BÁO CÁO THỰC HÀNH

Môn học: Nhập môn mạng máy tính

Buổi báo cáo: Lab 01

Tên chủ đề: Làm quen với Wireshark

***GVHD**: Nguyễn Văn Bảo*

***Ngày thực hiện**: 29/09/2025*

THÔNG TIN CHUNG:

Lớp: IT005.Q15.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Khoa Nguyên	24521190	24521190@gm.uit.edu.vn

1. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	4 tiếng
Link Video thực hiện *(nếu có)*	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất …	
Điểm tự đánh giá	

BÁO CÁO CHI TIẾT

1. Task 1: Mở đầu về mạng máy tính

a) Nội dung 1: Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa)

- Router (thiết bị định tuyến hoặc bộ định tuyến): là thiết bị mạng dùng để chuyển các gói dữ liệu đến các thiết bị đầu cuối

Hình 1 Router

- Switch: là bộ chuyển mạch được dùng để kết nối các đoạn mạng với nhau theo mô hình mạng hình sao (Switch chính là thiết bị trung tâm, tất cả các máy tính trong hệ thống mạng đều được nối dây về đây tạo thành một hệ thống mạng)

Hình 2 Switch

- Access Point (điểm truy cập): là một loại thiết bị mạng có khả năng tạo ra mạng cục bộ. Nó chó phép tạo ra các điểm truy cập cho phép các thiết bị khác kết nối được Wi-Fi

Hình 3 Access Point

b) Những vấn đề có thể xảy ra nếu không có kết nối Internet trong 5 phút

- Nếu không có Internet trong 5 phút thì cuộc sống chúng ta sẽ gặp rất nhiều thay đổi (dù 5 phút là một thời gian rất ngắn) và dẫn đến một hậu quả nặng nề trên mọi mặt:
    - Về truyền thông: Xảy ra vấn đề cập nhật thông tin chậm chạp cùng với việc hạn chế giao tiếp (vì đa số hiện nay đều giao tiếp qua email, ứng dụng mạng xã hội)
    - Về công việc: gián đoạn hoạt động kinh tế như mua sắm online, ngân hàng từ đó gây thiệt hại lớn cho các công ty, doanh nghiệp
    - Về cuộc sống: Ứng dụng giải trí bị hạn chế như nghe nhạc, xem phim, lướt web, mạng xã hội

⇨ Dù chỉ là 5 phút ngắn ngủi nhưng có thể dẫn đến những bất ổn, đảo lộn lớn trên mọi mặt của cuộc sống

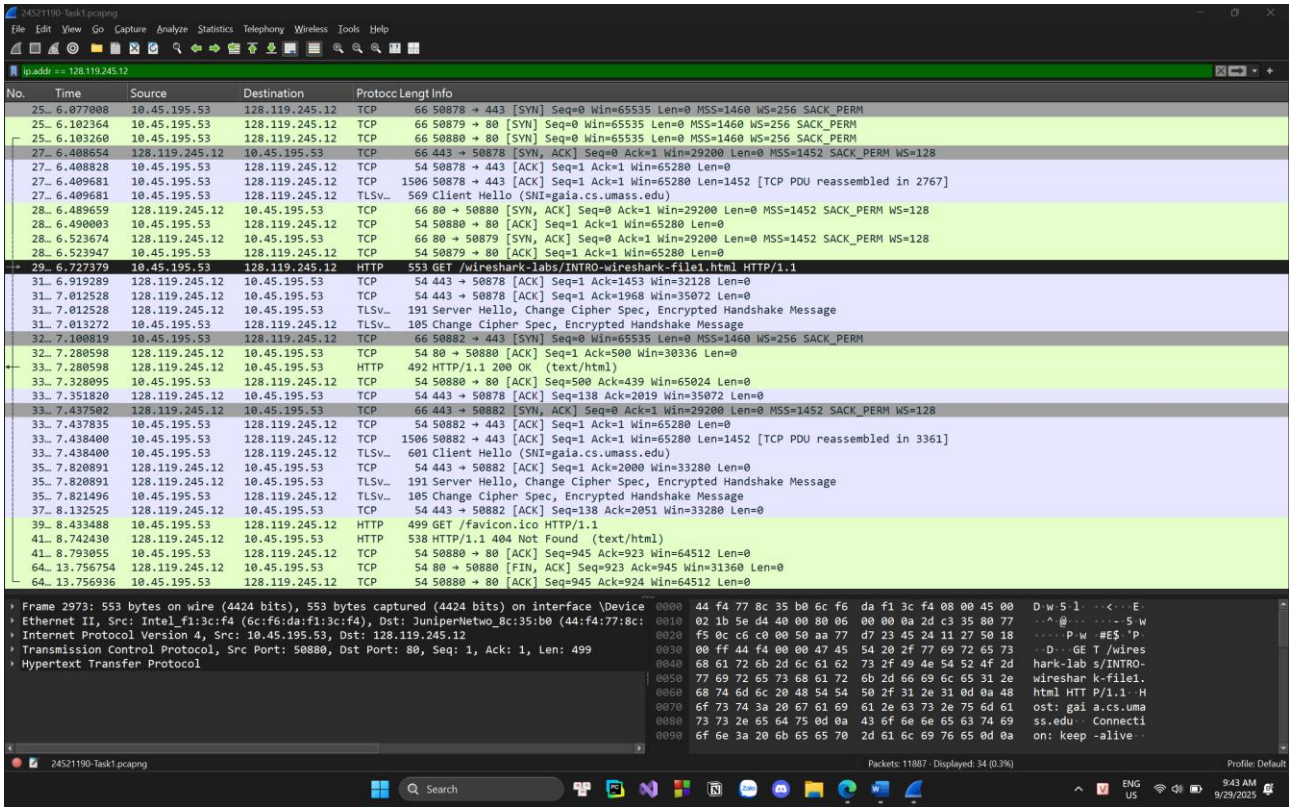
c) Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì ?

- Hiểu được các khái niệm cơ bản về mạng máy tính (các giao thức mạng máy tính, mô hình tham chiếu,…)
- Hiểu và mô tả được nguyên lý hoạt động của các tầng mạng: tầng ứng dụng, vận chuyển, mạng, liên kết dữ liệu và vật lý
- Có khả năng vận dụng kiến thức để đánh giá các hiện tượng thường gặp trong hoạt động của máy tính

2. Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

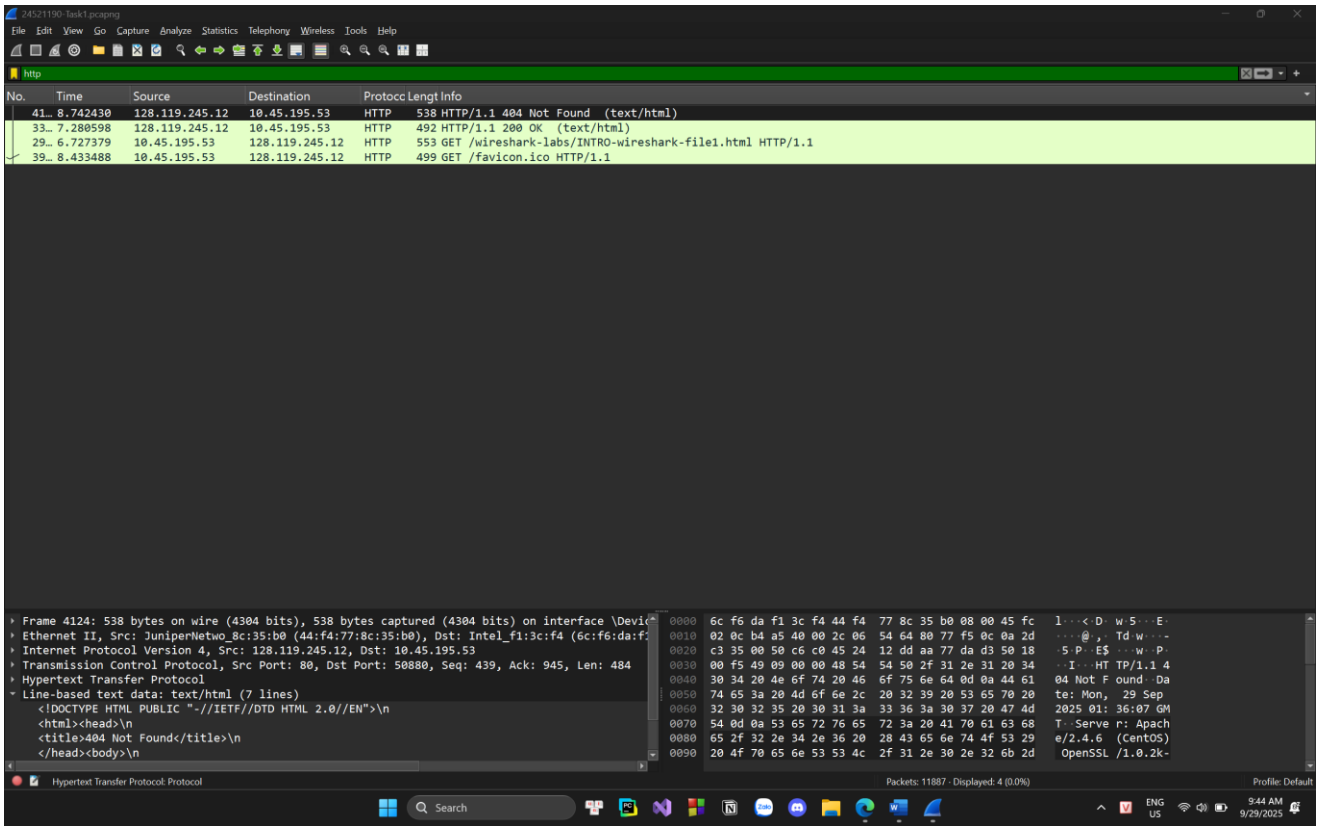
a) Nội dung 1: Tổng thời gian bắt gói tin đối với website đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu ?

- Tổng thời gian bắt gói tin đối với website đã thử nghiệm = thời gian bắt được gói tin ở web thử nghiệm đầu tiên – thời gian bắt được gói tin ở web thử nghiệm cuối cùng = 13.756936 – 6.077008 = 7.679928
- Tổng số gói tin bắt được: 11887



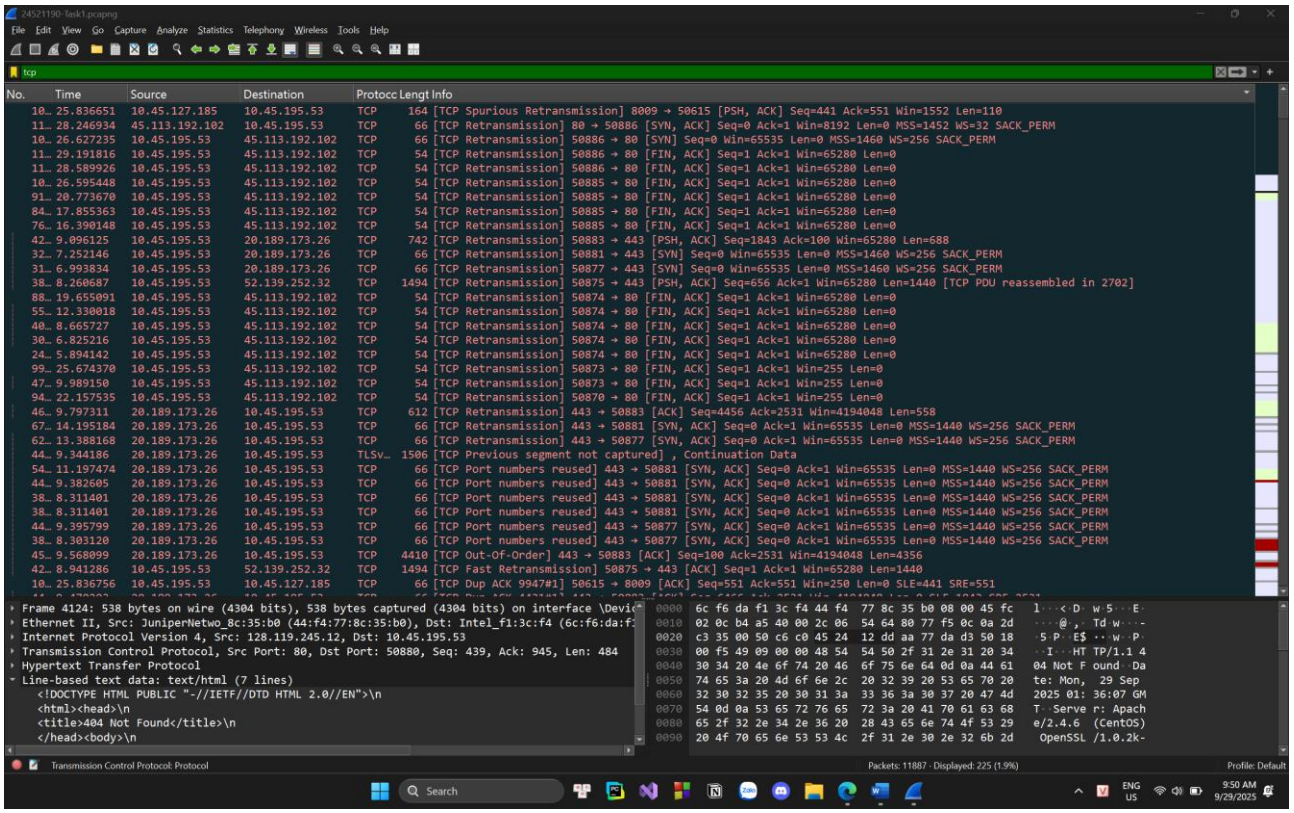
b) Nội dung 2: Trong các gói tin bắt được, có tổng cộng bao nhiêu gói tin HTTP

- Trong các gói tin bắt được, có tổng 4 gói tin HTTP. Ta biết được số lượng gói tin HTTP bằng cách sử dụng filter để lọc ra các gói tin có giao thức HTTP

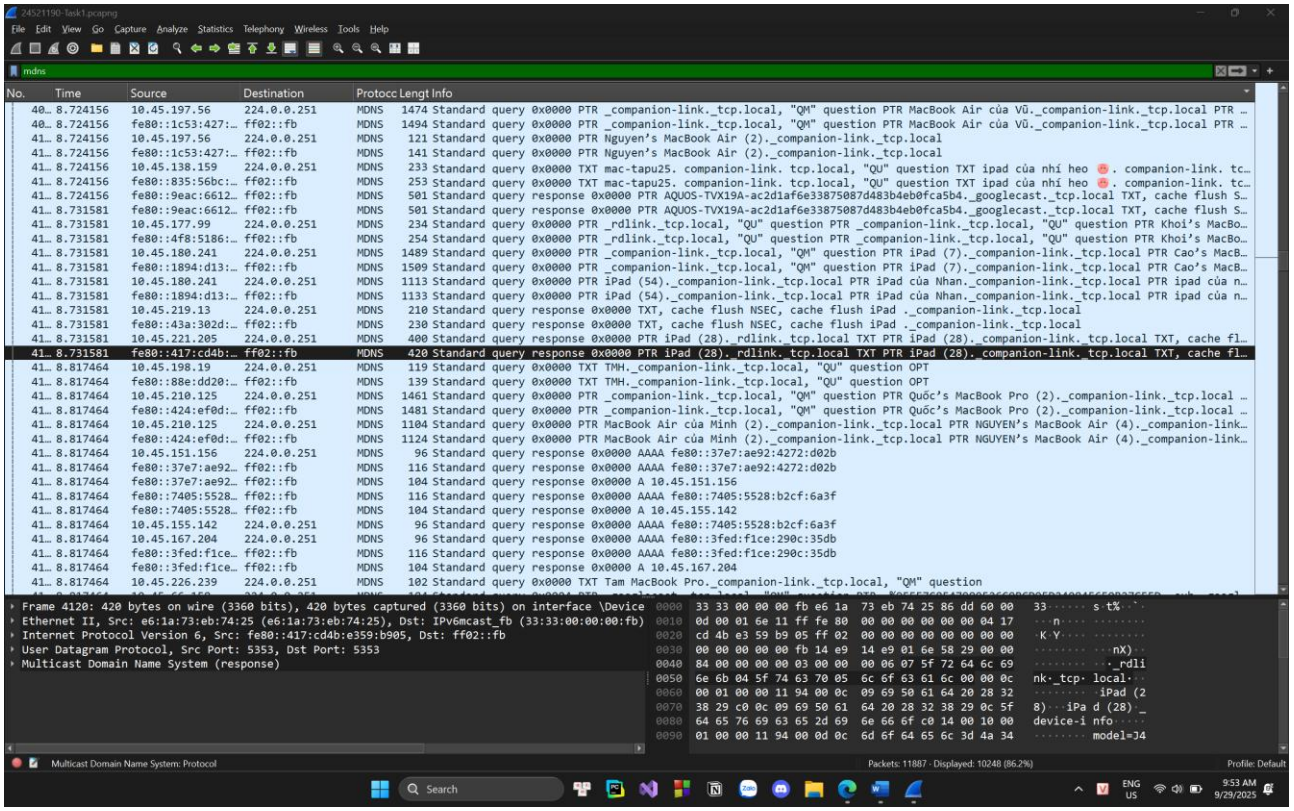


c) Nội dung 3: Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc "http" khi truy cập website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

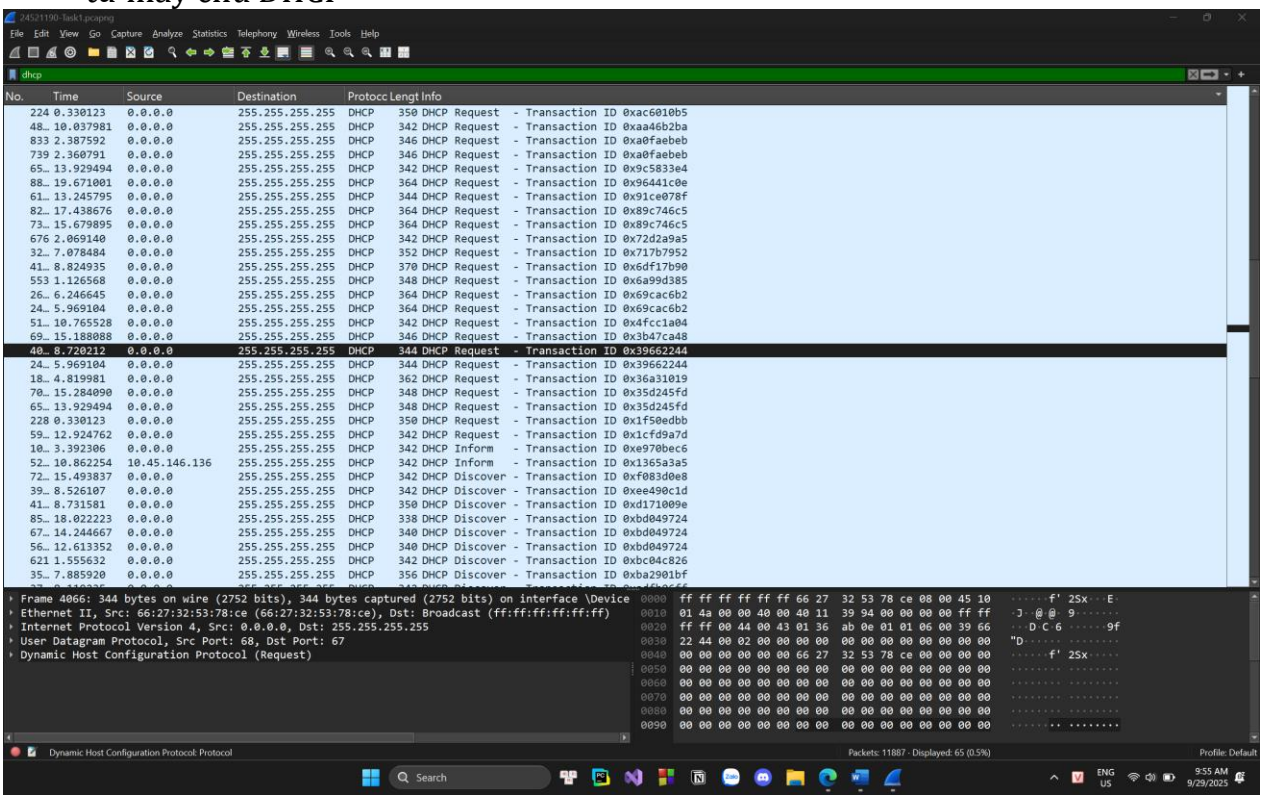
- TCP (Transmission Control Protocol): là một trong những giao thức quan trọng thuộc tầng vận chuyển (Transport Layer) trong mô hình TCP/IP. Gồm các đặc điểm chính: Thiết lập kết nối, kiểm soát luồng (flow control), kiểm soát tắc nghén (congestion control), đảm bảo tin cậy (data transfer reliable)



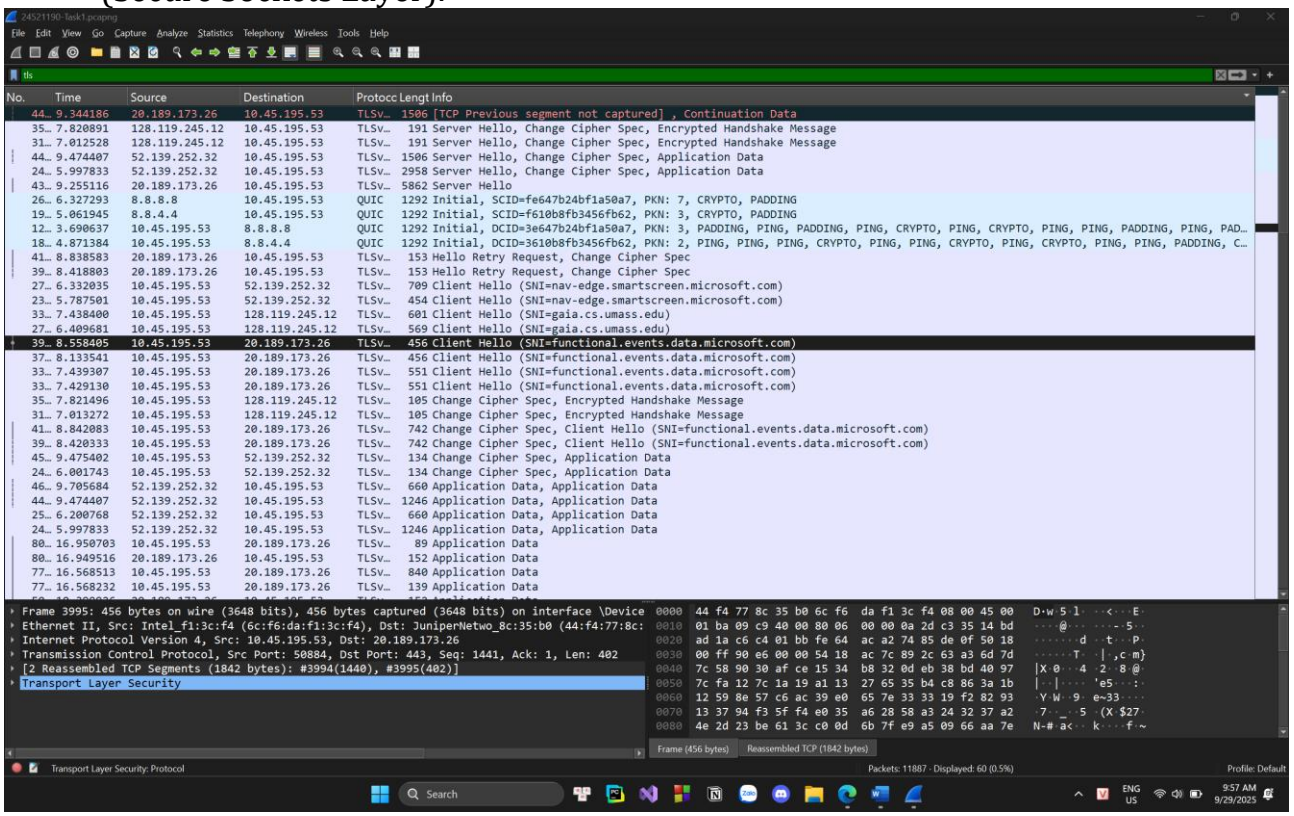
- MDNS (Multicast DNS): là một giao thức trong mạng máy tính cho phép các thiết bị tự động phát hiện nhau trong cùng một mạng cục bộ (LAN) mà không cần máy chủ DNS trung tâm. Nó thường được sử dụng trong các mạng gia định hoặc văn phòng nhỏ



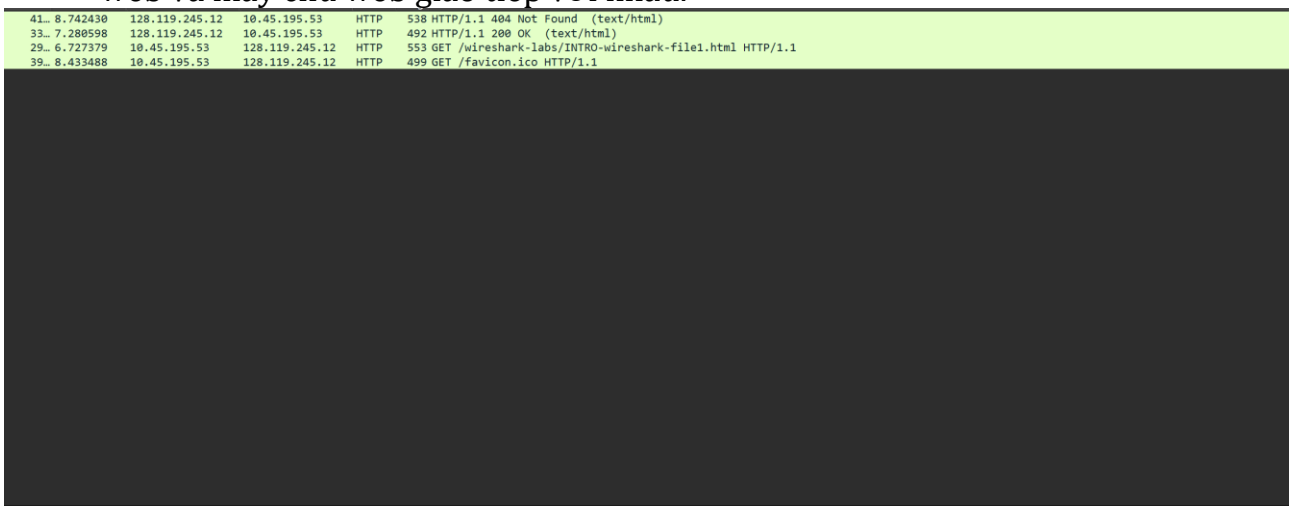
- DHCP (Dynamic Host Configuration Protocol): là giao thức thuộc tầng ứng dụng được dùng để cấp phát tự động các thông số cấu hình mạng cho thiết bị trong mạng (IP, subnet mask, gateway, DNS server,...). DHCP làm việc theo mô hình Client-Server. Khi một thiết bị kết nối vào mạng, nó sẽ tự động xin thông tin IP từ máy chủ DHCP



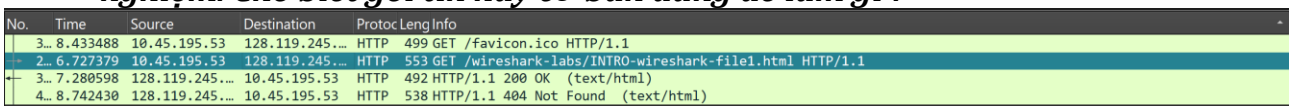
- TLS (Transport Layer Security): là một giao thức bảo mật ở tầng vận chuyển (Transport Layer), được dùng để mã hóa và đảm bảo an toàn dữ liệu khi truyền qua mạng (đặc biệt là Internet). TLS là phiên bản kế thừa và cải tiến của SSL (Secure Sockets Layer).



- HTTP (HyperText Transfer Protocol) là một giao thức ở tầng Ứng dụng (Application Layer), được dùng để truyền tải dữ liệu trên World Wide Web (như văn bản, hình ảnh, video, âm thanh...). Đây là nền tảng chính giúp trình duyệt web và máy chủ web giao tiếp với nhau.

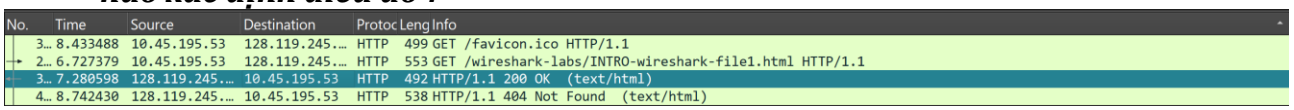


d) Nội dung 4: Xác định gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm. Cho biết gói tin này cơ bản dùng để làm gì ?



- Gói tin HTTP GET đầu tiên là gói có info: GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
- Tác dụng: Lấy tài nguyên ban đầu từ server bao gồm nội dung trang web,…

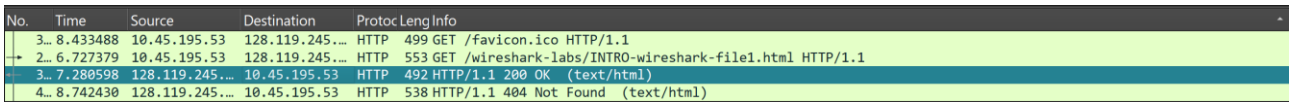
e) Nội dung 5: Xác định gói tin phản hồi của gói tin HTTP GET ở câu 4, thông tin nào xác định điều đó ?



- Gói tin phản hồi của gói tin HTTP GET ở câu 4 là gói có info: HTTP/1.1 200 OK (text/html)
- Ta biết được là do gói tin này được gửi từ source chính là IP của server đến IP của client và gói tin này phản hồi với mã 200 OK nghĩa là server đã phản hồi thành công nội dung gói tin cho client

f) Nội dung 6: Tính thời gian từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi có gói tin phản hồi HTTP 200 OK đối với website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).

- Thời gian từ khi gói tin HTTP GET đầu tiên đến khi có gói tin phản hồi HTTP 200 OK = 7.280598 – 6.727379 = 0.553219



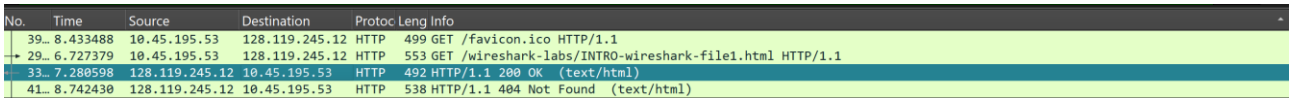
g) Nội dung 7: Nội dung hiển thị trên trang web gaia.cs.umass.edu "Congratulations! You've downloaded the first Wireshark lab file!" có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

- Vì đây là gói tin sử dụng HTTP nên thông tin mà server trả về không được mã hóa, do đó chắc chắn chúng ta sẽ thấy được nội dung hiển thị trên trang web, và ta tìm thông tin này trong tầng ứng dụng của gói tin phản hồi từ server

```
▸ Ethernet II, Src: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0), Dst: Intel_f1:3c:
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.195.53
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 50880, Seq: 1, Ack: 500
▸ 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
```

h) Nội dung 8: Hãy tìm hiểu về định dạng của địa chỉ IP và thử phỏng đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

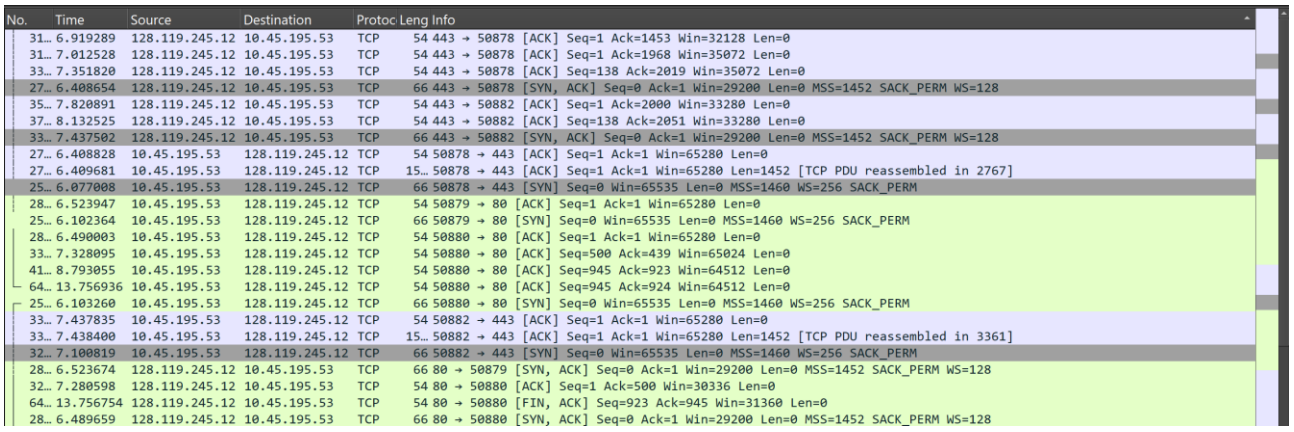
- Địa chỉ IP (Internet Protocol Address) là một dãy số dùng để định danh thiết bị trong mạng và cho phép các thiết bị giao tiếp với nhau. Hiện nay có hai phiên bản chính: IPv4 và IPv6.
- Độ dài: 32 bit (4 byte)
- Cách biểu diễn: Viết dưới dạng thập phân và chia thành 4 octet, ngăn cách bằng dấu chấm (ví dụ: 192.168.1.0)
- Phạm vi: từ 0.0.0.0 đến 255.255.255.255
- Phân loại địa chỉ: Public IP (dùng trên Internet) và Private IP (dùng trong LAN)
- Địa chỉ IP của gaia.cs.umass.edu là: 128.119.245.12
- Địa chỉ IP của máy tính đang sử dụng: 10.45.195.53



No.	Time	Source	Destination	Protoc	Leng	Info
39…	8.433488	10.45.195.53	128.119.245.12	HTTP	499	GET /favicon.ico HTTP/1.1
29…	6.727379	10.45.195.53	128.119.245.12	HTTP	553	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
33…	7.280598	128.119.245.12	10.45.195.53	HTTP	492	HTTP/1.1 200 OK (text/html)
41…	8.742430	128.119.245.12	10.45.195.53	HTTP	538	HTTP/1.1 404 Not Found (text/html)

i) Nội dung 9: Từ các nội dung trên, hãy mô tả cơ bản khi truy cập một website (ví dụ website đã thử nghiệm ở trên) thì quá trình gửi và nhận gói tin đã hoạt động như thế nào? Trình duyệt mà bạn đang sử dụng đóng vai trò gì?

- Các bước:
  + Nhập URL và phân giải tên miền do DNS thực hiện (phân giải tên miền thành địa chỉ IP)
  + Thiết lập mạng kết nối TCP (phía client gửi yêu cầu thiết lập kết nối TCP đến server và server gửi phản hồi đồng ý thiết lập kết nối lại cho phía client)



No.	Time	Source	Destination	Protoc	Leng	Info
31…	6.919289	128.119.245.12	10.45.195.53	TCP	54	443 → 50878 [ACK] Seq=1 Ack=1453 Win=32128 Len=0
31…	7.012528	128.119.245.12	10.45.195.53	TCP	54	443 → 50878 [ACK] Seq=1 Ack=1968 Win=35072 Len=0
33…	7.351820	128.119.245.12	10.45.195.53	TCP	54	443 → 50878 [ACK] Seq=138 Ack=2019 Win=35072 Len=0
27…	6.408654	128.119.245.12	10.45.195.53	TCP	66	443 → 50878 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
35…	7.820891	128.119.245.12	10.45.195.53	TCP	54	443 → 50882 [ACK] Seq=1 Ack=2000 Win=33280 Len=0
37…	8.132525	128.119.245.12	10.45.195.53	TCP	54	443 → 50882 [ACK] Seq=138 Ack=2051 Win=33280 Len=0
33…	7.437502	128.119.245.12	10.45.195.53	TCP	66	443 → 50882 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
27…	6.408828	10.45.195.53	128.119.245.12	TCP	54	50878 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
27…	6.409681	10.45.195.53	128.119.245.12	TCP	15…	50878 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1452 [TCP PDU reassembled in 2767]
25…	6.077008	10.45.195.53	128.119.245.12	TCP	66	50878 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
28…	6.523947	10.45.195.53	128.119.245.12	TCP	54	50879 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
25…	6.102364	10.45.195.53	128.119.245.12	TCP	66	50879 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
28…	6.490003	10.45.195.53	128.119.245.12	TCP	54	50880 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
33…	7.328095	10.45.195.53	128.119.245.12	TCP	54	50880 → 80 [ACK] Seq=500 Ack=439 Win=65024 Len=0
41…	8.793055	10.45.195.53	128.119.245.12	TCP	54	50880 → 80 [ACK] Seq=945 Ack=923 Win=64512 Len=0
64…	13.756936	10.45.195.53	128.119.245.12	TCP	54	50880 → 80 [ACK] Seq=945 Ack=924 Win=64512 Len=0
25…	6.103260	10.45.195.53	128.119.245.12	TCP	66	50880 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
33…	7.437835	10.45.195.53	128.119.245.12	TCP	54	50882 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
33…	7.438400	10.45.195.53	128.119.245.12	TCP	15…	50882 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=1452 [TCP PDU reassembled in 3361]
32…	7.100819	10.45.195.53	128.119.245.12	TCP	66	50882 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
28…	6.523674	128.119.245.12	10.45.195.53	TCP	66	80 → 50879 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
32…	7.280598	128.119.245.12	10.45.195.53	TCP	54	80 → 50880 [ACK] Seq=1 Ack=500 Win=30336 Len=0
64…	13.756754	128.119.245.12	10.45.195.53	TCP	54	80 → 50880 [FIN, ACK] Seq=923 Ack=945 Win=31360 Len=0
28…	6.489659	128.119.245.12	10.45.195.53	TCP	66	80 → 50880 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128

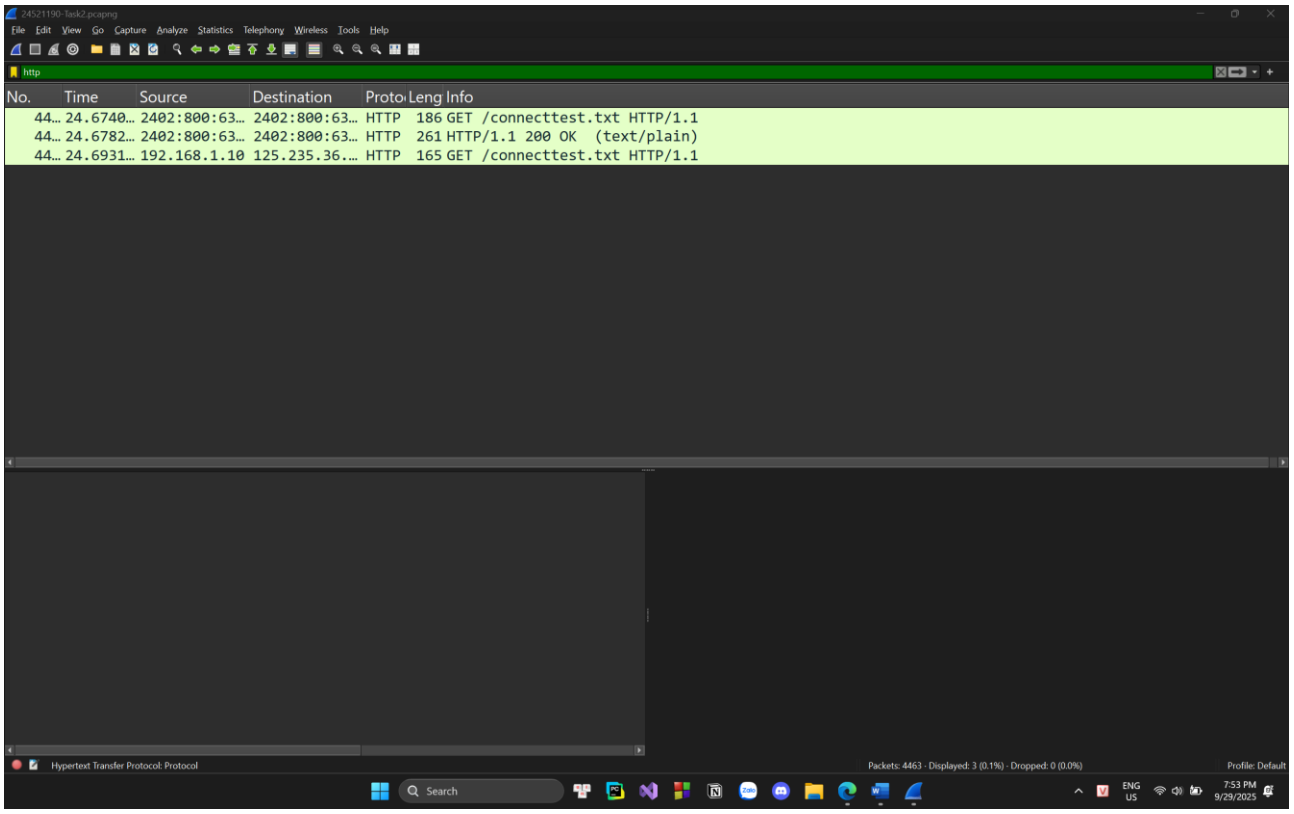
+ Client gửi yêu cầu HTTP và server trả về phản hồi HTTP

+ Trình duyệt hiển thị nội dung: server gửi về phản hồi HTTP chứa 1 file html gồm các đối tượng và tham chiếu đến đối tượng mà client yêu cầu

- Trình duyệt đang sử dụng đóng vai trò:
  + Cung cấp giao diện người dùng
  + Thực hiện giao thức: gửi HTTP request và xử lý HTTP response
  + Quản lý kết nối
  + Diễn dịch: Chuyển dữ liệu web (file html) thành giao diện đồ họa cho người dùng có thể tiếp cận được

j) Nội dung 10: Khi sử dụng bộ lọc "http" như ở đối với website ở Task 1 thì kết quả thu được như thế nào, có các gói tin HTTP tương tự không?

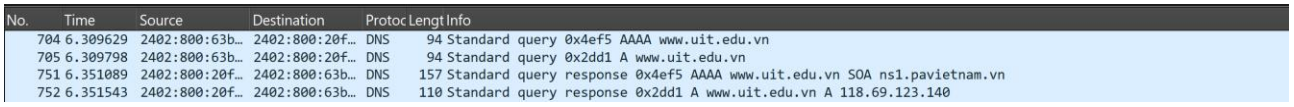
- Khi sử dụng bộ lọc "http" như ở đối với website ở Task 1 thì kết quả thu được sẽ không có gói tin http nào được bắt, bởi vì giao thức của gói tin lúc này không phải là http mà là https



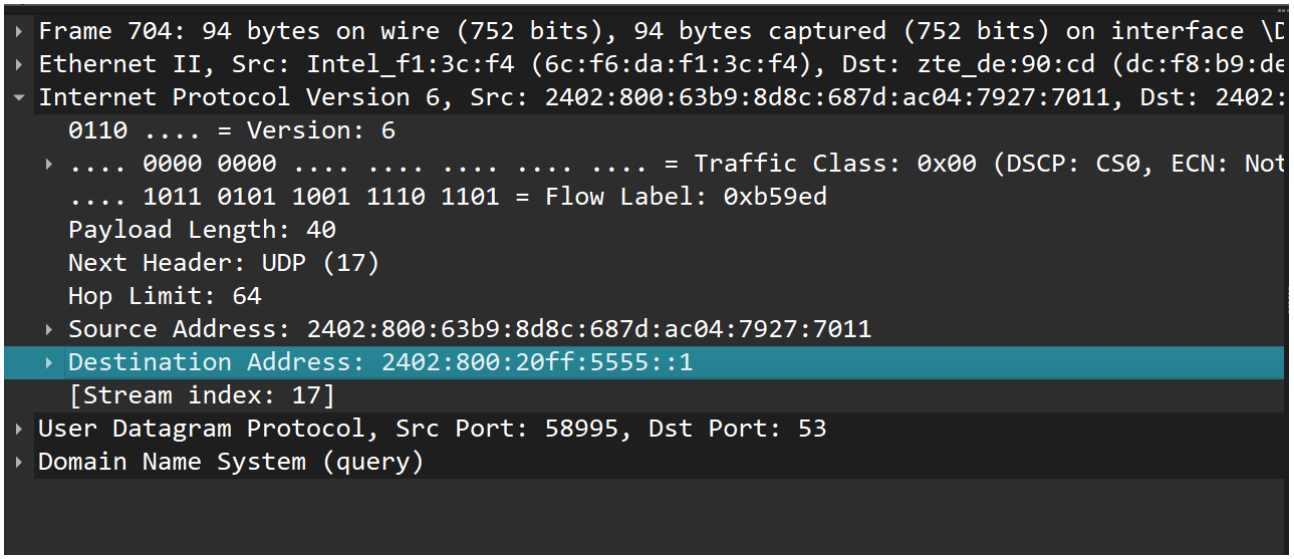
- Trong hình trên thì đúng là có các gói tin http bắt được, nhưng không phải là từ trang web uit.edu.vn mà chúng ta truy cập ban đầu mà đây là nhứng gói tin do các phần mềm khác giao tiếp với nhau và phần mềm Wireshark bắt được

k) Nội dung 11: Tìm cách xác định địa chỉ IP của website đã chọn là bao nhiêu? Địa chỉ IP của máy tính bạn lúc này là bao nhiêu?

- Lúc này, các gói tin không phải giao thức http nữa nên chúng ta không thể dùng cách tương tự như Task 1 để tìm địa chỉ IP của website đã chọn (ở đây là website uit.edu.vn) mà chúng ta sẽ xác định thông qua giao thức DNS.
- Lí do chúng ta xác định địa chỉ IP thông qua DNS: khi chúng ta tìm bằng cách nhập tên miền vào trình duyệt tìm kiếm thì trình duyệt không hiểu được tên miền đó mà phải thông qua một giao thức chuyển đổi tên miền sang địa chỉ IP để trình duyệt có thể truy cập được tới trang web chúng ta mong muốn đó là giao thức DNS. Do đó các gói tin bắt được theo giao thức DNS chắc chắn có gói tin chuyển đổi từ tên miền uit.edu.vn sang địa chỉ IP của tên miền này

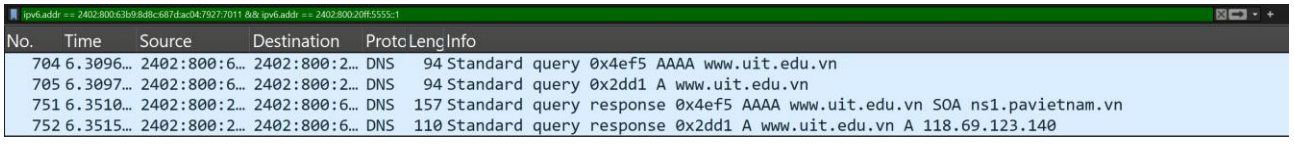


- Lúc này, 4 gói tin chính là các gói tin mà DNS chuyển đổi tên miền uit.edu.vn sang địa chỉ IP của tên miền đó. Do đó chúng ta biết được địa chỉ IP của tên miền uit.edu.vn là 2402:800:20ff:5555::1 (IPv6)

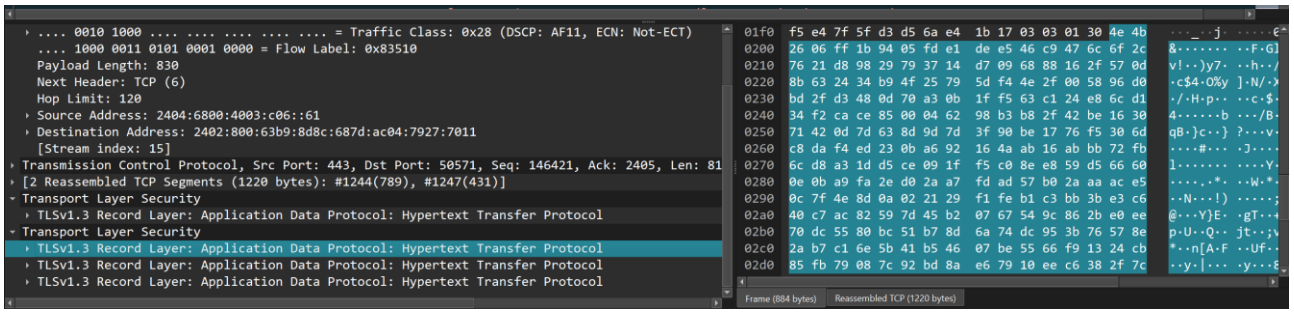


l) Nội dung 12: Sử dụng thành phần packet-display filter để hiển thị đầy đủ quá trình trao đổi gói tin giữa máy tính của bạn và website bằng cú pháp: ip.addr== && ip.addr== . Cho biết rằng bạn có thể thấy được nội dung trả về của website không? Mô tả.

- Vì IP address được định dạng theo Ipv6 nên ta sẽ dùng cú pháp thay thế là ipv6.addr == && ipv6.addr == để tìm kiếm các gói tin



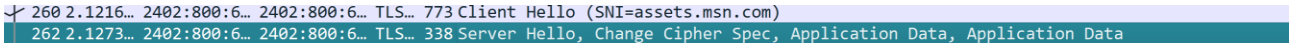
- Ta sẽ không thấy được nội dung trả về của website. Vì HTTPS chính là HTTP chạy trên TLS/SSL do đó HTTP response và request sẽ được mã hóa trước khi gửi qua mạng



- Ta sẽ thấy lúc này Record Layer chỉ là những kí tự được mã hóa nên chúng ta không thể đọc được nội dung trả về từ trang web

m) Nội dung 13: Hãy chỉ ra ít nhất 2 gói tin mà bạn cho rằng quan trọng khi truy cập website này. Tìm hiểu và mô tả ngắn gọn các giao thức này. Giải thích.

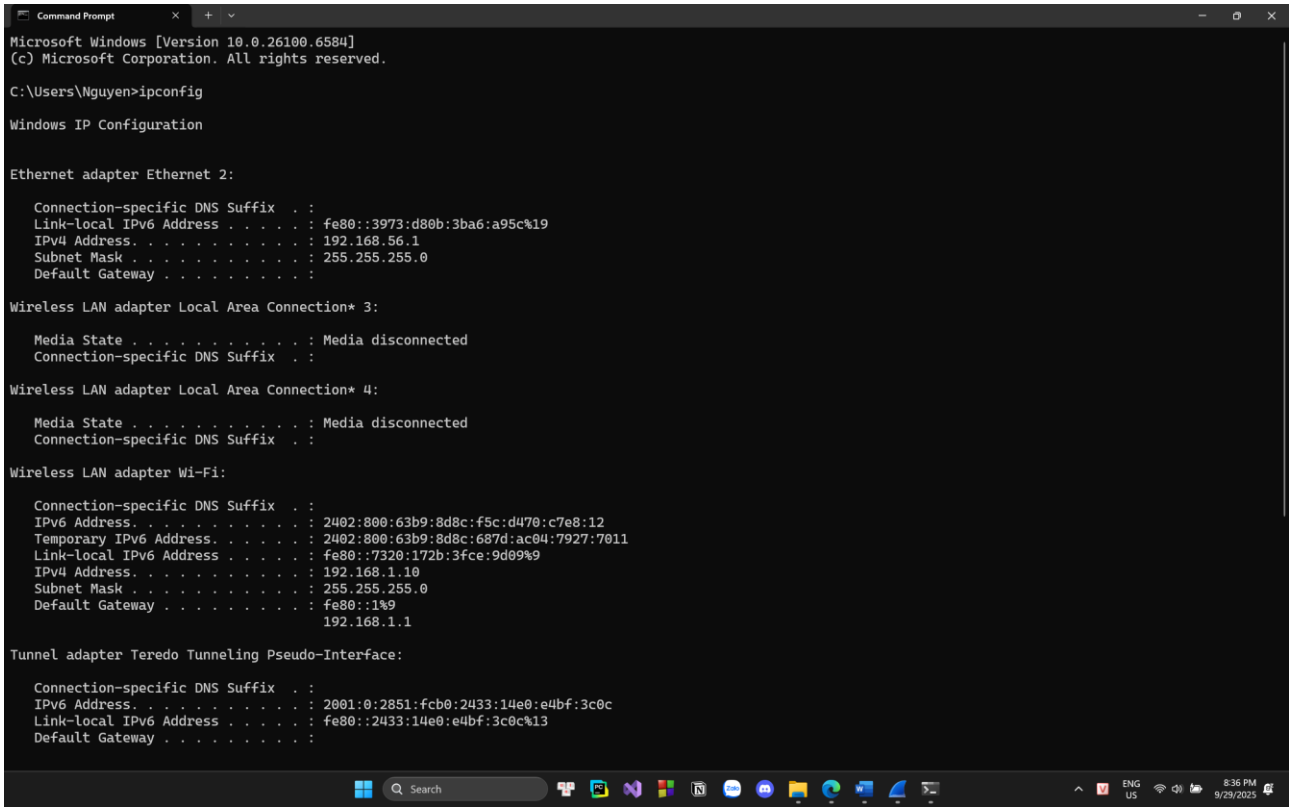
- TLS Client Hello: Gói này do client gửi đến server khi bắt đầu kết nối HTTPS. Đây chính là bước khởi đầu trong quá trình bắt tay TLS.
- TLS ServerHello: Chứng chỉ giúp xác thực danh tính server



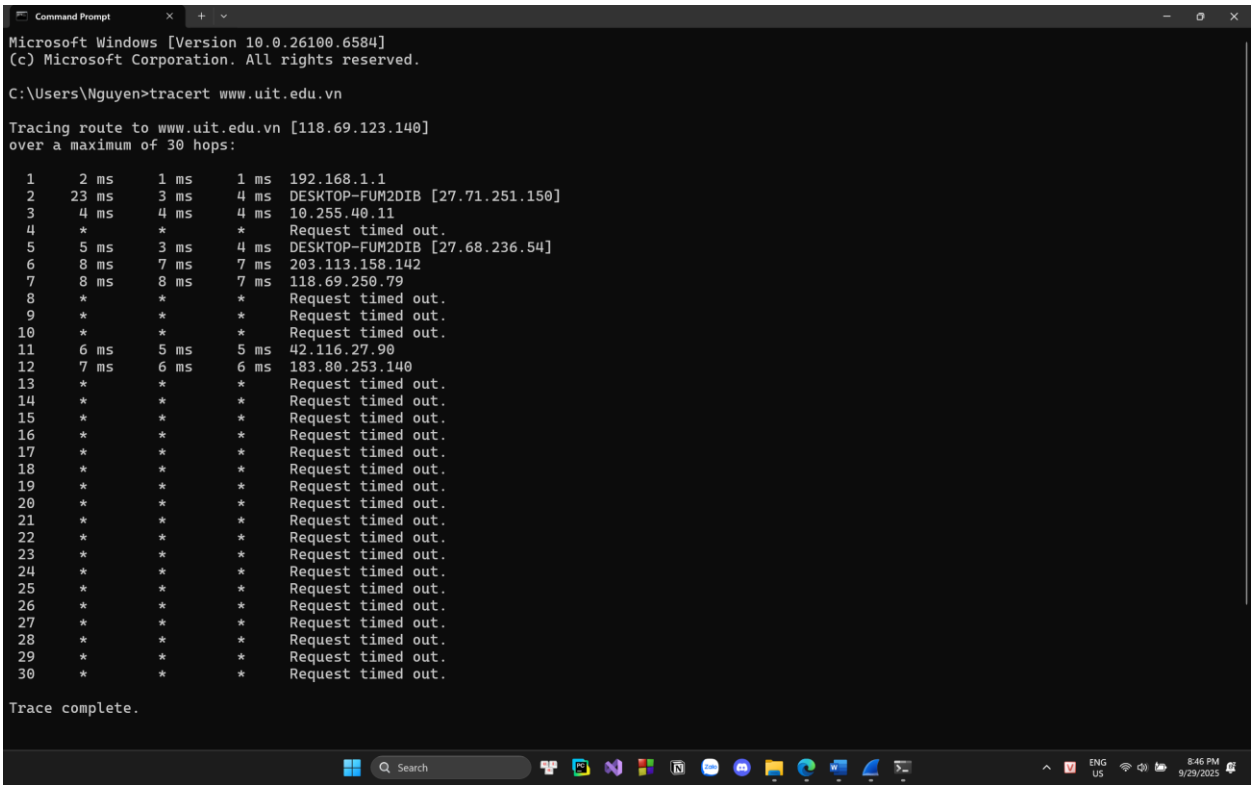
- Các giao thức được sử dụng:
  + TLS (Transport Layer Security): giao thức bảo mật lớp truyền tải và được đảm bảo mã hóa, toàn vẹn, xác thực cho dữ liệu HTTP
  + HTTPS: là HTTP chạy bên trong kênh bảo mật TLS và nội dung được mã hóa, chỉ có client và server giải mã được. Từ đó giúp người dùng truy cập web an toàn

n) Nội dung 14: 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 thực hiện để minh họa điều đó. Tìm được càng nhiều cách càng tốt.

- Cách 1: Sử dụng ipconfig trên terminal: Để thực hiện chúng ta tiến hành mở terminal bằng cách gõ cmd vào thanh tìm kiếm. Sau khi terminal được khởi động, chúng ta tiến hành nhập lệnh “ipconfig” để xem ip của máy chúng ta ở mục Ipv4 address: 192.168.1.0



- Cách 2: Sử dụng lệnh tracert trong cmd để tìm ip của trang web bất kỳ mà chúng ta muốn tìm địa chỉ IP. Để thực hiện chúng ta cũng mở terminal lên và gõ lệnh "tracert <tên_miền_trang_web>. Lúc này chúng ta sẽ biết được đường đi từ máy chúng ta đến server của trang web đó thông qua các hop



- Cách 3: Sử dụng các trang web DNS lookup online để tra. Ở đây ta sử dụng trang web https://whois.domaintools.com để tra cứu IP của google

Whois Record for Google.com

Domain Profile

Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	10,241 days old Created on 1997-09-15 Expires on 2028-09-13 Updated on 2024-08-02
Name Servers	NS1.GOOGLE.COM (has 18,706 domains) NS2.GOOGLE.COM (has 18,706 domains) NS3.GOOGLE.COM (has 18,706 domains) NS4.GOOGLE.COM (has 18,706 domains)
IP Address	142.251.33.68 - 70 other sites hosted on this server
IP Location	- Washington - Seattle - Google
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
IP History	1,159 changes on 1,159 unique IP addresses over 21 years

YÊU CẦU CHUNG

1) Đánh giá

- Chuẩn bị tốt các yêu cầu đặt ra trong bài thực hành.
- Sinh viên hiểu và tự thực hiện được bài thực hành, trả lời đầy đủ các yêu cầu đặt ra.
- Nộp báo cáo kết quả chi tiết những đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả *(nếu có)*; giải thích cho quan sát *(nếu có)*.
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

2) Báo cáo

- File .PDF hoặc .docx. Tập trung vào nội dung, giải thích.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Avo)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: LabX-MSSV1. (trong đó X là Thứ tự buổi Thực hành).
  Ví dụ: Lab01-21520001
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT