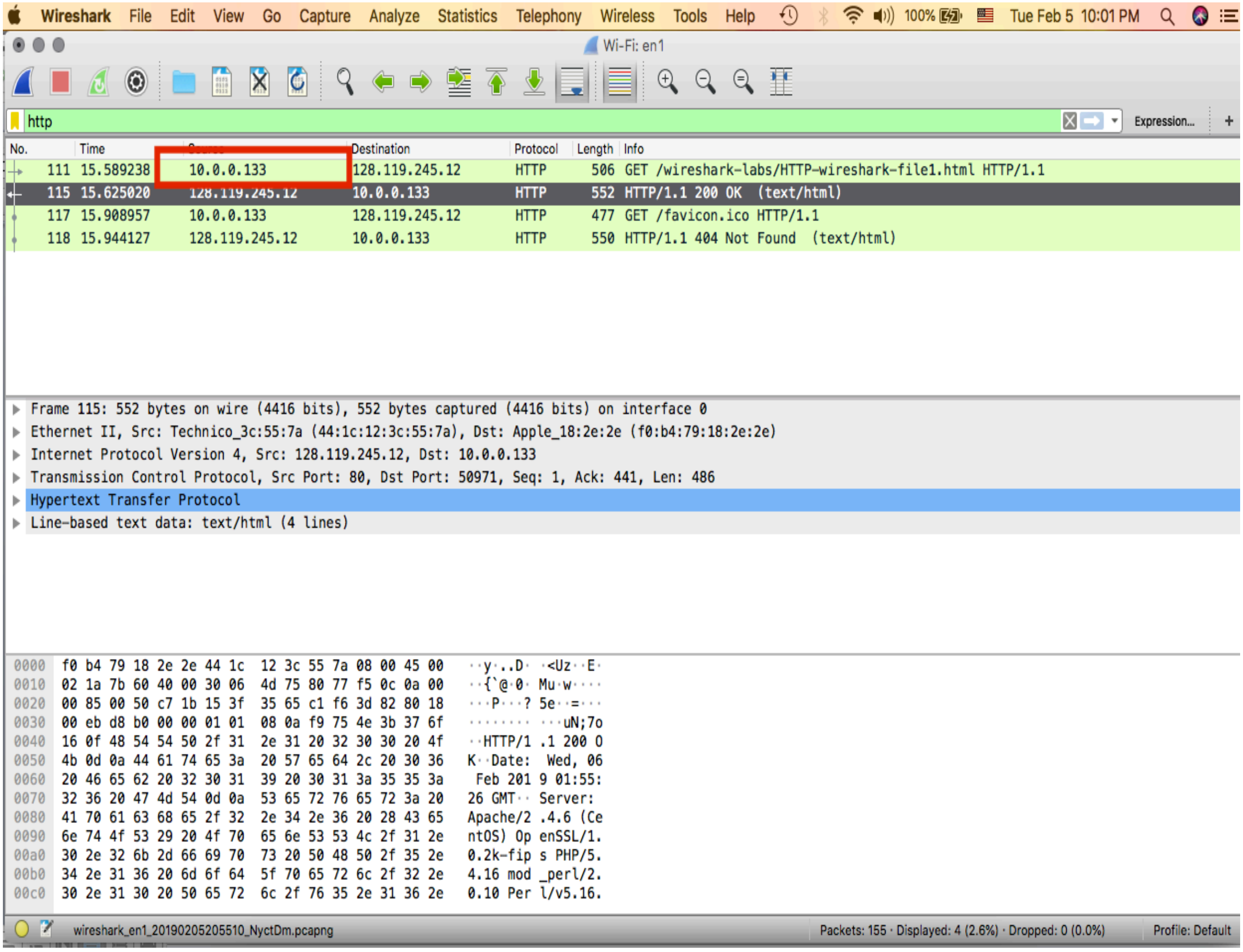
Shahad bin himd
IT520
LAB2

IP ADDRESS 10.0.0.133


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
100% Tue Feb 5 10:01 PM
Wi-Fi: en1
Expression...
+

```
http
```

```
No.   Time       Source          Destination     Protocol Length Info
  111 15.589238  10.0.0.133      128.119.245.12  HTTP      506  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  115 15.625020  128.119.245.12  10.0.0.133      HTTP      552  HTTP/1.1 200 OK  (text/html)
  117 15.908957  10.0.0.133      128.119.245.12  HTTP      477  GET /favicon.ico HTTP/1.1
  118 15.944127  128.119.245.12  10.0.0.133      HTTP      550  HTTP/1.1 404 Not Found  (text/html)
```

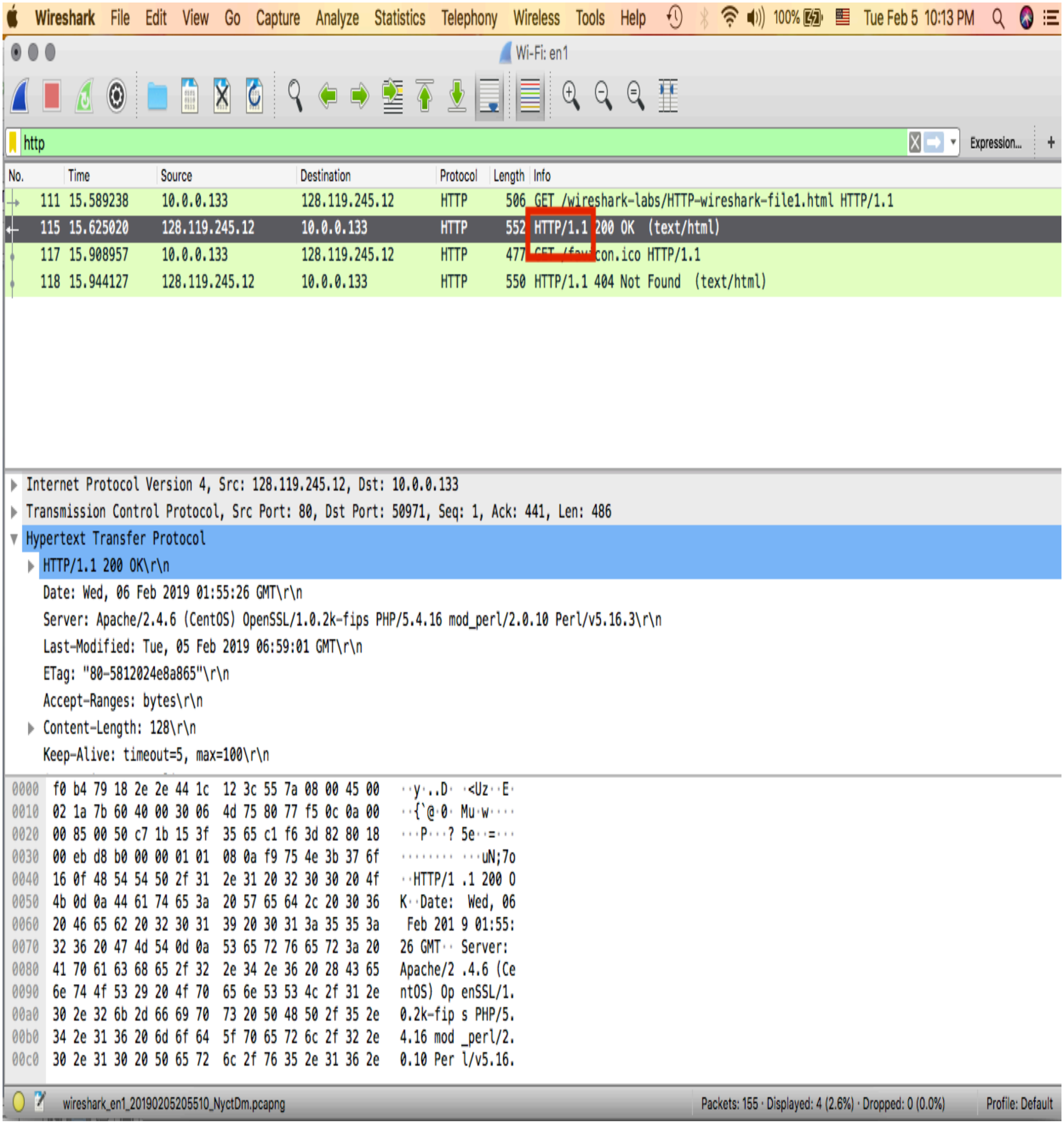
```
▶ Frame 115: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
▶ Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:2e)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50971, Seq: 1, Ack: 441, Len: 486
▶ Hypertext Transfer Protocol
▶ Line-based text data: text/html (4 lines)
```

```
0000  f0 b4 79 18 2e 2e 44 1c  12 3c 55 7a 08 00 45 00   ··y·..D· ·<Uz··E·
0010  02 1a 7b 60 40 00 30 06  4d 75 80 77 f5 0c 0a 00   ··{`@·0· Mu·w····
0020  00 85 00 50 c7 1b 15 3f  35 65 c1 f6 3d 82 80 18   ···P···? 5e··=···
0030  00 eb d8 b0 00 00 01 01  08 0a f9 75 4e 3b 37 6f   ········ ···uN;7o
0040  16 0f 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ··HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 57 65 64 2c 20 30 36   K··Date:  Wed, 06
0060  20 46 65 62 20 32 30 31  39 20 30 31 3a 35 35 3a    Feb 201 9 01:55:
0070  32 36 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   26 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 30 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.10 Per l/v5.16.
```

wireshark_en1_20190205205510_NyctDm.pcapng   Packets: 155 · Displayed: 4 (2.6%) · Dropped: 0 (0.0%)   Profile: Default

Is your browser running HTTP version 1.0 or 1.1?

HTTP version 1.1


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
100%
Tue Feb 5 10:13 PM
Wi-Fi: en1
Expression...
+

http

```
No.   Time       Source          Destination     Protocol  Length  Info
111   15.589238  10.0.0.133      128.119.245.12  HTTP      506     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
115   15.625020  128.119.245.12  10.0.0.133      HTTP      552     HTTP/1.1 200 OK  (text/html)
117   15.908957  10.0.0.133      128.119.245.12  HTTP      477     GET /favicon.ico HTTP/1.1
118   15.944127  128.119.245.12  10.0.0.133      HTTP      550     HTTP/1.1 404 Not Found  (text/html)
```

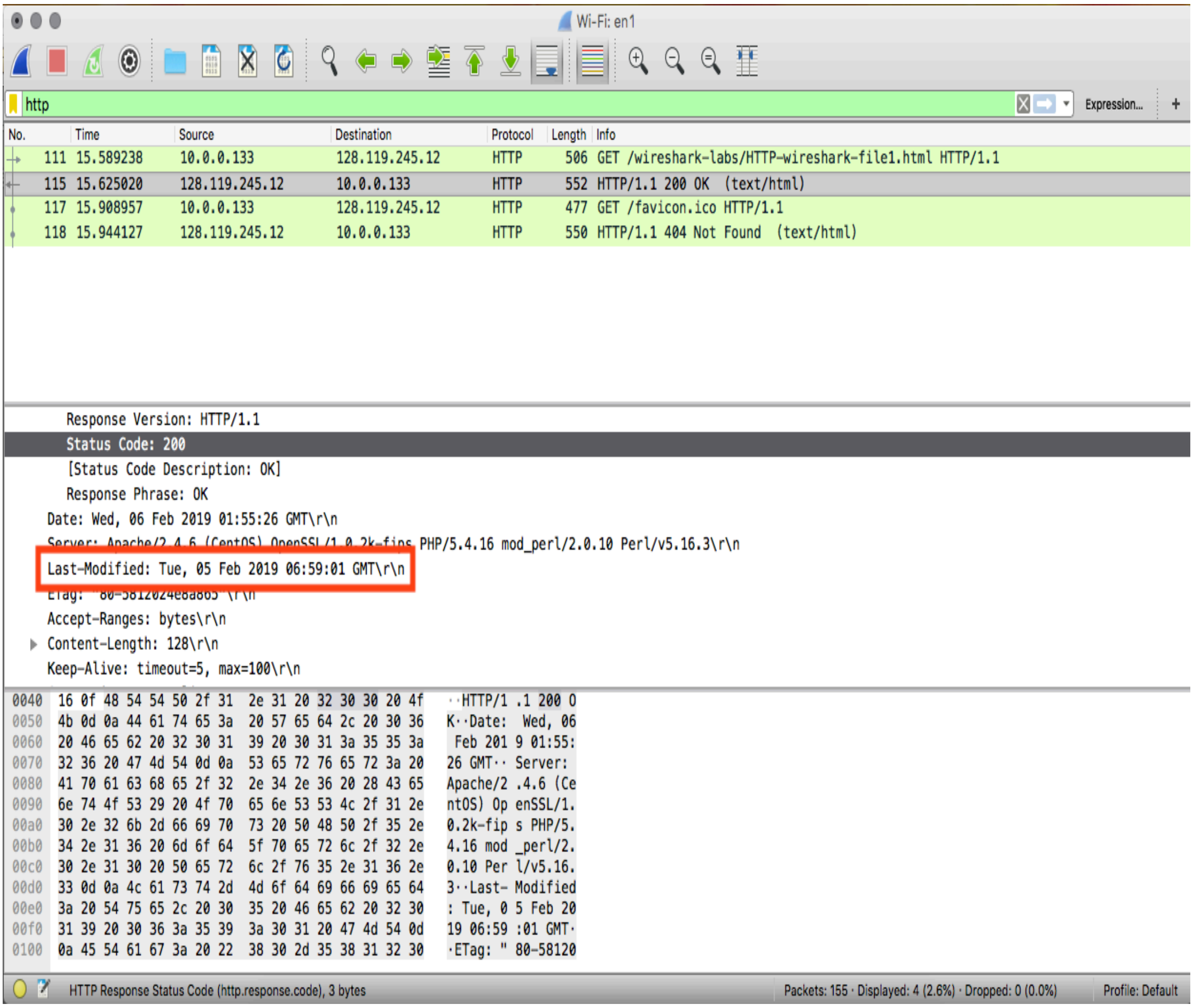
```
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50971, Seq: 1, Ack: 441, Len: 486
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Wed, 06 Feb 2019 01:55:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 05 Feb 2019 06:59:01 GMT\r\n
    ETag: "80-5812024e8a865"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

```
0000  f0 b4 79 18 2e 2e 44 1c  12 3c 55 7a 08 00 45 00   ··y·..D· ·<Uz··E·
0010  02 1a 7b 60 40 00 30 06  4d 75 80 77 f5 0c 0a 00   ··{`@·0· Mu·w····
0020  00 85 00 50 c7 1b 15 3f  35 65 c1 f6 3d 82 80 18   ···P···? 5e··=···
0030  00 eb d8 b0 00 00 01 01  08 0a f9 75 4e 3b 37 6f   ········ ···uN;7o
0040  16 0f 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ··HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 57 65 64 2c 20 30 36   K··Date:  Wed, 06
0060  20 46 65 62 20 32 30 31  39 20 30 31 3a 35 35 3a    Feb 201 9 01:55:
0070  32 36 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   26 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 30 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.10 Per l/v5.16.
```

```
wireshark_en1_20190205205510_NyctDm.pcapng    Packets: 155 · Displayed: 4 (2.6%) · Dropped: 0 (0.0%)    Profile: Default
```

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

Tue, 05 Feb. 2019 6:59 gmt



```
No.   Time       Source         Destination    Protocol Length Info
111   15.589238  10.0.0.133     128.119.245.12 HTTP     506    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
115   15.625020  128.119.245.12 10.0.0.133     HTTP     552    HTTP/1.1 200 OK  (text/html)
117   15.908957  10.0.0.133     128.119.245.12 HTTP     477    GET /favicon.ico HTTP/1.1
118   15.944127  128.119.245.12 10.0.0.133     HTTP     550    HTTP/1.1 404 Not Found  (text/html)
```

```
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
   Date: Wed, 06 Feb 2019 01:55:26 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
   Last-Modified: Tue, 05 Feb 2019 06:59:01 GMT\r\n
   ETag: "80-5812024e8a865"\r\n
   Accept-Ranges: bytes\r\n
 ▸ Content-Length: 128\r\n
   Keep-Alive: timeout=5, max=100\r\n
```

```
0040  16 0f 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ··HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 57 65 64 2c 20 30 36   K··Date:  Wed, 06
0060  20 46 65 62 20 32 30 31  39 20 30 31 3a 35 35 3a    Feb 201 9 01:55:
0070  32 36 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   26 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 30 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.10 Per l/v5.16.
00d0  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3··Last- Modified
00e0  3a 20 54 75 65 2c 20 30  35 20 46 65 62 20 32 30   : Tue, 0 5 Feb 20
00f0  31 39 20 30 36 3a 35 39  3a 30 31 20 47 4d 54 0d   19 06:59 :01 GMT·
0100  0a 45 54 61 67 3a 20 22  38 30 2d 35 38 31 32 30   ·ETag: " 80-58120
```

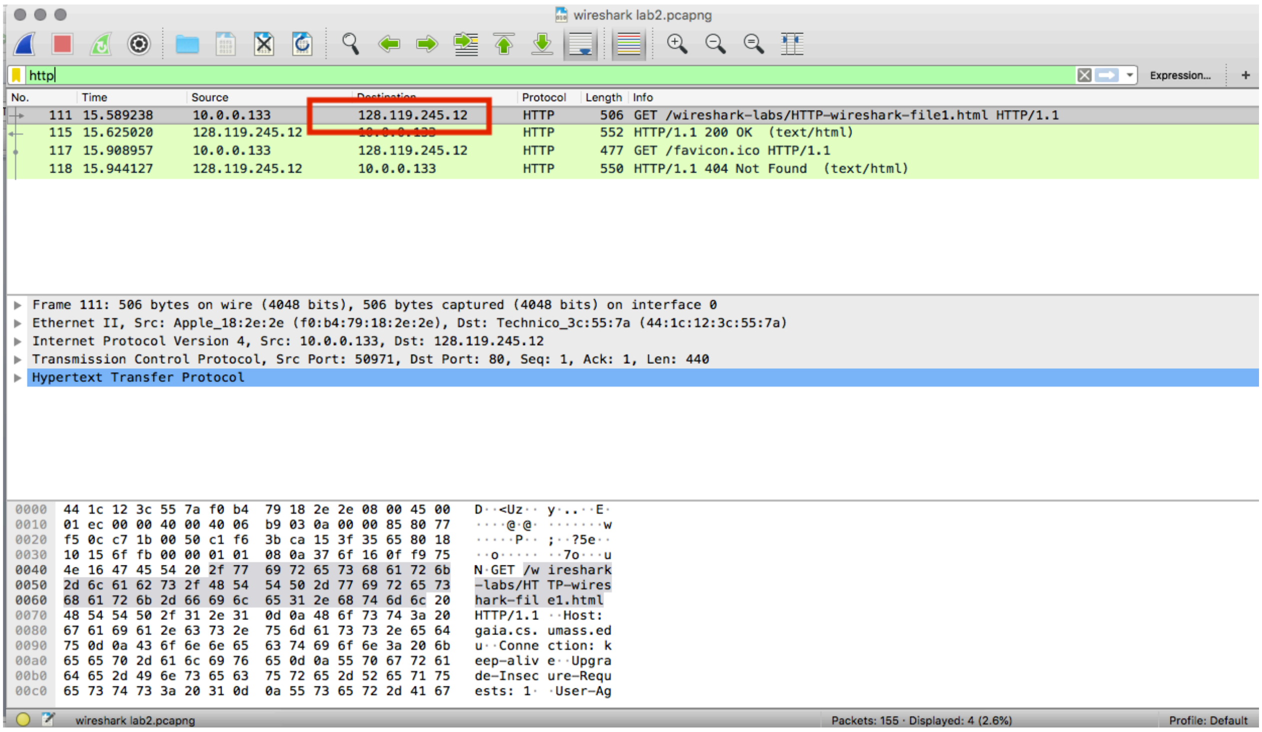
HTTP Response Status Code (http.response.code), 3 bytes

Packets: 155 · Displayed: 4 (2.6%) · Dropped: 0 (0.0%)

Profile: Default

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

128.119.245.12



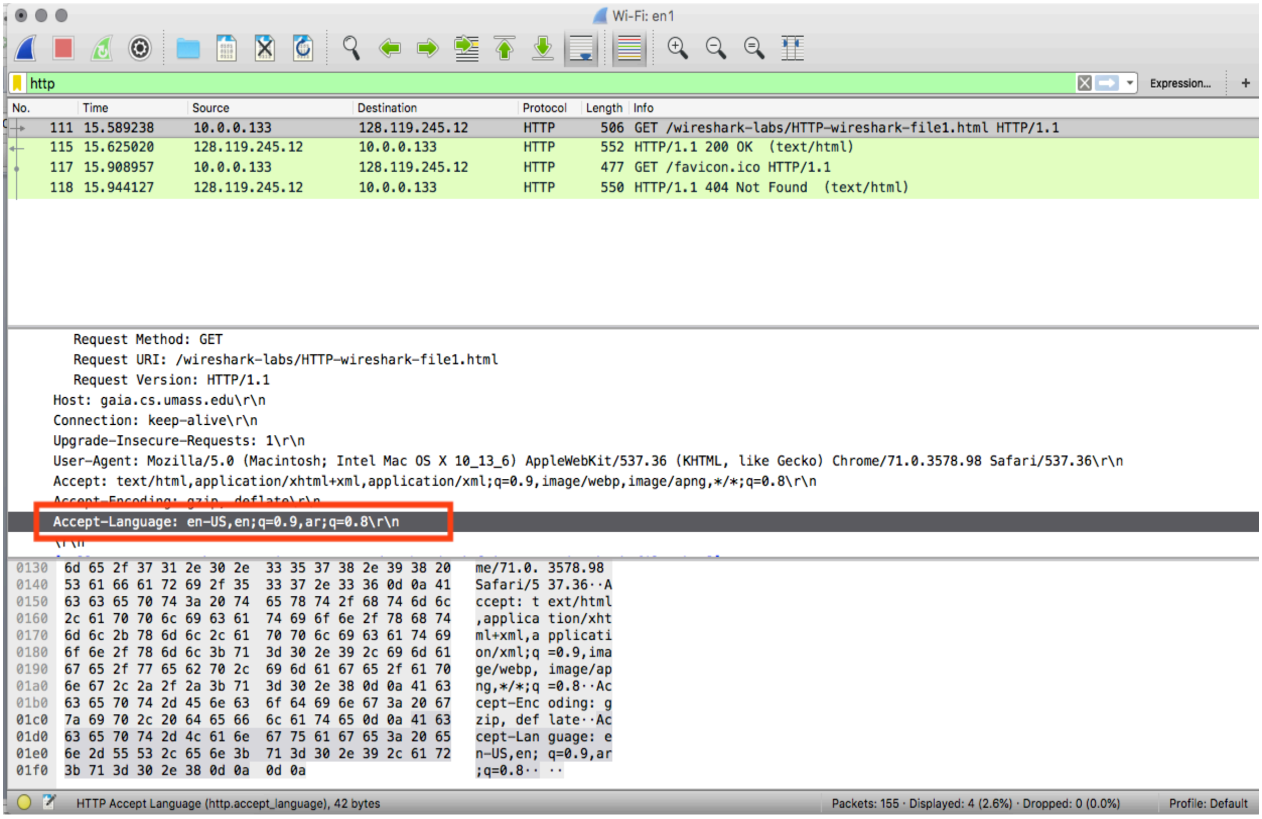
```
No.   Time       Source          Destination     Protocol Length Info
  111 15.589238  10.0.0.133      128.119.245.12  HTTP     506    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  115 15.625020  128.119.245.12  10.0.0.133      HTTP     552    HTTP/1.1 200 OK  (text/html)
  117 15.908957  10.0.0.133      128.119.245.12  HTTP     477    GET /favicon.ico HTTP/1.1
  118 15.944127  128.119.245.12  10.0.0.133      HTTP     550    HTTP/1.1 404 Not Found  (text/html)
```

```
▶ Frame 111: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
▶ Ethernet II, Src: Apple_18:2e:2e (f0:b4:79:18:2e:2e), Dst: Technico_3c:55:7a (44:1c:12:3c:55:7a)
▶ Internet Protocol Version 4, Src: 10.0.0.133, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 50971, Dst Port: 80, Seq: 1, Ack: 1, Len: 440
▶ Hypertext Transfer Protocol
```

```
0000  44 1c 12 3c 55 7a f0 b4  79 18 2e 2e 08 00 45 00   D··<Uz·· y·..··E·
0010  01 ec 00 00 40 00 40 06  b9 03 0a 00 00 85 80 77   ····@·@· ·······w
0020  f5 0c c7 1b 00 50 c1 f6  3b ca 15 3f 35 65 80 18   ·····P·· ;··?5e··
0030  10 15 6f fb 00 00 01 01  08 0a 37 6f 16 0f f9 75   ··o····· ··7o···u
0040  4e 16 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   N·GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 31 2e 68 74 6d 6c 20   hark-fil e1.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
00b0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00c0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
```

What languages does your browser indicate that it can accept to the server?

EN-US



```
No.   Time        Source          Destination     Protocol  Length  Info
111   15.589238   10.0.0.133      128.119.245.12  HTTP      506     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
115   15.625020   128.119.245.12  10.0.0.133      HTTP      552     HTTP/1.1 200 OK  (text/html)
117   15.908957   10.0.0.133      128.119.245.12  HTTP      477     GET /favicon.ico HTTP/1.1
118   15.944127   128.119.245.12  10.0.0.133      HTTP      550     HTTP/1.1 404 Not Found  (text/html)
```

```
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.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 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 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: en-US,en;q=0.9,ar;q=0.8\r\n
  \r\n
```

```
0130  6d 65 2f 37 31 2e 30 2e  33 35 37 38 2e 39 38 20   me/71.0. 3578.98
0140  53 61 66 61 72 69 2f 35  33 37 2e 33 36 0d 0a 41   Safari/5 37.36··A
0150  63 63 65 70 74 3a 20 74  65 78 74 2f 68 74 6d 6c   ccept: t ext/html
0160  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 68 74   ,applica tion/xht
0170  6d 6c 2b 78 6d 6c 2c 61  70 70 6c 69 63 61 74 69   ml+xml,a pplicati
0180  6f 6e 2f 78 6d 6c 3b 71  3d 30 2e 39 2c 69 6d 61   on/xml;q =0.9,ima
0190  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
01a0  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 0d 0a 41 63   ng,*/*;q =0.8··Ac
01b0  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 67   cept-Enc oding: g
01c0  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d 0a 41 63   zip, def late··Ac
01d0  63 65 70 74 2d 4c 61 6e  67 75 61 67 65 3a 20 65   cept-Lan guage: e
01e0  6e 2d 55 53 2c 65 6e 3b  71 3d 30 2e 39 2c 61 72   n-US,en; q=0.9,ar
01f0  3b 71 3d 30 2e 38 0d 0a  0d 0a                     ;q=0.8·· ··
```

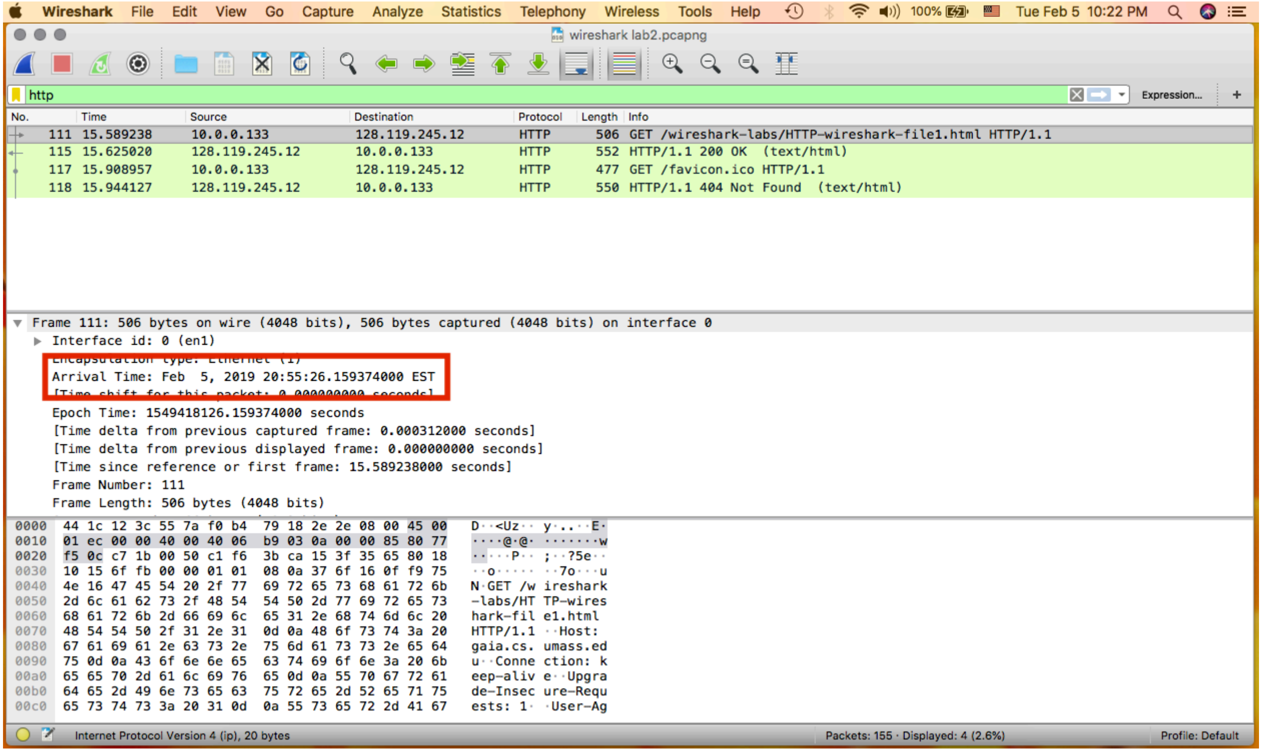
HTTP Accept Language (http.accept_language), 42 bytes

Packets: 155 · Displayed: 4 (2.6%) · Dropped: 0 (0.0%)

Profile: Default

When was the HTML file that you are retrieving created at the server?

Feb 5, 2019 20:55:26. 159 EST


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
100%
Tue Feb 5 10:22 PM
wireshark lab2.pcapng
Expression…
+

```
http
```

```
No.   Time        Source          Destination     Protocol  Length  Info
111   15.589238   10.0.0.133      128.119.245.12  HTTP      506     GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
115   15.625020   128.119.245.12  10.0.0.133      HTTP      552     HTTP/1.1 200 OK  (text/html)
117   15.908957   10.0.0.133      128.119.245.12  HTTP      477     GET /favicon.ico HTTP/1.1
118   15.944127   128.119.245.12  10.0.0.133      HTTP      550     HTTP/1.1 404 Not Found  (text/html)
```

```
▼ Frame 111: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface 0
  ▶ Interface id: 0 (en1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  5, 2019 20:55:26.159374000 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1549418126.159374000 seconds
    [Time delta from previous captured frame: 0.000312000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 15.589238000 seconds]
    Frame Number: 111
    Frame Length: 506 bytes (4048 bits)
```

```
0000  44 1c 12 3c 55 7a f0 b4  79 18 2e 2e 08 00 45 00   D··<Uz·· y·.···E·
0010  01 ec 00 00 40 00 40 06  b9 03 0a 00 00 85 80 77   ····@·@· ·······w
0020  f5 0c c7 1b 00 50 c1 f6  3b ca 15 3f 35 65 80 18   ·····P·· ;··?5e··
0030  10 15 6f fb 00 00 01 01  08 0a 37 6f 16 0f f9 75   ··o····· ··7o···u
0040  4e 16 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   N·GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 31 2e 68 74 6d 6c 20   hark-fil e1.html
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host:
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
00b0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00c0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
```

Internet Protocol Version 4 (ip), 20 bytes

Packets: 155 · Displayed: 4 (2.6%)

Profile: Default

```
    Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ar;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/favicon.ico]
    [HTTP request 2/2]
    [Prev request in frame: 111]
    [Response in frame: 118]
No.     Time           Source                Destination           Protocol Length Info
    118 15.944127      128.119.245.12        10.0.0.133            HTTP     550    HTTP/1.1 404
Not Found  (text/html)
Frame 118: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface 0
Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:
2e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
Transmission Control Protocol, Src Port: 80, Dst Port: 50971, Seq: 487, Ack: 852, Len: 484
Hypertext Transfer Protocol
    HTTP/1.1 404 Not Found\r\n
    Date: Wed, 06 Feb 2019 01:55:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r
\n
    Content-Length: 209\r\n
    Keep-Alive: timeout=5, max=99\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.035170000 seconds]
    [Prev request in frame: 111]
    [Prev response in frame: 115]
    [Request in frame: 117]
    File Data: 209 bytes
Line-based text data: text/html (7 lines)
```

```
No.     Time           Source                Destination           Protocol Length Info
    115 15.625020      128.119.245.12        10.0.0.133            HTTP     552    HTTP/1.1 200 
OK  (text/html)
Frame 115: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: Technico_3c:55:7a (44:1c:12:3c:55:7a), Dst: Apple_18:2e:2e (f0:b4:79:18:2e:
2e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.133
Transmission Control Protocol, Src Port: 80, Dst Port: 50971, Seq: 1, Ack: 441, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 06 Feb 2019 01:55:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r
\n
    Last-Modified: Tue, 05 Feb 2019 06:59:01 GMT\r\n
    ETag: "80-5812024e8a865"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\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: 0.035782000 seconds]
    [Request in frame: 111]
    [Next request in frame: 117]
    [Next response in frame: 118]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```