



THỰC HÀNH LAB 1
IT005.O118

MSSV: 22521060.

Tên: Lê Minh Nhựt.

- 1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?**

Địa chỉ trang web	Tổng thời gian bắt gói tin	Tổng số gói tin																																			
gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html	0,57453 s	4																																			
<div><div> http</div><table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>366</td><td>3.740758</td><td>172.30.24.126</td><td>128.119.245.12</td><td>HTTP</td><td>534</td><td>GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1</td></tr><tr><td>401</td><td>4.007369</td><td>128.119.245.12</td><td>172.30.24.126</td><td>HTTP</td><td>492</td><td>HTTP/1.1 200 OK (text/html)</td></tr><tr><td>404</td><td>4.043662</td><td>172.30.24.126</td><td>128.119.245.12</td><td>HTTP</td><td>480</td><td>GET /favicon.ico HTTP/1.1</td></tr><tr><td>515</td><td>4.315288</td><td>128.119.245.12</td><td>172.30.24.126</td><td>HTTP</td><td>538</td><td>HTTP/1.1 404 Not Found (text/html)</td></tr></tbody></table></div>			No.	Time	Source	Destination	Protocol	Length	Info	366	3.740758	172.30.24.126	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	401	4.007369	128.119.245.12	172.30.24.126	HTTP	492	HTTP/1.1 200 OK (text/html)	404	4.043662	172.30.24.126	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1	515	4.315288	128.119.245.12	172.30.24.126	HTTP	538	HTTP/1.1 404 Not Found (text/html)
No.	Time	Source	Destination	Protocol	Length	Info																															
366	3.740758	172.30.24.126	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1																															
401	4.007369	128.119.245.12	172.30.24.126	HTTP	492	HTTP/1.1 200 OK (text/html)																															
404	4.043662	172.30.24.126	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1																															
515	4.315288	128.119.245.12	172.30.24.126	HTTP	538	HTTP/1.1 404 Not Found (text/html)																															
PHẦN MỀM THÔNG KÊ Y TẾ (tkyt.vn)	0,034402 s	2																																			
<div><div> http</div><table><thead><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr></thead><tbody><tr><td>258</td><td>2.581127</td><td>172.30.24.126</td><td>103.124.60.105</td><td>HTTP</td><td>575</td><td>GET / HTTP/1.1</td></tr><tr><td>295</td><td>2.615529</td><td>103.124.60.105</td><td>172.30.24.126</td><td>HTTP</td><td>169</td><td>HTTP/1.0 302 Found</td></tr></tbody></table></div>			No.	Time	Source	Destination	Protocol	Length	Info	258	2.581127	172.30.24.126	103.124.60.105	HTTP	575	GET / HTTP/1.1	295	2.615529	103.124.60.105	172.30.24.126	HTTP	169	HTTP/1.0 302 Found														
No.	Time	Source	Destination	Protocol	Length	Info																															
258	2.581127	172.30.24.126	103.124.60.105	HTTP	575	GET / HTTP/1.1																															
295	2.615529	103.124.60.105	172.30.24.126	HTTP	169	HTTP/1.0 302 Found																															

Trong đó **tổng thời gian bắt gói tin** là thời gian gói tin cuối bắt được trừ cho gói tin đầu bắt được, **tổng số gói bắt được** là số gói tin http hiển thị trên màn hình.

- 2. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.**

Tên 5 loại giao thức:

- **DNS:** Cung cấp dịch vụ ánh xạ tên miền sang địa chỉ IP.
- **TCP:** Cung cấp kết nối đáng tin cậy giữa hai máy tính.

- **MDNS:** Giúp các thiết bị trong mạng tìm thấy nhau mà không cần biết địa chỉ IP của nhau.
- **SSDP:** Giúp các thiết bị trong mạng tìm thấy các dịch vụ mà chúng cần.
- **ARP:** Giúp các máy tính trong mạng tìm địa chỉ MAC của nhau.

3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).

- Web gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html mất $4,007369 - 3,740758 = 0,266611$ s.

No.	Time	Source	Destination	Protocol	Length	Info
366	3.740758	172.30.24.126	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
401	4.007369	128.119.245.12	172.30.24.126	HTTP	492	HTTP/1.1 200 OK (text/html)

- Web [PHẦN MỀM THÔNG KÊ Y TẾ \(tkyl.vn\)](http://phanmemthongkyte.tkyl.vn) mất $2,615529 - 2,581137 = 0,034402$ s.

No.	Time	Source	Destination	Protocol	Length	Info
258	2.581127	172.30.24.126	103.124.60.105	HTTP	575	GET / HTTP/1.1
295	2.615529	103.124.60.105	172.30.24.126	HTTP	169	HTTP/1.0 302 Found

Trong đó ở web thứ hai sẽ lấy thời gian tại HTTP 302 Found (thay cho HTTP 200 OK)

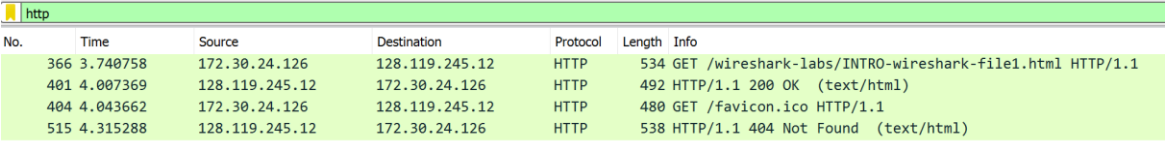
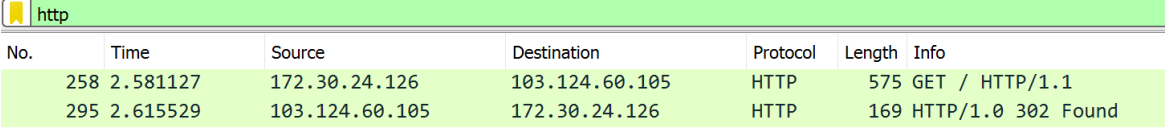
4. Nội dung hiển thị trên trang web gaia.cs.umass.edu “Congratulations! You've downloaded the first Wireshark lab file!” có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

Nội dung trên có nằm trong gói tin HTTP bắt được, cụ thể là trong phần Hypertext Transfer Protocol của gói tin HTTP 200 OK.

No.	Time	Source	Destination	Protocol	Length	Info
366	3.740758	172.30.24.126	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
401	4.007369	128.119.245.12	172.30.24.126	HTTP	492	HTTP/1.1 200 OK (text/html)
404	4.043662	172.30.24.126	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
515	4.315288	128.119.245.12	172.30.24.126	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 401: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface > Ethernet II, Src: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0), Dst: AzureWav_86:cb:9d (14:13:00:00:00:00) > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.30.24.126 > Transmission Control Protocol, Src Port: 80, Dst Port: 65162, Seq: 1, Ack: 481, Len: 4 > Hypertext Transfer Protocol > Line-based text data: text/html (3 lines)	<pre> 00d0 66 69 65 64 3a 20 54 68 75 2c 20 32 38 20 53 65 66 69 65 64 3a 20 54 68 75 2c 20 32 38 20 53 65 00e0 70 20 32 30 32 33 20 30 35 3a 35 39 3a 30 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 36 00f0 30 36 36 35 30 31 33 33 63 62 63 34 22 0d 0a 41 06650133 cbc4" :A 0100 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by 0110 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 65 73 3a 20 62 79 tes-Content-Len 0120 67 74 68 3a 20 38 31 0d 0a 4b 65 65 70 2d 41 6c 0a 4b 65 65 70 2d 41 6c gth: 81-Keep-Al 0130 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 65 6f 75 74 3d 35 2c 20 ive: tim eout=5, 0140 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 max=100: .Connect 0150 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Kee p-Alive. 0160 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 .Content -Type: t 0170 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 ext/html ; charse 0180 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c t=UTF-8-...<html 0190 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f 6e >.Congra tulation 01a0 73 21 20 20 59 6f 75 27 76 65 20 64 6f 77 6e 6c si You've downl 01b0 6f 61 64 65 64 20 74 68 65 20 66 69 72 73 74 20 loaded the first 01c0 57 69 72 65 73 68 61 72 6b 20 6c 61 62 20 66 69 Wireshar k lab fi 01d0 6c 65 21 0a 3c 2f 68 74 6d 6c 3e 0a le!</ht ml> 01e0 </pre>
--	--

5. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

Địa chỉ web	Địa chỉ IP của máy tính đang sử dụng	Địa chỉ IP website
gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html	172.30.24.126	128.119.245.12
<div>  </div>		
PHẦN MỀM THỐNG KÊ Y TẾ (tkyl.vn)	172.30.24.126	103.124.60.105
<div>  </div>		

Do địa chỉ IP ban đầu sẽ là từ máy tính cá nhân gửi yêu cầu tới IP của web, sau khi nhận được yêu cầu IP của web sẽ phản hồi về, cứ như thế IP máy tính nhận được gói tin và tiếp tục phản hồi.

6. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.

***Diễn biến:**

- Khách truy cập gửi yêu cầu HTTP GET đến máy chủ của web. Yêu cầu này chứa thông tin về đường dẫn đến trang web mà khách truy cập muốn xem.
- Máy chủ web nhận được yêu cầu HTTP và trả lời bằng một gói tin HTTP phản hồi. Gói tin này chứa thông tin về nội dung của trang web, bao gồm văn bản, hình ảnh, ...
- Khách truy cập sẽ nhận được gói tin HTTP phản hồi và giải mã nội dung của nó. Nội dung này sau đó được hiển thị trên trình duyệt web của khách truy cập.

★ Câu hỏi mở rộng:

Địa chỉ IP dùng để nhận diện và liên lạc giữa các thiết bị trên mạng Internet. Mỗi thiết bị khi kết nối Internet đều được cấp một địa chỉ IP duy nhất, giúp các thiết bị có thể xác định và giao tiếp với nhau một cách chính xác.

Cụ thể, địa chỉ IP có các chức năng sau:

- **Nhận diện thiết bị:** Địa chỉ IP giúp các thiết bị trên mạng Internet có thể nhận diện nhau. Khi một thiết bị muốn gửi dữ liệu đến một thiết bị khác, nó cần biết địa chỉ IP của thiết bị đó.
- **Liên lạc giữa các thiết bị:** Địa chỉ IP giúp các thiết bị trên mạng Internet có thể giao tiếp với nhau. Khi một thiết bị muốn gửi dữ liệu đến một thiết bị khác, nó sẽ sử dụng địa chỉ IP của thiết bị đó để định tuyến đường truyền dữ liệu.

- **Để xem địa chỉ IP của máy tính** hoặc trang web có thể dùng wire shark để truy cập vào trang web. Địa chỉ IP sẽ nằm ở phần source và destination.

Trong ví dụ bên dưới địa chỉ IP máy tính sử dụng là 172.30.24.126 và địa chỉ IP trang web là 103.124.60.105.

http						
No.	Time	Source	Destination	Protocol	Length	Info
258	2.581127	172.30.24.126	103.124.60.105	HTTP	575	GET / HTTP/1.1
295	2.615529	103.124.60.105	172.30.24.126	HTTP	169	HTTP/1.0 302 Found