THỰC HÀNH NHẬP MÔN MẠNG MÁY TÍNH
Lab 1 - Wireshark Getting Started

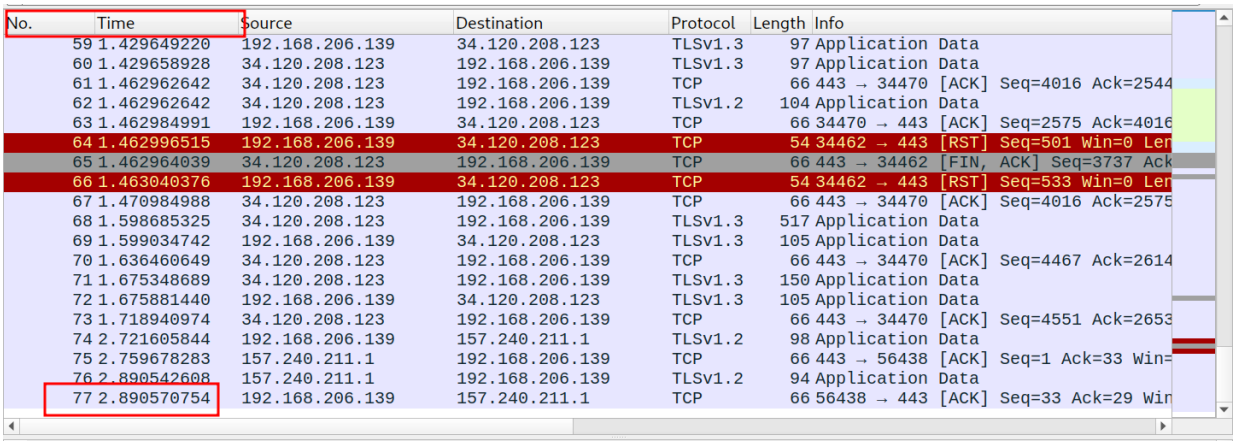
Họ và tên: Lê Hoàng Khánh
MSSV: 21522205
Lớp: IT005.N12.MMCL.1

Website dùng để bắt gói tin:
- Website 1: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
- Wensite 2: https://daa.uit.edu.vn/

Câu 1:

- Website 1:

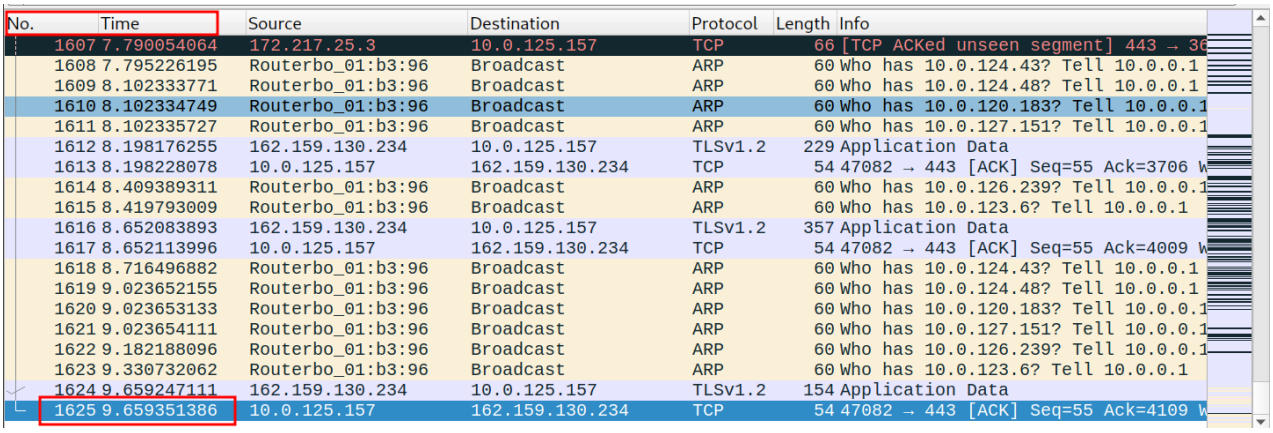
+ Tổng số gói tin: 77
+ Tổng thời gian 2.890570754 giây



No.	Time	Source	Destination	Protocol	Length	Info
59	1.429649220	192.168.206.139	34.120.208.123	TLSv1.3	97	Application Data
60	1.429658928	34.120.208.123	192.168.206.139	TLSv1.3	97	Application Data
61	1.462962642	34.120.208.123	192.168.206.139	TCP	66	443 → 34470 [ACK] Seq=4016 Ack=2544
62	1.462962642	34.120.208.123	192.168.206.139	TLSv1.2	104	Application Data
63	1.462984991	192.168.206.139	34.120.208.123	TCP	66	34470 → 443 [ACK] Seq=2575 Ack=4016
64	1.462996515	192.168.206.139	34.120.208.123	TCP	54	34462 → 443 [RST] Seq=501 Win=0 Len
65	1.462964039	34.120.208.123	192.168.206.139	TCP	66	443 → 34462 [FIN, ACK] Seq=3737 Ack
66	1.463040376	192.168.206.139	34.120.208.123	TCP	54	34462 → 443 [RST] Seq=533 Win=0 Len
67	1.470984988	34.120.208.123	192.168.206.139	TCP	66	443 → 34470 [ACK] Seq=4016 Ack=2575
68	1.598685325	34.120.208.123	192.168.206.139	TLSv1.3	517	Application Data
69	1.599034742	192.168.206.139	34.120.208.123	TLSv1.3	105	Application Data
70	1.636460649	34.120.208.123	192.168.206.139	TCP	66	443 → 34470 [ACK] Seq=4467 Ack=2614
71	1.675348689	34.120.208.123	192.168.206.139	TLSv1.3	150	Application Data
72	1.675881440	192.168.206.139	34.120.208.123	TLSv1.3	105	Application Data
73	1.718940974	34.120.208.123	192.168.206.139	TCP	66	443 → 34470 [ACK] Seq=4551 Ack=2653
74	2.721605844	192.168.206.139	157.240.211.1	TLSv1.2	98	Application Data
75	2.759678283	157.240.211.1	192.168.206.139	TCP	66	443 → 56438 [ACK] Seq=1 Ack=33 Win=
76	2.890542608	157.240.211.1	192.168.206.139	TLSv1.2	94	Application Data
77	2.890570754	192.168.206.139	157.240.211.1	TCP	66	56438 → 443 [ACK] Seq=33 Ack=29 Win

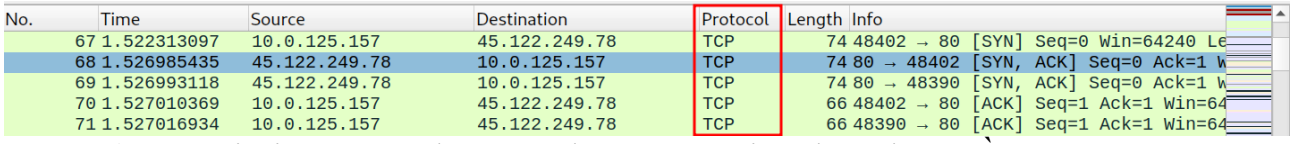
- Website 2:

+ Tổng số gói tin: 1625
+ Tổng thời gian: 9.659351386 giây



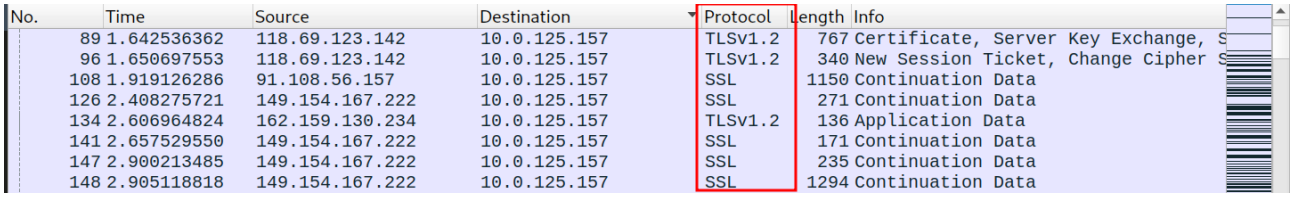
No.	Time	Source	Destination	Protocol	Length	Info
1607	7.790054064	172.217.25.3	10.0.125.157	TCP	66	[TCP ACKed unseen segment] 443 → 36
1608	7.795226195	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.124.43? Tell 10.0.0.1
1609	8.102333771	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.124.48? Tell 10.0.0.1
1610	8.102334749	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.120.183? Tell 10.0.0.1
1611	8.102335727	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.127.151? Tell 10.0.0.1
1612	8.198176255	162.159.130.234	10.0.125.157	TLSv1.2	229	Application Data
1613	8.198228078	10.0.125.157	162.159.130.234	TCP	54	47082 → 443 [ACK] Seq=55 Ack=3706 W
1614	8.409389311	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.126.239? Tell 10.0.0.1
1615	8.419793009	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.123.6? Tell 10.0.0.1
1616	8.652083893	162.159.130.234	10.0.125.157	TLSv1.2	357	Application Data
1617	8.652113996	10.0.125.157	162.159.130.234	TCP	54	47082 → 443 [ACK] Seq=55 Ack=4009 W
1618	8.716496882	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.124.43? Tell 10.0.0.1
1619	9.023652155	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.124.48? Tell 10.0.0.1
1620	9.023653133	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.120.183? Tell 10.0.0.1
1621	9.023654111	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.127.151? Tell 10.0.0.1
1622	9.182188096	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.126.239? Tell 10.0.0.1
1623	9.330732062	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.123.6? Tell 10.0.0.1
1624	9.659247111	162.159.130.234	10.0.125.157	TLSv1.2	154	Application Data
1625	9.659351386	10.0.125.157	162.159.130.234	TCP	54	47082 → 443 [ACK] Seq=55 Ack=4109 W

Câu 2:



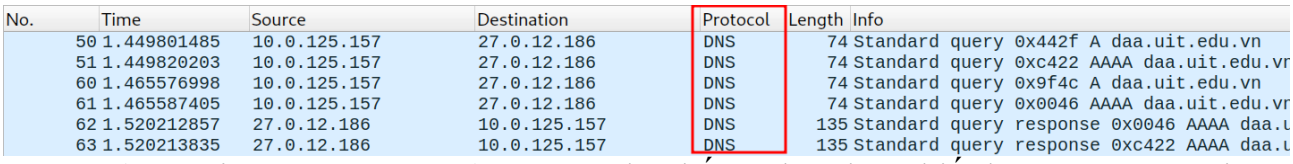
No.	Time	Source	Destination	Protocol	Length	Info
67	1.522313097	10.0.125.157	45.122.249.78	TCP	74	48402 → 80 [SYN] Seq=0 Win=64240 Le
68	1.526985435	45.122.249.78	10.0.125.157	TCP	74	80 → 48402 [SYN, ACK] Seq=0 Ack=1 W
69	1.526993118	45.122.249.78	10.0.125.157	TCP	74	80 → 48390 [SYN, ACK] Seq=0 Ack=1 W
70	1.527010369	10.0.125.157	45.122.249.78	TCP	66	48402 → 80 [ACK] Seq=1 Ack=1 Win=64
71	1.527016934	10.0.125.157	45.122.249.78	TCP	66	48390 → 80 [ACK] Seq=1 Ack=1 Win=64

- TCP (Transmission Control Protocol)**:** Là một giao thức thuộc tầng Transport của bộ giao thức TPC/IP. Qua đó các ứng dụng nằm trên các máy chủ có thể tạo các kết nối với nhau để truyền dữ liệu hoặc các gói tin với nhau. Giao thức này còn đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự.



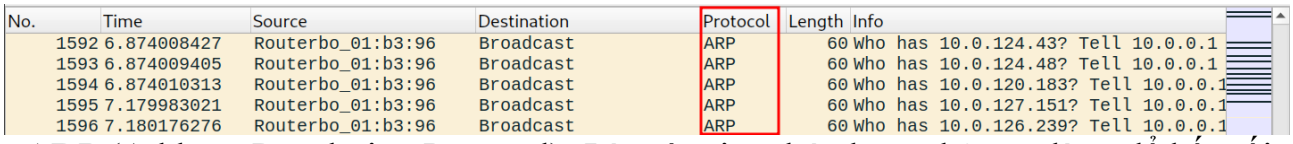
No.	Time	Source	Destination	Protocol	Length	Info
89	1.642536362	118.69.123.142	10.0.125.157	TLSv1.2	767	Certificate, Server Key Exchange, S
96	1.650697553	118.69.123.142	10.0.125.157	TLSv1.2	340	New Session Ticket, Change Cipher S
108	1.919126286	91.108.56.157	10.0.125.157	SSL	1150	Continuation Data
126	2.408275721	149.154.167.222	10.0.125.157	SSL	271	Continuation Data
134	2.606964824	162.159.130.234	10.0.125.157	TLSv1.2	136	Application Data
141	2.657529550	149.154.167.222	10.0.125.157	SSL	171	Continuation Data
147	2.900213485	149.154.167.222	10.0.125.157	SSL	235	Continuation Data
148	2.905118818	149.154.167.222	10.0.125.157	SSL	1294	Continuation Data

- SSL/TLS (Secure Sockets Layer/Transport Layer Security)**:** Là giao thức mật mã (encryption-based Internet security protocol) được thiết kế để cung cấp truyền thông tin an toàn qua một mạng máy tính. Qua đó mã hóa giao tiếp giữa các ứng dụng, web và máy chủ, chẳng hạn như duyệt web tải một trang web. TLS cũng có thể được sử dụng để mã hóa các thông tin liên lạc khác như email, tin nhắn và thoại qua IP (VoIP). SSL là tiền thân của mã hõa hiện đại TLS được sử dụng ngày nay, SSL và TLS là cùng chức năng, nó chỉ khác nhau về ký hiệu. Website có chứng chỉ SSL/TLS thì sẽ có HTTPS thay vì HTTP ở URL.



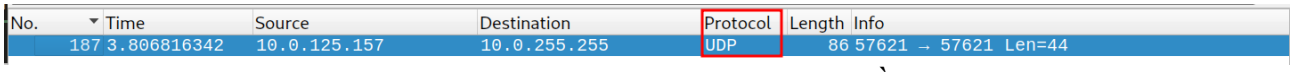
No.	Time	Source	Destination	Protocol	Length	Info
50	1.449801485	10.0.125.157	27.0.12.186	DNS	74	Standard query 0x442f A daa.uit.edu.vn
51	1.449820203	10.0.125.157	27.0.12.186	DNS	74	Standard query 0xc422 AAAA daa.uit.edu.vn
60	1.465576998	10.0.125.157	27.0.12.186	DNS	74	Standard query 0x9f4c A daa.uit.edu.vn
61	1.465587405	10.0.125.157	27.0.12.186	DNS	74	Standard query 0x0046 AAAA daa.uit.edu.vn
62	1.520212857	27.0.12.186	10.0.125.157	DNS	135	Standard query response 0x0046 AAAA daa.u
63	1.520213835	27.0.12.186	10.0.125.157	DNS	135	Standard query response 0xc422 AAAA daa.u

- DNS (Domain Name System)**:** Là một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên Internet. Nhiệm vụ cơ bản của DNS là "dịch" một tên miền quen thuộc với người dùng thành một địa chỉ IP giúp các máy tính sử dụng để nhận dạng chính xác nhau trên hệ thống mạng toàn cầu.



No.	Time	Source	Destination	Protocol	Length	Info
1592	6.874008427	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.124.43? Tell 10.0.0.1
1593	6.874009405	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.124.48? Tell 10.0.0.1
1594	6.874010313	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.120.183? Tell 10.0.0.1
1595	7.179983021	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.127.151? Tell 10.0.0.1
1596	7.180176276	Routerbo_01:b3:96	Broadcast	ARP	60	Who has 10.0.126.239? Tell 10.0.0.1

- ARP (Address Resolution Protocol)**:** Là một giao thức hoặc thủ tục dùng để kết nối giao thức Internet IP (Internet Protocol) luôn thay đổi với một địa chỉ máy chủ vật lý cố định. Máy chủ cố định này còn được gọi là địa chỉ điều khiển truy cập phương tiện MAC (Media Access Control) trong mạng cục bộ LAN (local-area network). ARP là một giao thức ánh xạ rất cần thiết. Độ dài của địa chỉ IP và địa chỉ MAC rất khác nhau. Địa chỉ IPv4 thông dụng có độ dài 32 bit, trong khi đó địa chỉ MAC dài đến 48 bit. Do đó, chúng cần "một người" trung gian để dịch 32 thành 48 và ngược lại để chúng "nhận ra nhau".

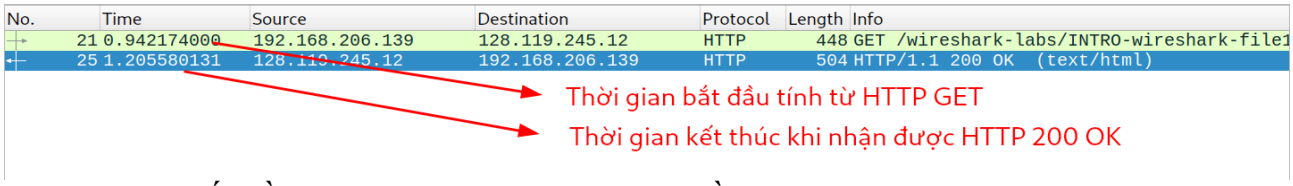


No.	Time	Source	Destination	Protocol	Length	Info
187	3.806816342	10.0.125.157	10.0.255.255	UDP	86	57621 → 57621 Len=44

-UDP (User Datagram Protocol): Là một giao thức thuộc tầng Transport của bộ giao thức TPC/IP. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP làm, các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái của nó nên nó hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu (VD: DNS, Streaming, VoIP).

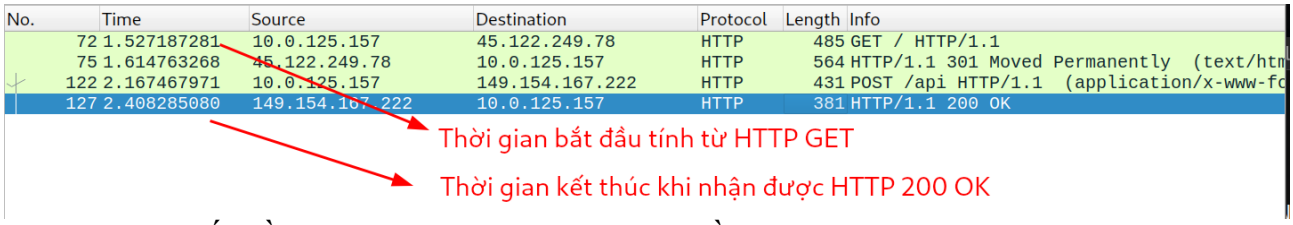
Câu 3:

- Website 1:



+ Thời gian bắt đầu từ khi gói tin HTTP GET đầu tiên được gửi là 0.942174000 giây.
+ Thời gian kết thúc khi nhận được gói tin HTTP 200 OK là 1.205580131 giây.
=> Tổng thời gian từ khi gói tin HTTP GET đầu được gửi đến khi nhận được gói HTTP 200 OK là: 0.263406131 giây.

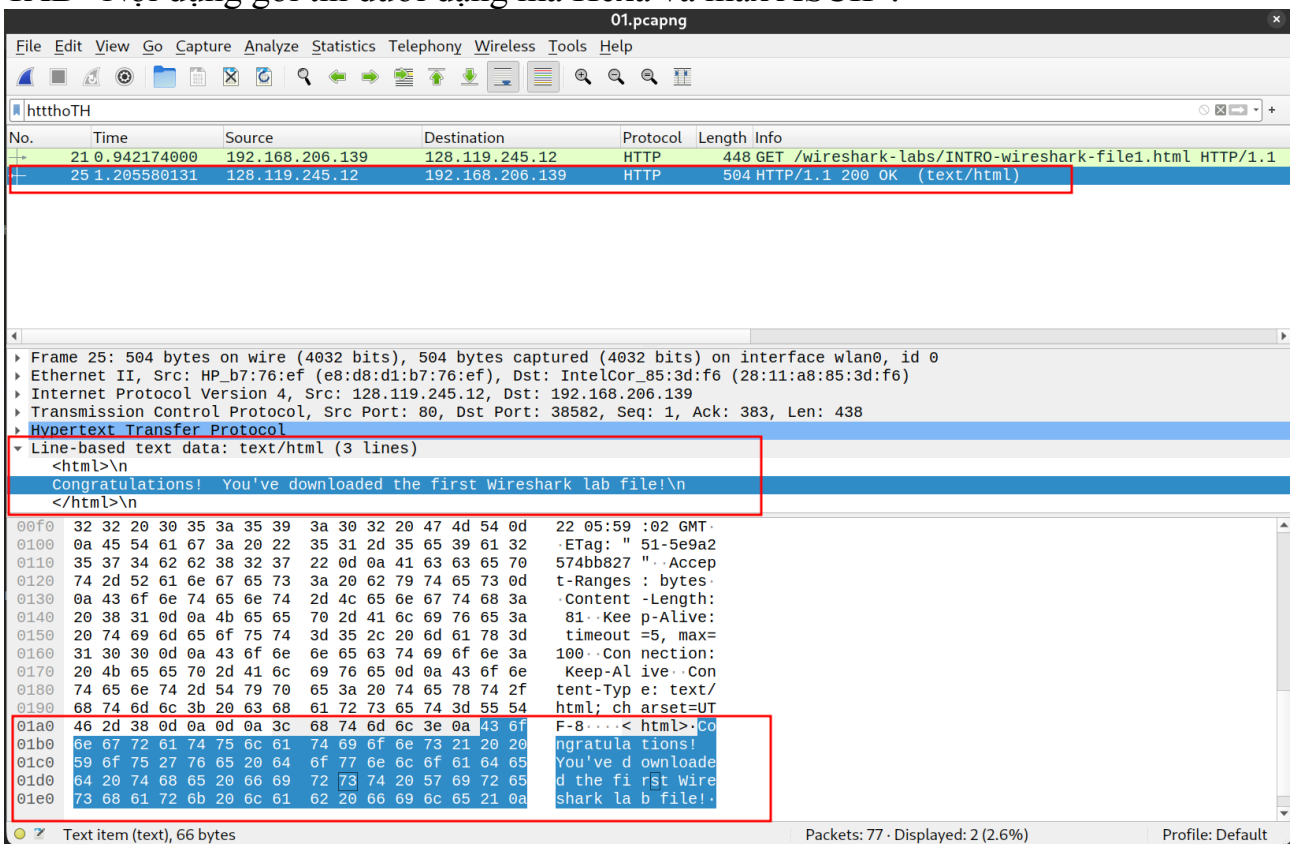
- Website 2:



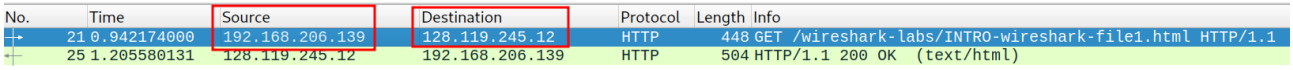
+ Thời gian bắt đầu từ khi gói tin HTTP GET đầu tiên được gửi là 1.527187281 giây.
+ Thời gian kết thúc khi nhận được gói tin HTTP 200 OK là 2.408285080 giây.
=> Tổng thời gian từ khi gói tin HTTP GET đầu được gửi đến khi nhận được gói HTTP 200 OK là: 0.881097799 giây.

Câu 4:

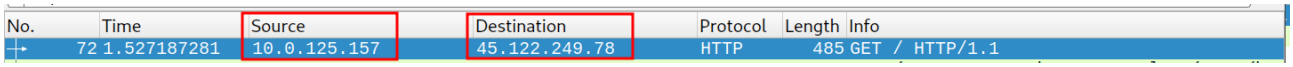
Nội dung hiển thị trên trang web gaia.cs.umass.edu được bắt ở gói tin HTTP 200 OK. Ta có thể thấy được nội dung này sau khi lựa chọn gói tin HTTP 200 OK, qua TAB "Chi tiết gói tin" => "Line-based text data" hoặc chúng ta cũng có thể thấy được qua TAB "Nội dụng gói tin dưới dạng mã Hexa và max ASCII".



Câu 5:



- HTTP GET là gói tin đuọc gửi từ máy tính của đang sử dụng đến Website gaia.cs.umass.edu. Do đó qua 2 cột Source và Destination ta xác định đượcc. Địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12 và địa chỉ máy đang sử dụng là 192.168.206.139.



- Tương tự ta có địa chỉ IP của daa.uit.edu.vn là 45.122.249.78 và địa chỉ máy đang sử dụng là 10.0.125.157.

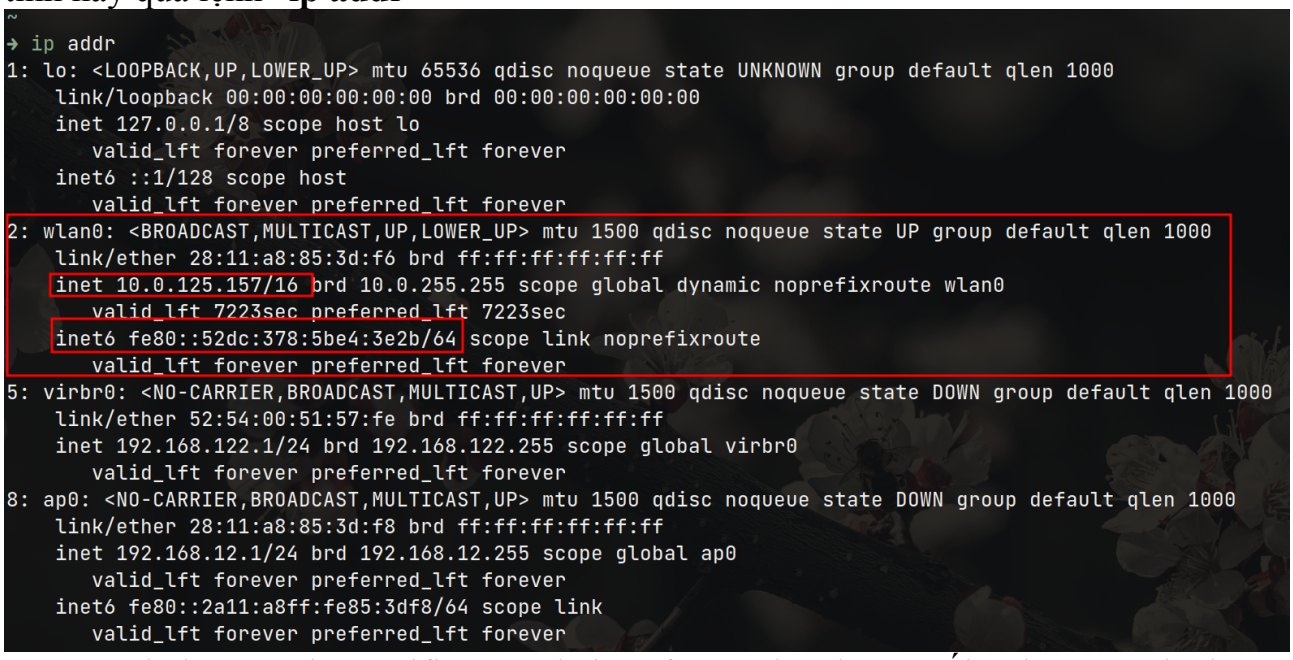
Câu 6:

- Vì đây là mô hình Server – Cilent nên đầu tiên trình duyệt (cilent) gửi một request với request method (GET, POST...) qua giao thức HTTP (HTTP request) tới server.
- Sau đó server sẽ xem xét gói tin và phân tích, nếu tập tin yêu cầu là hợp lệ thì server sẽ trả lại gòi tin kèm với header và status code là 200.
- Và cuối cùng khi máy tính nhận được gói tin, trình duyệt(cilent) sẽ xuất ra những dữ liệu từ file HTML lên màn hình.

Mở rộng:

- IP sẽ giúp các thiết bị trên mạng Internet có thể phân biệt, chia sẻ và giao tiếp với nhau. Nó sẽ cung cấp danh tính cho các thiết bị khi chúng kết nối mạng tương tự như địa chỉ nhà có vị trí cụ thể.

- Ở đây máy tính đang sử dụng Linux, chúng ta có thể biết đuọc địa chỉ IP của máy tính này qua lệnh "**ip addr**"



- Máy tính đang sử dụng wifi nên sẽ là interface sẽ là wlan0. Đối với IPv4 sẽ là dòng inet, còn đối với IPv6 sẽ là dòng inet6. Đây chính là địa chỉ ip của máy tính đang sử dụng.

- Để có thể xem được địa chỉ IP của một trang web nào đó (ở đây là daa.uit.edu.vn), ta sử dùng lệnh "**ping + tên trang web**".