

HTTP

I. Mục tiêu và yêu cầu

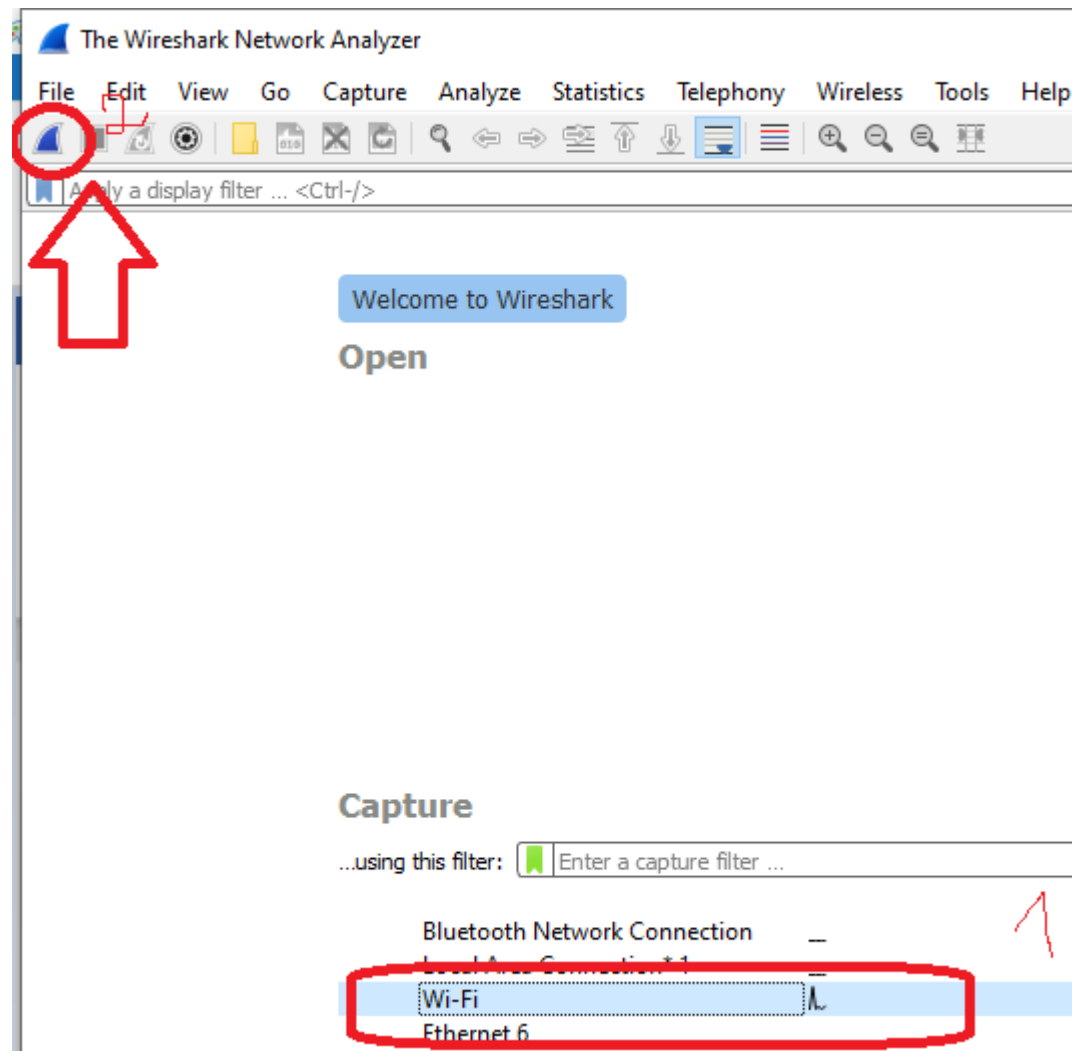
- Hiểu và trình bày được các loại gói của giao thức HTTP
- Thao tác được trên wireshark để lọc trích các thông tin cần thiết
- Sinh viên thực hiện thành thạo, trả lời các câu hỏi, giảng viên sẽ vấn đáp trực tiếp hoặc chấm thực hành thông qua video sinh viên gửi.
- Khi làm video, sinh viên chọn website tùy ý, và phải chứng minh được video là do sinh viên làm.

II. Nội dung

II.1. Lọc trích gói GET HTTP

B1. Mở Wireshark với quyền admin

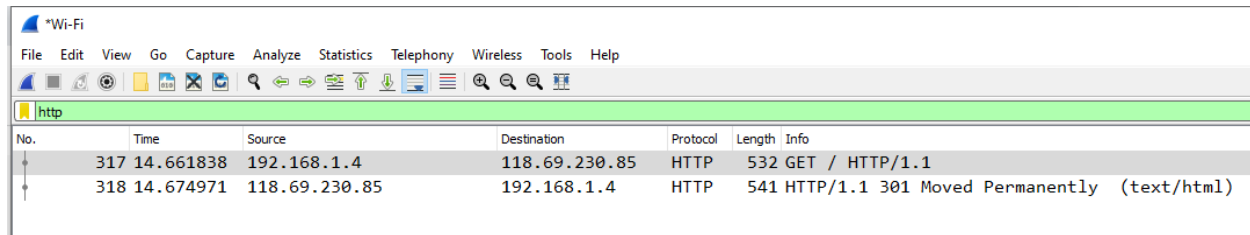
B2. Chọn mạng, card mạng bắt lưu lượng, ở đây ta chọn card không dây → nhấn nút để bắt đầu bắt gói



B3. Vào trình duyệt nhập link <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

B4. Nhấn nút hình vuông màu đỏ trên wireshark để dừng bắt gói.

B5. Vào vị trí lọc gói nhập http để lọc

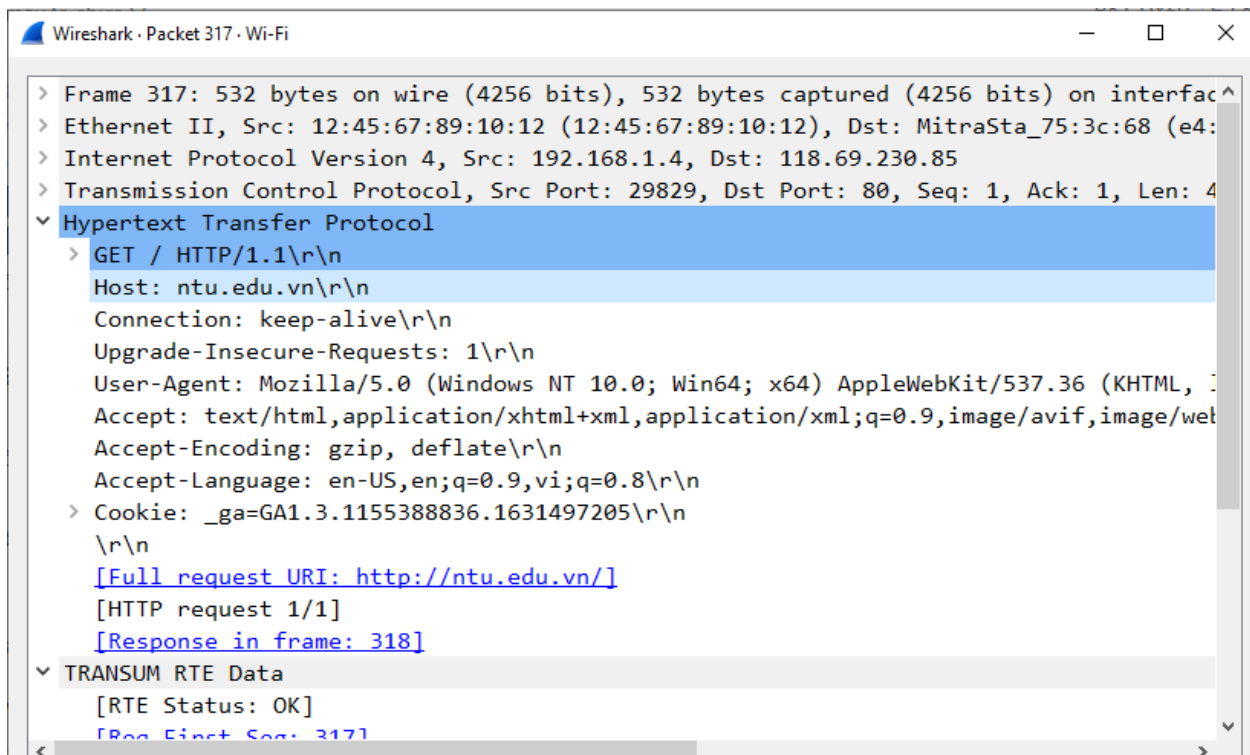


No.	Time	Source	Destination	Protocol	Length	Info
317	14.661838	192.168.1.4	118.69.230.85	HTTP	532	GET / HTTP/1.1
318	14.674971	118.69.230.85	192.168.1.4	HTTP	541	HTTP/1.1 301 Moved Permanently (text/html)

Như vậy ta bắt được một gói GET HTTP và một gói phản hồi với code 301.

Câu 1. Các bạn nhớ lại code 301 là có nghĩa là gì?

Câu 2. Mở nội dung gói tin GET, hãy trả lời các câu hỏi sau:



1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the server?
4. What is the status code returned from the server to your browser?
5. When was the HTML file that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your browser?
7. By inspecting the raw data in the packet content window, do you see any headers

within the data that are not displayed in the packet-listing window? If so, name one.

II.2. Bắt gói tin HTTP CONDITIONAL GET/response

- Đầu tiên ta xóa hết lịch sử trình duyệt
- Sau đó mở phiên bắt gói tin mới trên wireshark
- Mở trình duyệt nhập URL sau, mở file tương ứng:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>
- Tiếp tục ta lại nhập URL lại thêm 1 lần nữa (hoặc đơn giản là f5)
- Sau đó dừng bắt gói tin
- Nhập vào vị trí lọc ta lọc gói http, kết quả có thể như sau:

```
1157 42.901461 192.168.1.4 128.119.229.125 HTTP 571 GET /ece374/assignments/Lab_Assignment_2.pdf HTTP/1.1
2908 208.413340 192.168.1.4 128.119.229.125 HTTP 651 GET /ece374/assignments/Lab_Assignment_2.pdf HTTP/1.1
2914 208.689203 128.119.229.125 192.168.1.4 HTTP 270 HTTP/1.1 304 Not Modified
```

```
> Transmission Control Protocol, Src Port: 1027, Dst Port: 80, Seq: 1, Ack: 1, Len: 597
▼ Hypertext Transfer Protocol
  > GET /ece374/assignments/Lab_Assignment_2.pdf HTTP/1.1\r\n
    Host: www.ecs.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; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.3
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-e
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,vi;q=0.8\r\n
    If-None-Match: "33075-50-1b08b3f-0"\r\n
    If-Modified-Since: Thu, 08 Jan 2015 03:28:07 GMT\r\n
    \r\n
  [Full request URI: http://www.ecs.umass.edu/ece374/assignments/Lab_Assignment_2.pdf]
```

Sau đó trả lời các câu hỏi:

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
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?
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

II.3. HTTP Authentication

Vì HTTP gửi dữ liệu dạng text tường minh nên khi chặn bắt gói tin này có thể dễ dàng đọc được các thông tin trao đổi trong đó có thông tin đăng nhập.

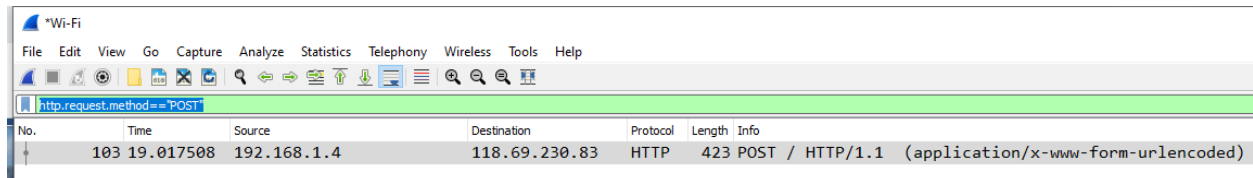
B1. Mở wireshark và tiến hành bắt gói tin

B2. Mở trình duyệt nhập URL: <http://thuvien.ntu.edu.vn/>

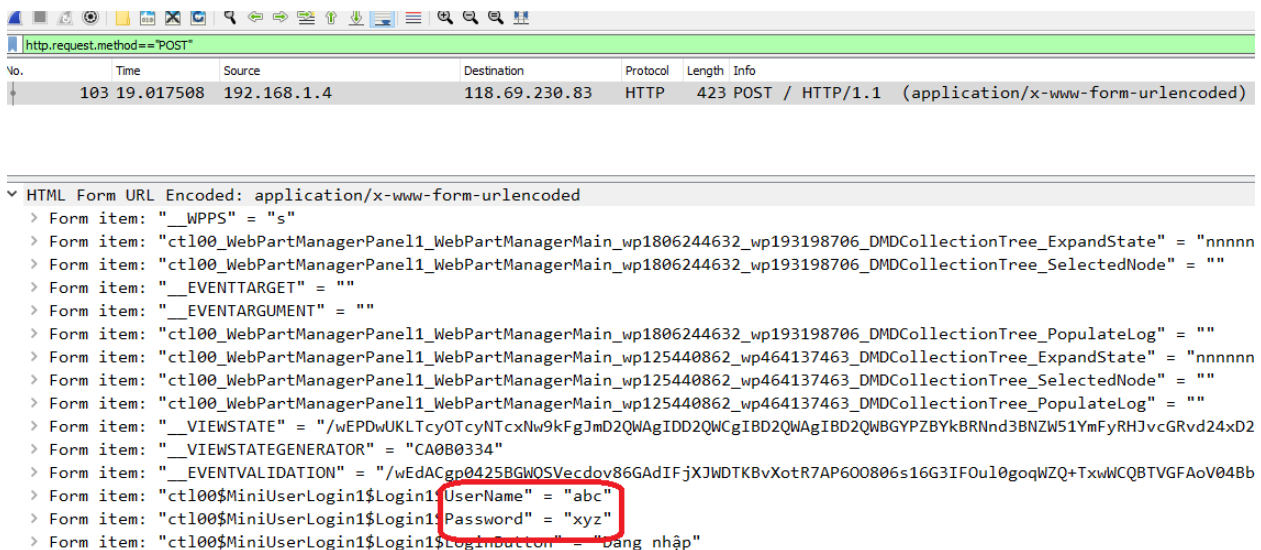
B3. Nhập vào username, và mật khẩu bất kì → Đăng nhập

B4. Dừng bắt gói tin trên wireshark

B5. Nhập vào phần lọc để lọc gói POST của HTTP bằng biểu thức `http.request.method=="POST"`



B6. Mở gói tin và đọc thông tin các trường, đặc biệt có thể đọc được thông tin username và mật khẩu.



Yêu cầu: Sinh viên thực hiện và bắt gói tin tương tự sau đó phân tích

II.4: Xác thực có mã hóa

- Mở Wireshark và bắt gói tin

- Vào trình duyệt và nhập vào URL sau;

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html

- Nhập username là "wireshark-student" và pass là "network"

- Nhấn đăng nhập

- Dừng bắt gói tin trên wireshark

- Lọc http trên wireshark

No.	Time	Source	Destination	Protocol	Length	Info
22	2.807808	128.119.245.12	192.168.1.4	HTTP	770	HTTP/1.1 401 Unauthorized (text/html)
81	9.806035	192.168.1.4	117.18.237.29	OCSP	499	Request
83	9.846521	117.18.237.29	192.168.1.4	OCSP	793	Response
221	20.739327	192.168.1.4	128.119.245.12	HTTP	638	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1

> Frame 221: 638 bytes on wire (5104 bits), 638 bytes captured (5104 bits) on interface \Device\NPF_{7F3D0932-722A-427F-8650-3C20D851E23B}, interface 0

> Ethernet II, Src: 12:45:67:89:10:12 (12:45:67:89:10:12), Dst: MitraSta_75:3c:68 (e4:ab:89:75:3c:68)

> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 2329, Dst Port: 80, Seq: 1, Ack: 1, Len: 584

> Hypertext Transfer Protocol

> GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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 d2lyZXNoYXJrLXN0dWR1bnRzM5ldHdvcms=\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/94.0.4606.61 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\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,vi;q=0.8\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]

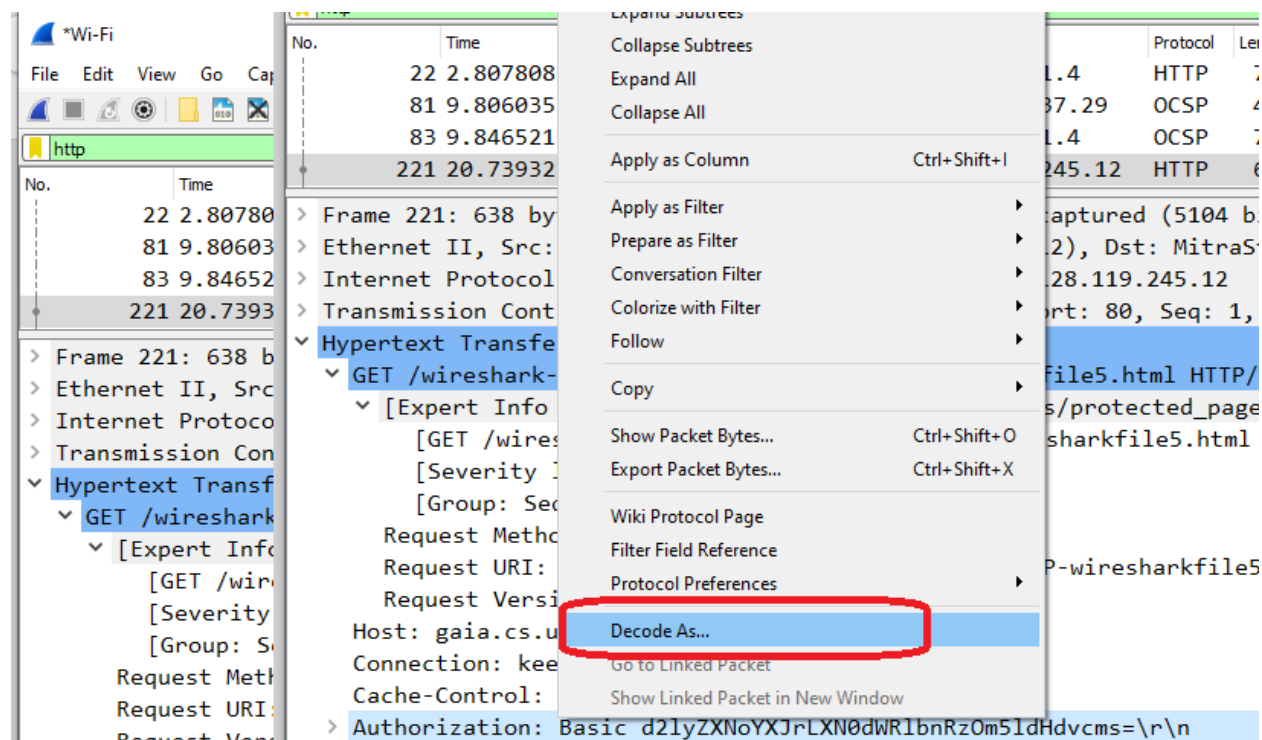
[HTTP request 1/1]

Để giải mã cụm từ mã hóa sau từ Basic, copy cụm từ này vào website

<https://www.motobit.com/util/base64-decoder-encoder.asp>

Dạng mã hóa này là Base64

Hoặc sinh viên có thể sử dụng chức năng decode trên wireshark để giải mã, nhấn chuột phải vào vị trí Authorization và chọn Decode As:



II.5. Dạng HTTP chứa gói tin lớn

Xóa lịch sử

Sinh viên làm tương tự để bắt gói tin với trường hợp URL là

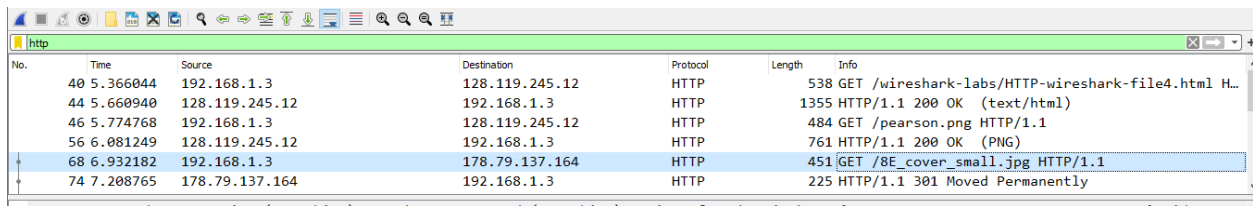
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

Sau đó trả lời các câu hỏi sau:

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
14. What is the status code and phrase in the response?
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

II.6. HTTP có đối tượng được nhúng

Sinh viên bắt gói tin tương tự với URL là <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>



No.	Time	Source	Destination	Protocol	Length	Info
40	5.366044	192.168.1.3	128.119.245.12	HTTP	538	GET /wireshark-labs/HTTP-wireshark-file4.html H...
44	5.660940	128.119.245.12	192.168.1.3	HTTP	1355	HTTP/1.1 200 OK (text/html)
46	5.774768	192.168.1.3	128.119.245.12	HTTP	484	GET /pearson.png HTTP/1.1
56	6.081249	128.119.245.12	192.168.1.3	HTTP	761	HTTP/1.1 200 OK (PNG)
68	6.932182	192.168.1.3	178.79.137.164	HTTP	451	GET /8E_cover_small.jpg HTTP/1.1
74	7.208765	178.79.137.164	192.168.1.3	HTTP	225	HTTP/1.1 301 Moved Permanently

Sau đó trả lời các câu hỏi sau:

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain