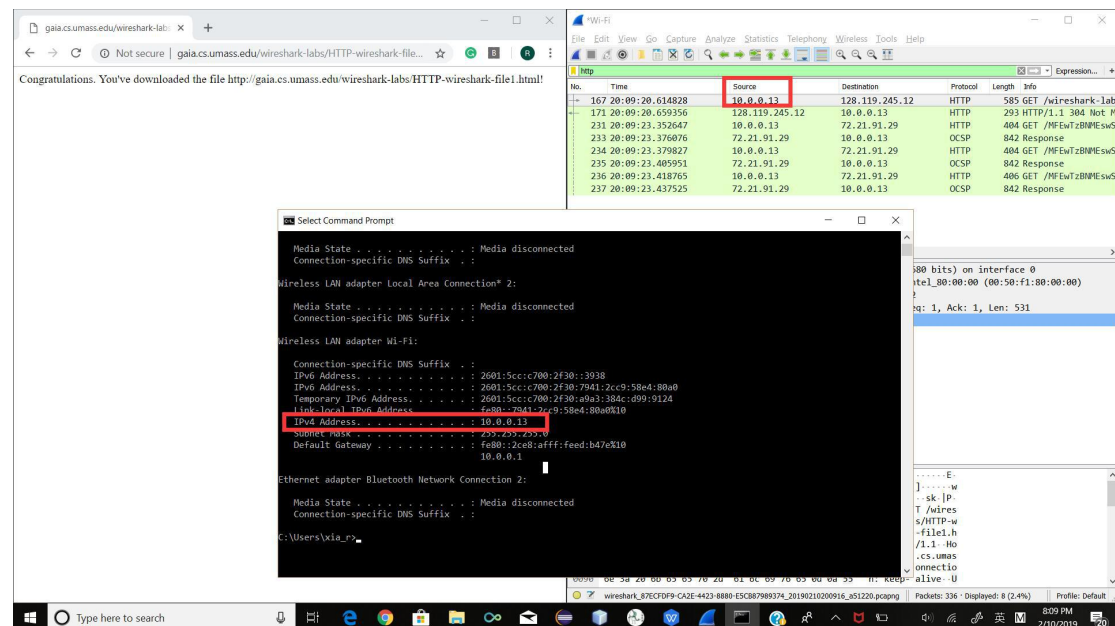
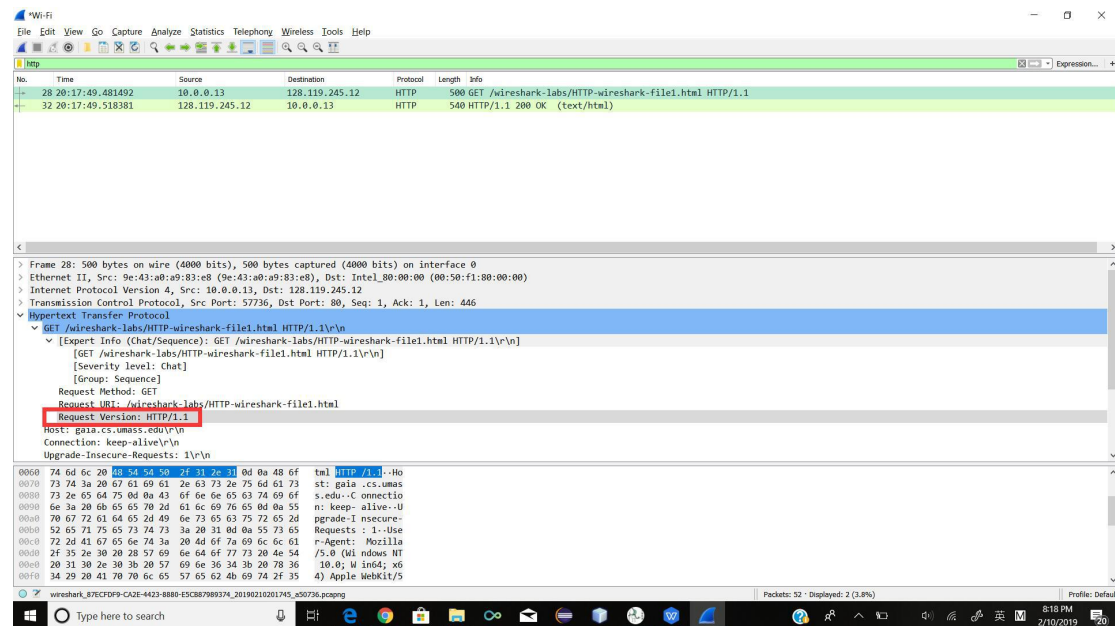


IP address:



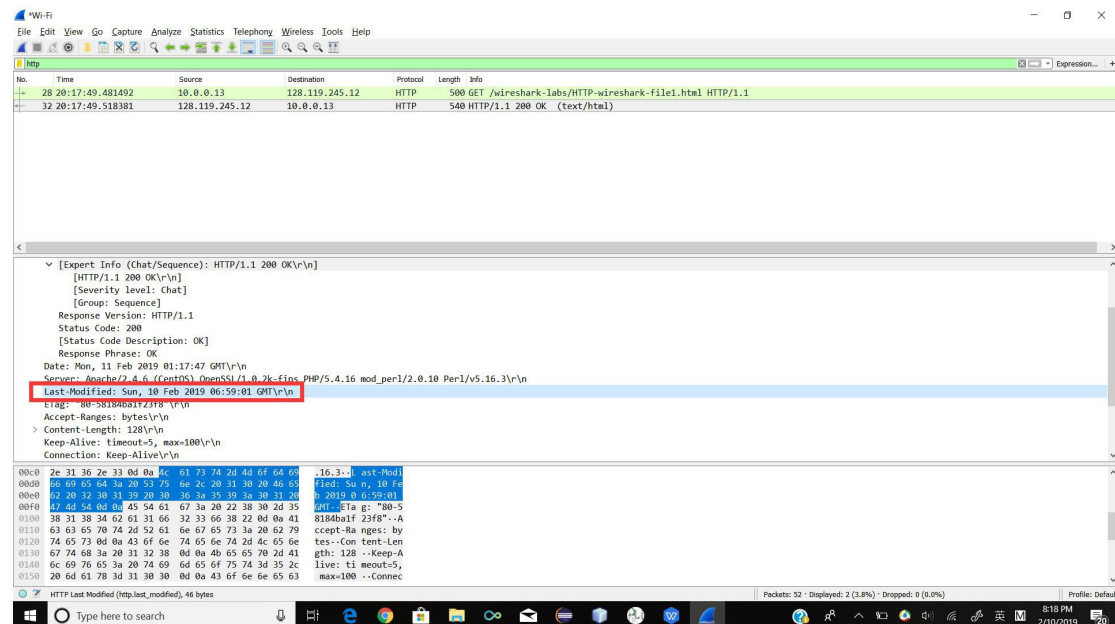
My IP is 10.0.0.13

1. Is your browser running HTTP version 1.0 or 1.1?



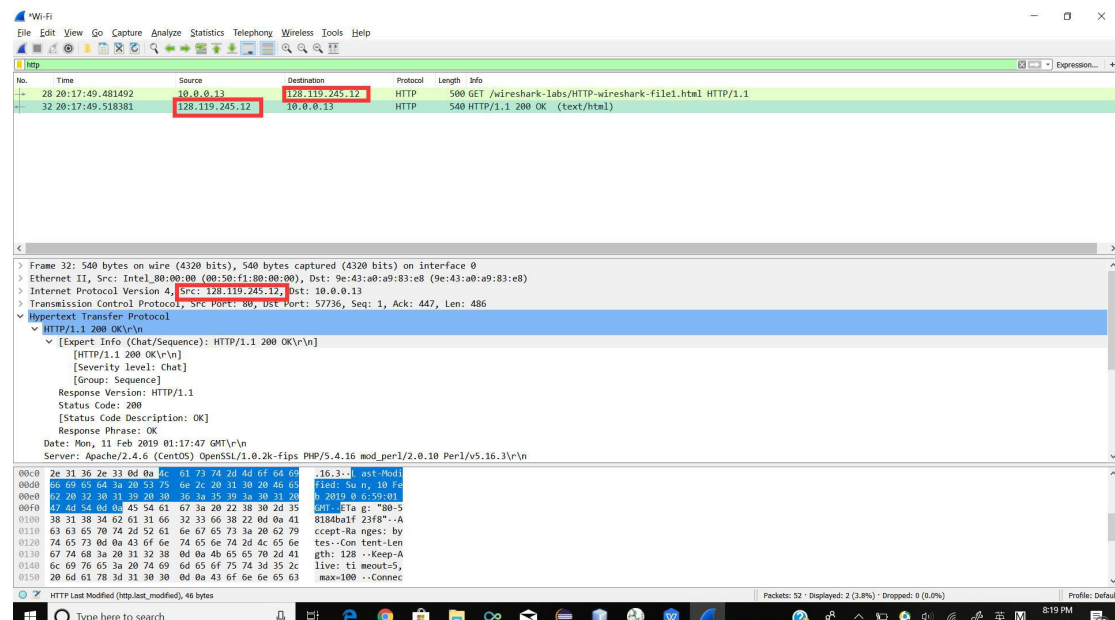
As circled, it is running HTTP 1.1

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



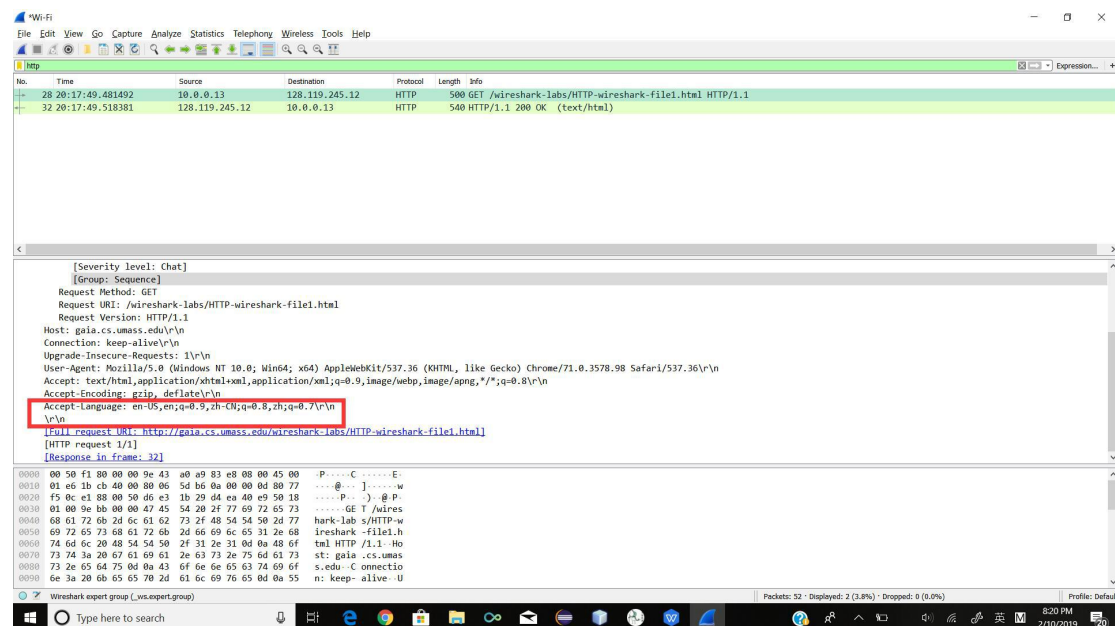
Last modified date: Sun, 10 February 2019, 06:59:01 GMT

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



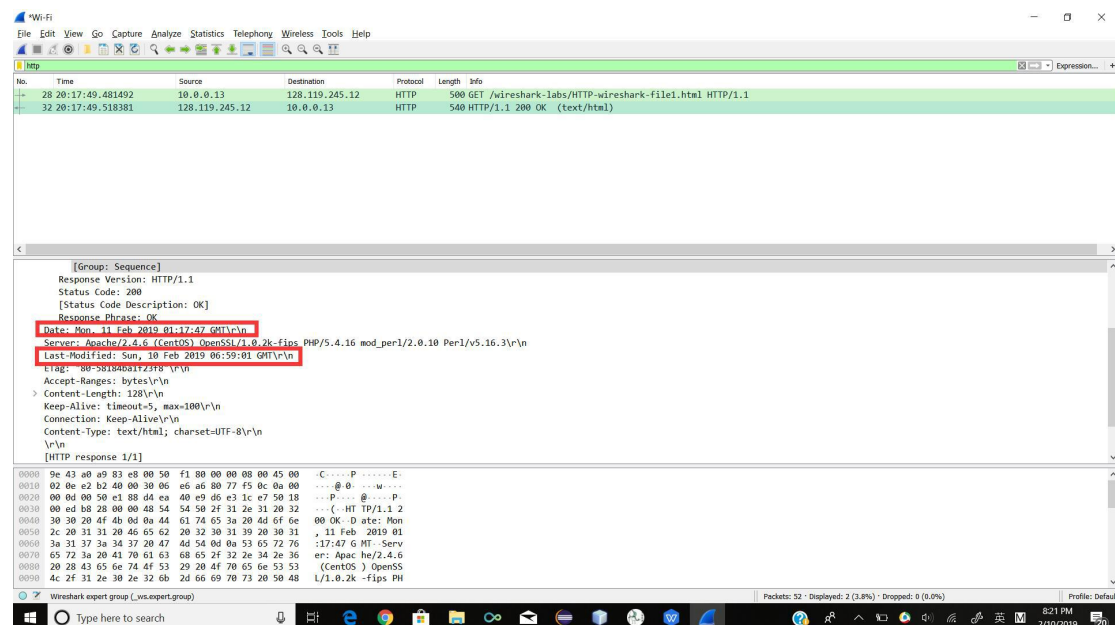
IP address in found in three spots. The IP address for the website is 128.119.245.12

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



It takes en-US, en, zh-CN, zh.

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



Cannot find the date of creation. But Wireshark shows date and time of receiving the file and the last modified date of that file. Date of receiving

is Mon, 11 Feb 2019, 01:17:47 GMT and last modified date is Sun, 10 Feb 2019, 06:59:01 GMT.

Full print of HTTP OK message next page

No.	Time	Source	Destination	Protocol	Length	Info
32	20:17:49.518381	128.119.245.12	10.0.0.13	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 32: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Interface id: 0 (\Device\NPF_{87ECDFD9-CA2E-4423-8880-E5CB87989374})
Interface name: \Device\NPF_{87ECDFD9-CA2E-4423-8880-E5CB87989374}
Encapsulation type: Ethernet (1)
Arrival Time: Feb 10, 2019 20:17:49.518381000 Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1549847869.518381000 seconds
[Time delta from previous captured frame: 0.000001000 seconds]
[Time delta from previous displayed frame: 0.036889000 seconds]
[Time since reference or first frame: 3.332047000 seconds]
Frame Number: 32
Frame Length: 540 bytes (4320 bits)
Capture Length: 540 bytes (4320 bits)
[Frame is marked: True]
[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: Intel_80:00:00 (00:50:f1:80:00:00), Dst: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
Destination: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
Address: 9e:43:a0:a9:83:e8 (9e:43:a0:a9:83:e8)
.... 1. = LG bit: Locally administered address (this is NOT the factory default)
.... 0 = IG bit: Individual address (unicast)
Source: Intel_80:00:00 (00:50:f1:80:00:00)
Address: Intel_80:00:00 (00:50:f1:80:00:00)
.... 0. = LG bit: Globally unique address (factory default)
.... 0 = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.13
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 526
Identification: 0xe2b2 (58034)
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.. = Don't fragment: Set
..0. = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 48
Protocol: TCP (6)
Header checksum: 0xe6a6 [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
Destination: 10.0.0.13
Transmission Control Protocol, Src Port: 80, Dst Port: 57736, Seq: 1, Ack: 447, Len: 486
Source Port: 80
Destination Port: 57736
[Stream index: 3]
[TCP Segment Len: 486]
Sequence number: 1 (relative sequence number)
[Next sequence number: 487 (relative sequence number)]
Acknowledgment number: 447 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... 1.. = Push: Set
....0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags:AP...]
Window size value: 237
[Calculated window size: 30336]
[Window size scaling factor: 128]
Checksum: 0xb828 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.032662000 seconds]
[Bytes in flight: 486]
[Bytes sent since last PSH flag: 486]
[Timestamps]
[Time since first frame in this TCP stream: 0.069710000 seconds]
[Time since previous frame in this TCP stream: 0.000001000 seconds]
TCP payload (486 bytes)
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n\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: Mon, 11 Feb 2019 01:17:47 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n
ETag: "80-58184ba1f23f8"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
[Content length: 128]
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: 0.036889000 seconds]
[Request in frame: 28]
File Data: 128 bytes
Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```