



Lab 1

BÁO CÁO BÀI THỰC HÀNH SỐ 1

Làm quen với Wireshark

Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Giảng viên hướng dẫn	ThS. Đỗ Thị Hương Lan
Sinh viên thực hiện	Nguyễn Duy Khang (22520619)
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	22/09/2019 – 29/09/2019
Tự chấm điểm	9.5/10

A. CÁC BƯỚC THỰC HÀNH

Gợi ý: Ghi rõ từng bước thực hành, chụp hình ảnh screenshot để báo cáo thêm trực quan

B. TRẢ LỜI CÁC CÂU HỎI

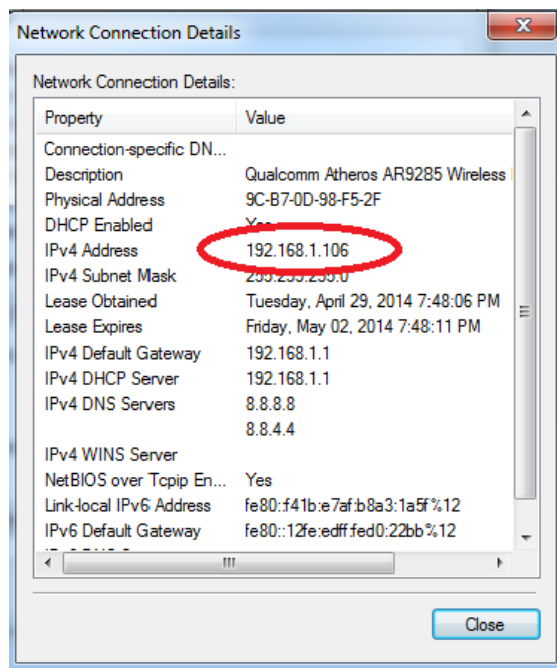
Gợi ý: Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

Trả lời: 192.168.1.106

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks**. Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



1. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

Lab 1: Làm quen với Wireshark

No.	Time	Source	Destination
533	77.962303	142.250.207.78	192.168.220.1
534	77.962573	192.168.220.195	142.250.207.7
535	78.000706	142.250.207.78	192.168.220.1
536	78.342156	192.168.220.67	224.0.0.251
537	78.701606	192.168.220.107	239.255.255.2
538	79.267590	192.168.220.150	239.255.255.2
539	79.784867	192.168.220.107	239.255.255.2
540	80.088686	192.168.123.1	224.0.0.1

- Tổng thời gian bắt gói tin của em là 80.088686 giây
 - Số gói tin bắt được là 540 gói
2. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol). Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.
- 3 giao thức khác nhau gồm: DNS, HTTP, TCP

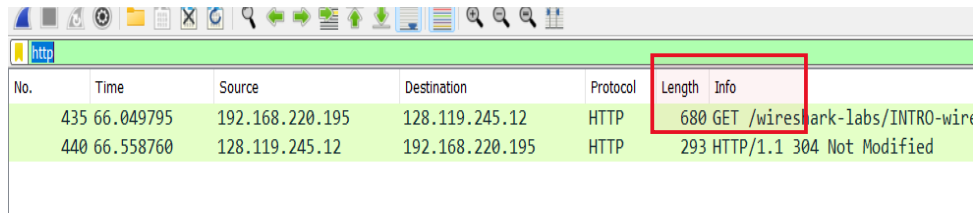
240	25.762024	192.168.220.195	20.190.144.166	TCP	
243	25.764379	192.168.220.195	20.190.144.166	TCP	
244	25.955523	192.168.220.195	20.190.144.166	TCP	
209	23.897529	192.168.220.195	20.190.144.166	TCP	
271	32.235251	192.168.220.195	209.97.170.78	TCP	
284	32.414842	192.168.220.195	209.97.170.78	TCP	
286	32.419253	192.168.220.195	209.97.170.78	TCP	
291	33.696167	192.168.220.195	209.97.170.78	TCP	
8	2.426316	192.168.54.4	192.168.220.195	DNS	129 Standard query query
508	77.635583	192.168.54.4	192.168.220.195	DNS	163 Standard query response
398	59.160951	192.168.54.4	192.168.220.195	DNS	92 Standard query response
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293 HTTP/1.1 304 Not Modified

- DNS (Domain Name Server): là một giao thức tiêu chuẩn cho phép người dùng nhập địa chỉ của một trang web và tự động khám phá địa chỉ giao thức Internet (Internet Protocol hay IP) cho trang web đó.
- TCP (Transmission Control Protocol): là một giao thức mạng quan trọng được sử dụng trong việc truyền dữ liệu qua một mạng nào đó. Chức năng của giao thức TCP là để kiểm soát độ tin cậy của việc truyền dữ liệu.
- HTTP (Hypertext Transfer Protocol): là một giao thức truyền tải siêu văn bản. Đây là giao thức tiêu chuẩn cho World Wide Web (www) để truyền tải dữ liệu dưới dạng văn bản, âm thanh, hình ảnh, video từ Web Server tới trình duyệt web của người dùng và ngược lại.

No.	Time	Source	Destination	Protocol	Length	Info
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293	HTTP/1.1 304 Not Modified

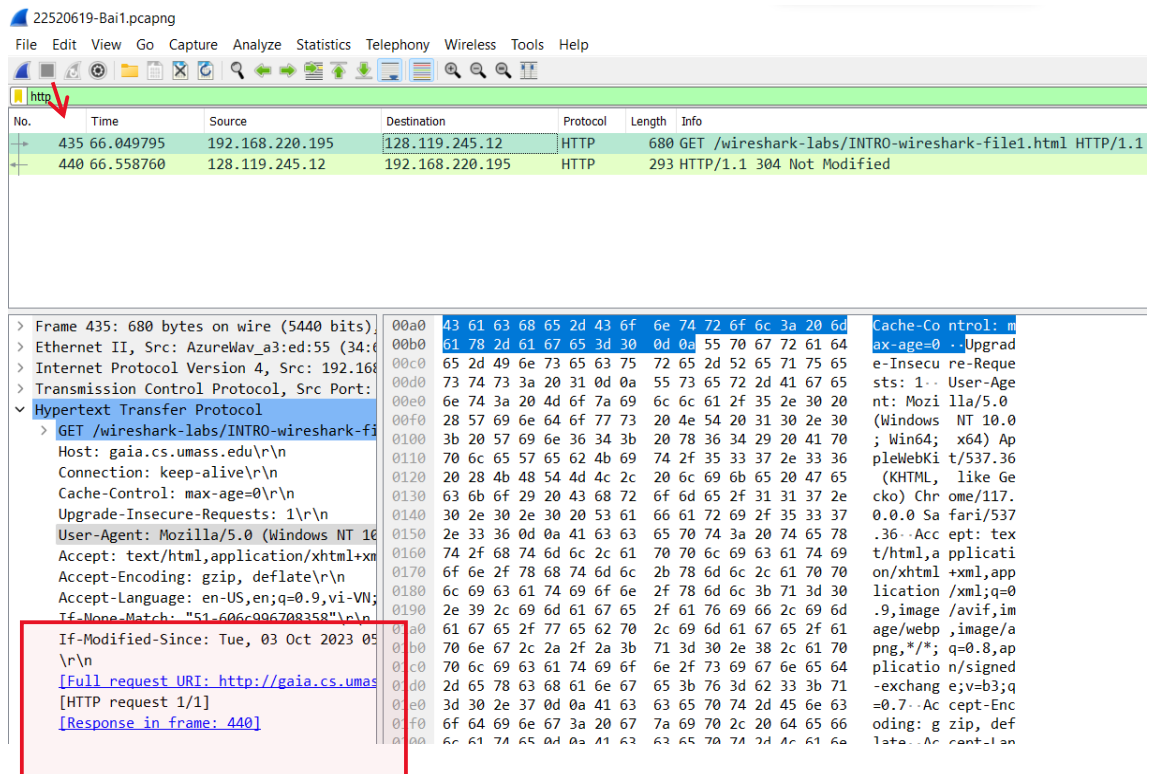
3. Có bao nhiêu gói tin HTTP? Tỷ lệ % số gói tin HTTP/Tổng số gói tin?
- Có 2 gói tin HTTP, và tỷ lệ số gói tin là 2/540
4. Có bao nhiêu gói tin HTTP GET?
- Quan sát cột info: có 1 gói tin HTTP GET

Lab 1: Làm quen với Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293	HTTP/1.1 304 Not Modified

5. Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server gaia.cs.umass.edu?



22520619-Bai1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 435: 680 bytes on wire (5440 bits) [Captured] (Ethernet II, Src: AzureWav_a3:ed:55 (34:69:b3:4c:55:ed), Dst: 02:00:0c:00:00:00 (02:00:0c:00:00:00))

> Ethernet II, Src: AzureWav_a3:ed:55 (34:69:b3:4c:55:ed), Dst: 02:00:0c:00:00:00 (02:00:0c:00:00:00)

> Internet Protocol Version 4, Src: 192.168.220.195, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 5440, Dst Port: 80

> Hypertext Transfer Protocol

> GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Host: gaia.cs.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/117.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9,vi-VN;q=0.7\r\n

If-None-Match: "51-606c906708358"\r\n

If-Modified-Since: Tue, 03 Oct 2023 05:00:00 GMT\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 440]

- Thông qua Packet Details, ta thấy gói tin thứ 435 có HTTP request 1/1 nên đây là gói tin đầu tiên được gửi đến.
6. Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?
- Thông qua Packet Details, ta thấy gói tin thứ 435 có Response in frame: 440 nên gói tin thứ 440 là gói tin phản hồi cho gói HTTP GET ở trên

Lab 1: Làm quen với Wireshark

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request and response. The packet list table at the top shows two packets:

No.	Time	Source	Destination	Protocol	Length	Info
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293	HTTP/1.1 304 Not Modified

A red arrow points to the packet list table. The packet details pane on the left shows the selected packet (440) and its details:

- Frame 435: 680 bytes on wire (5440 bits)
- Ethernet II, Src: AzureWav_a3:ed:55 (34:6d:63:68:65:2d), Dst: 192.168.220.195
- Internet Protocol Version 4, Src: 192.168.220.195, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 55876, Dst Port: 80
- Hypertext Transfer Protocol
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 - Host: gaia.cs.umass.edu
 - Connection: keep-alive
 - Cache-Control: max-age=0
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.9,vi-VN;q=0.8
 - If-None-Match: "51-606c996708358"
 - If-Modified-Since: Tue, 03 Oct 2023 05:59:02 GMT

The packet bytes pane on the right shows the raw data of the selected packet (440) in hexadecimal and ASCII.

7. Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)?
 - Quan sát cửa sổ chi tiết gói tin số 440, ở mục Time since request: 0.508965 second nghĩa là mất 0.508965 giây từ lúc gửi gói tin HTTP GET đến khi nhận được gói tin phản hồi

Lab 1: Làm quen với Wireshark

Wireshark packet capture showing an HTTP 304 Not Modified response. The packet list shows frame 440 as the response. The packet details pane shows the HTTP response structure, including status, date, server, and connection info. A red arrow points to the 'Request in frame: 435' link.

No.	Time	Source	Destination	Protocol	Length	Info
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680	GET /
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293	HTTP/1.1 304 Not Modified

Packet details for frame 440:

- Frame 440: 293 bytes on wire (2344 bits)
- Ethernet II, Src: JuniperN_8c:35:b0 (44:4c:99:8c:35:b0), Dst: 192.168.220.195
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.220.195
- Transmission Control Protocol, Src Port: 80, Dst Port: 80
- Hypertext Transfer Protocol
 - HTTP/1.1 304 Not Modified\r\n
 - Date: Wed, 04 Oct 2023 02:11:50 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k\r\n
 - Connection: Keep-Alive\r\n
 - Keep-Alive: timeout=5, max=100\r\n
 - ETag: "51-606c996708358"\r\n
 - \r\n
 - [HTTP response 1/1]
 - [Time since request: 0.508965000 seconds]
 - [Request in frame: 435]
 - [Request URI: http://gaia.cs.umass.edu/]

8. Dự đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì? Tại sao?

Wireshark packet capture showing an HTTP GET request and a 304 Not Modified response. Red arrows point to the Source and Destination IP addresses in the packet list.

No.	Time	Source	Destination	Protocol	Length	Info
435	66.049795	192.168.220.195	128.119.245.12	HTTP	680	GET /wireshark-labs/INTRO-wireshark
440	66.558760	128.119.245.12	192.168.220.195	HTTP	293	HTTP/1.1 304 Not Modified

- Thông qua phần Destination của gói tin 435, ta thấy đây là điểm đến gaia.cs.umass.edu được gửi từ máy tính, nên 128.119.245.12 là địa chỉ của gaia.cs.umass.edu
- Địa chỉ IP của máy dự đoán sẽ nằm ở phần Source, chính là nguồn gửi gói tin đến điểm đến, nguồn gửi ở đây là máy tính, vậy địa chỉ IP của máy đang sử dụng có thể là 192.168.220.195

9. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

Lab 1: Làm quen với Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
305	14.765875	192.168.220.195	192.168.54.4	TCP	54	60048 → 53 [FIN, ACK] S
306	14.765896	192.168.220.195	192.168.20.4	TCP	54	60046 → 53 [FIN, ACK] S
307	14.765908	192.168.220.195	192.168.20.4	TCP	54	60046 → 53 [RST, ACK] S
308	15.284771	192.168.220.195	192.168.20.4	TCP	89	[TCP Retransmission] 60
309	15.539519	192.168.220.195	49.213.95.49	TLSv1.2	101	Application Data
310	15.666369	192.168.20.4	192.168.220.195	TCP	66	[TCP Dup ACK 291#1] 53
311	15.666407	192.168.220.195	192.168.20.4	TCP	54	60046 → 53 [RST] Seq=36
312	15.739872	192.168.220.195	192.168.54.4	TCP	89	[TCP Retransmission] 60

- Tổng thời gian bắt gói tin của em là 15.739872 giây
- Số gói tin bắt được là 312 gói

10. . Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol)?

Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó?

50	5.015495	192.168.220.57	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
57	5.016733	192.168.220.57	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
58	5.017484	192.168.20.4	192.168.220.195	TCP	66	53 → 60038 [SYN, ACK] Seq=0
59	5.017531	192.168.220.195	192.168.20.4	TCP	54	60038 → 53 [ACK] Seq=1 Ack=1
60	5.017788	192.168.220.195	192.168.20.4	TCP	56	60038 → 53 [PSH, ACK] Seq=1
61	5.017806	192.168.220.195	192.168.20.4	DNS	85	Standard query 0x198b A celu

- 3 giao thức khác nhau xuất hiện trong cột giao thức gồm: TCP, DNS, SSDP
- DNS (Domain Name Server): là một giao thức tiêu chuẩn cho phép người dùng nhập địa chỉ của một trang web và tự động khám phá địa chỉ giao thức Internet (Internet Protocol hay IP) cho trang web đó.
- TCP (Transmission Control Protocol): là một giao thức mạng quan trọng được sử dụng trong việc truyền dữ liệu qua một mạng nào đó. Chức năng của giao thức TCP là để kiểm soát độ tin cậy của việc truyền dữ liệu
- SSDP: SSDP là viết tắt của Simple Service Discovery Protocol, nghĩa là Giao thức khám phá dịch vụ đơn giản, SSDP là tiêu chuẩn cho các dịch vụ quảng cáo trên mạng TCP/IP và phát hiện ra chúng. Giao thức Universal Plug and Play (UPnP) sử dụng SSDP để thông báo và tìm thiết bị theo thứ tự, chẳng hạn như để truyền video từ nguồn đến hệ thống phát lại.

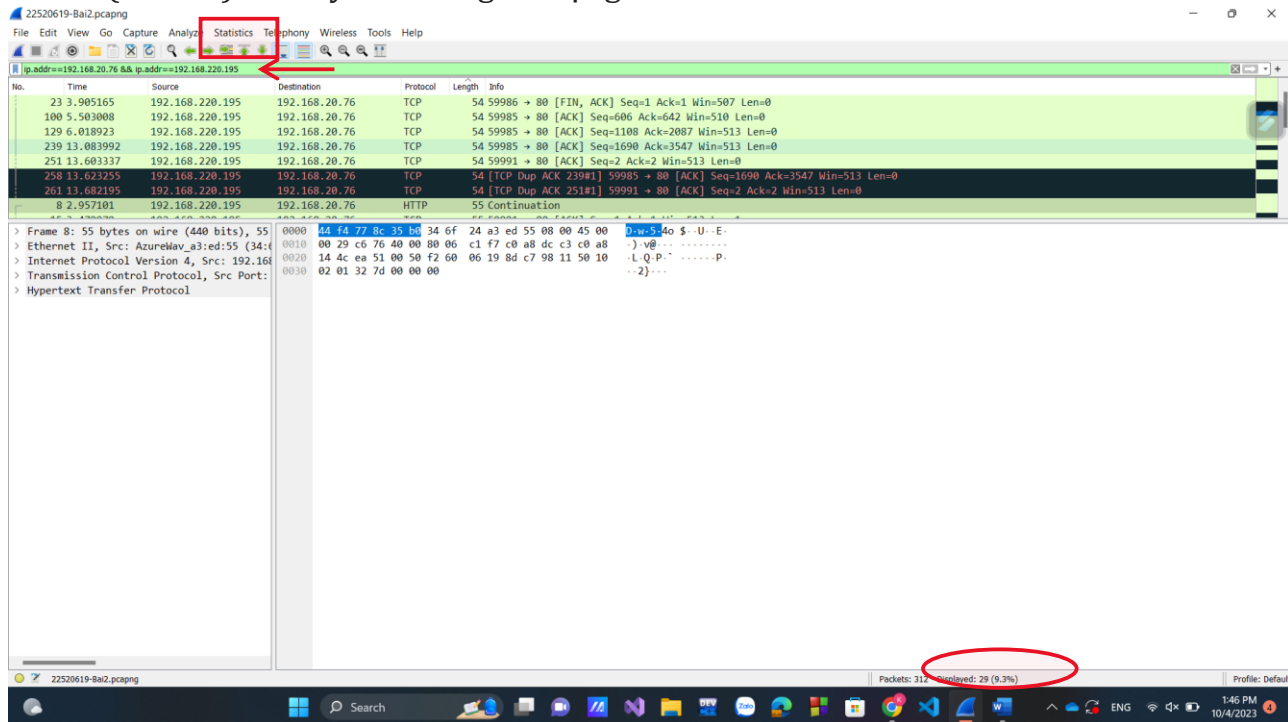
11. Tìm cách để xác định địa chỉ IP của trang web đã chọn ở Bước 8. Địa chỉ IP trang web đã chọn là gì ?

No.	Time	Source	Destination	Protocol	Length	Info
8	2.957101	192.168.220.195	192.168.20.76	HTTP	55	Continuation
46	4.929139	192.168.220.195	192.168.20.76	HTTP	658	GET / HTTP/1.1
76	5.453305	192.168.20.76	192.168.220.195	HTTP	695	HTTP/1.1 304 Not Modified
105	5.559978	192.168.220.195	192.168.20.76	HTTP	556	GET /select2/ajax/get_settings HTTP/1.1
124	5.967896	192.168.20.76	192.168.220.195	HTTP/1.1	1499	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
134	6.754724	192.168.220.195	192.168.20.76	HTTP	636	GET /sites/all/libraries/flexslider/fonts/flexslider-icon.woff HTTP/1.1

> Frame 46: 658 bytes on wire (5264 bits),	0030	02 01 b6 af 00 00 47 45	54 20 2f 20 48 54 54 50GE T / HTTP
> Ethernet II, Src: AzureWav_a3:ed:55 (34:6d:63:74:2e:65), Dst: 192.168.20.76 (08:00:0a:2d:2d:61)	0040	2f 31 2e 31 0d 0a 48 6f	73 74 3a 20 63 65 6c 75	/1.1. Host: celu
> Internet Protocol Version 4, Src: 192.168.220.195, Dst: 192.168.20.76	0050	69 74 2e 65 64 75 2e 76	6e 0d 0a 43 6f 6e 6e 65	it.edu.vn - Conne
> Transmission Control Protocol, Src Port: 53, Dst Port: 80	0060	63 74 69 6f 6e 3a 20 6b	65 65 70 2d 61 6c 69 76	ction: keep-aliv
> Hypertext Transfer Protocol	0070	65 0d 0a 55 70 67 72 61	64 65 2d 49 6e 73 65 63	e - Upgra de-Insec
> GET / HTTP/1.1	0080	75 72 65 2d 52 65 71 75	65 73 74 73 3a 20 31 0d	ure-Reqe sts: 1-
> Host: celu.it.edu.vn	0090	0a 55 73 65 72 2d 41 67	65 6e 74 3a 20 4d 6f 7a	User-Ag ent: Moz
> Connection: keep-alive	00a0	69 6c 6c 61 2f 35 2e 30	20 28 57 69 6e 64 6f 77	illa/5.0 (Window
> Upgrade-Insecure-Requests: 1	00b0	73 20 4e 54 20 31 30 2e	30 3b 20 57 69 6e 36 34	s NT 10.0; Win64
> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36	00c0	3b 20 78 36 34 29 20 41	70 70 6c 65 57 65 62 4b	; x64) A ppleWebK
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	00d0	69 74 2f 35 33 37 2e 33	36 20 28 4b 48 54 4d 4c	it/537.3 6 (KHTML
> Accept-Encoding: gzip, deflate	00e0	2c 20 6c 69 6b 65 20 47	65 63 6b 6f 29 20 43 68	, like G ecko) Ch
> Accept-Language: en-US,en;q=0.9,vi-VN;q=0.8	00f0	72 6f 6d 65 2f 31 31 37	2e 30 2e 30 2e 30 20 53	rome/117 .0.0.0 S
>	0100	61 66 61 72 69 2f 35 33	37 2e 33 36 0d 0a 41 63	afari/53 7.36--Ac
>	0110	63 65 70 74 3a 20 74 65	78 74 2f 68 74 6d 6c 7c	cent: te xt/html.

Lab 1: Làm quen với Wireshark

- Thông qua chi tiết gói tin, ta thấy gói tin số 46 là gói tin mà máy tính gửi đến địa chỉ trang web đã chọn, nên ở mục Destination (điểm đến) là địa chỉ của trang web đó
 - Do đó, địa chỉ của trang web đã chọn là 192.168.20.76
12. Số lượng gói tin và khối lượng dữ liệu được gửi (trao đổi) giữa Địa chỉ trang web ở trên (Câu 11) và máy tính đang sử dụng ?



- Để xem số lượng gói tin và khối lượng dữ liệu được trao đổi giữa địa chỉ trang web celuit.edu.vn với máy tính đang sử dụng, ta chọn Statistics -> Conversations -> IPv4

Ethernet · 1														IPv4 · 1		IPv6		TCP · 3		UDP	
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Re Start	Duration	Bits/s A → B	Bits/s B → A								
192.168.220.195	192.168.20.76	29	10 kB	29	100.00%	16	4 kB	13	6 kB	2.97101	10.8364	3183 bits/s	4267 bits/s								

- Ta thấy tổng số lượng gói tin là 29, có thể quan sát ở mục Packets
- Ta thấy khối lượng dữ liệu trao đổi từ A -> B là 4kB và B->A là 6kB, suy ra tổng khối lượng dữ liệu trao đổi giữa A và B là 10kB trong đó A là địa chỉ của máy tính, B là địa chỉ của trang web sử dụng