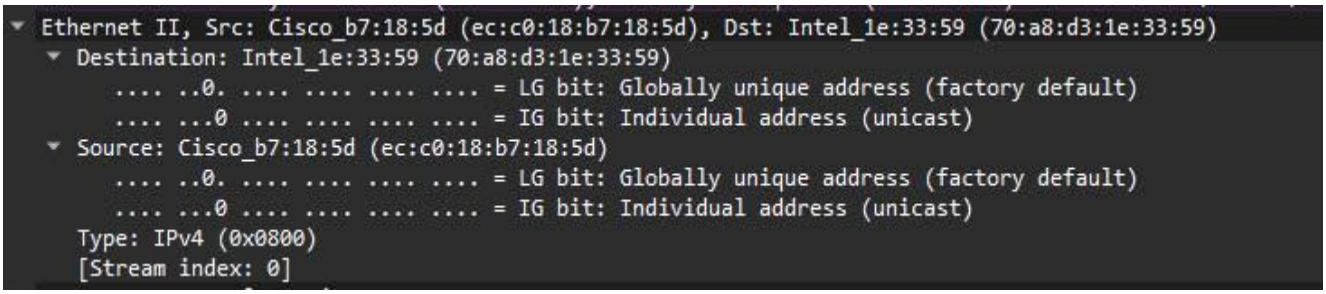
BÀI THỰC HÀNH 4

Phân tích theo từng tầng trong mô hình OSI :

Tầng 1 : Không hiển thị trực tiếp trên WireShark

Tầng 2 :



1.Nguồn (Source):

Địa chỉ MAC nguồn là Cisco_b7:18:5d (ec:c0:18:b7:18:5d). Địa chỉ này là duy nhất, được gán cho thiết bị Cisco, và có dấu hiệu là một địa chỉ unicast (địa chỉ duy nhất, không phải broadcast hay multicast).

2.Đích (Destination):

Địa chỉ MAC đích là Intel_1e:33:59 (70:a8:d3:1e:33:59). Địa chỉ này cũng là unicast, tức là chỉ định một thiết bị cụ thể nhận gói tin.

3.Thông tin Ethernet:

Cả nguồn và đích đều có bit LG (Locally Administrated bit) được đặt là 0, điều này có nghĩa là đây là các địa chỉ MAC được cấp phát toàn cầu (Globally Unique Address).

Đây là thông tin tiêu chuẩn của lớp liên kết dữ liệu (Layer 2) trong mô hình OSI.

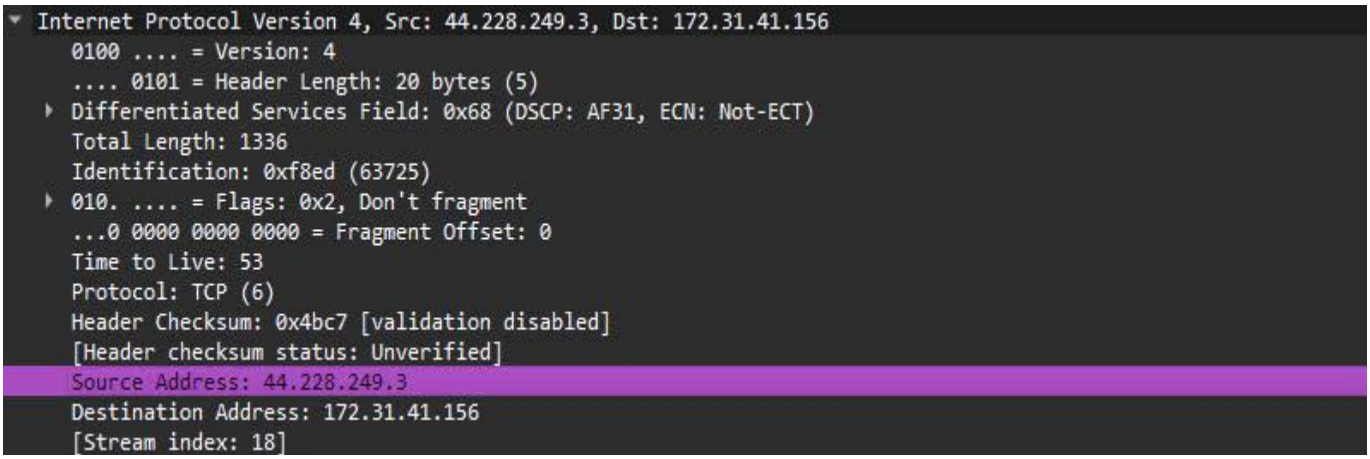
3.Loại gói (Type):

Gói này có loại là IPv4 (0x0800), nghĩa là nó chứa dữ liệu thuộc giao thức IP phiên bản 4.

4.Stream Index:

Gói này thuộc về một stream với index 0, chỉ ra rằng đây là một phần của một kết nối TCP hoặc UDP

Tầng 3 :



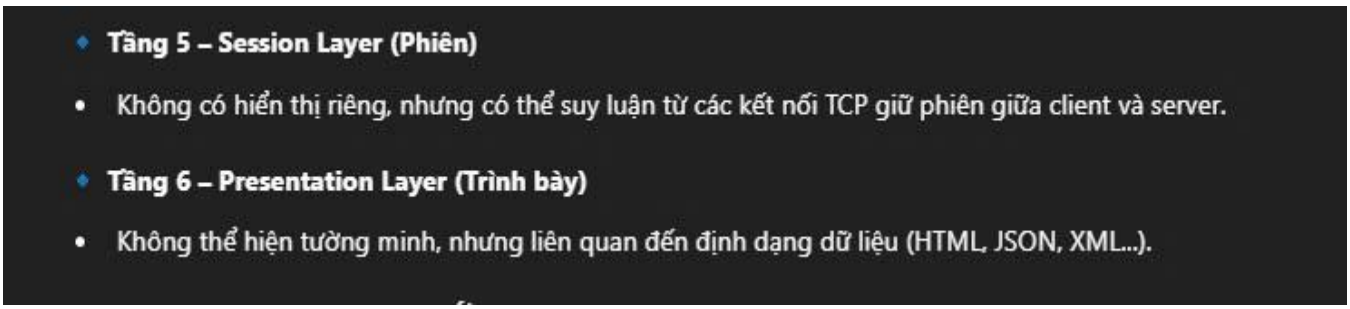
- **Thông tin chung:**

Phiên bản IP: Gói này sử dụng phiên bản IP là IPv4 (Version 4).

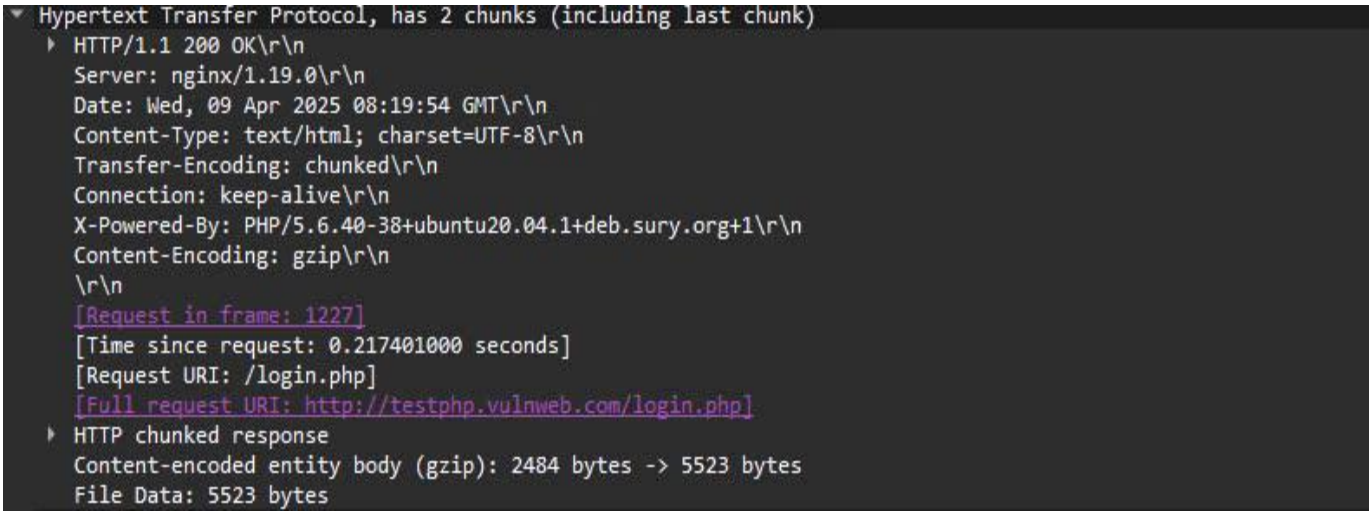
Địa chỉ nguồn (Source Address): 44.228.249.3. Đây là địa chỉ IP nguồn của gói.

Địa chỉ đích (Destination Address): 172.31.41.156. Đây là địa chỉ IP đích của gói.

Tầng 5 + 6 :



Tầng 7 :


Hypertext Transfer Protocol, has 2 chunks (including last chunk)
HTTP/1.1 200 OK\r\n
Server: nginx/1.19.0\r\n
Date: Wed, 09 Apr 2025 08:19:54 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n
Content-Encoding: gzip\r\n
\r\n
[Request in frame: 1227]
[Time since request: 0.217401000 seconds]
[Request URI: /login.php]
[Full request URI: http://testphp.vulnweb.com/login.php]
HTTP chunked response
Content-encoded entity body (gzip): 2484 bytes -> 5523 bytes
File Data: 5523 bytes