

BÁO CÁO THỰC HÀNH LAP01

Môn học: Nhập môn mạng máy tính

Lớp: IT005.M17.1

Họ tên: Nguyễn Mạnh Đức

MSSV: 20521196

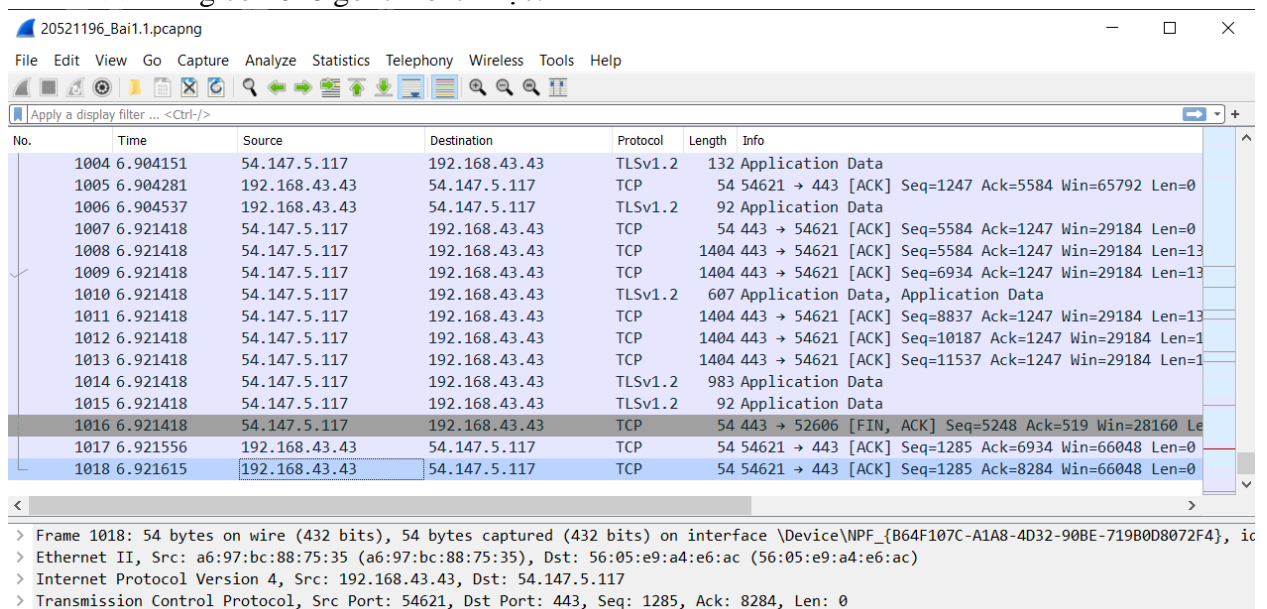
Phân tích kết quả bắt gói tin từ Wireshark

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

1.1 Ở trang web gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

>> Tổng thời gian bắt gói tin trong từng trang web: 6.921615s.

>> Tổng có 1018 gói tin bắt được.



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|----------|---------------|---------------|----------|--------|---|
| 1004 | 6.904151 | 54.147.5.117 | 192.168.43.43 | TLSv1.2 | 132 | Application Data |
| 1005 | 6.904281 | 192.168.43.43 | 54.147.5.117 | TCP | 54 | 54621 → 443 [ACK] Seq=1247 Ack=5584 Win=65792 Len=0 |
| 1006 | 6.904537 | 192.168.43.43 | 54.147.5.117 | TLSv1.2 | 92 | Application Data |
| 1007 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 54 | 443 → 54621 [ACK] Seq=5584 Ack=1247 Win=29184 Len=0 |
| 1008 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 1404 | 443 → 54621 [ACK] Seq=5584 Ack=1247 Win=29184 Len=13 |
| 1009 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 1404 | 443 → 54621 [ACK] Seq=6934 Ack=1247 Win=29184 Len=13 |
| 1010 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TLSv1.2 | 607 | Application Data, Application Data |
| 1011 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 1404 | 443 → 54621 [ACK] Seq=8837 Ack=1247 Win=29184 Len=13 |
| 1012 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 1404 | 443 → 54621 [ACK] Seq=10187 Ack=1247 Win=29184 Len=1 |
| 1013 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 1404 | 443 → 54621 [ACK] Seq=11537 Ack=1247 Win=29184 Len=1 |
| 1014 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TLSv1.2 | 983 | Application Data |
| 1015 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TLSv1.2 | 92 | Application Data |
| 1016 | 6.921418 | 54.147.5.117 | 192.168.43.43 | TCP | 54 | 443 → 52606 [FIN, ACK] Seq=5248 Ack=519 Win=28160 Len=0 |
| 1017 | 6.921556 | 192.168.43.43 | 54.147.5.117 | TCP | 54 | 54621 → 443 [ACK] Seq=1285 Ack=6934 Win=66048 Len=0 |
| 1018 | 6.921615 | 192.168.43.43 | 54.147.5.117 | TCP | 54 | 54621 → 443 [ACK] Seq=1285 Ack=8284 Win=66048 Len=0 |

> Frame 1018: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B64F107C-A1A8-4D32-90BE-719B0D8072F4}, ic
> Ethernet II, Src: a6:97:bc:88:75:35 (a6:97:bc:88:75:35), Dst: 56:05:e9:a4:e6:ac (56:05:e9:a4:e6:ac)
> Internet Protocol Version 4, Src: 192.168.43.43, Dst: 54.147.5.117
> Transmission Control Protocol, Src Port: 54621, Dst Port: 443, Seq: 1285, Ack: 8284, Len: 0

1.2 Ở trang web <https://www.uit.edu.vn>

>> Tổng thời gian bắt gói tin trong từng trang web: 11.171915s .

>> Tổng có 2591 gói tin bắt được.

20521196_Bai1.2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|--------------|---------------|----------|--------|----------------------|
| 2577 | 11.098013 | 52.112.45.15 | 192.168.43.43 | UDP | 173 | 3480 → 50013 Len=131 |
| 2578 | 11.098013 | 52.112.45.15 | 192.168.43.43 | UDP | 120 | 3481 → 50040 Len=78 |
| 2579 | 11.098013 | 52.112.45.15 | 192.168.43.43 | UDP | 181 | 3480 → 50013 Len=139 |
| 2580 | 11.098192 | 52.112.45.15 | 192.168.43.43 | UDP | 968 | 3481 → 50040 Len=926 |
| 2581 | 11.098192 | 52.112.45.15 | 192.168.43.43 | UDP | 968 | 3481 → 50040 Len=926 |
| 2582 | 11.107662 | 52.112.45.15 | 192.168.43.43 | UDP | 172 | 3480 → 50013 Len=130 |
| 2583 | 11.128850 | 52.112.45.15 | 192.168.43.43 | UDP | 152 | 3480 → 50013 Len=110 |
| 2584 | 11.147751 | 52.112.45.15 | 192.168.43.43 | UDP | 120 | 3481 → 50040 Len=78 |
| 2585 | 11.147751 | 52.112.45.15 | 192.168.43.43 | UDP | 901 | 3481 → 50040 Len=859 |
| 2586 | 11.147751 | 52.112.45.15 | 192.168.43.43 | UDP | 901 | 3481 → 50040 Len=859 |
| 2587 | 11.156510 | 52.112.45.15 | 192.168.43.43 | UDP | 901 | 3481 → 50040 Len=859 |
| 2588 | 11.156510 | 52.112.45.15 | 192.168.43.43 | UDP | 168 | 3480 → 50013 Len=126 |
| 2589 | 11.156510 | 52.112.45.15 | 192.168.43.43 | UDP | 917 | 3481 → 50040 Len=875 |
| 2590 | 11.156510 | 52.112.45.15 | 192.168.43.43 | UDP | 917 | 3481 → 50040 Len=875 |
| 2591 | 11.171915 | 52.112.45.15 | 192.168.43.43 | UDP | 178 | 3480 → 50013 Len=136 |

< >

> Frame 1: 1400 bytes on wire (11200 bits), 1400 bytes captured (11200 bits) on interface \Device\NPF_{B64F107C-A1A8-4D32-90...}

> Ethernet II, Src: a6:97:bc:88:75:35 (a6:97:bc:88:75:35), Dst: 56:05:e9:a4:e6:ac (56:05:e9:a4:e6:ac)

> Internet Protocol Version 4, Src: 192.168.43.43, Dst: 52.178.17.2

> Transmission Control Protocol, Src Port: 50105, Dst Port: 443, Seq: 1, Ack: 1, Len: 1346

> Transport Layer Security

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.

>>5 giao thức khác nhau xuất hiện trong cột giao thức:TCP, UDP, DNS, QUIC, STUN

Chức năng chính:

TCP: giúp máy chủ được nối mạng kết nối được với nhau, qua đó có thể trao đổi dữ liệu hoặc các gói tin. Đảm bảo chuyển giao dữ liệu tới nơi 1 cách đáng tin cậy và đúng thứ tự.

UDP: gửi những dữ liệu ngắn gọi là datagram tới máy khác, nhanh và hiệu quả đối với các mục tiêu có kích thước nhỏ.

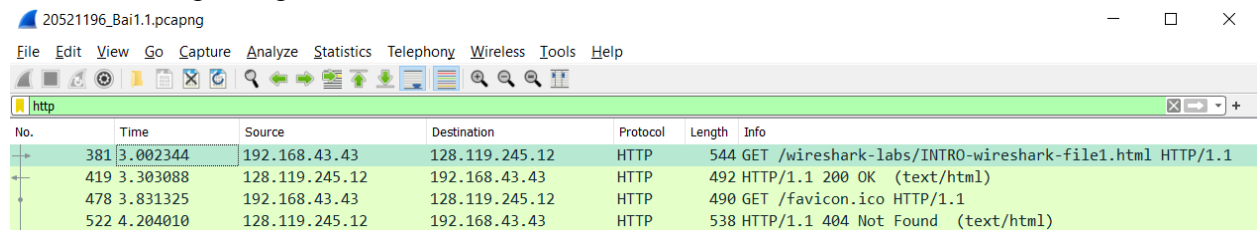
DNS: dịch tên miền thành một địa chỉ IP hoặc dịch 1 địa chỉ IP thành tên miền.

QUIC: nhằm thay thế TCP, tăng tốc các giao thức mạng nhằm giảm thiểu thời gian phản ứng của trang web.

STUN: cho phép các máy khách tìm ra địa chỉ công khai của mình

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 website đã thử nghiệm.

>> Mất khoảng thời gian : $3.303088 - 3.002344 = 0.300854s$.



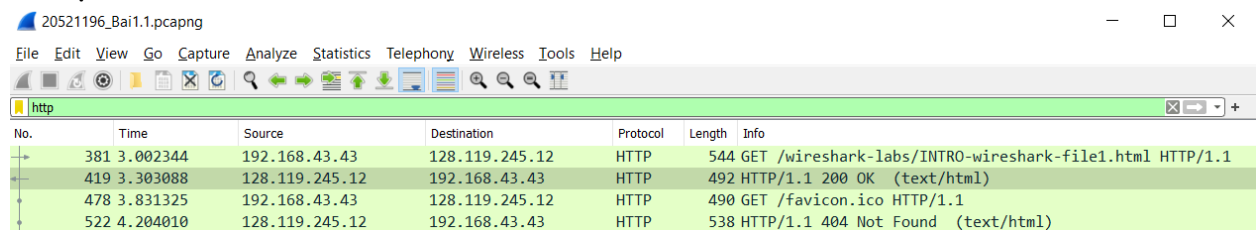
20521196_Bai1.1.pcapng

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 381 | 3.002344 | 192.168.43.43 | 128.119.245.12 | HTTP | 544 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 419 | 3.303088 | 128.119.245.12 | 192.168.43.43 | HTTP | 492 | HTTP/1.1 200 OK (text/html) |
| 478 | 3.831325 | 192.168.43.43 | 128.119.245.12 | HTTP | 490 | GET /favicon.ico HTTP/1.1 |
| 522 | 4.204010 | 128.119.245.12 | 192.168.43.43 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

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.

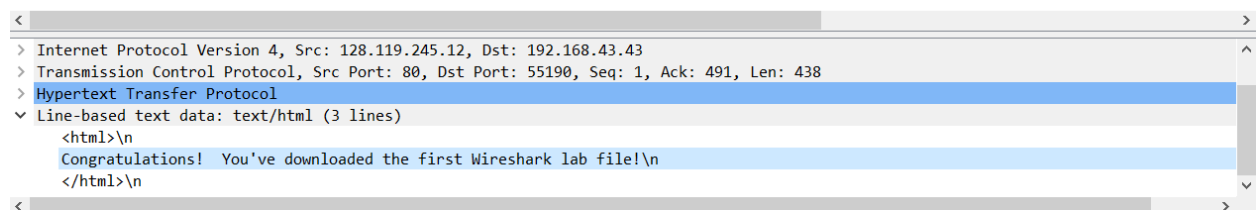
>> Nội dung hiển thị web gaia.cs.umass.edu xuất hiện trong gói tin HTTP bắt được.

>> Vị trí:



20521196_Bai1.1.pcapng

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 381 | 3.002344 | 192.168.43.43 | 128.119.245.12 | HTTP | 544 | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 |
| 419 | 3.303088 | 128.119.245.12 | 192.168.43.43 | HTTP | 492 | HTTP/1.1 200 OK (text/html) |
| 478 | 3.831325 | 192.168.43.43 | 128.119.245.12 | HTTP | 490 | GET /favicon.ico HTTP/1.1 |
| 522 | 4.204010 | 128.119.245.12 | 192.168.43.43 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |



< >

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.43

> Transmission Control Protocol, Src Port: 80, Dst Port: 55190, Seq: 1, Ack: 491, Len: 438

> Hypertext Transfer Protocol

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

<html>\n

Congratulations! You've downloaded the first Wireshark lab file!\n

</html>\n

< >

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

>> Địa chỉ IP của gaia.umass.edu là : 128.119.245.12

>> Địa chỉ IP của máy đang dùng là: 192.168.43.43

20521196_Bai1.1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|-------------|
| 381 | 3.002344 | 192.168.43.43 | 128.119.245.12 | HTTP | 544 | GET /wiresh |
| 419 | 3.303088 | 128.119.245.12 | 192.168.43.43 | HTTP | 492 | HTTP/1.1 20 |
| 478 | 3.831325 | 192.168.43.43 | 128.119.245.12 | HTTP | 490 | GET /favico |
| 522 | 4.204010 | 128.119.245.12 | 192.168.43.43 | HTTP | 538 | HTTP/1.1 40 |

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.
1. Khi truy cập trang web, trình duyệt sẽ gọi tới máy chủ DNS để biên dịch URL trang web thành một địa chỉ IP, mỗi trang web có địa chỉ IP riêng biệt. Khi tìm thấy địa chỉ IP của trang web chúng ta đang vào, địa chỉ IP đó sẽ được trả về cho trình duyệt.
 2. Trình duyệt sẽ sử dụng địa chỉ IP đó để yêu cầu HTTP gọi tới Server lưu trữ trang web đó. Nó sẽ kết nối cổng số 80 trên Server bằng giao thức TCP/IP.
 3. Nếu Server chấp nhận thì sẽ gửi lại thông báo "200 OK". Và sau đó trình duyệt sẽ truy xuất mã HTML của trang web cụ thể được yêu cầu.
 4. Khi trình duyệt của bạn nhận được mã HTML đó từ Server thì nó sẽ hiển thị ra cửa sổ của trình duyệt một trang web hoàn chỉnh.
 5. Khi chúng ta đóng trình duyệt thì quá trình kết nối với Server sẽ kết thúc.