

### BÀI THỰC HÀNH 3

Họ tên: Nguyễn Trần Bảo Anh

MSSV: 22520066

#### **Bắt gói và phân tích UDP**

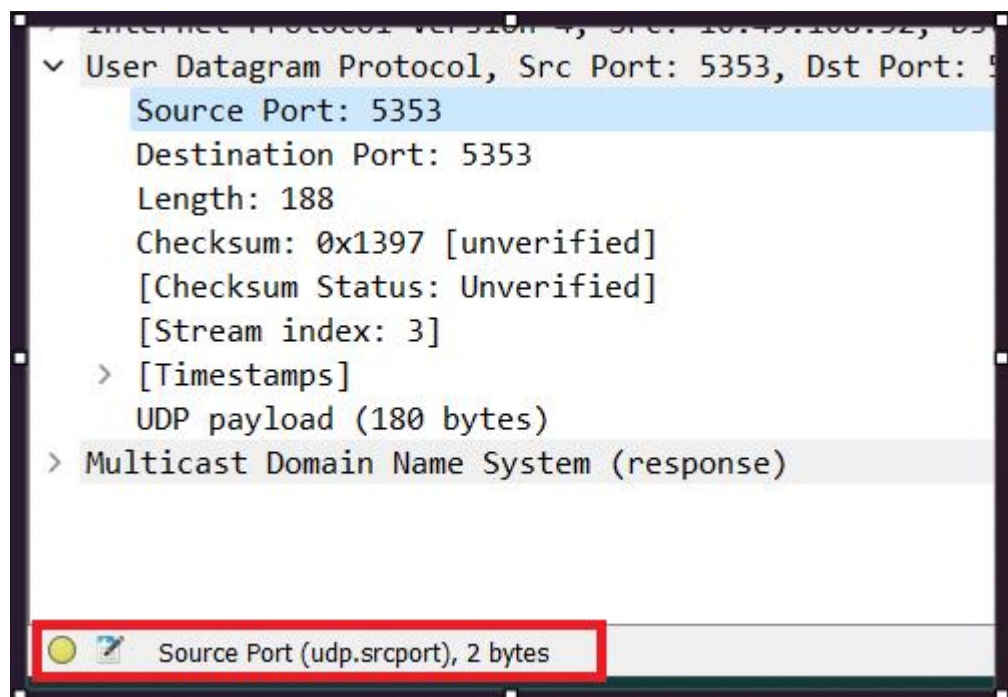
##### **1. Chọn một gói tin UDP, xác định các trường (field) trong UDP header?**

- Source port: Số hiệu cổng nơi đã gửi gói dữ liệu (datagram).
- Destination port: Số hiệu cổng nơi datagram được chuyển tới.
- Length: Độ dài tổng cộng kể cả phần header của gói UDP datagram.
- Checksum: Trường checksum dùng cho việc kiểm tra lỗi của phần header và dữ liệu, nếu phát hiện lỗi thì UDP datagram sẽ bị loại bỏ mà không có thông báo trả về nơi gửi.


```
▼ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  Source Port: 5353
  Destination Port: 5353
  Length: 188
  Checksum: 0x1397 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  > [Timestamps]
  UDP payload (180 bytes)
  > Multicast Domain Name System (response)
```

##### **2. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?**


- Độ dài của mỗi trường trong UDP header là 2 bytes.



✓ User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
Source Port: 5353  
Destination Port: 5353  
Length: 188  
Checksum: 0x1397 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 3]  
> [Timestamps]  
UDP payload (180 bytes)  
> Multicast Domain Name System (response)


 Destination Port (udp.dstport), 2 bytes

✓ User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
Source Port: 5353  
Destination Port: 5353  
Length: 188  
Checksum: 0x1397 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 3]  
> [Timestamps]  
UDP payload (180 bytes)  
> Multicast Domain Name System (response)

 Length in octets including this header and the data (udp.length), 2 bytes

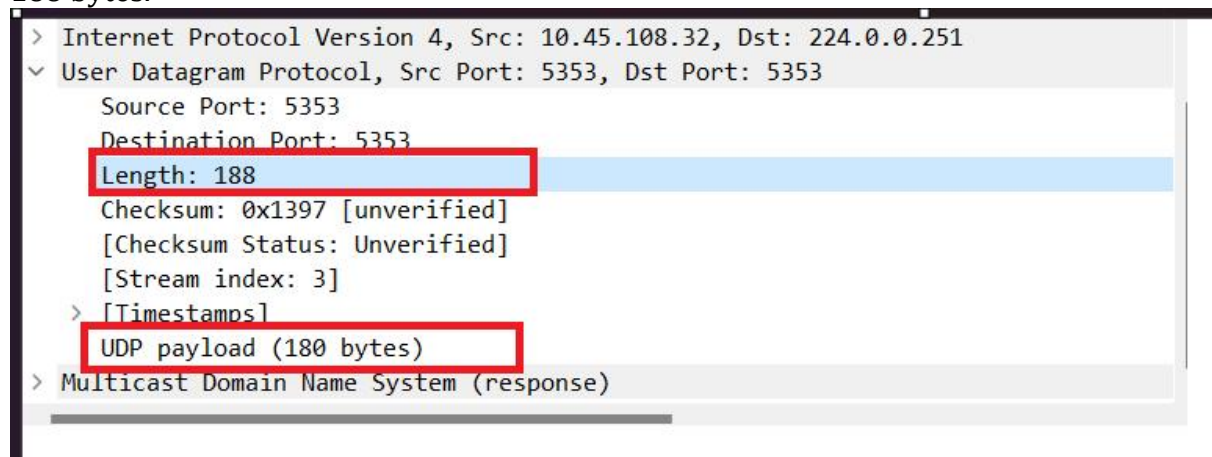
Internet Protocol Version 4, Src: 10.45.100.52, Dst: 224.0.0.251

✓ User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
Source Port: 5353  
Destination Port: 5353  
Length: 188  
Checksum: 0x1397 [unverified]  
[Checksum Status: Unverified]  
[Stream index: 3]  
> [Timestamps]  
UDP payload (180 bytes)  
> Multicast Domain Name System (response)

 Details at: [https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChAdvChecksums.html](https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html) (udp.checksum), 2 bytes

### 3. Giá trị của trường Length là độ dài của cái gì? Chứng minh?

Giá trị của trường Length trong UDP header là độ dài của 8 bytes UDP header cộng với 180 bytes của data (UDP payload) tương đương với độ dài 188 bytes.



### 4. Số bytes lớn nhất mà payload của UDP có thể chứa?

Số bytes tối đa mà UDP payload có thể chứa là  $2^{16} - 1$  trừ đi 8 bytes của header, tức là  $65535 - 8 = 65527$  bytes

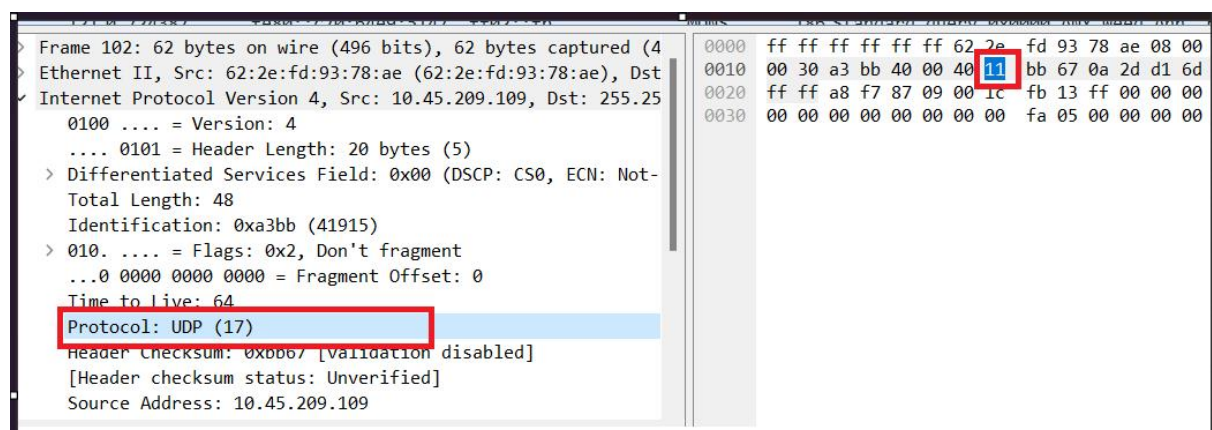
### 5. Giá trị lớn nhất có thể có của port nguồn?

Giá trị lớn nhất có thể có của port nguồn (Source port) là  $2^{16} - 1 = 65535$

### 6. Xác định protocol number của UDP (cả hệ 10 lẫn hệ 16)? Để trả lời câu hỏi này, chúng ta cần phải xem trường Protocol của IP header.

Protocol number UDP hệ 10 là 17

Protocol number UDP hệ 16 là 11





## Phân tích hành vi TCP

### 7. Tìm địa chỉ IP và TCP port của máy khách gửi file cho gaia.cs.umass.edu?

Địa chỉ IP của máy client là 10.45.86.179 và TCP port là 52076

http						
No.	Time	Source	Destination	Protocol	Length	Info
5301	15.730792	10.45.86.179	128.119.245.12	HTTP	1367	POST /wireshark-labs/lab3-1-reply.
5610	17.160154	128.119.245.12	10.45.86.179	HTTP	831	HTTP/1.1 200 OK (text/html)

> Frame 5301: 1367 bytes on wire (10936 bits), 1367 bytes captured (10936 bits) on interface \Device\NPF\_{7AEDC371-BB...}

> Ethernet II, Src: AzureWav\_70:22:28 (cc:47:40:70:22:28), Dst: JuniperN\_8c:35:b0 (44:f4:77:8c:35:b0)

> Internet Protocol Version 4, Src: 10.45.86.179, Dst: 128.119.245.12

▼ Transmission Control Protocol, Src Port: 52076, Dst Port: 80, Seq: 151621, Ack: 1, Len: 1313

Source Port: 52076

Destination Port: 80

[Stream index: 10]

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
4469	13.386926	10.45.86.179	128.119.245.12	TCP	54	52070 → 443 [FIN, ACK] Seq=1494
4470	13.386965	10.45.86.179	128.119.245.12	TCP	54	52070 → 443 [RST, ACK] Seq=1495
4471	13.387133	10.45.86.179	128.119.245.12	TCP	66	52075 → 80 [SYN] Seq=0 Win=64240
4472	13.387226	10.45.86.179	128.119.245.12	TCP	66	52076 → 80 [SYN] Seq=0 Win=64240
4558	13.644620	10.45.86.179	128.119.245.12	TCP	66	52077 → 80 [SYN] Seq=0 Win=64240
4570	13.669123	128.119.245.12	10.45.86.179	TCP	66	80 → 52076 [SYN, ACK] Seq=0 Ack=
4571	13.669256	10.45.86.179	128.119.245.12	TCP	54	52076 → 80 [ACK] Seq=1 Ack=1 Win=
4572	13.670036	10.45.86.179	128.119.245.12	TCP	666	52076 → 80 [PSH, ACK] Seq=1 Ack=

> Frame 4472: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{7AEDC371-BB...}

> Ethernet II, Src: AzureWav\_70:22:28 (cc:47:40:70:22:28), Dst: JuniperN\_8c:35:b0 (44:f4:77:8c:35:b0)

> Internet Protocol Version 4, Src: 10.45.86.179, Dst: 128.119.245.12

▼ Transmission Control Protocol, Src Port: 52076, Dst Port: 80, Seq: 0, Len: 0

Source Port: 52076

Destination Port: 80

[Stream index: 10]

### 8. Tìm địa chỉ IP của gaia.cs.umass.edu? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?

Địa chỉ IP server: 128.119.245.12 sử dụng port 80 để gửi và nhận các segments.

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
4469	13.386926	10.45.86.179	128.119.245.12	TCP	54	52070 → 443 [FIN, ACK] Seq=1494 Ack=
4470	13.386965	10.45.86.179	128.119.245.12	TCP	54	52070 → 443 [RST, ACK] Seq=1495 Ack=
4471	13.387133	10.45.86.179	128.119.245.12	TCP	66	52075 → 80 [SYN] Seq=0 Win=64240 Len=
4472	13.387226	10.45.86.179	128.119.245.12	TCP	66	52076 → 80 [SYN] Seq=0 Win=64240 Len=
4558	13.644620	10.45.86.179	128.119.245.12	TCP	66	52077 → 80 [SYN] Seq=0 Win=64240 Len=
4570	13.669123	128.119.245.12	10.45.86.179	TCP	66	80 → 52076 [SYN, ACK] Seq=0 Ack=1 Win=
4571	13.669256	10.45.86.179	128.119.245.12	TCP	54	52076 → 80 [ACK] Seq=1 Ack=1 Win=132
4572	13.670036	10.45.86.179	128.119.245.12	TCP	666	52076 → 80 [PSH, ACK] Seq=1 Ack=1 Win=

> Frame 4570: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{7AEDC371-BB...}

> Ethernet II, Src: JuniperN\_8c:35:b0 (44:f4:77:8c:35:b0), Dst: AzureWav\_70:22:28 (cc:47:40:70:22:28)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.86.179

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 52076, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 52076

[Stream index: 10]

**9. TCP SYN segment sử dụng sequence number nào để khởi tạo kết nối TCP giữa máy khách và gaia.cs.umass.edu? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?**

TCP SYN segment sử dụng sequence number là 0 vì nó được sử dụng để khởi tạo kết nối TCP giữa máy client và server.

Trong trường Flags, SYN flag được đặt thành 1 cho biết rằng segment này là một TCP SYN segment.

No.	Time	Source	Destination	Protocol	Length	Info
4469	13.386926	10.45.86.179	128.119.245.12	TCP	54	52070 → 443 [FIN, ACK] Seq=1494
4470	13.386965	10.45.86.179	128.119.245.12	TCP	54	52070 → 443 [RST, ACK] Seq=1495
4471	13.387133	10.45.86.179	128.119.245.12	TCP	66	52075 → 80 [SYN] Seq=0 Win=64240
4472	13.387226	10.45.86.179	128.119.245.12	TCP	66	52076 → 80 [SYN] Seq=0 Win=64240
4558	13.644620	10.45.86.179	128.119.245.12	TCP	66	52077 → 80 [SYN] Seq=0 Win=64240
4570	13.669123	128.119.245.12	10.45.86.179	TCP	66	80 → 52076 [SYN, ACK] Seq=0 Ack=

[Stream index: 10]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 3112946288  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 0  
Acknowledgment number (raw): 0  
1000 .... = Header Length: 32 bytes (8)  
Flags: 0x002 (SYN)  
000. .... = Reserved: Not set  
...0 .... = Accurate ECN: Not set  
.... 0... = Congestion Window Reduced: Not set  
.... .0.. = ECN-Echo: Not set  
.... ..0. = Urgent: Not set  
.... ...0 = Acknowledgment: Not set  
.... ....0... = Push: Not set  
.... ..0... = Reset: Not set  
.... ....1. = Syn: Set  
.... ....0 = Fin: Not set  
[TCP Flags: .....S.]

**10. Tìm sequence number của SYNACK segment được gửi bởi gaia.cs.umass.edu đến máy khách để trả lời cho SYN segment? Tìm giá trị của Acknowledgement trong SYNACK segment? Làm sao gaia.cs.umass.edu có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYNACK segment?**

Sequence number của gói tin SYN/ACK segment do server gửi đến máy client để trả lời cho SYN segment là 0.

Giá trị của trường Acknowledgement trong SYN/ACK segment là 1.

Một segment sẽ được xác định là SYN/ACK segment nếu cả giá trị SYN flag và Acknowledgement flag trong segment được đặt thành 1.

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
4472	13.387226	10.45.86.179	128.119.245.12	TCP	66	52076 → 80 [SYN] Seq=0 Win=64240 Len=0
4558	13.644620	10.45.86.179	128.119.245.12	TCP	66	52077 → 80 [SYN] Seq=0 Win=64240 Len=0
4570	13.669123	128.119.245.12	10.45.86.179	TCP	66	80 → 52076 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0

> Ethernet II, Src: JuniperN\_8c:35:b0 (44:f4:77:8c:35:b0), Dst: AzureWav\_70:22:28 (cc:47:40:70:22:28)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.86.179

✓ Transmission Control Protocol, Src Port: 80, Dst Port: 52076, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 52076

[Stream index: 10]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 671241118

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 3112946289

1000 .... = Header Length: 32 bytes (8)

✓ Flags: 0x012 (SYN, ACK)

000. .... = Reserved: Not set

...0 .... = Accurate ECN: Not set

....0... = Congestion Window Reduced: Not set

....0... = ECN-Echo: Not set

....0... = Urgent: Not set

....1... = Acknowledgment: Set

....0... = Push: Not set

....0... = Reset: Not set

> ....1. = Syn: Set

## 11.Tìm sequence number của TCP segment có chứa lệnh HTTP POST?

Sequence number của TCP segment có chứa lệnh HTTP POST: 1

tcp						
No.	Time	Source	Destination	Protocol	Length	Info
4583	13.670647	10.45.86.179	128.119.245.12	TCP	54	52075 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
4584	13.680558	128.119.245.12	10.45.86.179	TCP	56	[TCP Dup ACK 2131#1] 443 → 52070 [ACK] Seq=2422 Ack=1495 Win=32128 Len=0
4585	13.680558	128.119.245.12	10.45.86.179	TCP	56	443 → 52070 [ACK] Seq=2422 Ack=1495 Win=32128 Len=0
4623	13.909716	128.119.245.12	10.45.86.179	TCP	66	80 → 52077 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
4624	13.909898	10.45.86.179	128.119.245.12	TCP	54	52077 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
4686	14.096922	128.119.245.12	10.45.86.179	TCP	56	80 → 52076 [ACK] Seq=1 Ack=613 Win=30464 Len=0
4687	14.096950	10.45.86.179	128.119.245.12	TCP	1506	52076 → 80 [ACK] Seq=13681 Ack=1 Win=132096 Len=1452 [T...

> Frame 4686: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF\_{7AEDC371-BB4B-4043-919A-4B927C2C8A5A}

> Ethernet II, Src: JuniperN\_8c:35:b0 (44:f4:77:8c:35:b0), Dst: AzureWav\_70:22:28 (cc:47:40:70:22:28)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.45.86.179

✓ Transmission Control Protocol, Src Port: 80, Dst Port: 52076, Seq: 1, Ack: 613, Len: 0

Source Port: 80

Destination Port: 52076

[Stream index: 10]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 671241119

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 613 (relative ack number)

Acknowledgment number (raw): 3112946901

0101 .... = Header Length: 20 bytes (5)