Lab
3

BÁO CÁO BÀI THỰC HÀNH SỐ 3

Làm quen với Wireshark

Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Đoàn Phương Nam
Thời gian thực hiện	26/10/2023
Tự chấm điểm	10/10

TRẢ LỜI CÁC CÂU HỎI

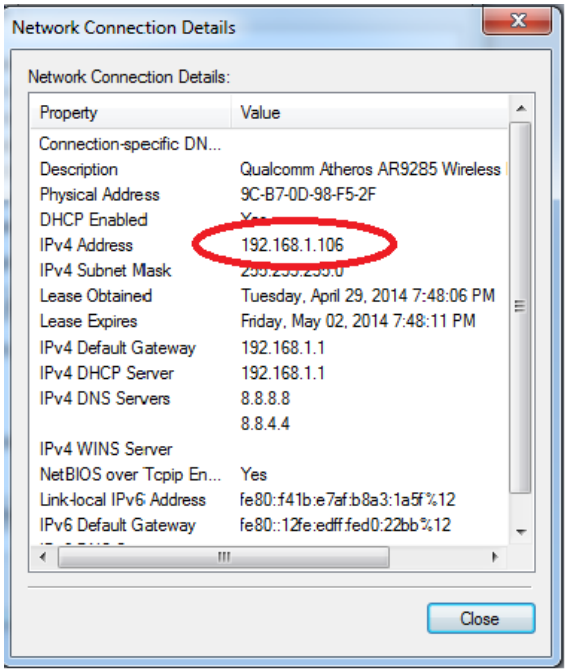
Gợi ý: *Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn*.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

Trả lời: *192.168.1.106*

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



Câu 1

IP address 192.168.222.83

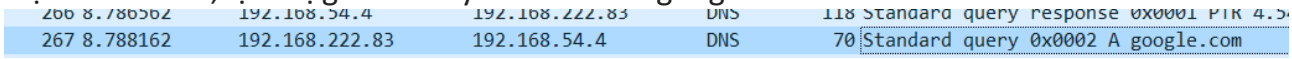
MAC address 08-97-98-E6-91-93

Default gateway IP address fe80::1a0f:76ff:fe92:f408%4
192.168.222.1

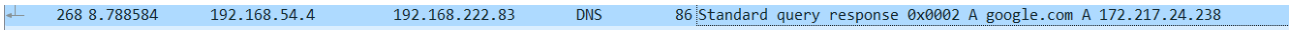
DNS server IP address 192.168.54.4
192.168.20.4

Câu 2

Tại danh sách ,định vị gói tin truy vấn domain google.com



Câu 3



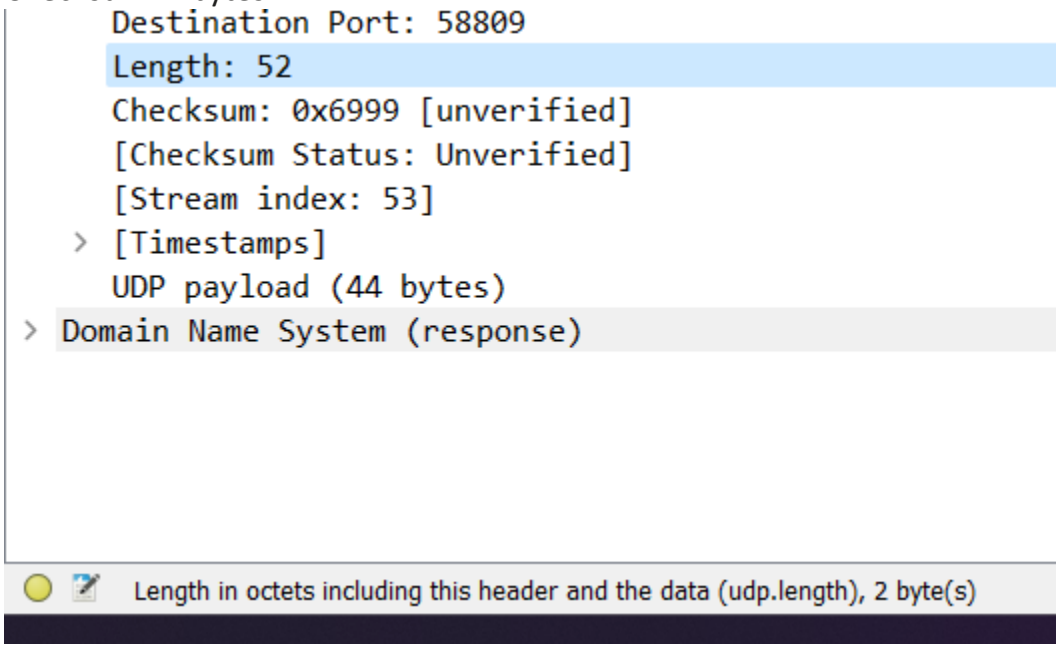
Tại danh sách, định vị gói tin phản hồi truy vấn trên

Câu 4

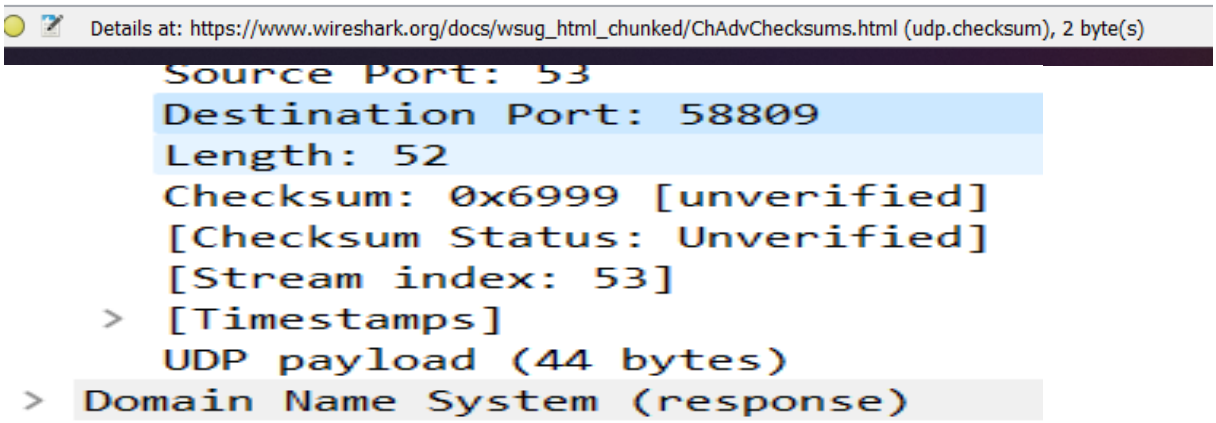
```
User Datagram Protocol, Src Port: 53
   Source Port: 53
   Destination Port: 58809
   Length: 52
   Checksum: 0x6999 [unverified]
   [Checksum Status: Unverified]
   [Stream index: 53]
 > [Timestamps]
   UDP payload (44 bytes)
```

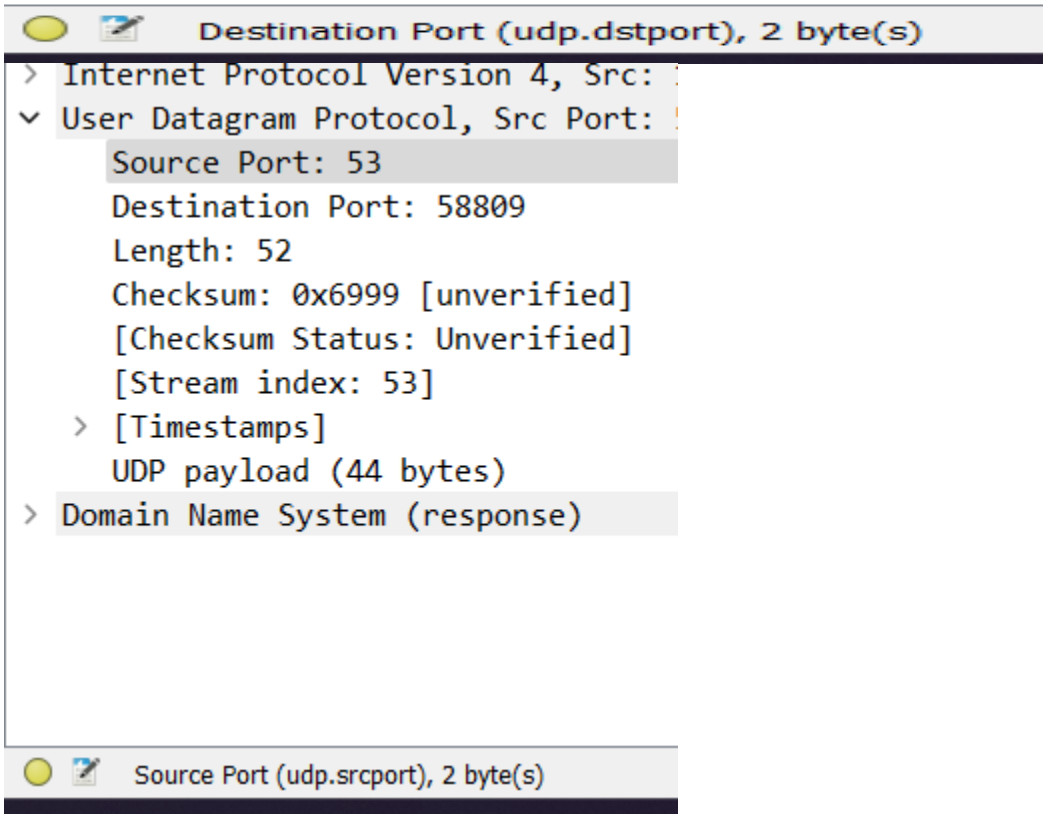
Xét gói tin số 268
Source Port: Port nguồn
Destination Port: Port đích
Length: Độ dài gói tin
Checksum: Giá trị kiểm tra

Câu 5
Source Port: 2 bytes
Destination Port: 2 bytes
Length: 2 bytes
Checksum: 2 bytes



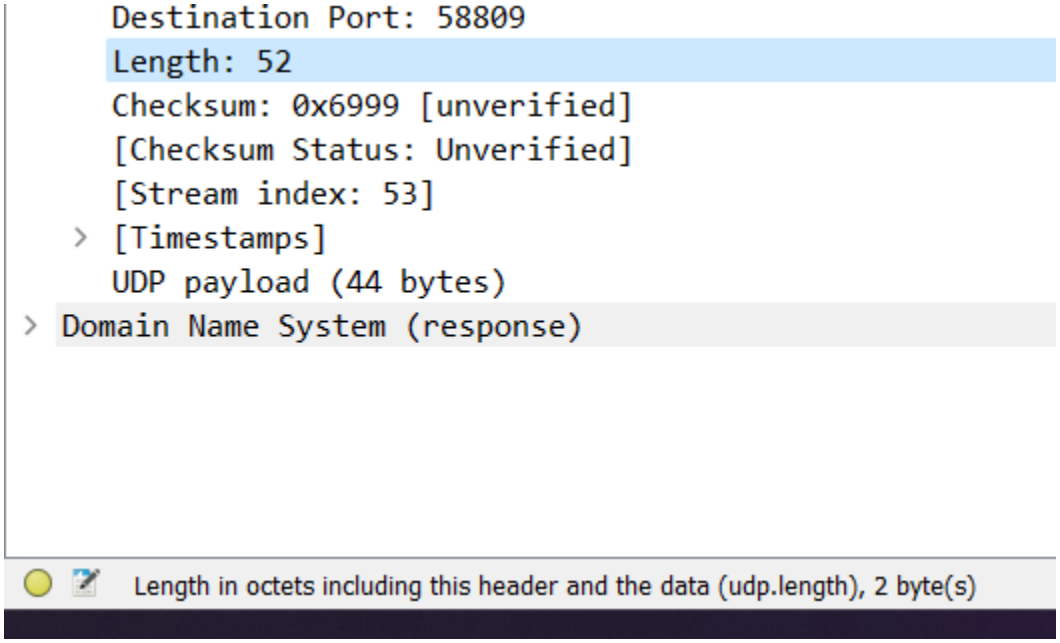
```
Checksum: 0x6999 [unverified]
[Checksum Status: Unverified]
[Stream index: 53]
> [Timestamps]
UDP payload (44 bytes)
> Domain Name System (response)
```





Câu 6

Trường Length xác định độ dài của toàn bộ datagram: header và data (trong trường hợp này là 52 bytes)

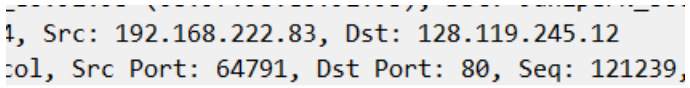


Câu 8

Địa chỉ IP và TCP port của clinet sử dụng:

192.168.222.83

64791

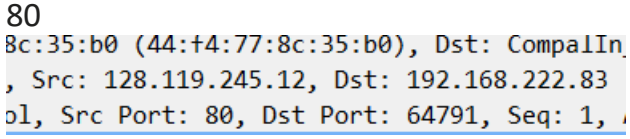


Câu 9

Địa chỉ gaia.cs.umass.edu là:

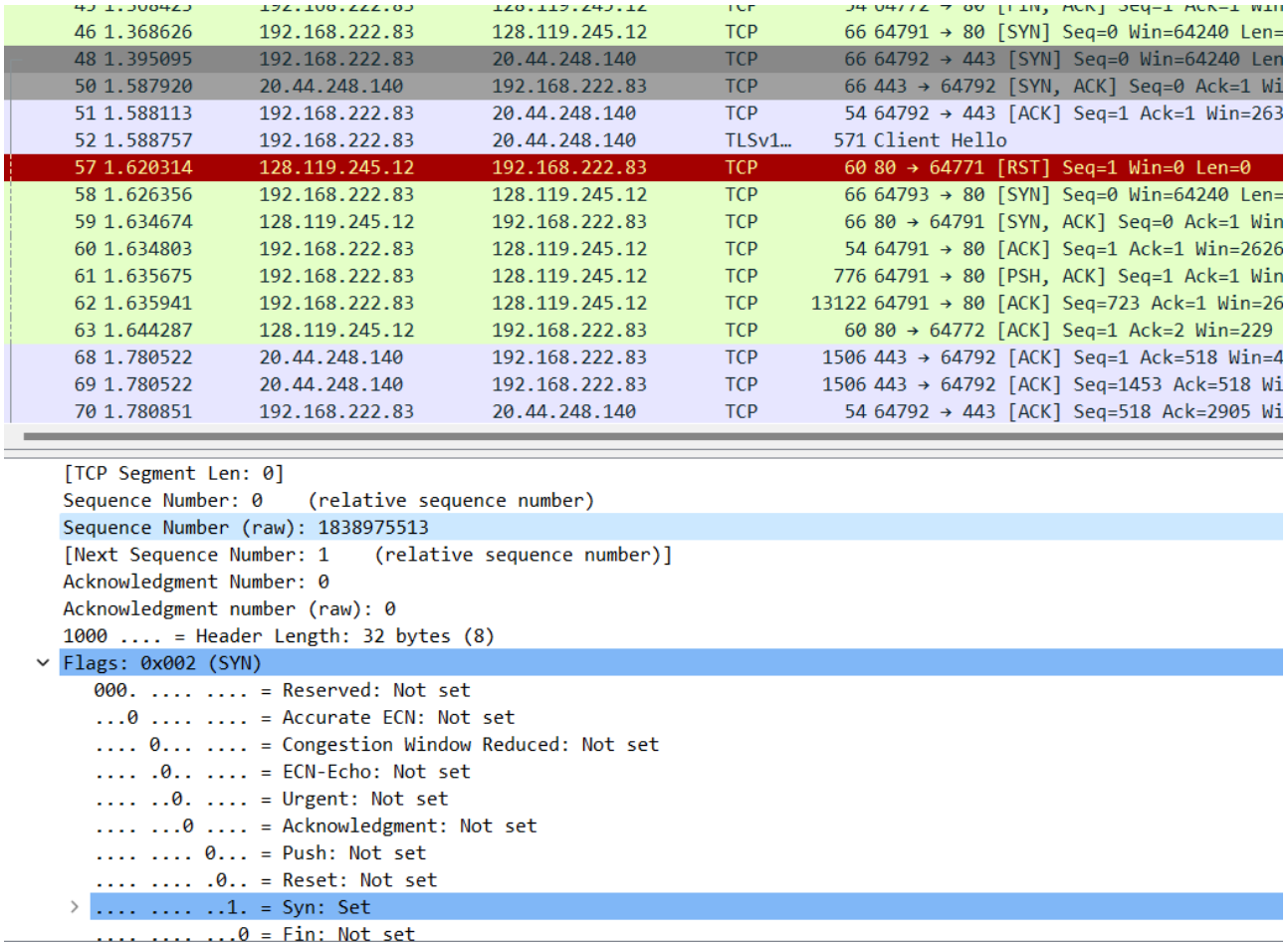
128.119.245.12

80



Câu 10

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



46	1.368626	192.168.222.83	128.119.245.12	TCP	66 64791 → 80 [SYN] Seq=0 Win=64240 Len=
48	1.395095	192.168.222.83	20.44.248.140	TCP	66 64792 → 443 [SYN] Seq=0 Win=64240 Len
50	1.587920	20.44.248.140	192.168.222.83	TCP	66 443 → 64792 [SYN, ACK] Seq=0 Ack=1 Wi
51	1.588113	192.168.222.83	20.44.248.140	TCP	54 64792 → 443 [ACK] Seq=1 Ack=1 Win=263
52	1.588757	192.168.222.83	20.44.248.140	TLSv1…	571 Client Hello
57	1.620314	128.119.245.12	192.168.222.83	TCP	60 80 → 64771 [RST] Seq=1 Win=0 Len=0
58	1.626356	192.168.222.83	128.119.245.12	TCP	66 64793 → 80 [SYN] Seq=0 Win=64240 Len=
59	1.634674	128.119.245.12	192.168.222.83	TCP	66 80 → 64791 [SYN, ACK] Seq=0 Ack=1 Win
60	1.634803	192.168.222.83	128.119.245.12	TCP	54 64791 → 80 [ACK] Seq=1 Ack=1 Win=2626
61	1.635675	192.168.222.83	128.119.245.12	TCP	776 64791 → 80 [PSH, ACK] Seq=1 Ack=1 Win
62	1.635941	192.168.222.83	128.119.245.12	TCP	13122 64791 → 80 [ACK] Seq=723 Ack=1 Win=26
63	1.644287	128.119.245.12	192.168.222.83	TCP	60 80 → 64772 [ACK] Seq=1 Ack=2 Win=229
68	1.780522	20.44.248.140	192.168.222.83	TCP	1506 443 → 64792 [ACK] Seq=1 Ack=518 Win=4
69	1.780522	20.44.248.140	192.168.222.83	TCP	1506 443 → 64792 [ACK] Seq=1453 Ack=518 Wi
70	1.780851	192.168.222.83	20.44.248.140	TCP	54 64792 → 443 [ACK] Seq=518 Ack=2905 Wi

```
[TCP Segment Len: 0]
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 1838975513
[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
```

Câu 11

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.

50	1.587920	20.44.248.140	192.168.222.83	TCP	66 443 → 64792 [SYN, ACK] Seq
51	1.588113	192.168.222.83	20.44.248.140	TCP	54 64792 → 443 [ACK] Seq=1 Ac
52	1.588757	192.168.222.83	20.44.248.140	TLSv1…	571 Client Hello
57	1.620314	128.119.245.12	192.168.222.83	TCP	60 80 → 64771 [RST] Seq=1 Win
58	1.626356	192.168.222.83	128.119.245.12	TCP	66 64793 → 80 [SYN] Seq=0 Win
59	1.634674	128.119.245.12	192.168.222.83	TCP	66 80 → 64791 [SYN, ACK] Seq=
60	1.634803	192.168.222.83	128.119.245.12	TCP	54 64791 → 80 [ACK] Seq=1 Ack
61	1.635675	192.168.222.83	128.119.245.12	TCP	776 64791 → 80 [PSH, ACK] Seq=
62	1.635941	192.168.222.83	128.119.245.12	TCP	13122 64791 → 80 [ACK] Seq=723 A
63	1.644287	128.119.245.12	192.168.222.83	TCP	60 80 → 64772 [ACK] Seq=1 Ack
68	1.780522	20.44.248.140	192.168.222.83	TCP	1506 443 → 64792 [ACK] Seq=1 Ac
69	1.780522	20.44.248.140	192.168.222.83	TCP	1506 443 → 64792 [ACK] Seq=1453
70	1.780851	192.168.222.83	20.44.248.140	TCP	54 64792 → 443 [ACK] Seq=518

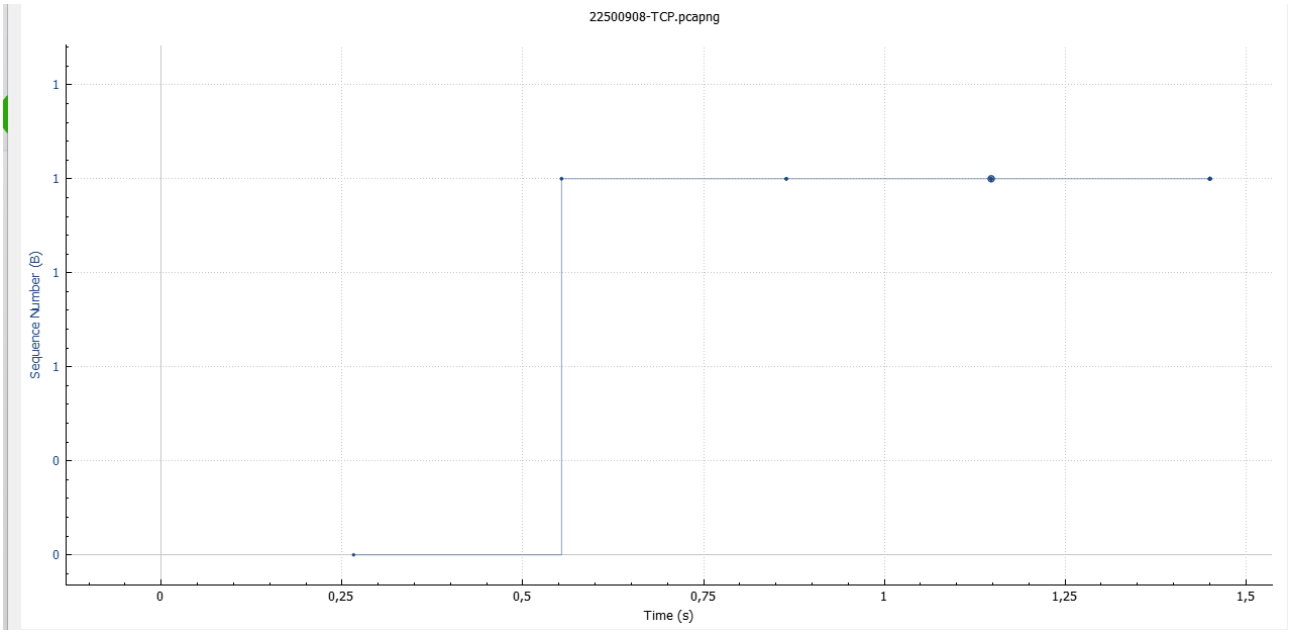
```
Sequence Number (raw): 1657579777
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 1838975514
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = 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
```

Câu 13

Độ dai của 6 segment đầu đều = 0

Lượng Buffer nhỏ nhất bên nhận gửi cho bên truyền: 30720

Câu 14



Có segment nào được gửi lại. Điều này có thể được giải thích bởi các gói có cùng sequence number tại các thời điểm khác nhau được tìm thấy.