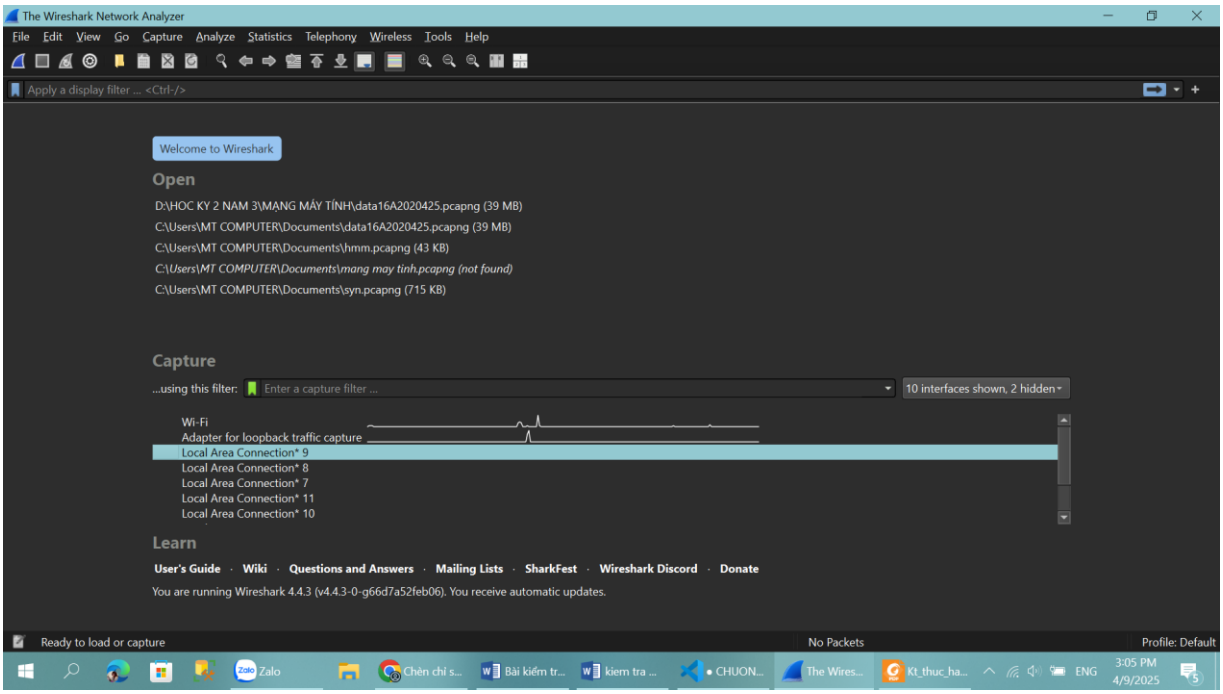
Phạm Thị Trà Giang	22174600025
Trần Trọng Chinh	22174600017

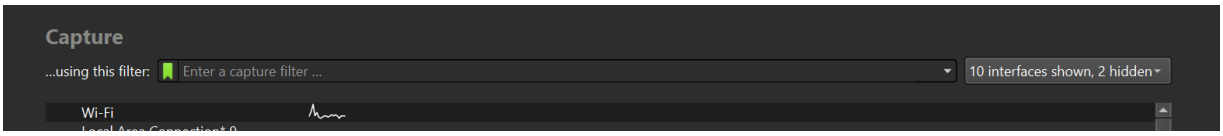
BÀI THỰC HÀNH 4 – PHIÊN TỔNG HỢP (LỚP K16A2)

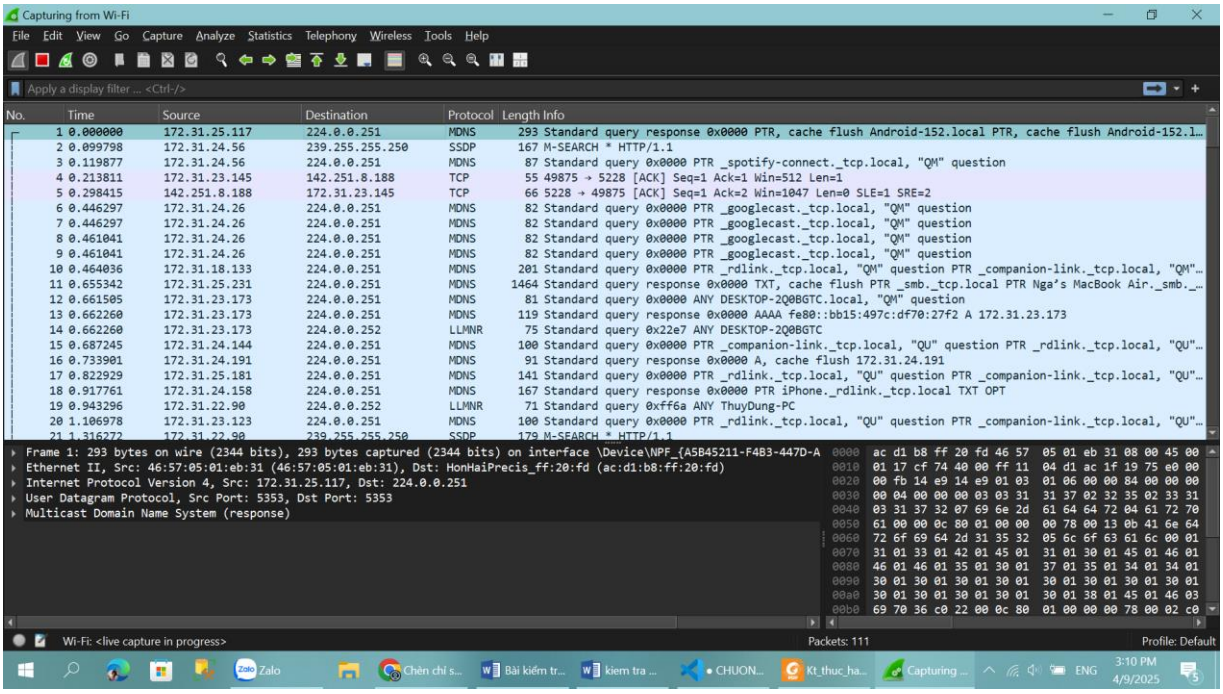
Bước 1 :

Mở Wireshark :



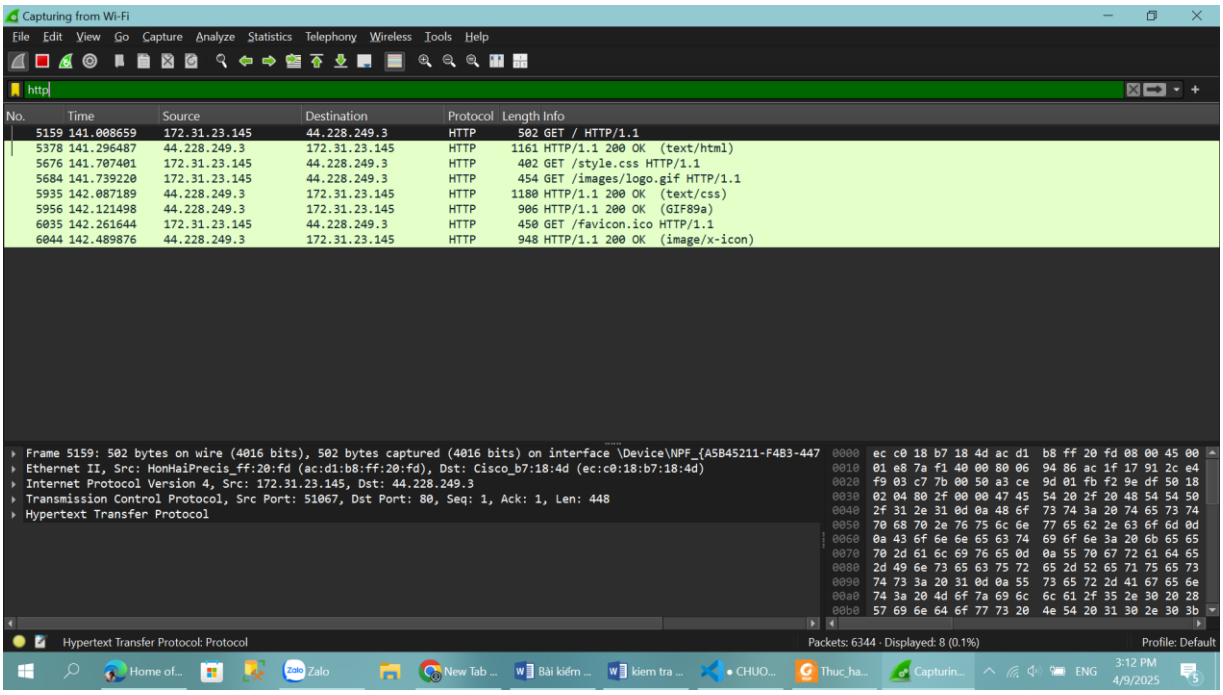
Chọn card mạng (Wifi) , bắt gói :



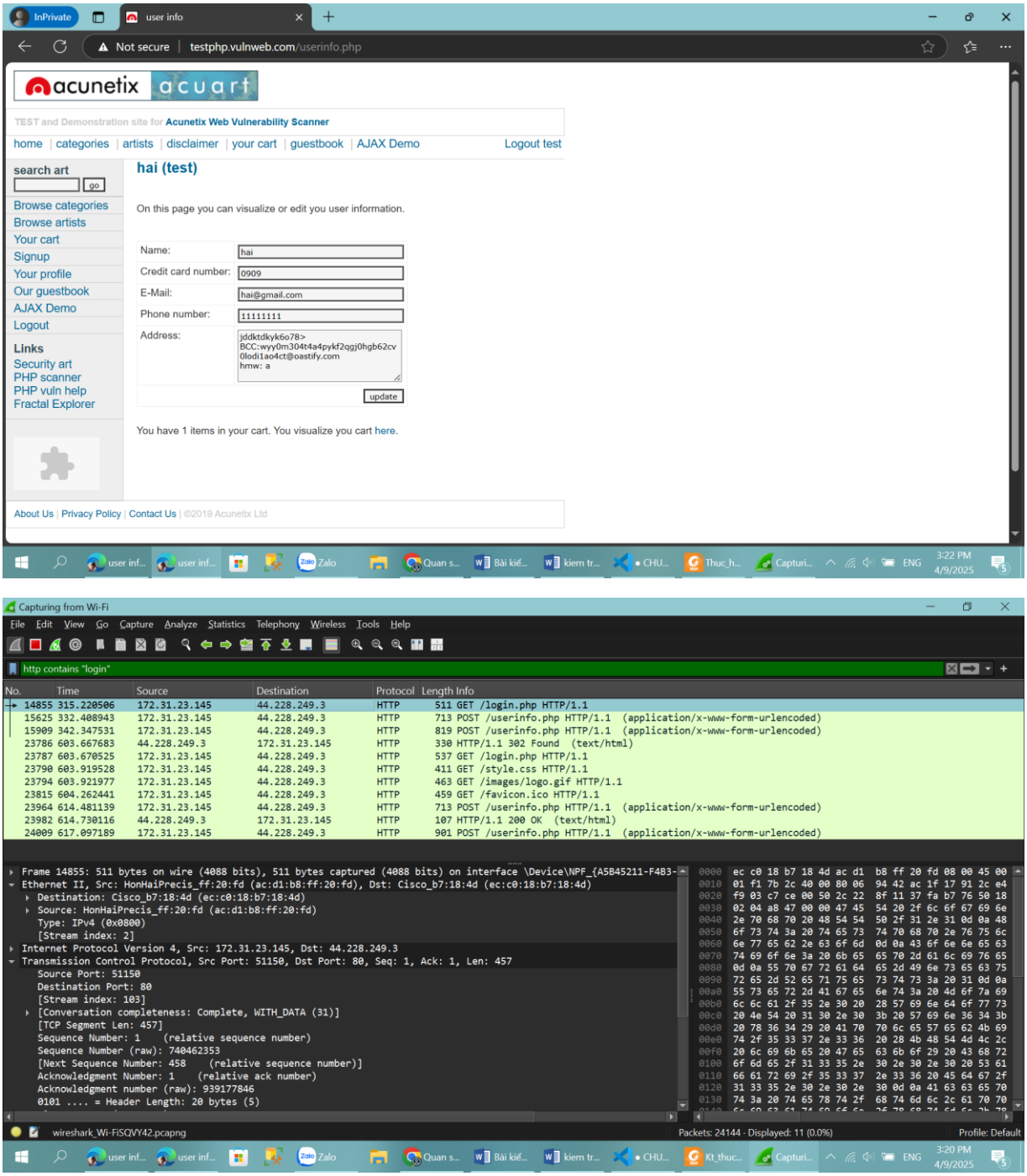


Bước 2 :

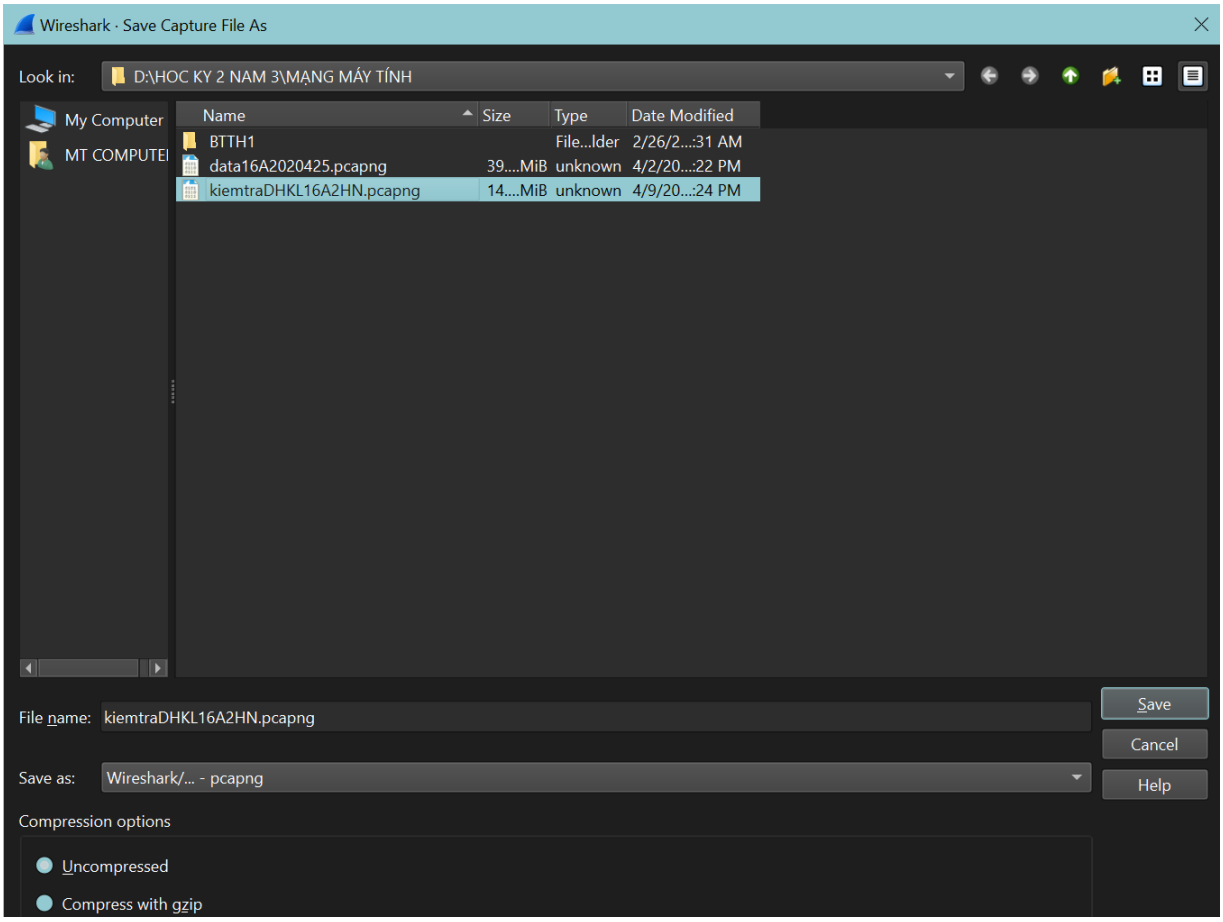
Lọc HTTP :



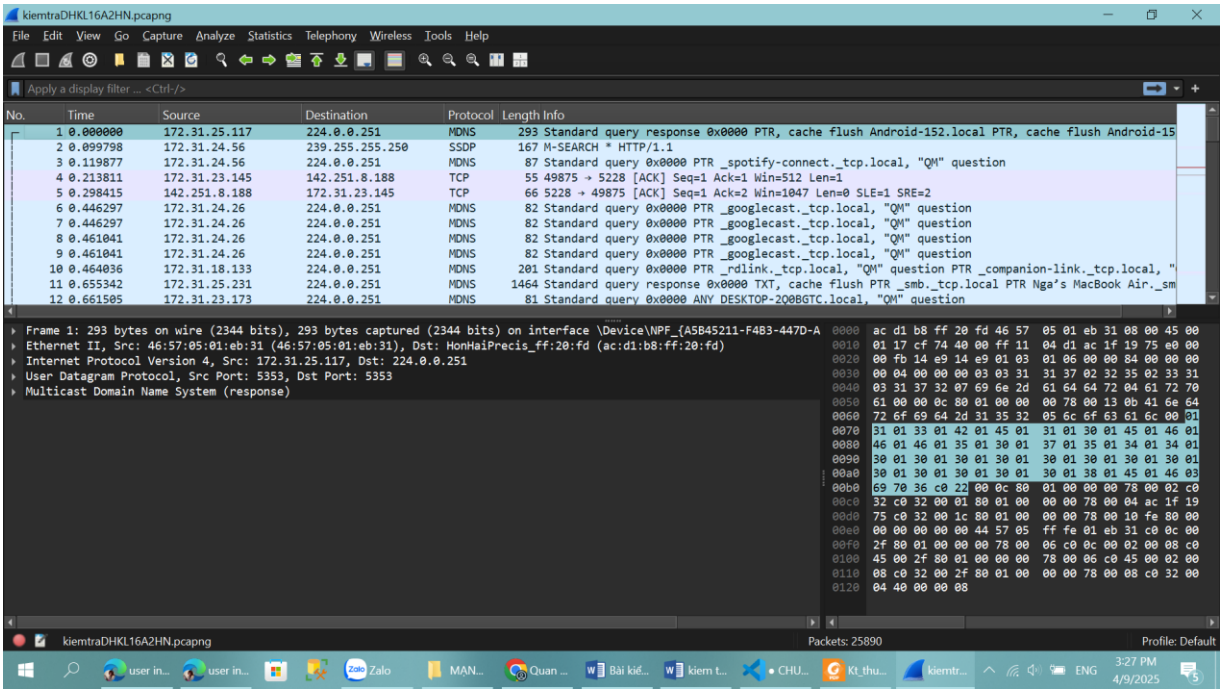
Truy cập một trang login, quan sát gói gửi dữ liệu :



Bước 3 : Lưu file kết quả bắt gói (.pcapng)



Bước 4 : Mở lại file đã lưu



Phân tích theo từng tầng trong mô hình OSI :

- Lớp 2 – Data Link (Liên kết dữ liệu)

- Giao thức: Ethernet II
- MAC nguồn: HonHaiPrecisi_ff:20:fd
- MAC đích: Cisco_b7:18:4d

- Lớp 3 – Network (Mạng)

- Giao thức: IPv4
- IP nguồn: 172.31.23.145
- IP đích: 44.228.249.3
- TTL: 103

- Lớp 4 – Transport (Giao vận)

- Giao thức: TCP
- Cổng nguồn: 51150
- Cổng đích: 80 (HTTP)
- Sequence number: 1 (Sequence number bắt đầu từ 1)
- Acknowledgment number: 993177846
- Flags: 0x018 (PSH, ACK)

- Lớp 5 – Session (Phiên kết nối)

- Giao thức HTTP/1.1 đang được sử dụng.
- Mặc dù HTTP không quản lý phiên trực tiếp, Connection: keep-alive có thể giúp duy trì kết nối giữa client và server trong suốt quá trình giao tiếp mà không cần phải thiết lập lại kết nối cho mỗi yêu cầu mới.

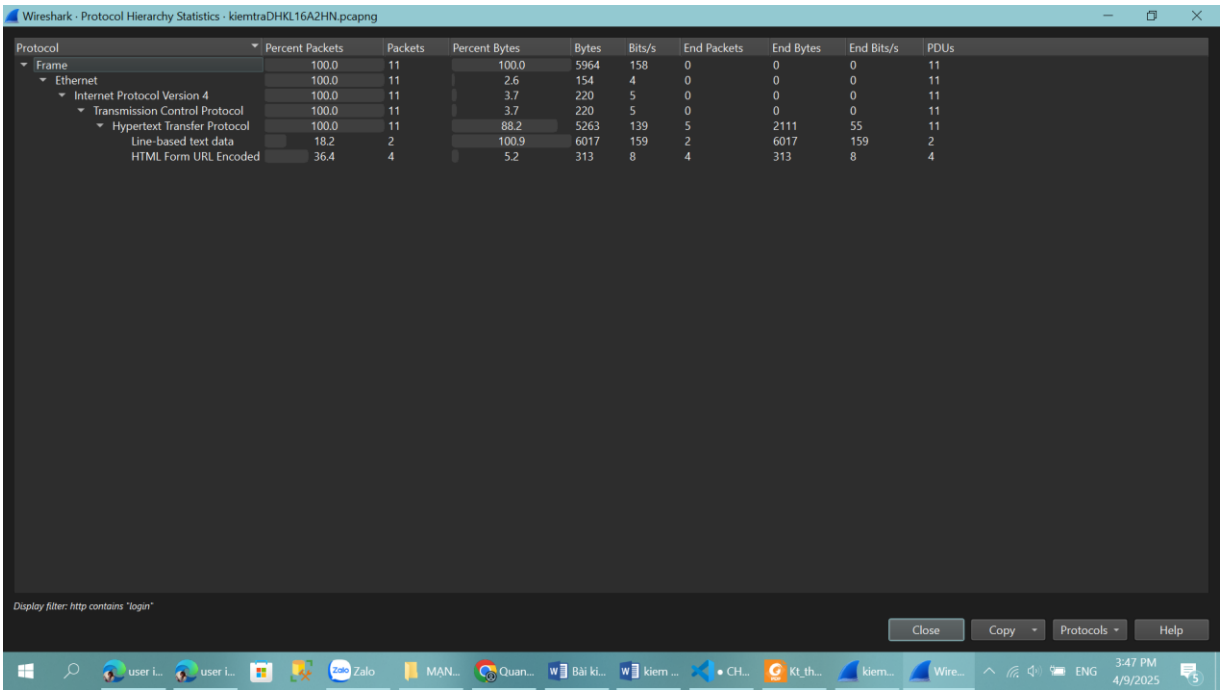
- Lớp 6 – Presentation (Trình bày)

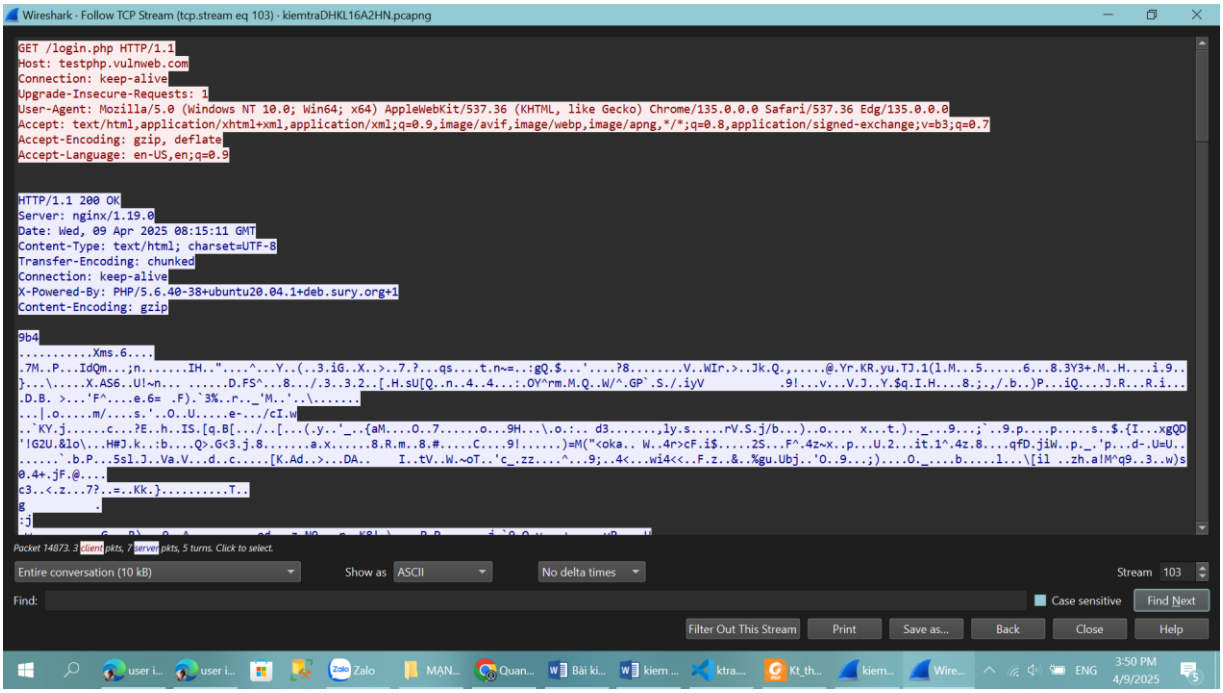
- Trong trường hợp này, Wireshark không thể hiển thị các thông tin mã hóa hoặc nén trực tiếp. Tuy nhiên, HTTP có thể mã hóa hoặc nén nội dung, nhưng Wireshark chủ yếu chỉ hiển thị các tiêu đề và nội dung của HTTP nếu không có mã hóa rõ ràng.

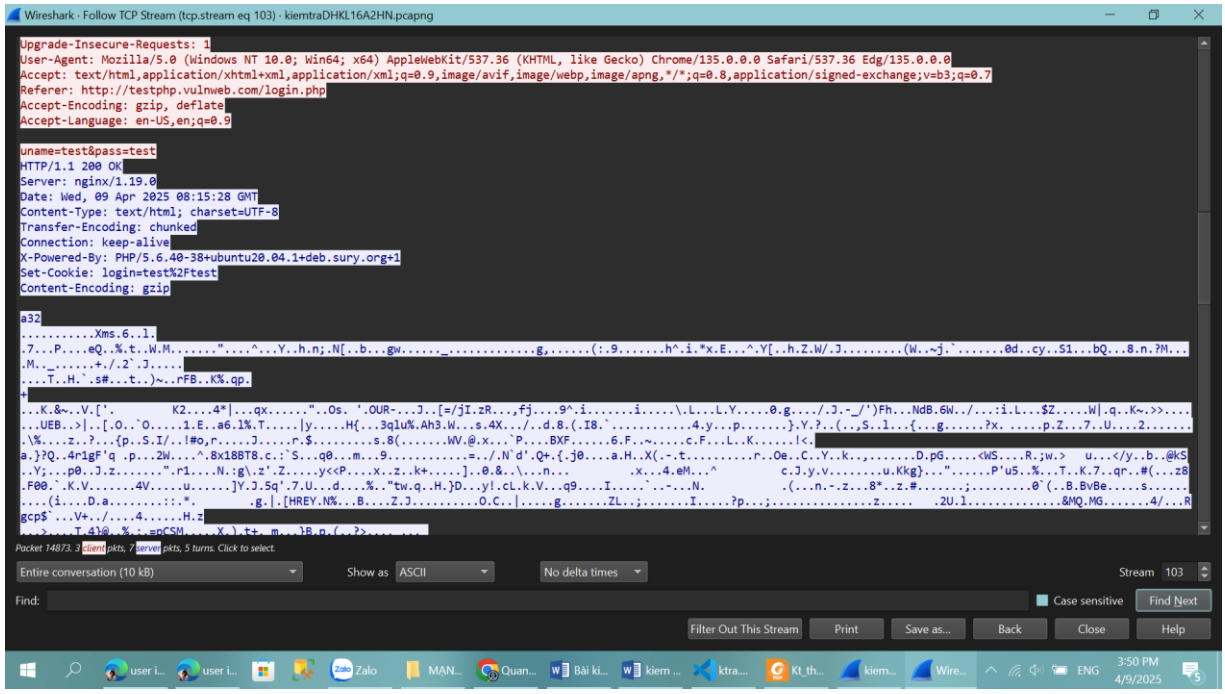
- Lớp 7 – Application (Ứng dụng)

- Giao thức: HTTP
- Phương thức HTTP: POST (gửi dữ liệu từ client đến server)
- URL: /userinfo.php
- Loại nội dung: application/x-www-form-urlencoded

Bước 5 : Sử dụng tính năng Protocol Hierarchy hoặc Follow TCP Stream để quan sát toàn cục.






Wireshark · Follow TCP Stream (tcp.stream eq 103) · kiemtraDHKL16A2HN.pcapng
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
uname=test&pass=test
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 09 Apr 2025 08:15:28 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
a32
Packet 14873. 3 client pkts, 7 server pkts, 5 turns. Click to select.
Entire conversation (10 kB)
Show as ASCII
No delta times
Stream 103
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
3:50 PM
4/9/2025