BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng máy tính

Buổi báo cáo: Lab 01

Tên chủ đề: Làm quen với Wireshark

GVHD: Phan Trung Phát

Ngày thực hiện: 22/09/2022

Ngày nộp báo cáo: 05/10/2022

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: IT005.N11.KHTN.1

STT	Họ và tên	MSSV	Email
1	Trương Thanh Minh	21520064	21520064@gm.uit.edu.vn

2. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	2 tuần
Link Video thực hiện *(nếu có)*	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất …	
Điểm tự đánh giá	9.5

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

I. Mở đầu về mạng máy tính

Mục tiêu và kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính:

- Nắm được kiến thức tổng quan về mạng.
- Biết được kiến thức cơ bản về các tầng mạng, các giao thức mạng.
- Vận dụng kiến thức đã học để biết được cách thực hiện một số cuộc tấn công và tránh khỏi các cuộc tấn công mạng.

II. Làm quen với Wireshark và thửu nghiệm bắt gói tin trong mạng

1) Tổng thời gian bắt gói tin trong từng trang web thử nghiệm và tổng số gói tin bắt được

- **Ở website thứ nhất (gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html):**

ip.addr == 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
20	0.227256	10.0.129.0	128.119.245.12	TCP	66	56982 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
45	0.445738	10.0.129.0	128.119.245.12	TCP	66	56986 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
46	0.445978	10.0.129.0	128.119.245.12	TCP	66	56987 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
65	0.503509	128.119.245.12	10.0.129.0	TCP	66	80 → 56982 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
66	0.503734	10.0.129.0	128.119.245.12	TCP	54	56982 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
67	0.504420	10.0.129.0	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
96	0.709861	128.119.245.12	10.0.129.0	TCP	66	80 → 56986 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
97	0.710247	10.0.129.0	128.119.245.12	TCP	54	56986 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
98	0.715020	128.119.245.12	10.0.129.0	TCP	66	80 → 56987 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
99	0.715241	10.0.129.0	128.119.245.12	TCP	54	56987 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
103	0.784427	128.119.245.12	10.0.129.0	TCP	60	80 → 56982 [ACK] Seq=1 Ack=481 Win=30336 Len=0
104	0.785384	128.119.245.12	10.0.129.0	HTTP	492	HTTP/1.1 200 OK (text/html)
106	0.832542	10.0.129.0	128.119.245.12	TCP	54	56982 → 80 [ACK] Seq=481 Ack=439 Win=131840 Len=0
110	1.071988	10.0.129.0	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
112	1.378824	128.119.245.12	10.0.129.0	HTTP	538	HTTP/1.1 404 Not Found (text/html)
114	1.423210	10.0.129.0	128.119.245.12	TCP	54	56982 → 80 [ACK] Seq=907 Ack=923 Win=131328 Len=0

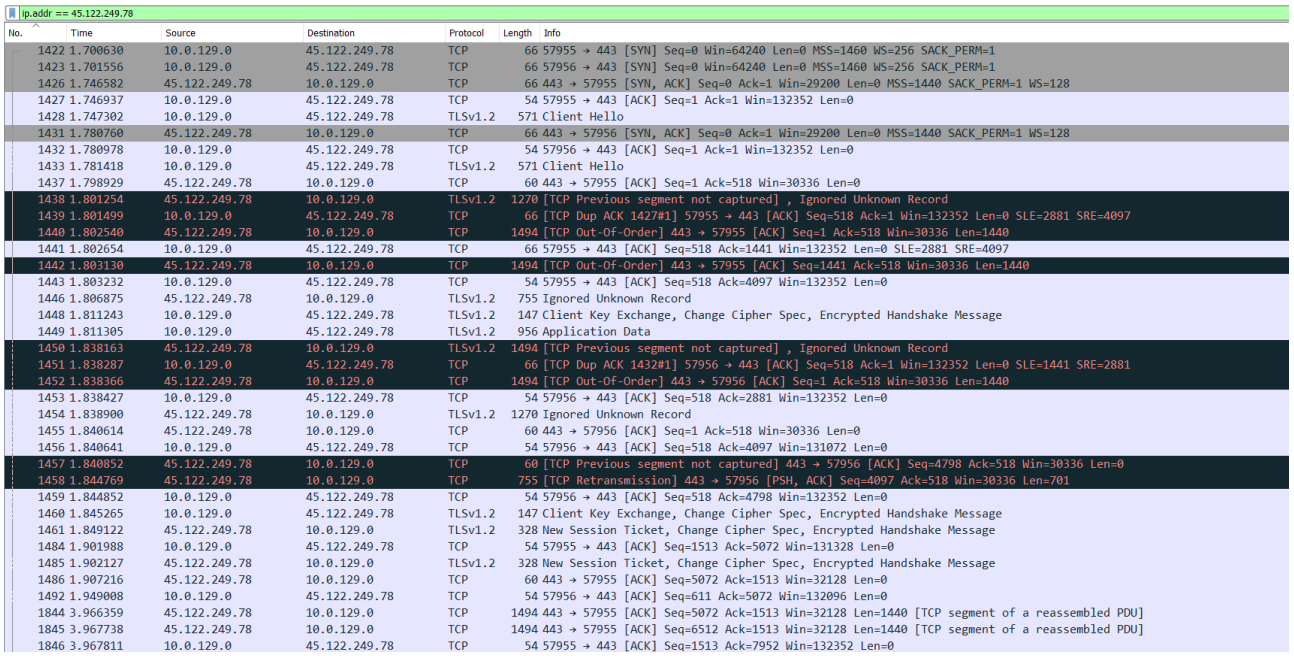
Hình 1: Bắt gói tin ở trang web đầu tiên

- Đầu tiên, ta lọc các gói tin vừa bắt được với địa chỉ IP của web (128.119.245.12)

  Thời gian thử nghiệm: t = 1.423210 – 0.227256 = 1.195954(s).

- Số gói tin bắt được là 16 (gói tin).

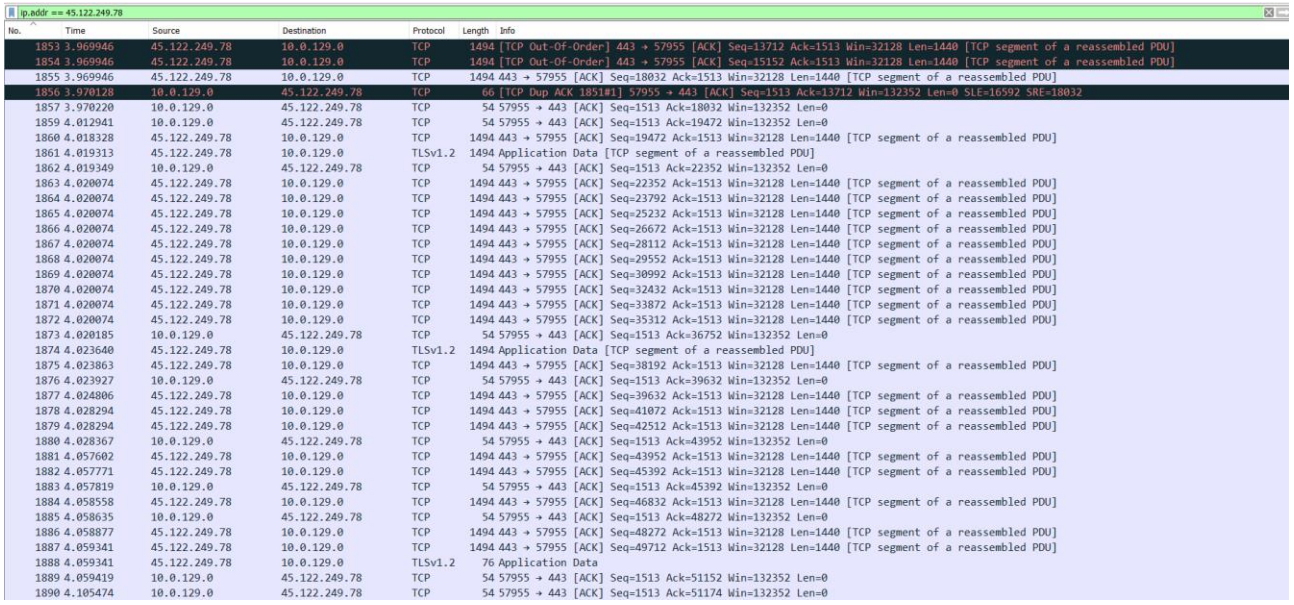
- **Ở website thứ hai (Cổng thông tin đào tạo | Trường Đại Học Công Nghệ Thông Tin (uit.edu.vn)):**



ip.addr == 45.122.249.78

No.	Time	Source	Destination	Protocol	Length	Info
1422	1.700630	10.0.129.0	45.122.249.78	TCP	66	57955 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1423	1.701556	10.0.129.0	45.122.249.78	TCP	66	57956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1426	1.746582	45.122.249.78	10.0.129.0	TCP	66	443 → 57955 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
1427	1.746937	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
1428	1.747302	10.0.129.0	45.122.249.78	TLSv1.2	571	Client Hello
1431	1.780760	45.122.249.78	10.0.129.0	TCP	66	443 → 57956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
1432	1.780978	10.0.129.0	45.122.249.78	TCP	54	57956 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
1433	1.781418	10.0.129.0	45.122.249.78	TLSv1.2	571	Client Hello
1437	1.798929	45.122.249.78	10.0.129.0	TCP	60	443 → 57955 [ACK] Seq=1 Ack=518 Win=30336 Len=0
1438	1.801254	45.122.249.78	10.0.129.0	TLSv1.2	1270	[TCP Previous segment not captured] , Ignored Unknown Record
1439	1.801499	10.0.129.0	45.122.249.78	TCP	66	[TCP Dup ACK 1427#1] 57955 → 443 [ACK] Seq=518 Ack=1 Win=132352 Len=0 SLE=2881 SRE=4097
1440	1.802540	45.122.249.78	10.0.129.0	TCP	1494	[TCP Out-Of-Order] 443 → 57955 [ACK] Seq=1 Ack=518 Win=30336 Len=1440
1441	1.802654	10.0.129.0	45.122.249.78	TCP	66	57955 → 443 [ACK] Seq=518 Ack=1441 Win=132352 Len=0 SLE=2881 SRE=4097
1442	1.803130	45.122.249.78	10.0.129.0	TCP	1494	[TCP Out-Of-Order] 443 → 57955 [ACK] Seq=1441 Ack=518 Win=30336 Len=1440
1443	1.803232	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=518 Ack=4097 Win=132352 Len=0
1446	1.806875	45.122.249.78	10.0.129.0	TLSv1.2	755	Ignored Unknown Record
1448	1.811243	10.0.129.0	45.122.249.78	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1449	1.811305	10.0.129.0	45.122.249.78	TLSv1.2	956	Application Data
1450	1.838163	45.122.249.78	10.0.129.0	TLSv1.2	1494	[TCP Previous segment not captured] , Ignored Unknown Record
1451	1.838287	10.0.129.0	45.122.249.78	TCP	66	[TCP Dup ACK 1432#1] 57956 → 443 [ACK] Seq=518 Ack=1 Win=132352 Len=0 SLE=1441 SRE=2881
1452	1.838366	45.122.249.78	10.0.129.0	TCP	1494	[TCP Out-Of-Order] 443 → 57956 [ACK] Seq=1 Ack=518 Win=30336 Len=1440
1453	1.838427	10.0.129.0	45.122.249.78	TCP	54	57956 → 443 [ACK] Seq=518 Ack=2881 Win=132352 Len=0
1454	1.838900	45.122.249.78	10.0.129.0	TLSv1.2	1270	Ignored Unknown Record
1455	1.840614	45.122.249.78	10.0.129.0	TCP	60	443 → 57956 [ACK] Seq=1 Ack=518 Win=30336 Len=0
1456	1.840641	10.0.129.0	45.122.249.78	TCP	54	57956 → 443 [ACK] Seq=518 Ack=4097 Win=131072 Len=0
1457	1.840852	45.122.249.78	10.0.129.0	TCP	60	[TCP Previous segment not captured] 443 → 57956 [ACK] Seq=4798 Ack=518 Win=30336 Len=0
1458	1.844769	45.122.249.78	10.0.129.0	TCP	755	[TCP Retransmission] 443 → 57956 [PSH, ACK] Seq=4097 Ack=518 Win=30336 Len=701
1459	1.844852	10.0.129.0	45.122.249.78	TCP	54	57956 → 443 [ACK] Seq=518 Ack=4798 Win=132352 Len=0
1460	1.845265	10.0.129.0	45.122.249.78	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1461	1.849122	45.122.249.78	10.0.129.0	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1484	1.901988	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=5072 Win=131328 Len=0
1485	1.902127	45.122.249.78	10.0.129.0	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1486	1.907216	45.122.249.78	10.0.129.0	TCP	60	443 → 57955 [ACK] Seq=5072 Ack=1513 Win=32128 Len=0
1492	1.949008	10.0.129.0	45.122.249.78	TCP	54	57956 → 443 [ACK] Seq=611 Ack=5072 Win=132096 Len=0
1844	3.966359	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=5072 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1845	3.967738	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=6512 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1846	3.967811	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=7952 Win=132352 Len=0

Hình 2: Những gói tin đầu tin bắt được ở web thứ hai



ip.addr == 45.122.249.78

No.	Time	Source	Destination	Protocol	Length	Info
1853	3.969946	45.122.249.78	10.0.129.0	TCP	1494	[TCP Out-Of-Order] 443 → 57955 [ACK] Seq=13712 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1854	3.969946	45.122.249.78	10.0.129.0	TCP	1494	[TCP Out-Of-Order] 443 → 57955 [ACK] Seq=15152 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1855	3.969946	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=18032 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1856	3.970128	10.0.129.0	45.122.249.78	TCP	66	[TCP Dup ACK 1851#1] 57955 → 443 [ACK] Seq=1513 Ack=13712 Win=132352 Len=0 SLE=16592 SRE=18032
1857	3.970220	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=18032 Win=132352 Len=0
1859	4.012941	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=19472 Win=132352 Len=0
1860	4.018328	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=19472 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1861	4.019313	45.122.249.78	10.0.129.0	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
1862	4.019349	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=22352 Win=132352 Len=0
1863	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=22352 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1864	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=23792 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1865	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=25232 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1866	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=26672 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1867	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=28112 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1868	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=29552 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1869	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=30992 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1870	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=32432 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1871	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=33872 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1872	4.020074	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=35312 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1873	4.020185	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=36752 Win=132352 Len=0
1874	4.023640	45.122.249.78	10.0.129.0	TLSv1.2	1494	Application Data [TCP segment of a reassembled PDU]
1875	4.023863	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=38192 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1876	4.023927	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=39632 Win=132352 Len=0
1877	4.024806	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=39632 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1878	4.028294	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=41072 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1879	4.028294	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=42512 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1880	4.028367	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=43952 Win=132352 Len=0
1881	4.057602	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=43952 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1882	4.057771	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=45392 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1883	4.057819	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=45392 Win=132352 Len=0
1884	4.058558	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=46832 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1885	4.058635	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=48272 Win=132352 Len=0
1886	4.058877	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=48272 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1887	4.059341	45.122.249.78	10.0.129.0	TCP	1494	443 → 57955 [ACK] Seq=49712 Ack=1513 Win=32128 Len=1440 [TCP segment of a reassembled PDU]
1888	4.059341	45.122.249.78	10.0.129.0	TLSv1.2	76	Application Data
1889	4.059419	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=51152 Win=132352 Len=0
1890	4.105474	10.0.129.0	45.122.249.78	TCP	54	57955 → 443 [ACK] Seq=1513 Ack=51174 Win=132352 Len=0

Hình 3: Những gói tin cuối cùng ở web thứ 2

- Tương tự ở website thứ nhất, ở bước đầu tiên, ta cũng lọc lại các gói tin bắt được bằng IP của website đó (45.122.249.78)

  Thời gian thử nghiệm là: t = 4.105474 – 1.700630 = 2.404844 (s).

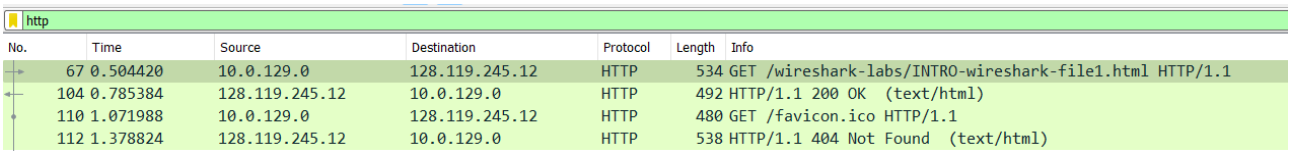
- Số gói tin bắt được là 80 (gói tin).

2) 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol)

- TCP (Transmission Control Protocol): Giao thức này có nhiệm vụ chia nhỏ dữ liệu ra thành các gói để truyền dữ liệu đi. Thiết lập các kết nối giữa các máy tính đảm bảo việc truyền dữ liệu thành công.
- HTTP (HyperText Transfer Protocol): Cho phép trao đổi thông tin (chủ yếu ở dạng siêu văn bản) qua Internet.
- ARP (Address Resolution Protocol): Là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network.
- SSDP (Simple Service Discovey Protocol): Là một giao thức được dùng để phát hiện dịch vụ mạng mà không cần tới sự trợ giúp của cấu hình dựa vào máy chủ như Dynamic Host Configuration Protocol (DHCP) và Domain Name System (DNS) và cấu hình mạng host tĩnh.
- DNS (Domain Name System): Là hệ thống phân giải tên miền. Nó cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên Internet. Nhờ giao thức này nên có thể chuyển đổi tên miền thành địa chỉ IP.

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.

- **Ở website thứ nhất:**



Hình 4: Các gói tin bắt được ở trang web thứ nhất sau khi dùng bộ lọc HTTP

Đầu tiên, ta dùng filter để lọc ra những lệnh có Protocol là HTTP. Khi lọc ra, thì ta thấy có 4 gói tin có có Protocol là HTTP.

Ta thấy rằng, gói tin HTTP GET đầu tiên được gửi vào lúc t1 = 0.504420.

Và gói tin HTTP 200 OK đầu tiên được nhận vào lúc t2 = 0.785384.

⇨ Thời gian từ khi gói tin HTTP GET đầu tiên đến HTTP 200 OK là t = t2 – t1 = 0.785384 - 0.504420 = 0.280964 (s).

? Vì sao gói tin trả về HTTP -200 OK chỉ xuất hiện khi bắt gói tin ở lần truy cập đầu tiên trên trình duyệt.

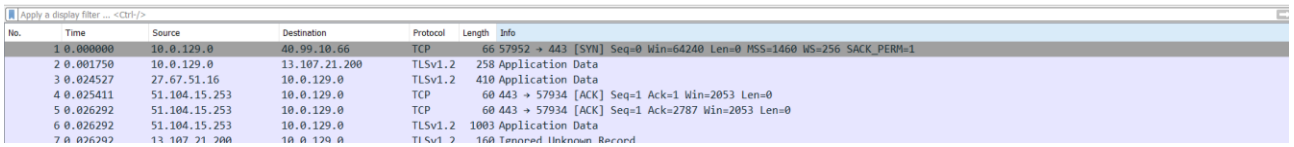
Ta thấy rằng, ở lần đầu tiên, gói tin trả về HTTP -200 OK chỉ xuất hiện khi bắt gói tin ở lần truy cập đầu tiên trên trình duyệt, còn những lần sau, nó trả về cho ta là HTTP -304 NOT MODIFIED.

Về lỗi HTTP 304, nó cho ta biết sự cố giao tiếp giữa trình duyệt của người dùng và máy chủ. Thông báo này cho trình duyệt biết rằng các tài nguyên được lưu trong bộ nhớ cache của trình duyệt đã không được sửa đổi kể từ lần truyền trước đó. Vì vậy, không cần phải truyền lại tài nguyên được yêu cầu cho máy khách một lần nữa. Do đó, trình duyệt hiển thị phiên bản được lưu trong bộ nhớ cahe của trang web.

Còn HTTP 200, nó cho ta biết là yêu cầu ta gửi lên đã được thành công.

Tóm lại, HTTP 200 chỉ xuất hiện ở lần đầu tiên mà request của ta gửi lên thành công. Tuy nhiên, sau đó, các tài nguyên được lưu trong bộ nhớ cache của trình duyệt đã không đổi kể từ lần trước đó (lần mà request của ta gửi lên trình duyệt thành công). Do đó, trình duyệt báo cho ta sự cố giao tiếp giữa trình duyệt của người dùng và máy chủ. Vì thế, nó gửi về cho ta HTTP 304 NOT MODIFIED.

- **Ở website thứ hai:**

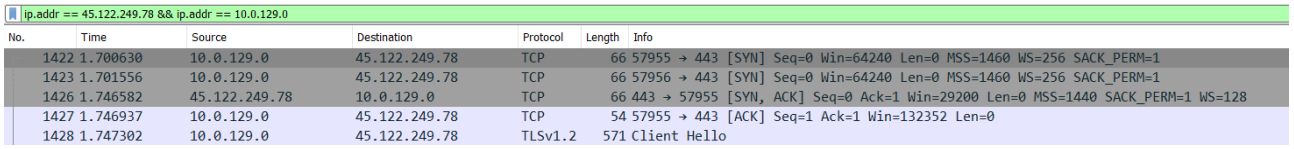


Hình 5: Những gói tin đầu tiên ta bắt được ở website thứ 2

Vì đây là trang web sử dụng giao thức https, do đó, ta không thể sử dụng bộ lọc http như ở trên. Thế nên ta phải sử dụng quy trình bắt tay 3 bước (3 way – handshake). Quy trình đó được mô tả như sau:

- **Bước 1 (SYN):** Trong bước đầu tiên, client thiết lập kết nối với máy chủ. Nó gửi một phân đoạn với SYN và thông báo cho máy chủ về việc client sẽ bắt đầu giao tiếp và với số thứ tự của nó. Client sẽ gửi một message yêu cầu kết nối với Server.
- **Bước 2 (SYN + ACK):** Trong bước này, máy chủ trả lời yêu cầu của client với bộ tín hiệu SYN-ACK (nếu đồng ý kết nối). Trong đó, ACK biểu thị phản hồi của phân đoạn được nhận và SYN biểu thị số thứ tự mà nó có thể bắt đầu với phân đoạn.
- **Bước 3 (ACK):** Ở bước cuối cùng, Client nhận phản hồi của máy chủ và thông báo tới máy chủ bằng một đoạn tin nhắn với ACK và thông báo với máy chủ là đã nhận được phản hồi. Sau đó, cả 2 thiết lập một kết nối đáng tin cậy mà chúng sẽ bắt đầu truyền dữ liệu.

Đầu tiên, ta dùng filter lọc bằng địa chỉ IP của website đó, và IP của máy mình. Cụ thể:



Hình 6: Những gói tin đầu tiên bắt được ở website thứ hai

- ip.addr == 45.122.249.78: Chính là địa chỉ IP của website ta đang bắt gói tin.
- ip.addr == 10.0.129.0: Là địa chỉ IP của máy tính của em đang sử dụng lúc thực hiện bắt gói tin.

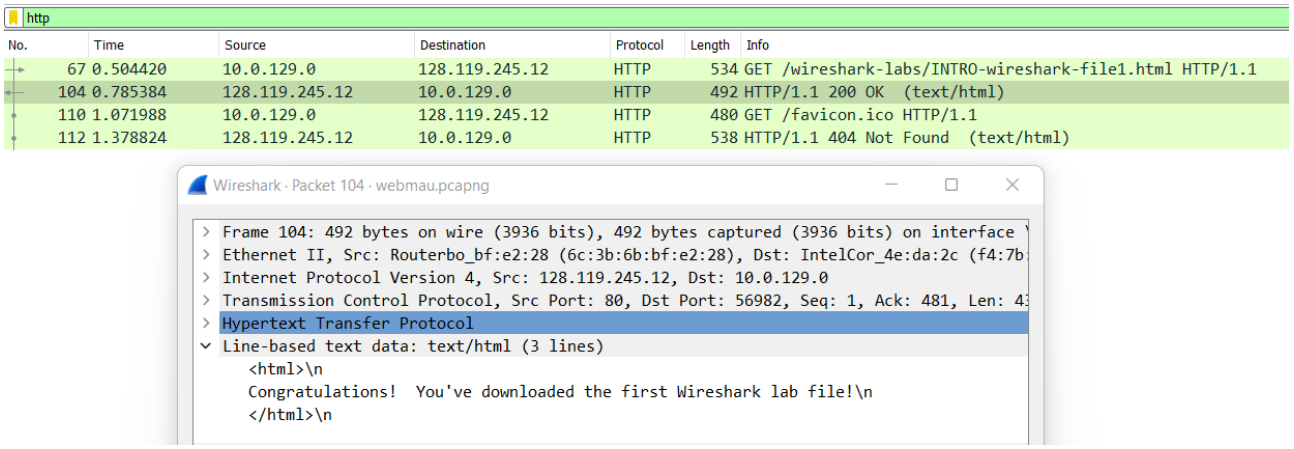
Từ hình trên, ta thấy:

- Gói tin [SYN] đầu tiên mà máy ta (Client) gửi yêu cầu tới máy chủ là gói tin No. 1422 ở thời điểm t1 = 1.700630.
- Gói tin [SYN, ACK] đầu tiên bắt được mà máy chủ phản hồi tới máy ta (Client) là gói tin No. 1426 tại thời điểm t2 = 1.746582.
- Gói tin [ACK] sau đó mà máy ta phản hồi lại cho máy chủ là đã nhận được thông báo là gói tin No. 1427 ở thời điểm t3 = 1.746937.

Tuy nhiên, để tính thời gian mà từ lúc Client gửi yêu cầu đầu tiên đến lúc máy chủ phản hồi thì ta chỉ cần sử dụng t1 và t2 để thực hiện tính toán.

⇨ Thời gian từ khi gói tin được gửi đi đầu tiên đến gói tin phản hồi đầu tiên là t = t2 – t1 = 1.746582 – 1.700630 = 0.045952 (s).

4) Nội dung hiển thị trên trang web gaia.cs.umass.edu có nằm trong 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.



Hình 7: Chi tiết của gói tin 200 OK

Trong các gói tin HTTP ta bắt được ở trang web đầu tiên, ta mở gói tin mà nó là HTTP 200 OK. Trong đó, ta thấy rằng nó có xuất hiện nội dung như sau: “Congratulations! You’re downloaded the first Wireshark lab file!”

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:

  Từ ảnh trên, ta thấy rằng, địa chỉ IP của trang trên là: 128.119.245.12

```
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.129.0
```

Hình 8: Địa chỉ IP của trang web đầu tiên

- Địa chỉ IP của trang web daa.uit.edu.vn:

  Để tìm địa chỉ của một trang web, ta sử dụng câu lệnh sau:

```
C:\Users\ACER>ping daa.uit.edu.vn

Pinging daa.uit.edu.vn [45.122.249.78] with 32 bytes of data:
Reply from 45.122.249.78: bytes=32 time=10ms TTL=56
Reply from 45.122.249.78: bytes=32 time=19ms TTL=56
Reply from 45.122.249.78: bytes=32 time=17ms TTL=56
Reply from 45.122.249.78: bytes=32 time=4ms TTL=56

Ping statistics for 45.122.249.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 19ms, Average = 12ms
```

Hình 9: Cách tìm địa chỉ IP của trang web thứ hai

  Sau khi gọi câu lệnh đó, ta dễ dàng biết được địa chỉ IP của trang daa.uit.edu.vn là 45.122.249.78

- Địa chỉ IP của máy tính đang sử dụng:

http

No.	Time	Source	Destination	Protocol	Length	Info
67	0.504420	10.0.129.0	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
104	0.785384	128.119.245.12	10.0.129.0	HTTP	492	HTTP/1.1 200 OK (text/html)
110	1.071988	10.0.129.0	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
112	1.378824	128.119.245.12	10.0.129.0	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Hình 10: Hình ảnh các gói tin bắt được ở web thứ 1 sau khi dùng bộ lọc http

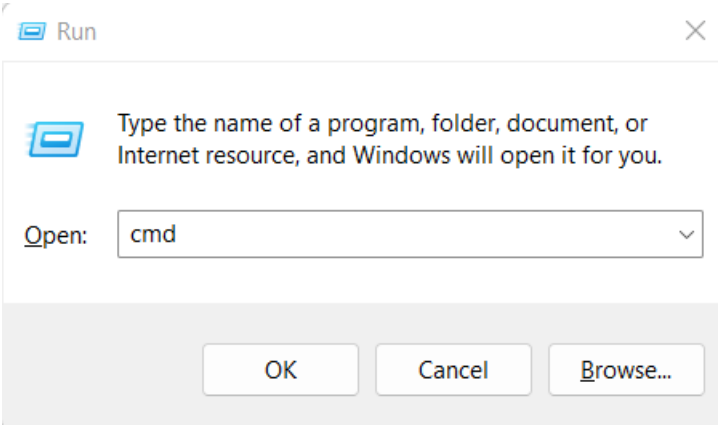
  Đây là các gói tin sau khi ta sử dụng bộ lọc http, ta thấy rằng, ở ở trên cùng, là gói mà ta gửi request từ máy ta lên server. Do đó, địa chỉ của máy ta lúc này là **Source**, hay nói cách khác, **địa chỉ IP** của **máy tính** ta đang dùng là **10.0.129.0.**

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 truy cập vào một trang web, trình duyệt sẽ gọi tới máy chủ DNS để biên dịch URL của trang web thành địa chỉ IP (mỗi trang web sẽ có một địa chỉ IP riêng biệt). Khi tìm thấy địa chỉ IP, địa chỉ IP đó sẽ được trả về cho trình duyệt.
- Sau đó, trình duyệt sẽ sử dụng địa chỉ IP vừa được trả về để yêu cầu HTTP gọi tới Server lưu trữ trang web đó.
- Nếu Server chấp nhận thì sẽ gửi lại thông báo "200 OK" (đối với trang web thứ nhất ở trên). Sau đó, trình duyệt sẽ truy xuất mã HTML của trang web được yêu cầu.
- Khi trình duyệt nhận được mã HTML đó từ Server thì nó sẽ hiển thị ra cửa sổ của trình duyệt một trang web hoàn chỉnh.
- Khi đóng trình duyệt thì quá trình kết nối với Server sẽ kết thúc.

***** Mở rộng: Theo bạn, địa chỉ IP dùng để làm gì và có cách nào khác để xem địa chỉ IP của máy tính và của một website khác hay không? Hãy thực hiện ví dụ minh họa.**

- **Địa chỉ IP được dùng làm gì và cách xem địa chỉ IP của máy tính và của một website khác?**
  - Địa chỉ IP được dùng để giúp các thiết bị mạng Internet phân biệt và nhận ra nhau, từ đó có thể giao tiếp với nhau. Các thiết bị trên mạng có các địa chỉ IP khác nhau.
  - Để xem địa chỉ IP của máy tính, ta thực hiện như sau:
    - Đầu tiên, ta nhấn Window + R, sau đó gõ lệnh cmd



Hình 11: Giao diện sau khi nhấn Window + R

- Sau đó, chạy lệnh ipconfig

```
C:\Users\ACER>ipconfig
```

Hình 12: Lệnh gọi để tìm IP trên máy tính

- Sau khi chạy xong lệnh trên, nó sẽ cho ta nhiều địa chỉ IP khác nhau, do đó, ta phải để ý thật kĩ lưỡng để không xem nhầm địa chỉ IP:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b1ad:46ae:112:c495%18
   IPv4 Address. . . . . . . . . . . : 10.0.129.0
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.0.0.1
```

Hình 13: IP của máy tính

Từ hình trên, ta có thể biết được địa chỉ IP của máy tính ta là 10.0.129.0.

- Để xem địa chỉ IP của một website khác, ta thực hiện như sau:
  - Đầu tiên, ta cũng mở Command Prompt như ở trên.
  - Sau đó, trong cmd, ta gõ lệnh ping + tên website mà ta muốn tìm kiếm.
  - Ví dụ ta muốn tìm địa chỉ IP của website daa.uit.edu.vn, ta thực hiện như sau:

```
C:\Users\ACER>ping daa.uit.edu.vn

Pinging daa.uit.edu.vn [45.122.249.78] with 32 bytes of data:
Reply from 45.122.249.78: bytes=32 time=10ms TTL=56
Reply from 45.122.249.78: bytes=32 time=19ms TTL=56
Reply from 45.122.249.78: bytes=32 time=17ms TTL=56
Reply from 45.122.249.78: bytes=32 time=4ms TTL=56

Ping statistics for 45.122.249.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 19ms, Average = 12ms
```

Hình 14: Lệnh tìm địa chỉ IP của một trang web

Qua ảnh trên, ta có thể dễ dàng biết được rằng, địa chỉ IP của website daa.uit.edu.vn là 45.122.249.78.