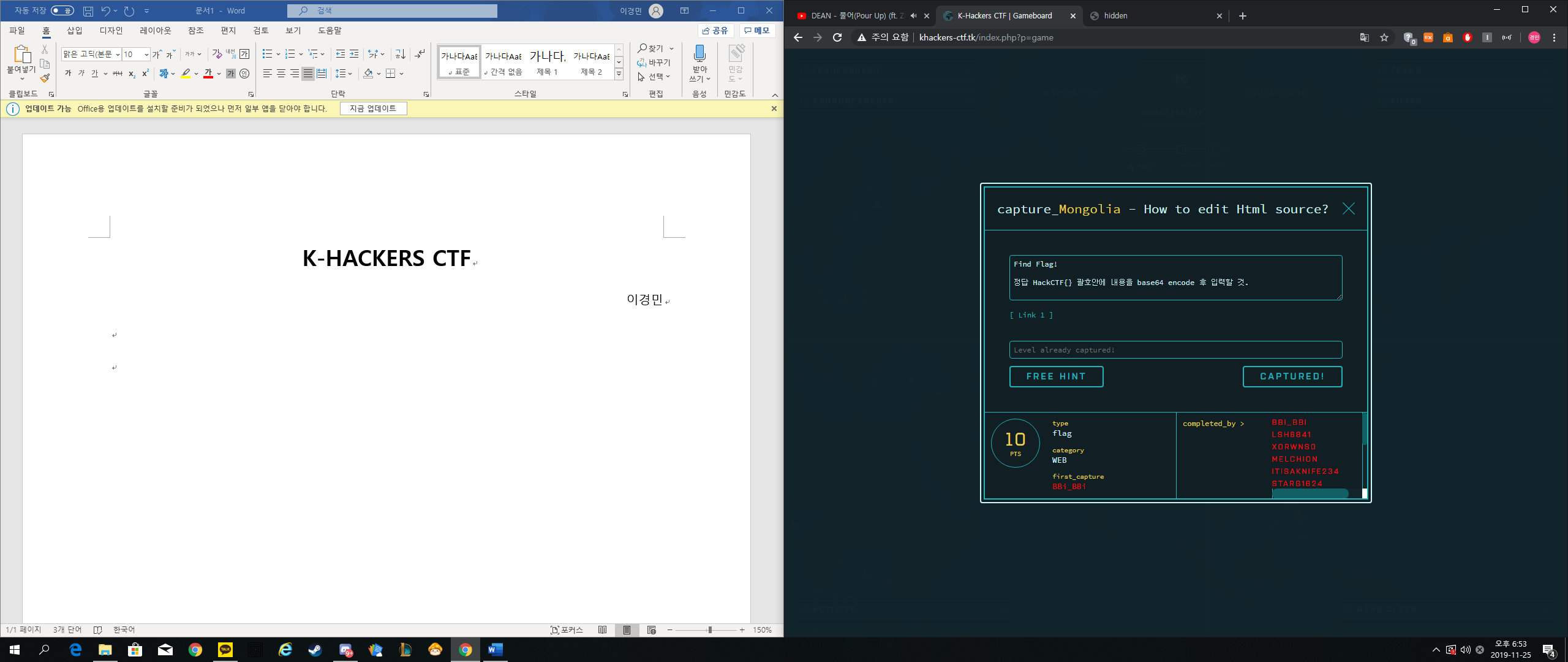
**K-HACKERS CTF**

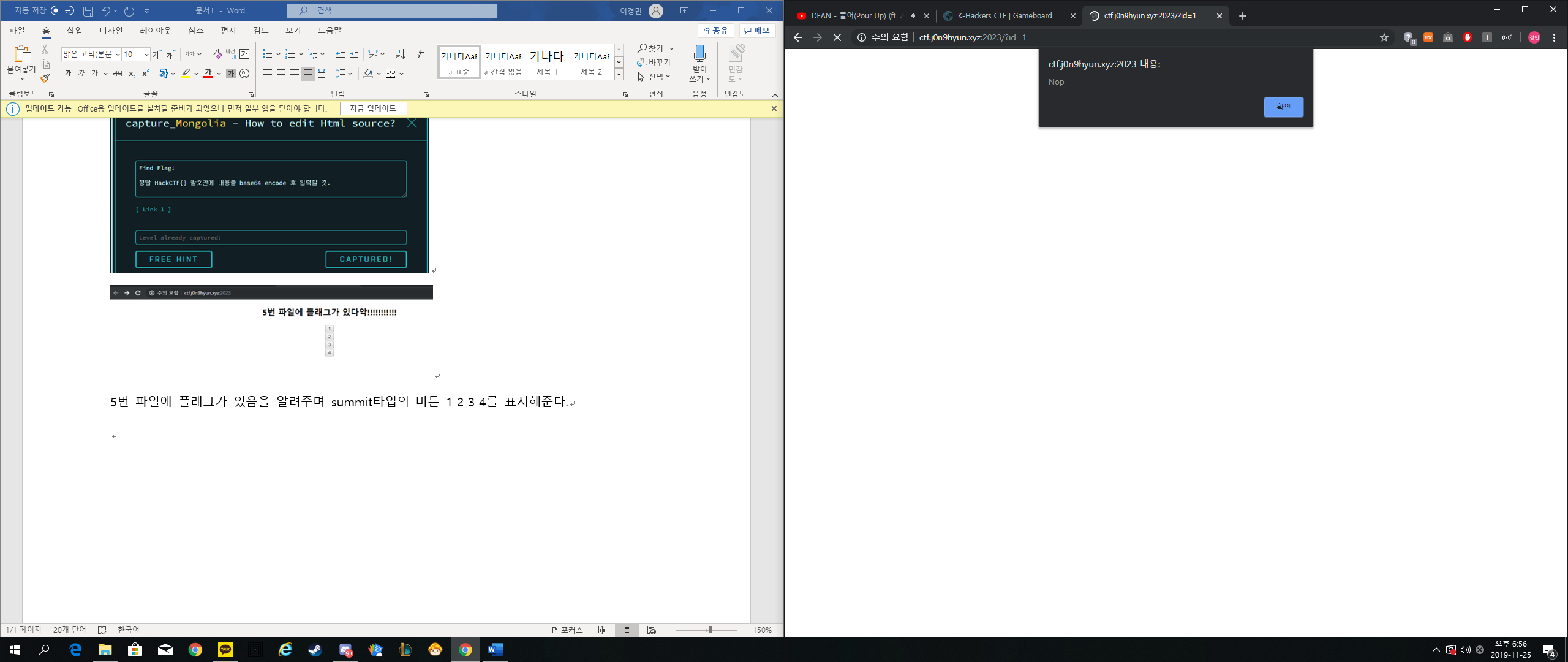
이경민

How to edit Html source?

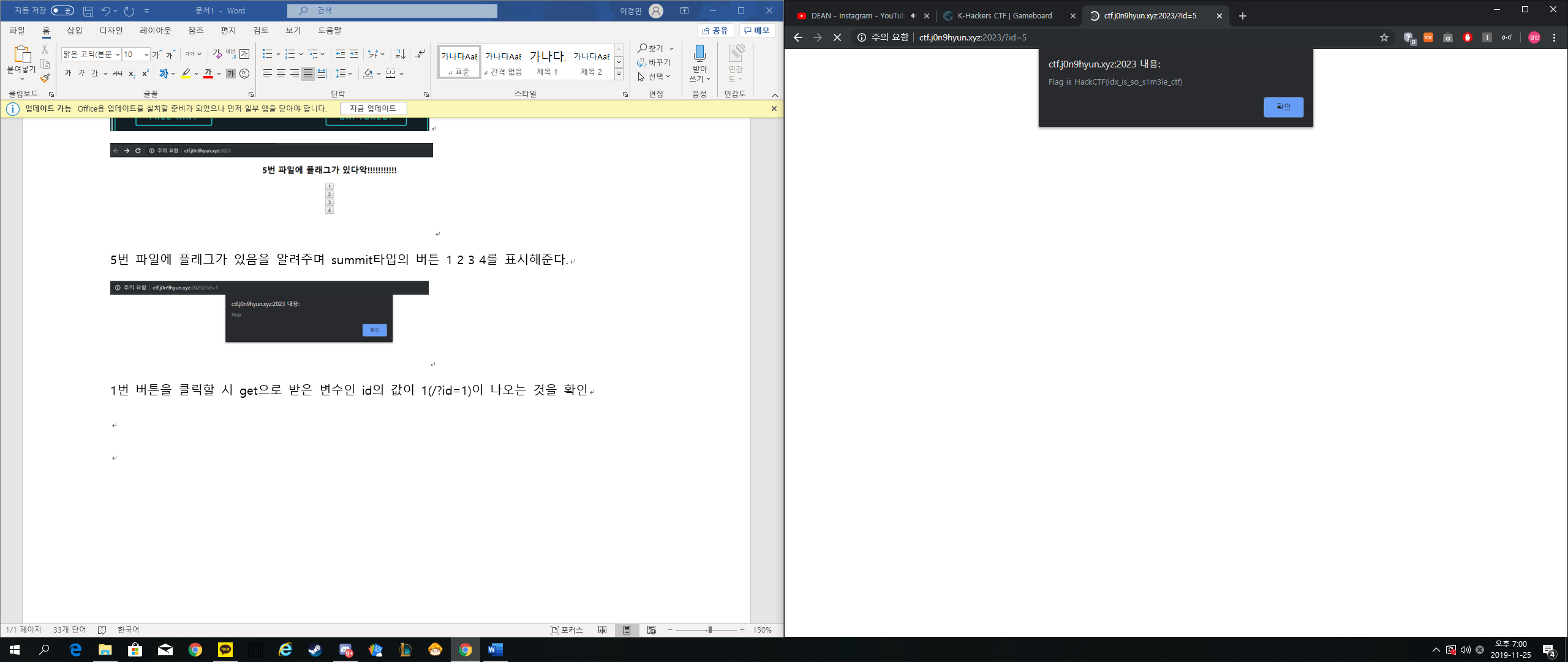




5번 파일에 플래그가 있음을 알려주며 summit타입의 버튼 1 2 3 4를 표시해준다.



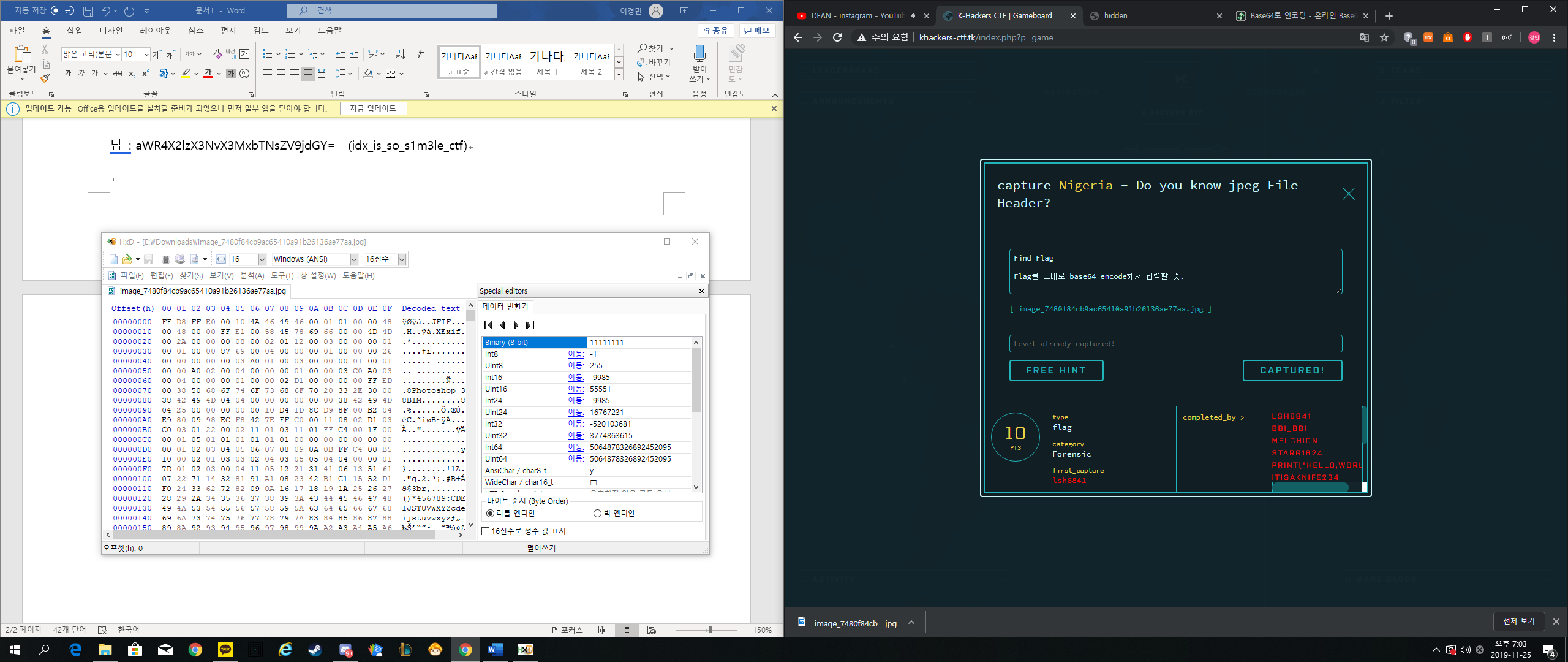
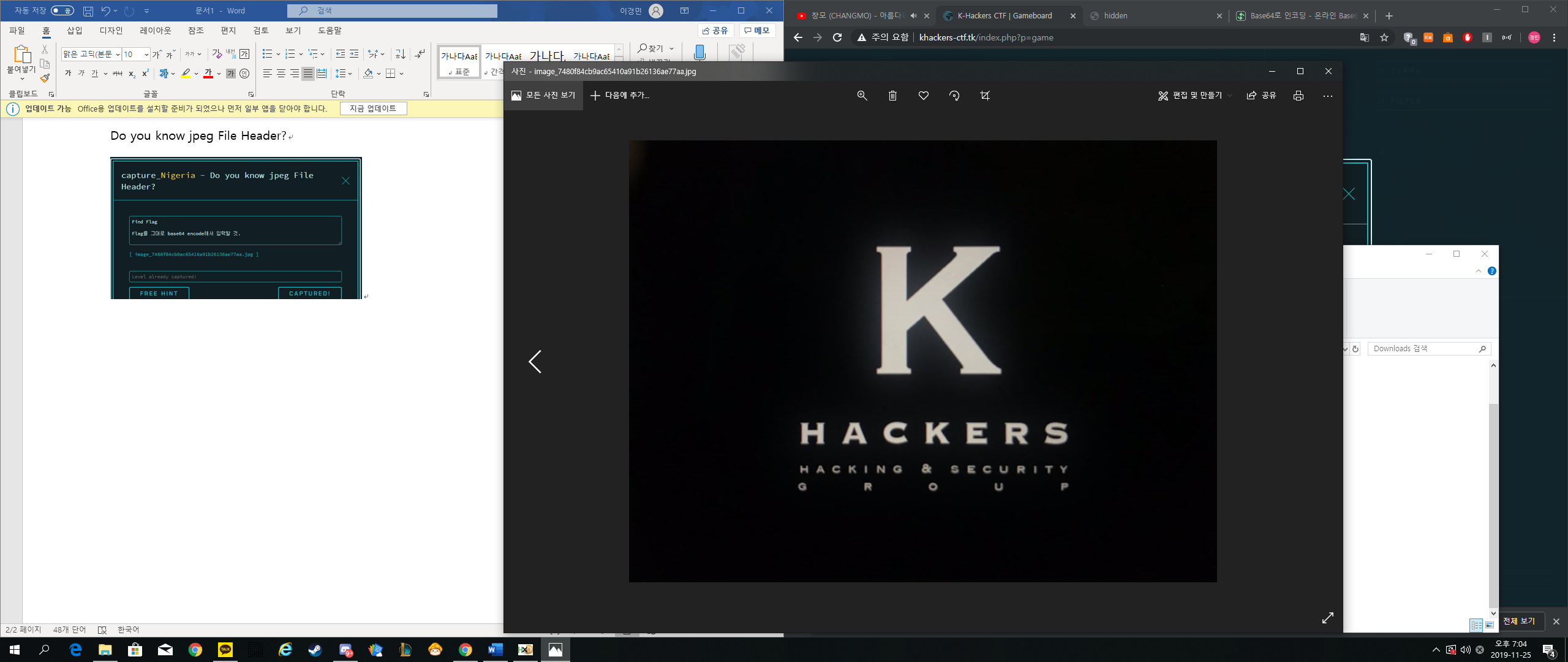
1번 버튼을 클릭할 시 get으로 받은 변수인 id의 값이 1(/?id=1)이 나오는 것을 확인



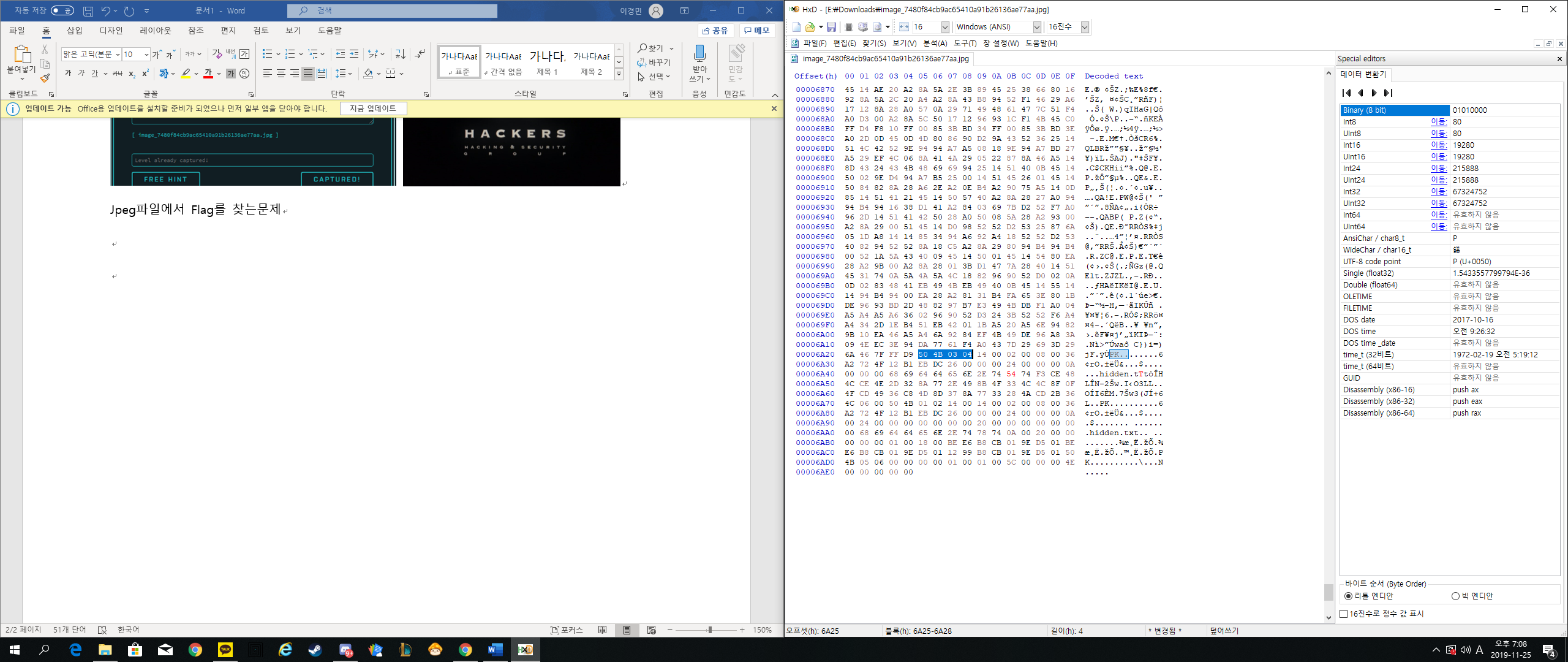
값을 5로 변경하여 Flag를 얻어냄

답 : aWR4X2lzX3NvX3MxbTNsZV9jdGY= (idx\_is\_so\_s1m3le\_ctf)

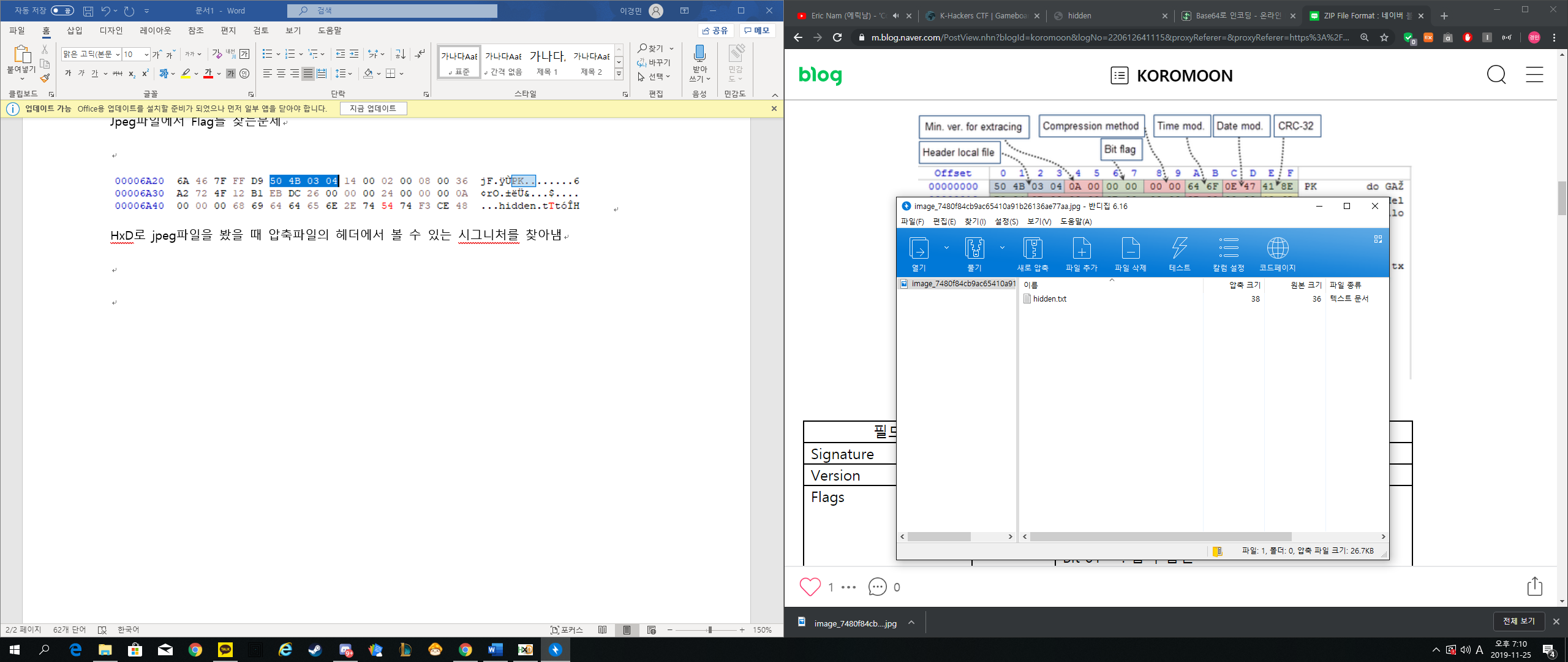
Do you know jpeg File Header?

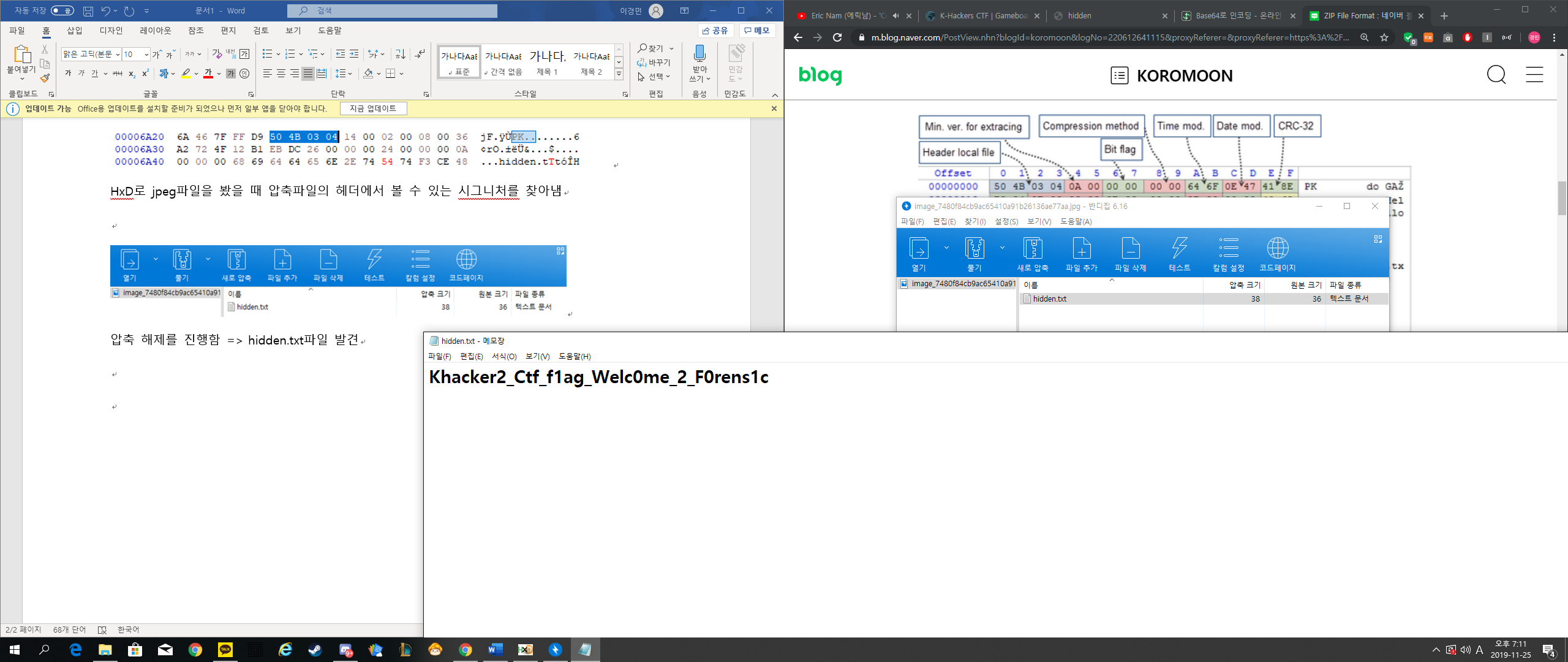
Jpeg파일에서 Flag를 찾는문제



HxD로 jpeg파일을 봤을 때 압축파일의 헤더에서 볼 수 있는 시그니처를 찾아냄



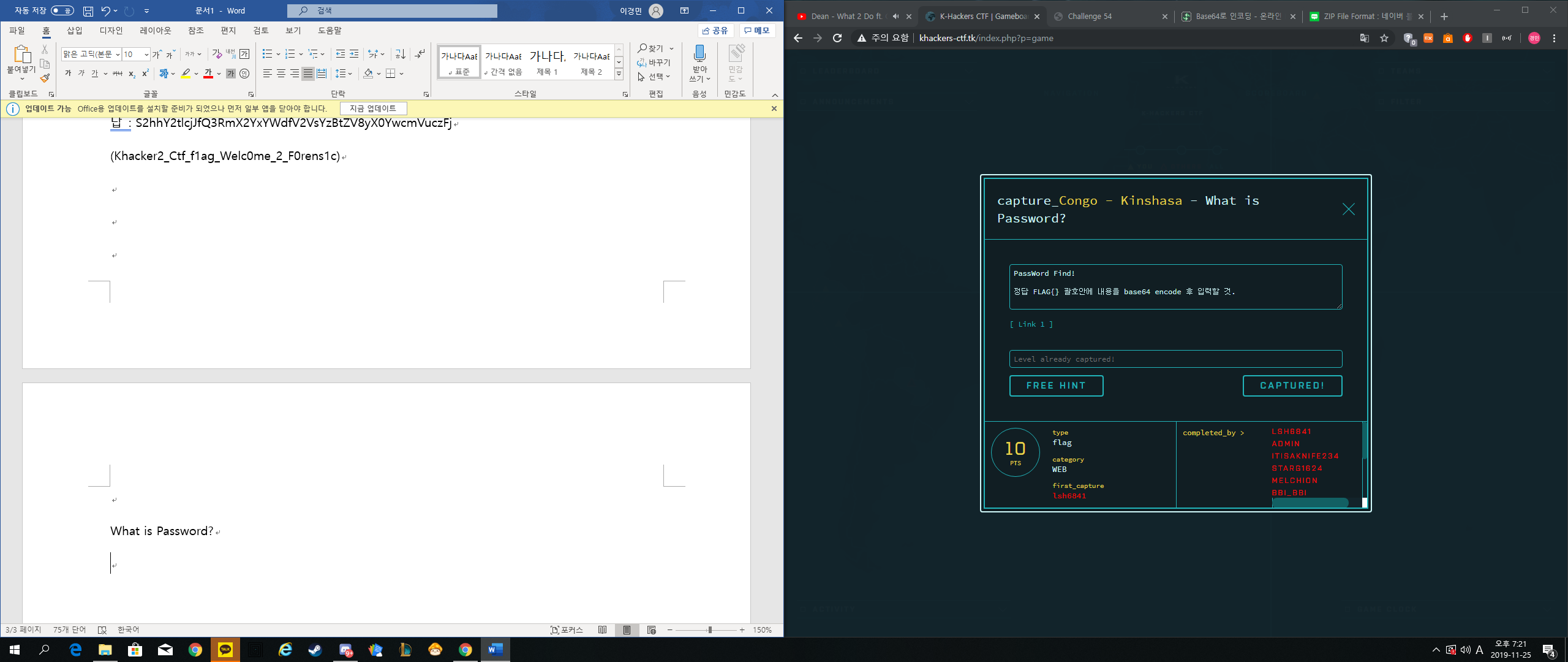
압축 해제를 진행함 => hidden.txt파일 발견

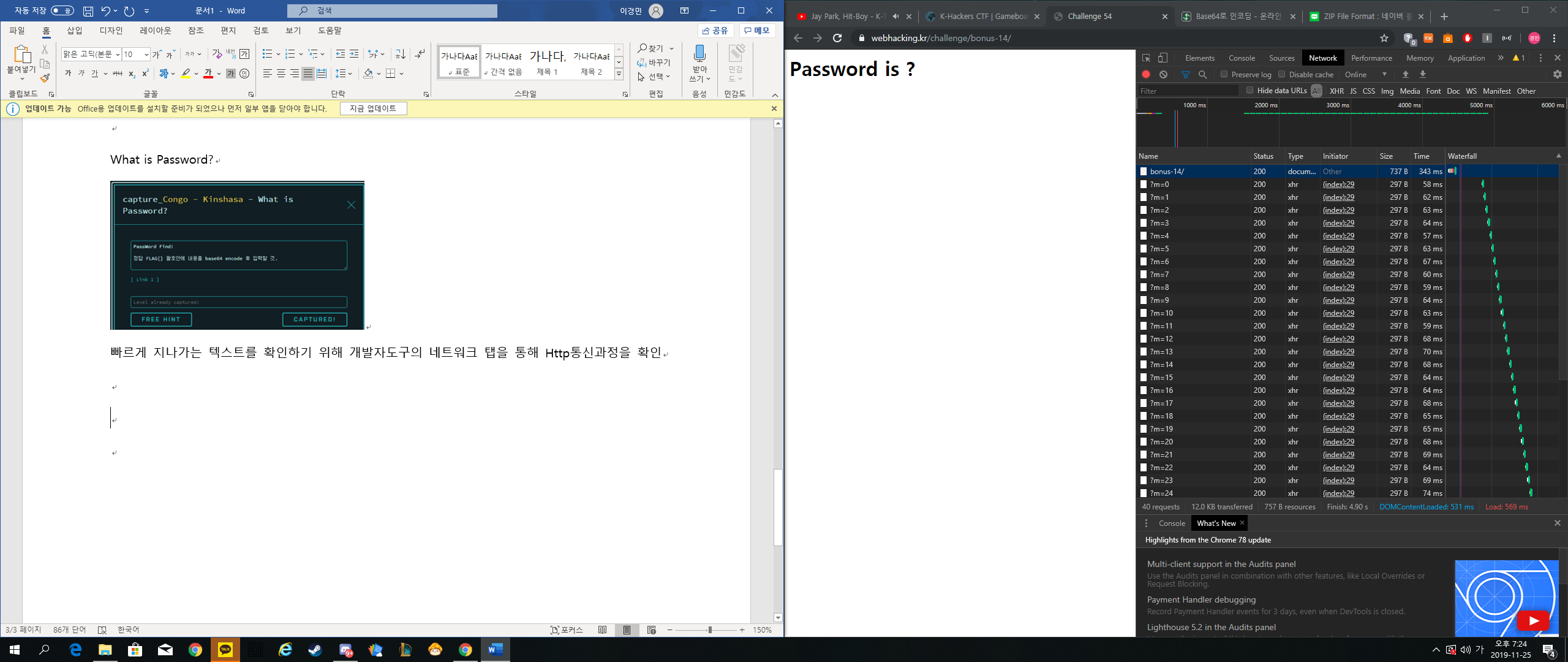


답 : S2hhY2tlcjJfQ3RmX2YxYWdfV2VsYzBtZV8yX0YwcmVuczFj

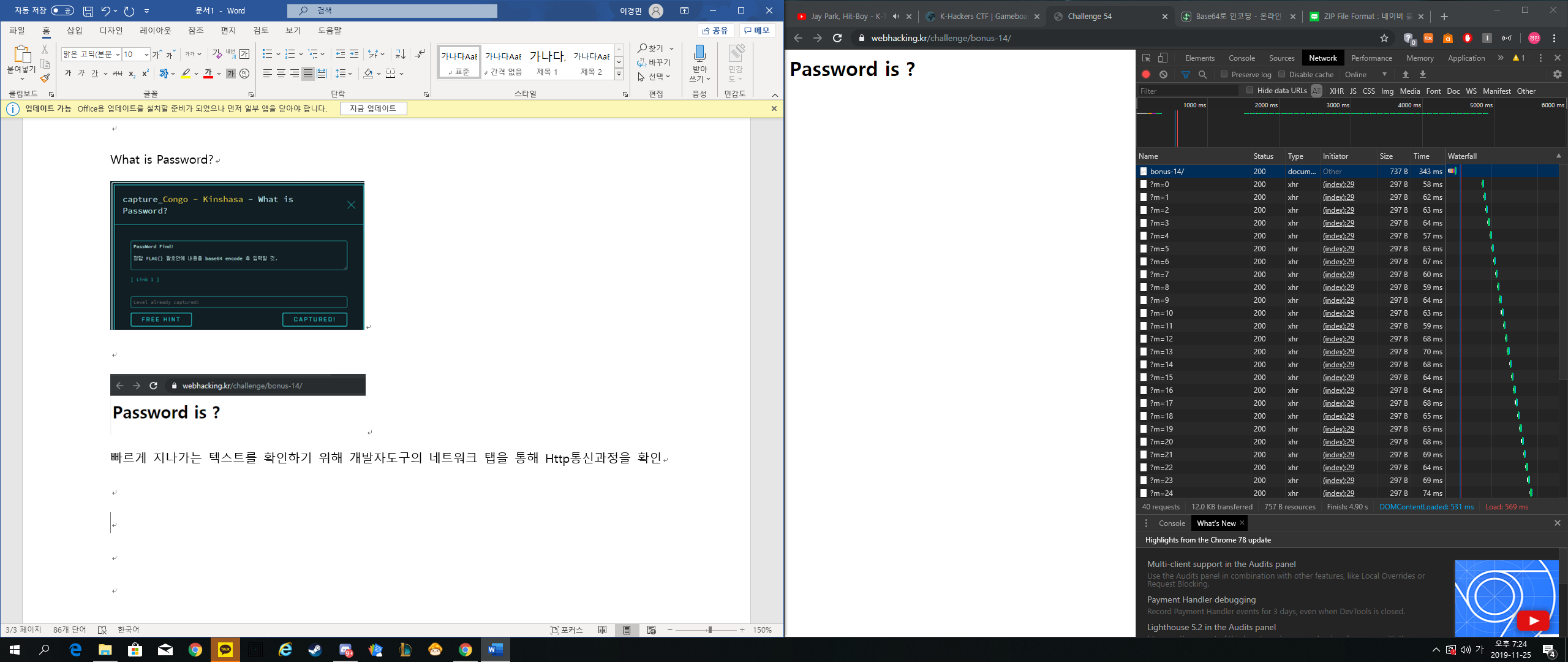
(Khacker2\_Ctf\_f1ag\_Welc0me\_2\_F0rens1c)

What is Password?





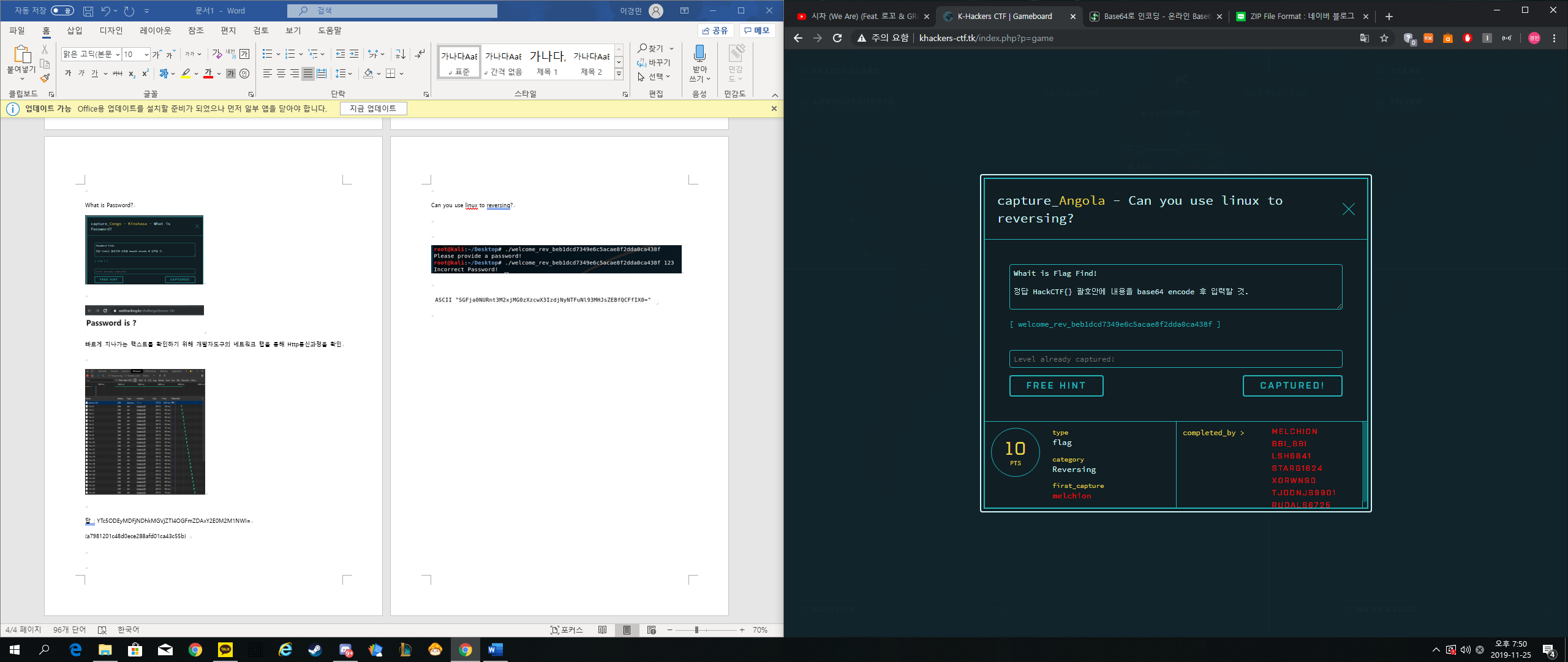
빠르게 지나가는 텍스트를 확인하기 위해 개발자도구의 네트워크 탭을 통해 Http통신과정을 확인



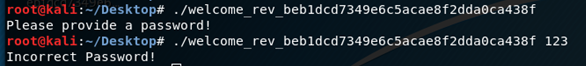
답 : YTc5ODEyMDFjNDhkMGVjZTI4OGFmZDAxY2E0M2M1NWI=

(a7981201c48d0ece288afd01ca43c55b)

Can you use linux to reversing?



ELF파일을 리버싱해 Flag를 찾는 문제



실행 시 인자 값을 함께 입력해야 하며 잘못된 값을 입력하면 Incorrect Password!가 출력된다

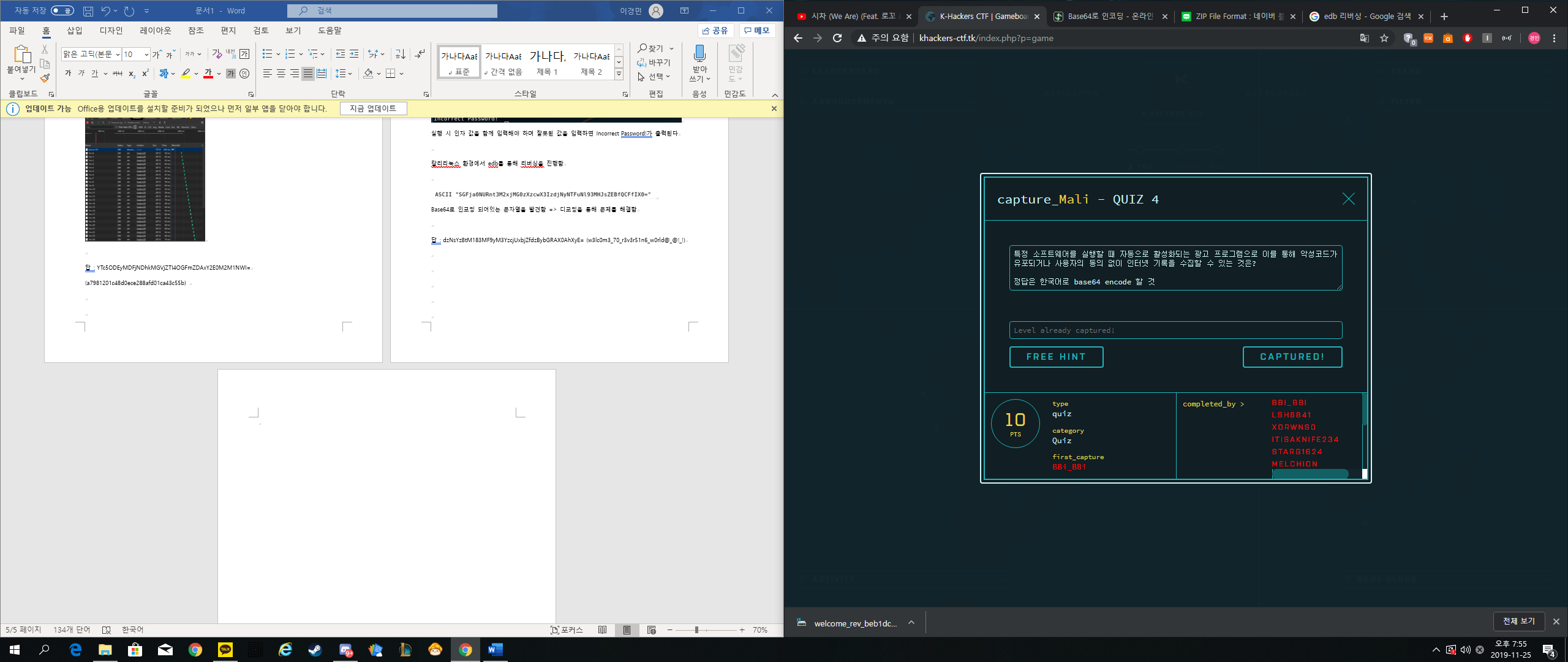
칼리리눅스 환경에서 edb를 통해 리버싱을 진행함



Base64로 인코딩 되어있는 문자열을 발견함 => 디코딩을 통해 문제를 해결함

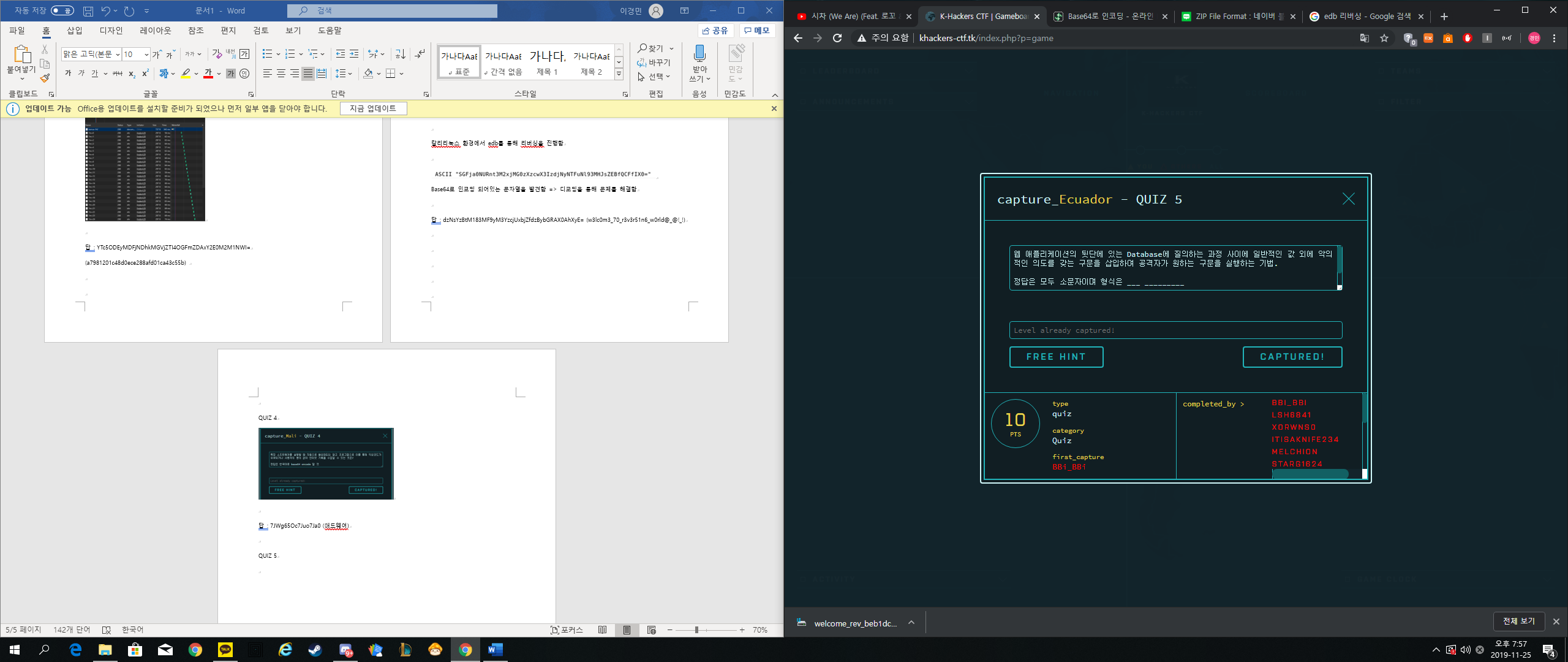
답 : dzNsYzBtM183MF9yM3YzcjUxbjZfdzBybGRAX0AhXyE= (w3lc0m3\_70\_r3v3r51n6\_w0rld@\_@!\_!)

QUIZ 4



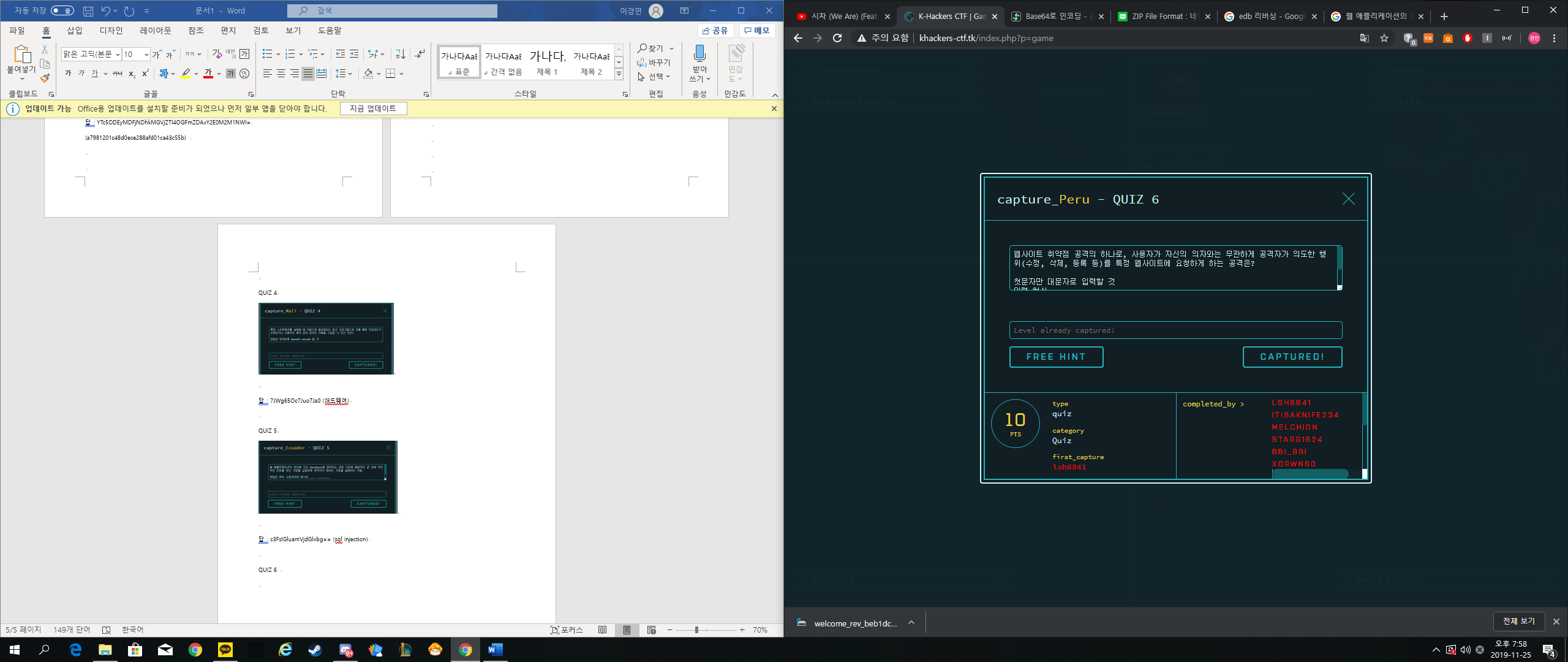
답 : 7JWg65Oc7Juo7Ja0 (애드웨어)

QUIZ 5



답 : c3FsIGluamVjdGlvbg== (sql injection)

QUIZ 6



답 : Q3Jvc3Mtc2l0ZSByZXF1ZXN0IGZvcmdlcnk= (Cross-site request forgery)