Kết quả bài kiểm tra chương 2

Gói tin HTTP là dữ liệu được gửi từ client (trình duyệt) đến server (máy chủ web) hoặc ngược lại, theo giao thức Hypertext Transfer Protocol – một giao thức tầng ứng dụng trong mô hình OSI.

Thành phần chính của gói tin HTTP:

Phương thức (Method): GET, POST, PUT, DELETE, v.v.

Đường dẫn (URI): tài nguyên được yêu cầu (VD: /login.php)

Phiên bản giao thức: HTTP/1.1, HTTP/2

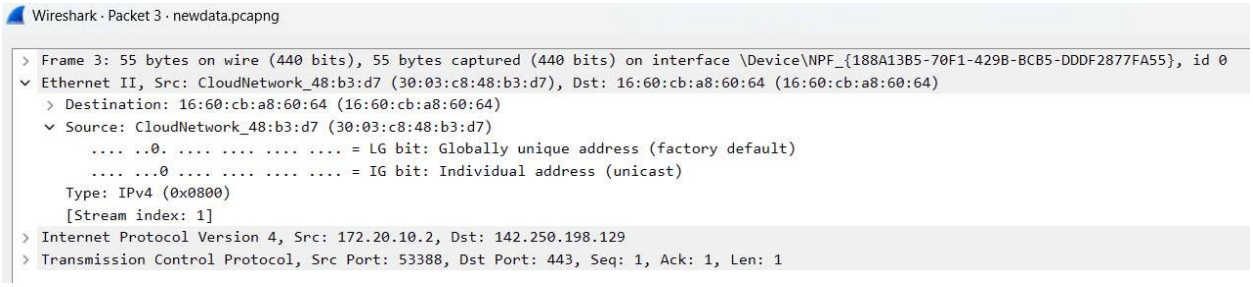
Các trường tiêu đề (Header): chứa thông tin trình duyệt, ngôn ngữ, định dạng chấp nhận,...

Dữ liệu (Body): (nếu là POST/PUT), có thể chứa thông tin đăng nhập, biểu mẫu, JSON...

Đặc điểm gói HTTP so với HTTPS:

HTTP không mã hóa, dễ bị đọc trộm (như ảnh bạn cung cấp).

HTTPS dùng TLS/SSL để mã hóa, bảo mật hơn nhưng không thấy rõ nội dung như HTTP.

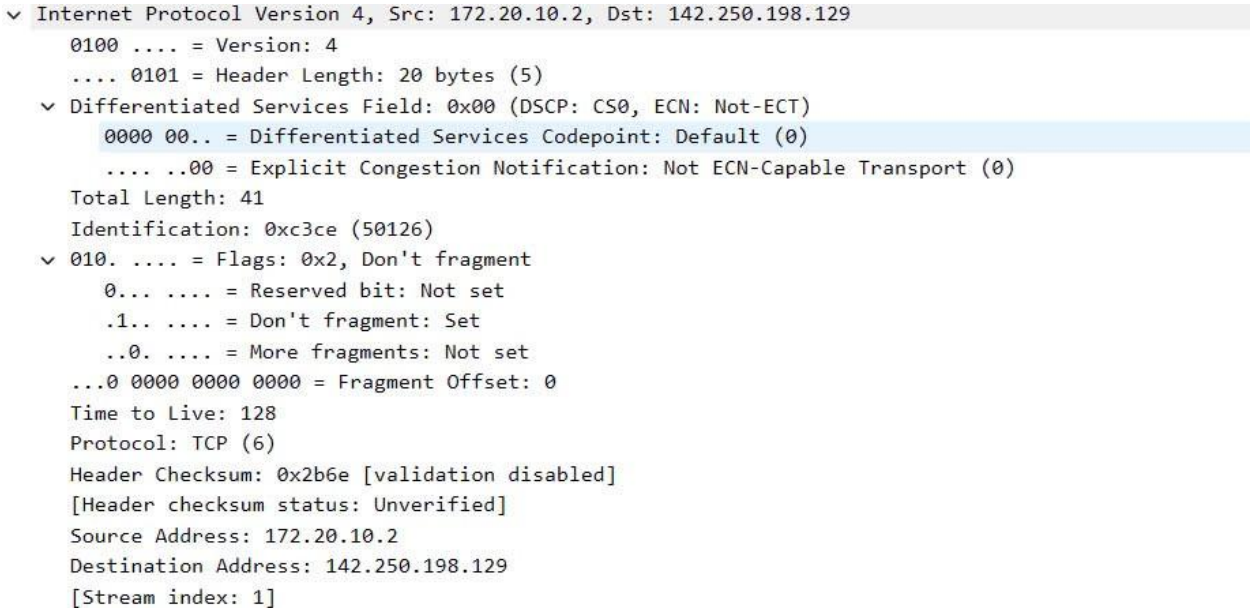


Tầng 2

Tên hiển thị: Ethernet II

Thông tin:

- Source (Địa chỉ MAC nguồn): 30:03:c8:48:b3:d7
- Destination (Địa chỉ MAC đích): 16:60:cb:a8:60:64



Tầng 3

Tên hiển thị: Internet Protocol Version 4

Thông tin:

Source (IP nguồn): 172.20.10.2

Destination (IP đích): 142.250.198.129

Header Length: 20 bytes (5)

TTL (Time to Live): 128

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Don't Fragment (DF) Flag: Đã được set

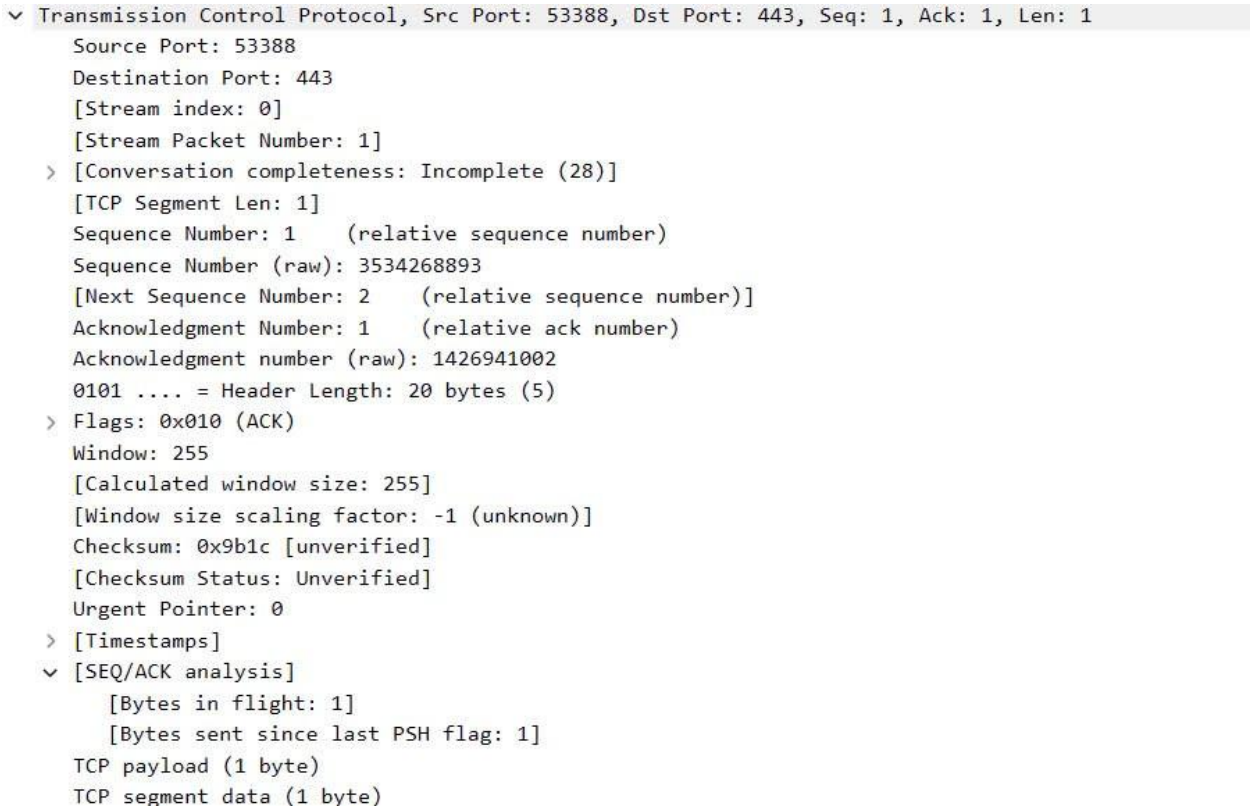
More Fragments (MF) Flag: Not set

Total Length: 41

Identification: 0xc3ce (50126)

Protocol: TCP (6)

Header Checksum: 0x2b6e (validation disabled)



Tầng 4: Transport (TCP)

Tên hiển thị: Transmission Control Protocol

Thông tin:

Source Port (Cổng nguồn): 53388

Destination Port (Cổng đích): 443 (HTTPS)

Flags: ACK (0x010)

Sequence Number: 1

Acknowledgment Number: 1

TCP Segment Length: 1 byte

Header Length: 20 bytes

Window size: 255

Checksum: 0x9b1c

Urgent Pointer: 0

Tầng 5–7: Session, Presentation, Application

Tên hiển thị: Hypertext Transfer Protocol (HTTP)

Thông tin:

HTTP Method: GET

Host: testphp.vulnweb.com

Full request URI: http://testphp.vulnweb.com/login.php

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

Connection: keep-alive

Upgrade-Insecure-Requests: 1

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: vi,fr-FR;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6

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

Phương thức: GET

URL: http://example.com/

==========

GÓI #2 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:08.455886

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

==========

GÓI #3 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:08.723891

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

==========

GÓI #4 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:08.727766

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

==========

GÓI #5 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:09.170023

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

==========

GÓI #6 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:25.970559

IP nguồn: 172.20.10.2

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

==========

GÓI #7 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:33.881093

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

Cookie: login=test%2Ftest

==========

GÓI #8 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:36.397625

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

Cookie: login=test%2Ftest

==========

GÓI #9 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:37.992050

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: GET

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

Cookie: login=test%2Ftest

==========

GÓI #10 Có chứa từ khoá

Thời gian: 2025-04-09 15:17:46.753715

IP nguồn: 172.20.10.2

IP đích: 44.228.249.3

Phương thức: POST

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

Cookie: login=test%2Ftest

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