

# 1

## BÁO CÁO THỰC HÀNH

**Môn học:** Nhập môn mạng máy tính

**Buổi báo cáo:** Lab 01

**Tên chủ đề:** Làm quen với Wireshark

*GVHD:* Ngô Khánh Khoa

*Ngày thực hiện:* 06/03/2024

*Ngày nộp báo cáo:* 20/03/2024

### **1. THÔNG TIN CHUNG:**

Lớp: IT005.O21.CTTN.1

STT	Họ và tên	MSSV	Email
1	Đoàn Đức Anh	23520041	23520041@gm.uit.edu.vn

# BÁO CÁO CHI TIẾT

---

## 1. Tổng thời gian bắt gói tin trong trang web đã thử nghiệm và tổng số gói tin bắt được:

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

No.	Time	Source	Destination	Protocol	Length	Info
15...	40.425781	172.20.26.104	128.119.245...	TCP	66	59063 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15...	40.475171	172.20.26.104	128.119.245...	TCP	66	59064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15...	40.679088	172.20.26.104	128.119.245...	TCP	66	59065 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15...	40.681396	128.119.245...	172.20.26.104	TCP	66	80 → 59063 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
15...	40.681498	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
15...	40.681701	172.20.26.104	128.119.245...	HTTP	550	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
15...	40.728839	128.119.245...	172.20.26.104	TCP	66	80 → 59064 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
15...	40.729011	172.20.26.104	128.119.245...	TCP	54	59064 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
15...	40.930881	128.119.245...	172.20.26.104	TCP	66	80 → 59065 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
15...	40.931021	172.20.26.104	128.119.245...	TCP	54	59065 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
15...	40.936757	128.119.245...	172.20.26.104	TCP	60	80 → 59063 [ACK] Seq=1 Ack=497 Win=30336 Len=0
15...	40.937552	128.119.245...	172.20.26.104	HTTP	492	HTTP/1.1 200 OK (text/html)
15...	40.981824	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=497 Ack=439 Win=131840 Len=0
15...	41.018288	172.20.26.104	128.119.245...	HTTP	496	GET /favicon.ico HTTP/1.1
15...	41.274409	128.119.245...	172.20.26.104	HTTP	538	HTTP/1.1 404 Not Found (text/html)
15...	41.324833	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=939 Ack=923 Win=131328 Len=0

-Thời gian thử nghiệm: 41.324833 – 40.425781 = 0.899052 (s)

-Tổng số gói tin bắt được: 16 gói tin

\*\*Thời gian trước 41.324833 là lúc truy cập website là https, được bảo mật mã hóa nên không nhận được nhận được flag, tuy nhiên ta có thể sử dụng tls để có thể hiện thị thông tin mong muốn. Bởi vì https là phiên bản bảo mật của http, nó sử dụng tls để mã hóa dữ liệu trước khi gửi qua mạng.

No.	Time	Source	Destination	Protocol	Length	Info
11...	30.930392	172.20.26.104	128.119.245...	TLS	571	Client Hello (SNI=gaia.cs.umass.edu)
11...	31.182631	128.119.245...	172.20.26.104	TLS	14...	Server Hello
11...	31.184004	128.119.245...	172.20.26.104	TLS	12...	Certificate, Server Key Exchange, Server Hello Done
11...	31.195938	172.20.26.104	128.119.245...	TLS	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
11...	31.444324	128.119.245...	172.20.26.104	TLS	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
11...	31.444776	172.20.26.104	128.119.245...	TLS	874	Application Data
11...	31.695946	128.119.245...	172.20.26.104	TLS	322	Application Data
11...	32.041237	172.20.26.104	128.119.245...	TLS	767	Client Hello (SNI=gaia.cs.umass.edu)
11...	32.290968	128.119.245...	172.20.26.104	TLS	191	Server Hello, Change Cipher Spec, Encrypted Handshake Message
11...	32.291367	172.20.26.104	128.119.245...	TLS	105	Change Cipher Spec, Encrypted Handshake Message
11...	33.132265	128.119.245...	172.20.26.104	TLS	85	Encrypted Alert
11...	33.133528	128.119.245...	172.20.26.104	TLS	85	Encrypted Alert

-Tại tcp.stream eq 29:

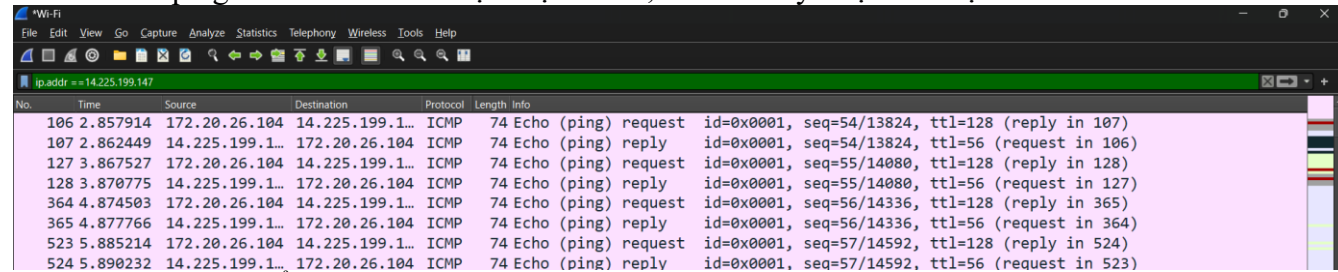
No.	Time	Source	Destination	Protocol	Length	Info
15...	40.425781	172.20.26.104	128.119.245...	TCP	66	59063 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
15...	40.681396	128.119.245...	172.20.26.104	TCP	66	80 → 59063 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM WS=128
15...	40.681498	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
15...	40.681701	172.20.26.104	128.119.245...	HTTP	550	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
15...	40.936757	128.119.245...	172.20.26.104	TCP	60	80 → 59063 [ACK] Seq=1 Ack=497 Win=30336 Len=0
15...	40.937552	128.119.245...	172.20.26.104	HTTP	492	HTTP/1.1 200 OK (text/html)
15...	40.981824	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=497 Ack=439 Win=131840 Len=0
15...	41.018288	172.20.26.104	128.119.245...	HTTP	496	GET /favicon.ico HTTP/1.1
15...	41.274409	128.119.245...	172.20.26.104	HTTP	538	HTTP/1.1 404 Not Found (text/html)
15...	41.324833	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=939 Ack=923 Win=131328 Len=0
15...	42.091801	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [FIN, ACK] Seq=939 Ack=923 Win=131328 Len=0
15...	43.161954	128.119.245...	172.20.26.104	TCP	60	80 → 59063 [FIN, ACK] Seq=923 Ack=940 Win=31360 Len=0
16...	43.162037	172.20.26.104	128.119.245...	TCP	54	59063 → 80 [ACK] Seq=940 Ack=924 Win=131328 Len=0

+Tổng thời gian thực hiện gói tin: 0.511771000 seconds

+Tổng số gói tin bắt được: 13

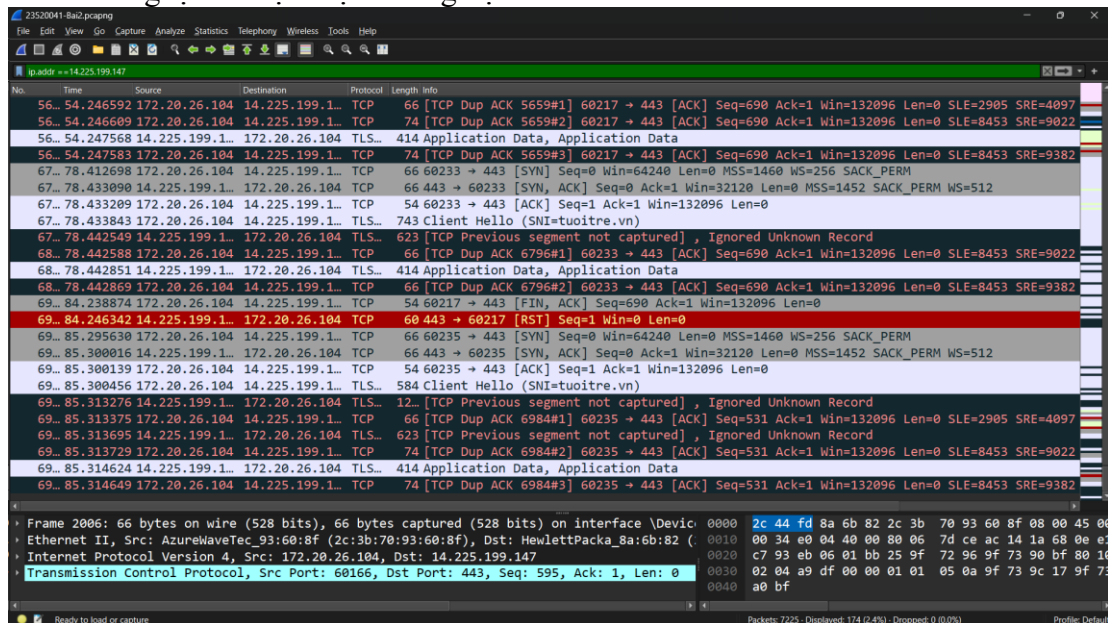
\*Ở website thứ hai: [tuoitre.vn](http://tuoitre.vn)

-Đầu tiên ta ping [tuoitre.vn](http://tuoitre.vn) để xác định địa chỉ IP, hành vi này được thể hiện trên wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
106	2.857914	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (reply in 107)
107	2.862449	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=54/13824, ttl=56 (request in 106)
127	3.867527	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 128)
128	3.870775	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=56 (request in 127)
364	4.874503	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (reply in 365)
365	4.877766	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=56/14336, ttl=56 (request in 364)
523	5.885214	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (reply in 524)
524	5.890232	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=56 (request in 523)

- Sau đó ta dùng lại để thực hiện thử nghiệm:



No.	Time	Source	Destination	Protocol	Length	Info
56	54.246592	172.20.26.104	14.225.199.1...	TCP	66	[TCP Dup ACK 5659#1] 60217 → 443 [ACK] Seq=690 Ack=1 Win=132096 Len=0 SLE=2905 SRE=4097
56	54.246609	172.20.26.104	14.225.199.1...	TCP	74	[TCP Dup ACK 5659#2] 60217 → 443 [ACK] Seq=690 Ack=1 Win=132096 Len=0 SLE=8453 SRE=9022
56	54.247568	14.225.199.1...	172.20.26.104	TLS...	414	Application Data, Application Data
56	54.247583	172.20.26.104	14.225.199.1...	TCP	74	[TCP Dup ACK 5659#3] 60217 → 443 [ACK] Seq=690 Ack=1 Win=132096 Len=0 SLE=8453 SRE=9382
67	78.412698	172.20.26.104	14.225.199.1...	TCP	66	60233 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
67	78.433090	14.225.199.1...	172.20.26.104	TCP	66	443 → 60233 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1452 SACK_PERM WS=512
67	78.433209	172.20.26.104	14.225.199.1...	TCP	54	60233 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
67	78.433843	172.20.26.104	14.225.199.1...	TLS...	743	Client Hello (SNI=tuoitre.vn)
67	78.442549	14.225.199.1...	172.20.26.104	TLS...	623	[TCP Previous segment not captured], Ignored Unknown Record
68	78.442869	172.20.26.104	14.225.199.1...	TCP	66	[TCP Dup ACK 6796#1] 60233 → 443 [ACK] Seq=690 Ack=1 Win=132096 Len=0 SLE=8453 SRE=9022
68	78.442851	14.225.199.1...	172.20.26.104	TLS...	414	Application Data, Application Data
68	78.442869	172.20.26.104	14.225.199.1...	TCP	66	[TCP Dup ACK 6796#2] 60233 → 443 [ACK] Seq=690 Ack=1 Win=132096 Len=0 SLE=8453 SRE=9382
69	84.238874	172.20.26.104	14.225.199.1...	TCP	54	60217 → 443 [FIN, ACK] Seq=690 Ack=1 Win=132096 Len=0
69	84.246342	14.225.199.1...	172.20.26.104	TCP	60	443 → 60217 [RST] Seq=1 Win=0 Len=0
69	85.295630	172.20.26.104	14.225.199.1...	TCP	66	60235 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
69	85.300016	14.225.199.1...	172.20.26.104	TCP	66	443 → 60235 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1452 SACK_PERM WS=512
69	85.300139	172.20.26.104	14.225.199.1...	TCP	54	60235 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
69	85.300456	172.20.26.104	14.225.199.1...	TLS...	584	Client Hello (SNI=tuoitre.vn)
69	85.313276	14.225.199.1...	172.20.26.104	TLS...	12	[TCP Previous segment not captured], Ignored Unknown Record
69	85.313375	172.20.26.104	14.225.199.1...	TCP	66	[TCP Dup ACK 6984#1] 60235 → 443 [ACK] Seq=531 Ack=1 Win=132096 Len=0 SLE=2905 SRE=4097
69	85.313695	14.225.199.1...	172.20.26.104	TLS...	623	[TCP Previous segment not captured], Ignored Unknown Record
69	85.313729	172.20.26.104	14.225.199.1...	TCP	74	[TCP Dup ACK 6984#2] 60235 → 443 [ACK] Seq=531 Ack=1 Win=132096 Len=0 SLE=8453 SRE=9022
69	85.314624	14.225.199.1...	172.20.26.104	TLS...	414	Application Data, Application Data
69	85.314649	172.20.26.104	14.225.199.1...	TCP	74	[TCP Dup ACK 6984#3] 60235 → 443 [ACK] Seq=531 Ack=1 Win=132096 Len=0 SLE=8453 SRE=9382

-Tổng thời gian thử nghiệm: 85.314649 – 2.857914 = 82.456735.

-Tổng số gói tin bắt được: 174

\*\*Vì quá nhiều gói tin nên ta có thể dùng cách dễ dàng và hiệu quả hơn:

File -> Export Specified Packets... -> All

## 2. 5 Giao thức khác nhau xuất hiện trong cột giao thức(Protocol) khi không áp dụng bộ lọc:

### 1. ARP (Address Resolution Protocol):

- Chức năng: Chuyển đổi địa chỉ IP (địa chỉ logic) sang địa chỉ MAC (địa chỉ vật lý) trên mạng LAN.
- Ví dụ: Khi bạn nhập địa chỉ website (URL) vào trình duyệt, ARP giúp máy tính của bạn tìm địa chỉ vật lý (địa chỉ MAC) của thiết bị lưu trữ website trên mạng của bạn.

### 2. DHCP (Dynamic Host Configuration Protocol):

- Chức năng: Tự động gán địa chỉ IP và các cài đặt cấu hình mạng khác cho các thiết bị trên mạng.
- Ví dụ: Khi bạn kết nối một thiết bị mới với mạng của mình, DHCP tự động gán cho thiết bị đó một địa chỉ IP, mặt nạ mạng con và các cài đặt khác cần thiết để giao tiếp với các thiết bị khác.

### 3. DNS (Domain Name System):

- Chức năng: Chuyển đổi tên miền dễ đọc (ví dụ: "[đã xoá URL không hợp lệ]") thành địa chỉ IP (ví dụ: "172.217.160.66") mà máy tính sử dụng để giao tiếp.
- Ví dụ: Khi bạn nhập "[đã xoá URL không hợp lệ]" vào trình duyệt, DNS sẽ chuyển đổi nó sang địa chỉ IP của máy chủ Google, cho phép máy tính của bạn kết nối và hiển thị trang web.

#### 4. QUIC (Quick UDP Internet Connections):

- Chức năng: Giao thức vận tải được xây dựng trên UDP nhằm cải thiện hiệu suất và bảo mật của kết nối web so với TCP truyền thống.
- Ví dụ: QUIC được sử dụng trong các giao thức như HTTP/3, cung cấp tốc độ tải nhanh hơn và kiểm soát tắc nghẽn tốt hơn cho việc duyệt web.

#### 5. SSDP (Simple Service Discovery Protocol):

- Chức năng: Được sử dụng để quảng cáo và khám phá các thiết bị và dịch vụ trên mạng cục bộ.
- Ví dụ: SSDP được sử dụng trong các ứng dụng như UPnP (Universal Plug and Play), cho phép các thiết bị như TV thông minh hoặc máy chủ phương tiện thông báo sự hiện diện và khả năng của chúng cho các thiết bị khác trên mạng.

#### 6. TCP (Transmission Control Protocol):

- Chức năng: Giao thức đáng tin cậy, hướng kết nối đảm bảo dữ liệu đến đúng thứ tự và không bị lỗi.
- Ví dụ: TCP được sử dụng cho các ứng dụng như truyền tệp, email và duyệt web, nơi đảm bảo tính toàn vẹn và độ tin cậy của dữ liệu là rất quan trọng.

#### 7. TLS (Transport Layer Security):

- Chức năng: Cung cấp giao tiếp an toàn qua TCP bằng cách mã hóa dữ liệu và xác thực các bên liên quan.
- Ví dụ: TLS được sử dụng trong các ứng dụng như HTTPS (HTTP an toàn) để bảo vệ dữ liệu nhạy cảm như thông tin đăng nhập và thông tin thanh toán.

#### 8. UDP (User Datagram Protocol):

Chức năng: Gửi các datagram (đơn vị dữ liệu) độc lập đến một điểm đến cụ thể.  
Ví dụ: Truyền phát video, âm thanh, trò chơi trực tuyến, DNS, DHCP, SNMP.

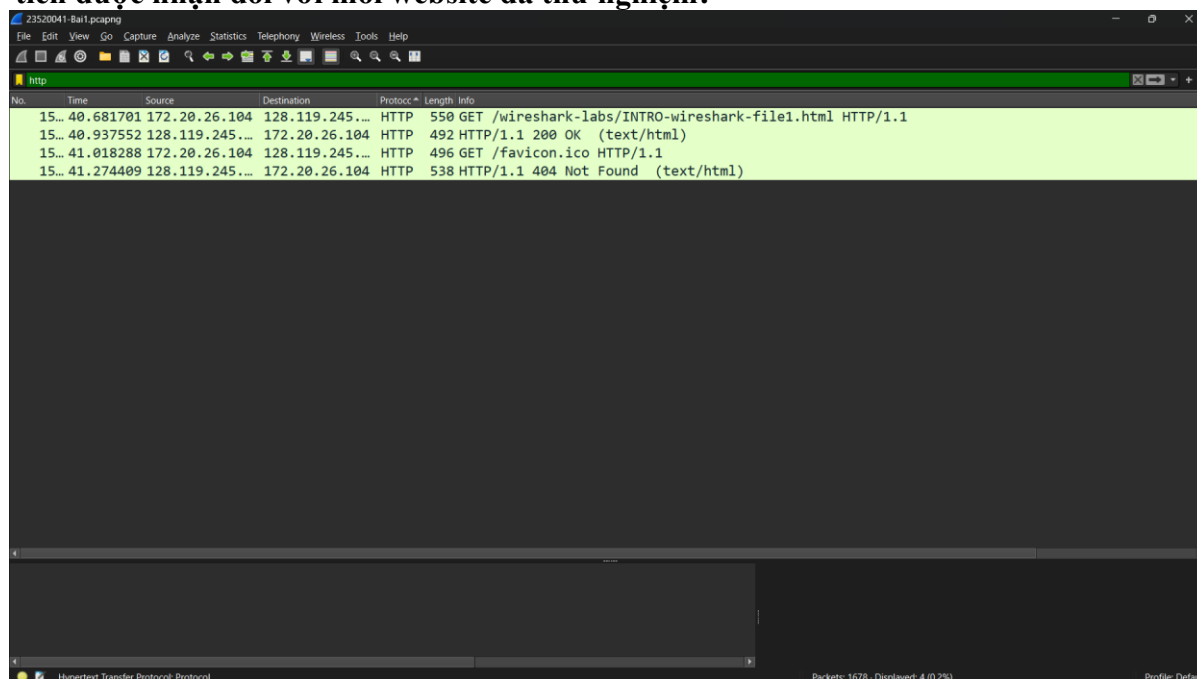
#### 9. SSL (Secure Sockets Layer):

Chức năng: Mã hóa dữ liệu, xác thực máy chủ và máy khách, bảo mật thông tin liên lạc.  
Ví dụ: HTTPS, VPN, email, FTP, IM.

#### 10. MNDP (Multicast Neighbor Discovery Protocol):

Chức năng: Cho phép các thiết bị thông báo sự hiện diện của mình và thu thập thông tin về các thiết bị khác trên cùng mạng.

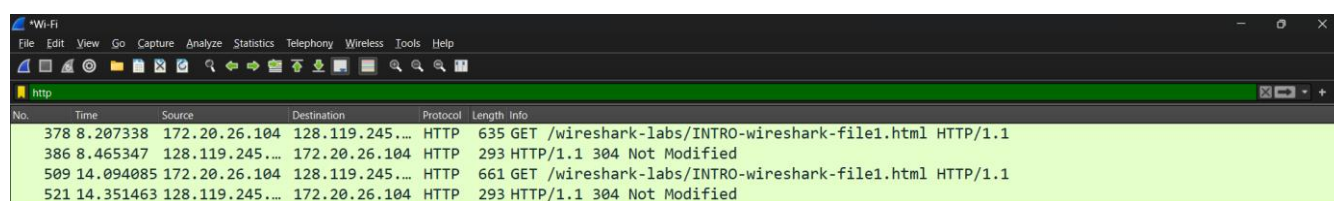
3. Thời gian từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm:



No.	Time	Source	Destination	Protocol	Length	Info
15...	40.681701	172.20.26.104	128.119.245...	HTTP	550	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
15...	40.937552	128.119.245...	172.20.26.104	HTTP	492	HTTP/1.1 200 OK (text/html)
15...	41.018288	172.20.26.104	128.119.245...	HTTP	496	GET /favicon.ico HTTP/1.1
15...	41.274409	128.119.245...	172.20.26.104	HTTP	538	HTTP/1.1 404 Not Found (text/html)

-Thời gian:  $40.937552 - 40.681701 = 0.255851(s)$

\* 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:



No.	Time	Source	Destination	Protocol	Length	Info
378	8.207338	172.20.26.104	128.119.245...	HTTP	635	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
386	8.465347	128.119.245...	172.20.26.104	HTTP	293	HTTP/1.1 304 Not Modified
509	14.094085	172.20.26.104	128.119.245...	HTTP	661	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
521	14.351463	128.119.245...	172.20.26.104	HTTP	293	HTTP/1.1 304 Not Modified

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 2:**



No	Time	Source	Destination	Protocol	Length	Info
106	2.857914	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=54/13824, ttl=128 (reply in 107)
107	2.862449	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=54/13824, ttl=56 (request in 106)
127	3.867527	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=128 (reply in 128)
128	3.870775	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=55/14080, ttl=56 (request in 127)
364	4.874503	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (reply in 365)
365	4.877766	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=56/14336, ttl=56 (request in 364)
523	5.885214	172.20.26.104	14.225.199.1...	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (reply in 524)
524	5.890232	14.225.199.1...	172.20.26.104	ICMP	74	Echo (ping) reply id=0x0001, seq=57/14592, ttl=56 (request in 523)
13...	10.504643	172.20.26.104	14.225.199.1...	TCP	54	60118 → 443 [FIN, ACK] Seq=1 Ack=1 Win=516 Len=0
13...	10.509437	14.225.199.1...	172.20.26.104	TCP	60	443 → 60118 [RST] Seq=1 Win=0 Len=0
19...	20.940428	172.20.26.104	14.225.199.1...	TCP	66	60166 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19...	20.945599	14.225.199.1...	172.20.26.104	TCP	66	443 → 60166 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1452 SACK_PERM WS=512
20...	20.945723	172.20.26.104	14.225.199.1...	TCP	54	60166 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
20...	20.946251	172.20.26.104	14.225.199.1...	TLS...	648	Client Hello (SNI=tuoitre.vn)

-Thời gian mà từ lúc gửi yêu cầu đến khi máy chủ phản hồi:  $20.945723 - 20.940428 = 0.005295(s)$ .

**\*\*Client Hello** cho thấy ta đã thành công trong việc truy cập website, tuy nhiên một vài lần dưới có thể do wifi máy tính hiện tại hoặc do website bị lỗi nên không thành công truy cập: *Bad request*

20...	21.043933	172.20.26.104	14.225.199.1...	TCP	66	60169 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
20...	21.048497	14.225.199.1...	172.20.26.104	TCP	66	80 → 60169 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1452 SACK_PERM WS=512
20...	21.048566	172.20.26.104	14.225.199.1...	TCP	54	60169 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
21...	23.916795	172.20.26.104	14.225.199.1...	TCP	54	60169 → 80 [FIN, ACK] Seq=1 Ack=1 Win=132096 Len=0
21...	23.921153	14.225.199.1...	172.20.26.104	HTTP	261	HTTP/1.1 400 Bad request (text/html)

#### 4. Nội dung hiển thị trên trang web [gaia.cs.umass.edu](http://gaia.cs.umass.edu) “Congratulations! You've downloaded the first Wireshark lab file!” có nằm trong các gói tin HTTP bắt được:

-Mở gói tin HTTP 200:

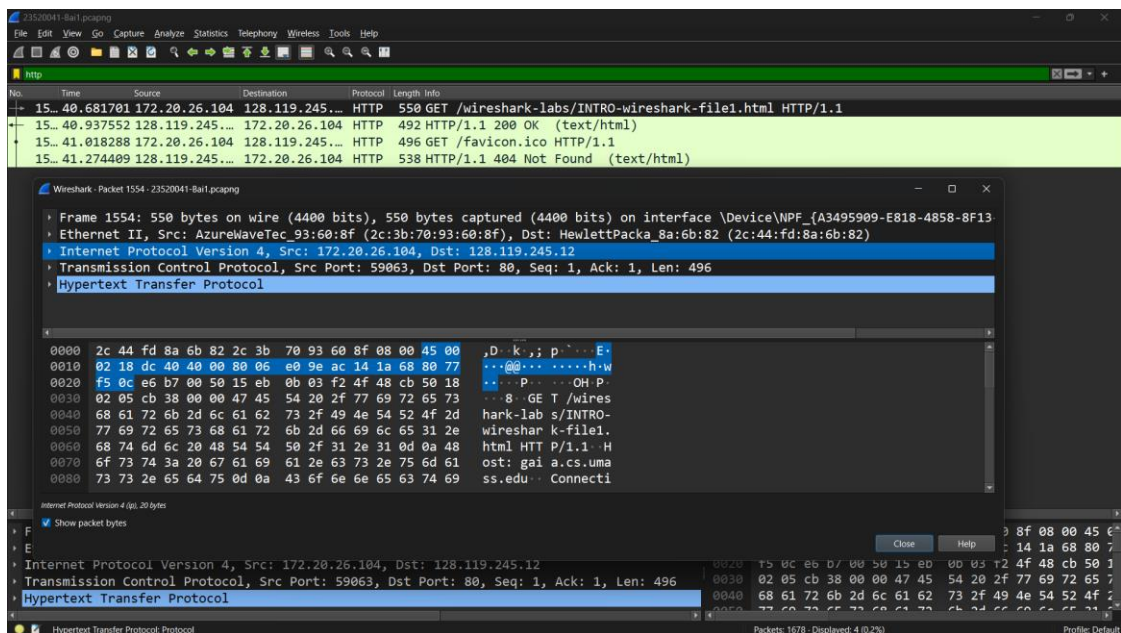
20250004.Bair.pnaging

</

#### 5. Địa chỉ IP của [gaia.cs.umass.edu](http://gaia.cs.umass.edu) và website đã chọn ở bước 10, địa chỉ IP của máy tính đang sử dụng :

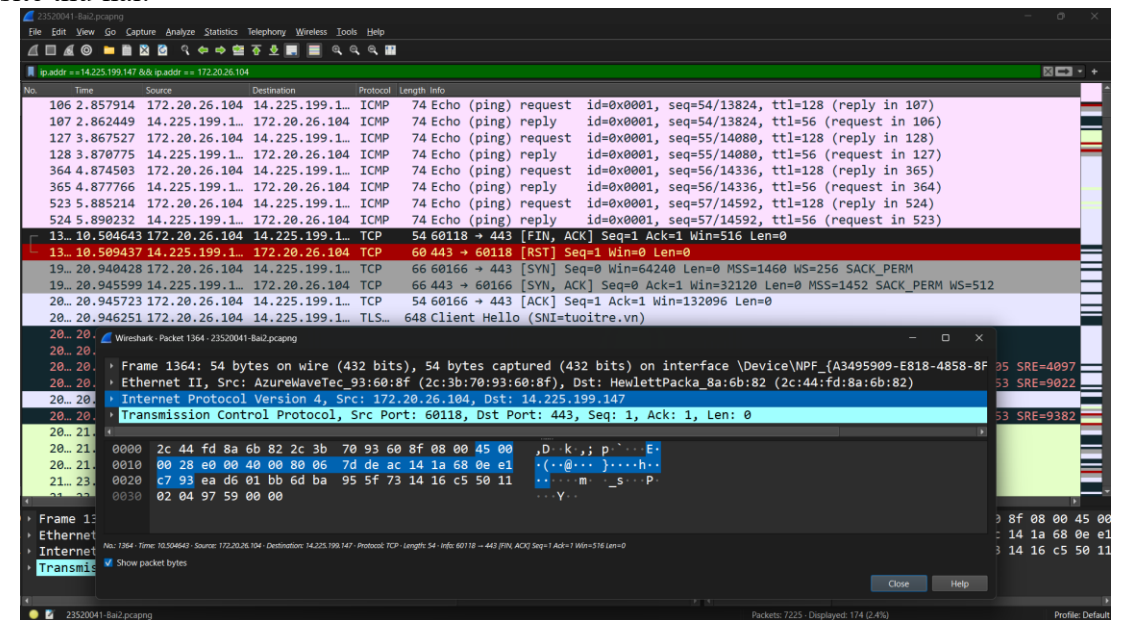
Dựa vào mục Source và Destination, ta có thể xác định được địa chỉ IP của website đã chọn ở bước 10 và máy tính:

*\*Ở website thứ nhất:*



+Địa chỉ IP của website thứ nhất([Trường Đại học Công nghệ Thông tin - UIT](http://128.119.245.12)):  
128.119.245.12

\*Ở website thứ hai:



+Địa chỉ IP của website thứ hai([Báo Tuổi Trẻ - Tin tức mới nhất, tin nhanh, tin nóng 24h \(tuoitre.vn\)](http://14.225.199.147)):  
14.225.199.147

-Địa chỉ IP của máy tính đang sử dụng(địa chỉ IP mạng Wifi đang sử dụng) :172.20.26.104

## 6. 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.

Diễn biến truy cập trang web qua Wireshark:

### 1. Yêu cầu DNS:

- Trình duyệt web gửi yêu cầu DNS đến máy chủ DNS để lấy địa chỉ IP của trang web.
- Máy chủ DNS trả về địa chỉ IP của trang web.

### 2. Kết nối TCP:

Trình duyệt web kết nối với máy chủ web bằng giao thức TCP.

### 3. Yêu cầu HTTP:

Trình duyệt web gửi yêu cầu HTTP đến máy chủ web.

Yêu cầu HTTP bao gồm phương thức (GET, POST, PUT, DELETE), URL, header, và body.

### 4. Phản hồi HTTP:

Máy chủ web gửi phản hồi HTTP đến trình duyệt web.

Phản hồi HTTP bao gồm mã trạng thái (200 OK, 404 Not Found, 500 Internal Server Error,...), header, và body.

### 5. Xử lý nội dung:

Trình duyệt web xử lý nội dung HTML, CSS, JavaScript, hình ảnh, video, v.v.

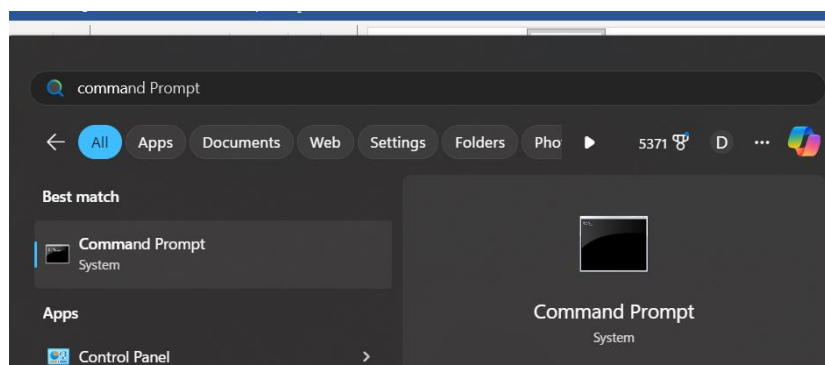
Trình duyệt web hiển thị trang web cho người dùng.

**\*\* 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 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.

\*Xem IP của máy tính:

Ta mở command prompt:



-Thực hiện lệnh: ipconfig

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::7908:d0e3:9317:fda0%18
IPv4 Address. . . . . : 172.20.26.104
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.20.0.1
```

-Ta thấy được địa chỉ IP của máy tính(wifi máy tính đang sử dụng): 172.20.26.104

\*Xem địa chỉ IP của một website:

+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 tuoitre.vn, ta thực hiện như sau:



```
C:\Users\DucAnh>ping tuoitre.vn
```

```
Pinging tuoitre.vn [14.225.199.147] with 32 bytes of data:  
Reply from 14.225.199.147: bytes=32 time=4ms TTL=56  
Reply from 14.225.199.147: bytes=32 time=3ms TTL=56  
Reply from 14.225.199.147: bytes=32 time=3ms TTL=56  
Reply from 14.225.199.147: bytes=32 time=5ms TTL=56
```

```
Ping statistics for 14.225.199.147:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

-Địa chỉ IP của website tuoitre.vn là 14.225.199.147