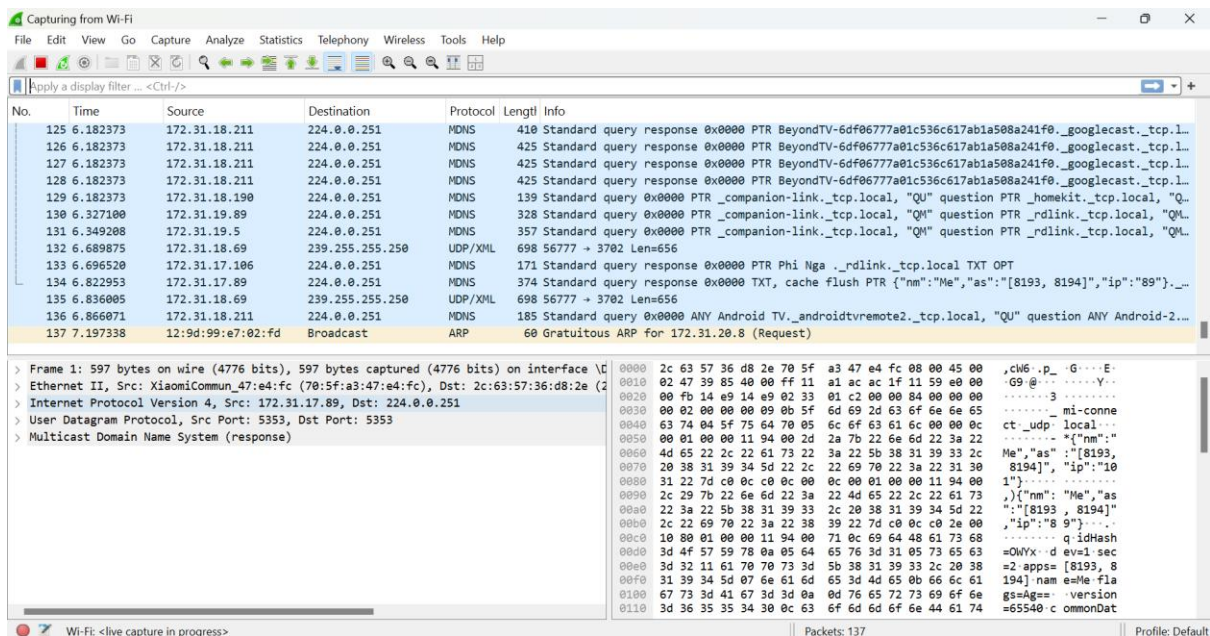


BÀI KIỂM TRA

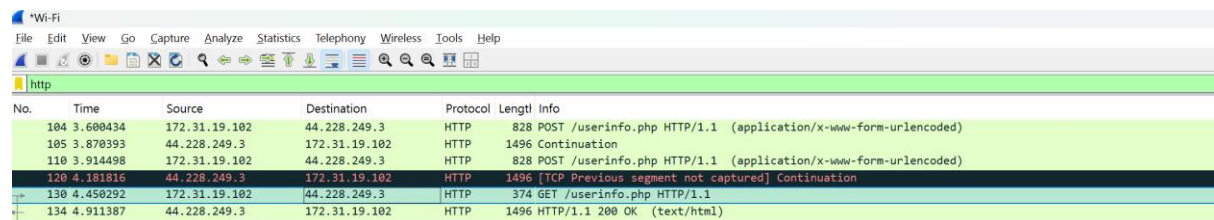
Họ và tên thành viên	Mã sinh viên
Phạm Thị Thu Trang	22174600030
Hoàng Sỹ Việt	22174600094

NỘI DUNG THỰC HIỆN:

Bước 1: Mở Wireshark, chọn card mạng, bắt gói tin truy cập 1 trang web.

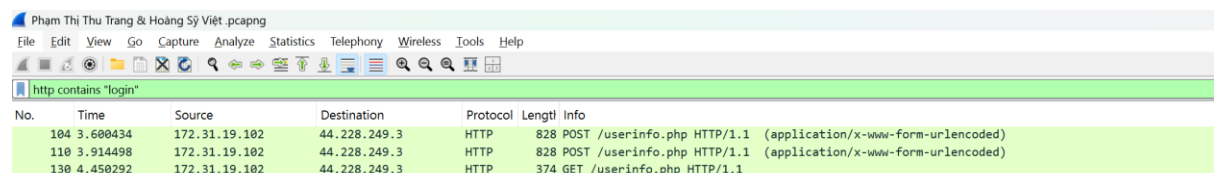


Bước 2: Lọc giao thức HTTP, truy cập một trang login, quan sát gói gửi dữ liệu:



No.	Time	Source	Destination	Protocol	Length	Info
104	3.600434	172.31.19.102	44.228.249.3	HTTP	828	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
105	3.870393	44.228.249.3	172.31.19.102	HTTP	1496	Continuation
110	3.914498	172.31.19.102	44.228.249.3	HTTP	828	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
120	4.181816	44.228.249.3	172.31.19.102	HTTP	1496	[TCP Previous segment not captured] Continuation
130	4.450292	172.31.19.102	44.228.249.3	HTTP	374	GET /userinfo.php HTTP/1.1
134	4.911387	44.228.249.3	172.31.19.102	HTTP	1496	HTTP/1.1 200 OK (text/html)

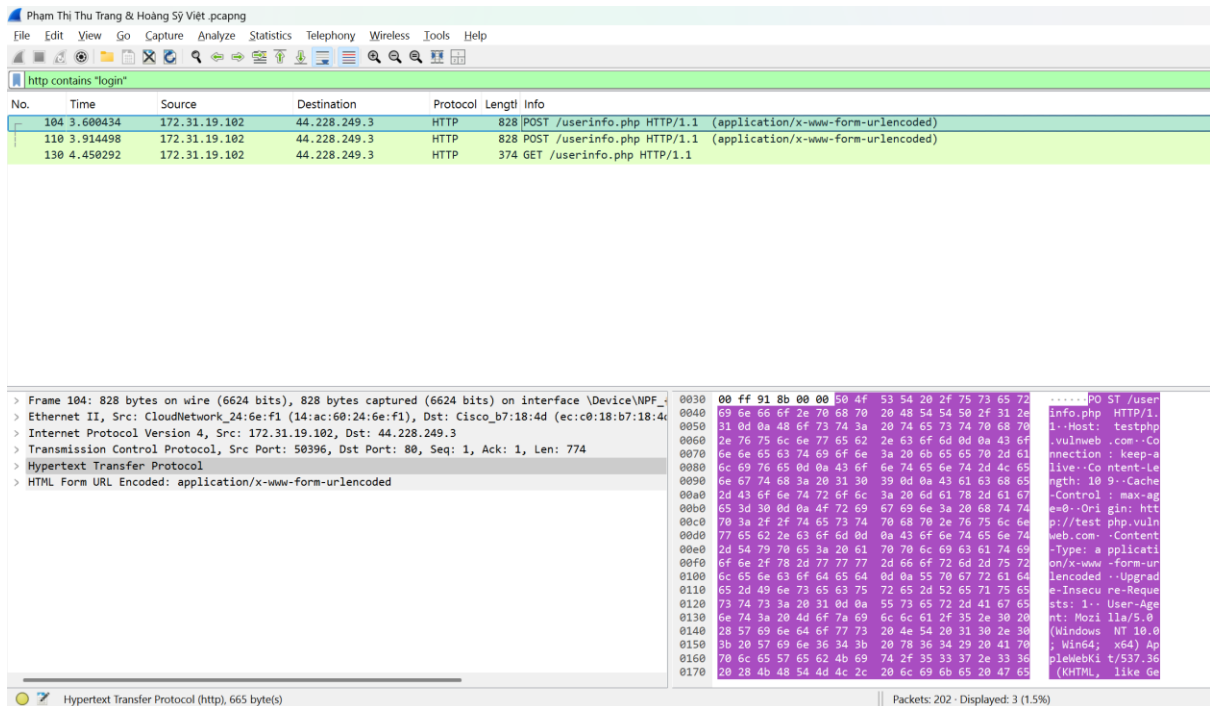
Bước 3: Lưu file kết quả bắt gói tin



No.	Time	Source	Destination	Protocol	Length	Info
104	3.600434	172.31.19.102	44.228.249.3	HTTP	828	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
110	3.914498	172.31.19.102	44.228.249.3	HTTP	828	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
130	4.450292	172.31.19.102	44.228.249.3	HTTP	374	GET /userinfo.php HTTP/1.1



Bước 4: Mở lại file đã lưu, phân tích từng lớp trong mô hình OSI



Tầng OSI	Tên tầng	Thông tin từ gói tin	Chi tiết
7	Application (Ứng dụng)	Hypertext Transfer Protocol (HTTP)	- Giao thức HTTP - Phương thức POST - Content-Type: application/x-www-form-urlencoded
6	Presentation (Trình diễn)	HTML Form URL Encoded	- Định dạng: application/x-www-form-urlencoded - Mã hóa dữ liệu form
5	Session (Phiên)	[Không hiển thị trực tiếp]	- Quản lý qua kết nối TCP - Không có thông tin phiên rõ ràng trong gói
4	Transport (Giao vận)	Transmission Control Protocol (TCP)	- Cổng nguồn: 50396 - Cổng đích: 80 (HTTP) - Sequence number: 1 - Acknowledgment number: 1 - Chiều dài dữ liệu: 774 bytes
3	Network (Mạng)	Internet Protocol Version 4	- IP nguồn: 172.31.19.102 - IP đích: 44.228.249.3

Tầng OSI	Tên tầng	Thông tin từ gói tin	Chi tiết
2	Data Link (Liên kết dữ liệu)	Ethernet II	- MAC nguồn: CloudNetwork_24:6e (14:ac:60:24:6e) - MAC đích: Cisco_b7:18:4d (ec:c0:18:b7:18:4d) - Kích thước frame: 828 bytes
1	Physical (Vật lý)	[Không hiển thị trực tiếp]	- Interface: \Device\NPF_{B09BFD5D-9054-4991-AD63-7DAC52C4E126} - 6624 bits truyền trên dây

Bước 5: Sử dụng tính năng Protocol Hierarchy hoặc TCP Stream để quan sát toàn cục

Wireshark · Follow HTTP Stream (tcp.stream eq 5) · Phạm Thị Thu Trang & Hoàng Sỹ Việt.pcapng

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 109
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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
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
Referer: http://testphp.vulnweb.com/userinfo.php
Accept-Encoding: gzip, deflate
Accept-Language: vi,en-US;q=0.9,en;q=0.8
Cookie: login=test%2Ftest

username=admin&ucc=1234-5678-2300-9000&uemail=email%40email.com&uphone=2323345&uaddress=21+street&update=update
..[[[.....<i.....~.....?..*..).h...S....1....B%t&.j.+].5...!tD.JXDr(...O.z..%..)+.L...p.....|.....`1\$M..J....Y..... PS..
....."S...?6.ho.....q..4E.7.....Zp...SS.....dZ.0.V&..F]_E.h...l..P.{6:.E...Q.s.}....4.1!.G..U...[.....8....^D..."d...
.....R..C.]..p..z..}F..X.@m[G..0....%.w....}v..... 5....#...\.l..?#.N...z.ip..Q... 0.R~:....HMr>....a.../.,....>....
..kC....K...>....5W...
}.....s0..Z./G>...! @D...`a.wTy.*rC.6....c.]..oj>.i.....u.....M0..U...I(...\.....".t.DU.:1.../.....:w...=-i...>A..S...{.}.M<}>
N..8..'.AMj.B.\.....Nz.....}@...;wz.....5u.....}.%O.a\$X...E.xw.j.....[.=j.x.(...Q...~.%G...O.....+fB..m'.....Nz.Jt..
W..c4.3.....u1o5.....].+
...%=.z.5..M..ij.x.....^V..t@.ftA...&9^J....'.g.....p8Ln.....}.zz.q.....0%w.*.Yd2....Q..0..1..".r.}]...n:
>1x1z.....k;<...#.....R.N.e....".....1.B.....yG..cJ];y.....y.(A)....[.X's..F.g...bx}.Uz].'.
..w"-..[.....D.&..&.....S.5.hh-]...28..7.m_I..oy.....?..y...a?..
..n#Xj...#.....dz?J]...ji~..1'x.C.1...r}4...Vm.|.B.i.f.Y..S...On.ZUE..")=.7..\.Z.....
..m.'@...npzHUX<..a.n..Cb..I...{H...f}...>.....qO..t...A.....Z&q...*.N'2^..U&..vK.t...y....
..*z...v.....vy..4..k.....vt+.h.....6e.^R g.J<^
..6.=d.....Y.5..e..A.|;.....@j.Q...I5...[.....z.....gp...d.V.!q...91'.1;G_@OY...Wb.....\..y.N.2.n....\$a;.^..pgu...
+1...1...vN..z[/[...#.o..^..qS.1.[z.....oIg...
0

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (2216 bytes) Show as ASCII No delta times Stream 5

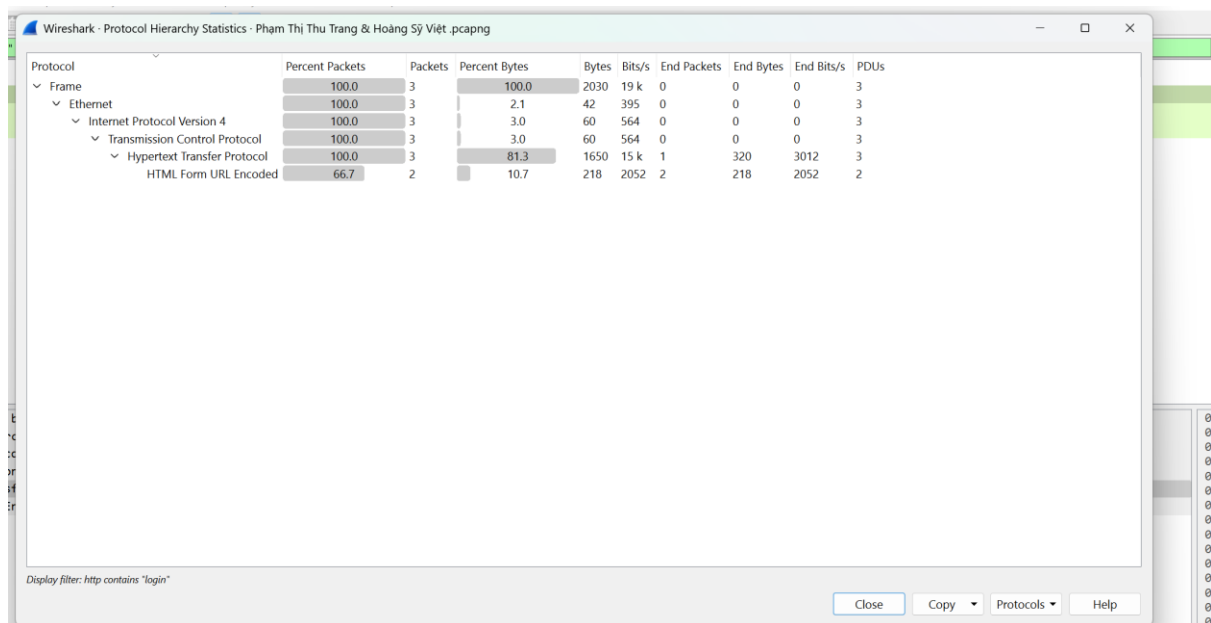
Find: Case sensitive Find Next

Filter Out This Stream Print Save as... Back Close Help

Wireshark · Follow TCP Stream (tcp.stream eq 5) · Phạm Thị Thu Trang & Hoàng Sỹ Việt.pcapng

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 109
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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
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
Referer: http://testphp.vulnweb.com/userinfo.php
Accept-Encoding: gzip, deflate
Accept-Language: vi,en-US;q=0.9,en;q=0.8
Cookie: login=test%2Ftest

username=admin&ucc=1234-5678-2300-9000&uemail=email%40email.com&uphone=2323345&uaddress=21+street&update=update
..[[[.....<i.....~.....?..*..).h...S....1....B%t&.j.+].5...!tD.JXDr(...O.z..%..)+.L...p.....|.....`1\$M..J....Y..... PS..
....."S...?6.ho.....q..4E.7.....Zp...SS.....dZ.0.V&..F]_E.h...l..P.{6:.E...Q.s.}....4.1!.G..U...[.....8....^D..."d...
.....R..C.]..p..z..}F..X.@m[G..0....%.w....}v..... 5....#...\.l..?#.N...z.ip..Q... 0.R~:....HMr>....a.../.,....>....
..kC....K...>....5W...
}.....s0..Z./G>...! @D...`a.wTy.*rC.6....c.]..oj>.i.....u.....M0..U...I(...\.....".t.DU.:1.../.....:w...=-i...>A..S...{.}.M<}>
N..8..'.AMj.B.\.....Nz.....}@...;wz.....5u.....}.%O.a\$X...E.xw.j.....[.=j.x.(...Q...~.%G...O.....+fB..m'.....Nz.Jt..
W..c4.3.....u1o5.....].+
...%=.z.5..M..ij.x.....^V..t@.ftA...&9^J....'.g.....p8Ln.....}.zz.q.....0%w.*.Yd2....Q..0..1..".r.}]...n:
>1x1z.....k;<...#.....R.N.e....".....1.B.....yG..cJ];y.....y.(A)....[.X's..F.g...bx}.Uz].'.
..w"-..[.....D.&..&.....S.5.hh-]...28..7.m_I..oy.....?..y...a?..
..n#Xj...#.....dz?J]...ji~..1'x.C.1...r}4...Vm.|.B.i.f.Y..S...On.ZUE..")=.7..\.Z.....
..m.'@...npzHUX<..a.n..Cb..I...{H...f}...>.....qO..t...A.....Z&q...*.N'2^..U&..vK.t...y....
..*z...v.....vy..4..k.....vt+.h.....6e.^R g.J<^
..6.=d.....Y.5..e..A.|;.....@j.Q...I5...[.....z.....gp...d.V.!q...91'.1;G_@OY...Wb.....\..y.N.2.n....\$a;.^..pgu...
+1...1...vN..z[/[...#.o..^..qS.1.[z.....oIg...
0



Đặc điểm	Mô tả
Loại giao thức	TCP là giao thức tầng 4 (transport layer), nền tảng cho HTTP tầng 7.
Kết nối	Sử dụng keep-alive giữ kết nối TCP mở, giảm overhead tái thiết lập.
Đảm bảo thứ tự	TCP chia nhỏ dữ liệu thành segment và đảm bảo đúng thứ tự khi đến nơi.
Đảm bảo độ tin cậy	Tự động gửi lại gói tin nếu bị mất trong quá trình truyền.
Kiểm soát lưu lượng	Điều chỉnh lượng dữ liệu gửi để không vượt quá khả năng tiếp nhận.
Kiểm soát tắc nghẽn	Tự động giảm tốc độ gửi khi phát hiện nghẽn mạng.

Bước 6: Viết mã Python dùng thư viện PyShark để truy xuất thông tin tầng 2 và tầng 3 từ file .pcapng.

```
import pyshark

# Đường dẫn đến file .pcapng đã thu được bằng Wireshark
file_path = r'C:\study\bai_kiem_tra\Bai Kiểm Tra\Phạm Thị Thu Trang & Hoàng Sỹ Việt .pcapng'

# Tạo đối tượng đọc file gói tin
cap = pyshark.FileCapture(file_path, use_json=True, keep_packets=False)

# Duyệt qua từng gói tin trong file
for i, pkt in enumerate(cap):
    try:
        print(f"\n=== Gói {i+1} ===")

        # Tầng 2: Data Link Layer (Ethernet)
        if 'eth' in pkt:
            print("Tầng 2 - MAC nguồn (Source MAC):", pkt.eth.src)
            print("Tầng 2 - MAC đích (Destination MAC):", pkt.eth.dst)

        # Tầng 3: Network Layer (IP)
        if 'ip' in pkt:
            print("Tầng 3 - IP nguồn (Source IP):", pkt.ip.src)
            print("Tầng 3 - IP đích (Destination IP):", pkt.ip.dst)
            print("Tầng 3 - Giao thức:", pkt.ip.proto)

    except Exception as e:
        print(f"Lỗi tại gói #{i+1}: {e}")

# Giới hạn số gói để xem (tùy chọn)
if i >= 10:
    break
```

Dưới đây là kết quả:

```
=== Gói 1 ===
Tầng 2 - MAC nguồn (Source MAC): 42:33:b6:6c:fe:6a
Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1
Tầng 3 - IP nguồn (Source IP): 172.31.19.143
Tầng 3 - IP đích (Destination IP): 224.0.0.251
Tầng 3 - Giao thức: 17
```

==== Gói 2 ====

Tầng 2 - MAC nguồn (Source MAC): f6:2f:87:d5:68:69

Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1

Tầng 3 - IP nguồn (Source IP): 172.31.19.207

Tầng 3 - IP đích (Destination IP): 224.0.0.251

Tầng 3 - Giao thức: 17

==== Gói 3 ====

Tầng 2 - MAC nguồn (Source MAC): ec:c0:18:b7:18:4d

Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1

Tầng 3 - IP nguồn (Source IP): 34.237.73.95

Tầng 3 - IP đích (Destination IP): 172.31.19.102

Tầng 3 - Giao thức: 6

==== Gói 4 ====

Tầng 2 - MAC nguồn (Source MAC): 14:ac:60:24:6e:f1

Tầng 2 - MAC đích (Destination MAC): ec:c0:18:b7:18:4d

Tầng 3 - IP nguồn (Source IP): 172.31.19.102

Tầng 3 - IP đích (Destination IP): 34.237.73.95

Tầng 3 - Giao thức: 6

==== Gói 5 ====

Tầng 2 - MAC nguồn (Source MAC): 14:ac:60:24:6e:f1

Tầng 2 - MAC đích (Destination MAC): ec:c0:18:b7:18:4d

Tầng 3 - IP nguồn (Source IP): 172.31.19.102

Tầng 3 - IP đích (Destination IP): 13.107.246.73

Tầng 3 - Giao thức: 6

==== Gói 6 ====

Tầng 2 - MAC nguồn (Source MAC): ec:c0:18:b7:18:4d

Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1

Tầng 3 - IP nguồn (Source IP): 13.107.246.73

Tầng 3 - IP đích (Destination IP): 172.31.19.102

Tầng 3 - Giao thức: 6

==== Gói 7 ====

Tầng 2 - MAC nguồn (Source MAC): dc:b7:ac:0e:0e:e2

Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1

Tầng 3 - IP nguồn (Source IP): 34.237.73.95

Tầng 3 - IP đích (Destination IP): 172.31.19.102

Tầng 3 - Giao thức: 6

==== Gói 8 ====

Tầng 2 - MAC nguồn (Source MAC): dc:b7:ac:0e:0e:e2
Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1
Tầng 3 - IP nguồn (Source IP): 172.31.17.140
Tầng 3 - IP đích (Destination IP): 224.0.0.251
Tầng 3 - Giao thức: 17

==== Gói 9 ====

Tầng 2 - MAC nguồn (Source MAC): dc:b7:ac:0e:0e:e2
Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1
Tầng 3 - IP nguồn (Source IP): 172.31.18.211
Tầng 3 - IP đích (Destination IP): 224.0.0.251
Tầng 3 - Giao thức: 17

==== Gói 10 ====

Tầng 2 - MAC nguồn (Source MAC): dc:b7:ac:0e:0e:e2
Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1
Tầng 3 - IP nguồn (Source IP): 172.31.18.211
Tầng 3 - IP đích (Destination IP): 224.0.0.251
Tầng 3 - Giao thức: 17

==== Gói 11 ====

Tầng 2 - MAC nguồn (Source MAC): dc:b7:ac:0e:0e:e2
Tầng 2 - MAC đích (Destination MAC): 14:ac:60:24:6e:f1
Tầng 3 - IP nguồn (Source IP): 172.31.18.211
Tầng 3 - IP đích (Destination IP): 224.0.0.251
Tầng 3 - Giao thức: 17