

LAB 2.

1.



2.

1. Trình duyệt đang dùng HTTP 1.1. Server đang dùng HTTP 1.1

16	4.376683	192.168.1.10	192.168.1.12	HTTP	509 GET /21520328.html HTTP/1.1
17	4.383762	192.168.1.12	192.168.1.10	HTTP	637 HTTP/1.1 200 OK (text/html)

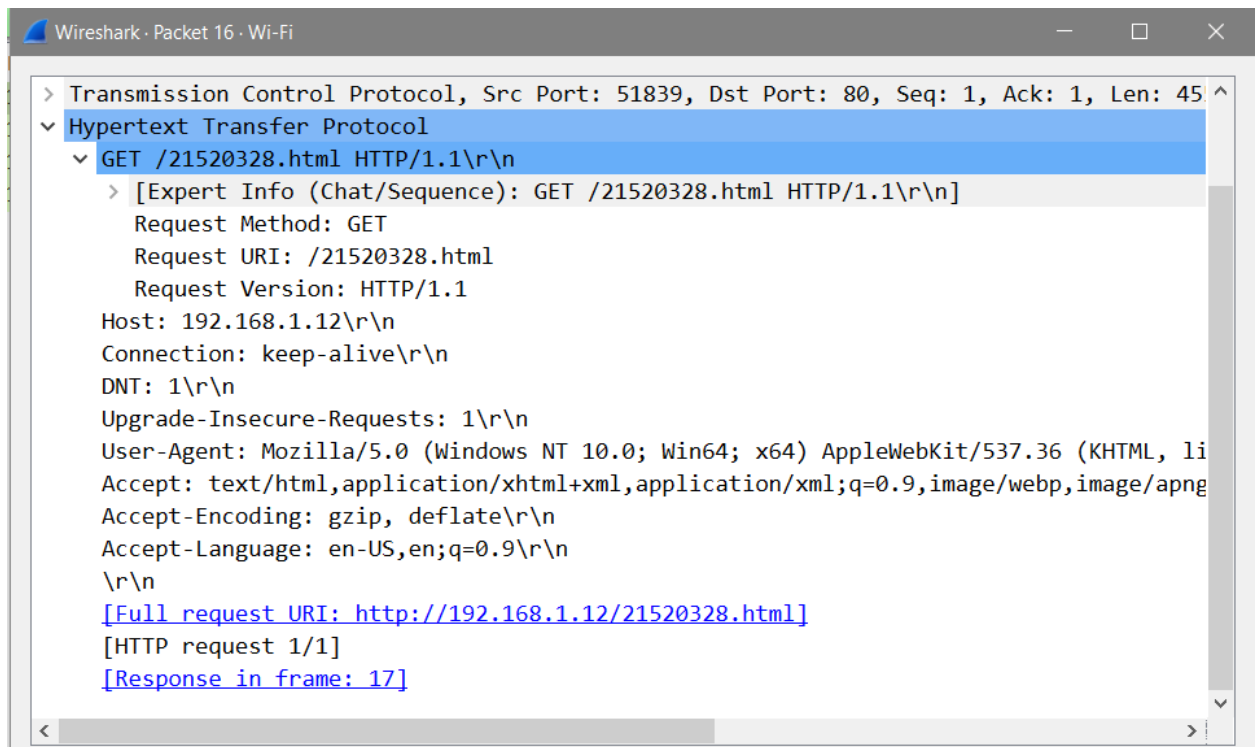
2. Địa chỉ IP của máy tính: 192.168.1.10

Địa chỉ IP của web server: 192.168.1.12

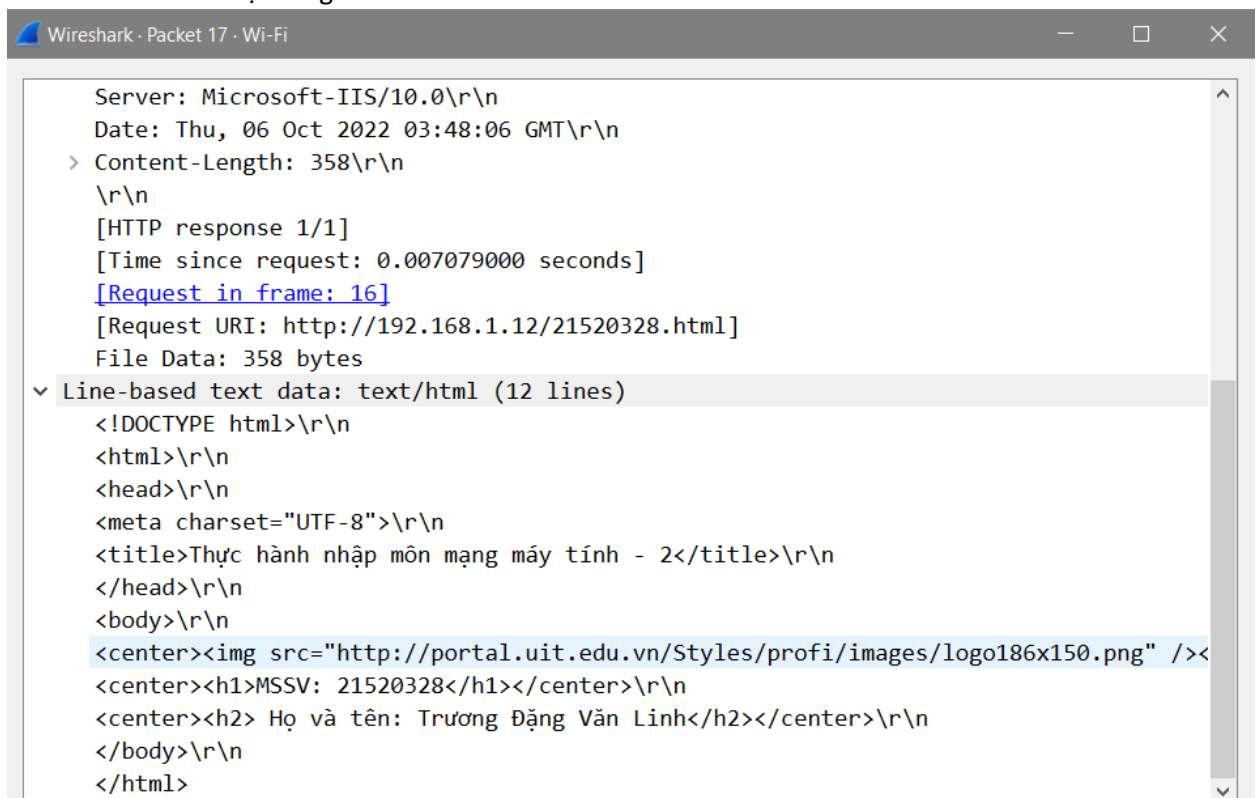
3. Status code: 200 OK

4. Server trả về 637 byte nội dung.

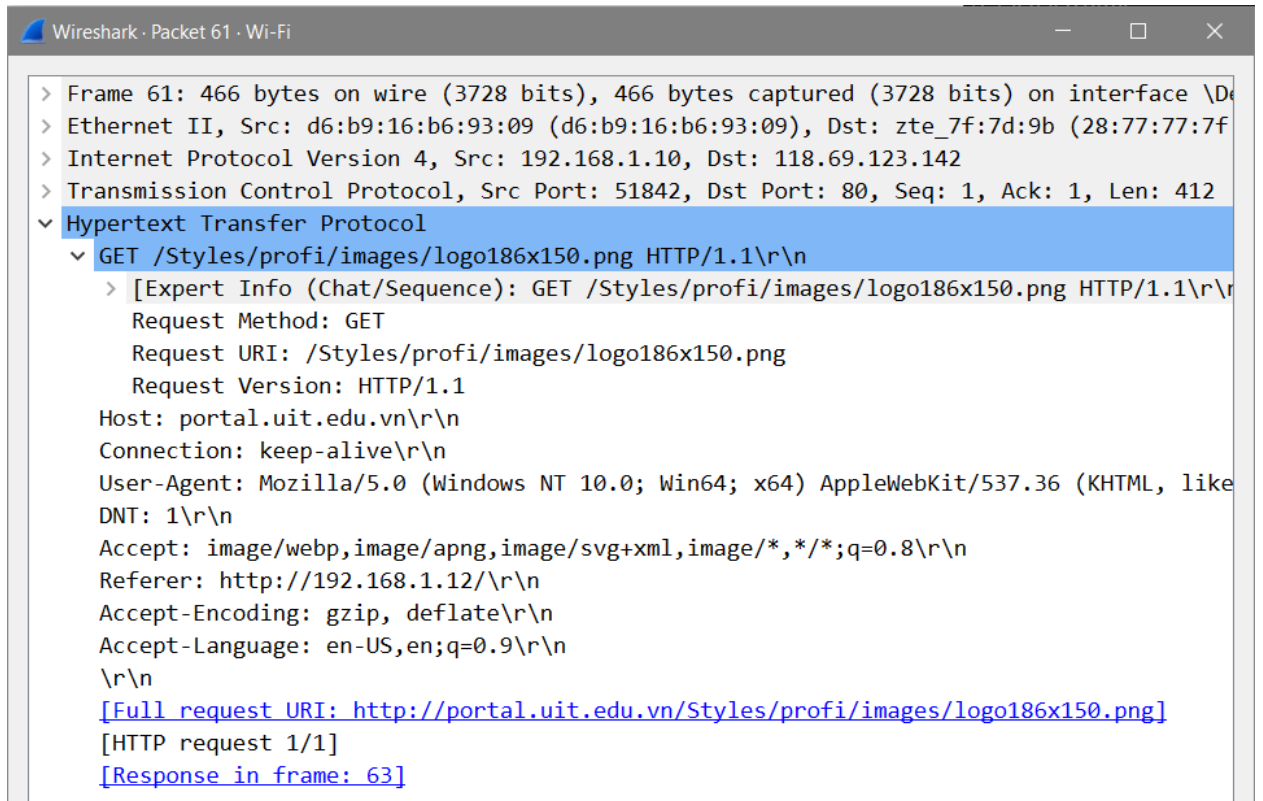
5. Không có dòng "IF-MODIFIED-SINCE":



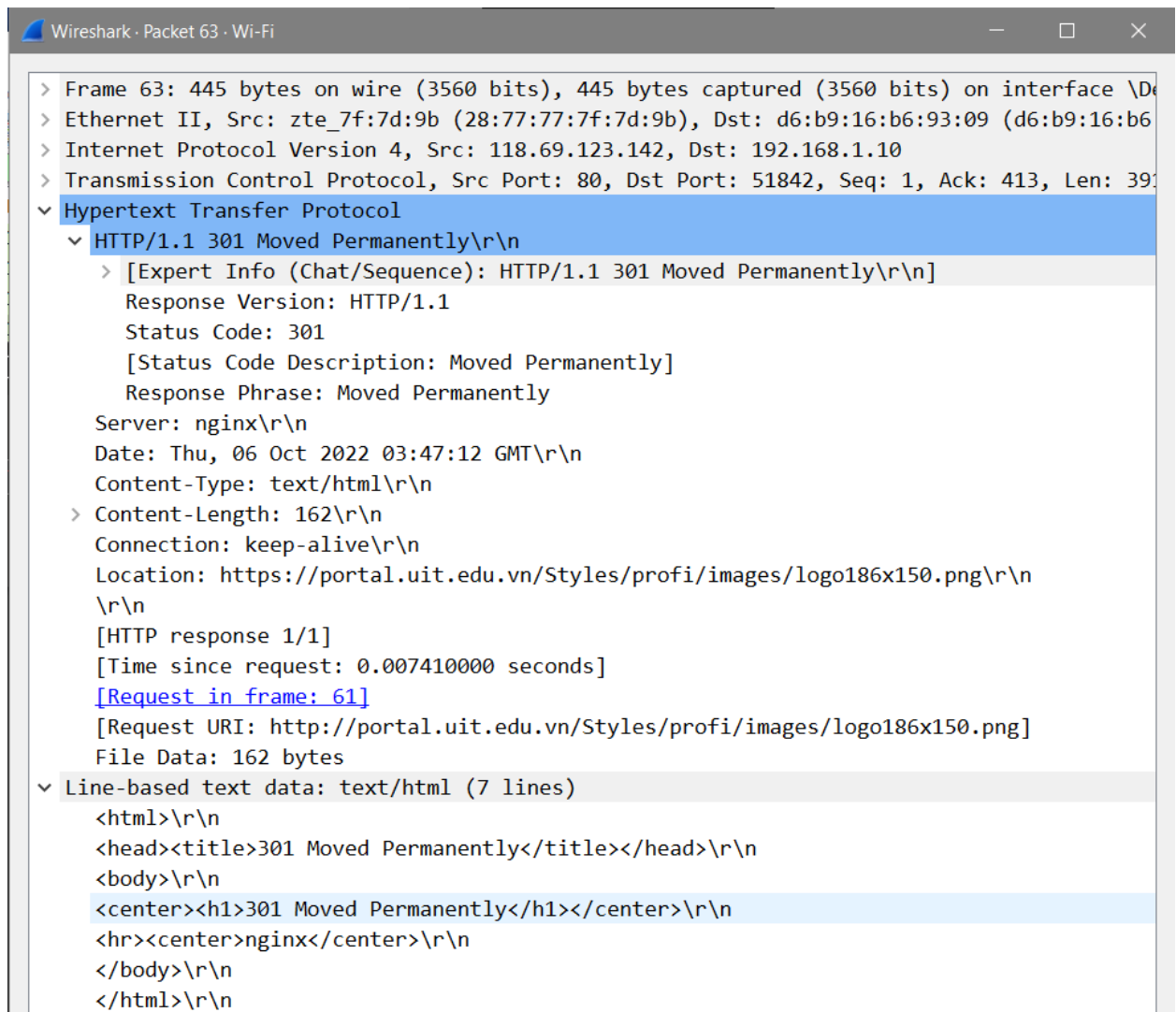
6. Server có trả về nội dung của file:



7. Không có dòng "IF-MODIFIED-SINCE":



8. Status code là 301 Moved Permanently. Ý nghĩa của status code là trang muốn truy cập đã được chuyển tiếp đến một trang khác. Server không trả về nội dung của file, nó trả về thông báo kết nối HTTP đã được chuyển sang kết nối HTTPS, sau đó trình duyệt điều hướng về kết nối HTTPS:



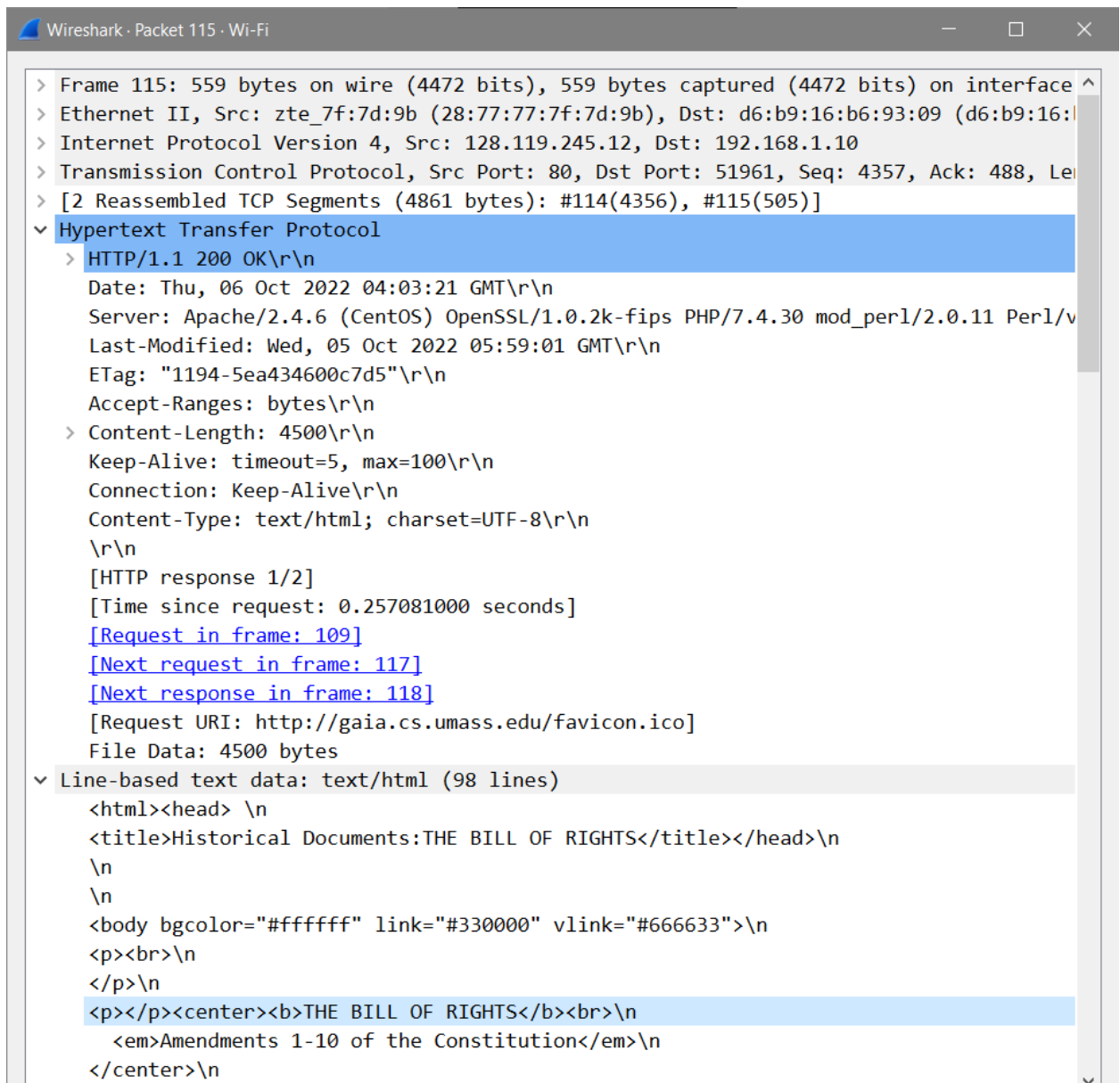
9. Trình duyệt gửi 2 HTTP GET. Đến 192.168.1.12 và 118.69.123.142 (portal.uit.edu.vn):

No.	Time	Source	Destination	Protocol	Length	Info
16	4.376683	192.168.1.10	192.168.1.12	HTTP	509	GET /21520328.html HTTP/1.1
17	4.383762	192.168.1.12	192.168.1.10	HTTP	637	HTTP/1.1 200 OK (text/html)
61	5.592484	192.168.1.10	118.69.123.142	HTTP	466	GET /Styles/profi/images/logo186x150.png HTTP/1.1
63	5.599894	118.69.123.142	192.168.1.10	HTTP	445	HTTP/1.1 301 Moved Permanently (text/html)

3.

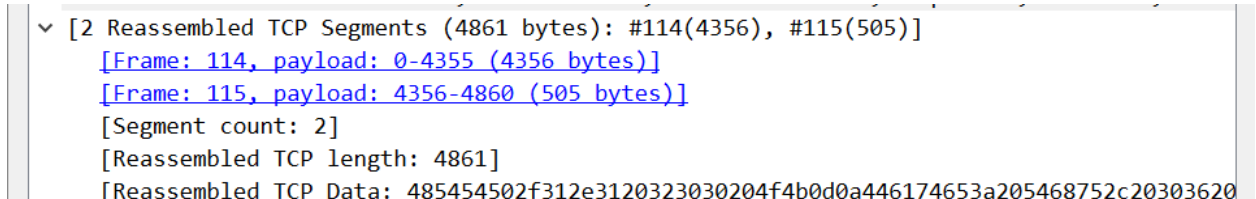
10. Trình duyệt gửi 2 HTTP GET. Dòng "THE BILL OF RIGHTS" ở trong gói tin phản hồi thứ nhất:

No.	Time	Source	Destination	Protocol	Length	Info
109	3.851978	192.168.1.10	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wireshark-f... HTTP/1.1
115	4.109059	128.119.245.12	192.168.1.10	HTTP	559	HTTP/1.1 200 OK (text/html)
117	4.144384	192.168.1.10	128.119.245.12	HTTP	487	GET /favicon.ico HTTP/1.1
118	4.401803	128.119.245.12	192.168.1.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)



```
Wireshark · Packet 115 · Wi-Fi
> Frame 115: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface ^
> Ethernet II, Src: zte_7f:7d:9b (28:77:77:7f:7d:9b), Dst: d6:b9:16:b6:93:09 (d6:b9:16:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 51961, Seq: 4357, Ack: 488, Le
> [2 Reassembled TCP Segments (4861 bytes): #114(4356), #115(505)]
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Thu, 06 Oct 2022 04:03:21 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v
    Last-Modified: Wed, 05 Oct 2022 05:59:01 GMT\r\n
    ETag: "1194-5ea434600c7d5"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.257081000 seconds]
    [Request in frame: 109]
    [Next request in frame: 117]
    [Next response in frame: 118]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 4500 bytes
  ▼ Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
    <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
```

11. Cần 2 TCP segments:



```
▼ [2 Reassembled TCP Segments (4861 bytes): #114(4356), #115(505)]
  [Frame: 114, payload: 0-4355 (4356 bytes)]
  [Frame: 115, payload: 4356-4860 (505 bytes)]
  [Segment count: 2]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a205468752c20303620
```

4.

12. Status code là 401 Unauthorized. Khi thực hiện HTTP GET đầu tiên, người dùng không được phép truy cập vì nó được bảo vệ bởi password và username. Do đó server trả về status code 401.

No.	Time	Source	Destination	Protocol	Length	Info
10	4.369028	192.168.1.10	128.119.245.12	HTTP	557	GET /wireshark-labs/protected_pages/HTTI
14	4.625105	128.119.245.12	192.168.1.10	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

13. Trường Authorization mới xuất hiện:

HTTP GET 1:

Wireshark · Packet 10 · Wi-Fi

- > Frame 10: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface \Device\NPF...
- > Ethernet II, Src: d6:b9:16:b6:93:09 (d6:b9:16:b6:93:09), Dst: zte_7f:7d:9b (28:77:77:7f:7f:7f)
- > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
- > Transmission Control Protocol, Src Port: 51983, Dst Port: 80, Seq: 1, Ack: 1, Len: 503
- ▼ Hypertext Transfer Protocol
 - > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - Connection: keep-alive\r\n
 - DNT: 1\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/80.0.4012.101 Safari/537.36\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n

[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html\]](#)
[\[HTTP request 1/1\]](#)
[\[Response in frame: 14\]](#)

HTTP GET 2:

Wireshark · Packet 196 · Wi-Fi

- > Frame 196: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF...
- > Ethernet II, Src: d6:b9:16:b6:93:09 (d6:b9:16:b6:93:09), Dst: zte_7f:7d:9b (28:77:77:7f:7f:7f)
- > Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
- > Transmission Control Protocol, Src Port: 51984, Dst Port: 80, Seq: 1, Ack: 1, Len: 588
- ▼ Hypertext Transfer Protocol
 - > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - Connection: keep-alive\r\n
 - Cache-Control: max-age=0\r\n
 - > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmMs=\r\n
 - DNT: 1\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/80.0.4012.101 Safari/537.36\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n

[\[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html\]](#)
[\[HTTP request 1/1\]](#)
[\[Response in frame: 205\]](#)