

Họ và tên: Trần Đức Trung

Phạm Văn Thắng

MSV :22174600059

MSV : 22174600059

Bước 1: Mở Wireshark, chọn card mạng, bắt gói khi truy cập một trang web.

Bước 2: Lọc giao thức HTTP, truy cập một trang login, quan sát gói gửi dữ liệu.

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area is divided into three panes. The top pane shows a list of captured packets, with the first packet (No. 1494) selected. The middle pane shows the details of the selected packet, which is an HTTP GET request to /userinfo.php. The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet list pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1494	33.553721	172.31.42.38	44.228.249.3	HTTP	526	GET /userinfo.php HTTP/1.1
1500	33.764668	44.228.249.3	172.31.42.38	HTTP	471	HTTP/1.1 200 OK (text/html)
1501	33.794219	172.31.42.38	44.228.249.3	HTTP	448	GET /favicon.ico HTTP/1.1
1506	34.004354	44.228.249.3	172.31.42.38	HTTP	948	HTTP/1.1 200 OK (image/x-icon)
1927	51.923417	172.31.42.38	44.228.249.3	HTTP	526	GET /userinfo.php HTTP/1.1
1931	52.134607	44.228.249.3	172.31.42.38	HTTP	330	HTTP/1.1 302 Found (text/html)
1932	52.143465	172.31.42.38	44.228.249.3	HTTP	523	GET /login.php HTTP/1.1
1957	52.354740	44.228.249.3	172.31.42.38	HTTP	1350	HTTP/1.1 200 OK (text/html)
1959	52.378394	172.31.42.38	44.228.249.3	HTTP	397	GET /style.css HTTP/1.1
1972	52.591259	172.31.42.38	44.228.249.3	HTTP	449	GET /images/logo.gif HTTP/1.1
2016	52.812199	44.228.249.3	172.31.42.38	HTTP	906	HTTP/1.1 200 OK (GIF89a)
2189	61.022962	172.31.42.38	44.228.249.3	HTTP	699	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2197	61.244372	44.228.249.3	172.31.42.38	HTTP	81	HTTP/1.1 200 OK (text/html)

The details pane shows the following information for the selected packet:

- Frame 1494: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface...
- Ethernet II, Src: Intel_c5:2f:60 (14:85:7f:c5:2f:60), Dst: Cisco_b7:18:5d (ec:c0:18:00:07:18:5d)
- Internet Protocol Version 4, Src: 172.31.42.38, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 53565, Dst Port: 80, Seq: 1, Ack: 1, Len: 526
- Hypertext Transfer Protocol
 - GET /userinfo.php HTTP/1.1\r\n
 - Host: testphp.vulnweb.com\r\n
 - Connection: keep-alive\r\n
 - Cache-Control: max-age=0\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - 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\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: vi-VN,vi;q=0.9\r\n

The raw packet data pane shows the hexadecimal and ASCII representation of the packet data.

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

The image shows a Windows File Explorer window. The address bar displays the path: This PC > New Volume (D:) > mang may tinh. The search bar contains the text 'Search mang may tinh'. The left sidebar shows the navigation pane with the following items:

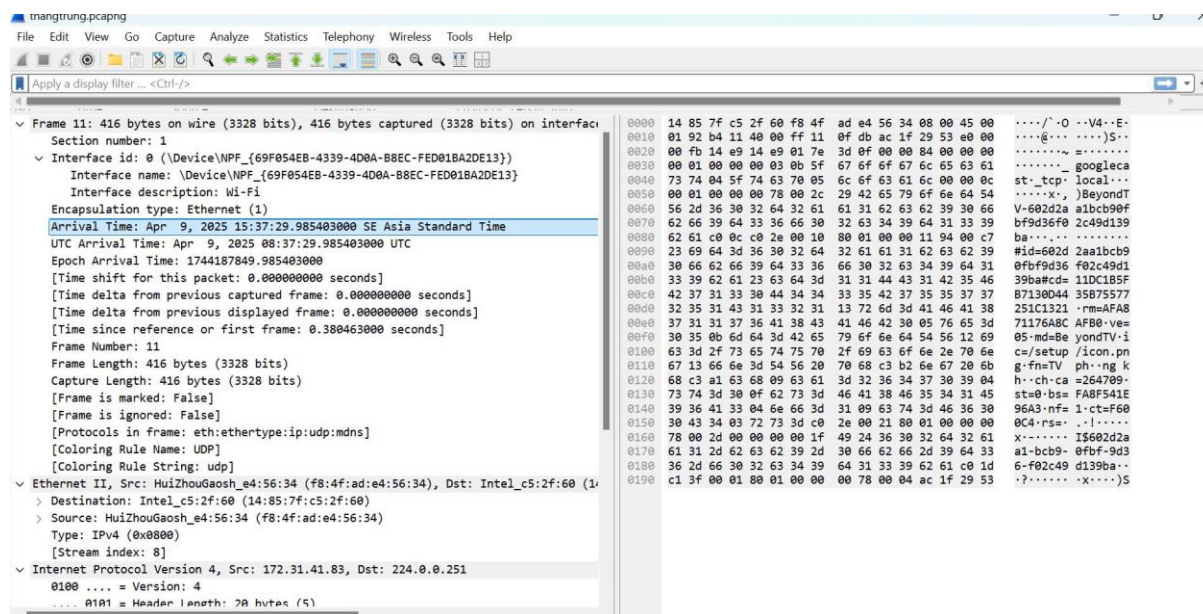
- Gallery
- thang - Personal
 - Documents
 - Pictures
- Documents
- Downloads
- phân tích hồi quy
- sylvester ft kronecker
- PROJECT
- code

The main pane shows the contents of the 'mang may tinh' folder:

Name	Date modified	Type	Size
kientra.py	4/9/2025 3:29 PM	Python File	1 KB
thangtrung.pcapng	4/9/2025 3:40 PM	Wireshark capture file	1,968 KB

The status bar at the bottom indicates '2 items'.

Bước 4: Mở lại file đã lưu, phân tích theo từng tầng trong mô hình OSI.



1. Thông tin tổng quan (Frame)

- Frame 11: Đây là gói tin thứ 11 được ghi nhận.
- Captured length: 416 bytes.
- Arrival Time: 15:37:29 ngày 9/4/2025 (Asia Standard Time).
- Gói tin được bắt từ giao diện Wi-Fi.

2. Ethernet II – Tầng liên kết dữ liệu (Layer 2)

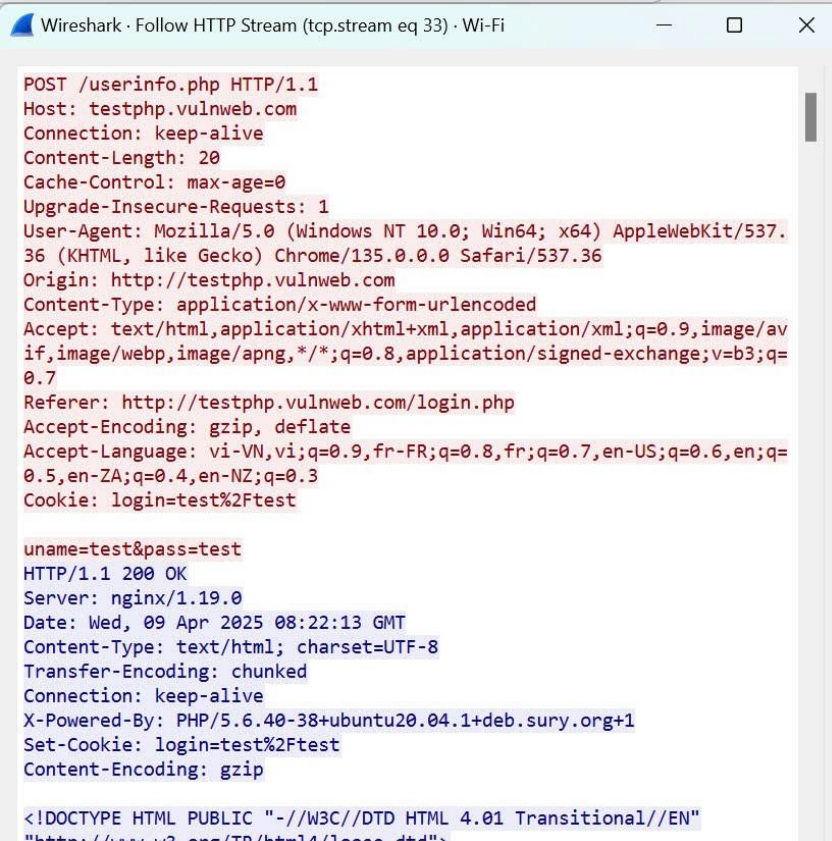
- MAC nguồn: HuiZhouasdh_e4:56:d4
- MAC đích: Intel_c5:2f:e7
- Type: IPv4 (0x0800)

3. IP – Tầng mạng (Layer 3)

- IP nguồn: 172.31.41.101
- IP đích: 224.0.0.251 (là địa chỉ multicast dùng cho dịch vụ MDNS – Multicast DNS)

- Cho thấy gói tin không phải HTTP, mà là gói khám phá dịch vụ trong mạng LAN.

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



```
Wireshark · Follow HTTP Stream (tcp.stream eq 33) · Wi-Fi

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 20
Cache-Control: max-age=0
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
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
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: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5,en-ZA;q=0.4,en-NZ;q=0.3
Cookie: login=test%2Ftest

uname=test&pass=test
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 09 Apr 2025 08:22:13 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

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
```

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

```

import pyshark

# Đường dẫn đến file .pcapng đã thu được bằng Wireshark
path = r'D:\mạng máy tính\thangtrung.pcapng' # Ghi đúng đường dẫn

# Tạo đối tượng đọc file gói tin, chỉ lọc các gói HTTP Request
cap = pyshark.FileCapture(path, display_filter='http.request')

print("Phân tích gói HTTP REQUEST chứa từ khoá 'login' hoặc 'test'\n")

# Duyệt qua từng gói tin trong file
for i, pkt in enumerate(cap):
    try:
        # Chuyển toàn bộ nội dung HTTP sang dạng chữ thường
        http_info = str(pkt.http).lower()

        # Nếu trong nội dung gói có chứa 'login' hoặc 'test'
        if 'login' in http_info or 'test' in http_info:
            print("=" * 50)
            print(f"GÓI #{i+1} Có chứa từ khoá")
            print("Thời gian:", pkt.sniff_time)

            # IP nguồn và IP đích
            src_ip = pkt.ip.src if hasattr(pkt, 'ip') else 'N/A'
            dst_ip = pkt.ip.dst if hasattr(pkt, 'ip') else 'N/A'
            print("IP nguồn:", src_ip)
            print("IP đích:", dst_ip)

            # Phương thức HTTP: GET hoặc POST
            if hasattr(pkt.http, 'request_method'):
                print("Phương thức:", pkt.http.request_method)

            # URL đầy đủ nếu có
            if hasattr(pkt.http, 'host') and hasattr(pkt.http, 'request_uri'):
                print("URL:", f"http://{pkt.http.host}{pkt.http.request_uri}")

            # Cookie
            if hasattr(pkt.http, 'cookie'):
                print("Cookie:", pkt.http.cookie)

            # Payload (nếu là POST)
            if hasattr(pkt.http, 'file_data'):
                print("Payload:", pkt.http.file_data)

    except Exception as e:
        print(f"[Lỗi tại gói #{i+1}]: {e}")

```

Kết quả:

Phân tích gói HTTP REQUEST chứa từ khoá 'login' hoặc 'test'

=====

GÓI #1 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:03.158661

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: GET

URL: http://testphp.vulnweb.com/userinfo.php

=====

GÓI #2 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:03.399159

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: GET

URL: http://testphp.vulnweb.com/favicon.ico

=====

GÓI #3 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:21.528357

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: GET

URL: http://testphp.vulnweb.com/userinfo.php

=====

GÓI #4 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:21.748405

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: GET

URL: http://testphp.vulnweb.com/login.php

=====

GÓI #5 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:21.983334

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: GET

URL: http://testphp.vulnweb.com/style.css

=====

GÓI #6 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:22.196199

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: GET

URL: <http://testphp.vulnweb.com/images/logo.gif>

=====

GÓI #7 Có chứa từ khoá

Thời gian: 2025-04-09 15:38:30.627902

IP nguồn: 172.31.42.38

IP đích: 44.228.249.3

Phương thức: POST

URL: <http://testphp.vulnweb.com/userinfo.php>

Payload: 75:6e:61:6d:65:3d:74:65:73:74:26:70:61:73:73:3d:74:65:73:74