

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA KHOA HỌC MÁY TÍNH



LAB 2: PHÂN TÍCH GÓI TIN HTTP
VỚI WIRESHARK

Sniffing HTTP Traffic with WireShark

Môn học: Nhập môn Mạng máy tính

GVHD: PHAN TRUNG PHÁT

Sinh viên thực hiện:

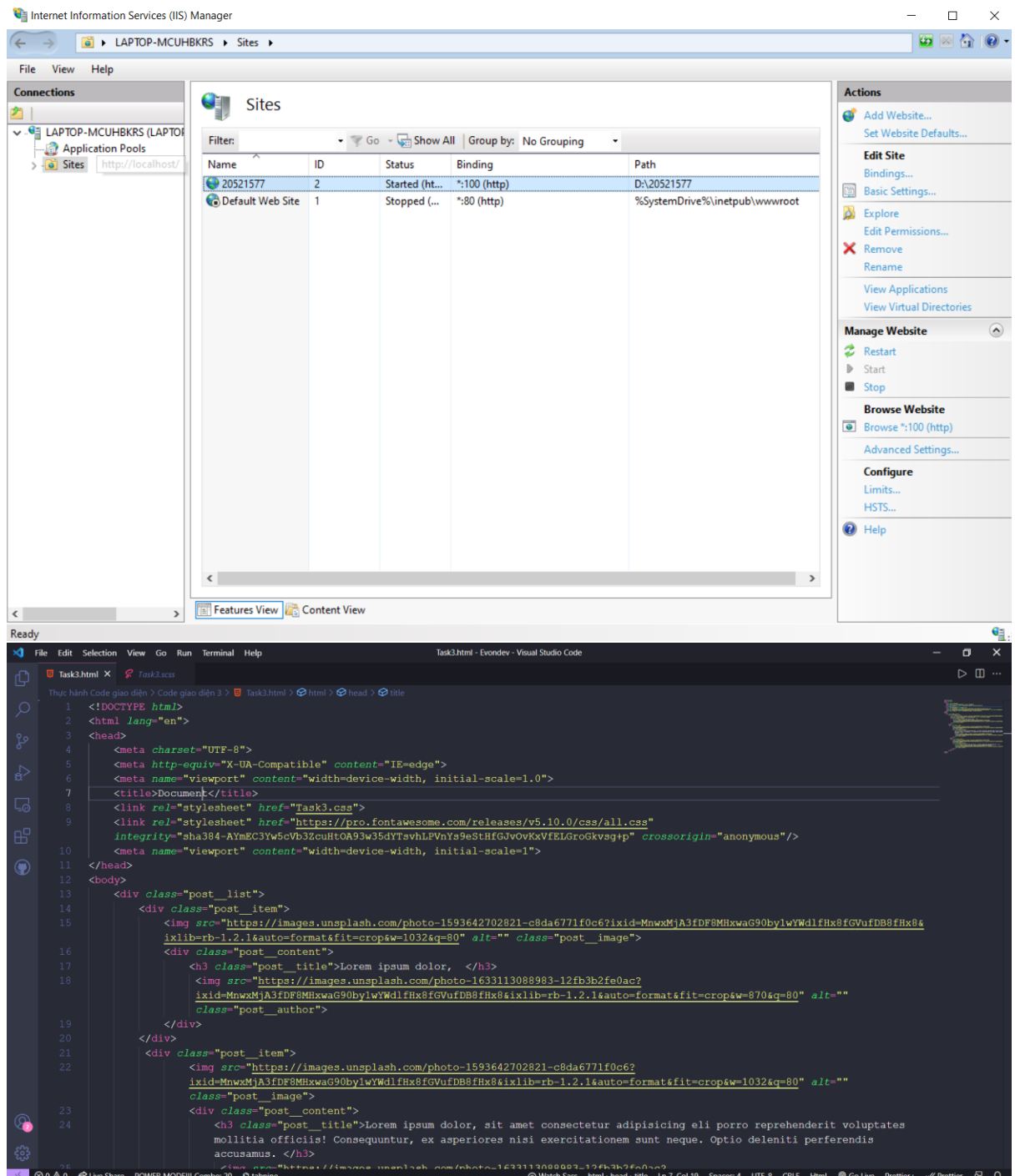
Võ Đăng Phi Long – 20521577

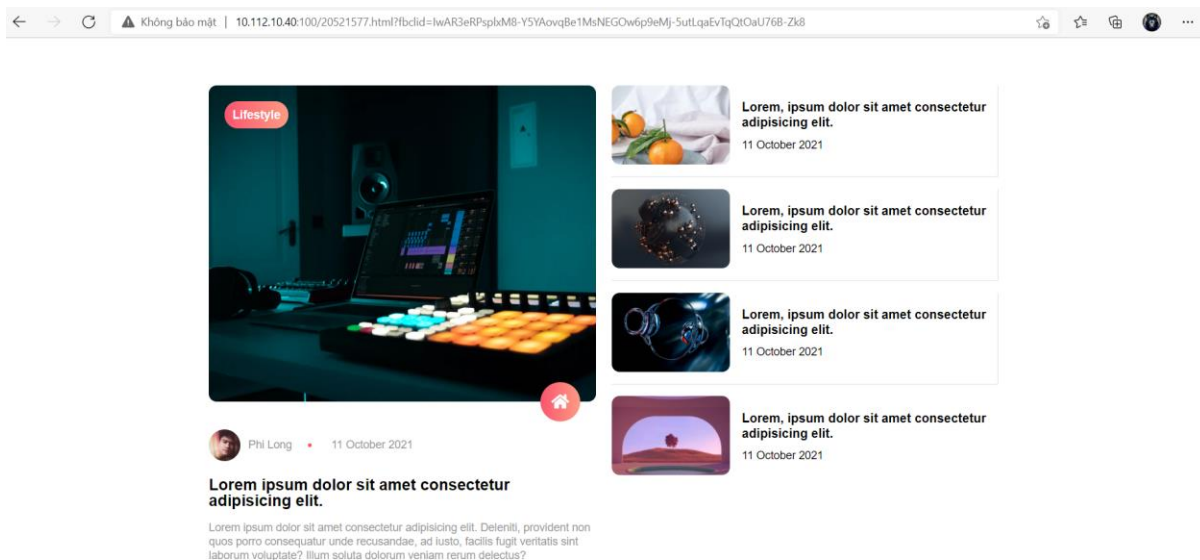
Quảng Trị, ngày 12 tháng 10 năm 2021.

1. Tạo 1 website đơn giản trên localhost:

Em đã lưu trang web với tên [20521577.html](http://localhost/20521577.html). Kích hoạt IIS đồng thời truy cập thành công trang web với đường dẫn của mình:

10.112.10.40:100/20521577.html





Với sự hỗ trợ của Open VPN, em đã truy cập được vào website của bạn cùng lớp với đường dẫn: 10.112.10.47/20522019.html



* Riêng URL của chính em gửi cho bạn khác lại truy cập không được.

2. HTTP GET/response có điều kiện:

- Em vẫn tiếp tục sử dụng URL của bạn trên (10.112.10.47/20522019.html) để phục vụ cho bài làm của mình. Tập lưu **Exercise1.pcapng**

2.1.

- *Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1?*

Trả lời: 1.1

No.	Time	Source	Destination	Protocol	Length	Info
7	0.064728	10.112.10.40	10.112.10.47	HTTP	539	GET /20522019.html HTTP/1.1
9	0.125732	10.112.10.47	10.112.10.40	HTTP	767	HTTP/1.1 200 OK (text/html)

> Frame 7: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{64F3A7B0-9911-4AFB-8E8A-1D6FEDA4785D}, id 0

> Ethernet II, Src: 00:ff:64:f3:a7:b0 (00:ff:64:f3:a7:b0), Dst: 00:ff:65:f3:a7:b0 (00:ff:65:f3:a7:b0)

> Internet Protocol Version 4, Src: 10.112.10.40, Dst: 10.112.10.47

> Transmission Control Protocol, Src Port: 61008, Dst Port: 80, Seq: 1, Ack: 1, Len: 485

> Hypertext Transfer Protocol

> GET /20522019.html HTTP/1.1\r\n

Host: 10.112.10.47\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: vi-VI,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n

\r\n

[Full request URI: http://10.112.10.47/20522019.html]

[HTTP request 1/1]

[Response in frame: 9]

- Phiên bản HTTP server đang sử dụng là bao nhiêu?

No.	Time	Source	Destination	Protocol	Length	Info
7	0.064728	10.112.10.40	10.112.10.47	HTTP	539	GET /20522019.html HTTP/1.1
9	0.125732	10.112.10.47	10.112.10.40	HTTP	767	HTTP/1.1 200 OK (text/html)

> Frame 9: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits) on interface \Device\NPF_{64F3A7B0-9911-4AFB-8E8A-1D6FEDA4785D}, id 0

> Ethernet II, Src: 00:ff:65:f3:a7:b0 (00:ff:65:f3:a7:b0), Dst: 00:ff:64:f3:a7:b0 (00:ff:64:f3:a7:b0)

> Internet Protocol Version 4, Src: 10.112.10.47, Dst: 10.112.10.40

> Transmission Control Protocol, Src Port: 80, Dst Port: 61008, Seq: 1, Ack: 486, Len: 713

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Content-Type: text/html\r\n

Last-Modified: Tue, 12 Oct 2021 02:28:12 GMT\r\n

Accept-Ranges: bytes\r\n

ETag: "43adaecd10bfd71:0"\r\n

Server: Microsoft-IIS/10.0\r\n

Date: Thu, 14 Oct 2021 04:24:49 GMT\r\n

> Content-Length: 488\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.061004000 seconds]

[Request in frame: 7]

2.2.

- Địa chỉ IP của máy tính bạn là bao nhiêu?

Trả lời: 10.112.10.40

No.	Time	Source	Destination	Protocol	Length	Info
7	0.064728	10.112.10.40	10.112.10.47	HTTP	539	GET /20522019.html HTTP/1.1
9	0.125732	10.112.10.47	10.112.10.40	HTTP	767	HTTP/1.1 200 OK (text/html)

- Cửa web server là bao nhiêu?

Trả lời: 10.112.10.47

No.	Time	Source	Destination	Protocol	Length	Info
7	0.064728	10.112.10.40	10.112.10.47	HTTP	539	GET
9	0.125732	10.112.10.47	10.112.10.40	HTTP	767	HTTP

2.3. Mã trạng thái (status code) trả về từ server là gì?

Trả lời: 200 OK

10.112.10.40	10.112.10.47	HTTP	539 GET /20522019.html HTTP/1.1
10.112.10.47	10.112.10.40	HTTP	767 HTTP/1.1 200 OK (text/html)

Server đã trả về một gói tin có nội dung: text. Ta nhìn vào dòng Content – Length (hoặc File Data kéo xuống dưới) thấy tổng cộng có 488 bytes

2.4. Server đã trả về cho trình duyệt bao nhiêu bytes nội dung?

Trả lời: 488

> Frame 9: 767 bytes on wire (6136 bits), 767 bytes captured (6136 bits) on interface \Device\NPF_{64F3A7B0-9911-4AFB-8E8A-1D6FEDA4785D}, id 0			
> Ethernet II, Src: 00:ff:65:f3:a7:b0 (00:ff:65:f3:a7:b0), Dst: 00:ff:64:f3:a7:b0 (00:ff:64:f3:a7:b0)			
> Internet Protocol Version 4, Src: 10.112.10.47, Dst: 10.112.10.40			
> Transmission Control Protocol, Src Port: 80, Dst Port: 61008, Seq: 1, Ack: 486, Len: 713			
▼ Hypertext Transfer Protocol			
> HTTP/1.1 200 OK\r\n			
Content-Type: text/html\r\n			
Last-Modified: Tue, 12 Oct 2021 02:28:12 GMT\r\n			
Accept-Ranges: bytes\r\n			
ETag: "43adaecd10bfd71:0"\r\n			
Server: Microsoft-IIS/10.0\r\n			
Date: Thu, 14 Oct 2021 04:24:49 GMT\r\n			
> Content-Length: 488\r\n			
\r\n			
[HTTP response 1/1]			
[Time since request: 0.061004000 seconds]			
[Request in frame: 71]			
0100	43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20	Content-Length:	
0110	34 38 38 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45	488...< !DOCTYPE	
0120	20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a	html>... <html>..	
0130	3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68	<head>... <meta ch	
0140	61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e	arset="U TF-8" />	
0150	0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70	.. <m eta http	

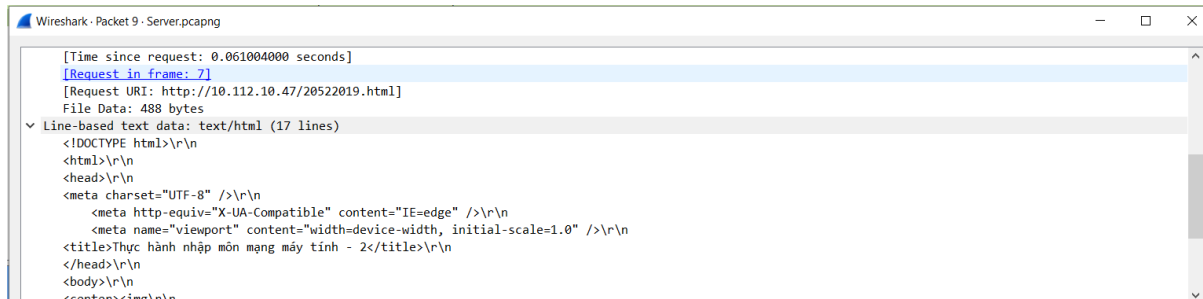
2.5. Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng “IF-MODIFIED - SINCE” hay không?

Trả lời: Không

Wireshark - Packet 7 - Server.pcapng			
> Frame 7: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{64F3A7B0-9911-4AFB-8E8A-1D6FEDA4785D}, id 0			
> Ethernet II, Src: 00:ff:64:f3:a7:b0 (00:ff:64:f3:a7:b0), Dst: 00:ff:65:f3:a7:b0 (00:ff:65:f3:a7:b0)			
> Internet Protocol Version 4, Src: 10.112.10.40, Dst: 10.112.10.47			
> Transmission Control Protocol, Src Port: 61008, Dst Port: 80, Seq: 1, Ack: 1, Len: 485			
▼ Hypertext Transfer Protocol			
> GET /20522019.html HTTP/1.1\r\n			
Host: 10.112.10.47\r\n			
Connection: keep-alive\r\n			
Upgrade-Insecure-Requests: 1\r\n			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n			
\r\n			
[Full request URI: http://10.112.10.47/20522019.html]			
0000	00 ff 65 f3 a7 b0 00 ff 64 f3 a7 b0 08 00 45 00	..e....d....E	
0010	02 0d 95 a3 40 00 08 06 3a 11 0a 70 0a 28 0a 70	...@...:..p(.p	
0020	0a 2f ee 50 00 50 29 a1 3a 8f 40 43 86 c9 50 18	..P.P):.@C.P	
0030	04 05 59 fe 00 00 47 45 54 20 2f 32 30 35 32 32	..Y...GE T /20522	
0040	30 31 39 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e	019.html HTTP/1.	
0050	31 0d 0a 48 6f 73 74 3a 20 31 30 2e 31 31 32 2e	1--Host: 10.112.	
0060	31 30 2e 34 37 0d 0a 43 6f 6e 6e 65 63 74 69 6f	10.47.-C connectio	
0070	6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55	n: keep-alive-U	
0080	70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d	pgrade-I nsecure-	
0090	52 65 71 75 65 73 74 73 3a 20 31 0d 0a 59 73 65	Requests : 1..Use	
00a0	72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61	r-Agent: Mozilla	
00b0	2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54	/5.0 (Windows NT	
00c0	20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36	10.0; Win64; x6	
00d0	34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35	4) AppleWebKit/5	
00e0	33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69	37.36 (KHTML, li	
00f0	6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65	ke Gecko) Chrome	
0100	2f 39 34 2e 30 2e 34 36 30 36 2e 38 31 20 53 61	/94.0.46 06.81 Sa	
0110	66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63	fari/537 .36..Acc	

2.6. Xem xét nội dung phản hồi từ server. Server có thật sự trả về nội dung của file HTML hay không? Tại sao?

Trả lời: Máy chủ đã response bằng cách nhìn vào dòng Line-base text data, ta thấy được nội dung của file html



The image shows a Wireshark packet capture window titled "Wireshark - Packet 9 - Server.pcapng". It displays the details of a selected packet, showing the "Line-based text data: text/html (17 lines)". The content is an HTML document with a DOCTYPE declaration, a meta charset of "UTF-8", a meta http-equiv of "X-UA-Compatible" with content="IE=edge", a meta name of "viewport" with content="width=device-width, initial-scale=1.0", and a title "Thực hành nhập môn mạng máy tính - 2". The body contains a center tag with an image tag.

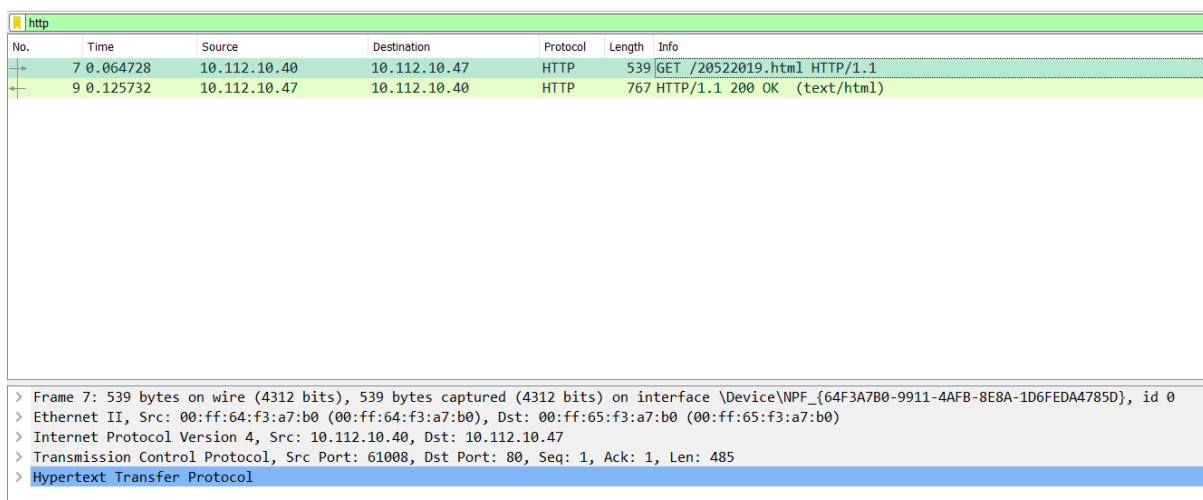
```
[Time since request: 0.061004000 seconds]
[Request in frame: 7]
[Request URI: http://10.112.10.47/20522019.html]
File Data: 488 bytes
Line-based text data: text/html (17 lines)
<!DOCTYPE html>\r\n
<html>\r\n
<head>\r\n
<meta charset="UTF-8" />\r\n
<meta http-equiv="X-UA-Compatible" content="IE=edge" />\r\n
<meta name="viewport" content="width=device-width, initial-scale=1.0" />\r\n
<title>Thực hành nhập môn mạng máy tính - 2</title>\r\n
</head>\r\n
<body>\r\n
<center><img>\r\n
```

Khi ta xóa Cache của trình duyệt rồi gửi Request GET “ĐẦU TIÊN” lên server để yêu cầu trả file về, file này chưa hề được lưu trong bộ nhớ Cache ở client nên file trực tiếp trả về từ Server.

2.7. Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng “IF-MODIFIED- SINCE” hay không? Nếu có, giá trị của IF-MODIFIED-SINCE là gì?

2.8. Mã trạng thái HTTP được trả về từ server tương ứng với HTTP GET thứ 2 là gì? Ý nghĩa nó là gì? Server có thật sự gửi về nội dung của file hay không? Giải thích

2.9. Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?



The image shows a Wireshark packet capture window titled "http". It displays a list of packets in a table format. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. There are two packets shown: packet 7 (GET /20522019.html HTTP/1.1) and packet 9 (HTTP/1.1 200 OK (text/html)).

No.	Time	Source	Destination	Protocol	Length	Info
7	0.064728	10.112.10.40	10.112.10.47	HTTP	539	GET /20522019.html HTTP/1.1
9	0.125732	10.112.10.47	10.112.10.40	HTTP	767	HTTP/1.1 200 OK (text/html)

Below the table, there is a detailed view of the selected packet (packet 9) showing the frame structure and the protocol details. The details pane shows the frame structure and the protocol details, including the Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers.

Như ảnh chụp trên, em chỉ bắt được một HTTP GET duy nhất, không có thứ 2 nên 3 câu hỏi trên chưa thể trả lời. Nên em sẽ tham khảo kết quả của bạn mình để trả lời theo hiểu biết của mình.

- **Câu 2.7:** Qua tham khảo, bài của bạn có xuất hiện dòng IF-MODIFIED-SINCE này ngày tại mục **Hypertext Transfer Protocol**
- **Câu 2.8:** Kết quả trả về 304 Not Modified \Rightarrow Ý nghĩa: Sử dụng cho mục đích caching. Cho client biết rằng Response chưa được điều chỉnh, nên client có thể tiếp tục sử dụng cùng phiên bản phản hồi trong bộ nhớ cache.
- **Câu 2.9:** Bài làm của bạn ấy có 3 HTTP GET gửi đến.

3. Truy cập các trang HTTP dài:

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

3.10.

- Trình duyệt đã gửi bao nhiêu HTTP GET?

No.	Time	Source	Destination	Protocol	Length	Info
101	2.880658	192.168.0.106	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
115	3.130055	128.119.245.12	192.168.0.106	HTTP	559	HTTP/1.1 200 OK (text/html)
117	3.323019	192.168.0.106	128.119.245.12	HTTP	501	GET /favicon.ico HTTP/1.1
118	3.571400	128.119.245.12	192.168.0.106	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Trả lời: Có 2 trình duyệt gửi yêu cầu HTTP GET đến máy chủ.

- Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

Trả lời: Nó nằm trong gói tin thứ 115

No.	Time	Source	Destination	Protocol	Length	Info
101	2.880658	192.168.0.106	128.119.245.12	HTTP	555	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
115	3.130055	128.119.245.12	192.168.0.106	HTTP	559	HTTP/1.1 200 OK (text/html)
117	3.323019	192.168.0.106	128.119.245.12	HTTP	501	GET /favicon.ico HTTP/1.1
118	3.571400	128.119.245.12	192.168.0.106	HTTP	538	HTTP/1.1 404 Not Found (text/html)

[Next response in frame: 118]	
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]	
File Data: 4500 bytes	
Line-based text data: text/html (98 lines)	
<pre> <html><head> \n <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n \n <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n <p>
\n </p>\n <p><p><center>THE BILL OF RIGHTS
\n Amendments 1-10 of the Constitution\n </center>\n \n <p>The Conventions of a number of the States having, at the time of adopting\n the Constitution, expressed a desire, in order to prevent misconstruction\n </pre>	
01f0	70 3e 3c 62 72 3e 0a 3c 2f 70 3e 0a 3c 70 3e 3c p> < /p> <p>
0200	2f 70 3e 3c 63 65 6e 74 65 72 3e 3c 62 3e 54 48 /p><center>er>T
0210	45 20 42 49 4c 4c 20 4f 46 20 52 49 47 48 54 53 E BILL O F RIGHTS
0220	3c 2f 62 3c 62 72 3e 0a 20 20 3c 65 6d 3e 41 A
0230	6d 65 6e 64 6d 65 6e 74 73 20 31 2d 31 30 20 6f mendment s 1-10 o

3.11. Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

Trả lời: Cần 3 TCP Segments

```
TCP payload (505 bytes)
TCP segment data (505 bytes)
> [3 Reassembled TCP Segments (4861 bytes): #112(2904), #114(1452), #115(505)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

4. Chứng thực HTTP

Trả lời các câu hỏi sau:

4.12. Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

Trả lời: 401 Unauthorized: là mã trạng thái HTTP có nghĩa là bạn đang cố gắng truy cập không thể tải cho đến khi bạn đăng nhập lần đầu bằng ID và password hợp lệ.

4.13. Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?

Trả lời: Xuất hiện một trường mới là Authorization.

```
> Transmission Control Protocol, Src Port: 56261, Dst Port: 80, Seq: 1, Ack: 1, Len: 618
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYXJrLlXN0dWRlbnRzOm5ldHdvcm0=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]
    [Response in frame: 119]
```