Lab 3

BÁO CÁO BÀI THỰC HÀNH SỐ 3

GIAO THỨC UDP & TCP

Môn học: Nhập môn mạng máy tính

Sinh viên thực hiện	Trần Thanh Hùng (23520580)
Thời gian thực hiện	10/04/2024 – 17/04/2024
Số câu đã hoàn thành	14/14

2.1.1

IP address	192.168.1.192
MAC address	04-7C-16-A3-F5-5E
Default gateway IP address	192.168.1.1
DNS server IP adress	192.168.1.1

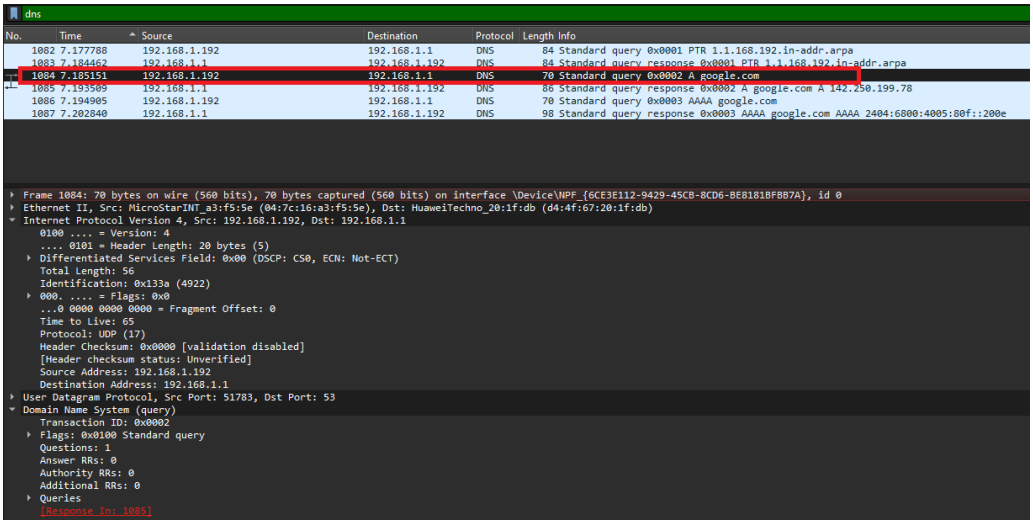
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 04-7C-16-A3-F5-5E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.192(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Saturday, April 13, 2024 16:00:38
   Lease Expires . . . . . . . . . . : Saturday, April 13, 2024 19:00:38
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

2.1.3

Câu 1:

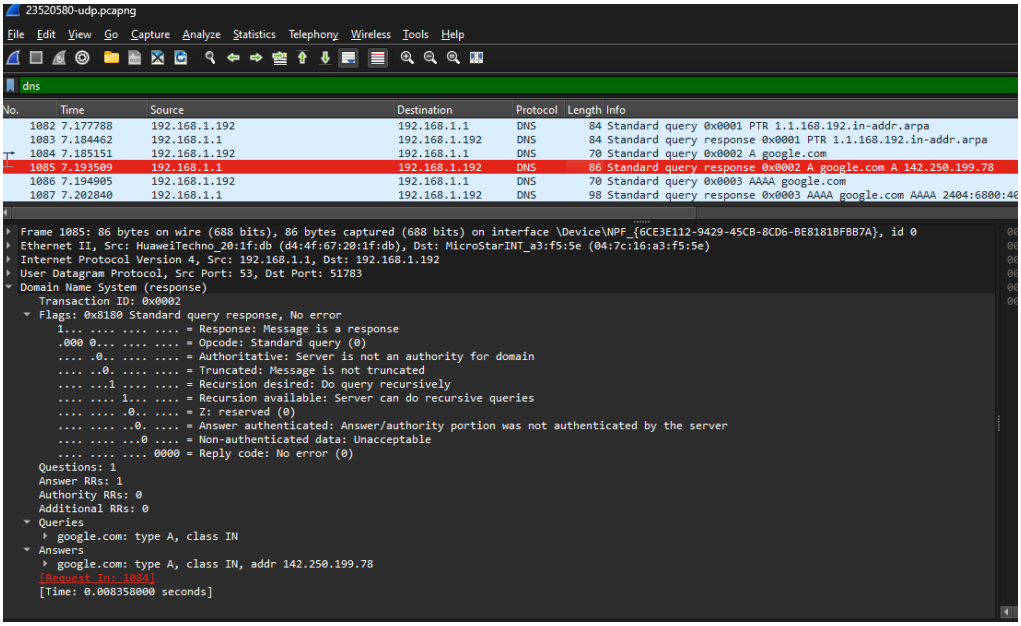
IP address	192.168.1.192
MAC address	04-7C-16-A3-F5-5E
Default gateway IP address	192.168.1.1
DNS server IP adress	192.168.1.1

Câu 2:



Gói truy vấn domain google.com nằm ở gói tin thứ 1084

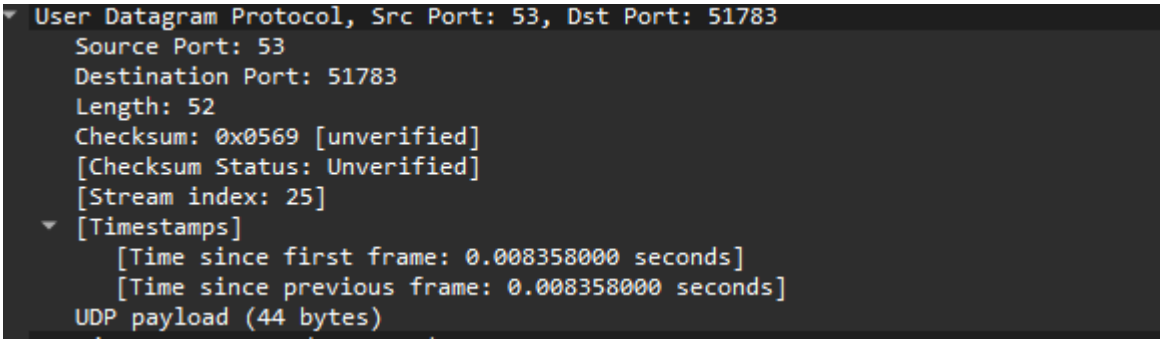
Câu 3:



Gói tin phản hồi nằm ở gói tin thứ 1085

Có địa chỉ IP đã truy vấn được là: 142.250.199.78

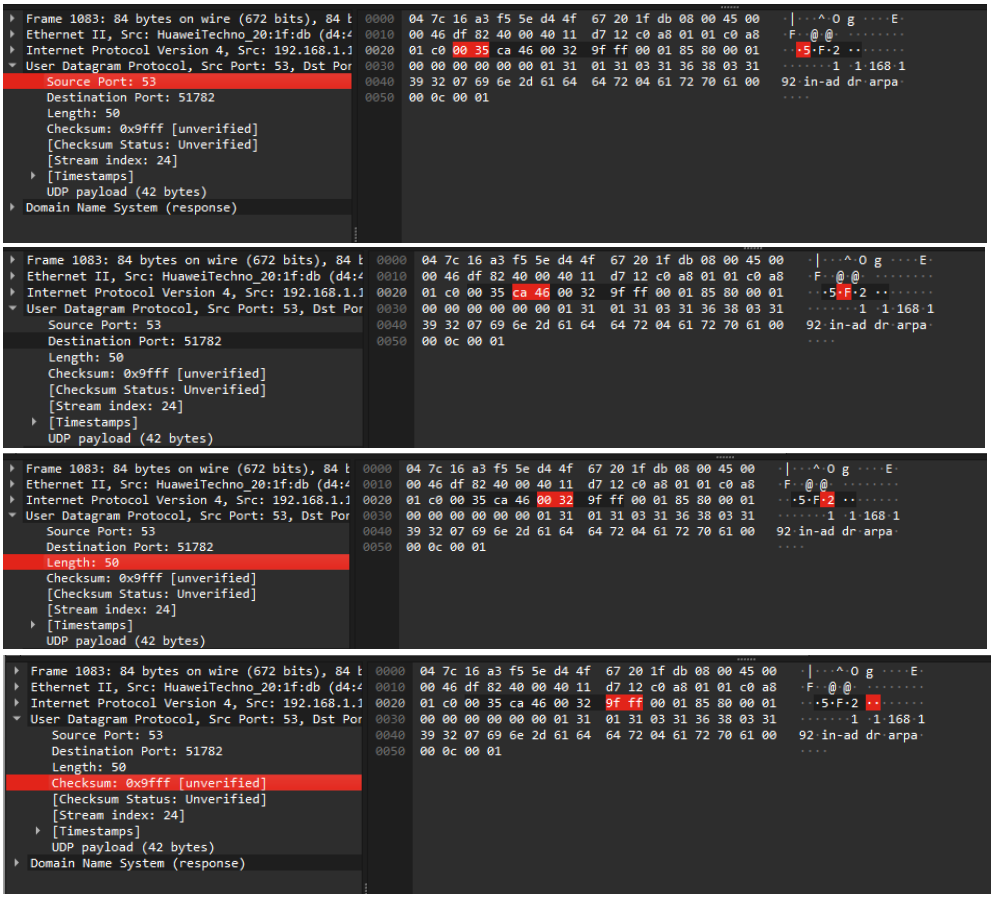
Câu 4:



Có 4 trường header:

1. Source Port (2byte): Xác định cổng của máy gửi dữ liệu
2. Destination Port (2byte): Xác định cổng của máy nhận dữ liệu
3. Length (2byte): Cho biết tổng chiều dài của
4. Checksum (2byte): Được sử dụng để kiểm tra lỗi gói tin UDP

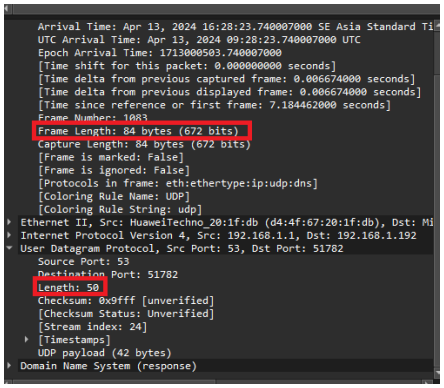
Câu 5. Qua thông tin hiển thị của Wireshark, xác định độ dài (***tính theo byte***) của mỗi trường trong UDP header?



Mỗi trường sẽ có độ dài là 2 byte

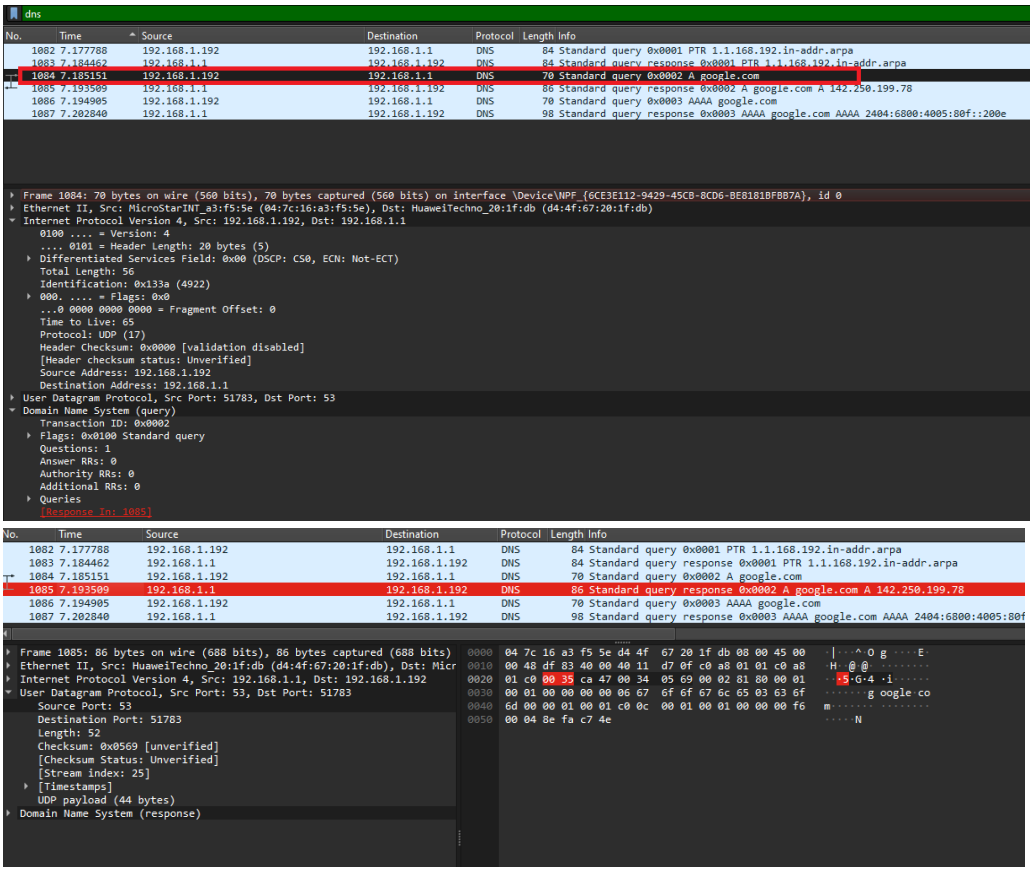
Câu 6. Giá trị của trường **Length** trong UDP header là độ dài của gì? Chứng minh nhận định này?

Trong UDP header, trường length là độ dài của gói tin UDP, bao gồm cả 4 trường của header và dữ liệu. Không phải toàn bộ gói tin



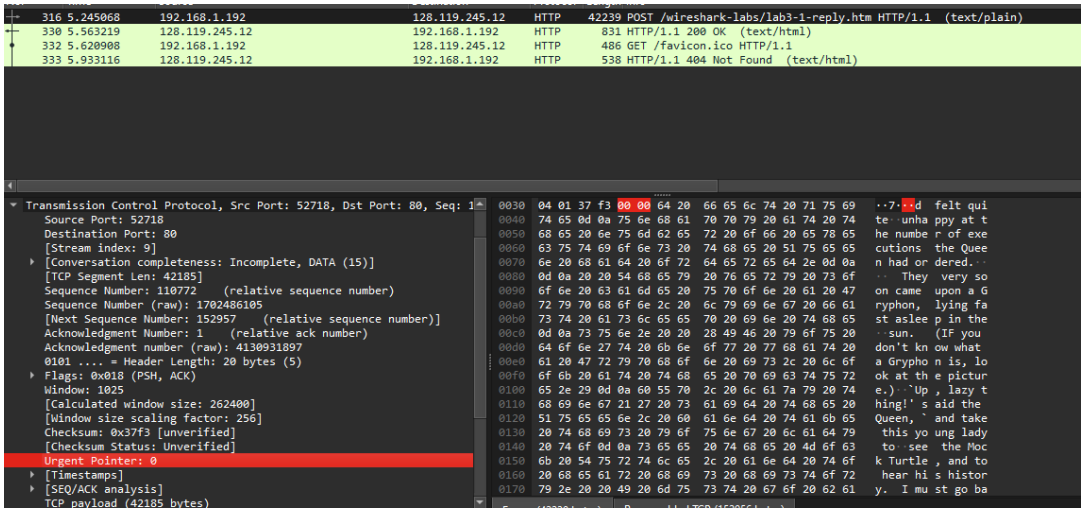
Ví dụ: gói tin 1083, toàn bộ gói tin có độ dài 84 byte nhưng phần UDP chỉ có 50 vì trong gói tin sẽ chứa thêm các thông tin khác như địa chỉ IP, thời gian, giao thức.

Câu 7. Quan sát 2 gói tin tìm được ở Câu 1 và 2, mô tả mối quan hệ giữa các địa chỉ IP và port number của 2 gói tin này.



Source port/IP, destination port/IP đã đổi chỗ cho nhau

Câu 8. Xác định IP và TCP port của client sử dụng để chuyển tệp sang gaia.cs.umass.edu là gì? **Gợi ý**: *Chọn một thông điệp HTTP và khám phá các chi tiết của gói tin TCP được sử dụng để mang thông điệp HTTP này*



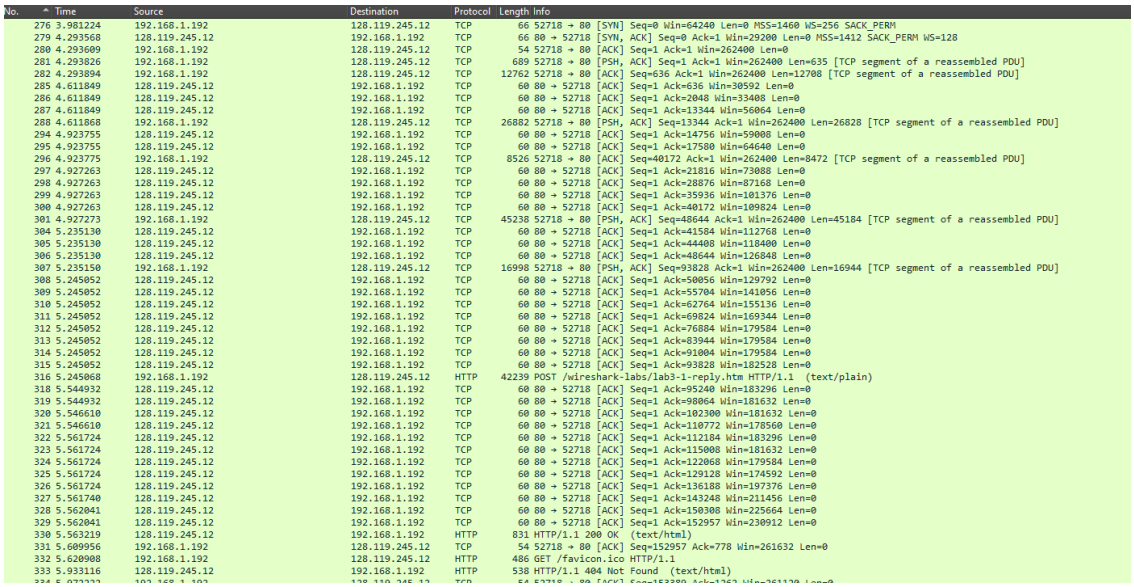
IP client là: 192.168.1.192

Port của client là: 52718

Câu 9. Địa chỉ IP của gaia.cs.umass.edu là gì? Trên số cổng nào nó gửi và nhận các segment TCP cho kết nối này?

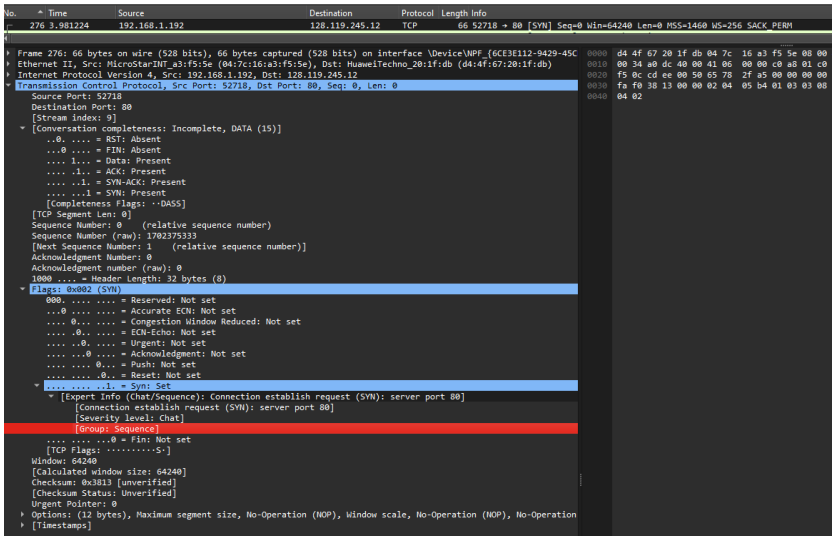
Địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12

Cổng gửi và nhận các segment TCP của gaia.cs.umass.edu là cổng 80.



No.	Time	Source	Destination	Protocol	Length	Info
276	3.981224	192.168.1.192	128.119.245.12	TCP	66	52718 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
279	4.293568	128.119.245.12	192.168.1.192	TCP	66	80 → 52718 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
280	4.293609	192.168.1.192	128.119.245.12	TCP	54	52718 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
281	4.293826	192.168.1.192	128.119.245.12	TCP	689	52718 → 80 [PSH, ACK] Seq=1 Ack=1 Win=262400 Len=635 [TCP segment of a reassembled PDU]
282	4.293894	192.168.1.192	128.119.245.12	TCP	12762	52718 → 80 [ACK] Seq=636 Ack=1 Win=262400 Len=12708 [TCP segment of a reassembled PDU]
285	4.611849	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=636 Win=30592 Len=0
286	4.611849	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=2048 Win=33408 Len=0
287	4.611849	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=13344 Win=56064 Len=0
288	4.611868	192.168.1.192	128.119.245.12	TCP	26882	52718 → 80 [PSH, ACK] Seq=13344 Ack=1 Win=262400 Len=26828 [TCP segment of a reassembled PDU]
294	4.923755	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=14756 Win=59008 Len=0
295	4.923755	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=17580 Win=64640 Len=0
296	4.923775	192.168.1.192	128.119.245.12	TCP	8526	52718 → 80 [ACK] Seq=40172 Ack=1 Win=262400 Len=8472 [TCP segment of a reassembled PDU]
297	4.927263	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=21816 Win=73088 Len=0
298	4.927263	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=28876 Win=87168 Len=0
299	4.927263	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=35936 Win=101376 Len=0
300	4.927263	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=40172 Win=109824 Len=0
301	4.927273	192.168.1.192	128.119.245.12	TCP	45238	52718 → 80 [PSH, ACK] Seq=48644 Ack=1 Win=262400 Len=45184 [TCP segment of a reassembled PDU]
304	5.235130	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=41584 Win=112768 Len=0
305	5.235130	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=44408 Win=118400 Len=0
306	5.235130	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=48644 Win=126848 Len=0
307	5.235150	192.168.1.192	128.119.245.12	TCP	16998	52718 → 80 [PSH, ACK] Seq=93828 Ack=1 Win=262400 Len=16944 [TCP segment of a reassembled PDU]
308	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=50056 Win=129792 Len=0
309	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=55704 Win=141056 Len=0
310	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=62764 Win=155136 Len=0
311	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=69824 Win=169344 Len=0
312	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=76884 Win=179584 Len=0
313	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=83944 Win=179584 Len=0
314	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=91004 Win=179584 Len=0
315	5.245052	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=93828 Win=182528 Len=0
316	5.245068	192.168.1.192	128.119.245.12	HTTP	42239	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
318	5.544932	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=95240 Win=183296 Len=0
319	5.544932	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=98064 Win=181632 Len=0
320	5.546610	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=102300 Win=181632 Len=0
321	5.546610	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=110772 Win=178560 Len=0
322	5.561724	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=112184 Win=183296 Len=0
323	5.561724	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=115008 Win=181632 Len=0
324	5.561724	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=122068 Win=179584 Len=0
325	5.561724	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=129128 Win=174592 Len=0
326	5.561724	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=136188 Win=197376 Len=0
327	5.561740	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=143248 Win=211456 Len=0
328	5.562041	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=150308 Win=225664 Len=0
329	5.562041	128.119.245.12	192.168.1.192	TCP	60	80 → 52718 [ACK] Seq=1 Ack=152957 Win=230912 Len=0
330	5.563219	128.119.245.12	192.168.1.192	HTTP	831	HTTP/1.1 200 OK (text/html)
331	5.609956	192.168.1.192	128.119.245.12	TCP	54	52718 → 80 [ACK] Seq=152957 Ack=778 Win=261632 Len=0
332	5.620908	192.168.1.192	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
333	5.933116	128.119.245.12	192.168.1.192	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Câu 10. 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? ***Gợi ý***: Quan sát trường Flags.

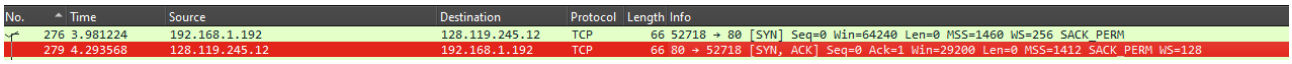


```
No.  Time      Source          Destination     Protocol  Length Info
276  3.981224  192.168.1.192   128.119.245.12  TCP       66     52718 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 276: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{6CE3E112-9429-45C
Ethernet II, Src: MicroStarINT_a3:f5:5e (04:7c:16:a3:f5:5e), Dst: HuaweiTechno_20:1f:db (d4:4f:67:20:1f:db)
Internet Protocol Version 4, Src: 192.168.1.192, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52718, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 52718
    Destination Port: 80
    [Stream index: 9]
  ▾ [Conversation completeness: Incomplete, DATA (15)]
      ..0. .... = RST: Absent
      ...0 .... = FIN: Absent
      .... 1... = Data: Present
      .... .1.. = ACK: Present
      .... ..1. = SYN-ACK: Present
      .... ...1 = SYN: Present
      [Completeness Flags: ··DASS]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1702375333
    [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
      ▾ [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
          [Connection establish request (SYN): server port 80]
          [Severity level: Chat]
          [Group: Sequence]
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x3013 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation
  ▸ [Timestamps]

0000  d4 4f 67 20 1f db 04 7c  16 a3 f5 5e 08 00
0010  00 34 a0 dc 40 00 41 06  00 00 c0 a8 01 c0
0020  f5 0c cd ee 00 50 65 78  2f a5 00 00 00 00
0030  fa f0 38 13 00 00 02 04  05 b4 01 03 03 08
0040  04 02
```

TCP SYN segment sử dụng sequence 0 để khởi tạo kết nối TCP

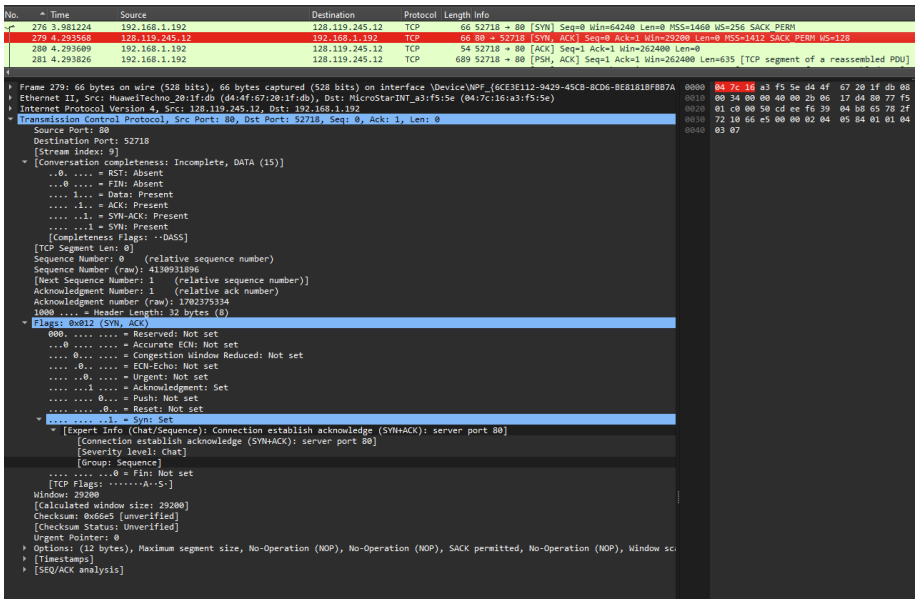
Có thể xem tại phần info của gói tin hoặc Sequence number ở phần thông tin khi bấm vào gói tin

Câu 11. Tìm **sequence number** của gói tin ***SYN/ACK segment*** được gửi bởi server đến client để trả lời cho SYN segment?



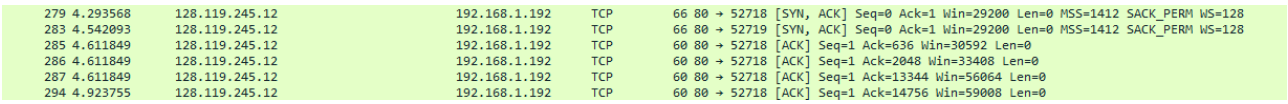
Sequence number của gói tin SYN/ACK segment đucọ gửi bởi server đến client là gói tin thứ 279

Câu 12. Tìm giá trị của **Acknowledgement** trong SYN/ACK segment? Làm sao server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYN/ACK segment?



Giá trị ACK trong SYN/ACK segment là 1, server xác định được giá trị đó thông qua bước bắt tay đầu tiên, sau đó lấy Seq + 1, ra AKC=1, biểu thị muốn nhận gói tin có Seq = 1. Có thể xác định đó là SYN/ACK segment thông qua cột info, hoặc bấm vào gói tin, kiểm tra trường flag và thấy cờ ACK và cờ SYN đều bật lên.

Câu 13. Tìm độ dài của từng segment trong bộ 6 segments đầu tiên trên? Tìm lượng buffer còn trống nhỏ nhất mà bên nhận thông báo cho bên gửi trong suốt truyền tin? ***Gợi ý:*** Buffer còn trống = giá trị Calculated window size (Win) trong các gói ACK mà server báo về bên gửi. Kiểm tra trong tất cả các gói chứa ACK từ server trả về máy tính để xác định giá trị nhỏ nhất. Có thể chỉ lọc các gói từ server bằng cách thêm điều kiện filter "*tcp and ip.src==IP của server*"



Gói số 279: 66

Gói số 283: 66

Gói số 285: 60

Gói số 286: 60

Gói số 287: 60

Gói số 294: 60

Buffer còn trống nhỏ nhất mà bên nhận thông báo về cho bên gửi là 29200.

Câu 14. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó?

Không có gói tin nào được gửi lại, Wireshark không đánh dấu gói tin màu đen [TCP Retransmission]