

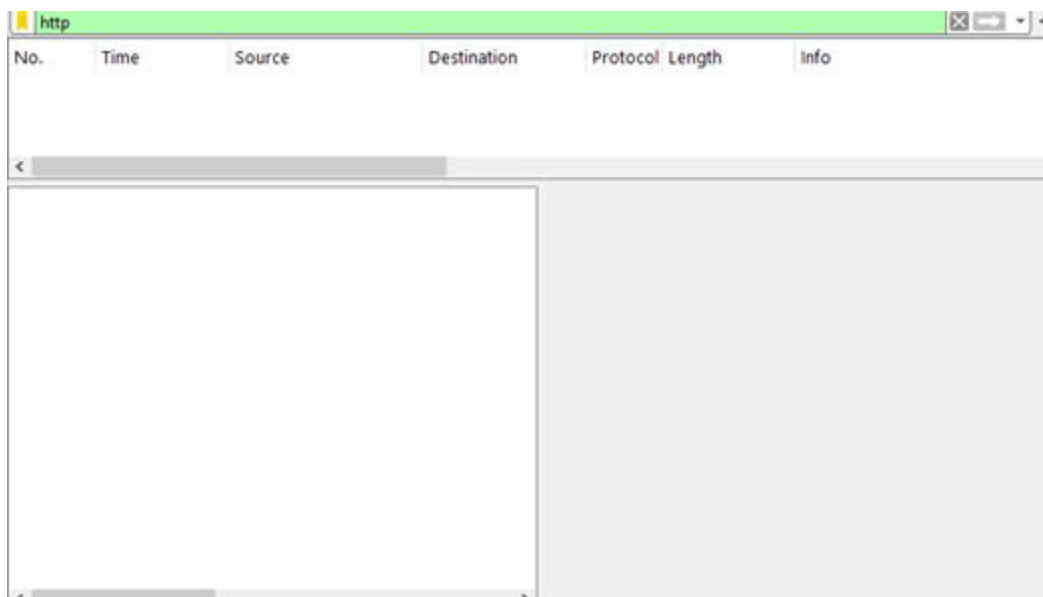
Bài Kiểm Tra DHKL16A1HN

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.

No.	Time	Source	Destination	Protocol	Length	Info
7876	52.728589	172.31.35.246	44.228.249.3	TCP	66	50508 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
7942	52.938012	44.228.249.3	172.31.35.246	TCP	66	80 → 50508 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
7944	52.938154	172.31.35.246	44.228.249.3	TCP	54	50508 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
7957	53.269186	172.31.35.246	44.228.249.3	HTTP	491	GET /images/logo.gif HTTP/1.1
7964	53.482999	44.228.249.3	172.31.35.246	TCP	60	80 → 50508 [PSH, ACK] Seq=1 Ack=438 Win=62336 Len=0
7965	53.482999	44.228.249.3	172.31.35.246	TCP	294	80 → 50508 [PSH, ACK] Seq=1 Ack=438 Win=62336 Len=240 [TCP PDU reassembled in 7970]
7966	53.482999	44.228.249.3	172.31.35.246	TCP	1506	[TCP Previous segment not captured] 80 → 50508 [PSH, ACK] Seq=1693 Ack=438 Win=62336 Len=1452 [TCP PDU reassembled in 7970]
7967	53.482999	44.228.249.3	172.31.35.246	TCP	1506	[TCP Out-Of-Order] 80 → 50508 [ACK] Seq=241 Ack=438 Win=62336 Len=1452 [TCP PDU reassembled in 7970]
7968	53.482999	44.228.249.3	172.31.35.246	TCP	1506	80 → 50508 [ACK] Seq=3145 Ack=438 Win=62336 Len=1452 [TCP PDU reassembled in 7970]
7969	53.482999	44.228.249.3	172.31.35.246	TCP	1506	80 → 50508 [PSH, ACK] Seq=4597 Ack=438 Win=62336 Len=1452 [TCP PDU reassembled in 7970]
7970	53.482999	44.228.249.3	172.31.35.246	HTTP	906	HTTP/1.1 200 OK (GIF89a)
7971	53.483112	172.31.35.246	44.228.249.3	TCP	66	50508 → 80 [ACK] Seq=438 Ack=241 Win=65280 Len=0 SLE=1693 SRE=3145
7972	53.483202	172.31.35.246	44.228.249.3	TCP	54	50508 → 80 [ACK] Seq=438 Ack=3145 Win=65280 Len=0
7973	53.483226	172.31.35.246	44.228.249.3	TCP	54	50508 → 80 [ACK] Seq=438 Ack=6901 Win=65280 Len=0
7976	53.551562	172.31.35.246	44.228.249.3	HTTP	487	GET /favicon.ico HTTP/1.1
8017	53.765009	44.228.249.3	172.31.35.246	TCP	60	80 → 50508 [ACK] Seq=6901 Ack=871 Win=61952 Len=0
8018	53.765009	44.228.249.3	172.31.35.246	TCP	295	80 → 50508 [PSH, ACK] Seq=6901 Ack=871 Win=61952 Len=241 [TCP PDU reassembled in 8019]

> Frame 10478: 743 bytes on wire (5944 bits), 743 bytes captured (5944 bits) on interface \Device\NPF{01E... > Ethernet II, Src: Intel_b7:18:5d (f4:6d:3f:b7:18:5d), Dst: Cisco_b7:18:5d (ec:c0:18:b7:18:5d) > Internet Protocol Version 4, Src: 172.31.35.246, Dst: 44.228.249.3 > Transmission Control Protocol, Src Port: 50508, Dst Port: 80, Seq: 871, Ack: 8036, Len: 689 > Hypertext Transfer Protocol > HTML Form URL Encoded: application/x-www-form-urlencoded	<pre> 0000  ec c0 18 b7 18 5d f4 6d 3f b7 18 5d 00 00 00 00  ....]...E- 0010  02 d9 00 3c 40 00 80 06 00 00 ac 1f 23 f6 2c e4  ....@...-...#... 0020  f9 03 c5 4c 00 50 3e ad 42 6d 40 f7 40 00 50 18  ....L.P&gt;...Bm@.P- 0030  00 fb f8 c8 00 00 50 4f 53 54 20 2f 75 73 65 72  .........PO ST /user 0040  69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e  info.php HTTP/1. 0050  31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70  1- Host: testphp 0060  2e 76 75 6c 6e 77 65 62 20 63 6f 6d 0a 43 6f  .vulnweb .com Co 0070  6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61  nnection : keep-a 0080  6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  live: Content-Le 0090  6e 67 74 68 3a 20 32 32 0d 0a 43 61 63 68 65 2d  ngth: 22 . Cache- 00a0  43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65  Control: max-age 00b0  3d 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70  =0 .Orig in: http 00c0  3a 2f 2f 74 65 73 74 70 68 70 2e 70 75 6e 74 74  //testphp.vulnweb 00d0  62 72 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d  .php.com Content- 00e0  54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f  Type: applicatio 00f0  6e 2f 78 2d 77 77 77 72 66 6f 72 6d 2d 75 72 6c  n/x-www-form-url 0100  65 6e 63 6f 64 65 64 0d 0a 55 70 67 72 61 64 65  encoded- Upgrade 0110  2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73  -Insecure- Reques 0120  74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e  ts: 1.0 ser-Agen 0130  74 3a 20 4d 6f 7a 69 6e 6e 61 2f 35 2e 30 20 28  t: Mozilla/5.0 ( 0140  57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b  Windows NT 10.0; 0150  20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70  Win64; x64) App 0160  6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20  leWebKit /537.36 </pre>
---	---

Wireshark - Packet 10478 - login\_test.pcapng

> Frame 10478: 743 bytes on wire (5944 bits), 743 bytes captured (5944 bits) on interface \Device\NPF\_{01D14539-FF3E-4EC1-AC6D-1AC173C0A106}, id 0  
> Ethernet II, Src: Intel\_be:31:92 (f4:6d:3f:be:31:92), Dst: Cisco\_b7:18:5d (ec:c0:18:b7:18:5d)  
> Internet Protocol Version 4, Src: 172.31.35.246, Dst: 44.228.249.3  
> Transmission Control Protocol, Src Port: 50508, Dst Port: 80, Seq: 871, Ack: 8036, Len: 689  
> Hypertext Transfer Protocol  
> HTML Form URL Encoded: application/x-www-form-urlencoded

```
0000  ec c0 18 b7 18 5d f4 6d 3f be 31 92 08 00 45 00  ....]..m?1...E-
0010  02 d9 00 3c 40 00 80 06 00 00 ac 1f 23 f6 2c e4  ...<@...#,,
0020  f9 03 c5 4c 00 50 3e ad 42 6d 40 f7 40 00 50 18  ...L P>-Bm@ @ P-
0030  00 fb f8 c8 00 00 50 4f 53 54 20 2f 75 73 65 72  ....-P0 ST /user
0040  69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e  info.php HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70  1-Host: testphp
0060  2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f  .vulnweb .com- Co
0070  6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61  nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65  live-Content-Le
0090  6e 67 74 68 3a 20 32 32 0d 0a 43 61 63 68 65 2d  ngth: 22 --Cache-
00a0  43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65  Control: max-age
00b0  3d 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70  =0-Orig in: http
00c0  3a 2f 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77  ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d  eb.com- Content-
00e0  54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f  Type: applicatio
00f0  6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c  n/x-www- form-url
0100  65 6e 63 6f 64 65 64 0d 0a 55 70 67 72 61 64 65  encoded-Upgrade
0110  2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73  -Insecur e-Reques
```

No.: 10478 · Time: 107.104621 · Source: 172.31.35.246 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 743 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

☒ Show packet bytes    Layout: Vertical (Stacked)    Close Help

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)