

Instructions:

1. Part 1: Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
5. Stop Wireshark packet capture.

- (For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.
- Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Questions:

Terminal Screenshot with the IP address of my computer:

IP Address : 192.168.1.193

```
Command Prompt
C:\Users\ariel>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : fios-router.home
    Link-local IPv6 Address . . . . . : fe80::bdc9:bdea:e111:c8c6%18
    IPv4 Address. . . . . : 192.168.1.193
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\ariel>
```

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

My browser is running HTTP version 1.1

The screenshot shows a Wireshark packet capture of an HTTP 1.1 GET request. The packet list on the left shows four packets. Packet 141 is the GET request, which is expanded in the packet details pane. The details pane shows the Hypertext Transfer Protocol section with the following fields:

- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
- 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
- Accept-Language: en-US
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Upgrade-Insecure-Requests: 1
- Accept-Encoding: gzip, deflate
- Host: gaia.cs.umass.edu
- If-Modified-Since: Wed, 06 Feb 2019 06:59:01 GMT
- If-None-Match: "80-5813442c3ae7e"
- Connection: Keep-Alive

The packet bytes pane at the bottom shows the raw data of the packet, including the HTTP request line and headers.

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

It was modified on Sunday, 10 February 2019 at 06:17:01 GMT

The screenshot shows a Wireshark packet capture of an HTTP 1.1 200 OK response. The packet list on the left shows four packets. Packet 144 is the 200 OK response, which is expanded in the packet details pane. The details pane shows the Hypertext Transfer Protocol section with the following fields:

- HTTP/1.1 200 OK
- Date: Sun, 10 Feb 2019 06:17:09 GMT
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
- Last-Modified: Sun, 10 Feb 2019 06:17:01 GMT
- ETag: "80-5818423e28c1d"
- Accept-Ranges: bytes
- Content-Length: 128
- Keep-Alive: timeout=5, max=100
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8

The packet bytes pane at the bottom shows the raw data of the packet, including the HTTP response line and headers.

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

The Ip address is: 128.119.245.12

The screenshot shows a Wireshark capture of an HTTP response. The packet list on the left shows four packets. Packet 144 is selected, showing an HTTP 200 OK response from 128.119.245.12 to 192.168.1.193. The packet details pane on the right shows the structure of the response, including the status bar, headers, and body. The status bar indicates 'HTTP/1.1 200 OK'. The headers include 'Date: Sun, 10 Feb 2019 06:17:09 GMT', 'Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3', 'Last-Modified: Sun, 10 Feb 2019 06:17:01 GMT', 'ETag: "80-5818423e28c1d"', 'Accept-Ranges: bytes', 'Content-Length: 128', 'Keep-Alive: timeout=5, max=100', 'Connection: Keep-Alive', and 'Content-Type: text/html; charset=UTF-8'. The body of the response is a line-based text data containing 4 lines.

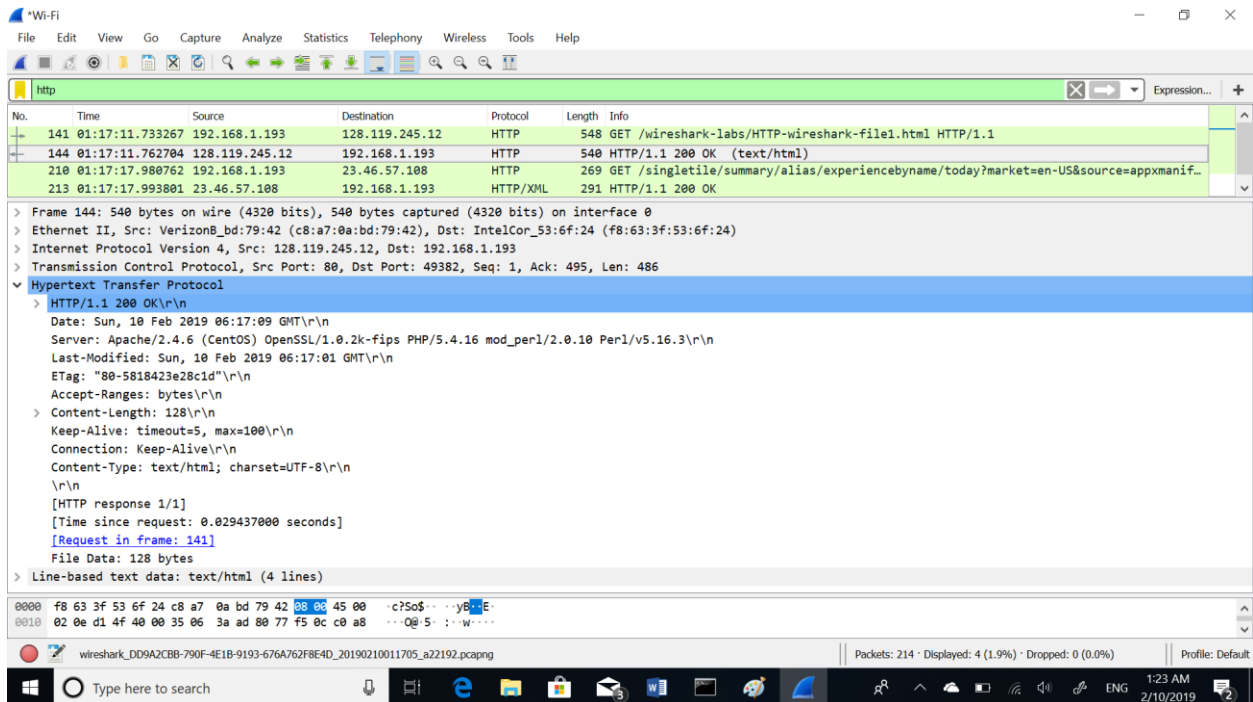
4. What languages does your browser indicate that it can accept to the server?

Language accepted: English-US

The screenshot shows a Wireshark capture of an HTTP request. The packet list on the left shows four packets. Packet 141 is selected, showing an HTTP GET request from 192.168.1.193 to 128.119.245.12. The packet details pane on the right shows the structure of the request, including the status bar, headers, and body. The status bar indicates 'GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1'. The headers include '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', 'Accept-Language: en-US', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8', 'Upgrade-Insecure-Requests: 1', 'Accept-Encoding: gzip, deflate', 'Host: gaia.cs.umass.edu', 'If-Modified-Since: Wed, 06 Feb 2019 06:59:01 GMT', and 'If-None-Match: "80-5813442c3ae7e"'. The body of the request is a line-based text data containing 1 line.

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

The answer is not available



The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area shows a list of captured packets. Packet 144 is selected, showing an HTTP GET request for the file `/wireshark-labs/HTTP-wireshark-file1.html`. The packet details pane shows the following information:

- Frame 144: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
- Ethernet II, Src: Verizon_08:00:0d:79:42:00 (c8:a7:0a:bd:79:42), Dst: IntelCor_53:6f:24 (f8:63:3f:53:6f:24)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.193
- Transmission Control Protocol, Src Port: 80, Dst Port: 49382, Seq: 1, Ack: 495, Len: 486
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Sun, 10 Feb 2019 06:17:09 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 06:17:01 GMT\r\n
 - ETag: "80-5818423e28c1d"\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: 0.029437000 seconds]
 - [\[Request in frame 141\]](#)
 - File Data: 128 bytes
- Line-based text data: text/html (4 lines)

The packet bytes pane shows the raw data of the selected packet, starting with the HTTP status line: `0000 f8 63 3f 53 6f 24 c8 a7 0a bd 79 42 00 00 45 00 c?SoS...yB:E-`.