

BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng máy tính

Buổi báo cáo: Lab 2

Tên chủ đề: Làm quen với Wireshark

GVHD: Phan Trung Phát

Ngày thực hiện: 16/10/2022

Ngày nộp báo cáo: 16/10/2022

1. THÔNG TIN CHUNG:

Lớp: IT005.N11.KHTN.1

ST T	Họ và tên	MSSV	Email
1	Lương Toàn Bách	21521845	21521845@gm.uit.edu.vn

2. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	2 tiếng
Link Video thực hiện (nếu có)	Không có
Ý kiến (nếu có) + Khó khăn + Đề xuất ...	Không có
Điểm tự đánh giá	9.0

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

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?

No.	Time	Source	Destination	Protocol	Length	Info
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)

Trình duyệt đang sử dụng phiên bản HTTP 1.1 và HTTP server 1.1

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 192.168.146.58

Địa chỉ của web server là 192.168.221.74

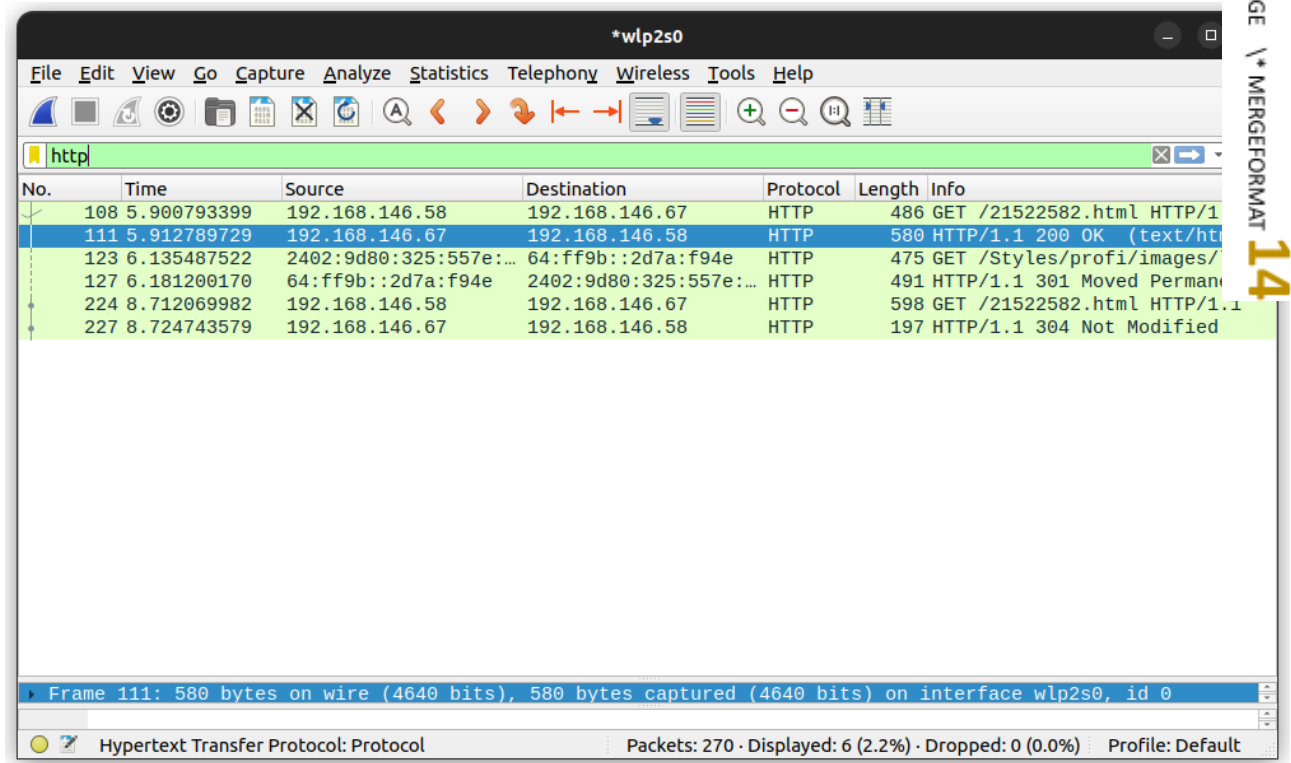
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
-----	-------------	----------------	----------------	------	-----	-----------------------------

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

111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)
-----	-------------	----------------	----------------	------	-----	-----------------------------

Mã trạng thái (status code) trả về từ server là: 200

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



Server đã trả về cho trình duyệt 580 bytes

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

No.	Time	Source	Destination	Protocol	Length	Info
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)
123	6.135487522	2402:9d80:325:557e::...	64:ff9b::2d7a:f94e	HTTP	475	GET /Styles/profi/images/log...
127	6.181200170	64:ff9b::2d7a:f94e	2402:9d80:325:557e::...	HTTP	491	HTTP/1.1 301 Moved Permanent...
224	8.712069982	192.168.146.58	192.168.146.67	HTTP	598	GET /21522582.html HTTP/1.1
227	8.724743579	192.168.146.67	192.168.146.58	HTTP	197	HTTP/1.1 304 Not Modified



Không có dòng “IF-MODIFIED-SINCE”

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?

No.	Time	Source	Destination	Protocol	Length	Info
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)
123	6.135487522	2402:9d80:325:557e::...	64:ff9b::2d7a:f94e	HTTP	475	GET /Styles/profi/images/logo186x150.png HTTP/1.1
127	6.181200170	64:ff9b::2d7a:f94e	2402:9d80:325:557e::...	HTTP	491	HTTP/1.1 301 Moved Permanently
224	8.712069982	192.168.146.58	192.168.146.67	HTTP	598	GET /21522582.html HTTP/1.1
227	8.724743579	192.168.146.67	192.168.146.58	HTTP	197	HTTP/1.1 304 Not Modified

```

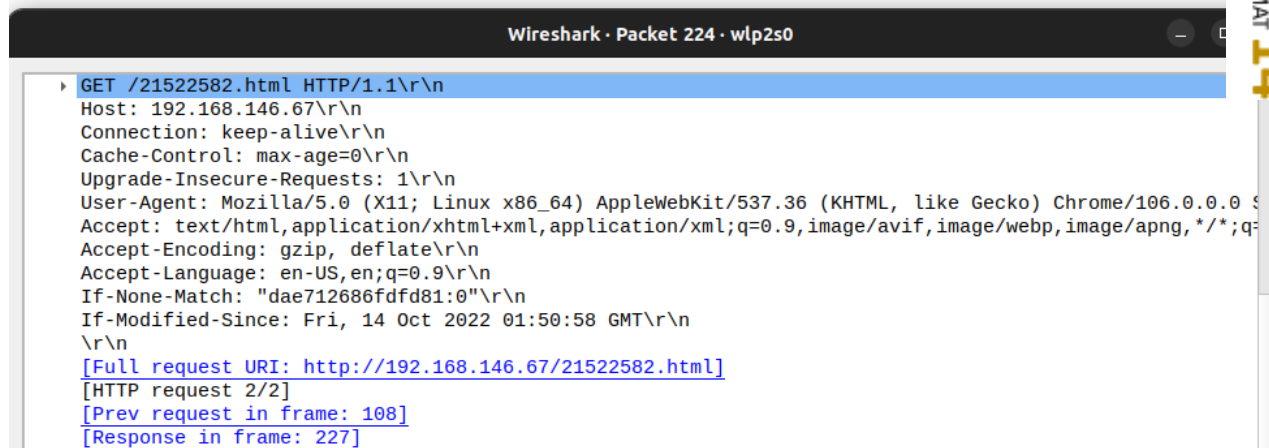
Wireshark - Packet 111 - wlp2s0

> Internet Protocol Version 4, Src: 192.168.146.67, Dst: 192.168.146.58
> Transmission Control Protocol, Src Port: 80, Dst Port: 53522, Seq: 1, Ack: 433, Len: 526
> Hypertext Transfer Protocol
  Line-based text data: text/html (13 lines)
    <!DOCTYPE html>\r\n
    <html>\r\n
    <head>\r\n
    <title>Thuc hinh nhap mon mang may tinh - 2</title>\r\n
    </head>\r\n
    <body>\r\n
    <center><img\r\n
    src="http://portal.uit.edu.vn/Styles/profi/images/logo186x150.png"/>\r\n
    ></center>\r\n
    <center><h1>MSSV: 21522582</h1></center>\r\n
    <center><h2> Ho va ten: TDT</h2></center>\r\n
    </body>\r\n
  
```

Server có trả lại file html. Vì đó là lần đầu tiên máy tính truy cập vào website đó nên chưa lưu cache

Câu 7: Xem xét nội dung của HTTP GET thứ 2. Bạn có thấy dòng “IF-MODIFIEDSINCE” hay không? Nếu có, giá trị của IF-MODIFIED-SINCE là gì?

No.	Time	Source	Destination	Protocol	Length	Info
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)
123	6.135487522	2402:9d80:325:557e::64	64:ff9b::2d7a:f94e	HTTP	475	GET /Styles/profi/images/...
127	6.181200170	64:ff9b::2d7a:f94e	2402:9d80:325:557e::64	HTTP	491	HTTP/1.1 301 Moved Permanently
224	8.712069982	192.168.146.58	192.168.146.67	HTTP	598	GET /21522582.html HTTP/1.1
227	8.724743579	192.168.146.67	192.168.146.58	HTTP	197	HTTP/1.1 304 Not Modified



Có dòng “IF-MODIFIED-SINCE”. Giá trị của “IF-MODIFIED-SINCE” là Fri, 20 Oct 2022 01:50:58 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

No.	Time	Source	Destination	Protocol	Length	Info
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)
123	6.135487522	2402:9d80:325:557e::64	64:ff9b::2d7a:f94e	HTTP	475	GET /Styles/profi/images/log...
127	6.181200170	64:ff9b::2d7a:f94e	2402:9d80:325:557e::64	HTTP	491	HTTP/1.1 301 Moved Permanent...
224	8.712069982	192.168.146.58	192.168.146.67	HTTP	598	GET /21522582.html HTTP/1.1
227	8.724743579	192.168.146.67	192.168.146.58	HTTP	197	HTTP/1.1 304 Not Modified

Status code request GET thứ 2 là 304 not modified

Ý nghĩa: Trang được yêu cầu không được sửa đổi kể từ lần cuối cùng.

Server không gửi về nội dung của file bởi không có sự thay đổi nên trang web vẫn hiển thị những nội dung của packet cũ.

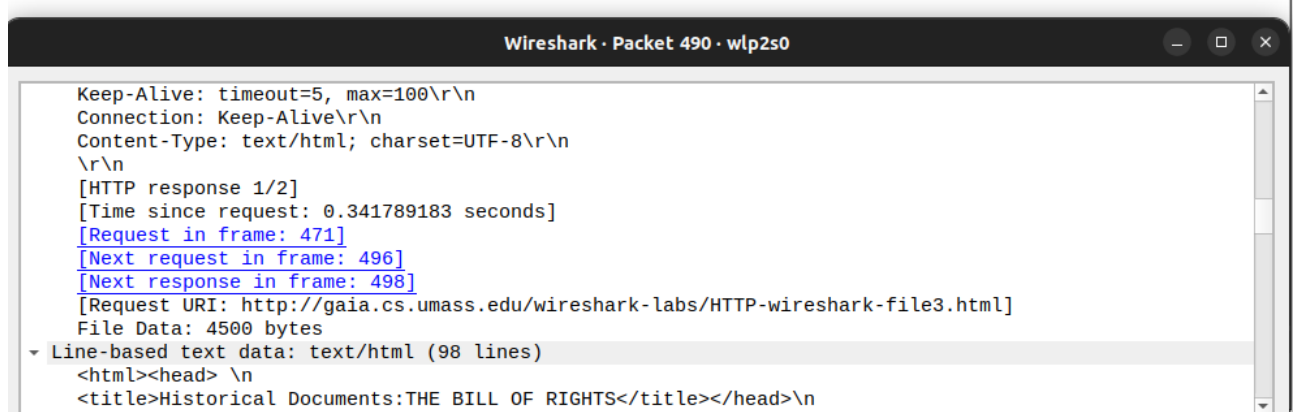
Câu 9: Trình duyệt đã gửi bao nhiêu HTTP GET? Đến những địa chỉ IP nào?

No.	Time	Source	Destination	Protocol	Length	Info
108	5.900793399	192.168.146.58	192.168.146.67	HTTP	486	GET /21522582.html HTTP/1.1
111	5.912789729	192.168.146.67	192.168.146.58	HTTP	580	HTTP/1.1 200 OK (text/html)
123	6.135487522	2402:9d80:325:557e::...	64:ff9b::2d7a:f94e	HTTP	475	GET /Styles/profi/images/...
127	6.181200170	64:ff9b::2d7a:f94e	2402:9d80:325:557e::...	HTTP	491	HTTP/1.1 301 Moved Permanently
224	8.712069982	192.168.146.58	192.168.146.67	HTTP	598	GET /21522582.html HTTP/1.1
227	8.724743579	192.168.146.67	192.168.146.58	HTTP	197	HTTP/1.1 304 Not Modified

Trình duyệt đã gửi 2 HTTP GET. Gửi tới địa chỉ: 192.168.146.58

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

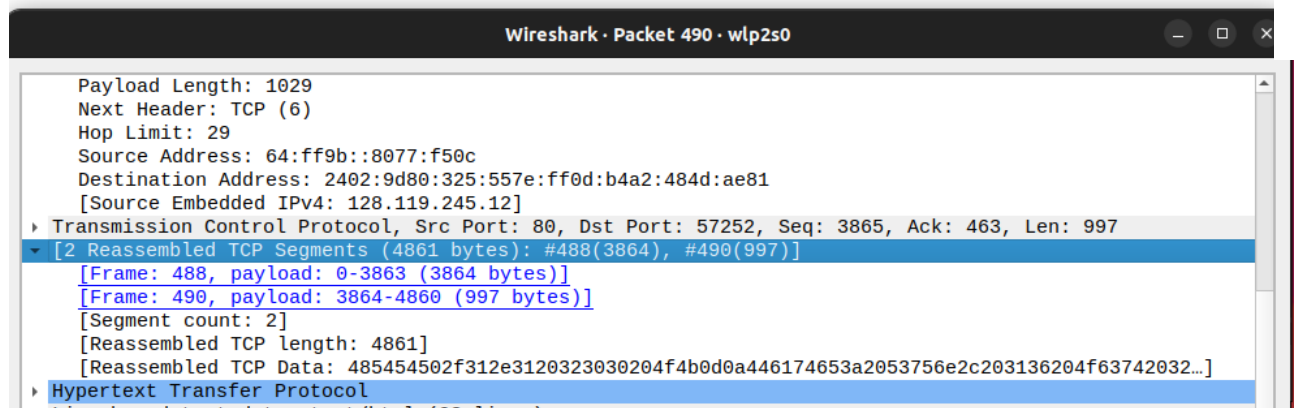
No.	Time	Source	Destination	Protocol	Length	Info
471	6.860833356	2402:9d80:325:557e::...	64:ff9b::8077:f50c	HTTP	548	GET /wireshark-labs/HTTP-wir...
490	7.202622539	64:ff9b::8077:f50c	2402:9d80:325:557e::...	HTTP	1083	HTTP/1.1 200 OK (text/html)
496	7.327658201	2402:9d80:325:557e::...	64:ff9b::8077:f50c	HTTP	494	GET /favicon.ico HTTP/1.1
498	7.692652237	64:ff9b::8077:f50c	2402:9d80:325:557e::...	HTTP	570	HTTP/1.1 404 Not Found (tex...



Trình duyệt đã gửi 1 HTTP GET. Dòng “THE BILL OF RIGHTS” được chứa trong gói tin phản hồi thứ 1

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

No.	Time	Source	Destination	Protocol	Length	Info
471	6.860833356	2402:9d80:325:557e::...	64:ff9b::8077:f50c	HTTP	548	GET /wireshark-labs/HTTP-wir..
490	7.202622539	64:ff9b::8077:f50c	2402:9d80:325:557e::...	HTTP	1083	HTTP/1.1 200 OK (text/html)
496	7.327658201	2402:9d80:325:557e::...	64:ff9b::8077:f50c	HTTP	494	GET /favicon.ico HTTP/1.1
498	7.692652237	64:ff9b::8077:f50c	2402:9d80:325:557e::...	HTTP	570	HTTP/1.1 404 Not Found (tex..



Cần 2 TCP segments để chứa hết HTTP response và nội dung của The Bill of Rights.

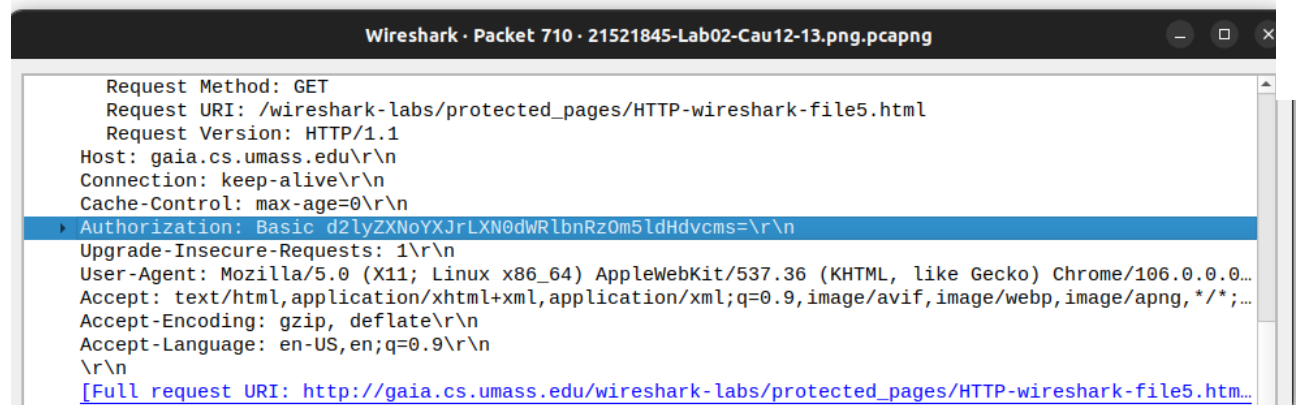
Câu 12: Mã trạng thái và ý nghĩa nó trong HTTP response tương ứng với HTTP GET đầu tiên là gì?

No.	Time	Source	Destination	Protocol	Length	Info
115	2.490401327	2402:9d80:325:557e::...	64:ff9b::8077:f50c	HTTP	564	GET /wireshark-labs/protecte...
138	2.842743879	64:ff9b::8077:f50c	2402:9d80:325:557e::...	HTTP	803	HTTP/1.1 401 Unauthorized (...)
710	18.315379542	2402:9d80:325:557e::...	64:ff9b::8077:f50c	HTTP	649	GET /wireshark-labs/protecte...
716	18.822000056	64:ff9b::8077:f50c	2402:9d80:325:557e::...	HTTP	576	HTTP/1.1 200 OK (text/html)

Ý nghĩa: Thông tin đăng nhập không hợp lệ

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

No.	Time	Source	Destination	Protocol	Length	Info
115	2.490401327	2402:9d80:325:557e:...	64:ff9b::8077:f50c	HTTP	564	GET /wireshark-labs/protecte..
138	2.842743879	64:ff9b::8077:f50c	2402:9d80:325:557e:...	HTTP	803	HTTP/1.1 401 Unauthorized (..
710	18.315379542	2402:9d80:325:557e:...	64:ff9b::8077:f50c	HTTP	649	GET /wireshark-labs/protecte..
716	18.822000056	64:ff9b::8077:f50c	2402:9d80:325:557e:...	HTTP	576	HTTP/1.1 200 OK (text/html)



Khi trình duyệt gửi HTTP GET lần thứ 2, trường dữ liệu mới xuất hiện trong HTTP GET là Authorization

HẾT