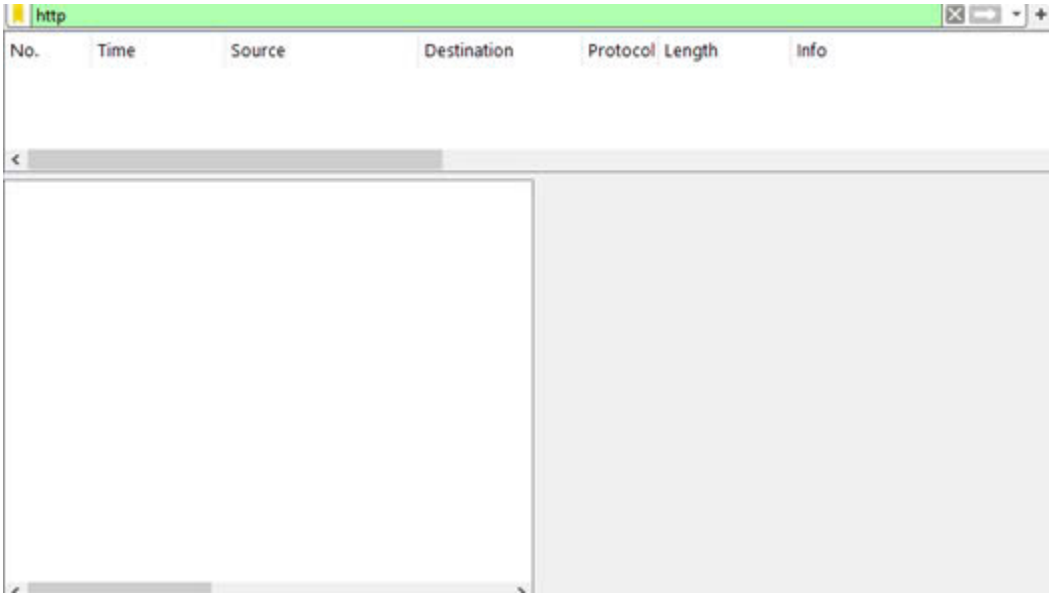
Bài Kiểm Tra DHKL16A1HN

Nguyễn Văn Duy 22174700011

Ninh Hữu Duy 22174600042

Bước 1: Mở wireshark, chọn card mạng Wifi, bắt đầu thu thập gói tin:

Lọc HTTP



Quan sát gói dữ liệu

Nhấn Enter để chỉ hiển thị các gói tin sử dụng giao thức HTTP.

Một số bộ lọc phổ biến:

Lọc các gói tin HTTP GET

http.request.method == "GET"

Lọc các gói tin HTTP POST:

http.request.method == "POST"

Lọc các gói tin HTTP chứa từ khóa “login”:

http contains "login"

Kiểm tra các cột:

Source: Địa chỉ IP của máy gửi.

Destination: Địa chỉ IP của máy nhận.

Protocol: Giao thức sử dụng (HTTP).

Info: Mô tả ngắn về gói tin như GET /index.html hoặc POST /login.

Bước 3:

Lưu file kết quả: login_test.pcapng

Bước 4:

Mở và trực quan hóa gói tin HTTP đã lưu

Mở file .pcapng đã lưu:

Vào menu File → Open, chọn file .pcap vừa lưu và nhấn Open.

Trực quan hóa và phân tích các trường của gói tin:

Frame: Thông tin chung như thời gian, độ dài gói tin.

Ethernet: Địa chỉ MAC nguồn và đích.

IP: Địa chỉ IP nguồn và đích, giao thức sử dụng (TCP).

TCP: Cổng nguồn, cổng đích, số thứ tự (Sequence Number).

HTTP: Các phương thức (GET, POST), URL, Header,...

Phân tích 1 gói HTTP theo các tầng:

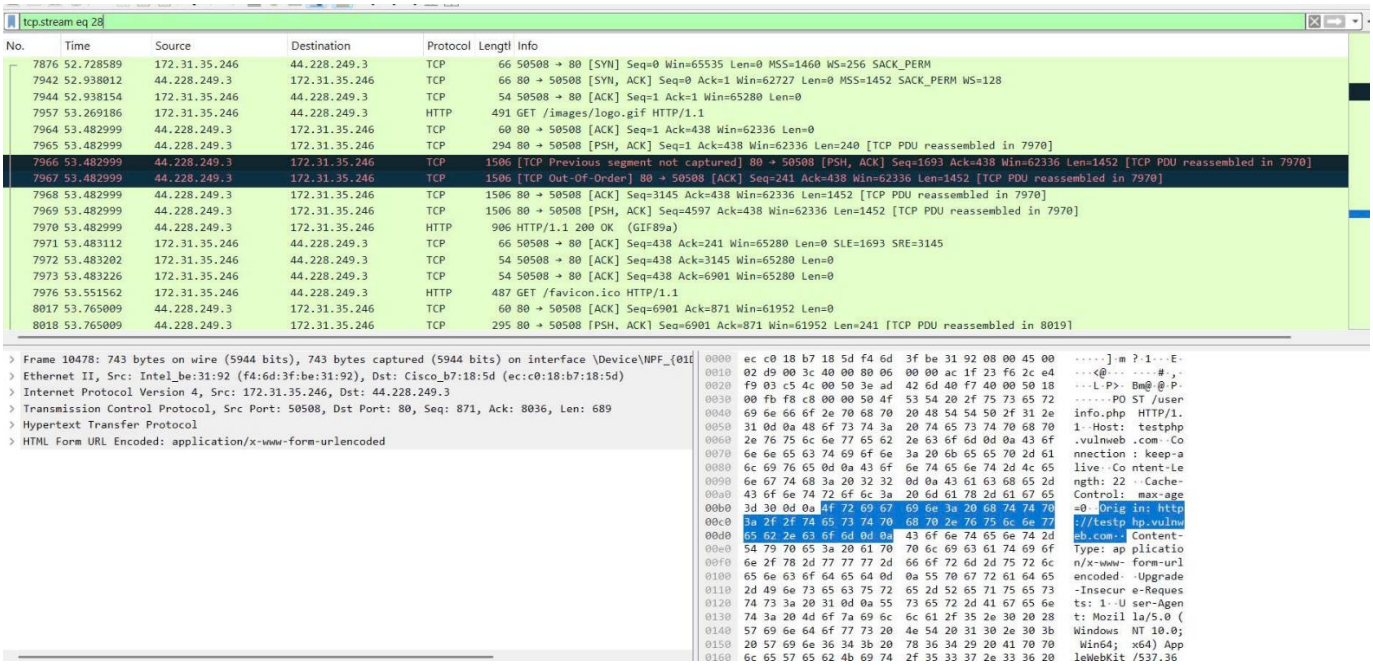
- **Tầng 2 (Data Link)**: Địa chỉ MAC nguồn và MAC đích.
- **Tầng 3 (Network)**: IP nguồn và IP đích.
- **Tầng 4 (Transport)**: Port nguồn/đích (thường là TCP 80).
- **Tầng 7 (Application)**: Dữ liệu HTTP.

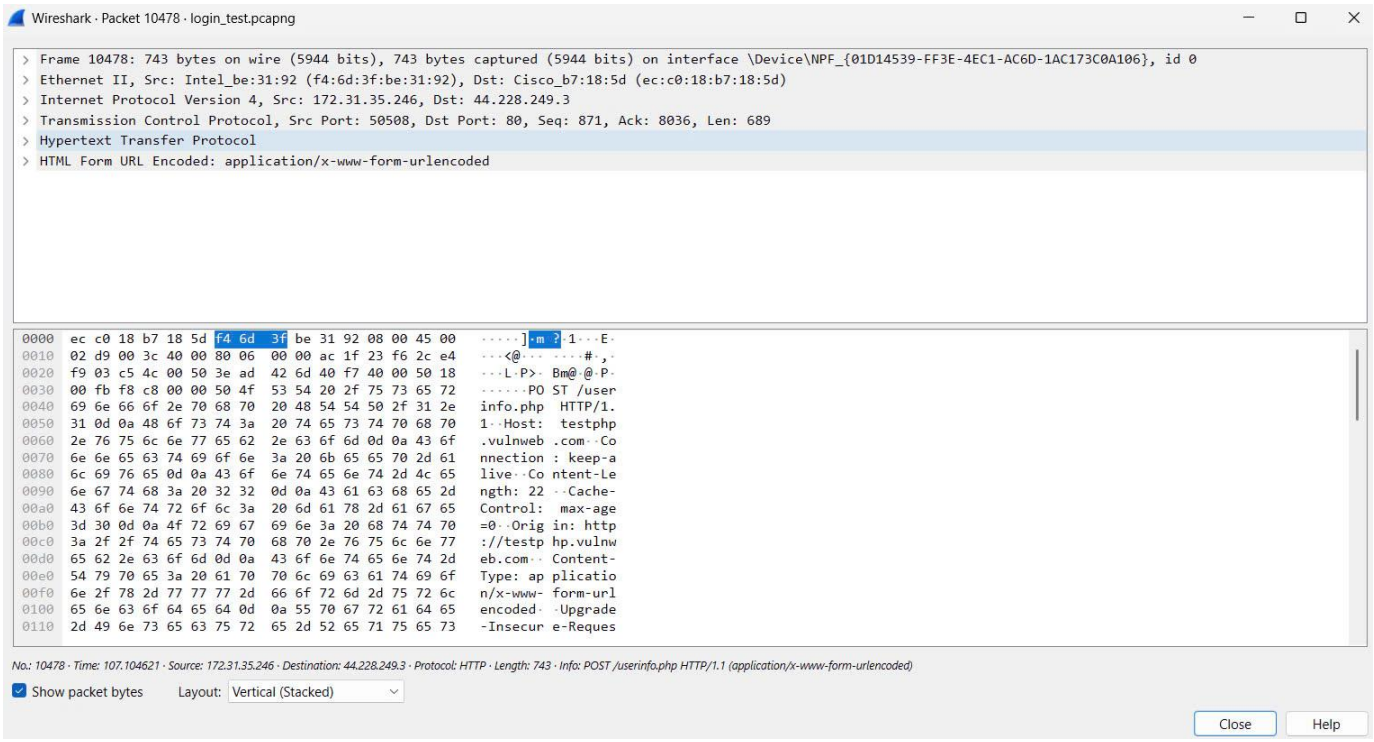
Lớp	Tên	Giao thức / Thông tin
1	Physical	Cáp mạng / tín hiệu
2	Data Link	Ethernet II – MAC: `f4:6d:3f:...` → `ec:c0:18:...`
3	Network	IPv4 – IP: `172.31.35.246` → `44.228.249.3`
4	Transport	TCP – Port: 50508 → 80
5	Session	HTTP Session
6	Presentation	Form URL Encoded
7	Application	HTTP POST Request

Bước 5: Lọc và phân tích gói tin HTTP bằng các biểu đồ trực quan

Dùng Statistics → Protocol Hierarchy để xem tỷ lệ HTTP, TCP, IP.

Dùng Follow TCP Stream để xem toàn bộ cuộc hội thoại.





Lớp	Tên	Giao thức / Thông tin
1	Physical	Cáp mạng / tín hiệu
2	Data Link	Ethernet II – MAC: `f4:6d:3f:...` → `ec:c0:18:...`
3	Network	IPv4 – IP: `172.31.35.246` → `44.228.249.3`
4	Transport	TCP – Port: 50508 → 80
5	Session	HTTP Session
6	Presentation	Form URL Encoded
7	Application	HTTP POST Request

Thông tin gói tin chính (Frame 10478):

Source IP: 172.31.35.246 (máy người dùng)

Destination IP: 44.228.249.3 (máy chủ)

Source Port: 50508

Destination Port: 80 (HTTP)

Protocol: HTTP

Length: 743 bytes

Method: POST

URL: /userinfo.php

Content-Type: application/x-www-form-urlencoded

Bước 6. Lập trình phân tích dữ liệu file: login_test.pcapng

Có 6 gói tin hợp lệ được phát hiện chứa từ khóa, cụ thể:

Gói	Thời gian	Phương thức	URL
#43	08:08:42.72	GET	`http://testphp.vulnweb.com/login.php`
#44	08:08:43.05	GET	`http://testphp.vulnweb.com/style.css`
#45	08:08:43.05	GET	`http://testphp.vulnweb.com/images/logo.gif`
#46	08:08:43.33	GET	`http://testphp.vulnweb.com/favicon.ico`
#101	08:09:36.89	POST	`http://testphp.vulnweb.com/userinfo.php` → Gửi thông tin `username=nduy&pass=123456`
#102	08:09:37.11	GET	`http://testphp.vulnweb.com/login.php`

Lỗi: No attribute named http ở phần lớn gói tin (trên 90%)

Nguyên nhân:

Các gói tin này không phải HTTP, có thể là:

TCP/UDP không có payload ứng dụng

Giao thức khác như TLS (HTTPS), DNS, ARP, v.v.

Gói bị mã hoá (do HTTPS)