

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

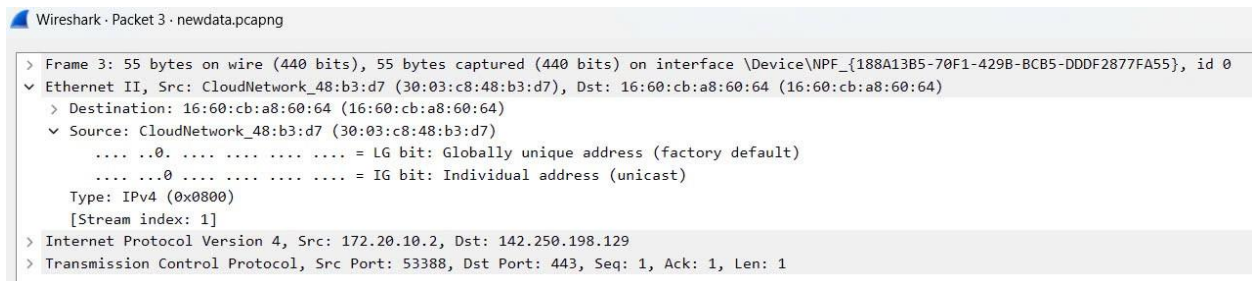
Các trường tiêu đề (Header): chứa thông tin trình duyệt, ngôn ngữ, định dạng chấp nhận,...

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

```

v Internet Protocol Version 4, Src: 172.20.10.2, Dst: 142.250.198.129
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 41
  Identification: 0xc3ce (50126)
  v 010. .... = Flags: 0x2, Don't fragment
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0x2b6e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.20.10.2
  Destination Address: 142.250.198.129
  [Stream index: 1]

```

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)

```

▼ Transmission Control Protocol, Src Port: 53388, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
  Source Port: 53388
  Destination Port: 443
  [Stream index: 0]
  [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (28)]
  [TCP Segment Len: 1]
  Sequence Number: 1      (relative sequence number)
  Sequence Number (raw): 3534268893
  [Next Sequence Number: 2      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 1426941002
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window: 255
  [Calculated window size: 255]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x9b1c [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  > [Timestamps]
  ▼ [SEQ/ACK analysis]
    [Bytes in flight: 1]
    [Bytes sent since last PSH flag: 1]
  TCP payload (1 byte)
  TCP segment data (1 byte)
```

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

```
▼ Hypertext Transfer Protocol
> GET /login.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\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,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: vi,fr-FR;q=0.9,fr;q=0.8,en-US;q=0.7,en;q=0.6\r\n
\r\n
[Response in frame: 11802]
[Full request URI: http://testphp.vulnweb.com/login.php]
```

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