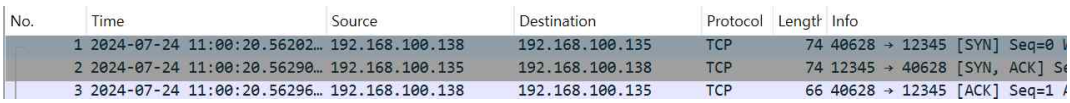
돈돈돈 쓰쓰쓰 돈돈돈

32기 안현진

문제 파일을 다운받았다. 와이어샤크 캡쳐 파일이다.

1. 패킷 분석



No.	Time	Source	Destination	Protocol	Length	Info
1	2024-07-24 11:00:20.56202…	192.168.100.138	192.168.100.135	TCP	74	40628 → 12345 [SYN] Seq=0
2	2024-07-24 11:00:20.56290…	192.168.100.135	192.168.100.138	TCP	74	12345 → 40628 [SYN, ACK] Se
3	2024-07-24 11:00:20.56296…	192.168.100.138	192.168.100.135	TCP	66	40628 → 12345 [ACK] Seq=1 A

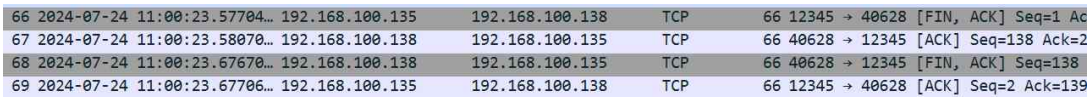
간단하게 패킷을 살펴보고 문제 풀이를 해보자. 총 69개의 패킷이 캡쳐되었고 1~3번 패킷은 3-Way handshake 과정이다. 신뢰성 있고 안정적인 연결을 설정하기 위해 사용한다.

->1번 패킷: 135가 138로, 포트 40628에서 포트 12345로 SYN 패킷을 보낸다. seq=0은 연결을 시작하겠다는 의미이다. 이것을 보고 연결 시작점을 알 수 있다. seq(Sequence Number)은 TCP 프로토콜 패킷 내에서 데이터의 순서를 추적하고 신뢰할 수 있는 데이터 전송을 보장하는 데 사용된다.
->2번 패킷: 138이 135로, SYN에 대한 ACK를 보내면서 SYN을 보낸다.
->3번 패킷: 135가 138로 ACK를 보내며 TCP연결이 성립된다.

SYN(Synchronize Sequence Number)은 연결을 요청할 때 사용한다.
ACK(Acknowledgement)는 패킷을 받았다는 응답을 할 때 사용한다.
PSH(Push) 플래그는 TCP 프로토콜에서 사용되는 플래그로, 데이터가 즉시 처리되도록 하는 역할을 한다.

```
[PSH, ACK] Seq=5 Ack=1 Win=64256 Len=1 TSval=3905454005 TSecr=1515121044
```

->PSH와 ACK 플래그가 설정된 패킷.
->Seq=5: 시퀀스 번호가 5번이라는 의미. 패킷이 전송하는 데이터가 연결 내에서 5번째 byte부터 시작됨을 의미한다.
->Ack=1: 송신 측이 수신 측으로부터 시퀀스 번호0까지 받았다는 의미. 이제 수신 측에서 1 이후의 데이터를 기다리고 있다는 의미이다.
->Win=64256: 윈도우 크기를 의미한다. 송신 측이 수신 측으로부터 추가로 받을 수 있는 데이터 양을 의미한다.
->Len=1: 이 패킷의 데이터 길이는 1byte라는 의미이다.
->TSval: 송신 측의 현재 타임스탬프 값.
->TSecr: 수신 측이 이전에 보낸 패킷에 포함된 타임스탬프 값. 수신 측이 보내는 응답에서 해당 타임스탬프를 그대로 돌려주는 것으로, 왕복 시간을 계산하는데 사용된다.



66	2024-07-24 11:00:23.57704…	192.168.100.135	192.168.100.138	TCP	66 12345 → 40628 [FIN, ACK] Seq=1 Ac
67	2024-07-24 11:00:23.58070…	192.168.100.138	192.168.100.135	TCP	66 40628 → 12345 [ACK] Seq=138 Ack=2
68	2024-07-24 11:00:23.67670…	192.168.100.138	192.168.100.135	TCP	66 40628 → 12345 [FIN, ACK] Seq=138
69	2024-07-24 11:00:23.67706…	192.168.100.135	192.168.100.138	TCP	66 12345 → 40628 [ACK] Seq=2 Ack=139

66~69번 패킷은 TCP연결을 종료하는 4-Way handshake 과정이다.

->66번 패킷: 138(클라이언트)이 135(서버)에게 FIN 플래그가 설정된 패킷을 보낸다. 클라이언트가 서버에게 더 이상 데이터를 전송하지 않겠다는 의미이다.
->67번 패킷: 135가 138에게 FIN 패킷을 성공적으로 확인했다는 의미로 ACK 패킷을 보낸다.
->68번 패킷: 135(서버)도 138(클라이언트)에게 더 이상 데이터를 보내지 않겠다는 의미로 FIN플래그를 보낸다.
->69번 패킷: 138도 FIN 패킷을 성공적으로 확인했다는 의미로 ACK를 보내고, TCP연결은 종료된다.

2. 문제 풀이

```
2e2e 2d2d2e2e2e 2e2d2d2d2d2e 2e2e2e 2e2e2d2d2e2d 2d2d 2d2d2d2d2d 2e2d2e 2e2e2e 2e
2e2e2d2d2e2d 2d2e2d2e 2d2d2d2d2d 2d2e2e 2e 2d2e2d2e2d2d
```

TCP 스트림 따라가기를 누르면 이런 메시지가 나타난다.

그리고 '돈돈돈 쓰쓰쓰 돈돈돈'을 구글에 검색하면 모스부호와 관련된 정보들이 나온다. 이걸 가지고 메시지를 해석해보자. 일단 2e와 2d를 모스부호로 변환해보았다. 2e는 · · - - - · 로, 2d는 · · - - - - · ·로 변환된다.

```
. . - - -  .  . . - - -  .  . . - - -  - . .  . . - - -  - . .  . . - - -  .  .
. - - -  .  . . - - -  .  . . - - -  .  . . - - -  - . .  . . - - -  - . .  . .
- - -  - . .  . . - - -  - . .  . . - - -  .  . . - - -  .  . . - - -  .  . .
- - -  .  . . - - -  .  . . - - -  .  . . - - -  - . .  . . - - -  - . .  . .
- - -  .  . . - - -  - . .  . . - - -  - . .  . . - - -  - . .  . . - - -
- . .  . . - - -  - . .  . . - - -  - . .  . . - - -  - . .  . . - - -  - . .  .
. - - -  .  . . - - -  - . .  . . - - -  .  . . - - -  .  . . - - -  .  . . -
- -  .  . . - - -  .  . . - - -  .  . . - - -  .  . . - - -  - . .  . . -
- -  - . .  . . - - -  .  . . - - -  - . .  . . - - -  - . .  . . - - -  .  . .
- - -  - . .  . . - - -  .  . . - - -  - . .  . . - - -  - . .  . . - - -  - .
.  . . - - -  - . .  . . - - -  - . .  . . - - -  - . .  . . - - -  .  . . - -
-  .  . . - - -  .  . . - - -  - . .  . . - - -  .  . . - - -  - . .  . . -
- -  .  . . - - -  - . .  . . - - -  - . .
```

문자열 전체를 모스부호로 번역하면 위의 결과가 나온다. 그런데 이 결과를 변환하면 flag 형식의 답이 나오지 않는다.

위의 결과는 모스부호 변환기를 사용했을때의 결과였다. 이게 문제였나 싶어서 '출력 가능 아스키 문자표'를 검색해 다시 한번 찾아보았다.

0101101	055	45	2D	-	12
0101110	056	46	2E	.	13

2e가 있나 검색해보니 아까와는 다른 결과가 나왔다. 2e와 2d가 각각 점과 선이라고 한다. 문자열을 점과 선으로 바꿔보면

```
.. --... .----. ... ..--.- -- ----- .-. ... . ..--.- -.-. ----- -.. . -.-.--
```

이런 결과물이 나온다. 이걸 모스부호 번역기로 번역해보면

```
I7'S_M0RSE_C0DE!
```

flag가 나온다. 플래그 형식에 맞추면 3S{I7'S_M0RSE_C0DE!}이다.

+찾아보니 2e에 대한 아스키 문자 자체, 그 문자에 해당하는 아스키 코드의 Hx, 모스 부호가 서로 다른 체계에서 나온것이라 해석 결과가 다른거라고 한다. 나는 아스키 코드가 아닌 모스부호로 접근해서 해석 결과가 다르게 나온거였다.

<참고자료>

3-Way Handshake — 다락방 (tistory.com)