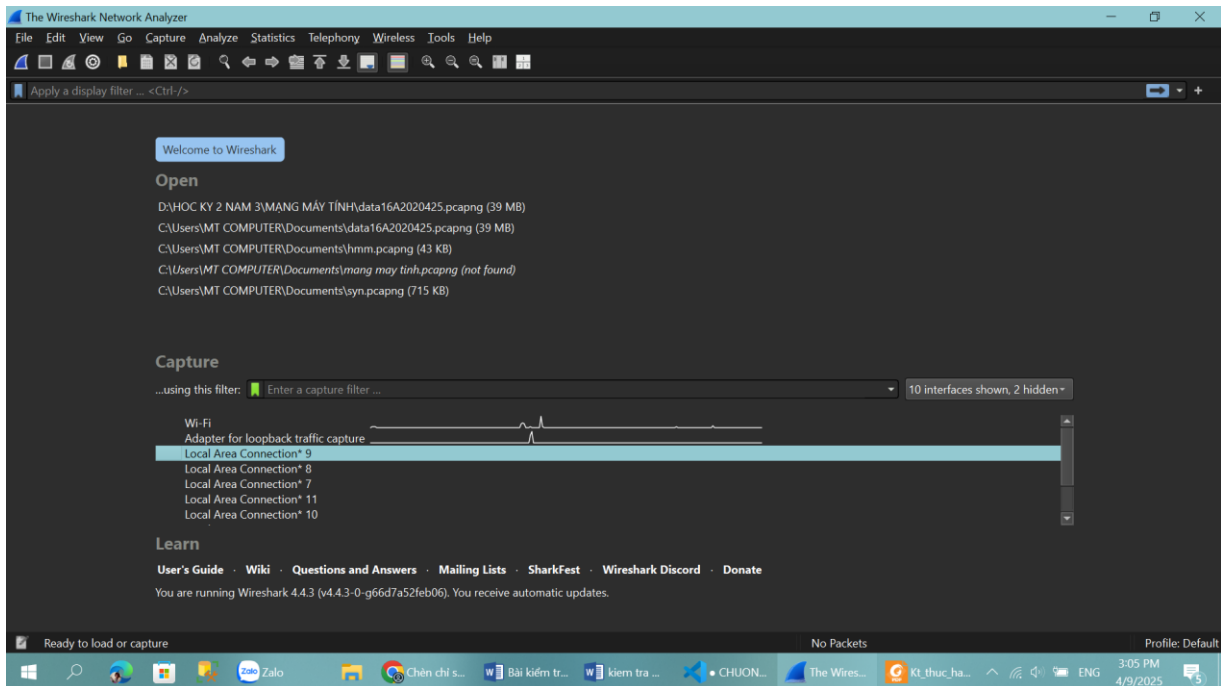


Phạm Thị Trà Giang	22174600025
Trần Trọng Chinh	22174600017

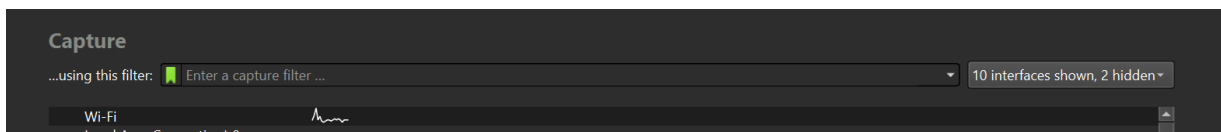
BÀI THỰC HÀNH 4 – PHIÊN TỔNG HỢP (LỚP K16A2)

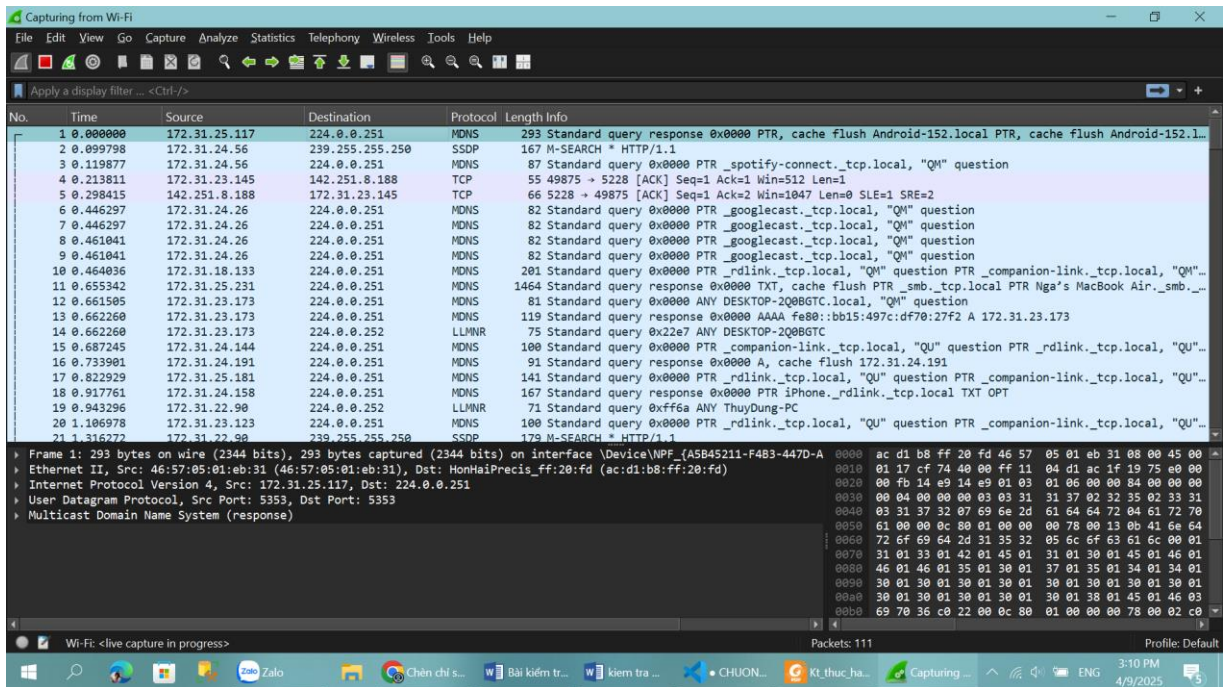
Bước 1 :

Mở Wireshark :



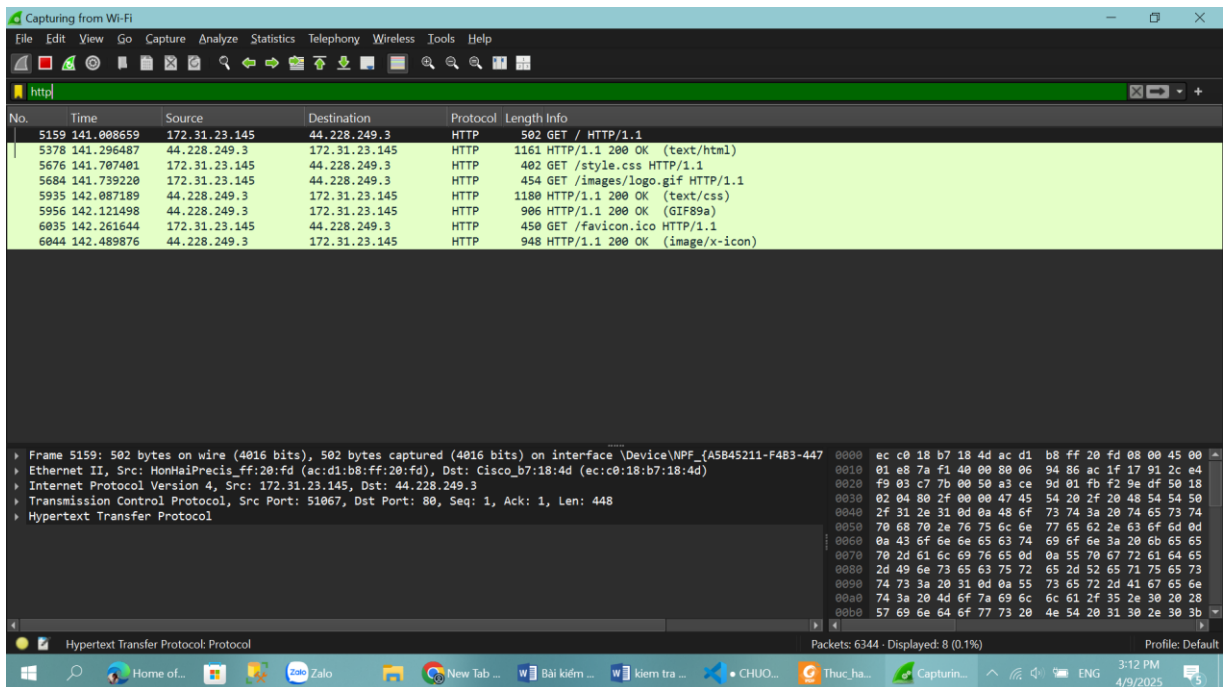
Chọn card mạng (Wifi) , bắt gói :



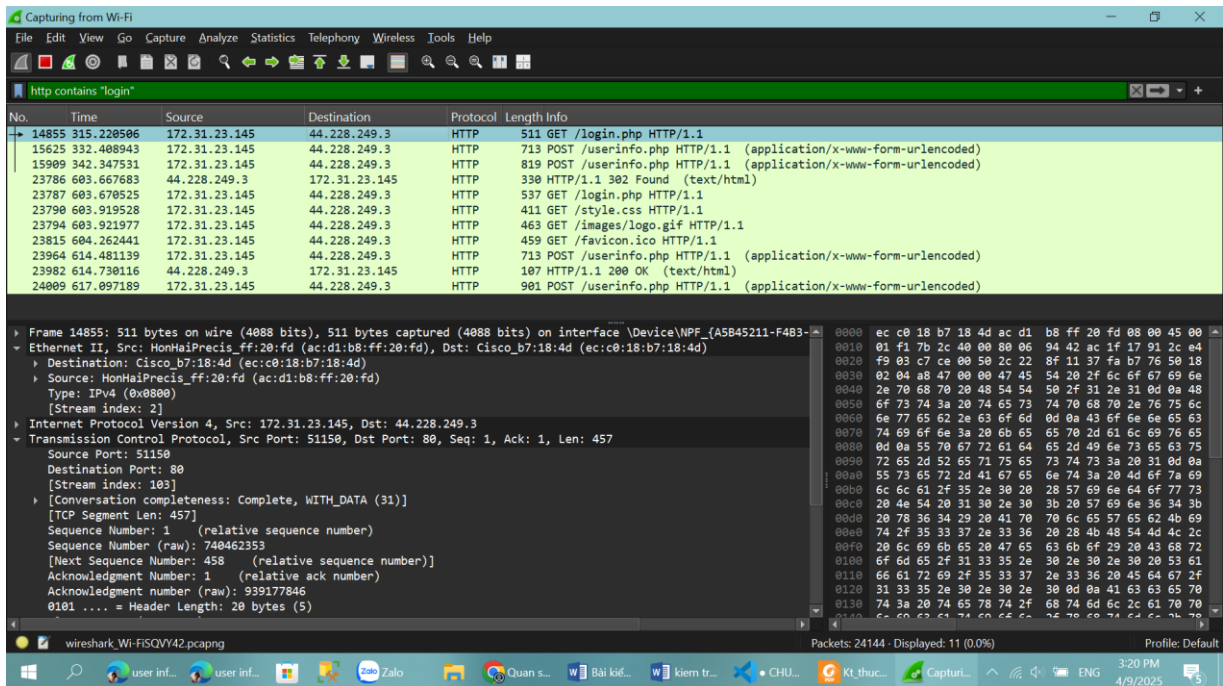
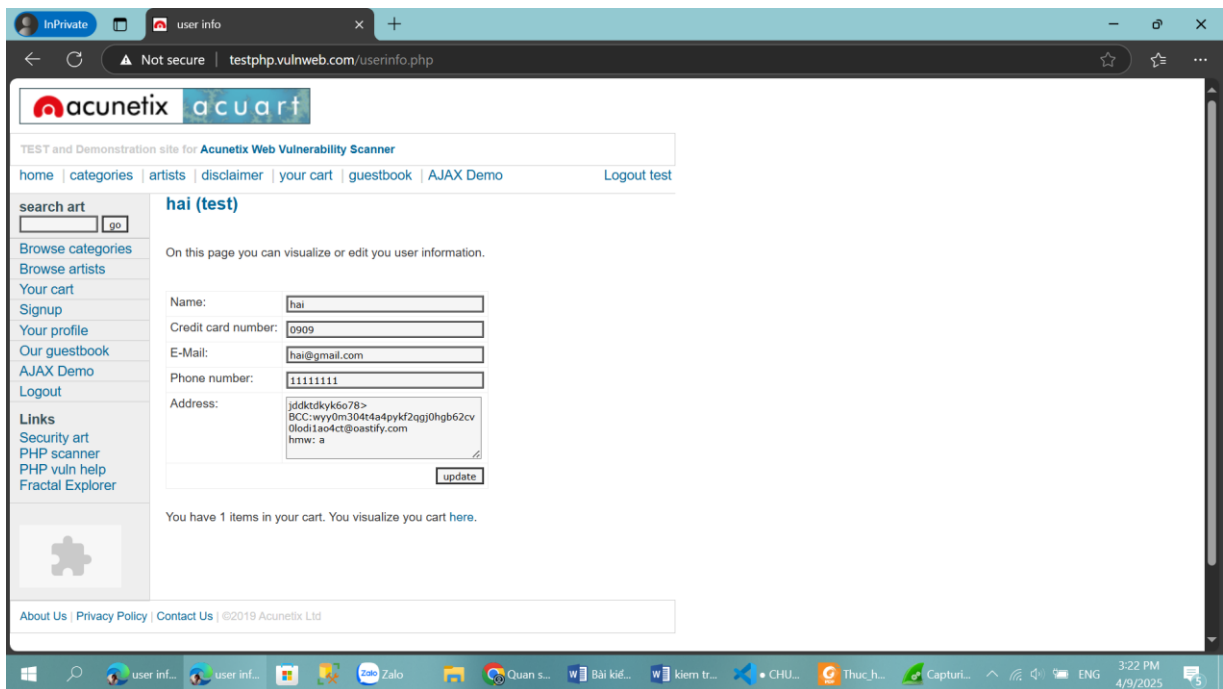


Bước 2 :

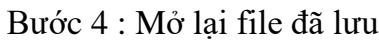
Lọc HTTP :



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



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



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 - Protocol Hierarchy Statistics - kiemtraDHL16A2HN.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU's
Frame	100.0	11	100.0	5964	158	0	0	0	11
Ethernet	100.0	11	2.6	154	4	0	0	0	11
Internet Protocol Version 4	100.0	11	3.7	220	5	0	0	0	11
Transmission Control Protocol	100.0	11	3.7	220	5	0	0	0	11
Hypertext Transfer Protocol	100.0	11	88.2	5263	139	5	2111	55	11
Line-based text data	18.2	2	100.9	6017	159	2	6017	159	2
HTML Form URL Encoded	36.4	4	5.2	313	8	4	313	8	4

Display filter: http contains "login"

Close Copy Protocols Help

user I... user I... Zalo MAN... Quan... Bài ki... kiem... CH... Kt_th... kiem... Wire... ENG 3:47 PM 4/9/2025

The screenshot displays the Wireshark network protocol analyzer interface. The top status bar indicates the capture source as 'Wiredeth - Follow TCP Stream (tcp stream eq 103)'. The main packet list pane shows a single captured packet at 14873.3 seconds, identified as a client packet (7 server packets) from 10.0.0.1 to 10.0.0.1.

The selected packet's details are expanded, revealing an HTTP GET request:

- GET /login.php HTTP/1.1**
- Host:** testphp.vulnweb.com
- Connection:** keep-alive
- 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
- Accept-Encoding:** gzip, deflate
- Accept-Language:** en-US,en;q=0.9

The packet bytes pane shows the raw data of the request, starting with the magic number 9B4 and followed by the HTTP message structure in hexadecimal and ASCII.

At the bottom, the packet summary states: "Packet 14873.3: client pkts: 7 server pkts, 5 turns. Click to select." Below this, there are controls for displaying the entire conversation (10 kB), showing the data as ASCII, and no delta times. On the right, there are buttons for "Find Next", "Stream 103", and other standard window management options.

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
.....Xms.6..1.
7...P...eQ.%t..W.M.....Y..h.nj.N[.b..gw.....g.....(:9.....h^i.*x.E...^Y[.h.Z.W/J.....(W..~j..^.....0d..cy..S1...bQ...8.n.?M..
M.....+/.2'.J.....
...T..H...s#...t...)~..RFB..K%qp.
+
...K.&~.V.['. K2...4*|...qx....."Os. 'OUR...J..[=jI.zR...fj...9^i.....i.....\L...L.Y....0.g..../.J.-/'Ph...NdB.6W.../...:i.L...\$Z....W|.q..K~.>...
...UEB...>|.[.O..`O.....1.E...a6.1%T.....|y.....H(...3qlu%Ah3.W...s.4X.../..d.8.(.1B.'.....4.y...p.....}Y..?(...S..i...{...g.....?x.....p.Z...7.U...2..
.\%.....z..?..{p..S.I/..!#0...r.....J.....r.....s.8(...WV.@x...`P...BXF.....6.F...~.....c.F...L..K.....l<..
a.}7Q..4rtgP'q .p...2W...^8x18B7B.c.'S...q0...m...9.....=../'N'd'.Qe.[.j0....a.H..X[.-t...t...r..Oe..C...Y..k.....D.pG.....<WS...R.jw.> u...</y...b..@kS
l.Vj...p0..J.z....."r1...N.:g\z'.Z...y<<P...X..z..k*...j].0.8.\.....N...^ c.J.y.V...u.Kkg].....P'u5.,%...T..K.7...qr..#(...z8
F00..K.V.....4V.....U.....]Y.J.5q'.7.U...d...%. "tw.q..H.JD...yl.cl.k.V...q9...I.....N...^ (...n..z...8*.z.#.....j.....0' (...B.BvBe...s...
....(i...D.a.....:*. g..[HREY.N%..B....Z.J.....O.C..|.....g.....ZL..j.....I.....?p...j.....z.....2U.1.....&MQ.MS.....4/...R
gcpS'...V+.../...4.....H.z.....T.418..%...=pCSM...X.)..t+...m...3B.p.(...>.....
Packet 14873: 3 [redacted] pkts, 7 [redacted] 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

Windows taskbar: user i..., user i..., Zalo, MAN..., Quan..., Bai ki..., kiem..., ktra..., Kt_th..., kiem..., Wire..., 3:50 PM 4/9/2025