

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	Mai Nguyễn Nam Phương (22521164)
Thời gian thực hiện	04/10/2023 – 11/10/2023
Tự chấm điểm	10/10

## TRẢ LỜI CÁC CÂU HỎI

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

**Trả lời:** Tổng thời gian bắt là 9.201211 giây và tổng số gói tin bắt được là 333.

Để xem tổng thời gian bắt của gói tin ta sẽ xem ở mục time của gói cuối cùng

Về tổng số gói sẽ là số packets mà Wireshark đã bắt được hoặc ta có thể xem số thứ tự cuối cùng trước khi ta dừng.

316	8.755050	fe80::f686:5909:750...	ff02:
317	8.755155	192.168.1.11	224.0
318	8.755248	fe80::f686:5909:750...	ff02:
319	8.755272	fe80::f686:5909:750...	ff02:
320	8.755351	192.168.1.11	224.0
321	8.756028	fe80::f686:5909:750...	ff02:
322	8.756050	192.168.1.11	224.0
323	8.758451	fe80::f686:5909:750...	ff02:
324	8.758495	192.168.1.11	224.0
325	8.758828	192.168.1.11	224.0
326	8.758911	fe80::f686:5909:750...	ff02:
327	8.759043	192.168.1.11	224.0
328	8.759134	fe80::f686:5909:750...	ff02:
329	8.759142	fe80::f686:5909:750...	ff02:
330	8.759222	192.168.1.11	224.0
331	9.000695	192.168.1.11	224.0
332	9.000746	fe80::f686:5909:750...	ff02:
333	9.201211	fe80::1	ff02:

|| Packets: 333 · Displayed: 2 (0.6%)

**Câu 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:** Có các giao thức là TCP, HTTP, DNS, UDP...

Chức năng của TCP: Thiết lập kết nối (cho phép 2 máy tính thiết lập như 1), đảm bảo tính toàn vẹn (đảm bảo dữ liệu truyền giữa 2 máy không xảy ra các vấn đề), điều khiển luồng (kiểm soát tốc độ truyền dữ liệu giữa 2 máy để đảm bảo an toàn cho máy chủ), xác nhận và tái gửi, kết thúc kết nối

Chức năng của HTTP: Truyền tải dữ liệu (truyền dữ liệu giữa máy tính máy chủ và trình duyệt web), yêu cầu và phản hồi (hoạt động dựa trên mô hình trình duyệt web gửi yêu

## Lab 1: Làm quen với Wireshark

cầu và máy chủ phản hồi), định dạng văn bản (sử dụng các thông điệp văn bản có định dạng đơn giản và dễ đọc cho việc truyền tải và giao tiếp giữa máy tính máy chủ và trình duyệt), khả năng tương tác (cho phép người dùng tương tác với các trang và thực hiện các hành động trên trang web)

Chức năng của DNS: Chuyển đổi tên miền và địa chỉ IP (giúp máy tính xác định địa chỉ IP tương ứng với một tên miền và ngược lại), phân giải tên miền (hỗ trợ quá trình phân giải tên miền bằng cách truy vấn các máy chủ DNS để tìm địa chỉ IP tương ứng cho một tên miền cụ thể), tạo hệ thống tên miền phân cấp (tổ chức các tên miền vào một cấu trúc phân cấp, giúp quản lý và quản trị tên miền trên Internet một cách hiệu quả)

Chức năng của UDP: Truyền dữ liệu không đáng tin cậy (cho phép gửi và nhận dữ liệu mà không đảm bảo tính toàn vẹn, độ tin cậy hoặc thứ tự. Điều này làm cho UDP nhanh hơn và ít tốn tài nguyên hơn so với giao thức TCP), nhưng cũng có nghĩa rằng dữ liệu có thể bị mất hoặc bị trùng lặp trong quá trình truyền tải.

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

**Trả lời:** Ta sẽ thấy được có 2 gói tin HTTP và ta thấy được tỷ lệ % là 0.6% nhờ mục displayed (đang hiển thị) khi ta nhập từ khóa vào filter

```
tcp.port == 80
```

Packets: 333 · Displayed: 2 (0.6%)

**Câu 4. Có bao nhiêu gói tin HTTP? Tỷ lệ % số gói tin HTTP/Tổng số gói tin?**

**Trả lời:** Chỉ có 1 gói tin HTTP GET nhờ vào cột info khi ta điền filter

No.	Time	Source	Destination	Protocol	Length	Info
151	5.073581	192.168.1.11	128.119.245.12	HTTP	645	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
169	5.320164	128.119.245.12	192.168.1.11	HTTP	293	HTTP/1.1 304 Not Modified

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

**Trả lời:** Dựa trên hình ảnh ta thấy được gói HTTP GET đầu tiên là packet số 151, có trường host là gaia.cs.umass.edu và các thông tin liên quan của gói

## Lab 1: Làm quen với Wireshark

Wireshark · Packet 151 · 22521164-Bai1.pcapng

```
> Frame 151: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface \Device\NPF_{5E4A74AA-D87B-42D2-A405-4FCF035A9348}, id 0
> Ethernet II, Src: Clevo_1c:95:54 (d4:93:90:1c:95:54), Dst: CigShang_a3:52:68 (ec:84:b4:a3:52:68)
> Internet Protocol Version 4, Src: 192.168.1.11, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59660, Dst Port: 80, Seq: 1, Ack: 1, Len: 591
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    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 Edg/117.0.2045.47\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "51-606ddb43d5ba0"\r\n
    If-Modified-Since: Wed, 04 Oct 2023 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

Câu 6. Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?

Trả lời: Dựa vào hình ảnh ta thấy được gói tin phản hồi ở câu 5 là gói tin số 169

Wireshark · Packet 151 · 22521164-Bai1.pcapng

```
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (591 bytes)
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    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 Edg/117.0.2045.47\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "51-606ddb43d5ba0"\r\n
    If-Modified-Since: Wed, 04 Oct 2023 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 169]
```

Câu 7. Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)?

Trả lời: Dựa trên thông tin của gói tin 169 thì tổng thời gian mất sẽ là 0.246583 giây

Wireshark · Packet 169 · 22521164-Bai1.pcapng

```
> Frame 169: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{5E4A74AA-D87B-42D2-A405-4FCF035A9348}, id 0
> Ethernet II, Src: CigShang_a3:52:68 (ec:84:b4:a3:52:68), Dst: Clevo_1c:95:54 (d4:93:90:1c:95:54)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.11
> Transmission Control Protocol, Src Port: 80, Dst Port: 59660, Seq: 1, Ack: 592, Len: 239
▼ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Wed, 04 Oct 2023 10:16:55 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-606ddb43d5ba0"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.246583000 seconds]
    [Request in frame: 151]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

Câu 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?

## Lab 1: Làm quen với Wireshark

**Trả lời:** Dựa trên gợi ý ta có thể thấy được câu trả lời, ví dụ như IP của máy tính sẽ là IP yêu cầu (Source) là 192.168.1.11 và IP của địa chỉ sẽ là IP phản hồi (Destination) là 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
151	5.073581	192.168.1.11	128.119.245.12	HTTP	645	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

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

**Trả lời:** Tương tự như câu 1 ta sẽ có tổng số gói tin bắt được là 435 gói và tổng thời gian là 10.69777 giây

425	9.597047	192.168.1.11	128.119.245.12	TCP	54	[TCP Retransmission] 59705 → 80 [Fin, ACK] Seq=1 Ack=1 Win=0 Len=0
424	9.423689	fe80::1	ff02::1:ffff:ff95	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:ffff:ffff:ffff:ff95 from ec:84:b4:a3:52:68
425	9.443680	fe80::1	ff02::1:ff65:f2e7	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:71c4:a811:6465:f2e7 from ec:84:b4:a3:52:68
426	9.696779	fe80::1	ff02::1:ff36:b26d	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:d30c:2219:3936:b26d from ec:84:b4:a3:52:68
427	9.829422	162.159.135.234	192.168.1.11	TLSv1.2	157	Application Data
428	9.843749	162.159.135.234	192.168.1.11	TLSv1.2	131	Application Data
429	9.843781	192.168.1.11	162.159.135.234	TCP	54	58987 → 443 [ACK] Seq=55 Ack=591 Win=510 Len=0
430	9.901449	fe80::1	2405:4802:a452:4a60::	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:18d0:c426:ba29:3de5 from ec:84:b4:a3:52:68
431	9.901478	2405:4802:a452:4a60::	fe80::1	ICMPv6	86	Neighbor Advertisement 2405:4802:a452:4a60:18d0:c426:ba29:3de5 (sol, ovr) is at d4:93:90:1c:95:54
432	10.242600	fe80::1	ff02::1:ff9b:3204	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:959f:13f2:fd9b:3204 from ec:84:b4:a3:52:68
433	10.423747	fe80::1	ff02::1:ffff:ff95	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:ffff:ffff:ffff:ff95 from ec:84:b4:a3:52:68
434	10.444645	fe80::1	ff02::1:ff65:f2e7	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:71c4:a811:6465:f2e7 from ec:84:b4:a3:52:68
435	10.697757	fe80::1	ff02::1:ff36:b26d	ICMPv6	86	Neighbor Solicitation for 2405:4802:a452:4a60:d30c:2219:3936:b26d from ec:84:b4:a3:52:68

**Câu 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.**

**Trả lời:** Có các giao thức là TCP, HTTP, DNS, UDP...

Chức năng của TCP: Thiết lập kết nối (cho phép 2 máy tính thiết lập như 1), đảm bảo tính toàn vẹn (đảm bảo dữ liệu truyền giữa 2 máy không xảy ra các vấn đề), điều khiển luồng (kiểm soát tốc độ truyền dữ liệu giữa 2 máy để đảm bảo an toàn cho máy chủ), xác nhận và tái gửi, kết thúc kết nối

Chức năng của HTTP: Truyền tải dữ liệu (truyền dữ liệu giữa máy tính máy chủ và trình duyệt web), yêu cầu và phản hồi (hoạt động dựa trên mô hình trình duyệt web gửi yêu cầu và máy chủ phản hồi), định dạng văn bản (sử dụng các thông điệp văn bản có định dạng đơn giản và dễ đọc cho việc truyền tải và giao tiếp giữa máy tính máy chủ và trình duyệt), khả năng tương tác (cho phép người dùng tương tác với các trang và thực hiện các hành động trên trang web)

Chức năng của DNS: Chuyển đổi tên miền và địa chỉ IP (giúp máy tính xác định địa chỉ IP tương ứng với một tên miền và ngược lại), phân giải tên miền (hỗ trợ quá trình phân giải tên miền bằng cách truy vấn các máy chủ DNS để tìm địa chỉ IP tương ứng cho một tên miền cụ thể), tạo hệ thống tên miền phân cấp (tổ chức các tên miền vào một

## Lab 1: Làm quen với Wireshark

cấu trúc phân cấp, giúp quản lý và quản trị tên miền trên Internet một cách hiệu quả)

Chức năng của UDP: Truyền dữ liệu không đáng tin cậy (cho phép gửi và nhận dữ liệu mà không đảm bảo tính toàn vẹn, độ tin cậy hoặc thứ tự. Điều này làm cho UDP nhanh hơn và ít tốn tài nguyên hơn so với giao thức TCP), nhưng cũng có nghĩa rằng dữ liệu có thể bị mất hoặc bị trùng lặp trong quá trình truyền tải.

**Câu 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:

No.	Time	Source	Destination	Protocol	Length	Info
95	4.860010	192.168.1.11	118.69.123.142	HTTP	649	GET / HTTP/1.1
99	4.886691	118.69.123.142	192.168.1.11	HTTP	625	HTTP/1.1 304 Not Modified
119	4.937317	192.168.1.11	118.69.123.142	HTTP	532	GET /select2/ajax/get_settings HTTP/1.1
161	5.032742	118.69.123.142	192.168.1.11	HTTP/1.1	1430	200 OK , JavaScript Object Notation (application/json)

Dựa trên hình ảnh trên ta sẽ thấy địa chỉ IP của trang web đã chọn ở mục Destination của gói 119 hoặc gói 95 là 118.69.123.142

**Câu 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:

Ethernet · 1		IPv4 · 1		IPv6	TCP · 8		UDP						
Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.11	118.69.123.142	44	5 kB	44	100.00%	38	3 kB	6	2 kB	4.854406	4.5426	5545 bits/s	4076 bits/s

Dựa trên cách 2 ta có:

Địa chỉ máy tính: 192.158.1.11 và địa chỉ trang web: 118.69.123.142

Vậy thì số lượng gói tin được trao đổi là 44 gói và khối lượng dữ liệu được gửi là 5 kB