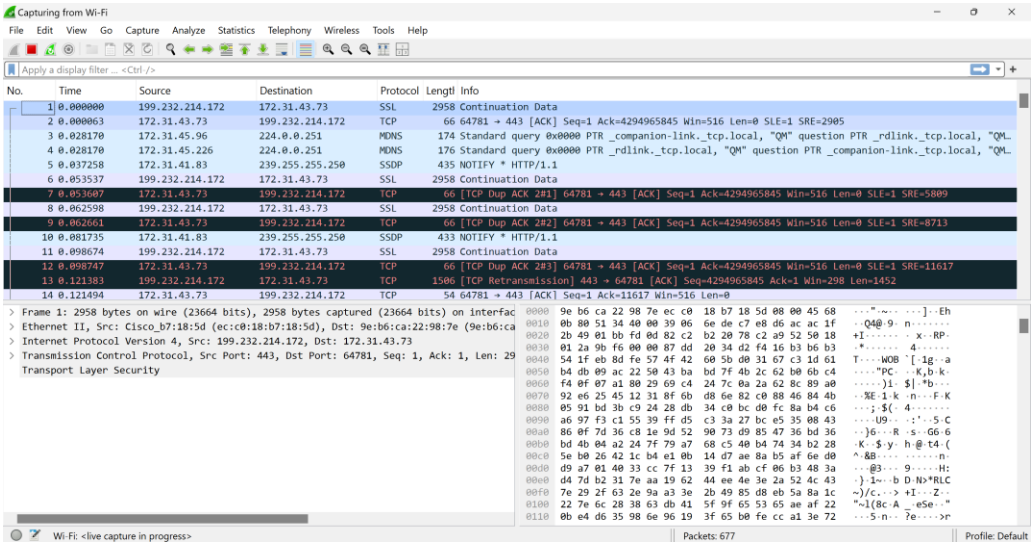
Họ và tên	Mã sinh viên
Hà Quang Vinh	22174600065
Lưu Nhật Nam	22174600109

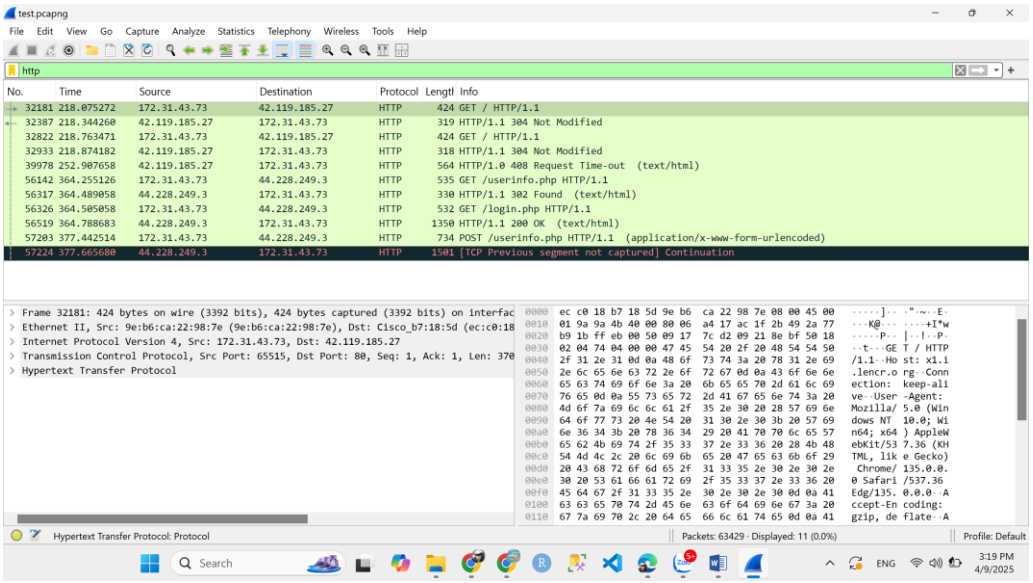
Lớp: DHKL16A2HN

BÁO CÁO BÀI THỰC HÀNH 4

Bước 1: Chọn card mạng wifi

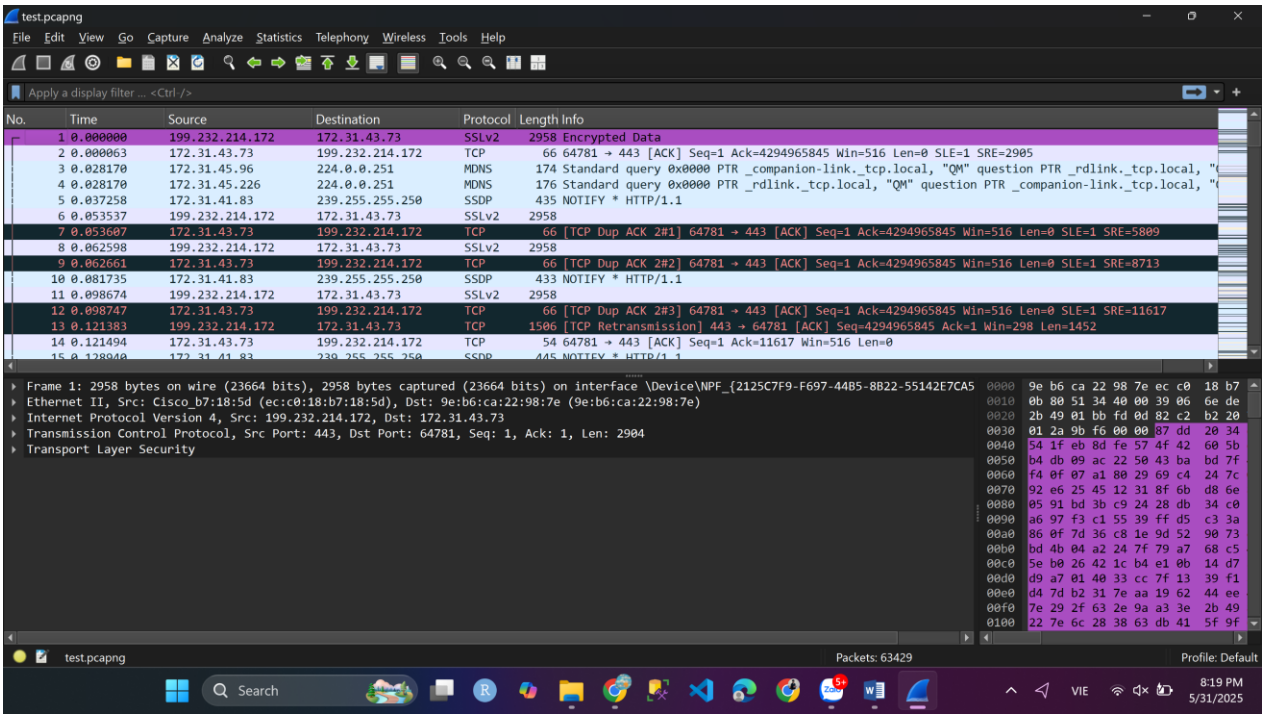


Bước 2: lọc giao thức http



Bước 3: Lưu file kết quả bắt gói

-Lưu file dưới tên test.pcapng



Bước 4:

Tầng 2 – Data Link Giao thức: Ethernet II.

Địa chỉ MAC: MAC nguồn: 9e:b6:ca:22:98:7e

MAC đích: ec:c0:18:b7:18:5d

Loại giao thức: 0x0800 -> IPv4.

Tầng 3 – Network Giao thức: IPv4.

Địa chỉ IP: IP nguồn: 172.31.43.73

IP đích: 44.228.249.3 TTL: 128 -> gợi ý hệ điều hành gửi có thể là Windows.

Tầng 4 – Transport Giao thức: TCP.

Cổng: Source port: 49242 Destination port: 80 (HTTP).

Flags: PSH, ACK -> đang đẩy dữ liệu tới máy chủ.

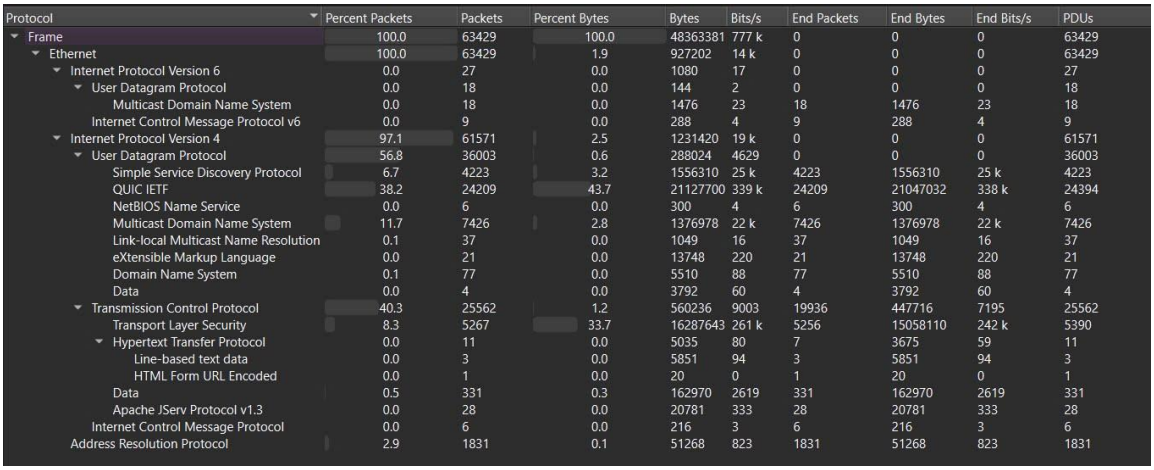
Sequence/Ack number: thể hiện đây là gói mang dữ liệu ứng dụng. TCP payload length: 481 bytes → có chứa dữ liệu ở tầng Application.

Tầng 5 – Session Dữ liệu session nằm trong quá trình TCP connection: sequence/ack + PSH/ACK thể hiện một phiên TCP đang hoạt động. Không có giao thức session độc lập như SIP/NetBIOS.

Tầng 6 – Presentation Không có SSL/TLS → dữ liệu không được mã hóa. Dữ liệu tầng Application (HTTP) được truyền dưới dạng plain text.

Tầng 7 – Application Giao thức: HTTP.

Bước 5:



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	63429	100.0	48363381	777 k	0	0	0	63429
Ethernet	100.0	63429	1.9	927202	14 k	0	0	0	63429
Internet Protocol Version 6	0.0	27	0.0	1080	17	0	0	0	27
User Datagram Protocol	0.0	18	0.0	144	2	0	0	0	18
Multicast Domain Name System	0.0	18	0.0	1476	23	18	1476	23	18
Internet Control Message Protocol v6	0.0	9	0.0	288	4	9	288	4	9
Internet Protocol Version 4	97.1	61571	2.5	1231420	19 k	0	0	0	61571
User Datagram Protocol	56.8	36003	0.6	288024	4629	0	0	0	36003
Simple Service Discovery Protocol	6.7	4223	3.2	1556310	25 k	4223	1556310	25 k	4223
QUIC IETF	38.2	24209	43.7	21127700	339 k	24209	21047032	338 k	24394
NetBIOS Name Service	0.0	6	0.0	300	4	6	300	4	6
Multicast Domain Name System	11.7	7426	2.8	1376978	22 k	7426	1376978	22 k	7426
Link-local Multicast Name Resolution	0.1	37	0.0	1049	16	37	1049	16	37
eXtensible Markup Language	0.0	21	0.0	13748	220	21	13748	220	21
Domain Name System	0.1	77	0.0	5510	88	77	5510	88	77
Data	0.0	4	0.0	3792	60	4	3792	60	4
Transmission Control Protocol	40.3	25562	1.2	560236	9003	19936	447716	7195	25562
Transport Layer Security	8.3	5267	33.7	16287643	261 k	5256	15058110	242 k	5390
Hypertext Transfer Protocol	0.0	11	0.0	5035	80	7	3675	59	11
Line-based text data	0.0	3	0.0	5851	94	3	5851	94	3
HTML Form URL Encoded	0.0	1	0.0	20	0	1	20	0	1
Data	0.5	331	0.3	162970	2619	331	162970	2619	331
Apache JServ Protocol v1.3	0.0	28	0.0	20781	333	28	20781	333	28
Internet Control Message Protocol	0.0	6	0.0	216	3	6	216	3	6
Address Resolution Protocol	2.9	1831	0.1	51268	823	1831	51268	823	1831

-Phân tích:

1. Tầng IP – Phân bổ IPv4 / IPv6

IPv4 chiếm ưu thế tuyệt đối: 97.1% số packet

IPv6 gần như không có (chỉ 27 packet, 0% dung lượng)

-Tập trung vào phân tích IPv4 là hợp lý.

2. Tầng Transport (UDP/TCP)

UDP – 56.8% số packet, nhưng chỉ chiếm 0.6% dung lượng

QUIC (chiếm 38.2%): Dấu hiệu sử dụng HTTP/3 hoặc Chrome truy cập site hỗ trợ QUIC.

TCP – 40.3% số packet, nhưng chiếm đến 1.2% dung lượng

Chủ yếu phục vụ TLS và HTTP.

3. Application Layer

Transport Layer Security (TLS) – 33.7% dung lượng

Gói mã hóa, khả năng là HTTPS.

Rất nhiều lưu lượng đang được mã hóa, không thấy nội dung bên trong.

HTTP – Chiếm rất nhỏ:

Chỉ có 11 packet (0%) không mã hóa (HTTP thô)

Gồm: GET, HTML Form, line-based text

- Chính là đoạn bạn đang theo dõi (/userinfo.php)

-Một số giao thức khác:

Apache JServ Protocol v1.3 (AJP): Web server Java (Tomcat) đang chạy.

XML, mDNS, DNS, SSDP, NetBIOS: chủ yếu để định danh thiết bị trong mạng nội bộ.

Bước 6: Viết mã Python dùng thư viện PyShark để truy xuất thông tin tầng 2 và tầng 3 từ file .pcapng.

-Một số kết quả chạy được từ phân tích gói tin:

```
Đang phân tích tối đa 10 gói tin...

GÓI TIN #1
  Ethernet:
    • MAC nguồn     : ec:c0:18:b7:18:5d
    • MAC đích      : 9e:b6:ca:22:98:7e
    • Loại Ethernet : 0x0800
  IPv4:
    • IP nguồn      : 199.232.214.172
    • IP đích       : 172.31.43.73
    • TTL           : 57
    • Protocol      : 6
--------------------------------------------------
GÓI TIN #2
  Ethernet:
    • MAC nguồn     : 9e:b6:ca:22:98:7e
    • MAC đích      : ec:c0:18:b7:18:5d
    • Loại Ethernet : 0x0800
  IPv4:
    • IP nguồn      : 172.31.43.73
    • IP đích       : 199.232.214.172
    • TTL           : 128
    • Protocol      : 6
--------------------------------------------------
GÓI TIN #3
  Ethernet:
    • MAC nguồn     : 0e:96:a8:05:d0:1d
    • MAC đích      : 9e:b6:ca:22:98:7e
    • Loại Ethernet : 0x0800
  IPv4:
    • IP nguồn      : 172.31.45.96
    • IP đích       : 224.0.0.251
    • TTL           : 255
    • Protocol      : 17
--------------------------------------------------
```