

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

Web1:

http						
No.	Time	Source	Destination	Protocol	Length	Info
41	1.956236	10.45.192.93	128.119.245.12	HTTP	569	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
57	2.270210	128.119.245.12	10.45.192.93	HTTP	492	HTTP/1.1 200 OK (text/html)

Số gói tin bắt được : $57-41=16$ gói tin và tổng thời gian bắt gói tin là: 0.313974s

Web 2: uit.edu.vn

No.	Time	Source	Destination	Protocol	Length	Info
199	3.787507	10.45.192.93	192.168.20.23	HTTP	495	GET / HTTP/1.1
208	3.839830	192.168.20.23	10.45.192.93	HTTP	552	HTTP/1.1 301 Moved Permanently (text/html)

Số gói tin bắt được là $208-199=9$ gói tin và tổng thời gian bắt gói tin là: 0.52323s

Câu 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

DNS: biến tên miền thành địa chỉ IP, để khi người dùng nhập tên miền thì sẽ dịch lại thành địa chỉ IP, từ đó giúp máy tính truy cập đến server máy chủ chứa webpage đó

MDNS: tương tự như DNS nhưng chỉ hoạt động trong mạng nội bộ

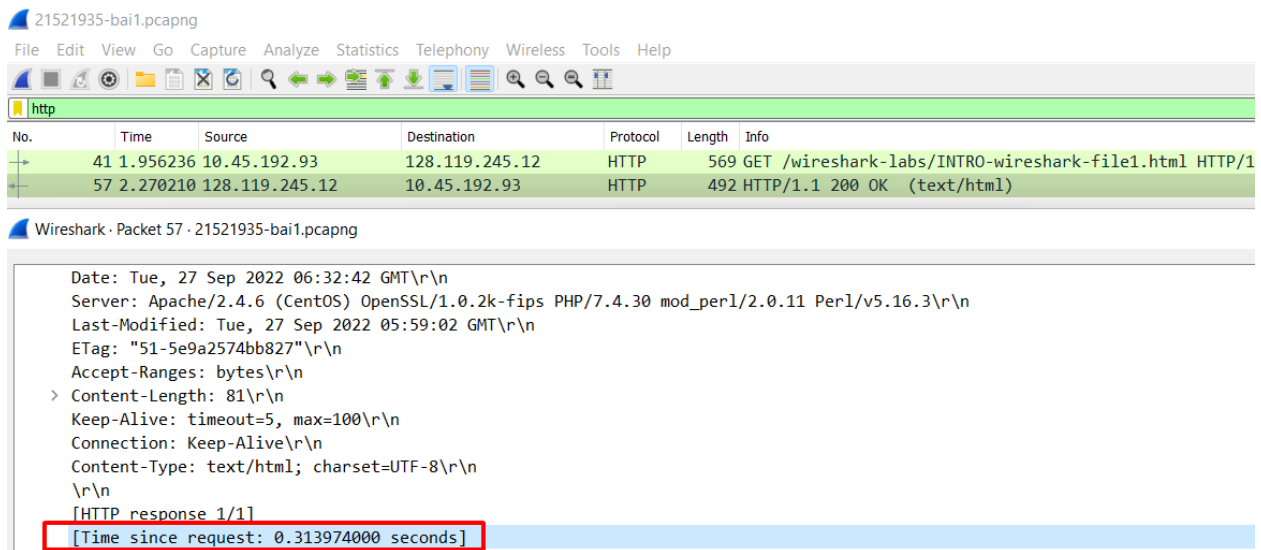
TCP: kiểm soát mức độ tin cậy của việc truyền dữ liệu. Dữ liệu được truyền theo dạng gói tin, các gói này là các cụm dữ liệu được truyền hoàn toàn độc lập trên mạng, được tập hợp lại với nhau khi chúng đến địa chỉ đích và sau đó trả về dữ liệu gốc

UDP: giao thức tương tự như TCP nhưng không kiểm soát mức độ tin cậy, có thể bị rớt 1 phần gói khi truyền đi

SSDP: một giao thức mạng dùng để quảng cáo

Câu 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 1: 0.313974s



21521935-bai1.pcapng

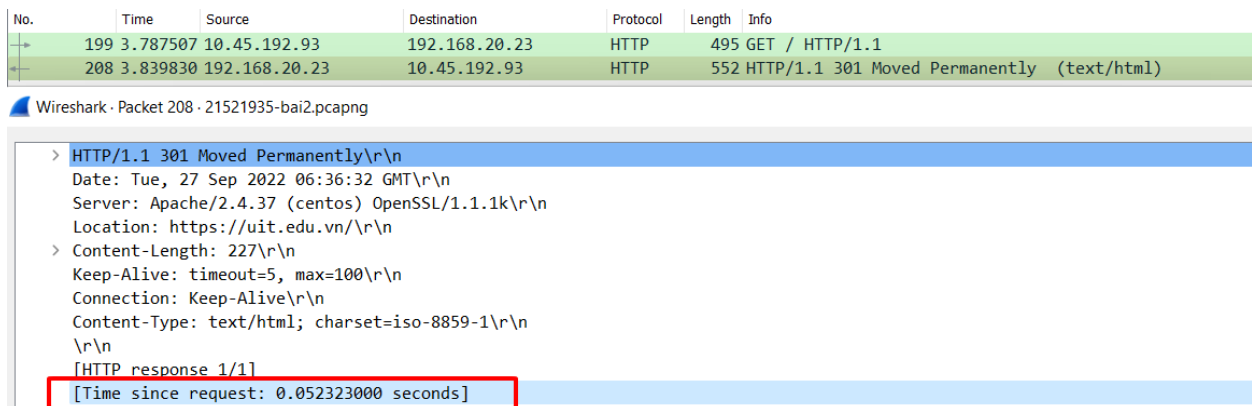
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
41	1.956236	10.45.192.93	128.119.245.12	HTTP	569	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
57	2.270210	128.119.245.12	10.45.192.93	HTTP	492	HTTP/1.1 200 OK (text/html)

Wireshark · Packet 57 · 21521935-bai1.pcapng

```
Date: Tue, 27 Sep 2022 06:32:42 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Tue, 27 Sep 2022 05:59:02 GMT\r\n
ETag: "51-5e9a2574bb827"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.313974000 seconds]
```

Web 2(uit.edu.vn): 0.52323s



No.	Time	Source	Destination	Protocol	Length	Info
199	3.787507	10.45.192.93	192.168.20.23	HTTP	495	GET / HTTP/1.1
208	3.839830	192.168.20.23	10.45.192.93	HTTP	552	HTTP/1.1 301 Moved Permanently (text/html)

Wireshark · Packet 208 · 21521935-bai2.pcapng

```
> HTTP/1.1 301 Moved Permanently\r\n
Date: Tue, 27 Sep 2022 06:36:32 GMT\r\n
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k\r\n
Location: https://uit.edu.vn/\r\n
> Content-Length: 227\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.052323000 seconds]
```

Câu 4 vị trí : 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 các gói tin HTTP bắt được.
- Nội dung trên nằm trong vùng “Line-based text data: text/html”

Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
File Data: 81 bytes

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

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

Câu 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 IP của gaia.cs.umass.edu là: 128.119.245.12

Địa chỉ IP của máy tính là: 10.45.192.93

No.	Time	Source	Destination	Protocol	Length	Info
41	1.956236	10.45.192.93	128.119.245.12	HTTP	569	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
57	2.270210	128.119.245.12	10.45.192.93	HTTP	492	HTTP/1.1 200 OK (text/html)

Câu 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

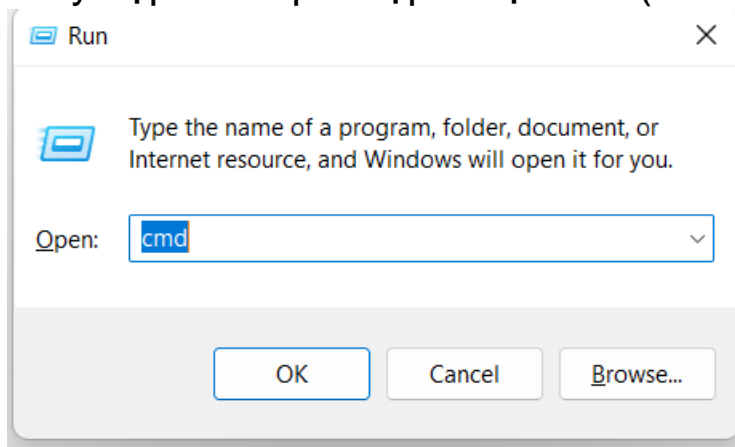
Khi người dùng duyệt web, trình duyệt sẽ kết nối và giao tiếp với name server: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>, thông qua DNS sẽ dịch lại thành địa chỉ IP: 128.119.245.12(địa chỉ của name server) . Sau đó dùng địa chỉ này kết nối máy tính tới server lưu nội dung webpage thông qua giao thức HTTP. Lúc này client(máy tính) sẽ gửi lệnh get đến server(máy chủ), và từ server sẽ gửi lại nội dung webpage cho client. Đoạn nội dung này chứa những đoạn code web , sau đó được trình duyệt dịch lại và hiển thị trang web trên màn hình

Mở rộng: địa chỉ IP như địa chỉ nhà ngoài đời. Nó dùng để xác định tính duy nhất của các thiết bị như điện thoại, laptop... và thông qua các giao thức trong mạng để giao tiếp các thiết bị với nhau

Có nhiều cách để coi địa chỉ IP, dưới đây là 2 cách phổ biến

Cách 1:

Truy cập cmd qua hộp thoại Run (CTRL R để mở hộp thoại)



Từ hộp thoại cmd, nhập ipconfig

```
Command Prompt
Microsoft Windows [Version 10.0.22000.918]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ngovu>ipconfig
```

Địa chỉ IP trong ví dụ này là 10.0.159.45

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . : 
Link-local IPv6 Address . . . . . : fe80::18c1:9ab4:ce19:ed3a%19
IPv4 Address. . . . . : 10.0.159.45
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.0.0.1

C:\Users\ngovu>
```

Cách 2:

Mở Task manager(CTRL shift S để mở nhanh)

Task Manager

File Options View

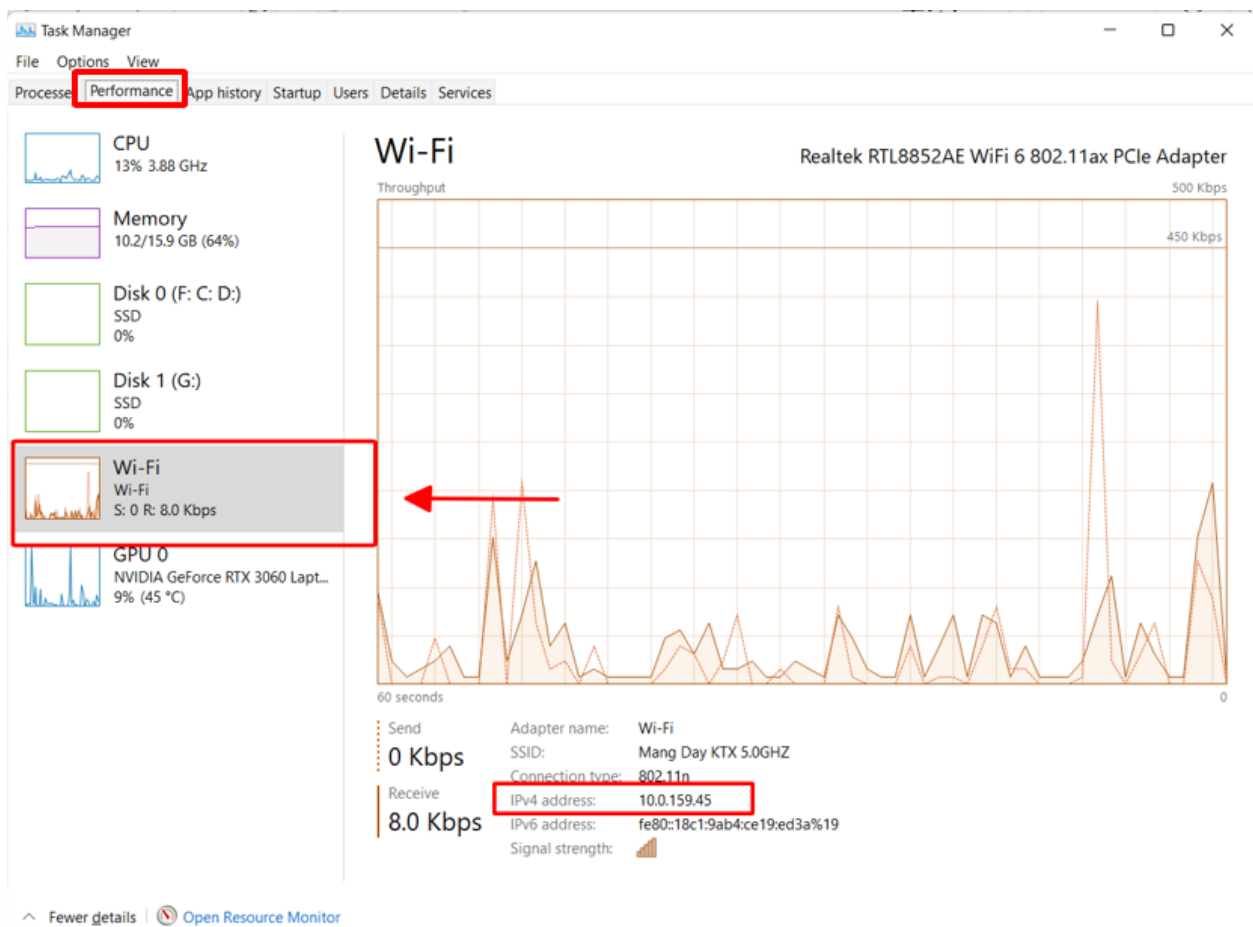
Processes Performance App history Startup Users Details Services

Name	Status	11% CPU	64% Memory	0% Disk	0% Network	0% GPU	GPU engine	Power usage	Power usage tr...
> Google Chrome (35)		0.1%	1,616.1 MB	0.1 MB/s	0.1 Mbps	0%	GPU 0 - 3D	Very low	Very low
> Zalo (32 bit) (11)		0%	387.0 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
> Discord (32 bit) (6)		0.2%	197.5 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
> Spotify (8)		0%	188.3 MB	0.1 MB/s	0 Mbps	0.1%	GPU 0 - 3D	Very low	Very low
> Kaspersky Lab launcher (32 bit)		0%	116.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Explorer		0.1%	96.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Microsoft Word		0%	96.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Kaspersky Password Manager (32 ...)		0%	83.6 MB	0 MB/s	0.1 Mbps	0%		Very low	Very low
> Foxit PDF Reader 12.0 (32 bit)		0%	64.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Microsoft Edge (11)		0%	62.3 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
Desktop Window Manager		1.8%	49.7 MB	0 MB/s	0 Mbps	0.2%	GPU 0 - 3D	Low	Very low
> SQL Server Windows NT - 64 Bit		5.3%	47.3 MB	0 MB/s	0 Mbps	0%		High	Very low
> Task Manager		1.4%	36.7 MB	0.1 MB/s	0 Mbps	0%		Low	Very low
> Phone Link (2)		0%	34.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> LenovoVantageService		0%	33.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Steam Client WebHelper		0%	31.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
WMI Provider Host		0%	30.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Windows Input Experience (3)		0%	29.0 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
Steam Client WebHelper		0%	25.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
> Service Host: Diagnostic Policy Se...		0%	23.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low

< Fewer details

End task

Vào thẻ performance rồi chọn biểu tượng mạng như Wifi hoặc Lan để xem



Địa chỉ IP: 10.0.159.45