Câu 1: Trình duyệt đang sử dụng phiên bản HTTP 1.0 hay 1.1? Phiên bản HTTP server đang sử dụng là bao nhiêu?

Trình duyệt đang sử dụng bản 1.1. Phiên bản HTTP server đang sử dụng bản 1.1

```
518 GET /20520605.html HTTP/1.1
499 HTTP/1.1 200 OK  (text/html)
```

Câu 2: Địa chỉ IP của máy tính bạn là bao nhiêu? Của web server là bao nhiêu?

Địa chỉ IP của máy tính là 192.168.1.2

Địa chỉ IP của server là 3.17.7.232

Câu 3: Mã trạng thái (status code) trả về từ server là gì?

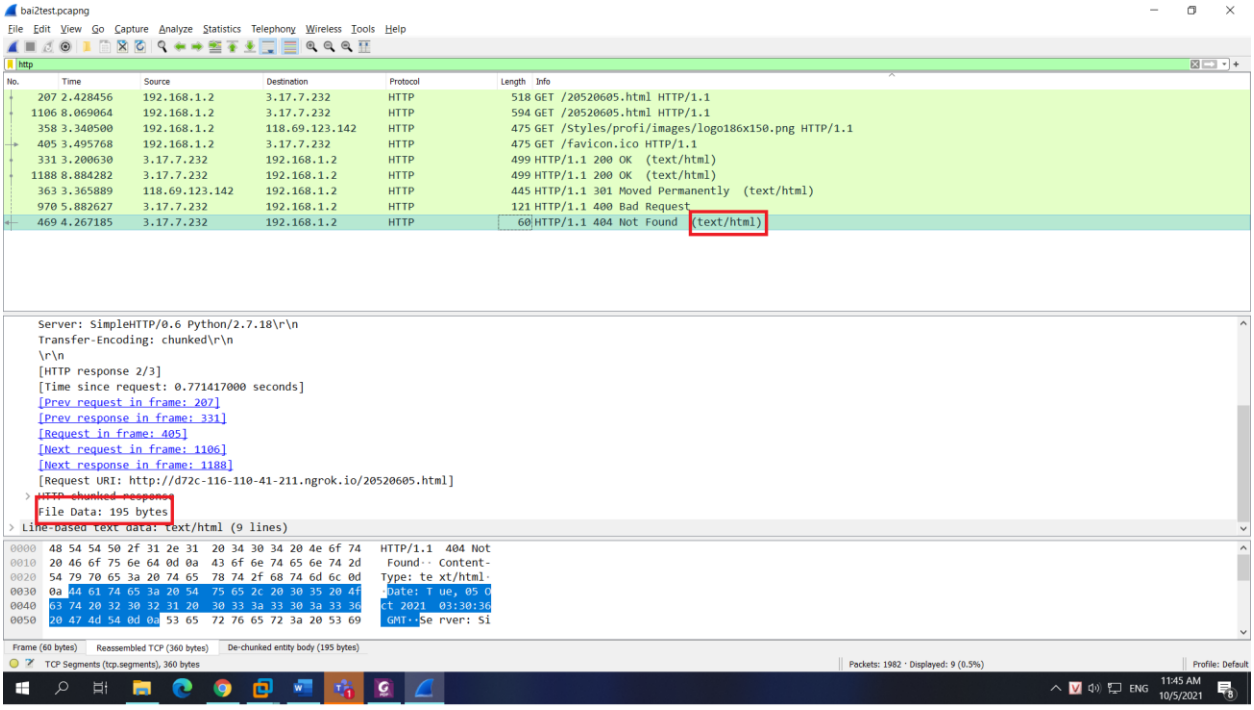
Các mã trạng thái (status code) trả về từ server là 200 OK, 301 Moved Permanently, 400 Bad Request, 404 Not Found

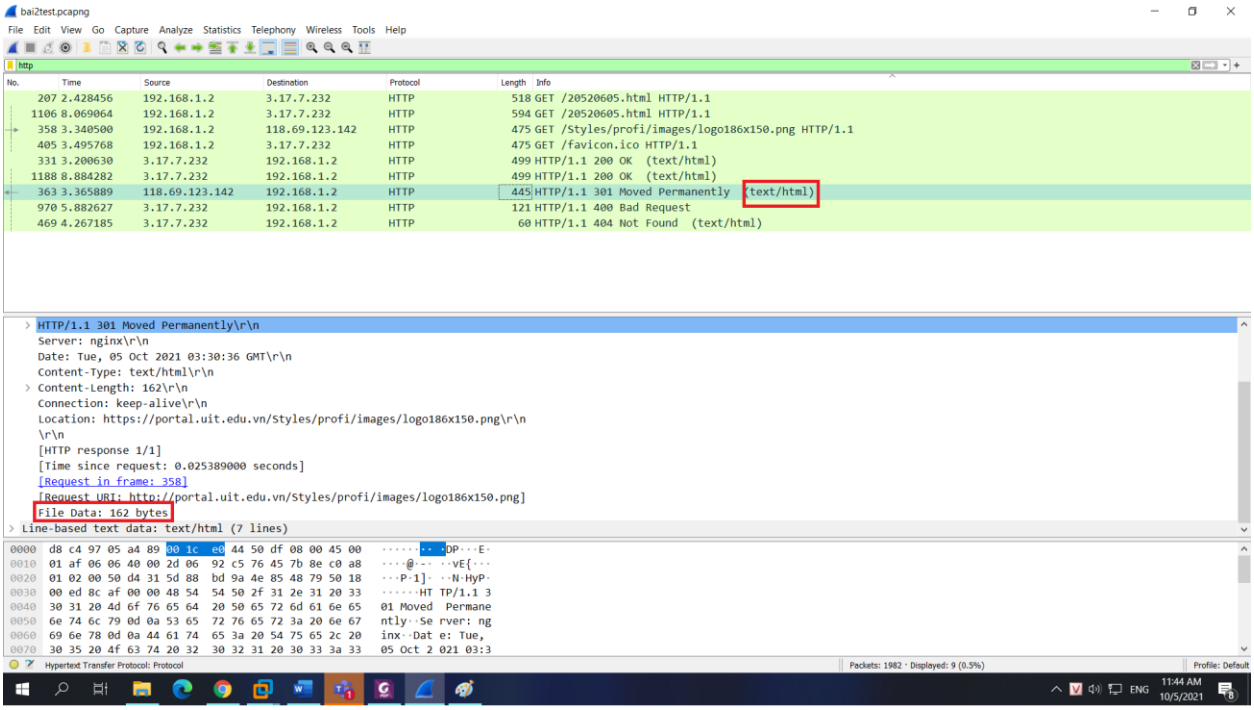
```
HTTP/1.1 200 OK  (text/html)
HTTP/1.1 200 OK  (text/html)
HTTP/1.1 301 Moved Permanently  (text/html)
HTTP/1.1 400 Bad Request
HTTP/1.1 404 Not Found  (text/html)
```

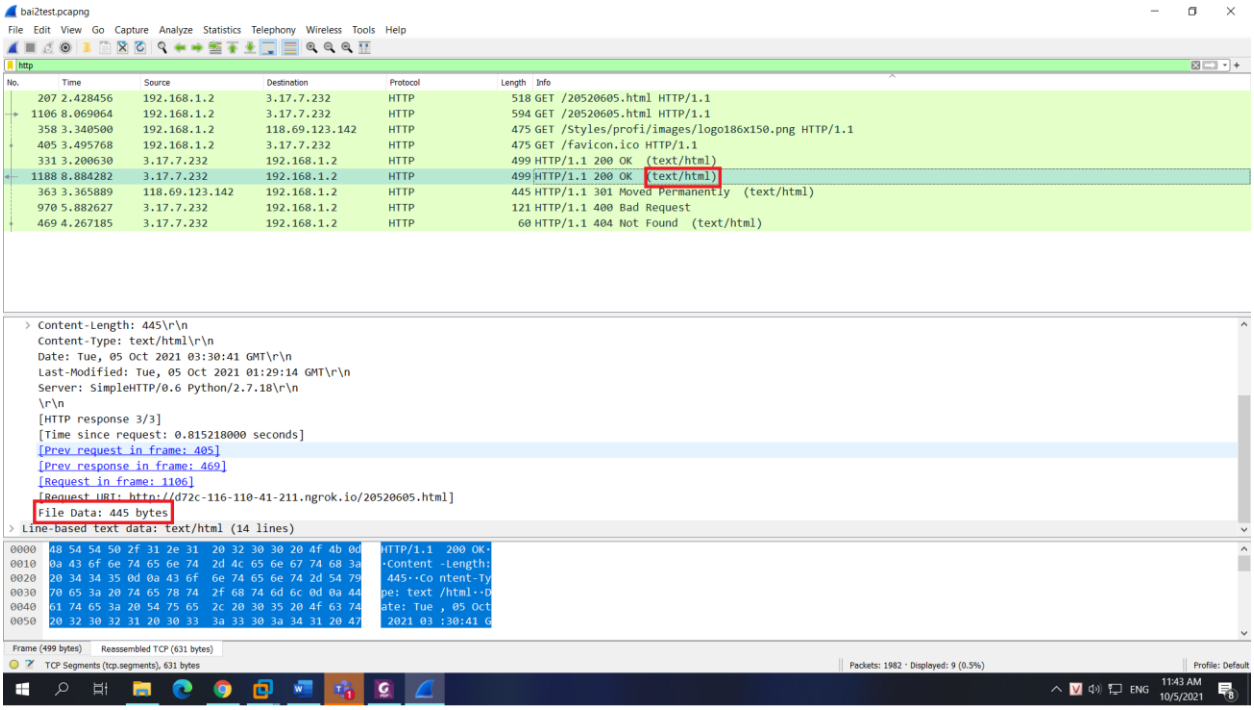
Câu 4: Server đã trả về cho trình duyệt bao nhiêu bytes nội dung?

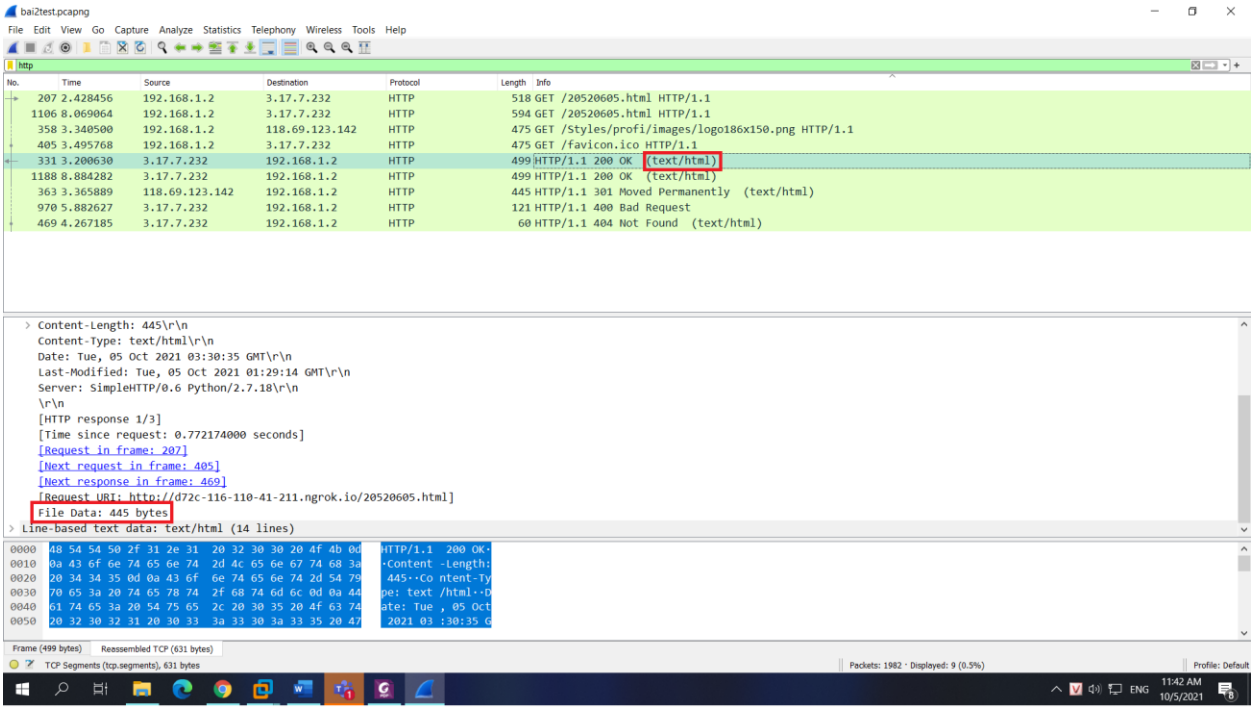
Trả về 4 gói tin: text

Với 445, 445, 162 và 195 bytes ứng với mỗi tập tin


bai2test.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
207 2.428456 192.168.1.2 3.17.7.232 HTTP 518 GET /20520605.html HTTP/1.1
1106 8.069064 192.168.1.2 3.17.7.232 HTTP 594 GET /20520605.html HTTP/1.1
358 3.340500 192.168.1.2 118.69.123.142 HTTP 475 GET /Styles/profi/images/logo186x150.png HTTP/1.1
405 3.495768 192.168.1.2 3.17.7.232 HTTP 475 GET /favicon.ico HTTP/1.1
331 3.200630 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
1188 8.884282 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
363 3.365889 118.69.123.142 192.168.1.2 HTTP 445 HTTP/1.1 301 Moved Permanently (text/html)
970 5.882627 3.17.7.232 192.168.1.2 HTTP 121 HTTP/1.1 400 Bad Request
469 4.267185 3.17.7.232 192.168.1.2 HTTP 60 HTTP/1.1 404 Not Found (text/html)
Server: SimpleHTTP/0.6 Python/2.7.18\r\n
Transfer-Encoding: chunked\r\n
\r\n
[HTTP response 2/3]
[Time since request: 0.771417000 seconds]
[Prev request in frame: 207]
[Prev response in frame: 331]
[Request in frame: 405]
[Next request in frame: 1106]
[Next response in frame: 1188]
[Request URI: http://d72c-116-110-41-211.ngrok.io/20520605.html]
HTTP chunked response
File Data: 195 bytes
Line-based text data: text/html (9 lines)
0000 48 54 54 50 2f 31 2e 31 20 34 30 34 20 4e 6f 74 HTTP/1.1 404 Not
0010 20 46 6f 75 6e 64 0d 0a 43 6f 6e 74 65 6e 74 2d Found·· Content-
0020 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d Type: te xt/html·
0030 0a 44 61 74 65 3a 20 54 75 65 2c 20 30 35 20 4f ·Date: T ue, 05 O
0040 63 74 20 32 30 32 31 20 30 33 3a 33 30 3a 33 36 ct 2021 03:30:36
0050 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 53 69 GMT··Se rver: Si
Frame (60 bytes) Reassembled TCP (360 bytes) De-chunked entity body (195 bytes)
TCP Segments (tcp.segments), 360 bytes
Packets: 1982 · Displayed: 9 (0.5%)
Profile: Default
ENG 11:45 AM 10/5/2021

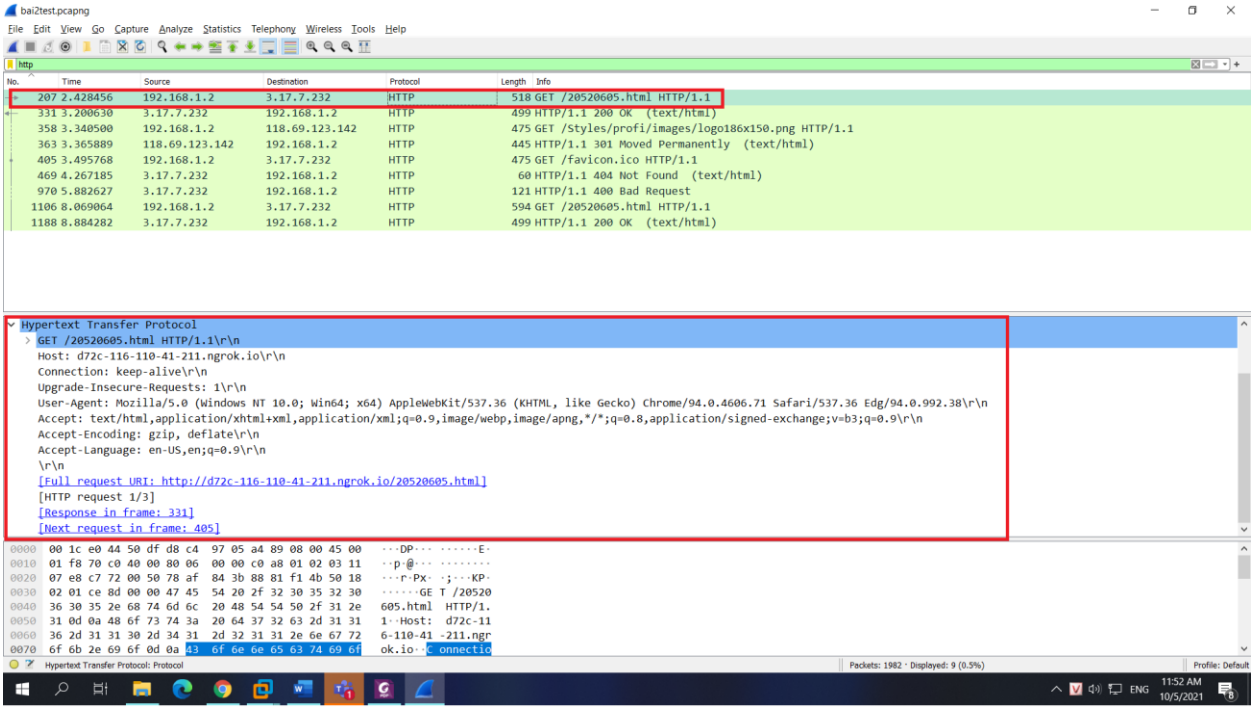

bai2test.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
207 2.428456 192.168.1.2 3.17.7.232 HTTP 518 GET /20520605.html HTTP/1.1
1106 8.069064 192.168.1.2 3.17.7.232 HTTP 594 GET /20520605.html HTTP/1.1
358 3.340500 192.168.1.2 118.69.123.142 HTTP 475 GET /Styles/profi/images/logo186x150.png HTTP/1.1
405 3.495768 192.168.1.2 3.17.7.232 HTTP 475 GET /favicon.ico HTTP/1.1
331 3.200630 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
1188 8.884282 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
363 3.365889 118.69.123.142 192.168.1.2 HTTP 445 HTTP/1.1 301 Moved Permanently (text/html)
970 5.882627 3.17.7.232 192.168.1.2 HTTP 121 HTTP/1.1 400 Bad Request
469 4.267185 3.17.7.232 192.168.1.2 HTTP 60 HTTP/1.1 404 Not Found (text/html)
HTTP/1.1 301 Moved Permanently\r\n
Server: nginx\r\n
Date: Tue, 05 Oct 2021 03:30:36 GMT\r\n
Content-Type: text/html\r\n
Content-Length: 162\r\n
Connection: keep-alive\r\n
Location: https://portal.uit.edu.vn/Styles/profi/images/logo186x150.png\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.025389000 seconds]
[Request in frame: 358]
[Request URI: http://portal.uit.edu.vn/Styles/profi/images/logo186x150.png]
File Data: 162 bytes
Line-based text data: text/html (7 lines)
0000 d8 c4 97 05 a4 89 00 1c e0 44 50 df 08 00 45 00 ·····DP···E·
0010 01 af 06 06 40 00 2d 06 92 c5 76 45 7b 8e c0 a8 ····@·-· ··vE{···
0020 01 02 00 50 d4 31 5d 88 bd 9a 4e 85 48 79 50 18 ···P·1]· ··N·HyP·
0030 00 ed 8c af 00 00 48 54 54 50 2f 31 2e 31 20 33 ·····HT TP/1.1 3
0040 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 01 Moved Permane
0050 6e 74 6c 79 0d 0a 53 65 72 76 65 72 3a 20 6e 67 ntly··Se rver: ng
0060 69 6e 78 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 inx··Dat e: Tue,
0070 30 35 20 4f 63 74 20 32 30 32 31 20 30 33 3a 33 05 Oct 2 021 03:3
Hypertext Transfer Protocol: Protocol
Packets: 1982 · Displayed: 9 (0.5%)
Profile: Default
ENG 11:44 AM 10/5/2021


bai2test.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
207 2.428456 192.168.1.2 3.17.7.232 HTTP 518 GET /20520605.html HTTP/1.1
1106 8.069064 192.168.1.2 3.17.7.232 HTTP 594 GET /20520605.html HTTP/1.1
358 3.340500 192.168.1.2 118.69.123.142 HTTP 475 GET /Styles/profi/images/logo186x150.png HTTP/1.1
405 3.495768 192.168.1.2 3.17.7.232 HTTP 475 GET /favicon.ico HTTP/1.1
331 3.200630 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
1188 8.884282 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
363 3.365889 118.69.123.142 192.168.1.2 HTTP 445 HTTP/1.1 301 Moved Permanently (text/html)
970 5.882627 3.17.7.232 192.168.1.2 HTTP 121 HTTP/1.1 400 Bad Request
469 4.267185 3.17.7.232 192.168.1.2 HTTP 60 HTTP/1.1 404 Not Found (text/html)
Content-Length: 445\r\n
Content-Type: text/html\r\n
Date: Tue, 05 Oct 2021 03:30:41 GMT\r\n
Last-Modified: Tue, 05 Oct 2021 01:29:14 GMT\r\n
Server: SimpleHTTP/0.6 Python/2.7.18\r\n
\r\n
[HTTP response 3/3]
[Time since request: 0.815218000 seconds]
[Prev request in frame: 405]
[Prev response in frame: 469]
[Request in frame: 1106]
[Request URI: http://d72c-116-110-41-211.ngrok.io/20520605.html]
File Data: 445 bytes
Line-based text data: text/html (14 lines)
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK·
0010 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
0020 20 34 34 35 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 445··Co ntent-Ty
0030 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 44 pe: text /html··D
0040 61 74 65 3a 20 54 75 65 2c 20 30 35 20 4f 63 74 ate: Tue , 05 Oct
0050 20 32 30 32 31 20 30 33 3a 33 30 3a 34 31 20 47 2021 03 :30:41 G
Frame (499 bytes) Reassembled TCP (631 bytes)
TCP Segments (tcp.segments), 631 bytes
Packets: 1982 · Displayed: 9 (0.5%)
Profile: Default
ENG 11:43 AM 10/5/2021


bai2test.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
207 2.428456 192.168.1.2 3.17.7.232 HTTP 518 GET /20520605.html HTTP/1.1
1106 8.069064 192.168.1.2 3.17.7.232 HTTP 594 GET /20520605.html HTTP/1.1
358 3.340500 192.168.1.2 118.69.123.142 HTTP 475 GET /Styles/profi/images/logo186x150.png HTTP/1.1
405 3.495768 192.168.1.2 3.17.7.232 HTTP 475 GET /favicon.ico HTTP/1.1
331 3.200630 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
1188 8.884282 3.17.7.232 192.168.1.2 HTTP 499 HTTP/1.1 200 OK (text/html)
363 3.365889 118.69.123.142 192.168.1.2 HTTP 445 HTTP/1.1 301 Moved Permanently (text/html)
970 5.882627 3.17.7.232 192.168.1.2 HTTP 121 HTTP/1.1 400 Bad Request
469 4.267185 3.17.7.232 192.168.1.2 HTTP 60 HTTP/1.1 404 Not Found (text/html)
Content-Length: 445\r\n
Content-Type: text/html\r\n
Date: Tue, 05 Oct 2021 03:30:35 GMT\r\n
Last-Modified: Tue, 05 Oct 2021 01:29:14 GMT\r\n
Server: SimpleHTTP/0.6 Python/2.7.18\r\n
\r\n
[HTTP response 1/3]
[Time since request: 0.772174000 seconds]
[Request in frame: 207]
[Next request in frame: 405]
[Next response in frame: 469]
[Request URI: http://d72c-116-110-41-211.ngrok.io/20520605.html]
File Data: 445 bytes
Line-based text data: text/html (14 lines)
0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK·
0010 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
0020 20 34 34 35 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 445··Co ntent-Ty
0030 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 44 pe: text /html··D
0040 61 74 65 3a 20 54 75 65 2c 20 30 35 20 4f 63 74 ate: Tue , 05 Oct
0050 20 32 30 32 31 20 30 33 3a 33 30 3a 33 35 20 47 2021 03 :30:35 G
Frame (499 bytes) Reassembled TCP (631 bytes)
TCP Segments (tcp.segments), 631 bytes
Packets: 1982 · Displayed: 9 (0.5%)
Profile: Default
ENG 11:42 AM 10/5/2021

Câu 5: Xem xét nội dung của HTTP GET đầu tiên. Bạn có thấy dòng “IF-MODIFIEDSINCE” hay không?

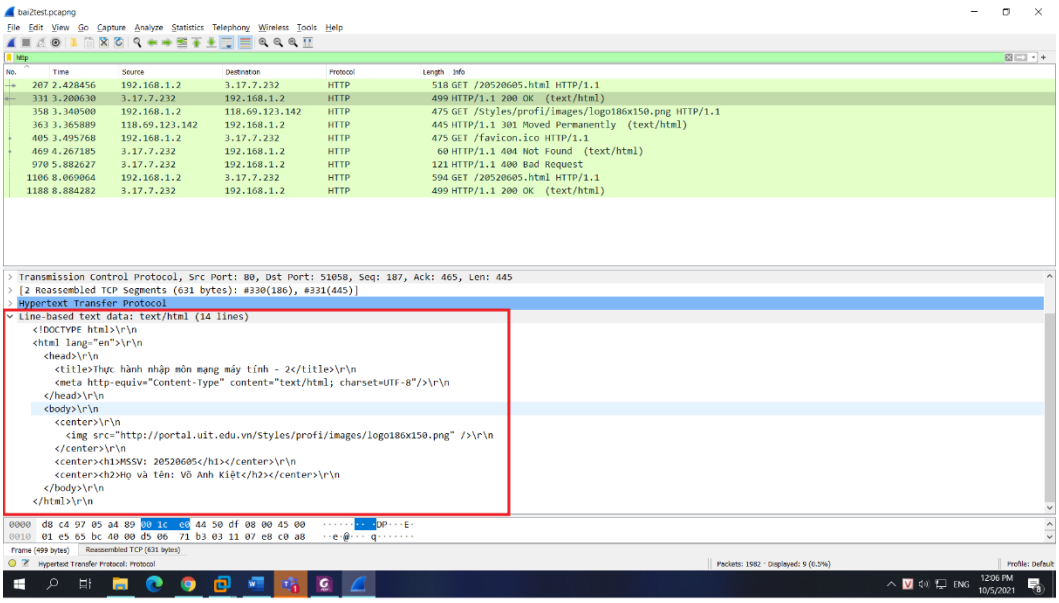
Xem xét nội dung của HTTP GET đầu tiên. Không tìm thấy dòng chữ“IF-MODIFIEDSINCE”



Câu 6: Xem xét nội dung phản hồi từ server. Server có thật sự trả về nội dung của file HTML hay không? Tại sao?

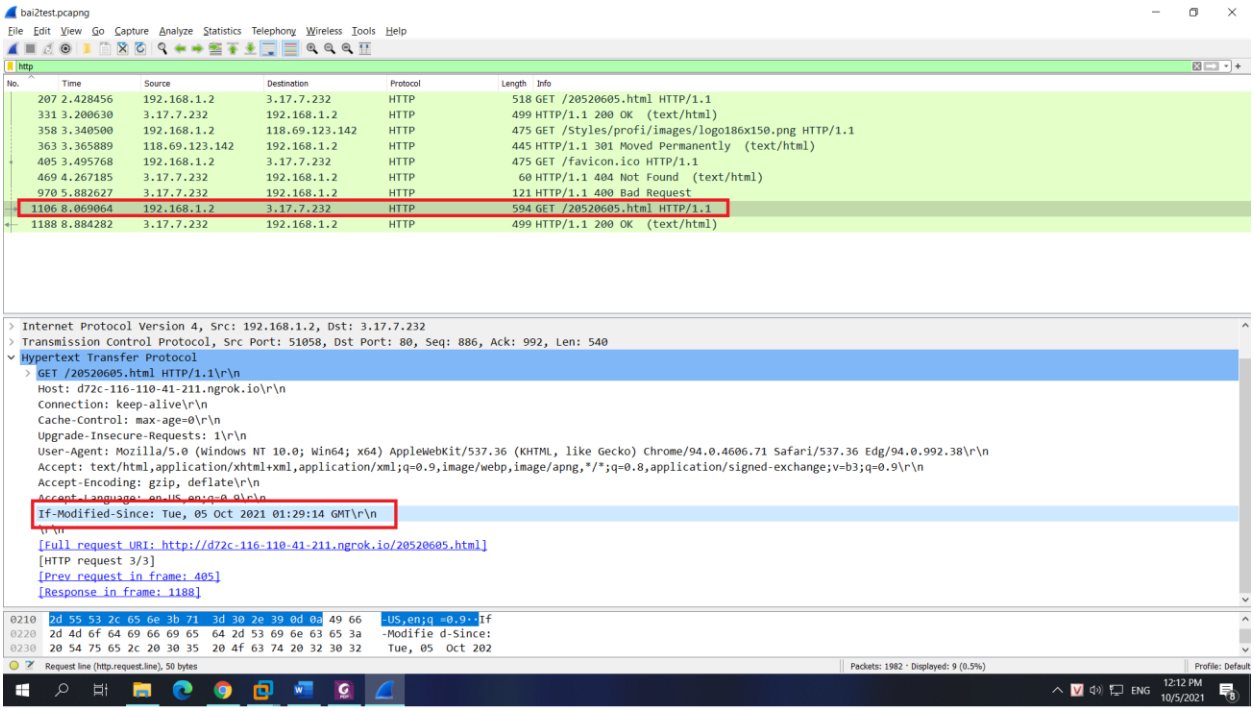
Quá trình phản hồi từ server: Client gửi yêu cầu file -> Server tìm kiếm file -> Server trả kết quả về Client -> Client tải về và hiển thị.

(trong trường hợp nếu như file cần tìm đã có sẵn ở bộ nhớ đệm cache thì sẽ lấy từ cache đem về còn nếu file yêu cầu thực sự chưa có thì sẽ yêu cầu Server tìm và gửi về cho Client). Như vậy nội dung file HTMl (do đã xóa Cache, nên khi ta yêu cầu get thì thì Server sẽ trả file này trực tiếp từ Server.



Câu 7:

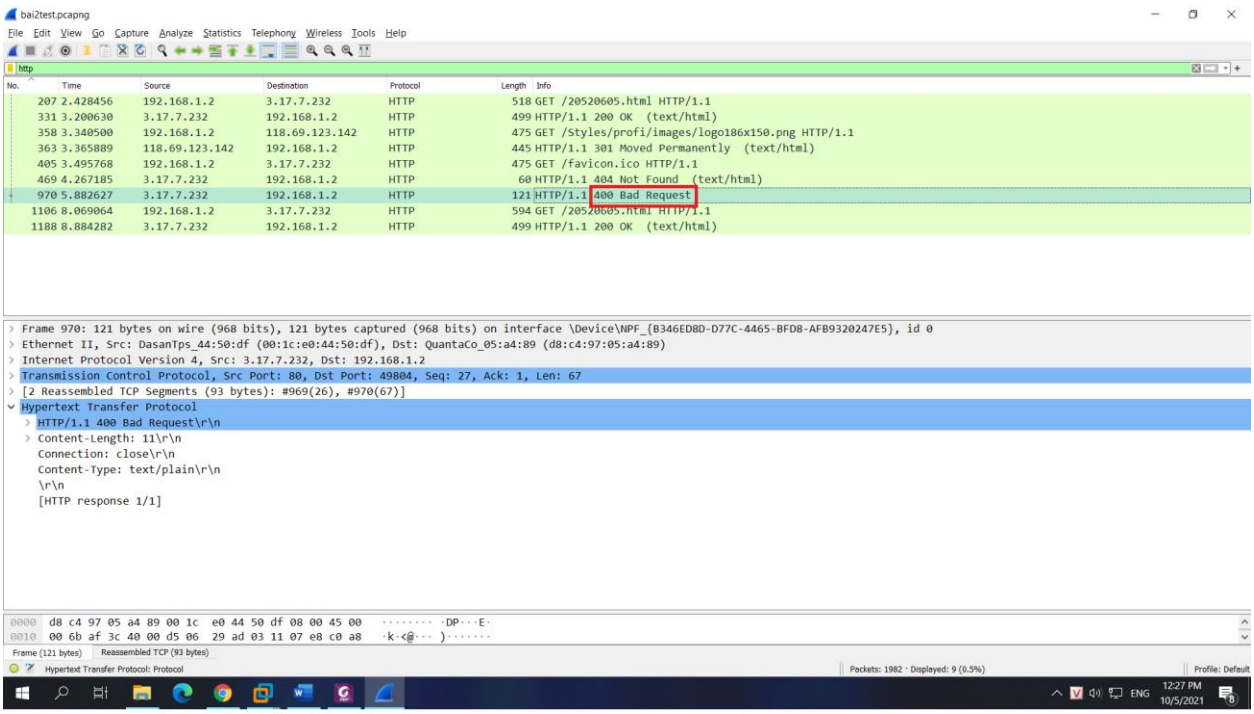
Đã thấy dòng “IF-MODIFIED-SINCE” với nội dung là: Tue, 05 Oct 2021 01:29:14 GMT\r\n



Câu 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.

Trả kết quả là 400 Bad Request: cho biết yêu cầu được gửi đến máy chủ website, thường là yêu cầu tải 1 trang web bị sai hoặc gián đoạn và server sẽ không hiểu request này. Lỗi này xuất hiện khi bạn cố gắng vào 1 trang web nhưng không thể truy cập được.

Server không gửi nội dung của file. Chúng ta có thể dễ dàng kiểm tra điều này ở phần mở rộng trong hình phía bên dưới.



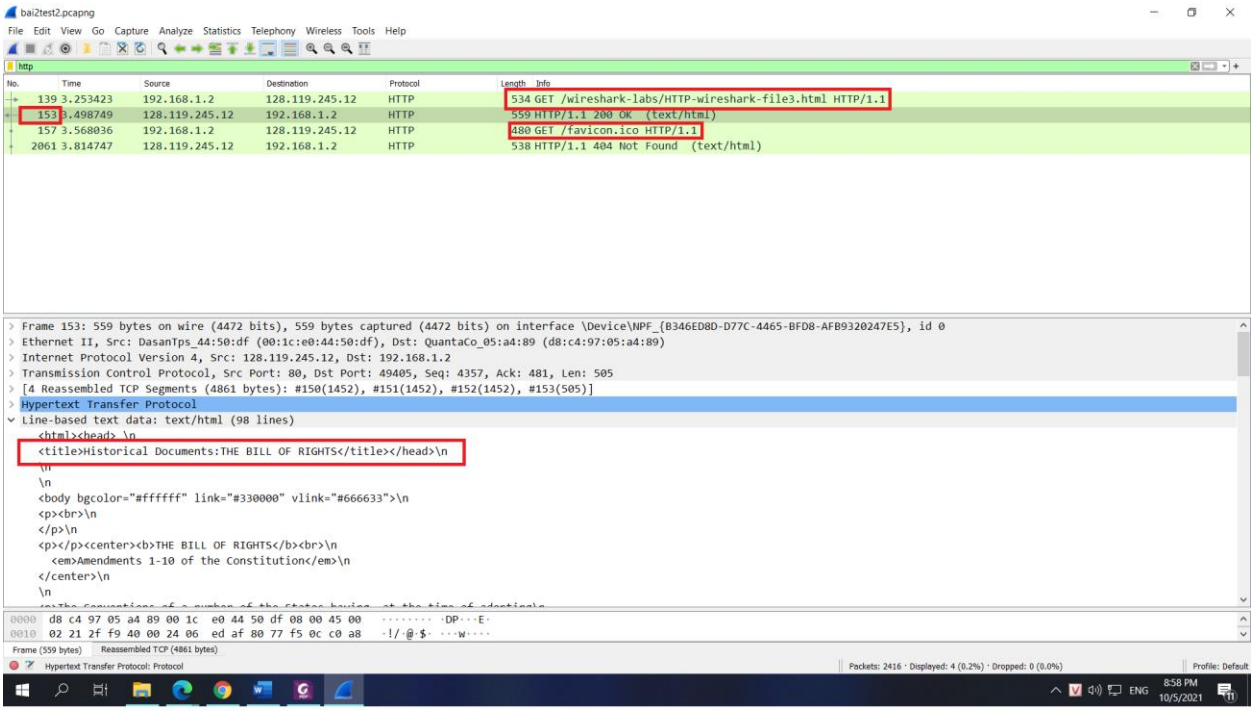
Câu 9: Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

Trình duyệt đã gửi 4 HTTP GET. 3 cái đến IP 3.17.7.232 đây là IP cấu hình web server của Kali Linux khi xử dụng “ngrok” và 1 cái đến IP 118.69.123.142 chứa hình ảnh logo UIT từ portal.uit.edu.vn

Source	Destination	Protocol	Length	Info
192.168.1.2	3.17.7.232	HTTP	518	GET /20520605.html HTTP/1.1
192.168.1.2	3.17.7.232	HTTP	594	GET /20520605.html HTTP/1.1
192.168.1.2	118.69.123.142	HTTP	475	GET /Styles/profi/images/logo186x150.png HTTP/1.1
192.168.1.2	3.17.7.232	HTTP	475	GET /favicon.ico HTTP/1.1

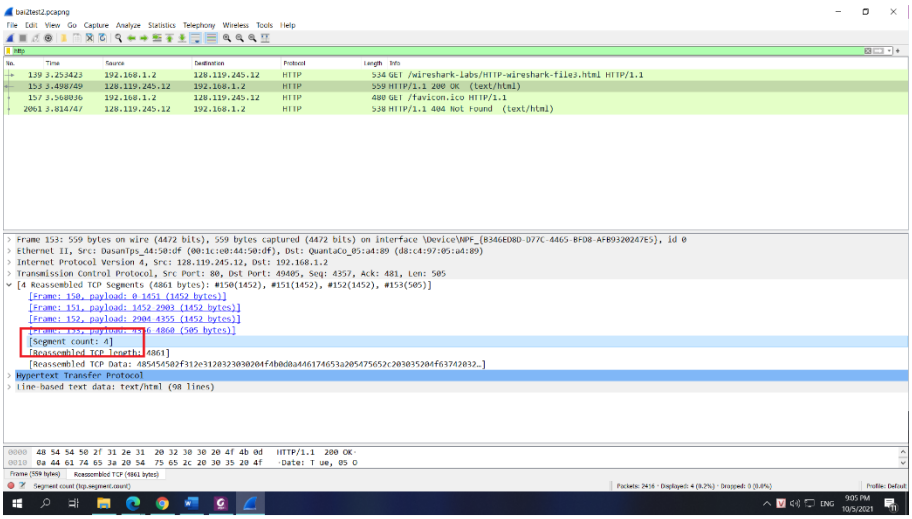
Câu 10: Trình duyệt đã gửi bao nhiêu HTTP GET? Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ mấy?

Gửi 2 HTTP GET. Dòng Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi số 153



Câu 11: Cần bao nhiêu TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights?

Cần có 4 TCP segments để thõa yêu cầu



Câu 12: Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

Mã trạng thái: 401 Unauthorized

Ý nghĩa: thông báo website vẫn tồn tại, hoạt động nhưng người dùng không thể truy cập vào do không được cấp quyền truy cập hay sở hữu quyền truy cập bao gồm tài khoản và mật khẩu không hợp lệ.

No.	Time	Source	Destination	Protocol	Length	Info
72	3.264118	192.168.1.2	128.119.245.12	HTTP	549	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
76	3.516932	128.119.245.12	192.168.1.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
255	17.552822	192.168.1.2	128.119.245.12	HTTP	634	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
280	17.806038	128.119.245.12	192.168.1.2	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Câu 13: Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu nào mới nào xuất hiện trong HTTP GET?

Trường dữ liệu mới: Authorization và Credentials

Trong Credentials chứa tài khoản và mật khẩu để xác nhận nếu muốn truy cập vào web