



# Lab 1

## BÁO CÁO BÀI THỰC HÀNH SỐ 1

# Làm quen với Wireshark

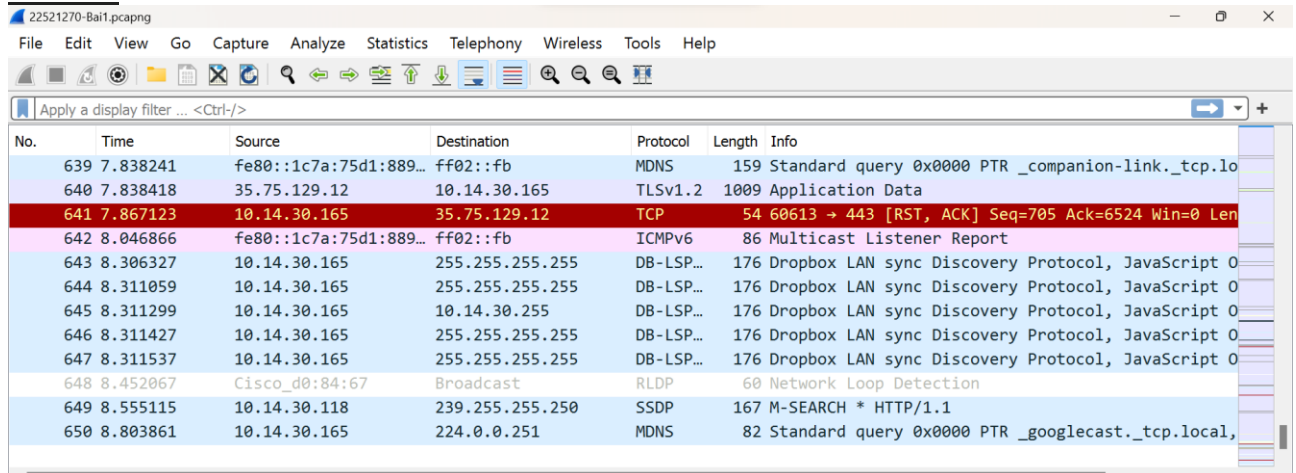
## Wireshark Getting Started

**Môn học: Nhập môn Mạng máy tính**

Sinh viên thực hiện	ĐẶNG ĐỨC TÀI (22521270)
Thời gian thực hiện	04/10/2023 – 05/10/2023
Tự chấm điểm	10/10

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

**Trả lời:**

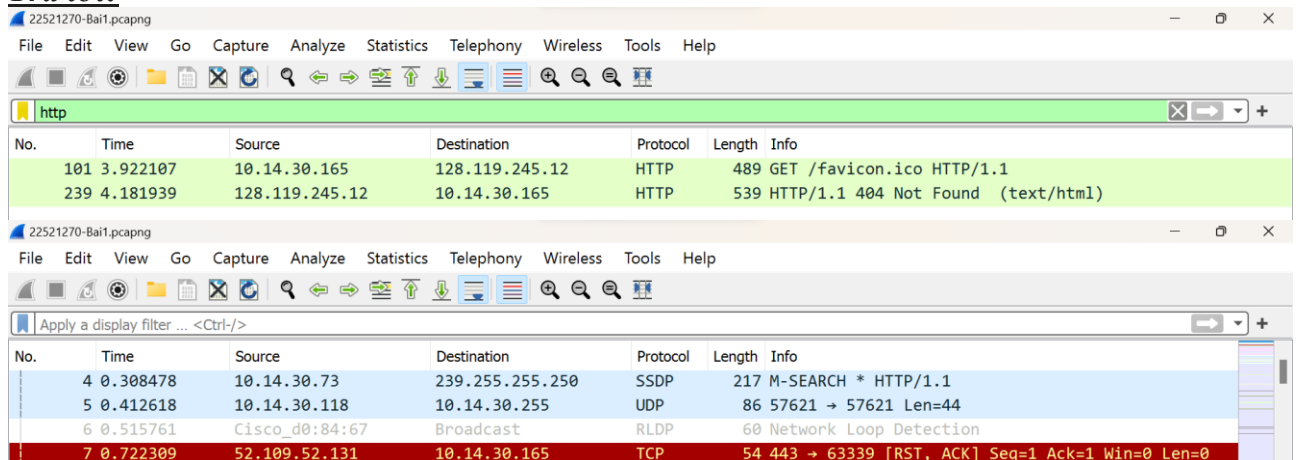


No.	Time	Source	Destination	Protocol	Length	Info
639	7.838241	fe80::1c7a:75d1:889...	ff02::fb	MDNS	159	Standard query 0x0000 PTR _companion-link._tcp.lo
640	7.838418	35.75.129.12	10.14.30.165	TLSv1.2	1009	Application Data
641	7.867123	10.14.30.165	35.75.129.12	TCP	54	60613 → 443 [RST, ACK] Seq=705 Ack=6524 Win=0 Len=0
642	8.046866	fe80::1c7a:75d1:889...	ff02::fb	ICMPv6	86	Multicast Listener Report
643	8.306327	10.14.30.165	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol, JavaScript 0
644	8.311059	10.14.30.165	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol, JavaScript 0
645	8.311299	10.14.30.165	10.14.30.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol, JavaScript 0
646	8.311427	10.14.30.165	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol, JavaScript 0
647	8.311537	10.14.30.165	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol, JavaScript 0
648	8.452067	Cisco_d0:84:67	Broadcast	RLDP	60	Network Loop Detection
649	8.555115	10.14.30.118	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
650	8.803861	10.14.30.165	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local,

- Tổng thời gian bắt gói tin là: **8.803861 (giây)**
- Tổng số gói tin bắt được là: **650 (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.

**Trả lời:**



No.	Time	Source	Destination	Protocol	Length	Info
101	3.922107	10.14.30.165	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
239	4.181939	128.119.245.12	10.14.30.165	HTTP	539	HTTP/1.1 404 Not Found (text/html)
4	0.308478	10.14.30.73	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5	0.412618	10.14.30.118	10.14.30.255	UDP	86	57621 → 57621 Len=44
6	0.515761	Cisco_d0:84:67	Broadcast	RLDP	60	Network Loop Detection
7	0.722309	52.109.52.131	10.14.30.165	TCP	54	443 → 63339 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Các giao thức xuất hiện trong cột Protocol là: HTTP, UDP, TCP...

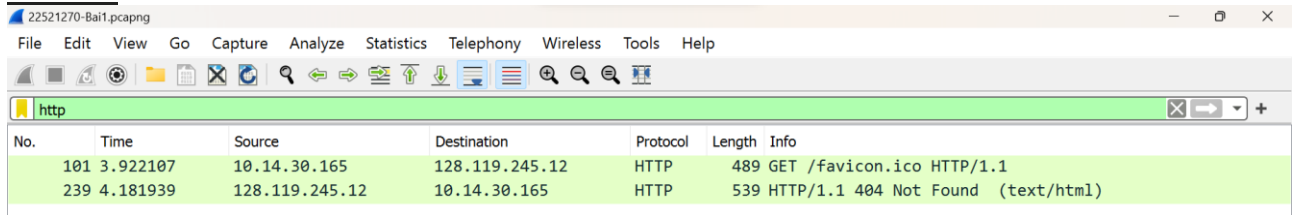
+ **Giao thức HTTP:** là giao thức ở tầng ứng dụng; là giao thức truyền tải siêu văn bản được sử dụng trong web dùng để truyền tải dữ liệu giữa Web server đến các trình duyệt web và ngược lại. Giao thức này chủ yếu sử dụng cổng 80.

+ **Giao thức UDP:** là giao thức ở tầng vận chuyển, truyền dữ liệu không tin cậy và không theo thứ tự và giao thức này không đảm bảo sự toàn vẹn dữ liệu tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu có kích thước nhỏ và yêu cầu khẩn cấp về thời gian.

+ **Giao thức TCP:** là giao thức ở tầng vận chuyển, truyền dữ liệu tin cậy; đảm bảo trao đổi thành công giữa các gói dữ liệu qua các thiết bị mạng. Nó đảm bảo không có sự mất mát nào xảy ra trong quá trình truyền tin.

### 3. Có bao nhiêu gói tin HTTP? Tỷ lệ % số gói tin HTTP/Tổng số gói tin?

Trả lời:

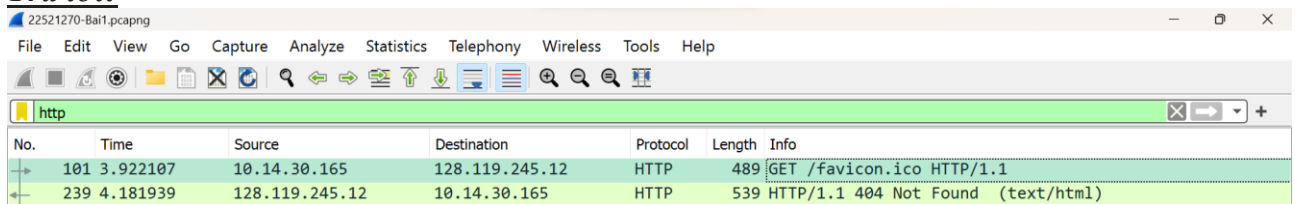


No.	Time	Source	Destination	Protocol	Length	Info
101	3.922107	10.14.30.165	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
239	4.181939	128.119.245.12	10.14.30.165	HTTP	539	HTTP/1.1 404 Not Found (text/html)

- Có 2 gói tin HTTP.
- Tỷ lệ % số gói tin HTTP/Tổng số gói tin là: **0.31%**

### 4. Có bao nhiêu gói tin HTTP GET?

Trả lời:



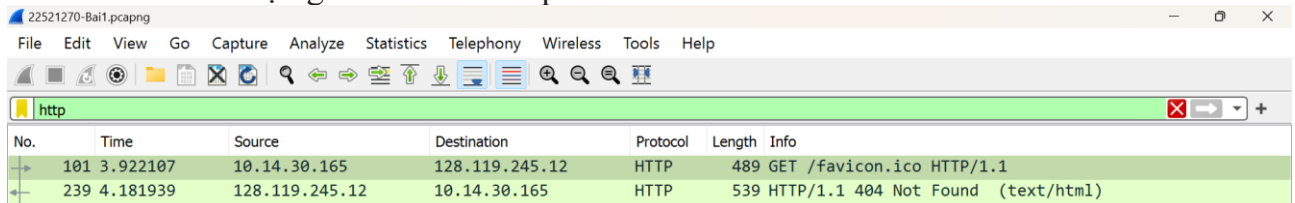
No.	Time	Source	Destination	Protocol	Length	Info
101	3.922107	10.14.30.165	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
239	4.181939	128.119.245.12	10.14.30.165	HTTP	539	HTTP/1.1 404 Not Found (text/html)

- Có 1 gói tin HTTP GET.

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

Trả lời:

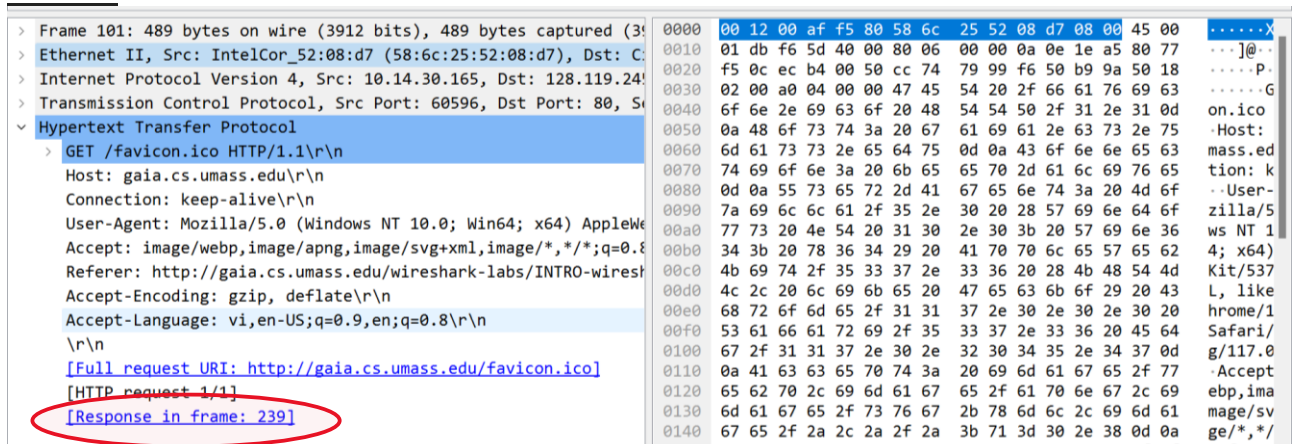
- Bước 1: Gõ “HTTP” trên filter.
- Bước 2: Chọn gói tin có bắt đầu là “GET” ở cột Info.
- Bước 3: Click chọn gói tin và xem ở phần detail.



No.	Time	Source	Destination	Protocol	Length	Info
101	3.922107	10.14.30.165	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
239	4.181939	128.119.245.12	10.14.30.165	HTTP	539	HTTP/1.1 404 Not Found (text/html)

### 6. Xác định gói tin phản hồi cho gói HTTP GET?

Trả lời:



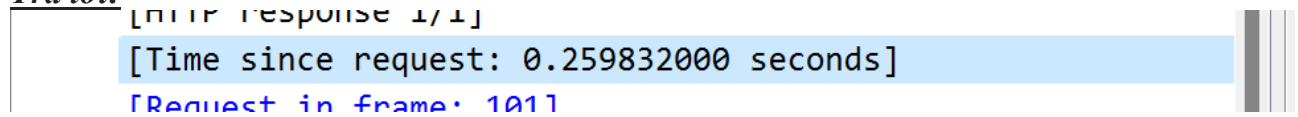
Frame	Time	Source	Destination	Protocol	Length	Info
101	3.922107	10.14.30.165	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
239	4.181939	128.119.245.12	10.14.30.165	HTTP	539	HTTP/1.1 404 Not Found (text/html)

## Lab 1: Làm quen với Wireshark

- Dựa vào **Response in frame** ta xác định được gói tin phản hồi có STT là: **239**

### 7. Mất bao lâu từ lúc gửi gói tin HTTP GET đến khi nhận được gói tin phản hồi?

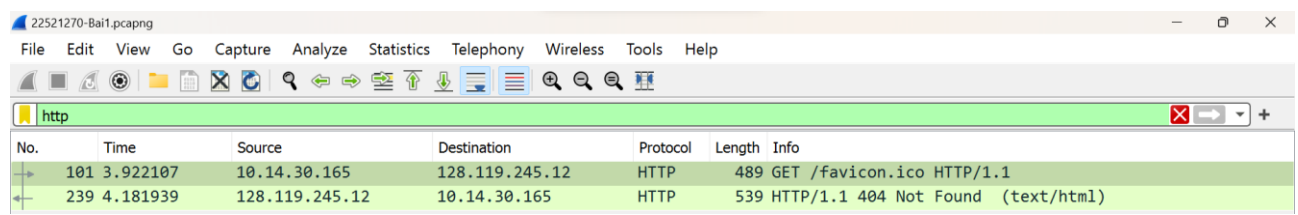
Trả lời:



- Thời gian từ lúc gửi gói tin HTTP GET đến khi nhận được gói tin phản hồi là: **0.259832s**

### 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?

Trả lời:



- Đối với gói tin 101, là gói tin gửi đi chứa thông điệp từ sender gửi đến server web nên có thể dự đoán:

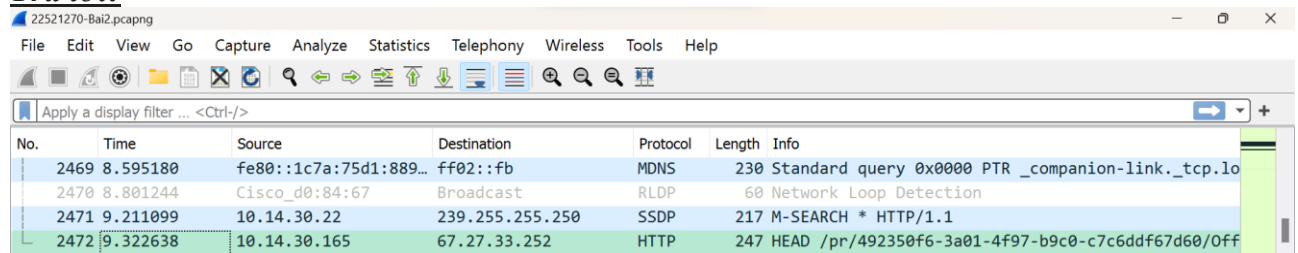
+ Địa chỉ IP của source (bên gửi request – máy tính đang sử dụng) là: **10.14.30.165**

+ Địa chỉ IP của gaia.cs.umass.edu (bên nhận request) là: **128.119.245.12**

**Sử dụng file 22521270-Bai2.pcapng**

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

Trả lời:

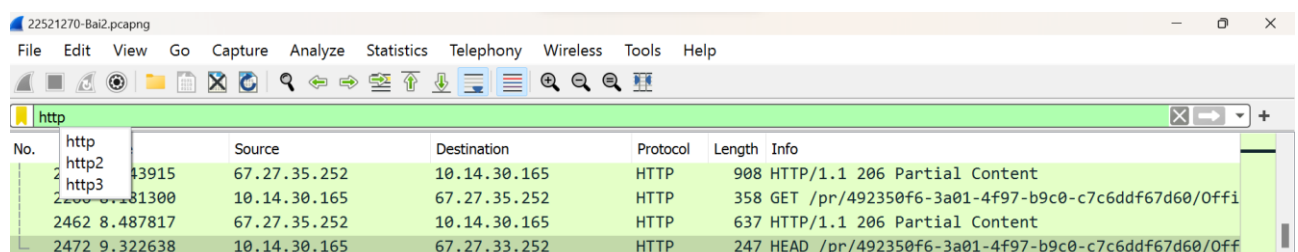


- Tổng thời gian bắt gói tin là: **9.322638 (giây)**

- Tổng số gói tin bắt được là: **2472 (gói)**

### 10. Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức? Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

Trả lời:



## Lab 1: Làm quen với Wireshark

The top screenshot shows a packet capture with the filter 'udp'. The packet list shows one packet (No. 2464) at time 8.492205, source 10.14.30.22, destination 255.255.255.255, protocol UDP, length 43, and info 55056 → 8899 Len=1.

The bottom screenshot shows a packet capture with the filter 'tcp'. The packet list shows two packets (Nos. 2463 and 2465) at times 8.487884 and 8.496605, source 10.14.30.165, destination 67.27.35.252, protocol TCP, length 54, and info 60963 → 80 [ACK] Seq=305 Ack=348084 Win=524800 Le and 60963 → 80 [FIN, ACK] Seq=305 Ack=348084 Win=5248.

- Các giao thức xuất hiện trong cột Protocol là: HTTP, UDP, TCP...

+ **Giao thức HTTP:** là giao thức ở tầng ứng dụng; là giao thức truyền tải siêu văn bản được sử dụng trong web dùng để truyền tải dữ liệu giữa Web server đến các trình duyệt web và ngược lại. Giao thức này chủ yếu sử dụng cổng 80.

+ **Giao thức UDP:** là giao thức ở tầng vận chuyển, truyền dữ liệu không tin cậy và không theo thứ tự và giao thức này không đảm bảo sự toàn vẹn dữ liệu tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu có kích thước nhỏ và yêu cầu khẩn khe về thời gian.

+ **Giao thức TCP:** là giao thức ở tầng vận chuyển, truyền dữ liệu tin cậy; đảm bảo trao đổi thành công giữa các gói dữ liệu qua các thiết bị mạng. Nó đảm bảo không có sự mất mát nào xảy ra trong quá trình truyền tin.

### 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 ?

#### Trả lời:

- Bước 1: Gõ “http” trong filter.

The screenshot shows a packet capture with the filter 'http'. The packet list shows several packets (Nos. 25, 35, 66, 89, 99) at various times, source 10.14.30.165, destination 67.27.35.252, protocol HTTP, and info GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Offi and HTTP/1.1 206 Partial Content.

- Bước 2: Chọn từng gói tin và xác định đường dẫn celuit.edu.vn

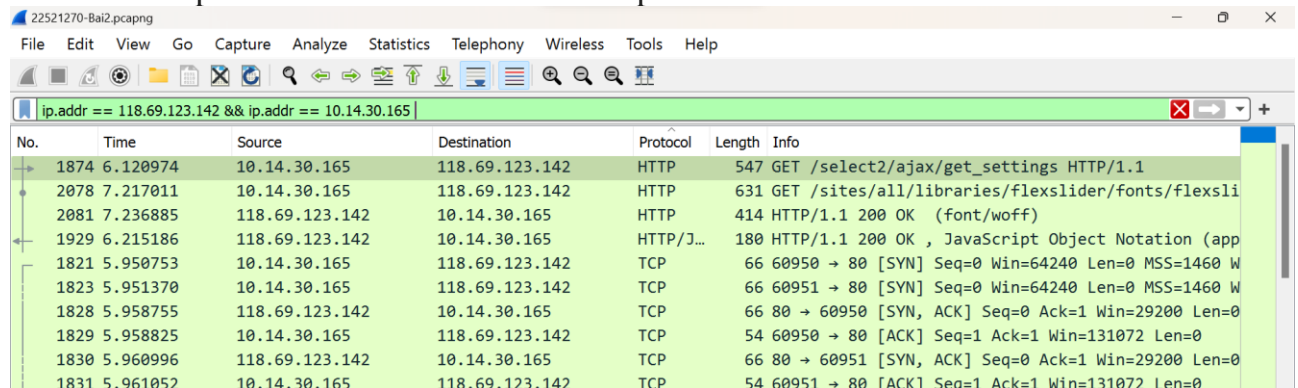
The screenshot shows a packet capture with the filter 'http'. The packet list shows one packet (No. 1874) at time 6.120974, source 10.14.30.165, destination 118.69.123.142, protocol HTTP, length 547, and info GET /select2/ajax/get\_settings HTTP/1.1. The packet details show the full request URI: http://www.celuit.edu.vn/select2/ajax/get\_.

- Địa chỉ IP của trang web đã chọn là: 118.69.123.142

**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 ?**

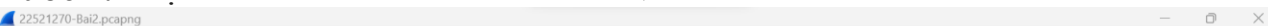
**Trả lời:**

**Bước 1:** Gõ ip.addr == 118.69.123.142 && ip.addr == 10.14.30.165



No.	Time	Source	Destination	Protocol	Length	Info
1874	6.120974	10.14.30.165	118.69.123.142	HTTP	547	GET /select2/ajax/get_settings HTTP/1.1
2078	7.217011	10.14.30.165	118.69.123.142	HTTP	631	GET /sites/all/libraries/flexslider/fonts/flexsli
2081	7.236885	118.69.123.142	10.14.30.165	HTTP	414	HTTP/1.1 200 OK (font/woff)
1929	6.215186	118.69.123.142	10.14.30.165	HTTP/J...	180	HTTP/1.1 200 OK , JavaScript Object Notation (app
1821	5.950753	10.14.30.165	118.69.123.142	TCP	66	60950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
1823	5.951370	10.14.30.165	118.69.123.142	TCP	66	60951 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
1828	5.958755	118.69.123.142	10.14.30.165	TCP	66	80 → 60950 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
1829	5.958825	10.14.30.165	118.69.123.142	TCP	54	60950 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1830	5.960996	118.69.123.142	10.14.30.165	TCP	66	80 → 60951 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
1831	5.961052	10.14.30.165	118.69.123.142	TCP	54	60951 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0

**Bước 2:** Chọn Statistics > Conversations > IPv4



The image shows the Wireshark interface with the 'Statistics' pane open to the 'Conversations' tab. The 'IPv4' section is selected, showing a single conversation between 10.14.30.165 and 118.69.123.142. The 'Conversation Settings' pane on the left shows 'Name resolution' and 'Show packet details' are unchecked. The main table displays the following data:

Conversation Settings		Ethernet · 1	IPv4 · 1	IPv6	TCP · 2	UDP			
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes
10.14.30.165	118.69.123.142	16	5 kB	16	100.00%	8	2 kB	8	3 kB

- Số lượng gói tin: **16 gói**
- Khối lượng dữ liệu được gửi: **5kB**