

**MSSV: 21520417**

**Họ tên: Huỳnh Ngọc Quý**

**Câu 1:**

Website: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

Tổng thời gian bắt gói tin:  $3.222726 - 2.442403 = 0.780323$  (s).

Tổng số gói tin bắt được: 4.

No.	Time	Source	Destination	Protocol	Length	Info
2194	2.442403	172.30.182.96	128.119.245.12	HTTP	543	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2513	2.832722	128.119.245.12	172.30.182.96	HTTP	492	HTTP/1.1 200 OK (text/html)
2595	2.859644	172.30.182.96	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
2985	3.222726	128.119.245.12	172.30.182.96	HTTP	538	HTTP/1.1 404 Not Found (text/html)

**Câu 2:**

5 giao thức khác nhau xuất hiện trong cột giao thức khi không áp dụng bộ lọc “http” khi truy cập website <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> và chức năng của các giao thức này:

**1. TCP**

Kiểm soát mức độ tin cậy của việc truyền dữ liệu.

**2. HTTP**

Truyền tải dữ liệu giữa Web server đến các trình duyệt Web và ngược lại. Giao thức này sử dụng cổng 80 (port 80) là chủ yếu.

**3. UDP**

Thiết lập các kết nối có độ trễ thấp và không chịu lỗi giữa các ứng dụng trên internet.

**4. DNS**

Giúp liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị trên Internet

**5. SSDP**

Cung cấp các thông tin cần thiết để tạo ra các kết nối giữa các thiết bị có kết nối mạng internet

13 0.071788	108.157.30.31	172.30.182.96	TCP	56 443 → 58986 [ACK] Seq=1 Ack=32 Win=131 Len=0
2513 2.832722	128.119.245.12	172.30.182.96	HTTP	492 HTTP/1.1 200 OK (text/html)
2206 2.494678	172.30.163.27	172.30.255.255	UDP	305 54915 → 54915 Len=263
1712 1.934322	172.30.182.96	192.168.54.4	DNS	76 Standard query 0xaed8 A r.msftstatic.com
761 0.949790	172.30.185.214	239.255.255.250	SSDP	218 M-SEARCH * HTTP/1.1

### Câu 3:

Thời gian từ khi gói tin **HTTP GET đầu tiên** được gửi cho đến khi **HTTP 200 OK đầu tiên** được nhận là:  $2.832722 - 2.442403 = 0.390319$  (s)

http					
No.	Time	Source	Destination	Protocol	Length Info
2194	2.442403	172.30.182.96	128.119.245.12	HTTP	543 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2513	2.832722	128.119.245.12	172.30.182.96	HTTP	492 HTTP/1.1 200 OK (text/html)

### Câu 4:

Nội dung hiển thị trên trang web **gaia.cs.umass.edu**:

“Congratulations! You've downloaded the first Wireshark lab file!”

**Có** nằm trong các gói tin HTTP bắt được.

Vị trí nội dung này nằm ở:

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2194	2.442403	172.30.182.96	128.119.245.12	HTTP	543	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2513	2.832722	128.119.245.12	172.30.182.96	HTTP	492	HTTP/1.1 200 OK (text/html)
2595	2.859644	172.30.182.96	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
2985	3.222726	128.119.245.12	172.30.182.96	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 2513: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{A827C446-05D2-4D95-B2D2-3888749E8386}, id 0

> Ethernet II, Src: JuniperN\_8c:35:b0 (44:f4:77:8c:35:b0), Dst: IntelCor\_a2:48:06 (f0:9e:4a:a2:48:06)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.30.182.96

> Transmission Control Protocol, Src Port: 80, Dst Port: 59009, Seq: 1, Ack: 490, Len: 438

> Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)

```
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n
```

Offset	Hex	ASCII
0120	74 65 73 0d 0a 43 6f 6e	tes--Con tent-Len
0130	67 74 68 3a 20 38 31 0d	gth: 81-Keep-Al
0140	69 76 65 3a 20 74 69 6d	ive: tim eout=5,
0150	6d 61 78 3d 31 30 30 0d	max=100-Connect
0160	69 6f 6e 3a 20 4b 65 65	ion: Kee p-Alive-
0170	0a 43 6f 6e 74 65 6e 74	-Content -Type: t
0180	65 78 74 2f 68 74 6d 6c	ext/html ; charse
0190	74 3d 55 54 46 2d 38 0d	t-UTF-8 -html
01a0	3e 0a 43 6f 6e 67 72 61	>> Congra tulation
01b0	73 21 20 20 59 6f 75 27	s! You' ve downl
01c0	6f 61 64 65 64 20 74 68	oaded th e first
01d0	57 69 72 65 73 68 61 72	Wireshar k lab fi
01e0	6c 65 21 0a 3c 2f 68 74	le!</ht ml>-

Text item (text), 66 bytes

Packe

## Câu 5:

Địa chỉ IP của **gaia.cs.umass.edu** là: 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
2194	2.442403	172.30.182.96	128.119.245.12	HTTP	543	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2513	2.832722	128.119.245.12	172.30.182.96	HTTP	492	HTTP/1.1 200 OK (text/html)
2595	2.859644	172.30.182.96	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
2985	3.222726	128.119.245.12	172.30.182.96	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Địa chỉ IP của máy tính đang sử dụng là: 172.30.182.96

No.	Time	Source	Destination	Protocol	Length	Info
2194	2.442403	172.30.182.96	128.119.245.12	HTTP	543	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
2513	2.832722	128.119.245.12	172.30.182.96	HTTP	492	HTTP/1.1 200 OK (text/html)
2595	2.859644	172.30.182.96	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
2985	3.222726	128.119.245.12	172.30.182.96	HTTP	538	HTTP/1.1 404 Not Found (text/html)

## Câu 6:

Diễn biến khi truy cập vào một trang web:

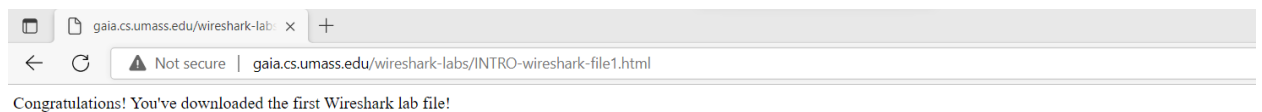
1. Khi truy cập trang web, trình duyệt sẽ gọi tới máy chủ DNS để biên dịch URL trang web thành một địa chỉ IP, mỗi trang web có địa chỉ IP riêng biệt. Khi tìm thấy địa chỉ IP của trang web chúng ta đang vào, địa chỉ IP đó sẽ được trả về cho trình duyệt.
2. Trình duyệt sẽ sử dụng địa chỉ IP đó để yêu cầu HTTP gọi tới Server lưu trữ trang web đó. Nó sẽ kết nối cổng số 80 trên Server bằng giao thức TCP/IP.

2194	2.442403	172.30.182.96	128.119.245.12	HTTP	543 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
------	----------	---------------	----------------	------	---

3. Nếu Server chấp nhận thì sẽ gửi lại thông báo "200 OK". Và sau đó trình duyệt sẽ truy xuất mã HTML của trang web cụ thể được yêu cầu.

2513	2.832722	128.119.245.12	172.30.182.96	HTTP	492 HTTP/1.1 200 OK (text/html)
------	----------	----------------	---------------	------	---------------------------------

4. Khi trình duyệt của bạn nhận được mã HTML đó từ Server thì nó sẽ hiển thị ra cửa sổ của trình duyệt một trang web hoàn chỉnh.



5. Khi chúng ta đóng trình duyệt thì quá trình kết nối với Server sẽ kết thúc.