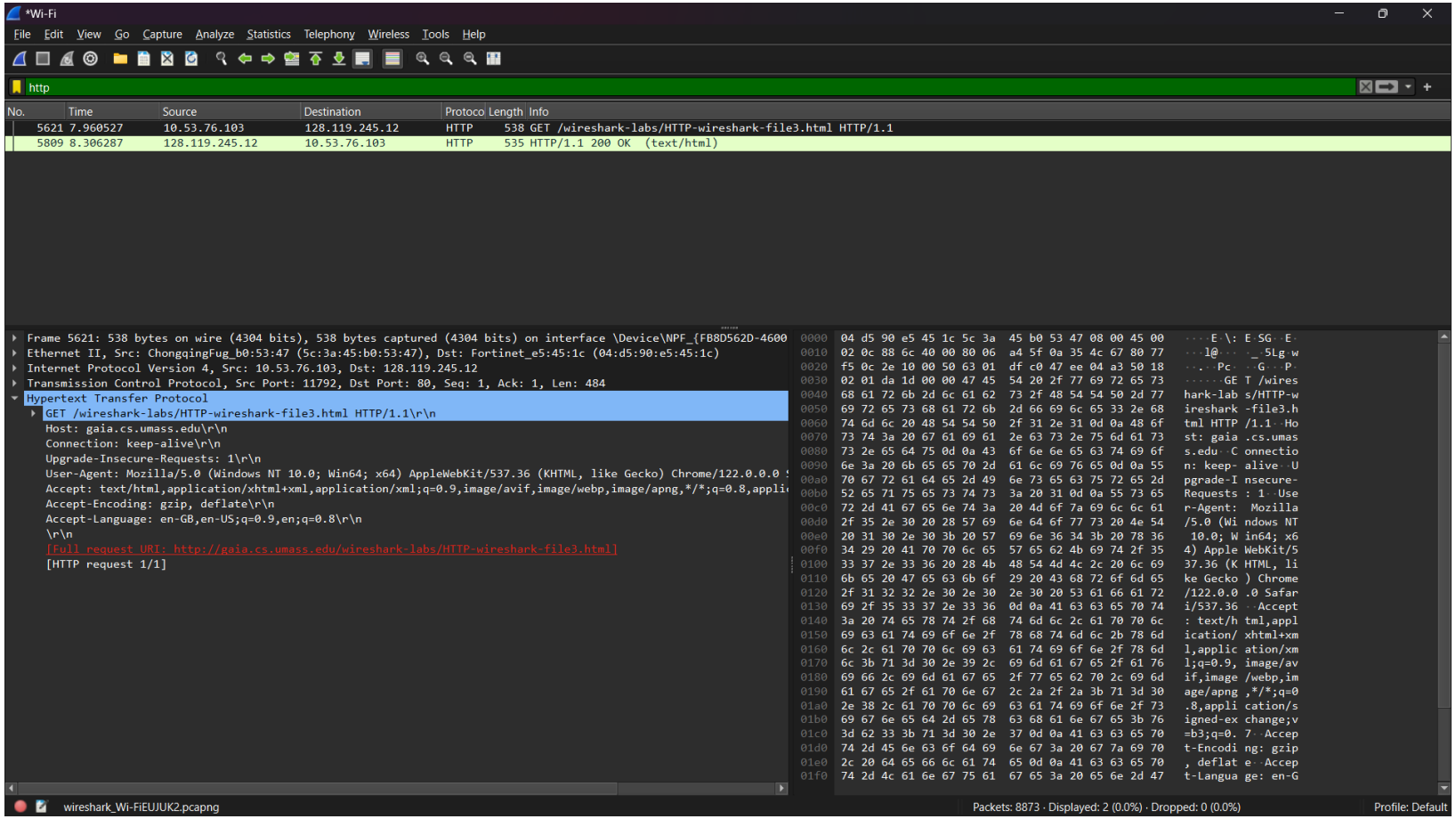
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

A:The response was “304 Not Modified” for the second HTTP GET request.

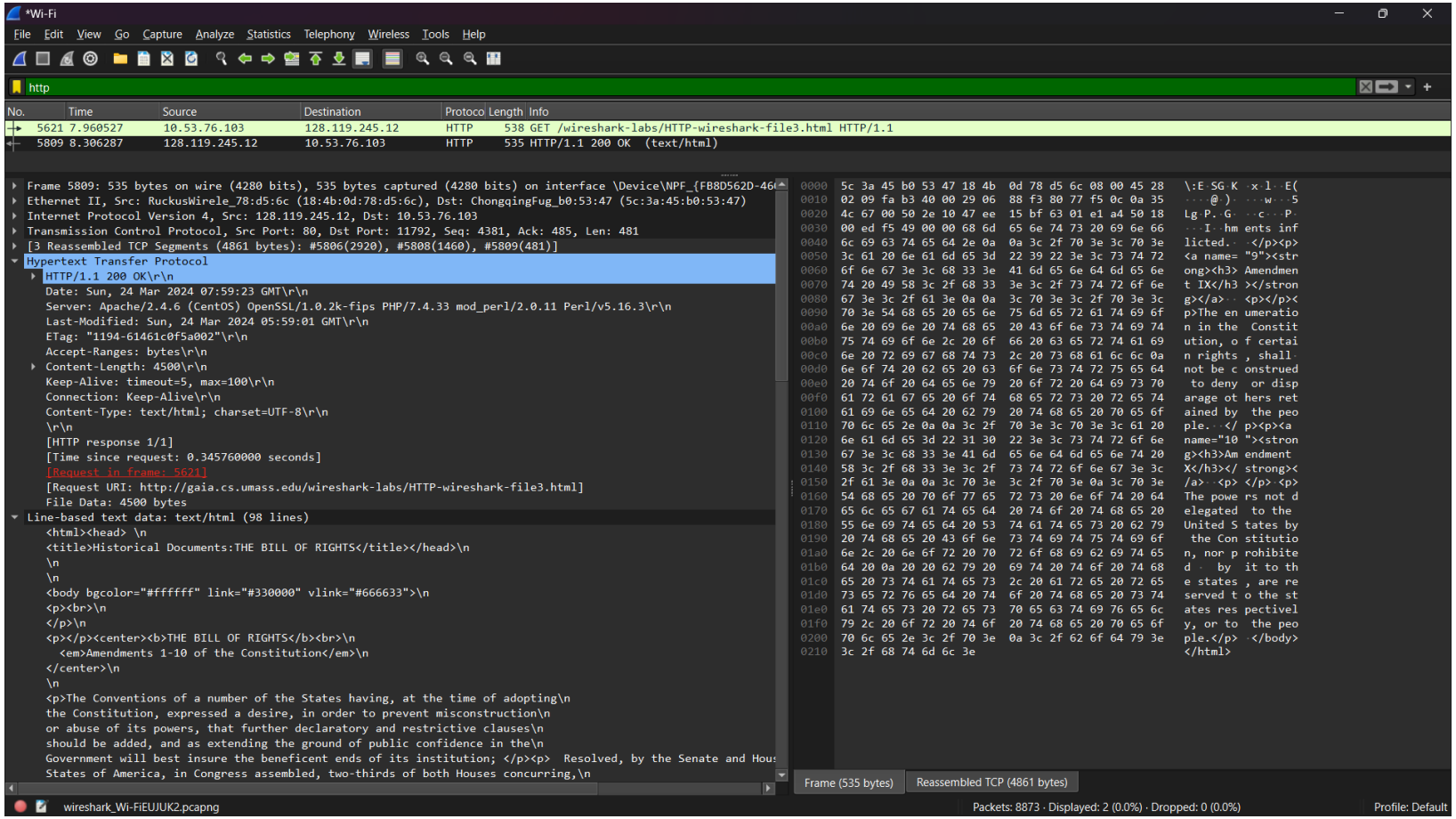
The server did not return explicitly the contents of the file. It was picked from the browser cache.

3. Retrieving Long Documents

get


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Length Info
5621 7.960527 10.53.76.103 128.119.245.12 HTTP 538 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
5809 8.306287 128.119.245.12 10.53.76.103 HTTP 535 HTTP/1.1 200 OK (text/html)
Frame 5621: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{FB8D562D-4600
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 11792, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file3.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/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[HTTP request 1/1]
0000 04 d5 90 e5 45 1c 5c 3a 45 b0 53 47 08 00 45 00 ····E·\: E·SG··E·
0010 02 0c 88 6c 40 00 80 06 a4 5f 0a 35 4c 67 80 77 ···l@··· ·_·5Lg·w
0020 f5 0c 2e 10 00 50 63 01 df c0 47 ee 04 a3 50 18 ·····Pc· ··G···P·
0030 02 01 da 1d 00 00 47 45 54 20 2f 77 69 72 65 73 ·····GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 33 2e 68 ireshark -file3.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1··Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu··C onnectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive··U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1··Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6
00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
0120 2f 31 32 32 2e 30 2e 30 2e 30 20 53 61 66 61 72 /122.0.0 .0 Safar
0130 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 i/537.36 ··Accept
0140 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl
0150 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/ xhtml+xm
0160 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,applic ation/xm
0170 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 l;q=0.9, image/av
0180 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d if,image /webp,im
0190 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 age/apng ,*/*;q=0
01a0 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 .8,appli cation/s
01b0 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 igned-ex change;v
01c0 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 63 65 70 =b3;q=0. 7··Accep
01d0 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encodi ng: gzip
01e0 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 , deflat e··Accep
01f0 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 47 t-Langua ge: en-G
wireshark_Wi-FiEUJUK2.pcapng
Packets: 8873 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

response


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Length Info
5621 7.960527 10.53.76.103 128.119.245.12 HTTP 538 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
5809 8.306287 128.119.245.12 10.53.76.103 HTTP 535 HTTP/1.1 200 OK (text/html)
Frame 5809: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{FB8D562D-46
Ethernet II, Src: RuckusWirele_78:d5:6c (18:4b:0d:78:d5:6c), Dst: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.53.76.103
Transmission Control Protocol, Src Port: 80, Dst Port: 11792, Seq: 4381, Ack: 485, Len: 481
[3 Reassembled TCP Segments (4861 bytes): #5806(2920), #5808(1460), #5809(481)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 24 Mar 2024 07:59:23 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
Last-Modified: Sun, 24 Mar 2024 05:59:01 GMT\r\n
ETag: "1194-61461c0f5a002"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 4500\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 1/1]
[Time since request: 0.345760000 seconds]
[Request in frame: 5621]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
File Data: 4500 bytes
Line-based text data: text/html (98 lines)
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
\n
\n
<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n

\n
\n
THE BILL OF RIGHTS
\n
Amendments 1-10 of the Constitution\n
\n
\n
The Conventions of a number of the States having, at the time of adopting\n
the Constitution, expressed a desire, in order to prevent misconstruction\n
or abuse of its powers, that further declaratory and restrictive clauses\n
should be added, and as extending the ground of public confidence in the\n
Government will best insure the beneficent ends of its institution; Resolved, by the Senate and Hous
States of America, in Congress assembled, two-thirds of both Houses concurring,\n
0000 5c 3a 45 b0 53 47 18 4b 0d 78 d5 6c 08 00 45 28 \:E SG K x l E(
0010 02 09 fa b3 40 00 29 06 88 f3 80 77 f5 0c 0a 35 @) w 5
0020 4c 67 00 50 2e 10 47 ee 15 bf 63 01 e1 a4 50 18 Lg P G c P
0030 00 ed f5 49 00 00 68 6d 65 6e 74 73 20 69 6e 66 I hm ents inf
0040 6c 69 63 74 65 64 2e 0a 0a 3c 2f 70 3e 3c 70 3e licted.
0050 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 <str
0060 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e ong><h3> Amendmen
0070 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e t IX</h3 ></stron
0080 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c g> <
0090 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f p>The en umeratio
00a0 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 n in the Constit
00b0 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 ution, o f certai
00c0 6e 20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a n rights , shall
00d0 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64 not be c onstrued
00e0 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 69 73 70 to deny or disp
00f0 61 72 61 67 65 20 6f 74 68 65 72 73 20 72 65 74 arage ot hers ret
0100 61 69 6e 65 64 20 62 79 20 74 68 65 20 70 65 6f ained by the peo
0110 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c 61 20 ple. </ p> <a
0120 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 72 6f 6e name="10 "><stron
0130 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e 74 20 g><h3>Am endment
0140 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e 67 3e 3c X</h3></ strong><
0150 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 0a 3c 70 3e /a>
0160 54 68 65 20 70 6f 77 65 72 73 20 6e 6f 74 20 64 The powe rs not d
0170 65 6c 65 67 61 74 65 64 20 74 6f 20 74 68 65 20 elegated to the
0180 55 6e 69 74 65 64 20 53 74 61 74 65 73 20 62 79 United S tates by
0190 20 74 68 65 20 43 6f 6e 73 74 69 74 75 74 69 6f the Con stitutio
01a0 6e 2c 20 6e 6f 72 20 70 72 6f 68 69 62 69 74 65 n, nor p rohibite
01b0 64 20 0a 20 20 62 79 20 69 74 20 74 6f 20 74 68 d by it to th
01c0 65 20 73 74 61 74 65 73 2c 20 61 72 65 20 72 65 e states , are re
01d0 73 65 72 76 65 64 20 74 6f 20 74 68 65 20 73 74 served t o the st
01e0 61 74 65 73 20 72 65 73 70 65 63 74 69 76 65 6c ates res pectivel
01f0 79 2c 20 6f 72 20 74 6f 20 74 68 65 20 70 65 6f y, or to the peo
0200 70 6c 65 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e ple. </body>
0210 3c 2f 68 74 6d 6c 3e </html>
Frame (535 bytes)
Reassembled TCP (4861 bytes)
wireshark_Wi-FiEUJUK2.pcapng
Packets: 8873 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

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?

A: One request ,5621

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

A: 5809, HTTP/1.1 200 OK (text/html)

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

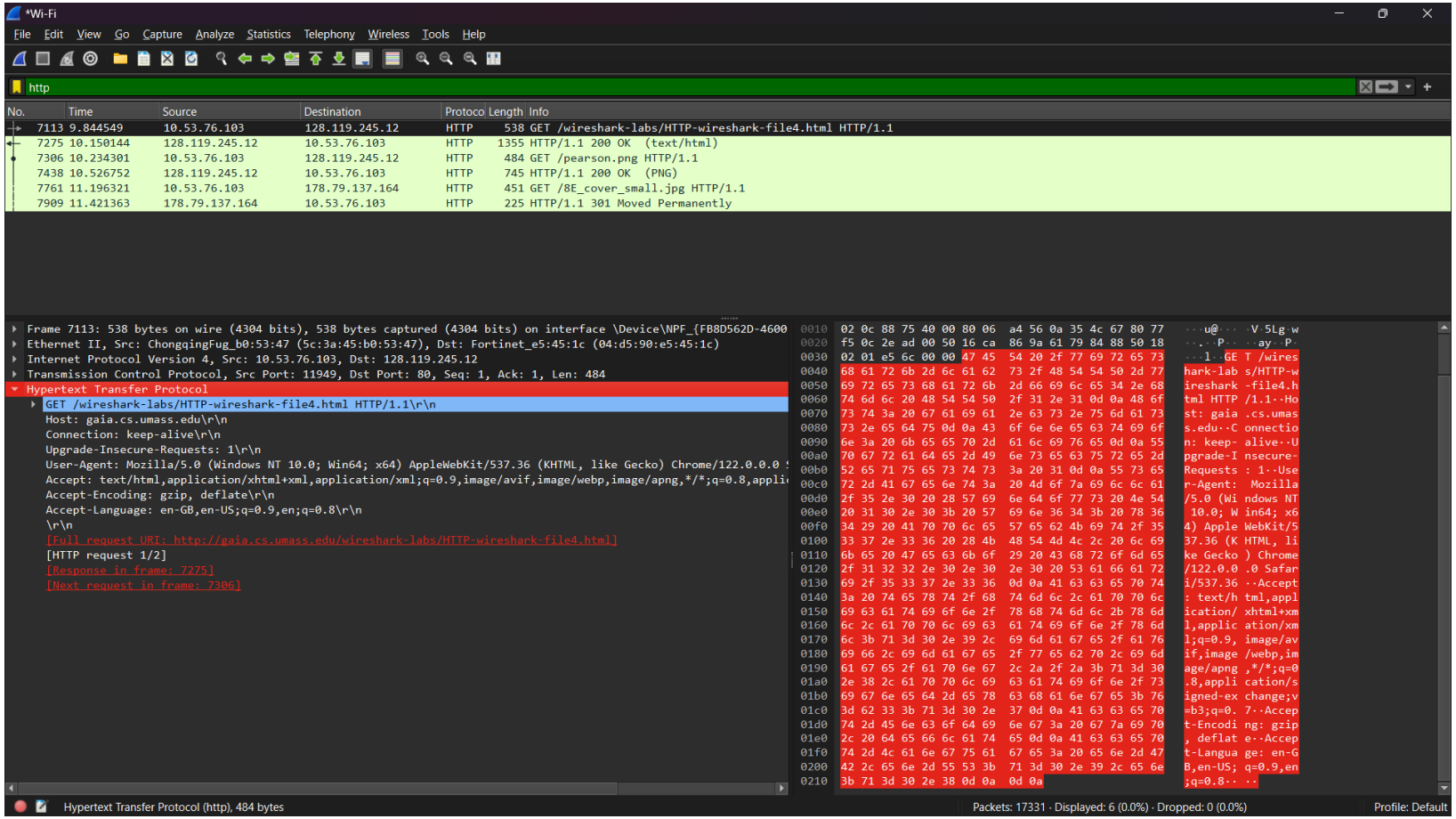
A: HTTP/1.1 200 OK (text/html)

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

A: Three data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

4. HTML Documents with Embedded Objects

First get


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Length Info
7113 9.844549 10.53.76.103 128.119.245.12 HTTP 538 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
7275 10.150144 128.119.245.12 10.53.76.103 HTTP 1355 HTTP/1.1 200 OK (text/html)
7306 10.234301 10.53.76.103 128.119.245.12 HTTP 484 GET /pearson.png HTTP/1.1
7438 10.526752 128.119.245.12 10.53.76.103 HTTP 745 HTTP/1.1 200 OK (PNG)
7761 11.196321 10.53.76.103 178.79.137.164 HTTP 451 GET /8E_cover_small.jpg HTTP/1.1
7909 11.421363 178.79.137.164 10.53.76.103 HTTP 225 HTTP/1.1 301 Moved Permanently
Frame 7113: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{FB8D562D-4600
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 11949, Dst Port: 80, Seq: 1, Ack: 1, Len: 484
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file4.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/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[HTTP request 1/2]
[Response in frame: 7275]
[Next request in frame: 7306]
0010 02 0c 88 75 40 00 80 06 a4 56 0a 35 4c 67 80 77 ···u@··· ·V·5Lg·w
0020 f5 0c 2e ad 00 50 16 ca 86 9a 61 79 84 88 50 18 ·····P·· ··ay··P·
0030 02 01 e5 6c 00 00 47 45 54 20 2f 77 69 72 65 73 ···l··GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 34 2e 68 ireshark -file4.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1··Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu··C onnectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive··U
00a0 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure-
00b0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1··Use
00c0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla
00d0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /5.0 (Wi ndows NT
00e0 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 10.0; W in64; x6
00f0 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 4) Apple WebKit/5
0100 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 37.36 (K HTML, li
0110 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 ke Gecko) Chrome
0120 2f 31 32 32 2e 30 2e 30 2e 30 20 53 61 66 61 72 /122.0.0 .0 Safar
0130 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 i/537.36 ··Accept
0140 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c : text/h tml,appl
0150 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d ication/ xhtml+xm
0160 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d l,applic ation/xm
0170 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 l;q=0.9, image/av
0180 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d if,image /webp,im
0190 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 age/apng ,*/*;q=0
01a0 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 .8,appli cation/s
01b0 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 igned-ex change;v
01c0 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 63 65 70 =b3;q=0. 7··Accep
01d0 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encodi ng: gzip
01e0 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 , deflat e··Accep
01f0 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d 47 t-Langua ge: en-G
0200 42 2c 65 6e 2d 55 53 3b 71 3d 30 2e 39 2c 65 6e B,en-US; q=0.9,en
0210 3b 71 3d 30 2e 38 0d 0a 0d 0a ;q=0.8·· ··
Hypertext Transfer Protocol (http), 484 bytes
Packets: 17331 · Displayed: 6 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

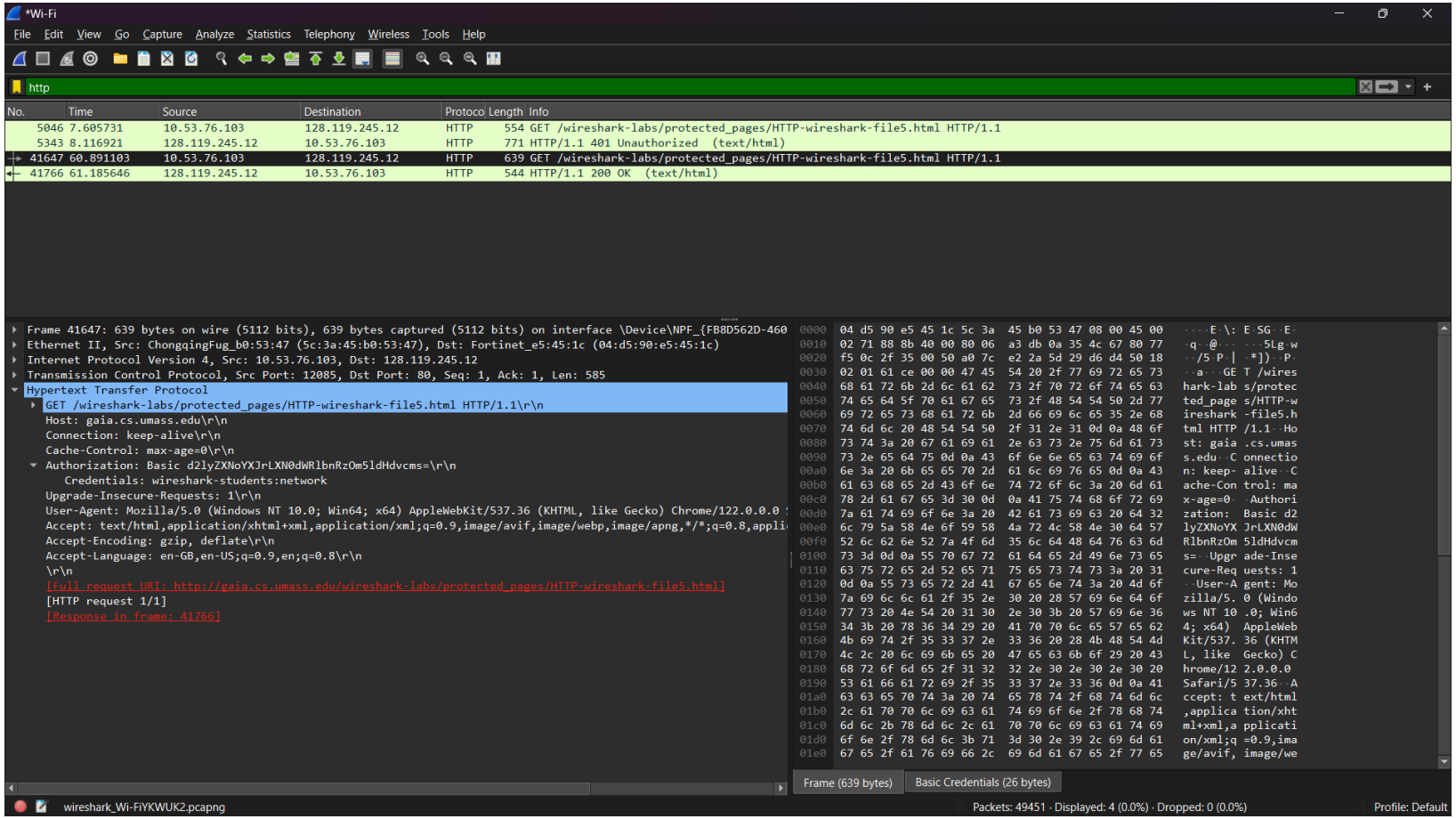
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

A: Three,128.119.245.12, 128.119.245.12, 178.79.137.164

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.

A: The two images were downloaded serially. Based on the timestamps from the previous screenshot, we observe that the second image is downloaded after receiving confirmation that the first image is downloaded.

5.HTTP Authentication


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Length Info
5046 7.605731 10.53.76.103 128.119.245.12 HTTP 554 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
5343 8.116921 128.119.245.12 10.53.76.103 HTTP 771 HTTP/1.1 401 Unauthorized (text/html)
41647 60.891103 10.53.76.103 128.119.245.12 HTTP 639 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
41766 61.185646 128.119.245.12 10.53.76.103 HTTP 544 HTTP/1.1 200 OK (text/html)
Frame 41647: 639 bytes on wire (5112 bits), 639 bytes captured (5112 bits) on interface \Device\NPF_{FB8D562D-460
Ethernet II, Src: ChongqingFug_b0:53:47 (5c:3a:45:b0:53:47), Dst: Fortinet_e5:45:1c (04:d5:90:e5:45:1c)
Internet Protocol Version 4, Src: 10.53.76.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 12085, Dst Port: 80, Seq: 1, Ack: 1, Len: 585
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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appli
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 41766]
0000 04 d5 90 e5 45 1c 5c 3a 45 b0 53 47 08 00 45 00 ····E·\: E·SG··E·
0010 02 71 88 8b 40 00 80 06 a3 db 0a 35 4c 67 80 77 ·q··@··· ···5Lg·w
0020 f5 0c 2f 35 00 50 a0 7c e2 2a 5d 29 d6 d4 50 18 ··/5·P·| ·*])··P·
0030 02 01 61 ce 00 00 47 45 54 20 2f 77 69 72 65 73 ··a···GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 70 72 6f 74 65 63 hark-lab s/protec
0050 74 65 64 5f 70 61 67 65 73 2f 48 54 54 50 2d 77 ted_page s/HTTP-w
0060 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 35 2e 68 ireshark -file5.h
0070 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1··Ho
0080 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0090 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu··C onnectio
00a0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 n: keep- alive··C
00b0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 ache-Con trol: ma
00c0 78 2d 61 67 65 3d 30 0d 0a 41 75 74 68 6f 72 69 x-age=0·· ·Authori
00d0 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 64 32 zation: Basic d2
00e0 6c 79 5a 58 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 lyZXNoYX JrLXN0dW
00f0 52 6c 62 6e 52 7a 4f 6d 35 6c 64 48 64 76 63 6d RlbnRzOm 5ldHdvcm
0100 73 3d 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 s=··Upgr ade-Inse
0110 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
0120 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ··User-A gent: Mo
0130 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo
0140 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 ws NT 10 .0; Win6
0150 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4; x64) AppleWeb
0160 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d Kit/537. 36 (KHTM
0170 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 L, like Gecko) C
0180 68 72 6f 6d 65 2f 31 32 32 2e 30 2e 30 2e 30 20 hrome/12 2.0.0.0
0190 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36··A
01a0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html
01b0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht
01c0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml,a pplicati
01d0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima
01e0 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 ge/avif, image/we
Frame (639 bytes)
Basic Credentials (26 bytes)
wireshark_Wi-FiYKWUK2.pcapng
Packets: 49451 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

A: HTTP/1.1 401 Unauthorized\r\n

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

A: Credentials