

**HỌ TÊN: NGUYỄN XUÂN TRỰC**

**MSSV: 1513804**

=====o0o=====

## LAB\_2A\_HTTP

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

### SOLUTION

Both of them are version 1.1

Source:

http						
No.	Time	Source	Destination	Protocol	Length	Info
6	07:47:27.530811	10.228.217.54	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
8	07:47:27.557324	13.107.4.52	10.228.217.54	HTTP	566	HTTP/1.1 200 OK (text/plain)
115	07:47:57.604422	10.228.217.54	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
117	07:47:57.604422	Wireshark · Packet 6 · WiFi				
158	07:48:27.72	> Internet Protocol Version 4, Src: 10.228.217.54, Dst: 13.107.4.52				
160	07:48:27.72	> Transmission Control Protocol, Src Port: 58543, Dst Port: 80, Seq: 1, Ack: 1, Len: 111				
186	07:48:57.84	Hypertext Transfer Protocol				
188	07:48:57.87	GET /connecttest.txt HTTP/1.1\r\n				
234	07:49:27.94	[Expert Info (Chat/Sequence): GET /connecttest.txt HTTP/1.1\r\n]				
236	07:49:27.98	[GET /connecttest.txt HTTP/1.1\r\n]				
308	07:49:51.27	[Severity level: Chat]				
309	07:49:51.27	[Group: Sequence]				
311	07:49:51.57	Request Method: GET				
314	07:49:51.57	Request URI: /connecttest.txt				
		Request Version: HTTP/1.1				
		Connection: Close\r\n				
		User-Agent: Microsoft NCSI\r\n				
		Host: www.msftconnecttest.com\r\n				
		\r\n				

Destination:

http						
No.	Time	Source	Destination	Protocol	Length	Info
6	07:47:27.530811	10.228.217.54	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
8	07:47:27.557324	13.107.4.52	10.228.217.54	HTTP	566	HTTP/1.1 200 OK (text/plain)
115	07:47:57.604422	Wireshark · Packet 6 · WiFi				
117	07:47:57.62	> Internet Protocol Version 4, Src: 10.228.217.54, Dst: 13.107.4.52				
158	07:48:27.72	> Transmission Control Protocol, Src Port: 58543, Dst Port: 80, Seq: 1, Ack: 1, Len: 111				
160	07:48:27.75	Hypertext Transfer Protocol				
186	07:48:57.84	GET /connecttest.txt HTTP/1.1\r\n				
188	07:48:57.87	[Expert Info (Chat/Sequence): GET /connecttest.txt HTTP/1.1\r\n]				
234	07:49:27.94	[GET /connecttest.txt HTTP/1.1\r\n]				
236	07:49:27.98	[Severity level: Chat]				
308	07:49:51.27	[Group: Sequence]				
309	07:49:51.27	Request Method: GET				
311	07:49:51.57	Request URI: /connecttest.txt				
314	07:49:51.57	Request Version: HTTP/1.1				
		Connection: Close\r\n				
		User-Agent: Microsoft NCSI\r\n				
		Host: www.msftconnecttest.com\r\n				
		\r\n				

2) What languages (if any) does your browser indicate that it can accept to the server?

### SOLUTION

en-US

http			Wireshark - Packet 578 - WiFi	
No.	Time	Source		
343	07:26:53.295358	10.228.217.54		
345	07:26:53.322344	13.107.4.52		
578	07:27:04.696991	10.228.217.54	GET /multi/check.php HTTP/1.1\r\n	
582	07:27:05.039170	96.43.128.70	[Expert Info (Chat/Sequence): GET /multi/check.php HTTP/1.1\r\n]	
936	07:27:23.456968	10.228.217.54	[GET /multi/check.php HTTP/1.1\r\n]	
943	07:27:23.498953	13.107.4.52	[Severity level: Chat]	
1647	07:27:53.606567	10.228.217.54	[Group: Sequence]	
1649	07:27:53.630536	13.107.4.52	Request Method: GET	
2230	07:28:23.696930	10.228.217.54	Request URI: /multi/check.php	
2232	07:28:23.797026	13.107.4.52	Request Version: HTTP/1.1	
2880	07:28:53.855999	10.228.217.54	Host: 96.43.128.70\r\n	
2882	07:28:53.880059	13.107.4.52	Connection: close\r\n	
3428	07:29:19.786728	10.228.217.54	Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd	
3433	07:29:20.030605	69.195.128.18	Accept-Language: en-US\r\n	
3496	07:29:24.105226	10.228.217.54	User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt\)\r\n	
3498	07:29:24.129272	13.107.4.52	Accept-Encoding: gzip, deflate\r\n	
			referer: http://cnn.com\r\n	

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

### SOLUTION

My computer : 10.228.217.54

gaia.cs.umass.edu : 128.119.245.12

http						
No.	Time	Source	Destination	Protocol	Length	Info
17	07:58:23.945344	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
21	07:58:24.010101	Wireshark - Packet 21 - WiFi				

[Time delta from previous captured frame: 0.014865000 seconds]  
[Time delta from previous displayed frame: 0.249666000 seconds]  
[Time since reference or first frame: 5.457114000 seconds]  
Frame Number: 21  
Frame Length: 293 bytes (2344 bits)  
Capture Length: 293 bytes (2344 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http]  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
> Ethernet II, Src: Holltech\_09:c3:b5 (b0:51:8e:09:c3:b5), Dst: IntelCor\_e2:6b:f2 (70:1c:e7:e2:6b:f2)  
▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.228.217.54  
    0100 .... = Version: 4  
        .... 0101 = Header Length: 20 bytes (5)

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

### SOLUTION

Status code: 304

No.	Time	Wireshark - Packet 21 - WiFi
17	07:58:2	
21	07:58:2	<ul style="list-style-type: none"> <li>&gt; Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.228.217.54</li> <li>&gt; Transmission Control Protocol, Src Port: 80, Dst Port: 50023, Seq: 1, Ack: 614, Len: 239</li> <li>▼ Hypertext Transfer Protocol <ul style="list-style-type: none"> <li>▼ HTTP/1.1 304 Not Modified\r\n <ul style="list-style-type: none"> <li>▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n] <ul style="list-style-type: none"> <li>[HTTP/1.1 304 Not Modified\r\n]</li> <li>[Severity level: Chat]</li> <li>[Group: Sequence]</li> </ul> </li> <li>Response Version: HTTP/1.1</li> <li>Status Code: 304</li> <li>[Status Code Description: Not Modified]</li> <li>Response Phrase: Not Modified</li> <li>Date: Mon, 12 Oct 2020 00:58:23 GMT\r\n</li> <li>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n</li> <li>Connection: Keep-Alive\r\n</li> </ul> </li> </ul> </li> </ul>

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

### SOLUTION

Mon, 12 Oct 2020

No.	Time	Wireshark - Packet 21 - WiFi
17	07:58:2	
21	07:58:2	<ul style="list-style-type: none"> <li>&gt; Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.228.217.54</li> <li>&gt; Transmission Control Protocol, Src Port: 80, Dst Port: 50023, Seq: 1, Ack: 614, Len: 239</li> <li>▼ Hypertext Transfer Protocol <ul style="list-style-type: none"> <li>▼ HTTP/1.1 304 Not Modified\r\n <ul style="list-style-type: none"> <li>▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n] <ul style="list-style-type: none"> <li>[HTTP/1.1 304 Not Modified\r\n]</li> <li>[Severity level: Chat]</li> <li>[Group: Sequence]</li> </ul> </li> <li>Response Version: HTTP/1.1</li> <li>Status Code: 304</li> <li>[Status Code Description: Not Modified]</li> <li>Response Phrase: Not Modified</li> <li>Date: Mon, 12 Oct 2020 00:58:23 GMT\r\n</li> <li>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n</li> <li>Connection: Keep-Alive\r\n</li> </ul> </li> </ul> </li> </ul>

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

### SOLUTION

Length: 496459

No.	Time	Wireshark - Packet 21 - WiFi
17	07:58:2	
21	07:58:2	<ul style="list-style-type: none"> <li>▼ Hypertext Transfer Protocol <ul style="list-style-type: none"> <li>▼ HTTP/1.1 200 OK\r\n <ul style="list-style-type: none"> <li>&gt; [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n] <ul style="list-style-type: none"> <li>Response Version: HTTP/1.1</li> <li>Status Code: 200</li> <li>[Status Code Description: OK]</li> <li>Response Phrase: OK</li> <li>Date: Mon, 12 Oct 2020 00:32:44 GMT\r\n</li> <li>Server: Apache/2.4.29 (Ubuntu)\r\n</li> <li>Last-Modified: Mon, 22 Feb 2016 21:37:15 GMT\r\n</li> <li>Etag: "7934b-52c62a2eaab42"\r\n</li> <li>Accept-Ranges: bytes\r\n</li> <li>Content-Length: 496459\r\n</li> <li>[Content length: 496459]</li> <li>Keep-Alive: timeout=5, max=100\r\n</li> <li>Connection: Keep-Alive\r\n</li> <li>Content-Type: application/pdf\r\n</li> <li>\r\n</li> <li>[HTTP response 1/1]</li> </ul> </li> </ul> </li> </ul> </li> </ul>

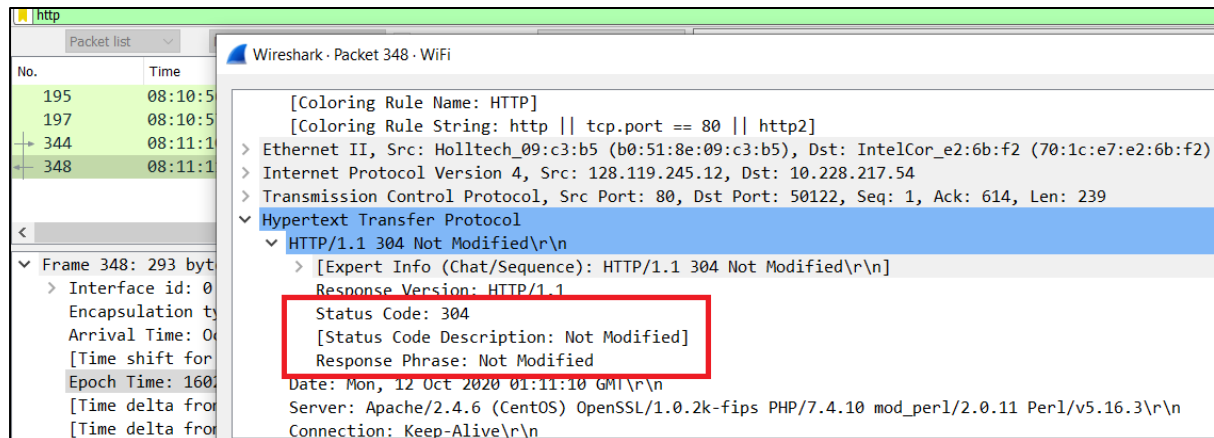
7) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

### SOLUTION

We got a response that said 'HTTP/1.1 304 Not Modified'.

Status code: 304

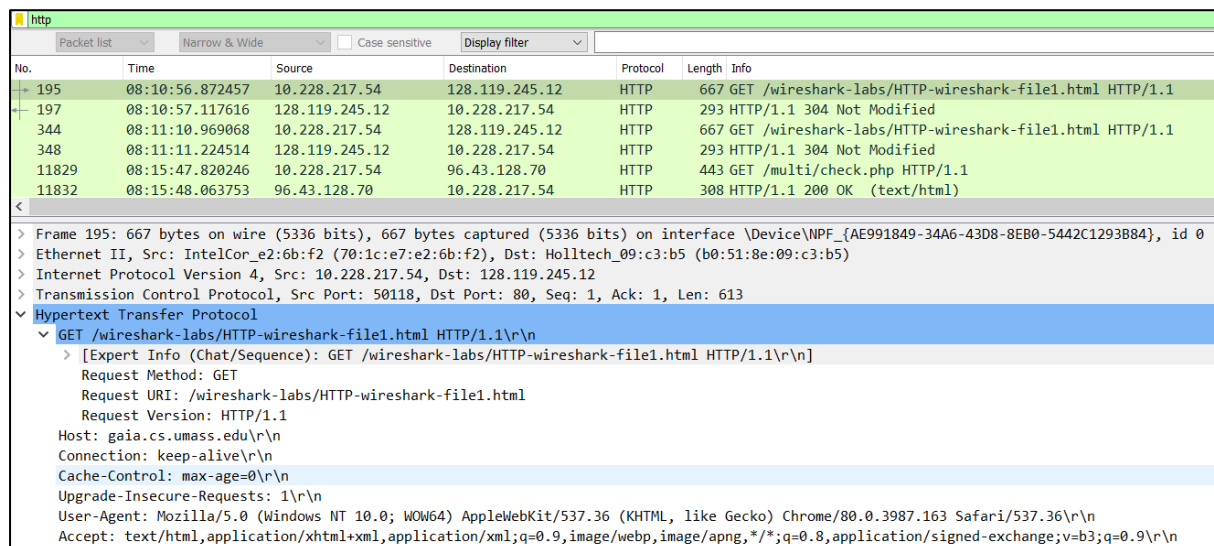
Response Phrase: Not Modified



8) When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

### SOLUTION

The screenshot of first HTTP GET message:



The screenshot of second HTTP GET message:

http							
Packet list		Narrow & Wide		Case sensitive		Display filter	
No.	Time	Source	Destination	Protocol	Length	Info	
195	08:10:56.872457	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	
197	08:10:57.117616	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified	
344	08:11:10.969068	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	
348	08:11:11.224514	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified	
11829	08:15:47.820246	10.228.217.54	96.43.128.70	HTTP	443	GET /multi/check.php HTTP/1.1	
11832	08:15:48.063753	96.43.128.70	10.228.217.54	HTTP	308	HTTP/1.1 200 OK (text/html)	

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
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
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8,vi;q=0.7,zh-CN;q=0.6,zh;q=0.5\r\n
If-None-Match: "80-5b15ee0e0d985"\r\n
If-Modified-Since: Sun, 11 Oct 2020 05:59:01 GMT\r\n
\r\n

9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

### SOLUTION

Not explicitly

http							
Packet list		Narrow & Wide		Case sensitive		Display filter	
No.	Time	Source	Destination	Protocol	Length	Info	
348	08:11:11.224514	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified	
11829	08:15:47.820246	10.228.217.54	96.43.128.70	HTTP	443	GET /multi/check.php HTTP/1.1	
11832	08:15:48.063753	96.43.128.70	10.228.217.54	HTTP	308	HTTP/1.1 200 OK (text/html)	
16718	08:17:07.081262	10.228.217.54	96.43.128.70	HTTP	443	GET /multi/check.php HTTP/1.1	
16723	08:17:07.423898	96.43.128.70	10.228.217.54	HTTP	308	HTTP/1.1 200 OK (text/html)	
20287	08:21:11.501472	10.228.217.54	96.43.128.70	HTTP	443	GET /multi/check.php HTTP/1.1	

Date: Mon, 12 Oct 2020 01:17:06 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: close\r\n
X-Powered-By: PHP/7.1.33\r\n
Content-Encoding: gzip\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.342636000 seconds]
[Request in frame: 16718]
[Request URI: http://96.43.128.70/multi/check.php]
> HTTP chunked response
Content-encoded entity body (gzip): 35 bytes -> 15 bytes
File Data: 15 bytes
Line-based text data: text/html (1 lines)
14.169.155.121

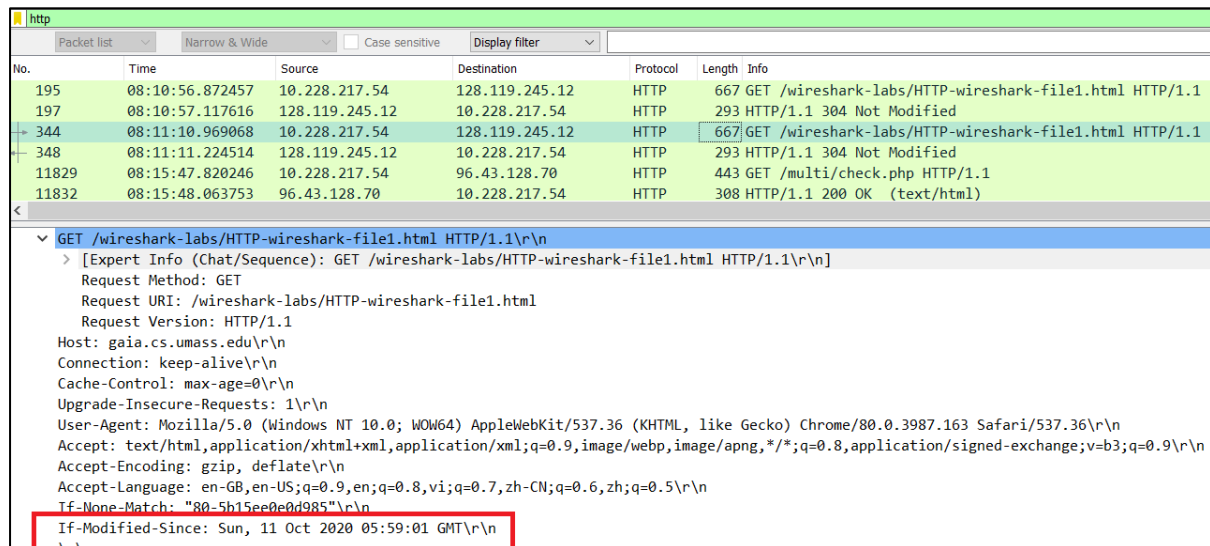
  

0000	31 34 2e 31 36 39 2e 31 35 35 2e 31 32 31 7c	14.169.155.121
------	--	----------------

10) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

### SOLUTION

Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage.



The image shows a Wireshark packet capture of an HTTP GET request. The packet list shows several packets, with packet 344 selected. The packet details pane shows the request structure, including the Host, Connection, Cache-Control, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language, If-None-Match, and If-Modified-Since headers. The If-Modified-Since header is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
195	08:10:56.872457	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
197	08:10:57.117616	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified
344	08:11:10.969068	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
348	08:11:11.224514	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified
11829	08:15:47.820246	10.228.217.54	96.43.128.70	HTTP	443	GET /multi/check.php HTTP/1.1
11832	08:15:48.063753	96.43.128.70	10.228.217.54	HTTP	308	HTTP/1.1 200 OK (text/html)

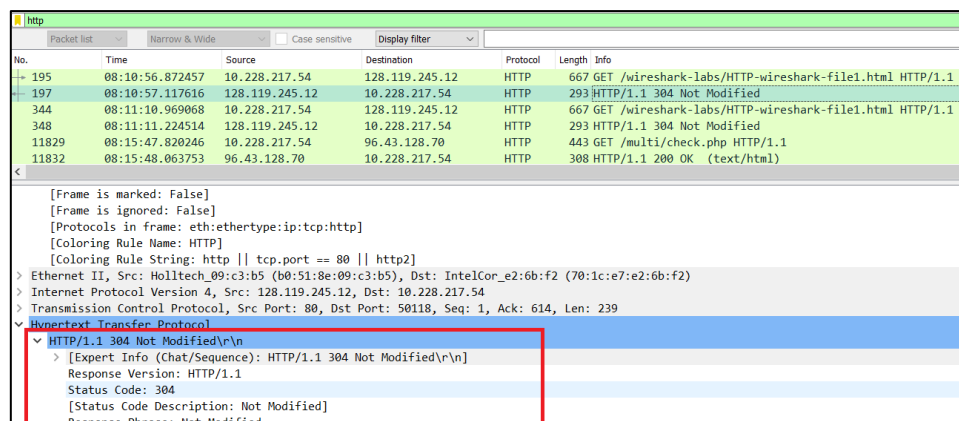
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n  
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]  
Request Method: GET  
Request URI: /wireshark-labs/HTTP-wireshark-file1.html  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-GB,en-US;q=0.9,en;q=0.8,vi;q=0.7,zh-CN;q=0.6,zh;q=0.5\r\nIf-None-Match: "80-5h15ee0e0d985"\r\nIf-Modified-Since: Sun, 11 Oct 2020 05:59:01 GMT\r\n\r\n

11) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

### SOLUTION

+ The HTTP status code is “304: Not Modified”

+ The server did not return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.



The image shows a Wireshark packet capture of an HTTP 304 Not Modified response. The packet list shows several packets, with packet 197 selected. The packet details pane shows the response structure, including the Status Code and Status Code Description. The status code and description are highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
195	08:10:56.872457	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
197	08:10:57.117616	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified
344	08:11:10.969068	10.228.217.54	128.119.245.12	HTTP	667	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
348	08:11:11.224514	128.119.245.12	10.228.217.54	HTTP	293	HTTP/1.1 304 Not Modified
11829	08:15:47.820246	10.228.217.54	96.43.128.70	HTTP	443	GET /multi/check.php HTTP/1.1
11832	08:15:48.063753	96.43.128.70	10.228.217.54	HTTP	308	HTTP/1.1 200 OK (text/html)

[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http]  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
> Ethernet II, Src: Holltech\_09:c3:b5 (b0:51:8e:09:c3:b5), Dst: IntelCor\_e2:6b:f2 (70:1c:e7:e2:6b:f2)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.228.217.54  
> Transmission Control Protocol, Src Port: 80, Dst Port: 50118, Seq: 1, Ack: 614, Len: 239  
Hypertext Transfer Protocol  
HTTP/1.1 304 Not Modified\r\n  
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]  
Response Version: HTTP/1.1  
Status Code: 304  
[Status Code Description: Not Modified]  
Response Phrase: Not Modified

## LAB\_2B\_DNS

1) Run `nslookup` to obtain the IP address of a Web server in Asia. What is the IP address of that server?

### SOLUTION

I performed `nslookup` for [www.vnexpress.net](http://www.vnexpress.net)

```
C:\Users\TRUC BK>nslookup www.vnexpress.net
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     vnexpress.net
Address:  111.65.250.2
Aliases:  www.vnexpress.net
```

2) Run `nslookup` to determine the authoritative DNS servers for a university in Europe.

### SOLUTION

I performed `nslookup` for a European University in Ioannina Greece

```
C:\Users\TRUC BK>nslookup -type=NS uoi.gr
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
uoi.gr  nameserver = sns1.grnet.gr
uoi.gr  nameserver = sns0.grnet.gr
uoi.gr  nameserver = kouzina.noc.uoi.gr
uoi.gr  nameserver = marina.noc.uoi.gr
```

3) Run `nslookup` so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

### SOLUTION

```
C:\Users\TRUC BK>nslookup mail.yahoo.com dns.google
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     edge.gycpi.b.yahoodns.net
Addresses: 2406:2000:a8:800::e6
           2406:2000:a8:800::e7
           119.161.8.11
           119.161.8.12
Aliases:  mail.yahoo.com
```

4) Locate the DNS query and response messages. Are then sent over UDP or TCP?

### SOLUTION

Screenshot for DNS query:

No.	Time	Source	Destination	Protocol	Length	Info
99	08:10:42.622238	8.8.8.8	10.228.217.54	DNS	106	Standard query response 0xe32d A data.alexa.com A 34.228.183.78 A 54.236.79.133
154	08:10:56.009898	10.228.217.54	8.8.8.8	DNS	74	Standard query 0x8ccf A www.google.com
155	08:10:56.049121	8.8.8.8	10.228.217.54	DNS	90	Standard query response 0x8ccf A www.google.com A 172.217.26.132
206	08:11:03.308733	10.228.217.54	8.8.8.8	DNS	75	Standard query 0xf411 A ssl.gstatic.com
207	08:11:03.315731	8.8.8.8	10.228.217.54	DNS	91	Standard query response 0xf411 A ssl.gstatic.com A 172.217.31.227
230	08:11:04.058227	10.228.217.54	8.8.8.8	DNS	79	Standard query 0x8da9 A clients6.google.com

> User Datagram Protocol, Src Port: 53, Dst Port: 58643
> Domain Name System (response)
Transaction ID: 0x7ed1
> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
> Queries
> translate.google.com: type A, class IN
Name: translate.google.com
[Name Length: 20]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

Screenshot for DNS response:

No.	Time	Source	Destination	Protocol	Length	Info
43	08:10:38.050319	10.228.217.54	8.8.8.8	DNS	80	Standard query 0x7ed1 A translate.google.com
44	08:10:38.103175	8.8.8.8	10.228.217.54	DNS	117	Standard query response 0x7ed1 A translate.google.com CNAME www3.l.google.com A 216.58.199.110
98	08:10:42.552339	10.228.217.54	8.8.8.8	DNS	74	Standard query 0xe32d A data.alexa.com
99	08:10:42.622238	8.8.8.8	10.228.217.54	DNS	106	Standard query response 0xe32d A data.alexa.com A 34.228.183.78 A 54.236.79.133
154	08:10:56.009898	10.228.217.54	8.8.8.8	DNS	74	Standard query 0x8ccf A www.google.com
155	08:10:56.049121	8.8.8.8	10.228.217.54	DNS	90	Standard query response 0x8ccf A www.google.com A 172.217.26.132

Additional RRs: 0
> Queries
> translate.google.com: type A, class IN
> Answers
> translate.google.com: type CNAME, class IN, cname www3.l.google.com
Name: translate.google.com
Type: CNAME (canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 21091 (5 hours, 51 minutes, 31 seconds)
Data length: 9
CNAME: www3.l.google.com
> www3.l.google.com: type A, class IN, addr 216.58.199.110
Name: www3.l.google.com
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 74 (1 minute, 14 seconds)
Data length: 4
Address: 216.58.199.110
[Request In: 43]
[Time: 0.052856000 seconds]

0000	70 1c e7 e2 6b f2 b0 51 8e 09 c3 b5 08 00 00 20	p...k.Q.....
0010	00 67 a4 cb 00 00 72 11 af 70 08 08 08 0a e4	g...r...p.....
0020	d9 36 00 35 e5 13 00 53 d7 28 7e d1 81 80 00 01	-6-5-5-(.....
0030	00 02 00 00 00 09 74 72 61 6e 73 6c 61 74 65	.....t translate
0040	06 67 6f 6f 6f 6c 65 03 63 6f 6d 00 00 01 00 01	.....google.com.....
0050	c0 0c 00 05 00 01 00 00 52 63 00 09 04 77 77 77	.....Rc.....www
0060	33 01 6c c0 16 c0 32 00 01 00 01 00 00 00 4a 00	3-1-...2-.....J-

They are sent over UDP.

5) What is the destination port for the DNS query message? What is the source port of DNS response message?

### SOLUTION



```

C:\Users\TRUC BK>ipconfig -all

Windows IP Configuration

    Host Name . . . . . : TrucBK
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : hcmut.edu.vn

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek PCIe GbE Family Controller
    Physical Address. . . . . : 98-40-BB-38-DC-A6
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix . :
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter
    Physical Address. . . . . : 0A-00-27-00-00-15
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::cc1d:2181:6db1:1254%21(Preferred)
    IPv4 Address. . . . . : 192.168.56.1(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
    DHCPv6 IAID . . . . . : 722075687
    DHCPv6 Client DUID. . . . . : 00-01-00-01-23-3A-AF-B3-98-40-BB-38-DC-A6
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VirtualBox Host-Only Network #2:

    Connection-specific DNS Suffix . :
    Description . . . . . : VirtualBox Host-Only Ethernet Adapter #2
    Physical Address. . . . . : 0A-00-27-00-00-0A
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::1449:39ea:d222:3a91%10(Preferred)
    IPv4 Address. . . . . : 192.168.99.1(Preferred)

```

6) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

SOLUTION