

**NAME: OBI CHIOMA BLESSING**

**[EMAIL: Obi.chioma@womentechsters.org](mailto:Obi.chioma@womentechsters.org)**

**ID: WT/21/173**

**PRACTICAL ACTIVITY 6**

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

Ans: The Server is running on HTTP version 1.1

The screenshot shows a Wireshark capture of network traffic on the \*eth0 interface. The packet list displays several HTTP packets. A red arrow points to the entry for packet 13, which is an HTTP 200 OK response from 10.0.2.15 to 128.119.245.12. The packet details pane shows the structure of this response, including the status code 200 and version 1.1. The status bar at the bottom indicates that the selected packet is an HTTP Last Modified response, 46 bytes in size.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.316890571	10.0.2.15	128.119.245.12	HTTP	422	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	1.741277552	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)
15	3.376914777	10.0.2.15	128.119.245.12	HTTP	303	GET /favicon.ico HTTP/1.1
17	4.148851424	128.119.245.12	10.0.2.15	HTTP	500	HTTP/1.1 404 Not Found (text/html)

Click to add text

Transmission Control Protocol, Src Port: 80, Dst Port: 44748, Seq: 1, Ack: 369, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Tue, 27 Jul 2021 00:36:35 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Mon, 26 Jul 2021 05:59:02 GMT\r\n

ETag: "80-5c8007336f8b0"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-

00d0 66 69 65 64 3a 20 4d 6f 6e 2c 20 32 36 20 4a 75 fied: Mo n, 26

HTTP Last Modified (http.last\_modified), 46 bytes

Packets: 28 · Displayed: 4 (14.3%) · Dropped: 0 (0.0%) · Profile: Default

2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

Ans: The acceptable language is English, the browser also provides the server with the accept encoding form.

Practicalactivity7.pptx - ...\*eth010:36 PM92%

\*eth0

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

http

No.	Time	Source	Destination	Protocol	Length	Info
48	18.343782008	10.0.2.15	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
50	18.734939773	128.119.245.12	10.0.2.15	HTTP	293	HTTP/1.1 304 Not Modified
52	19.454143905	10.0.2.15	128.119.245.12	HTTP	329	GET /favicon.ico HTTP/1.1
56	19.868342660	128.119.245.12	10.0.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)
32...	184.662336363	10.0.2.15	204.79.197.203	OCSP	436	Request
32...	184.942883062	204.79.197.203	10.0.2.15	OCSP	2336	Response

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nIf-Modified-Since: Mon, 26 Jul 2021 05:59:02 GMT\r\nIf-None-Match: "80-5c8007336f8b0"\r\nCache-Control: max-age=0\r\n

0120	70	2c	2a	2f	2a	3b	71	3d	30	2e	38	0d	0a	41	63	63	p,*/*;q=
0130	65	70	74	2d	4c	61	6e	67	75	61	67	65	3a	20	65	6e	pt-Lang uage:
0140	2d	55	53	2c	65	6e	3b	71	3d	30	2e	35	0d	0a	41	63	-US,en;q
0150	63	65	70	74	2d	45	6e	63	6f	64	69	6e	67	3a	20	67	cept-Enc oding:
0160	7a	69	70	2c	20	64	65	66	6c	61	74	65	0d	0a	43	6f	zip, def
0170	6e	6e	65	63	74	69	6f	6e	3a	20	6b	65	65	70	2d	61	nnection : keep-
0180	6c	69	76	65	0d	0a	55	70	67	72	61	64	65	2d	49	6e	live..Up grade-
0190	73	65	63	75	72	65	2d	52	65	71	75	65	73	74	73	3a	secure-R

HTTP Accept Language (http.accept\_language), 33 bytesPackets: 4886 · Displayed: 6 (0.1%) · Dropped: 0 (0.0%)Profile: Default

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

**Ans:** The source IP address is 10.0.2.15 while the Destination IP address is 128.119.245.12

The image shows a Wireshark network traffic capture on the \*eth0 interface. The packet list shows four packets, with packet 13 selected. Two red arrows point to the Source and Destination IP addresses in the packet list for packet 13: 128.119.245.12 (Source) and 10.0.2.15 (Destination).

No.	Time	Source	Destination	Protocol	Length	Info
9	0.316890571	10.0.2.15	128.119.245.12	HTTP	422	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	1.741277552	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)
15	3.376914777	10.0.2.15	128.119.245.12	HTTP	303	GET /favicon.ico HTTP/1.1
17	4.148851424	128.119.245.12	10.0.2.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

The packet details pane for packet 13 shows the following information:

- Transmission Control Protocol, Src Port: 80, Dst Port: 44748, Seq: 1, Ack: 369, Len: 486
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    - Response Version: HTTP/1.1
    - Status Code: 200
    - [Status Code Description: OK]
    - Response Phrase: OK
    - Date: Tue, 27 Jul 2021 00:36:35 GMT\r\n
    - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n
    - Last-Modified: Mon, 26 Jul 2021 05:59:02 GMT\r\n
    - ETag: "80-5c8007336f8b0"\r\n
    - Accept-Ranges: bytes\r\n
    - Content-Length: 128\r\n

The packet bytes pane shows the raw data of the selected packet, with the last modified date highlighted: .16.3..L ast- fied: Mo n, 26

HTTP Last Modified (http.last\_modified), 46 bytes

Packets: 28 · Displayed: 4 (14.3%) · Dropped: 0 (0.0%) · Profile: Default

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

**Ans:** The status code returned from the server to my browser is 200

The image shows a Wireshark network traffic capture. The top toolbar includes menus like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the toolbar is a packet list table with columns: No., Time, Source, Destination, Protocol, Length, and Info.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.316890571	10.0.2.15	128.119.245.12	HTTP	422	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	1.741277552	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)
15	3.376914777	10.0.2.15	128.119.245.12	HTTP	303	GET /favicon.ico HTTP/1.1
17	4.148851424	128.119.245.12	10.0.2.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Below the packet list, the details pane shows the selected packet (No. 13) expanded to show the Hypertext Transfer Protocol section. A red arrow points to the status code '200 OK'.

Transmission Control Protocol, Src Port: 80, Dst Port: 44748, Seq: 1, Ack: 369, Len: 486

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  - Response Version: HTTP/1.1
  - Status Code: 200
  - [Status Code Description: OK]
  - Response Phrase: OK
  - Date: Tue, 27 Jul 2021 00:36:35 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Mon, 26 Jul 2021 05:59:02 GMT\r\n
  - Etag: "80-5c8007336f8b0"\r\n
  - Accept-Ranges: bytes\r\n
  - Content-Length: 128\r\n

At the bottom, the packet bytes pane shows the raw data for the selected packet, with a hex dump and ASCII representation.

HTTP Last Modified (http.last\_modified), 46 bytes

Packets: 28 · Displayed: 4 (14.3%) · Dropped: 0 (0.0%) · Profile: Default

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

**Ans:** The HTML file was last modified on Monday 26 July 2021 at 5:59:02 GMT

The image shows a Wireshark network traffic capture. The top pane displays a list of packets. Packet 13 is selected, showing an HTTP 200 OK response from 128.119.245.12 to 10.0.2.15. The bottom pane shows the details of this packet, including the HTTP response structure and headers. A red arrow points to the 'Last-Modified' header value: 'Mon, 26 Jul 2021 05:59:02 GMT'.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.316890571	10.0.2.15	128.119.245.12	HTTP	422	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	1.741277552	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)
15	3.376914777	10.0.2.15	128.119.245.12	HTTP	303	GET /favicon.ico HTTP/1.1
17	4.148851424	128.119.245.12	10.0.2.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Transmission Control Protocol, Src Port: 80, Dst Port: 44748, Seq: 1, Ack: 369, Len: 486

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  - Response Version: HTTP/1.1
  - Status Code: 200
  - [Status Code Description: OK]
  - Response Phrase: OK
  - Date: Tue, 27 Jul 2021 00:36:35 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.1.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Mon, 26 Jul 2021 05:59:02 GMT\r\n
  - ETag: "80-5c8007336f8b0"\r\n
  - Accept-Ranges: bytes\r\n
  - Content-Length: 128\r\n

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-  
00d0 66 69 65 64 3a 20 4d 6f 6e 2c 20 32 36 20 4a 75 fied: Mo n, 26

HTTP Last Modified (http.last\_modified), 46 bytes

Packets: 28 · Displayed: 4 (14.3%) · Dropped: 0 (0.0%) Profile: Default



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

**Ans:** 128 bytes of content are being returned to the browser.

The image shows a Wireshark network traffic capture window. The top bar indicates the capture is on the \*eth0 interface. The packet list shows four HTTP packets. Packet 13 is selected, showing an HTTP 200 OK response from 128.119.245.12 to 10.0.2.15. The packet details pane shows the response structure, with the Content-Length field highlighted and a red arrow pointing to it. The Content-Length is 128 bytes. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.316890571	10.0.2.15	128.119.245.12	HTTP	422	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
13	1.741277552	128.119.245.12	10.0.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)
15	3.376914777	10.0.2.15	128.119.245.12	HTTP	303	GET /favicon.ico HTTP/1.1
17	4.148851424	128.119.245.12	10.0.2.15	HTTP	539	HTTP/1.1 404 Not Found (text/html)

[Group: Sequence]  
Response Version: HTTP/1.1  
Status Code: 200  
[Status Code Description: OK]  
Response Phrase: OK  
Date: Tue, 27 Jul 2021 00:36:35 GMT\r\n  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
Last-Modified: Mon, 26 Jul 2021 05:59:02 GMT\r\n  
ETag: "80-5c8007336f8b0"\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

0000 08 00 27 e5 98 01 52 54 00 12 35 02 08 00 45 00 ...RT

Expert Info (\_ws.expert) Packets: 28 · Displayed: 4 (14.3%) · Dropped: 0 (0.0%) Profile: Default

**7. By inspecting the raw data in the packet content pane, do you see any http headers within the data that are not displayed in the packet-listing window? If so, name one.**

**Ans:** I do not see any header that are not displayed in the packet-listing window.