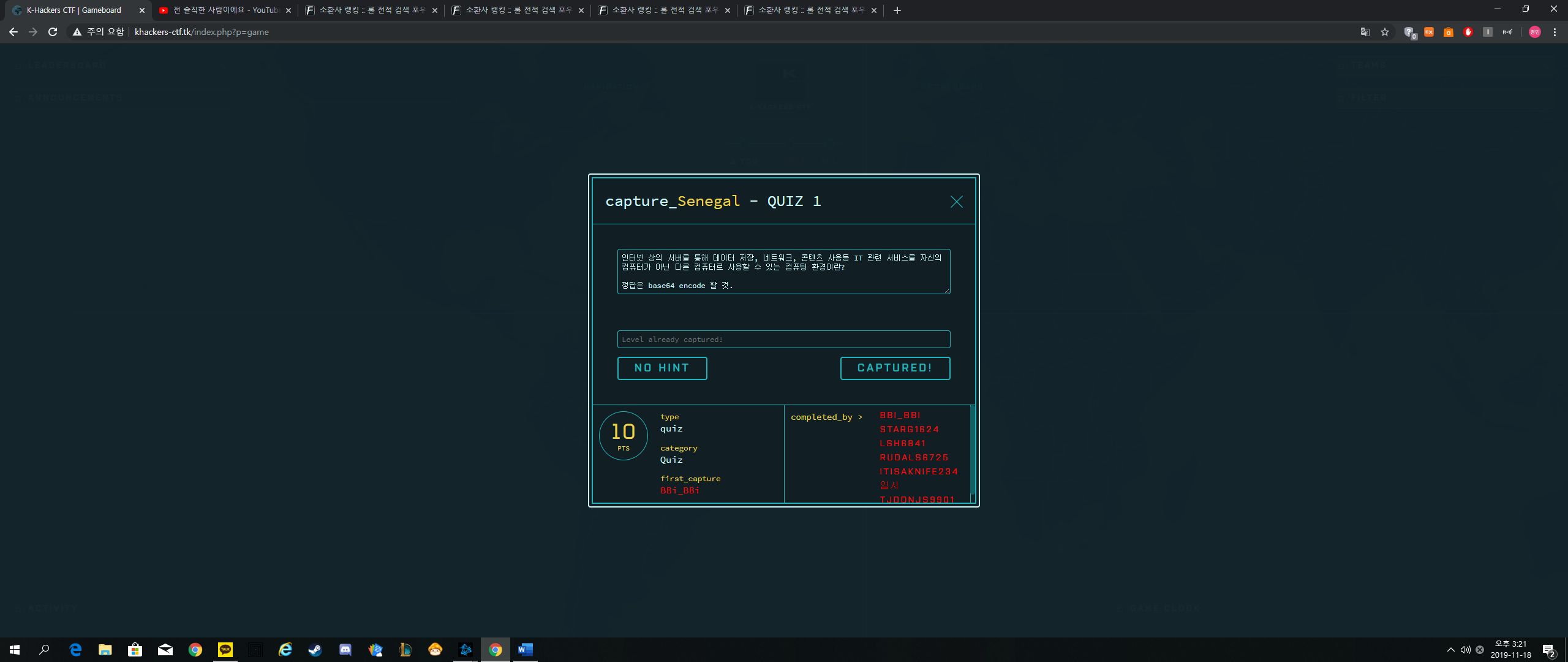
**K-HACKERS CTF**

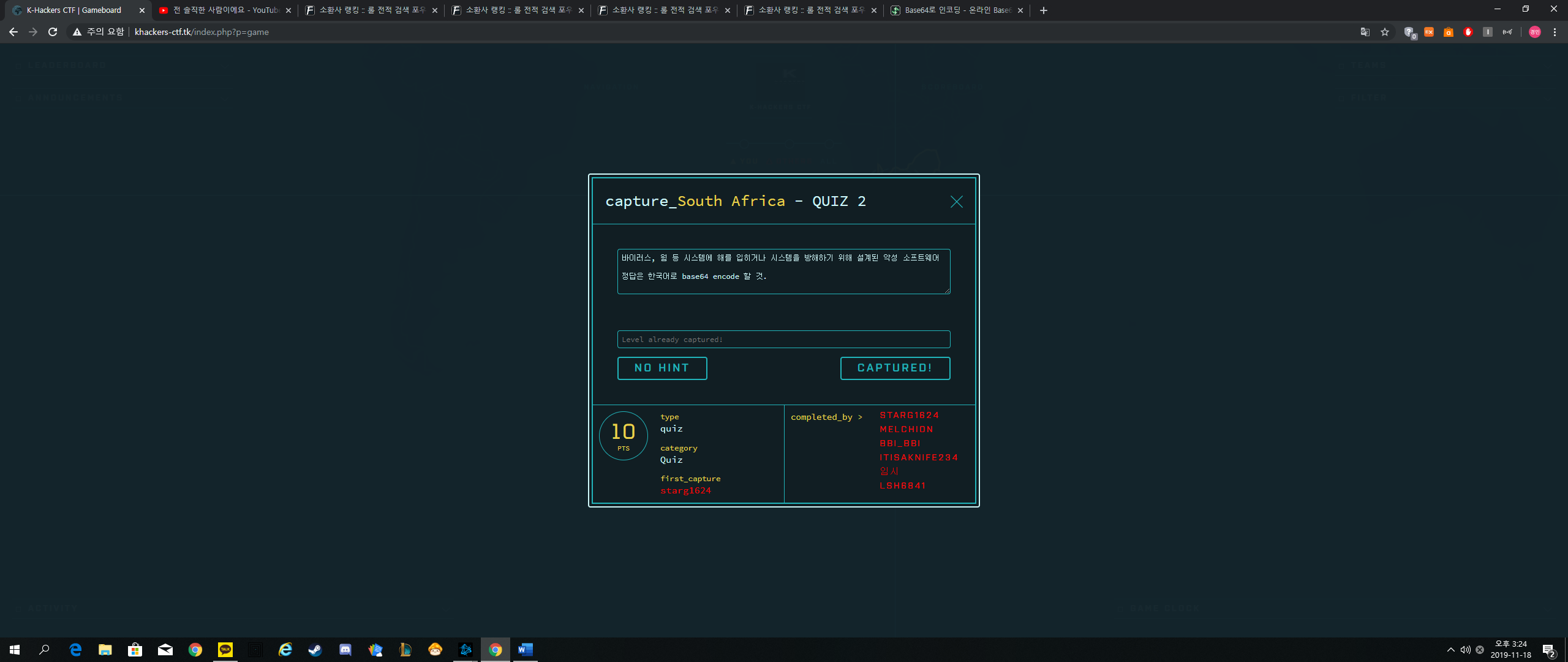
이경민

QUIZ 1



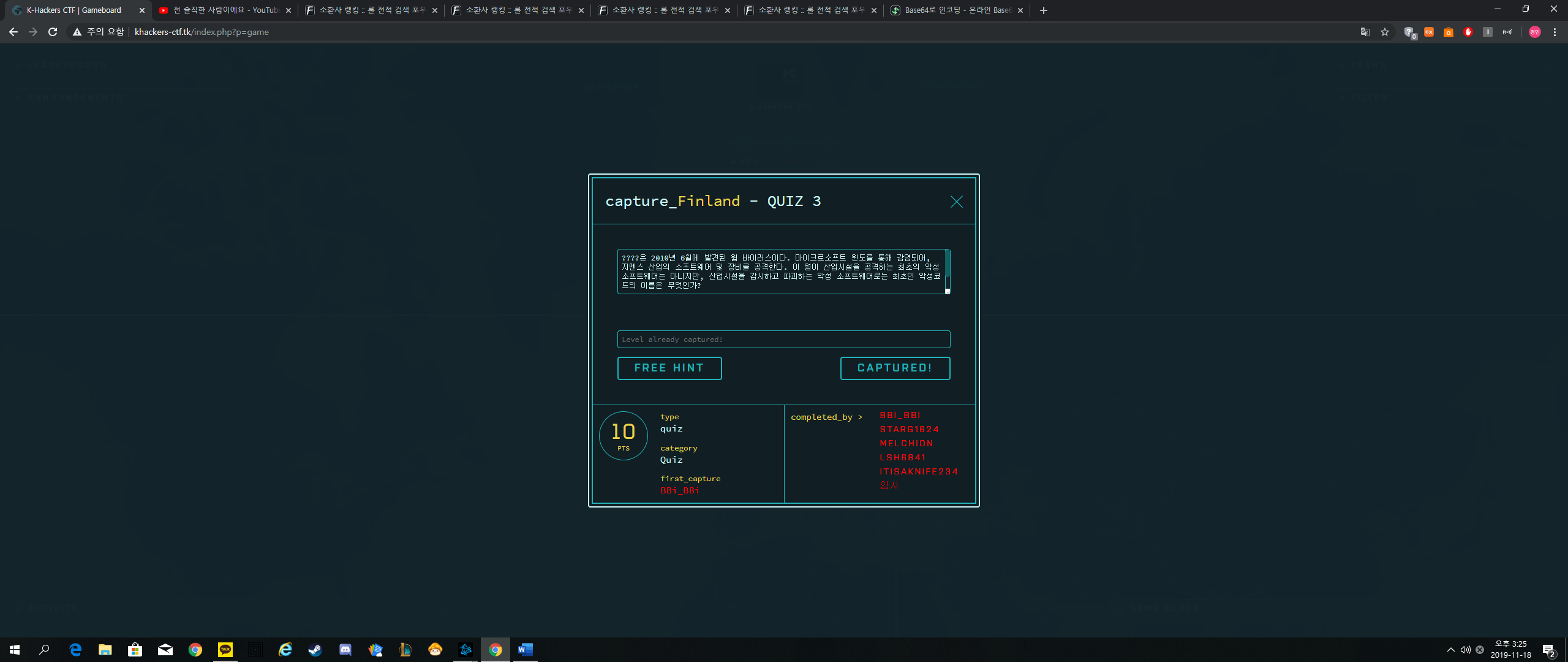
답 : 7YG065287Jqw65Oc7Lu07ZOo7YyF (클라우드컴퓨팅)

QUIZ 2



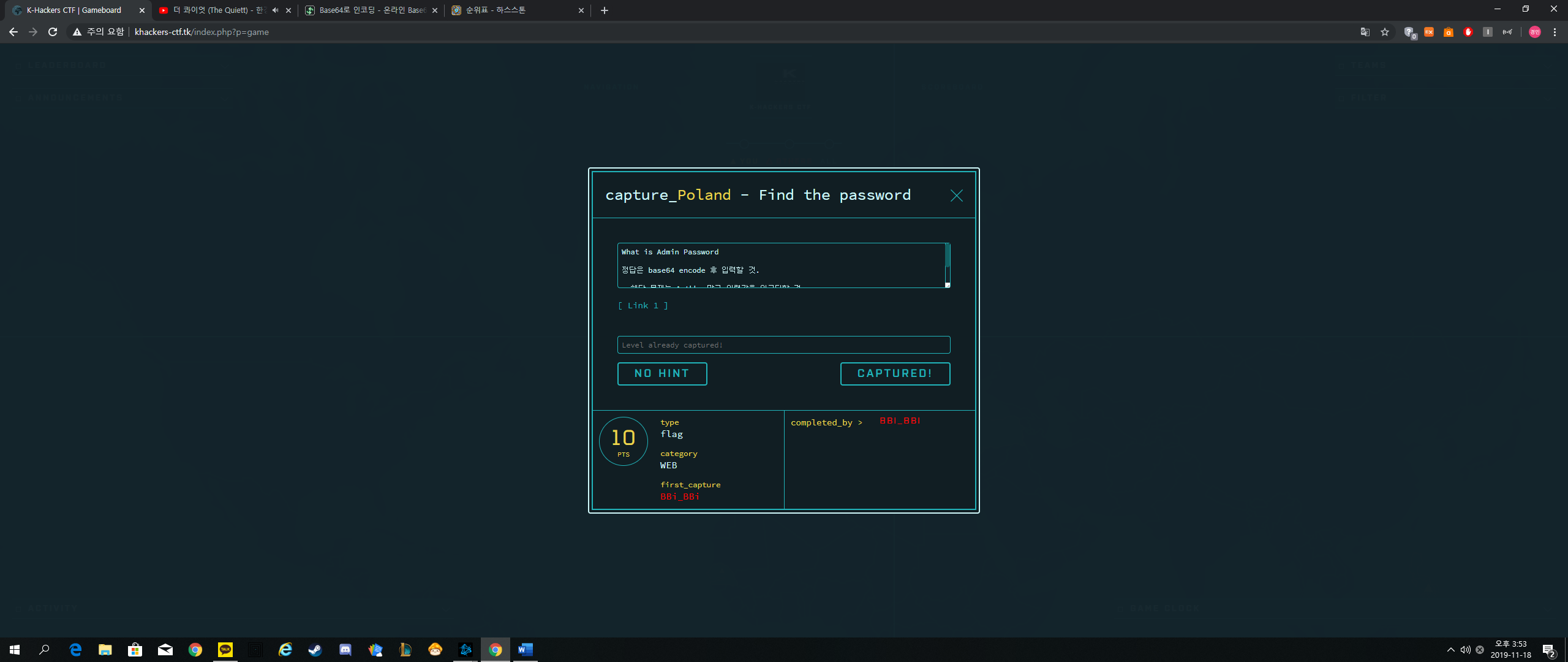
답 : 66mA7Juo7Ja0 (멀웨어)

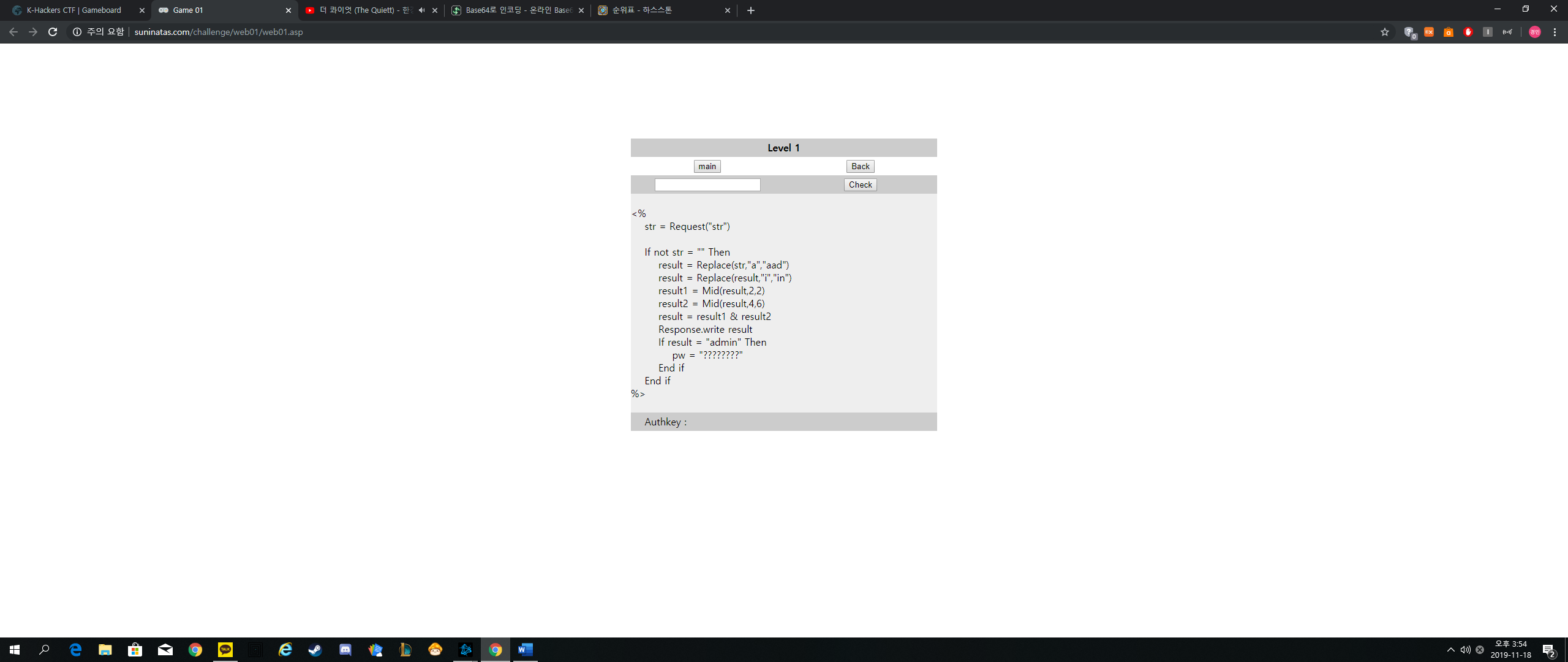
QUIZ 3



답 : 7Iqk7YSx7Iqk64S3 (스턱스넷)

Find the password





답 : YW1p (ami)

str에 문자열을 담음 (str = ami)

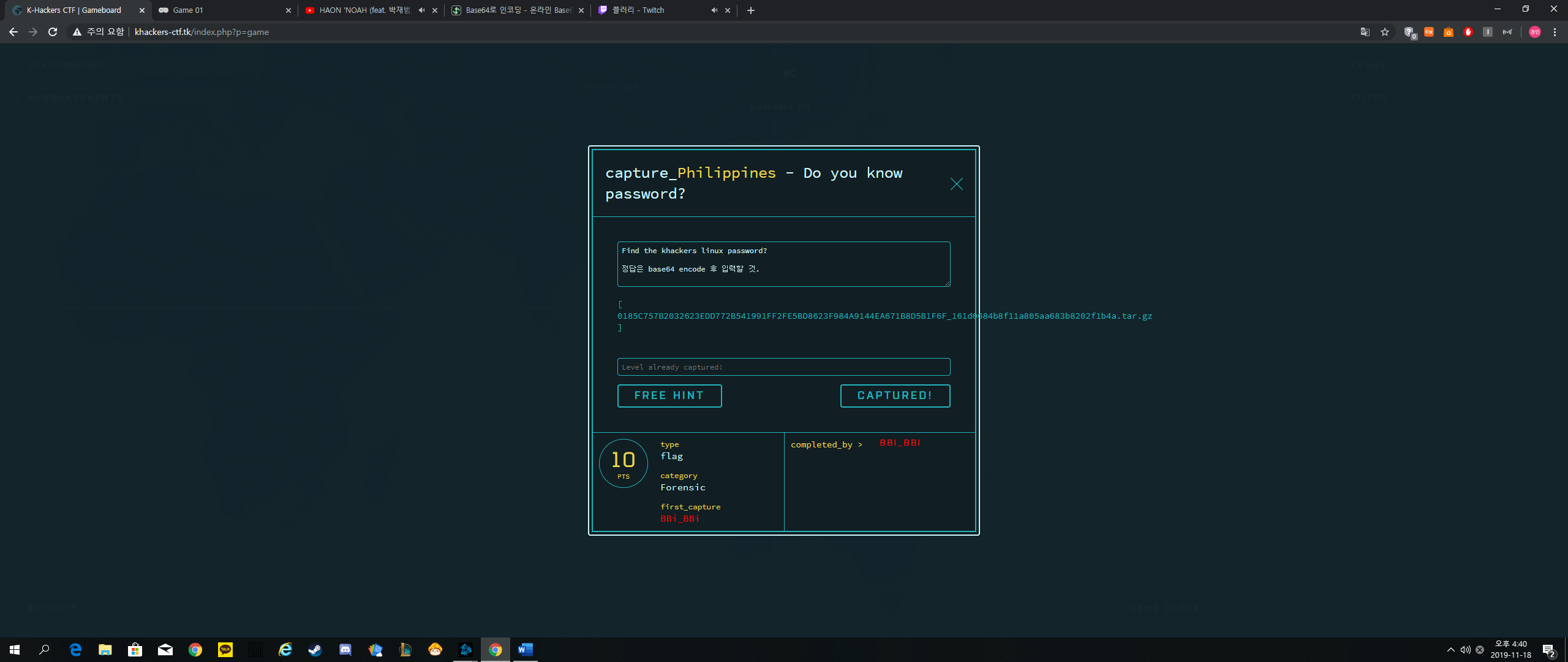
=> str의 a를 aad로 대체한후 result에 담음 (result = aadmi)

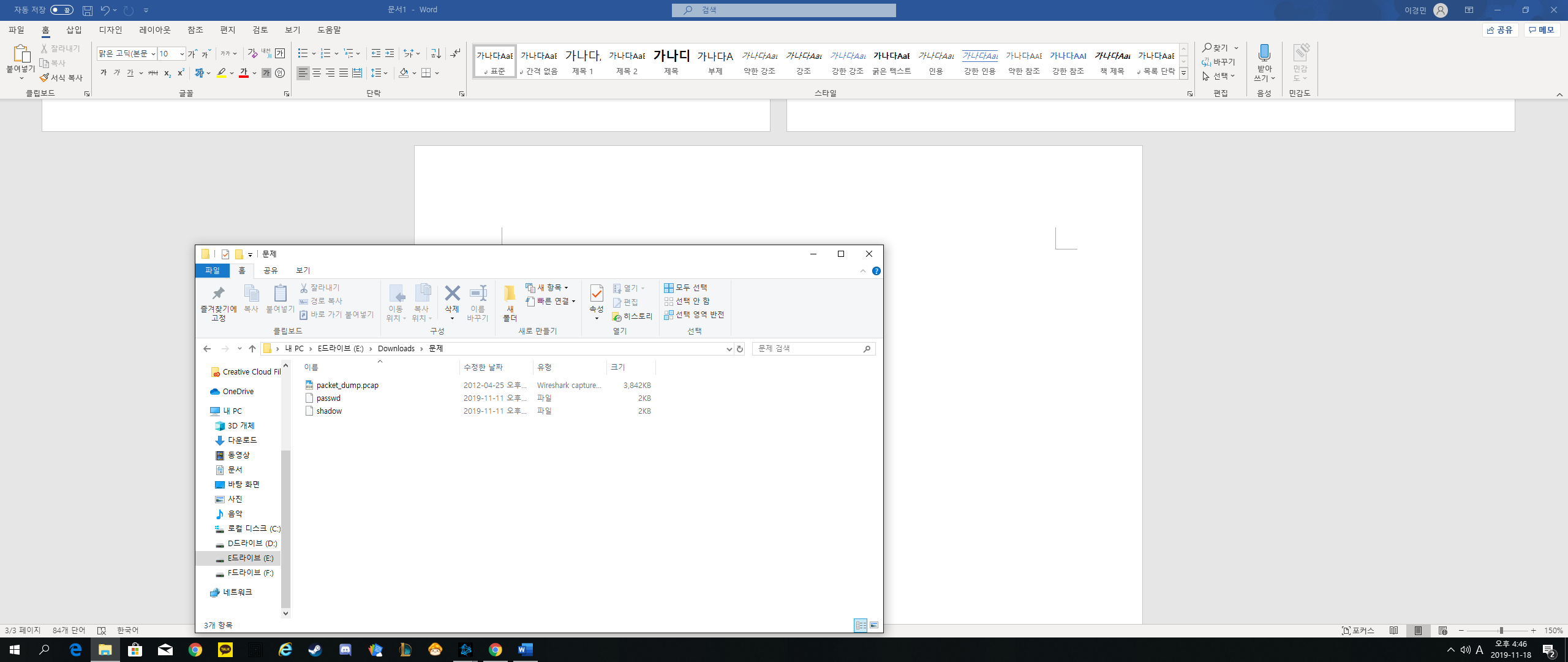
=> result 의 i를 in으로 대체, 다시 result에 담음 (result = aadmin)

=> result1과 result2에 Mid를 통해 result문자열을 잘라서 담음 (result1 = ad , result2 = min)

=> result에 result1과 result2를 이어 담음 (result = admin)

Do you know password?





khackers password를 찾기 위해 shadow에서 khackers부분을 추출

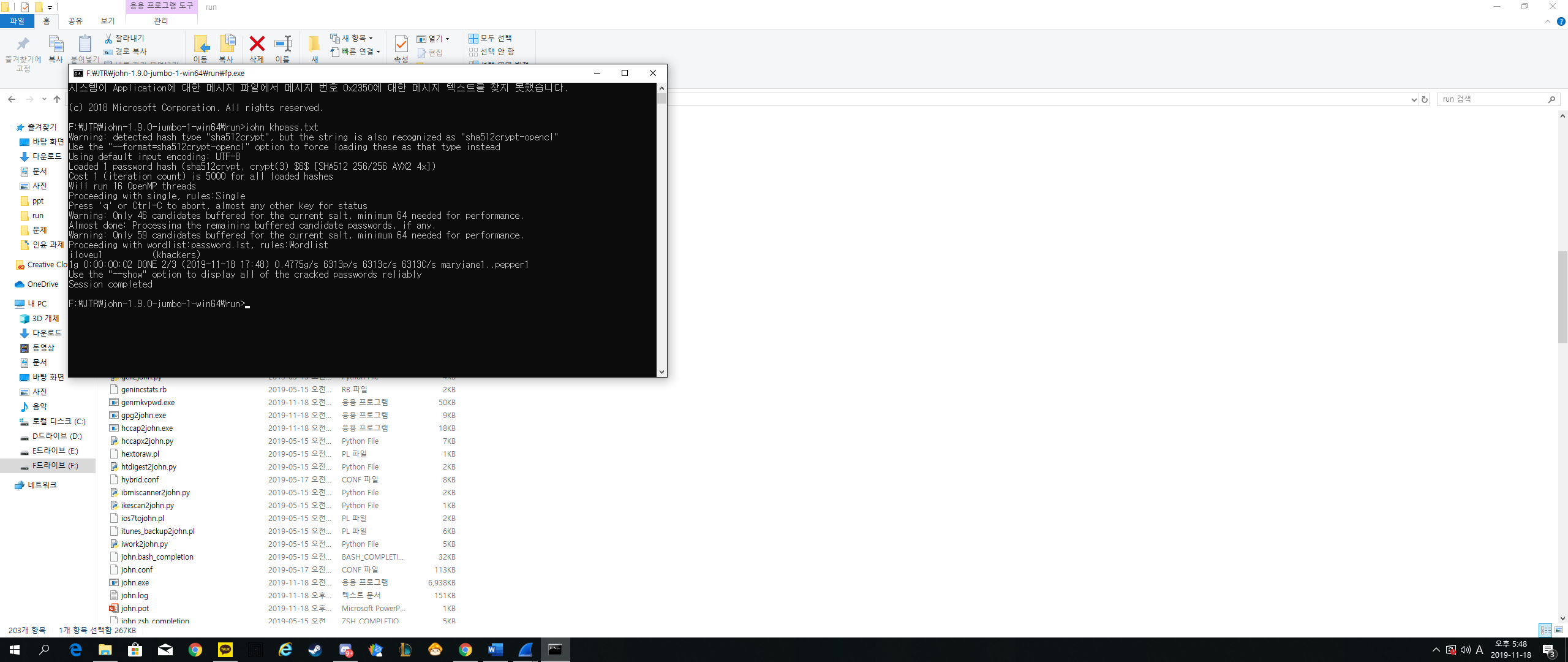
khackers:$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/:15427:0:99999:7:::

여기서 패스워드를 알아낼 때 필요한 부분은 아래와 같다.

$6$QlRlqGhj$BZoS9PuMMRHZZXz1Gde99W01u3kD9nP/zYtl8O2dsshdnwsJT/1lZXsLar8asQZpqTAioiey4rKVpsLm/bqrX/

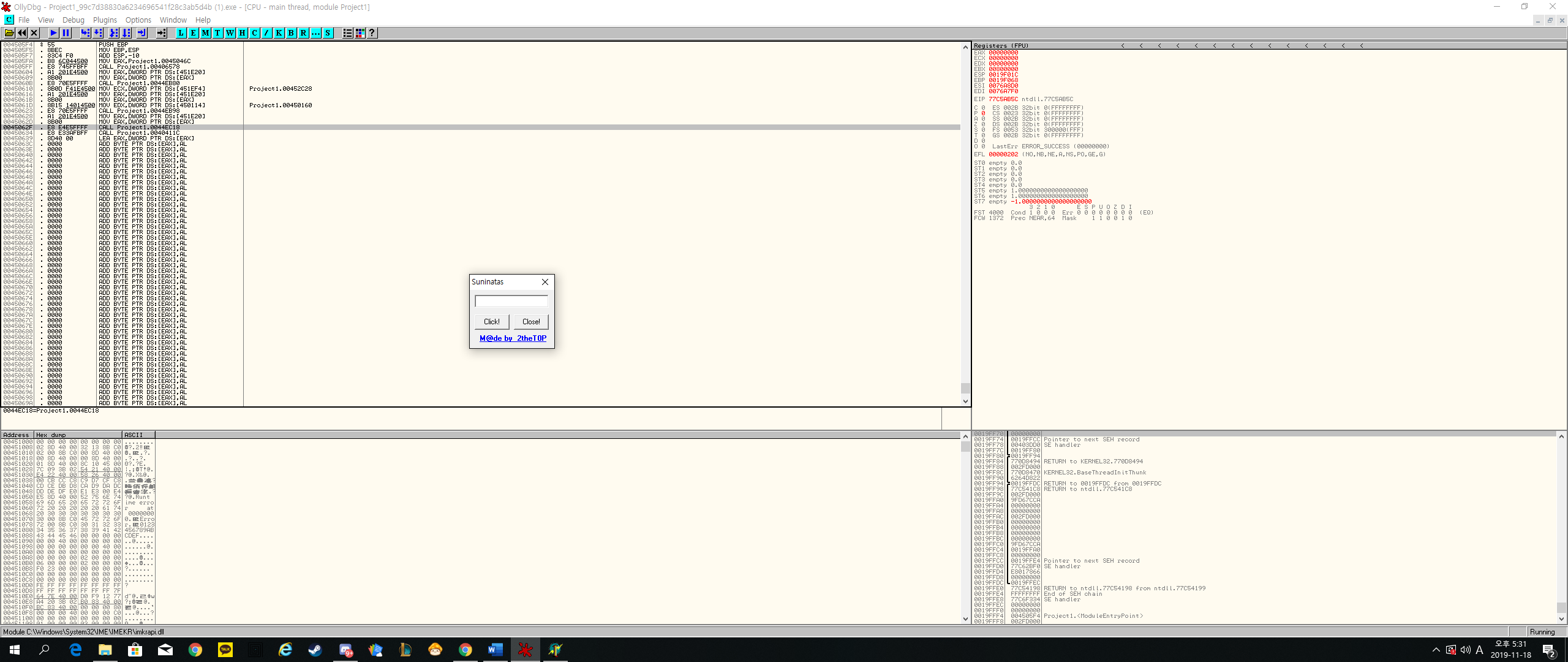
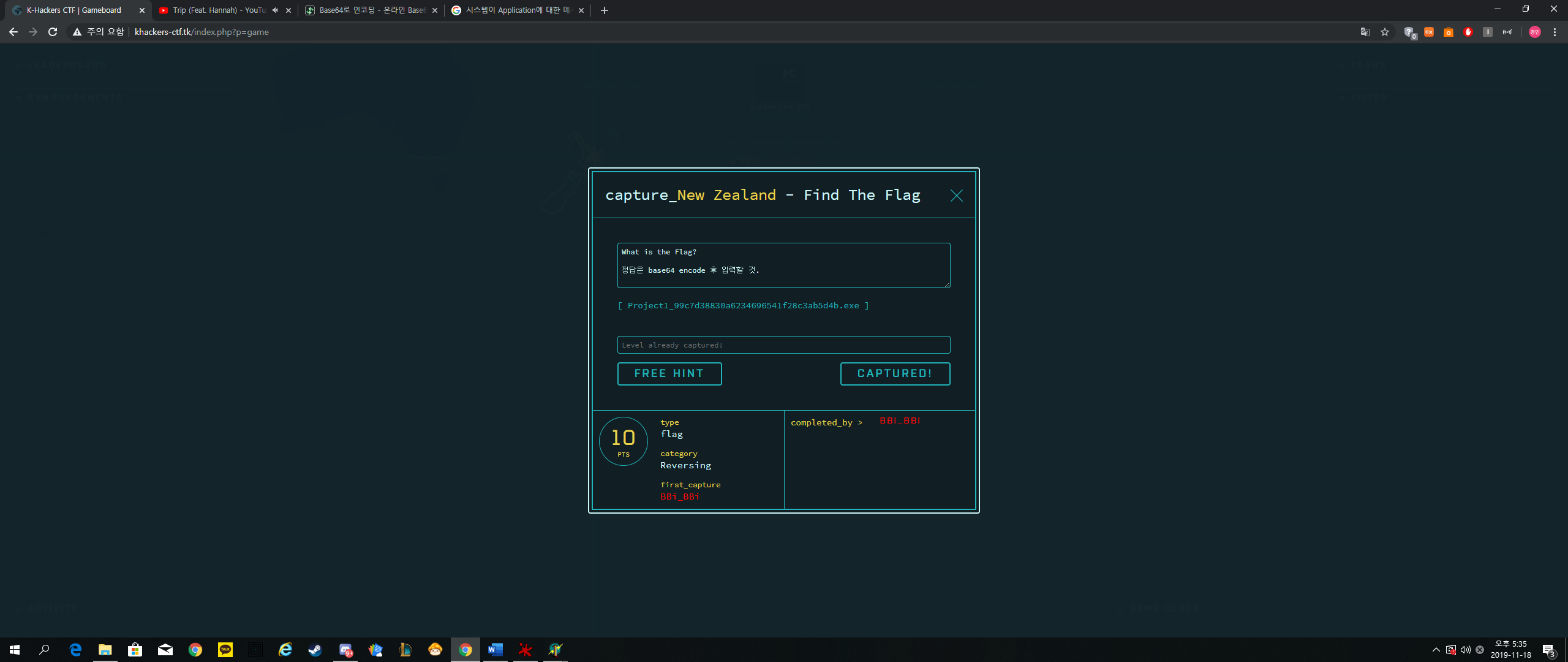
$hash id(6 = SHA-512) $salt $hash value로 구성되어 있음

이는 존 더 리퍼 툴을 이용해 해결할 수 있다.



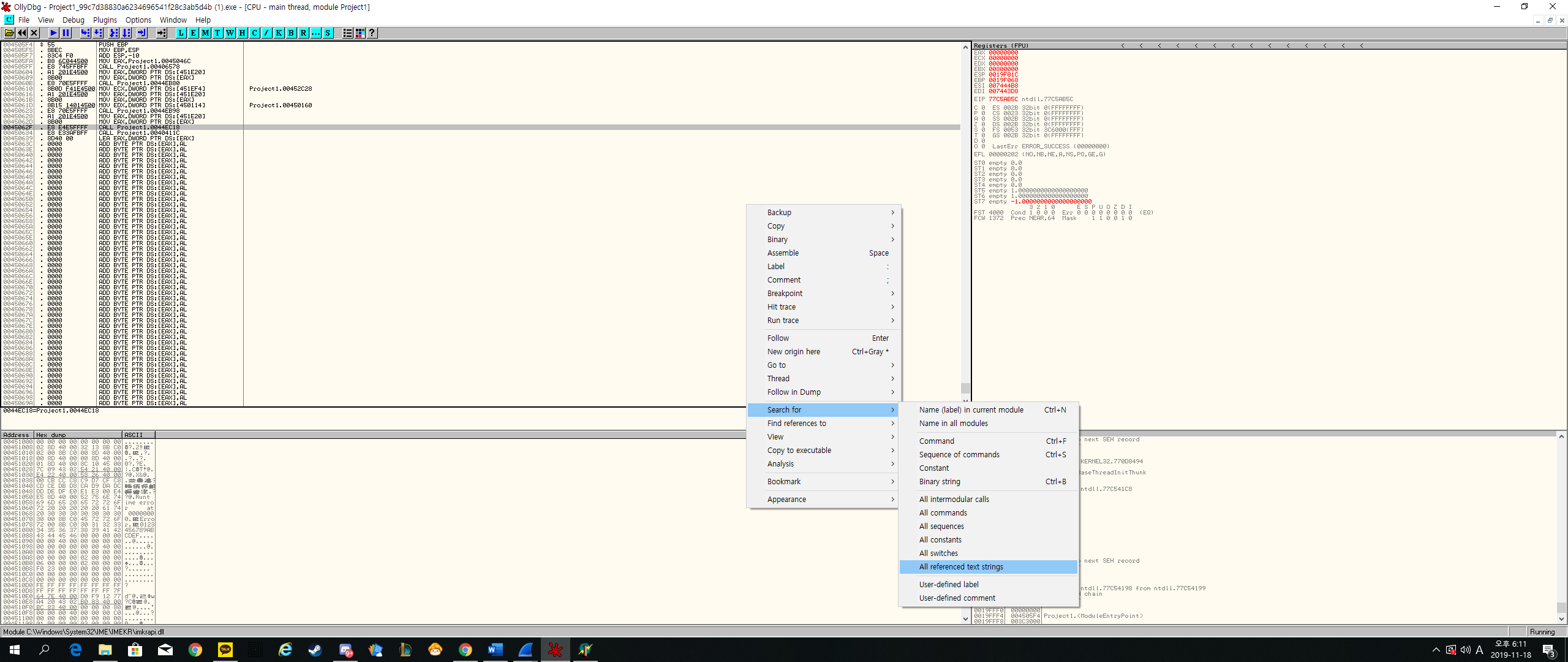
답 = aWxvdmV1MQ== (iloveu1)

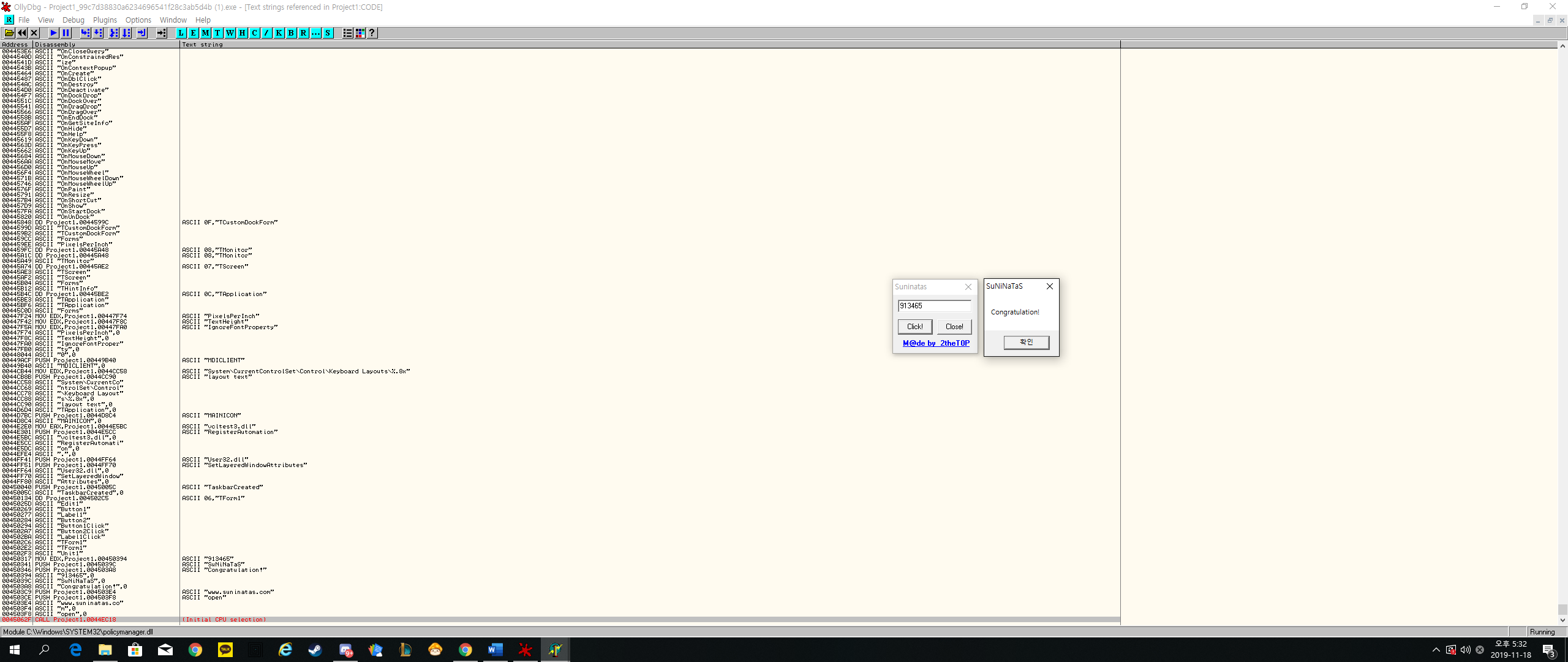
Find The Flag



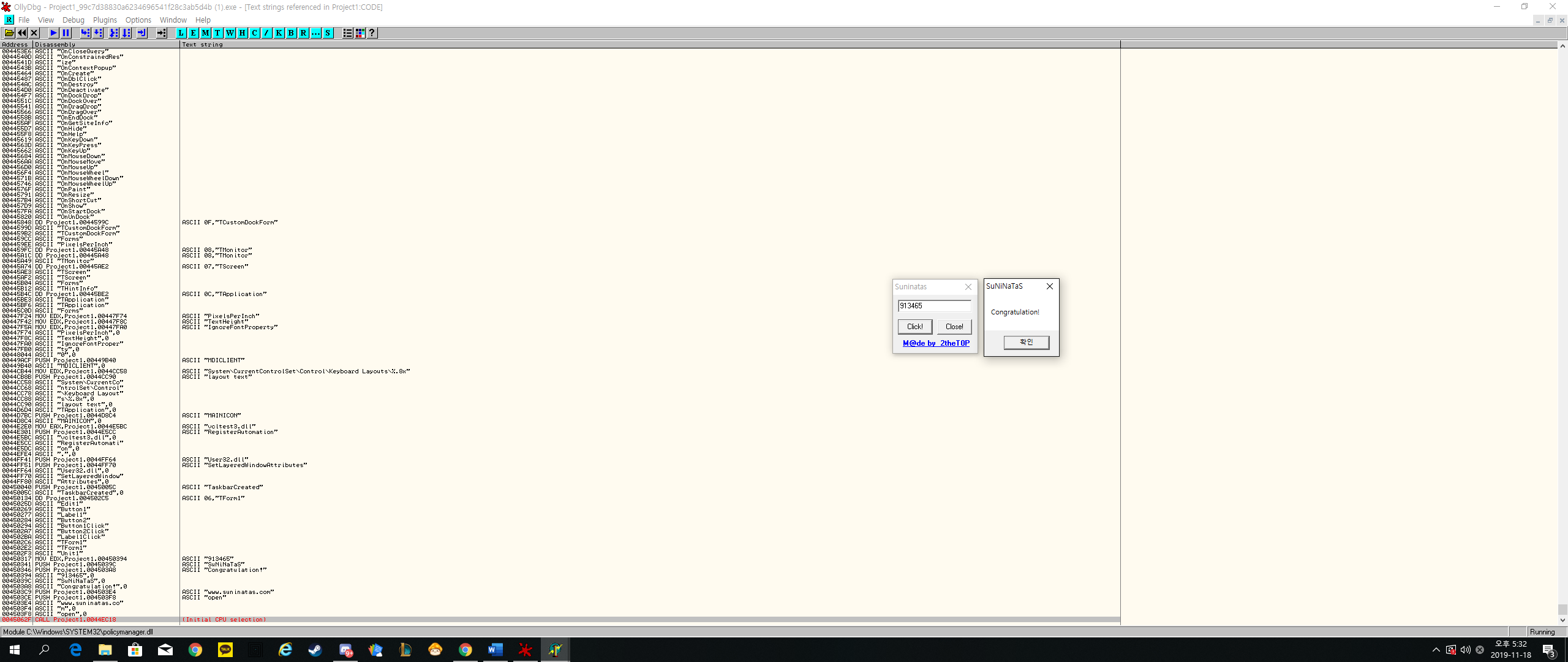
문제의 답을 입력한후 Click!을 누르게 되면 다음으로 넘어가는 형식

답을 찾기 위해 올리디버거를 통해 코드에 참조되는 문자열을 조회함





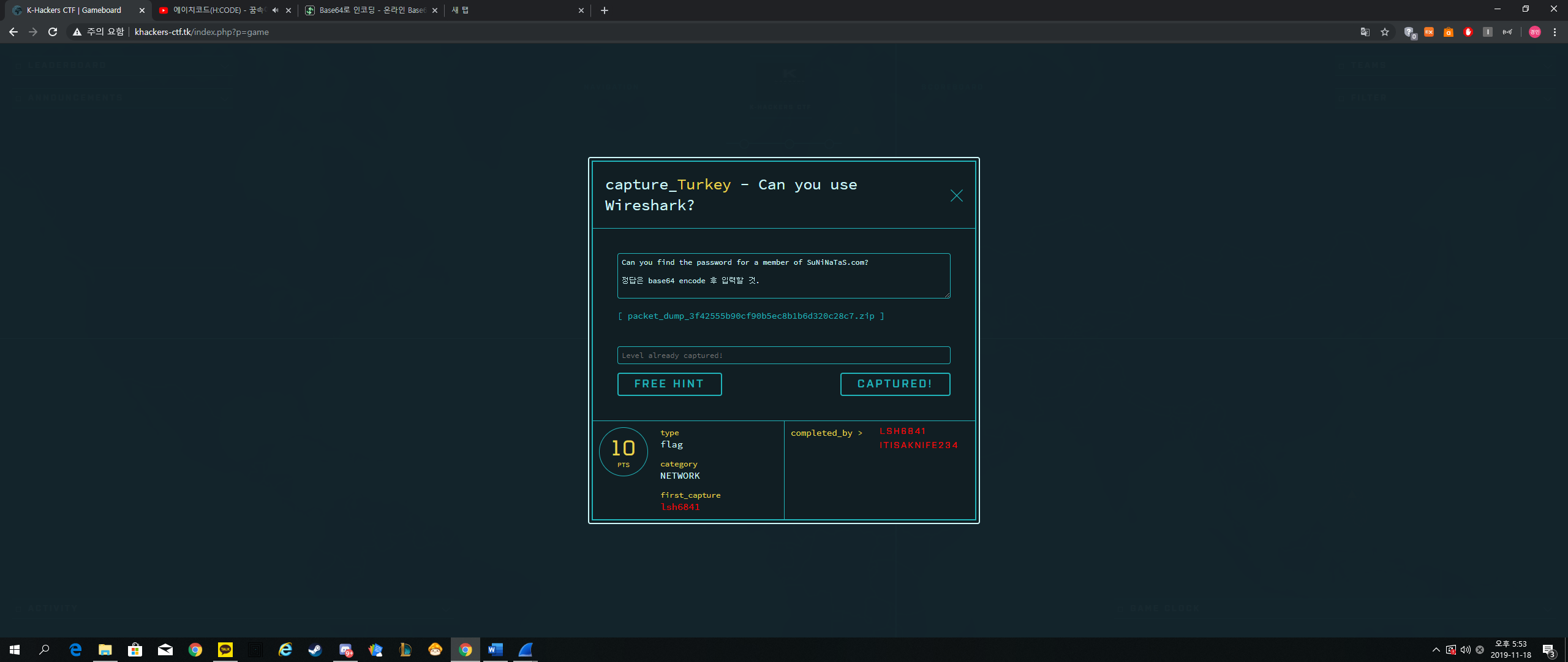
정답으로 추정되는 값을 발견함



Congratulation! 출력과 함께 문제가 해결됨

답 : OTEzNDY1 (913465)

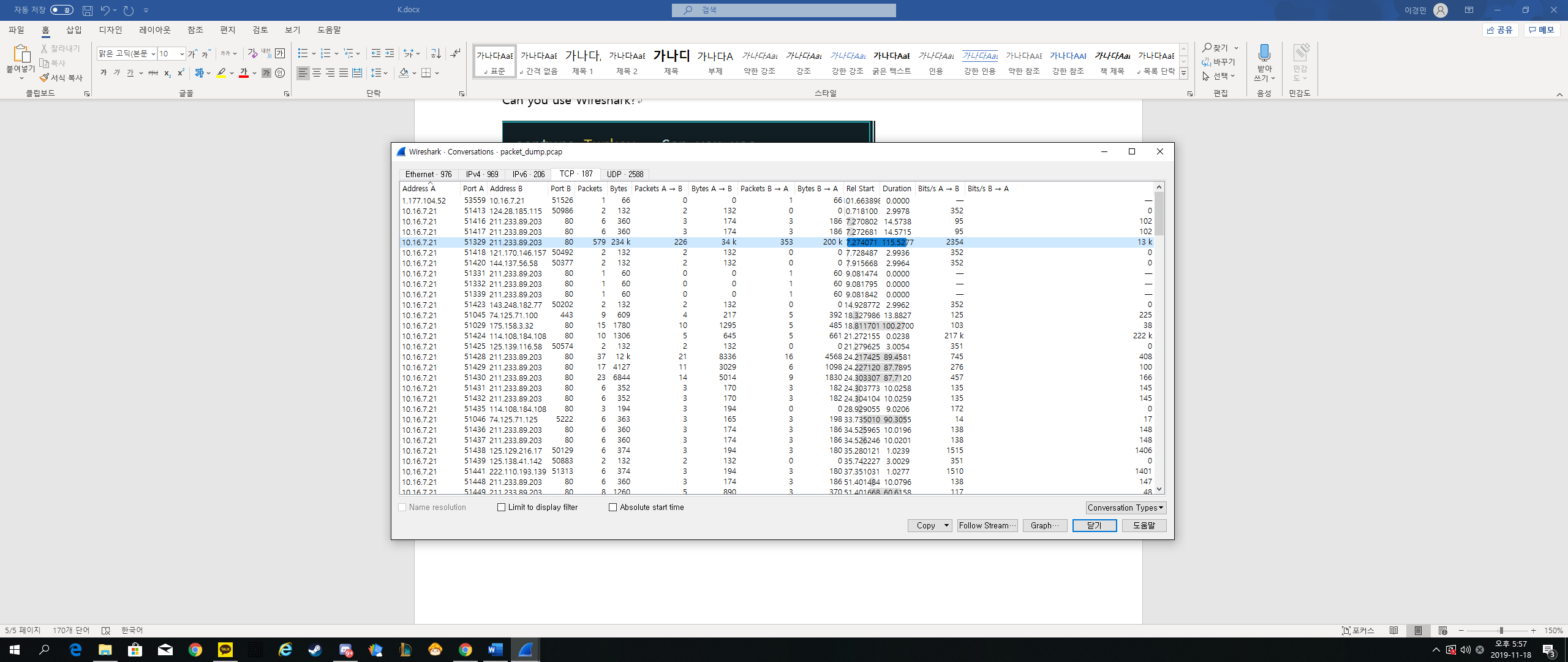
Can you use Wireshark?



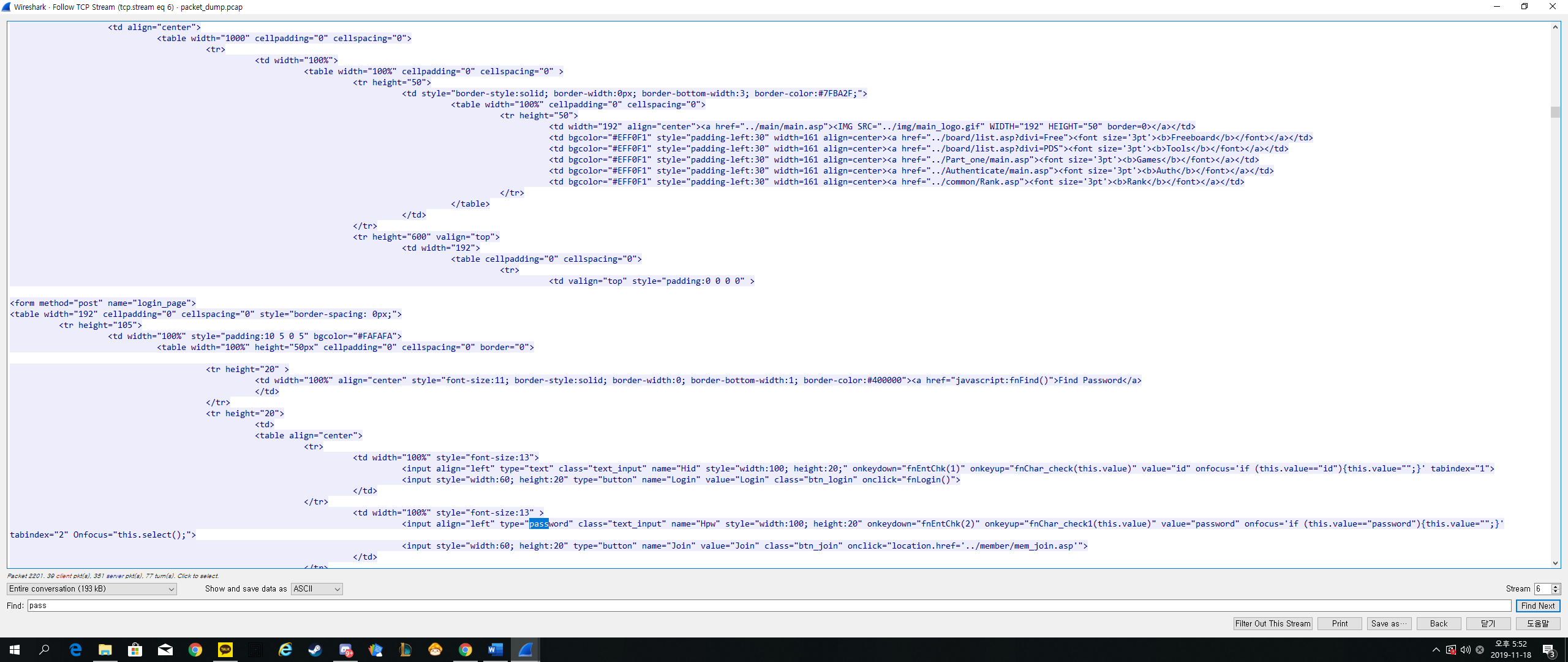
SuNiNaTaS멤버의 비밀번호를 찾는 문제

Wireshark를 통해 주어진 pcap파일을 분석

Conversations을 통해 TCP통신탭을 확인 (호스트 간의 연결 내용 확인)

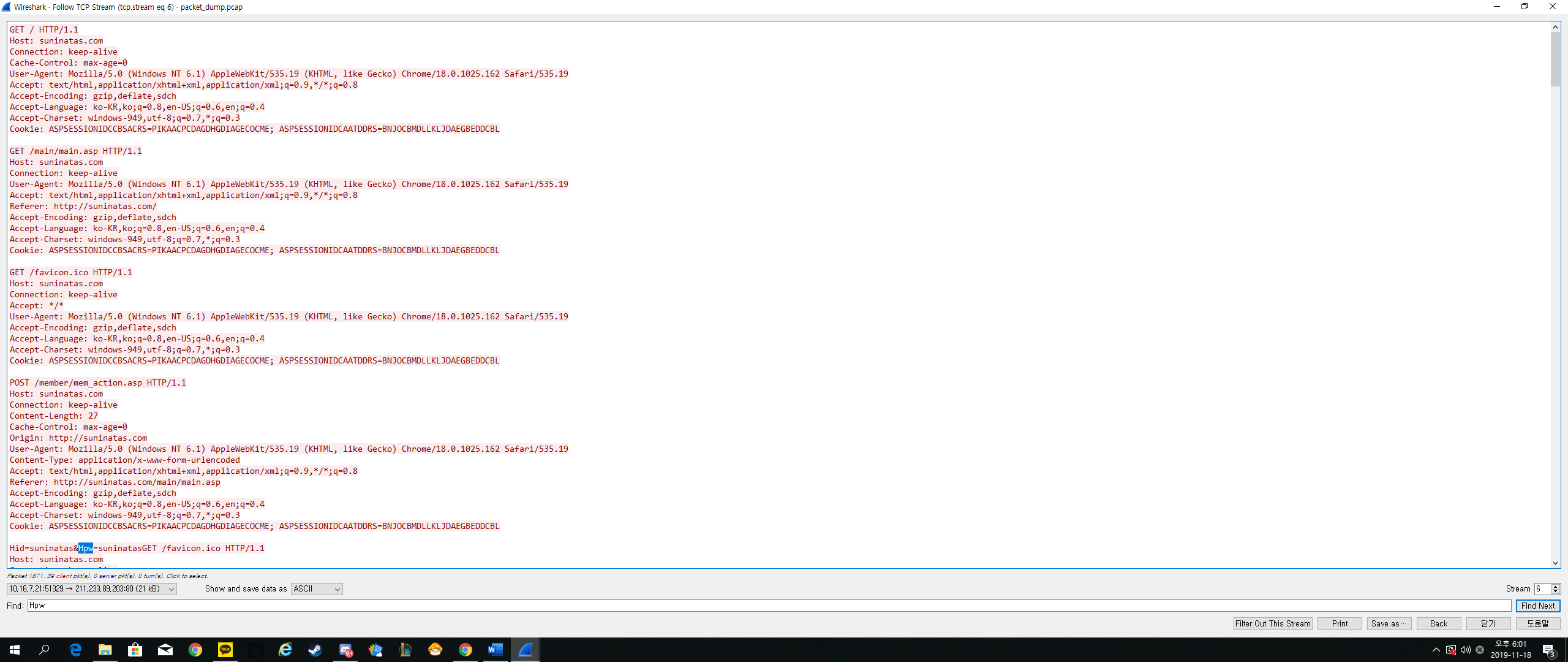


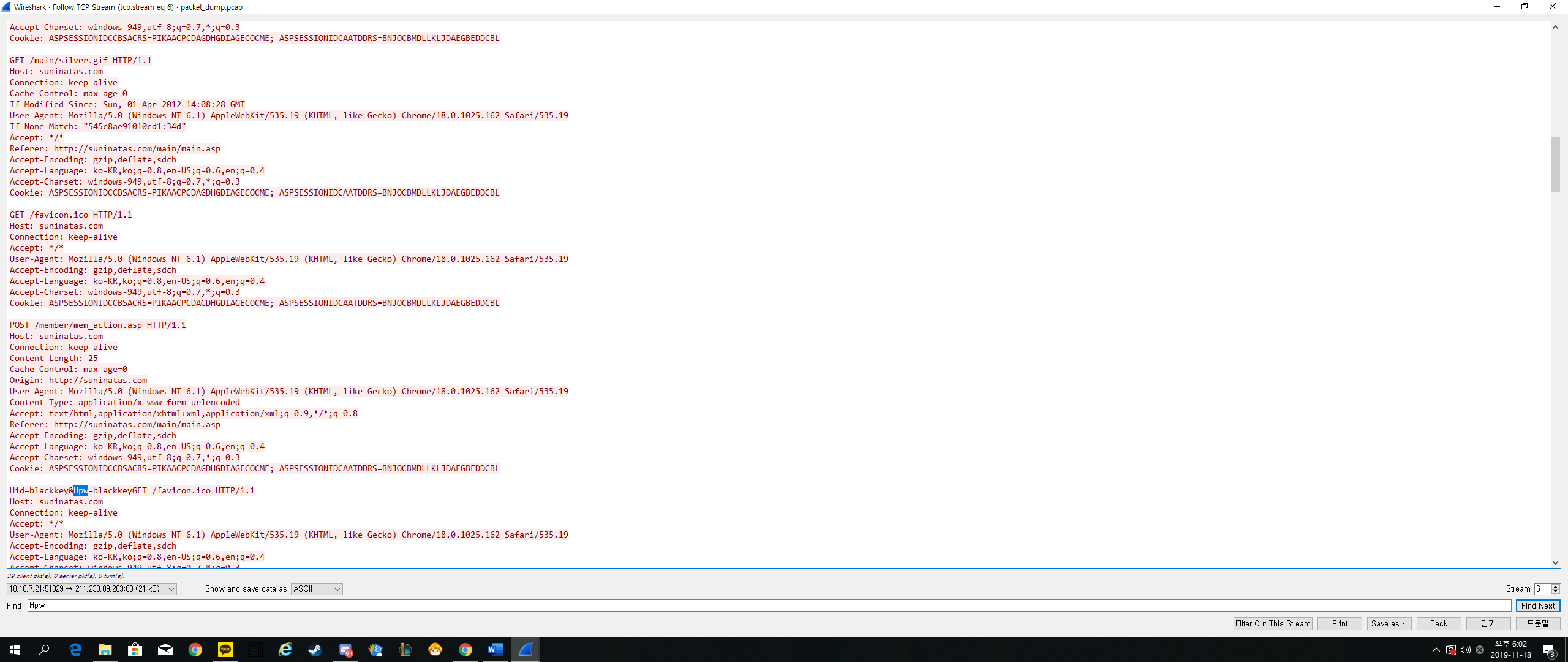
패킷을 확인하며 단서를 확인 할 만한 내용을 발견함

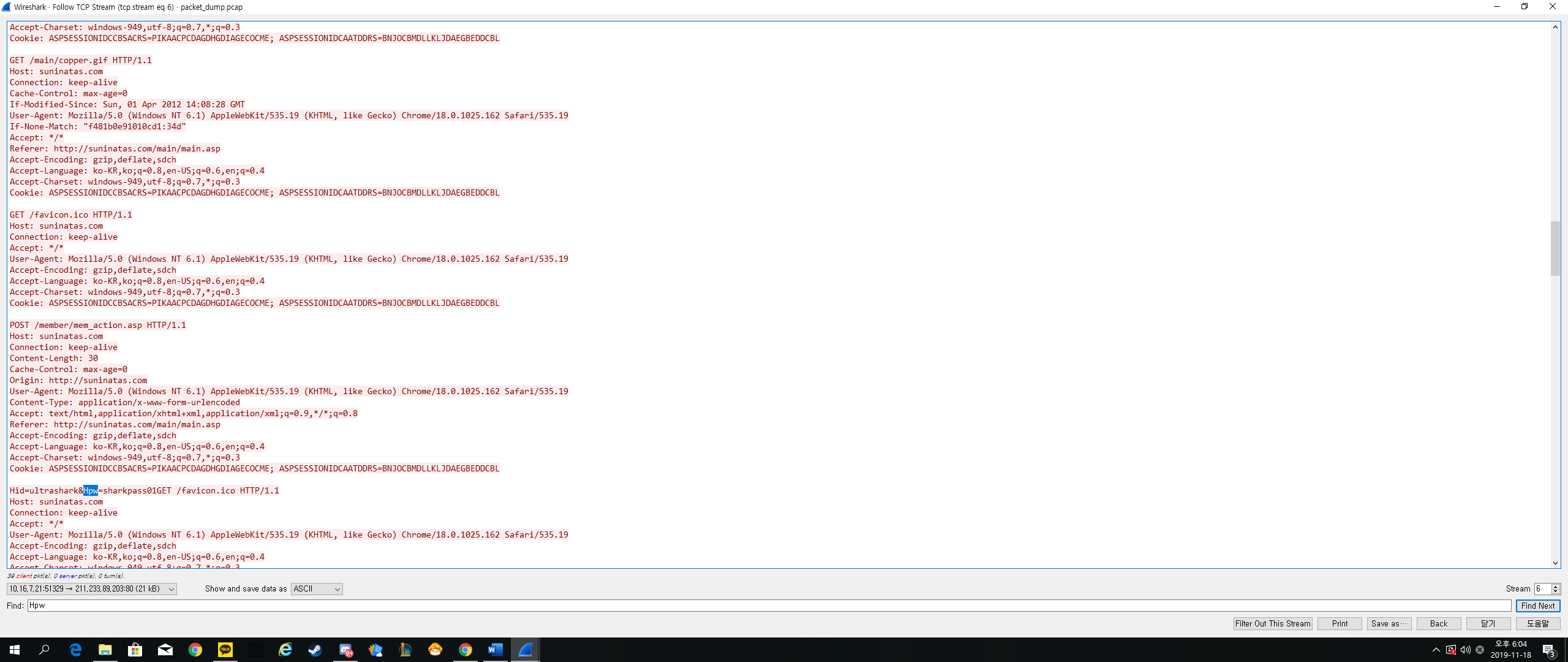


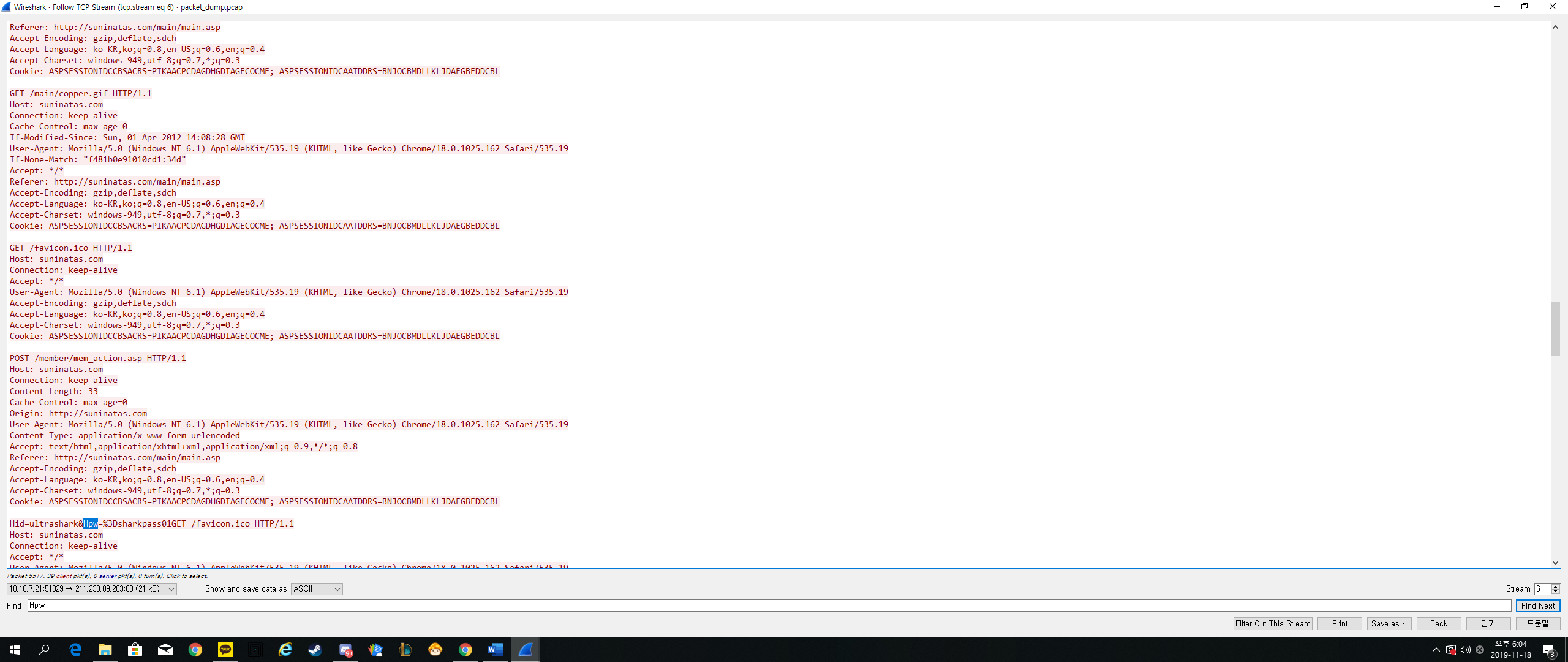
Value가 password인 Hpw를 발견

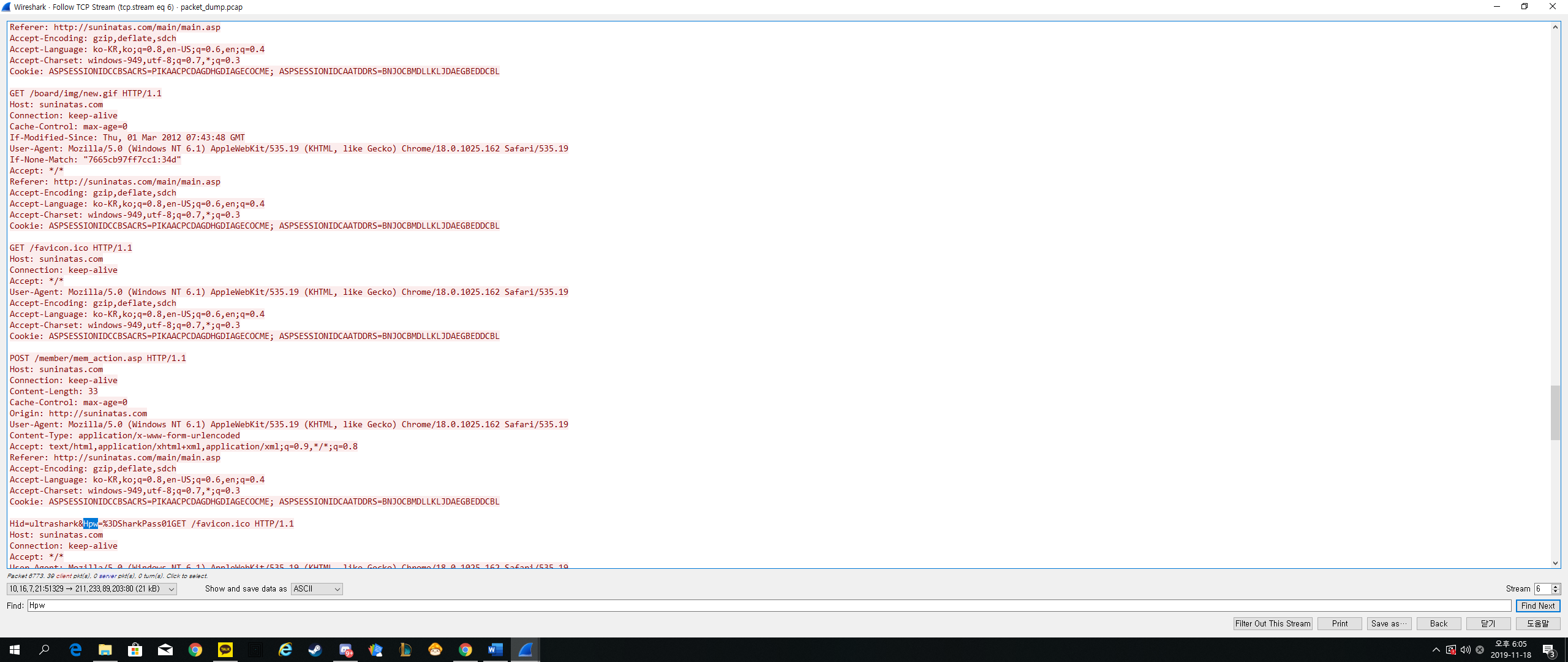
범위를 Hpw로 좁혀 검색











Suninatas, blackkey, sharkpass01, =sharkpass01, =SharkPass01

5개 모두 정답에 대입 하였을 때 =SharkPass01이 정답으로 확인됨

답 : PVNoYXJrUGFzczAx (=SharkPass01)