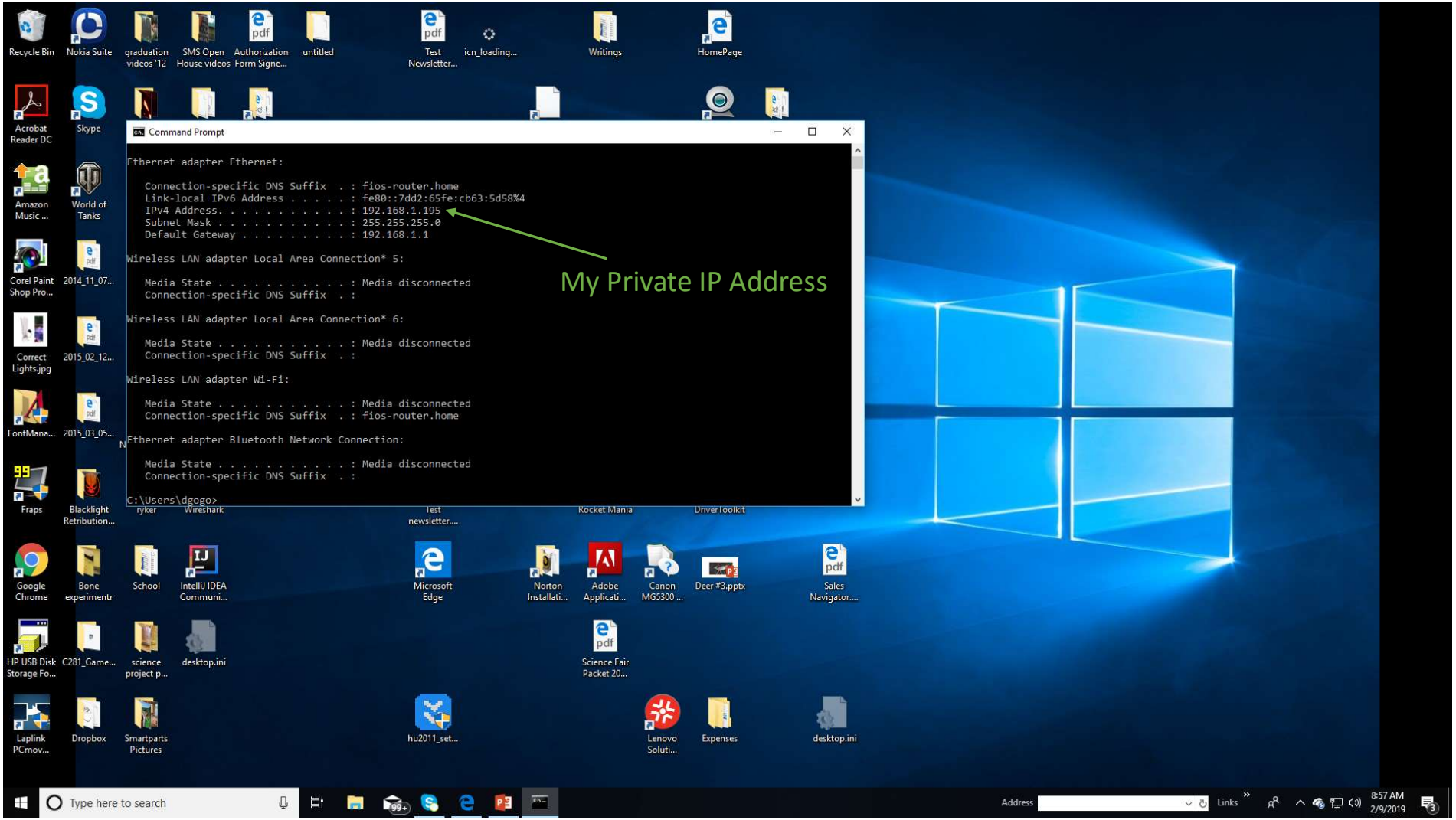
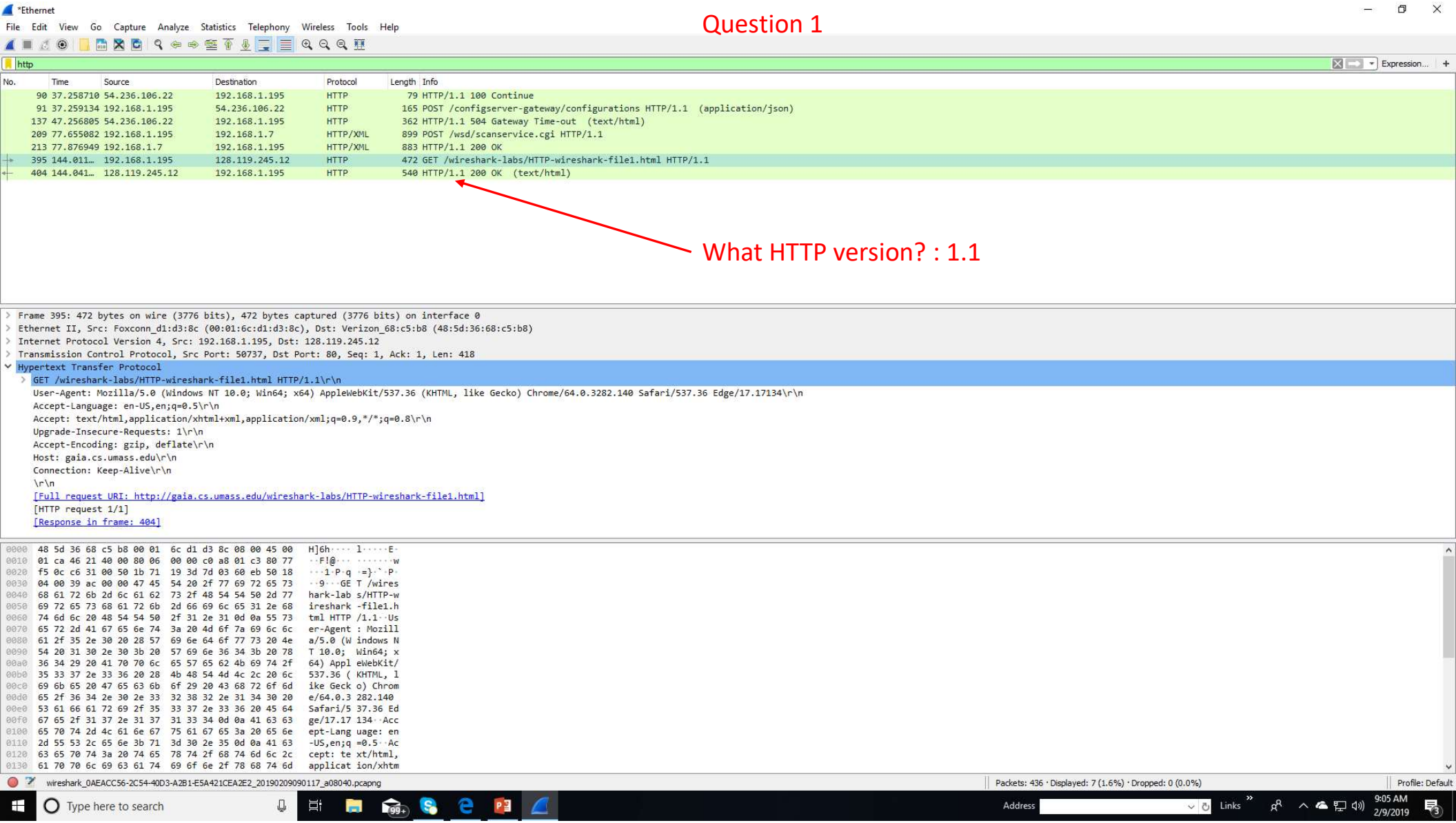
Wireshark Lab 2 - HTTP

IT 520 –A – Enterprise Infrastructure & Networks

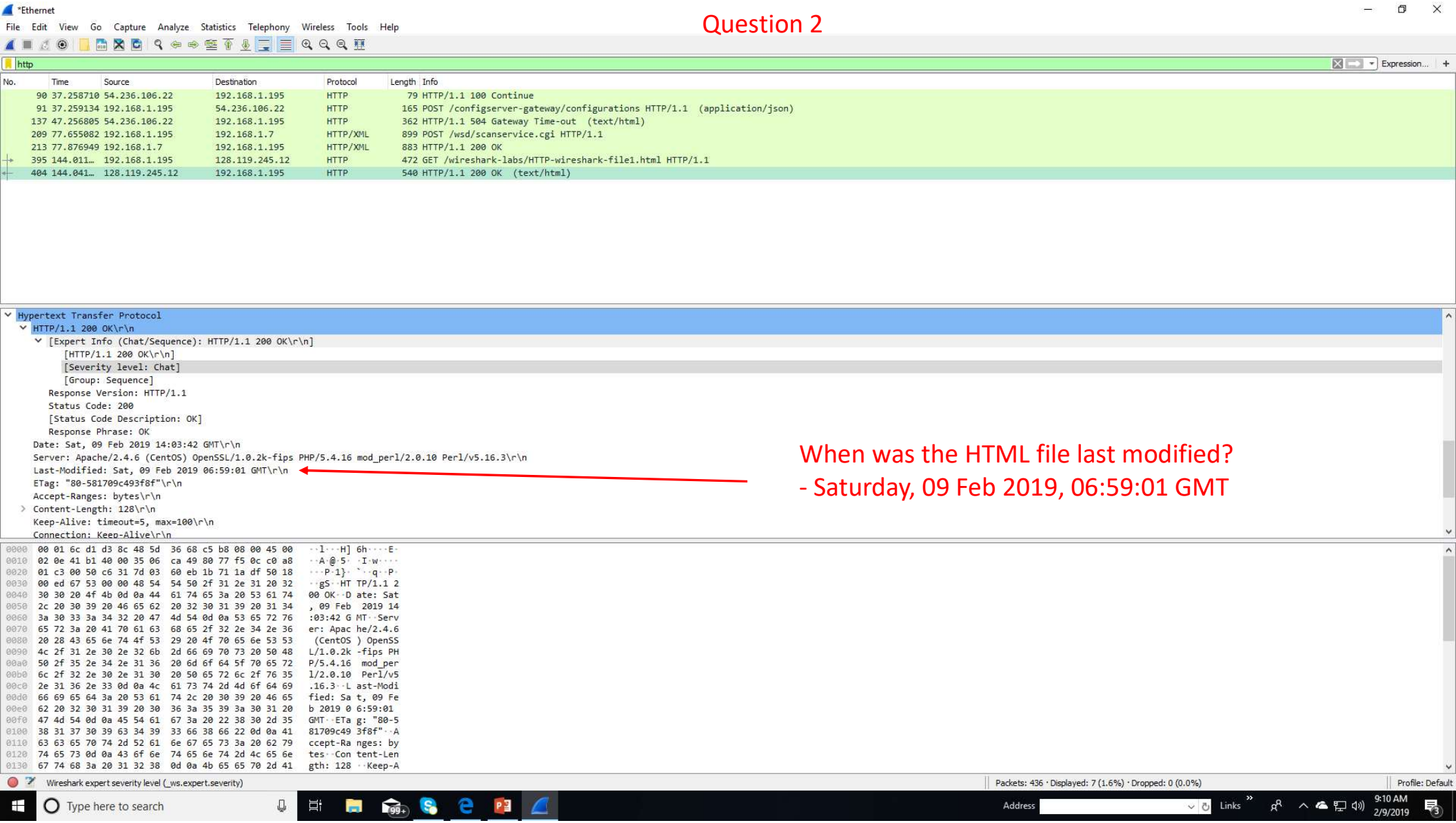
David Gogolkiewicz

IP Address


Command Prompt
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : fios-router.home
Link-local IPv6 Address . . . . . : fe80::7dd2:65fe:cb63:5d58%4
IPv4 Address. . . . . : 192.168.1.195
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Wireless LAN adapter Local Area Connection* 5:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 6:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : fios-router.home
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\dgogo>
My Private IP Address


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Question 1
http
Expression...
No. Time Source Destination Protocol Length Info
90 37.258710 54.236.106.22 192.168.1.195 HTTP 79 HTTP/1.1 100 Continue
91 37.259134 192.168.1.195 54.236.106.22 HTTP 165 POST /configserver-gateway/configurations HTTP/1.1 (application/json)
137 47.256805 54.236.106.22 192.168.1.195 HTTP 362 HTTP/1.1 504 Gateway Time-out (text/html)
209 77.655082 192.168.1.195 192.168.1.7 HTTP/XML 899 POST /wsd/scanservice.cgi HTTP/1.1
213 77.876949 192.168.1.7 192.168.1.195 HTTP/XML 883 HTTP/1.1 200 OK
395 144.011… 192.168.1.195 128.119.245.12 HTTP 472 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
404 144.041… 128.119.245.12 192.168.1.195 HTTP 540 HTTP/1.1 200 OK (text/html)
What HTTP version? : 1.1
Frame 395: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface 0
Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50737, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 404]
0000 48 5d 36 68 c5 b8 00 01 6c d1 d3 8c 08 00 45 00 H]6h···· l·····E·
0010 01 ca 46 21 40 00 80 06 00 00 c0 a8 01 c3 80 77 ··F!@··· ·······w
0020 f5 0c c6 31 00 50 1b 71 19 3d 7d 03 60 eb 50 18 ···1·P·q ·=}·`·P·
0030 04 00 39 ac 00 00 47 45 54 20 2f 77 69 72 65 73 ··9···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 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73 tml HTTP /1.1··Us
0070 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0080 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N
0090 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
00a0 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 64) Appl eWebKit/
00b0 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l
00c0 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Geck o) Chrom
00d0 65 2f 36 34 2e 30 2e 33 32 38 32 2e 31 34 30 20 e/64.0.3 282.140
00e0 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64 Safari/5 37.36 Ed
00f0 67 65 2f 31 37 2e 31 37 31 33 34 0d 0a 41 63 63 ge/17.17 134··Acc
0100 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e ept-Lang uage: en
0110 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63 -US,en;q =0.5··Ac
0120 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c cept: te xt/html,
0130 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d applicat ion/xhtm
wireshark_0AEACC56-2C54-40D3-A2B1-E5A421CEA2E2_20190209090117_a08040.pcapng
Packets: 436 · Displayed: 7 (1.6%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
Address
Links
9:05 AM
2/9/2019

Question 2



When was the HTML file last modified?

- Saturday, 09 Feb 2019, 06:59:01 GMT

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 3

http

No.	Time	Source	Destination	Protocol	Length	Info
90	37.258710	54.236.106.22	192.168.1.195	HTTP	79	HTTP/1.1 100 Continue
91	37.259134	192.168.1.195	54.236.106.22	HTTP	165	POST /configserver-gateway/configurations HTTP/1.1 (application/json)
137	47.256805	54.236.106.22	192.168.1.195	HTTP	362	HTTP/1.1 504 Gateway Time-out (text/html)
209	77.655082	192.168.1.195	192.168.1.7	HTTP/XML	899	POST /wsd/scanservice.cgi HTTP/1.1
213	77.876949	192.168.1.7	192.168.1.195	HTTP/XML	883	HTTP/1.1 200 OK
395	144.011…	192.168.1.195	128.119.245.12	HTTP	472	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
404	144.041…	128.119.245.12	192.168.1.195	HTTP	540	HTTP/1.1 200 OK (text/html)

What is the IP address of the gaia.cs.umass.edu server?
- 128.119.245.12

```
        [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
Date: Sat, 09 Feb 2019 14:03:42 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: Sat, 09 Feb 2019 06:59:01 GMT\r\n
ETag: "80-581709c493f8f"\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 1/1]
```

```
0000  00 01 6c d1 d3 8c 48 5d  36 68 c5 b8 08 00 45 00   ··l···H] 6h····E·
0010  02 0e 41 b1 40 00 35 06  ca 49 80 77 f5 0c c0 a8   ··A·@·5· ·I·w····
0020  01 c3 00 50 c6 31 7d 03  60 eb 1b 71 1a df 50 18   ···P·1}· `··q··P·
0030  00 ed 67 53 00 00 48 54  54 50 2f 31 2e 31 20 32   ··gS··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 30 39 20 46 65 62  20 32 30 31 39 20 31 34   , 09 Feb  2019 14
0060  3a 30 33 3a 34 32 20 47  4d 54 0d 0a 53 65 72 76   :03:42 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 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 61  74 2c 20 30 39 20 46 65   fied: Sa t, 09 Fe
00e0  62 20 32 30 31 39 20 30  36 3a 35 39 3a 30 31 20   b 2019 0 6:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  38 31 37 30 39 63 34 39  33 66 38 66 22 0d 0a 41   81709c49 3f8f"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
```

Wireshark expert severity level (_ws.expert.severity)

Packets: 436 · Displayed: 7 (1.6%) · Dropped: 0 (0.0%)

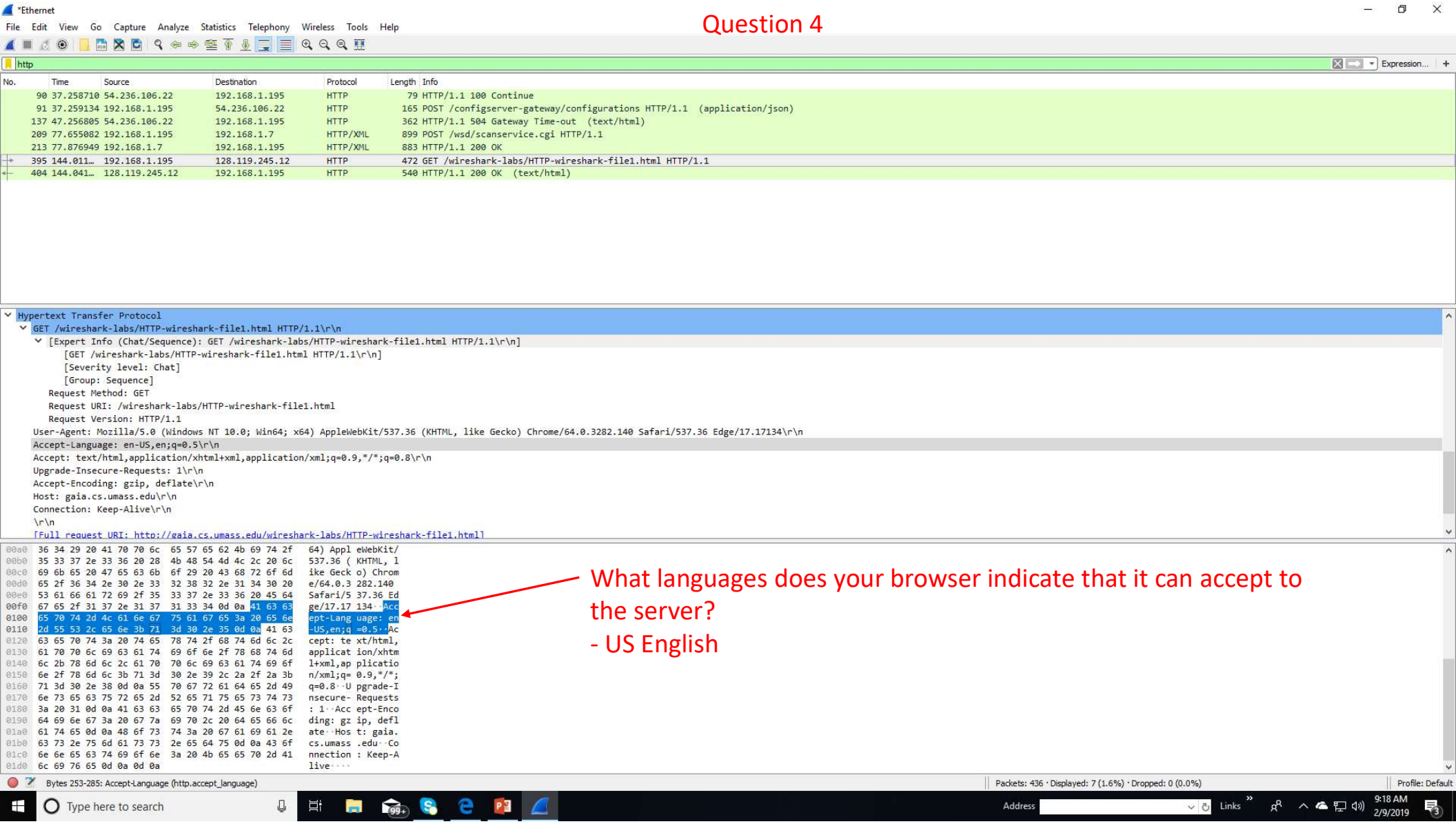
Profile: Default

Type here to search

Address Links

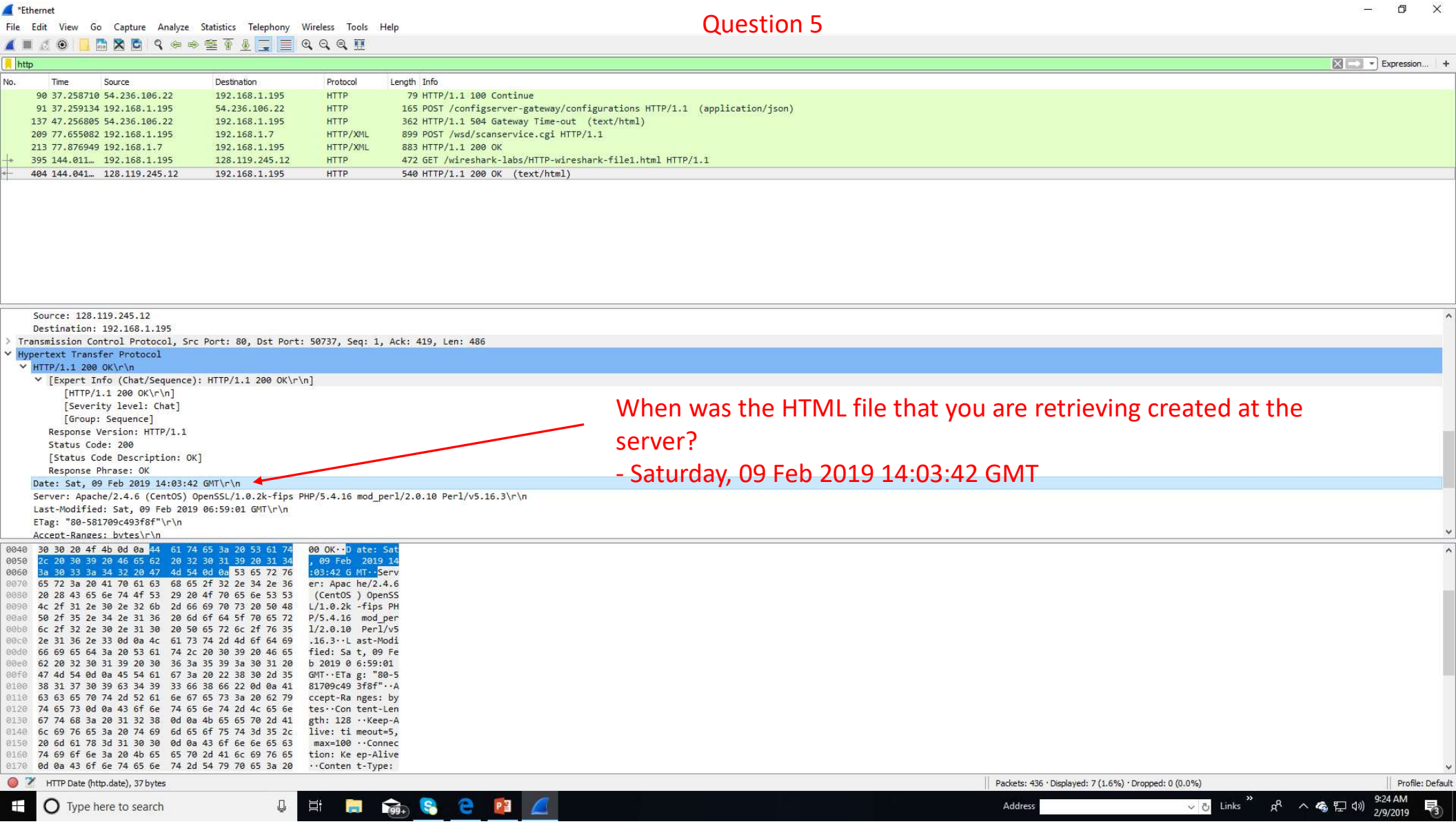
9:14 AM
2/9/2019

Question 4



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

- US English



Question 5

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

- Saturday, 09 Feb 2019 14:03:42 GMT

C:\Users\dgogo\AppData\Local\Temp\wireshark_0AEACC56-2C54-40D3-A2B1-E5A421CEA2E2_20190209090117_a08040.pcapng 436 total packets, 7 shown

```
No.     Time           Source                Destination           Protocol Length Info
    404 144.041870     128.119.245.12        192.168.1.195         HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 404: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
    Interface id: 0 (\Device\NPF_{0AEACC56-2C54-40D3-A2B1-E5A421CEA2E2})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb  9, 2019 09:03:41.791187000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1549721021.791187000 seconds
    [Time delta from previous captured frame: 0.000598000 seconds]
    [Time delta from previous displayed frame: 0.030861000 seconds]
    [Time since reference or first frame: 144.041870000 seconds]
    Frame Number: 404
    Frame Length: 540 bytes (4320 bits)
    Capture Length: 540 bytes (4320 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c)
    Destination: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c)
    Source: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.195
Transmission Control Protocol, Src Port: 80, Dst Port: 50737, Seq: 1, Ack: 419, Len: 486
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
    Date: Sat, 09 Feb 2019 14:03:42 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: Sat, 09 Feb 2019 06:59:01 GMT\r\n
    ETag: "80-581709c493f8f"\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 1/1]
    [Time since request: 0.030861000 seconds]
    [Request in frame: 395]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```