

1. Chọn một gói tin UDP, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó?

Chọn gói tin số 29 với giao thức RTP, mở rộng phần User Datagram Protocol.

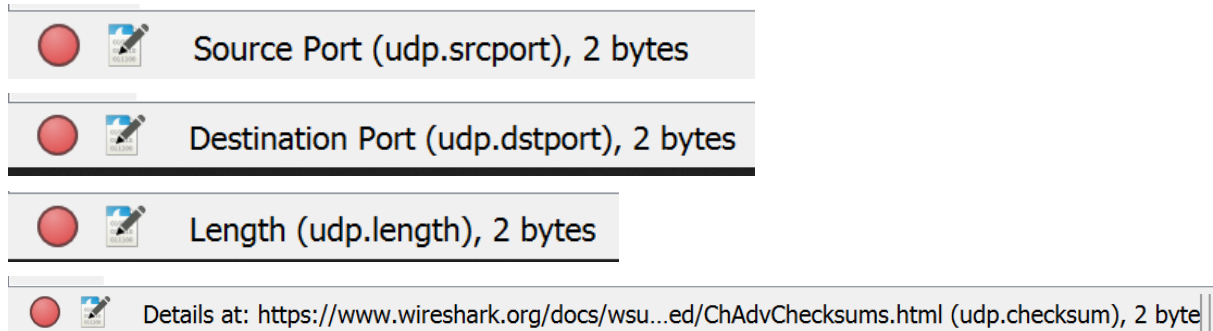
```
▼ User Datagram Protocol, Src Port: 51920, Dst Port: 51922
  Source Port: 51920
  Destination Port: 51922
  Length: 12
  Checksum: 0xaf36 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 3]
  > [Timestamps]
    UDP payload (4 bytes)
```

Các trường trong UDP header: Source Port, Destination Port, Length, Checksum.

- Source Port: Số port nguồn.
- Destination Port: Số port đích.
- Length: Độ dài được tính bằng byte của segment UDP, bao gồm cả header.
- Checksum: Dùng để kiểm tra segment có lỗi không.

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

Chọn gói tin 29. Chọn lần vào từng field và quan sát góc trái dưới.



Độ dài của các field trong UDP header:



- Source Port: 2 bytes.
- Destination Port: 2 bytes.
- Length: 2 bytes.
- Checksum: 2 bytes.

3. Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này?

Giá trị của length là độ dài được tính bằng byte của segment UDP, bao gồm cả header.

Length: 12

```
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> User Datagram Protocol, Src Port: 51920, Dst Port: 51922
> Real-Time Transport Protocol
```



  User Datagram Protocol (udp), 8 bytes

> [Timestamps]
UDP payload (4 bytes)

Real-Time Transport Protocol



Theo quan sát, UDP header là 8 bytes, UDP payload là 4 bytes, tổng là 12 bytes, đúng như giá trị của trường length.



4. Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa?

  Total Length (ip.len), 2 bytes

Trường total length của IP header có kích thước 2 bytes.



Kích thước tối đa gói tin là $2^{(2 * 8)} - 1 = 65535$ bytes.

  Internet Protocol Version 4 (ip), 20 bytes

  User Datagram Protocol (udp), 8 bytes

Số bytes lớn nhất mà payload là kích thước tối đa của gói tin trừ đi IP header và UDP header: $65535 - 20 - 8 = 65507$ bytes.

5. Giá trị lớn nhất có thể có của port nguồn (Source port)?

  Source Port (udp.srcport), 2 bytes

Trường source port của UDP header có kích thước 2 bytes.

Giá trị lớn nhất có thể có của port nguồn là $2^{(2 * 8)} - 1 = 65535$ bytes.

6. Tìm và kiểm tra một cặp gói tin sử dụng giao thức UDP gồm: gói tin do máy mình gửi và gói tin phản hồi của gói tin đó. Miêu tả mối quan hệ về port number của 2 gói tin này.

Tiến hành bắt gói tin khi truy cập một tên miền. Tìm dns. Chọn từng gói tin để tìm kiếm 2 gói tin có mũi tên trái, phải.

No.	Time	Source	Destination	Protocol	Length	Info
16	0.692423	2402:800:62af::1	2402:800:62b1:3...	ICMPv6	165	Destination Unreachable (no route to destination)
17	0.702197	192.168.1.8	203.113.188.1	DNS	97	Standard query 0x0802 AAAA r3---sn-8pxuuxa-nboz1.goog
18	0.702227	192.168.1.8	203.113.188.1	DNS	97	Standard query 0xadec A r3---sn-8pxuuxa-nboz1.google
19	0.778133	203.113.188.1	192.168.1.8	DNS	147	Standard query response 0xadec A r3---sn-8pxuuxa-nboz
20	0.778133	203.113.188.1	192.168.1.8	DNS	174	Standard query response 0x0802 AAAA r3---sn-8pxuuxa-n
426	6.397059	2402:800:62b1:3e22::...	2402:800:20ff:6...	DNS	95	Standard query 0xb4eb A dosomething.org

Ở gói tin 17

User Datagram Protocol, Src Port: 49796, Dst Port: 53
Source Port: 49796
Destination Port: 53

Ở gói tin 20

User Datagram Protocol, Src Port: 53, Dst Port: 49796
Source Port: 53
Destination Port: 49796

Số port nguồn của gói tin 17 là số port đích của gói tin 20 và ngược lại.

7. Tìm địa chỉ IP và TCP port của máy Client?

Tìm tcp.port == 8080. Quan sát info của gói tin bắt tay SYN..

Info
56536 → 8080 [SYN]

Số port trước mũi tên, tức 56536, là của client.

8. Tìm địa chỉ IP của Server? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?

Info
56536 → 8080 [SYN]

Quan sát tương tự câu 7. Số port sau mũi tên, tức 8080, là của server.

9. TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 1929481357

- Vào TCP header, số của sequence number (raw), tức 1929481357, chính là sequence number để khởi tạo kết nối TCP giữa client và server trong lần chạy này.

```
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): 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
```

- Thành phần cho biết segment đó là TCP SYN segment: Tại trường Flag trong TCP header, bit thứ 11 là 1 và bit thứ 8 bằng 0.

10.

Tim sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment?

Chọn gói trong info có [SYN, ACK], vào TCP header, quan sát sequence number (raw).

```
Transmission Control Protocol, Src Port: 8080, Dst Port: 56536
Source Port: 8080
Destination Port: 56536
[Stream index: 0]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3635023981
[Next Sequence Number: 1 (relative sequence number)]
```

Đáp án: 3635023981

Tim giá trị của Acknowledgement trong SYN/ACK segment?

Quan sát Acknowledgment number (raw) trong TCP header.

```
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1929481358
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
```

Đáp án: 1929481358

Làm sao server có thể xác định giá trị đó?

Giá trị đó do server sinh ngẫu nhiên.

Thành phần nào trong segment cho ta biết segment đó là SYN/ACK segment?

```
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): 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
```

Tại trường Flag trong TCP header, có bit thứ 8 và bit thứ 11 bằng 1.

11. Chỉ ra số thứ tự, thời gian gửi, thời gian nhận ACK, RTT của 6 segment đầu tiên mà server gửi cho client

STT	Thời gian gửi	Thời gian nhận ACK	RTT
4	6.969302	6.971203	0.001901
7	6.971203	6.992216	0.021013
8	6.991895	6.992216	0.000321
10	6.992216	9.529085	2.536869
13	9.529085	9.529304	0.000219
14	9.529146	9.529304	0.000158