환경 설정

* <https://www.inflearn.com/course/%ED%94%84%EB%A6%AC%EB%8B%A4-frida-%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C-%EB%AA%A8%EC%9D%98%ED%95%B4%ED%82%B9/lecture/23041?tab=curriculum>
* <https://www.inflearn.com/course/%ED%94%84%EB%A6%AC%EB%8B%A4-frida-%EC%95%88%EB%93%9C%EB%A1%9C%EC%9D%B4%EB%93%9C-%EB%AA%A8%EC%9D%98%ED%95%B4%ED%82%B9/lecture/23042?tab=curriculum>

**frida-ps**



//

R : 원격 프리다 서버에 연결

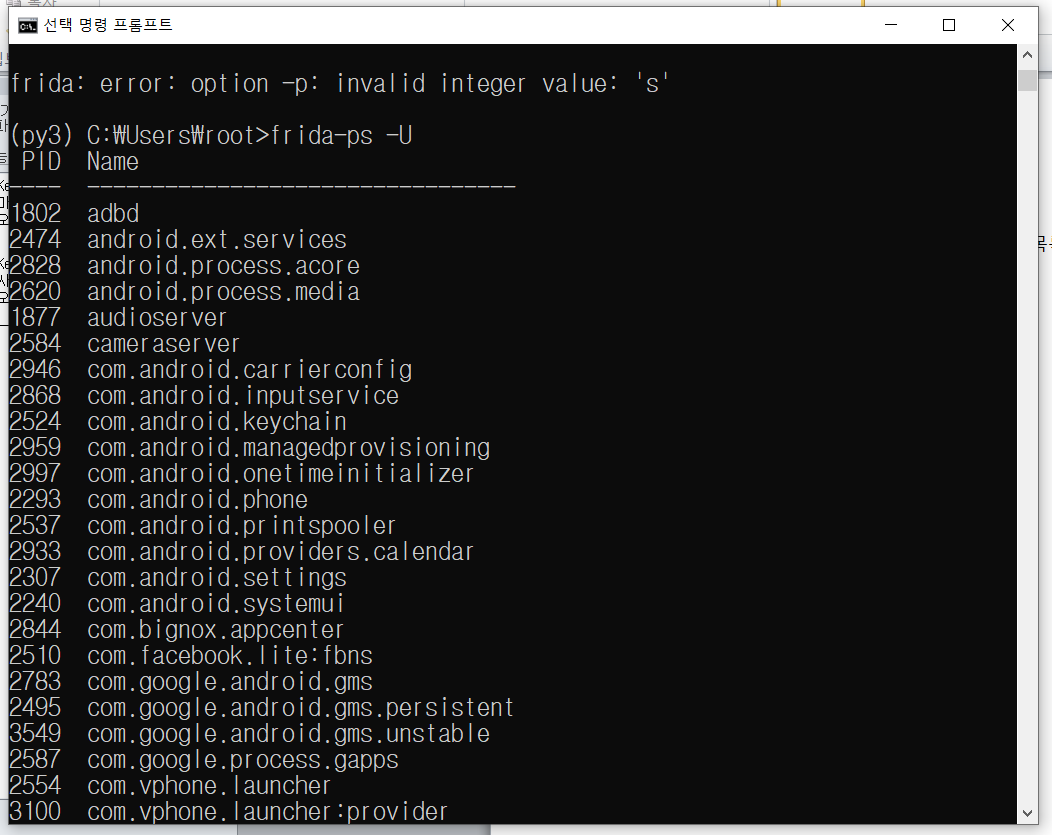
H : Host의 원격 프리다 서버에 연결

a : 애플리케이션 리스트만 출력

i : 설치된 모든 애플리케이션 포함 출력

**frida-ps –U**

: 연결된 디바이스에서 실행중인 모든 프로세스 목록 출력



frida-ps –Ua

: USB로 연결된 디바이스에서 실행 중인 앱 목록

**frida-trace**

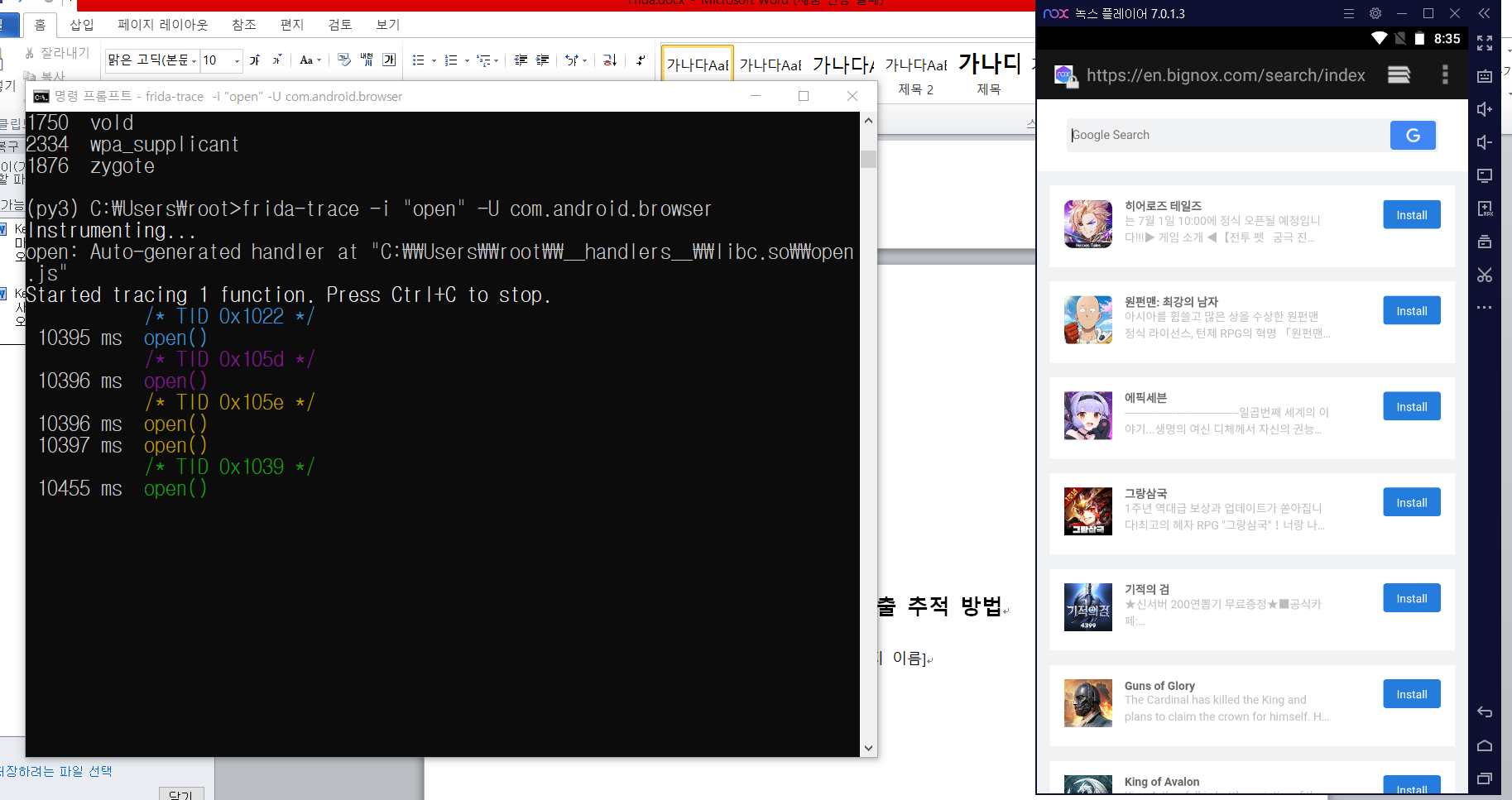
-I MODULE, --include-module=MODULE

: include module

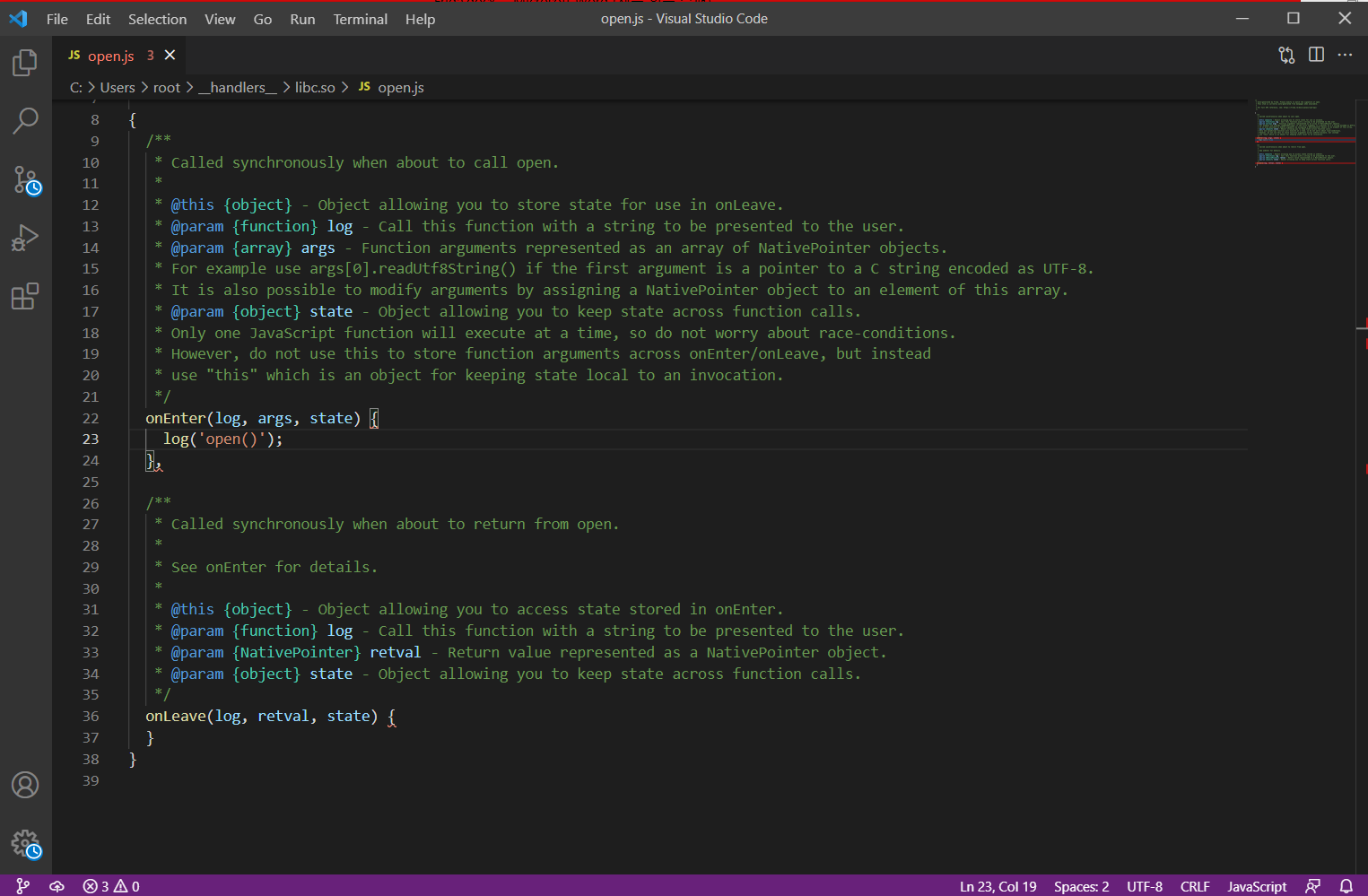
**frida-trace를 이용해 APIs 함수 호출 추적 방법**

frida-trace –i “검색하고 싶은 API명” –U [앱 패키지 이름]

ex) frida-trace –i “open” –U com.android.chrome

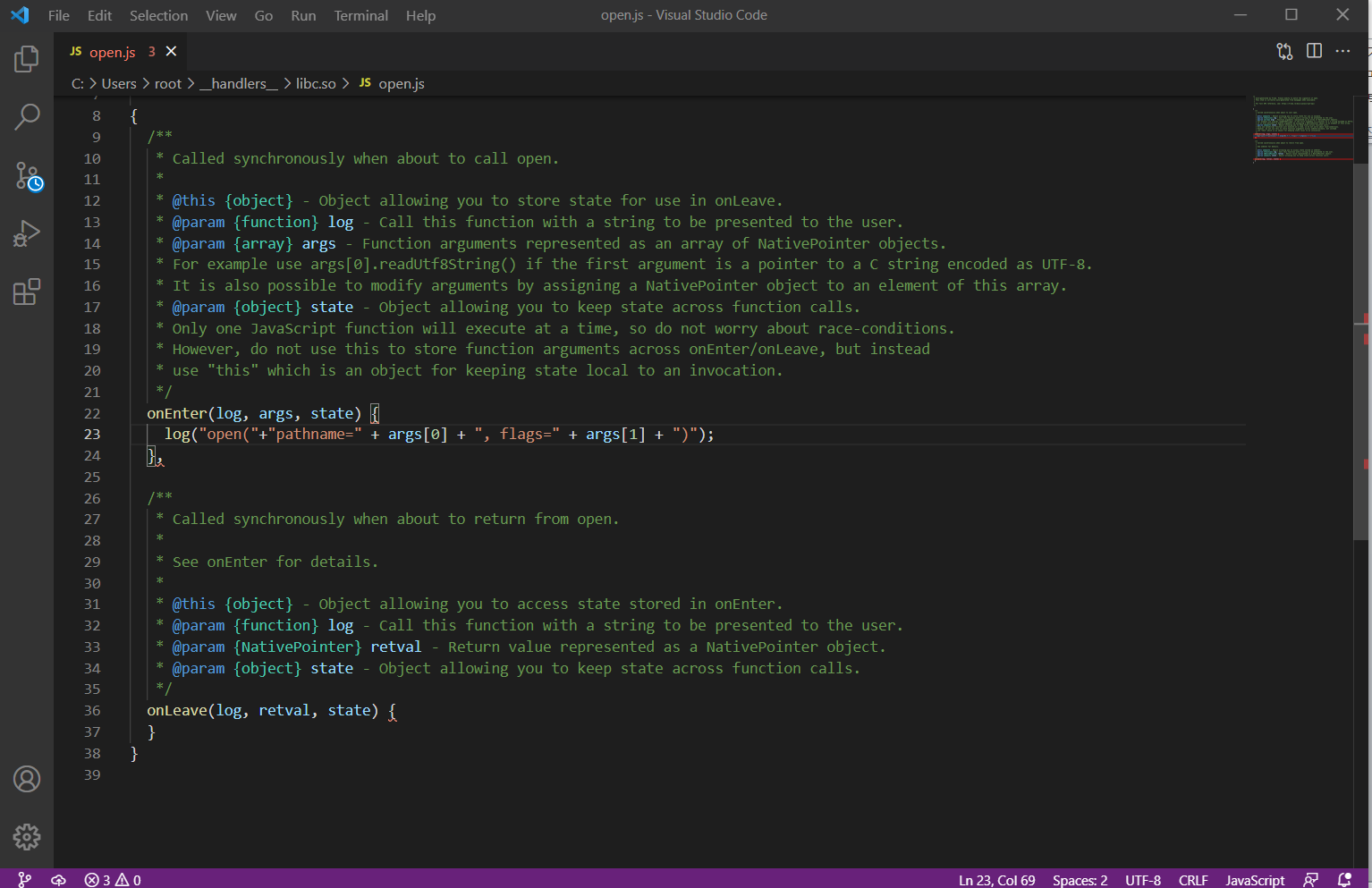


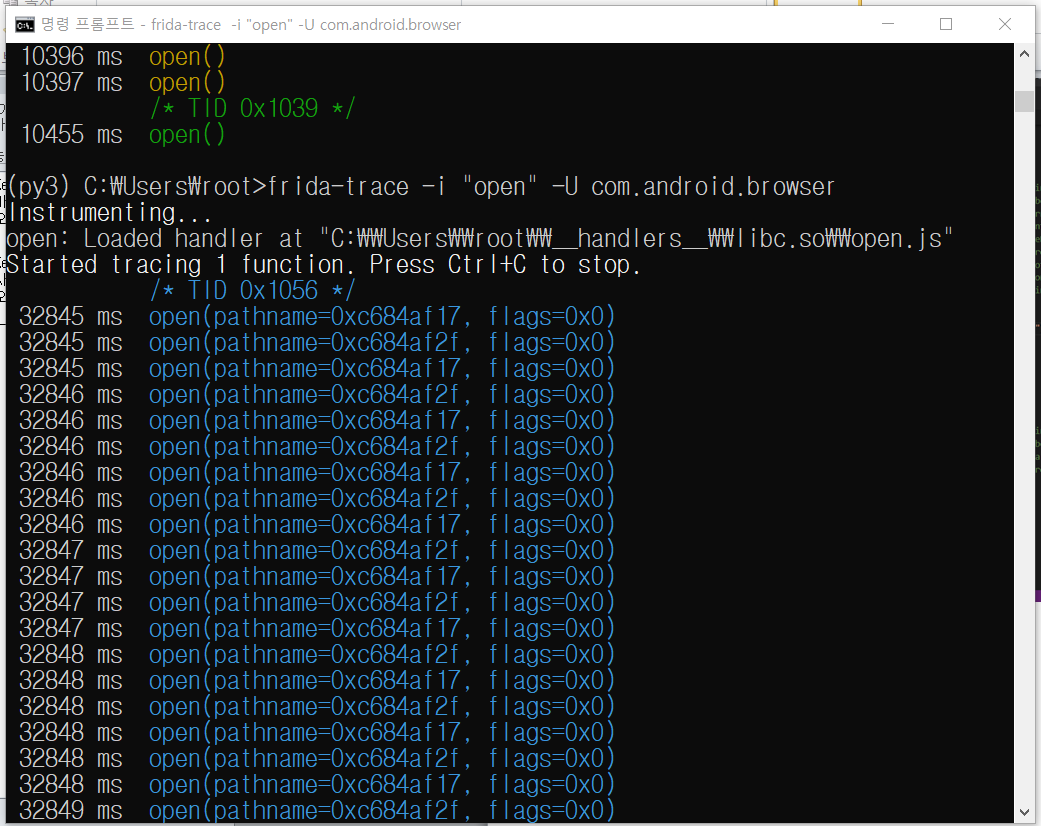
(변경 전)

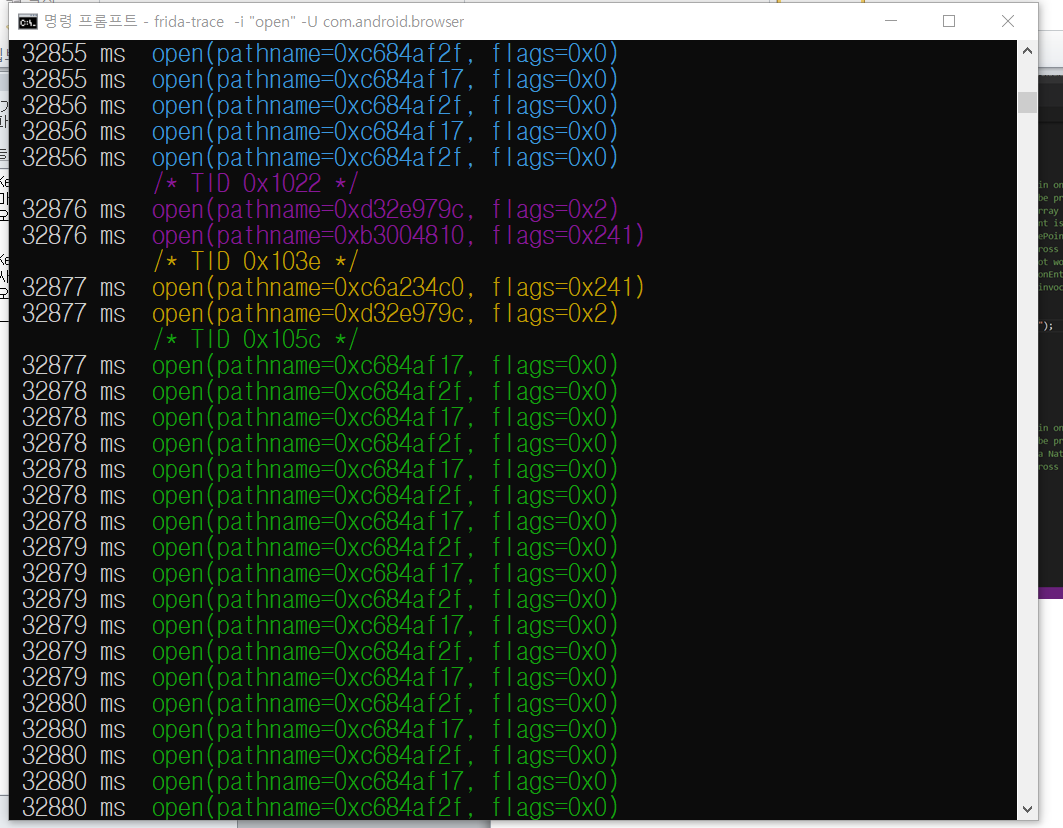


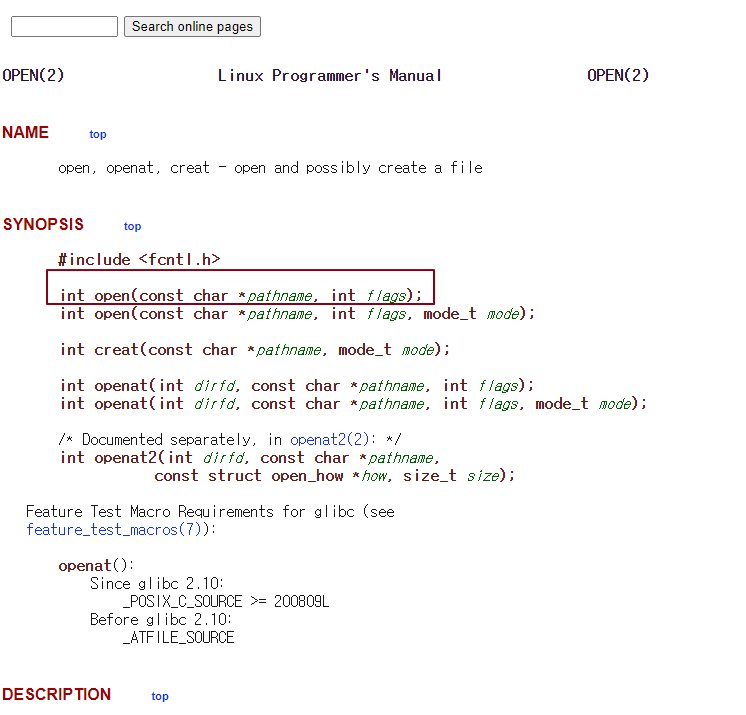
onEnter 부분에서 소스코드를 수정하여 인자로 전달되는 값 확인이 가능

(변경 후)

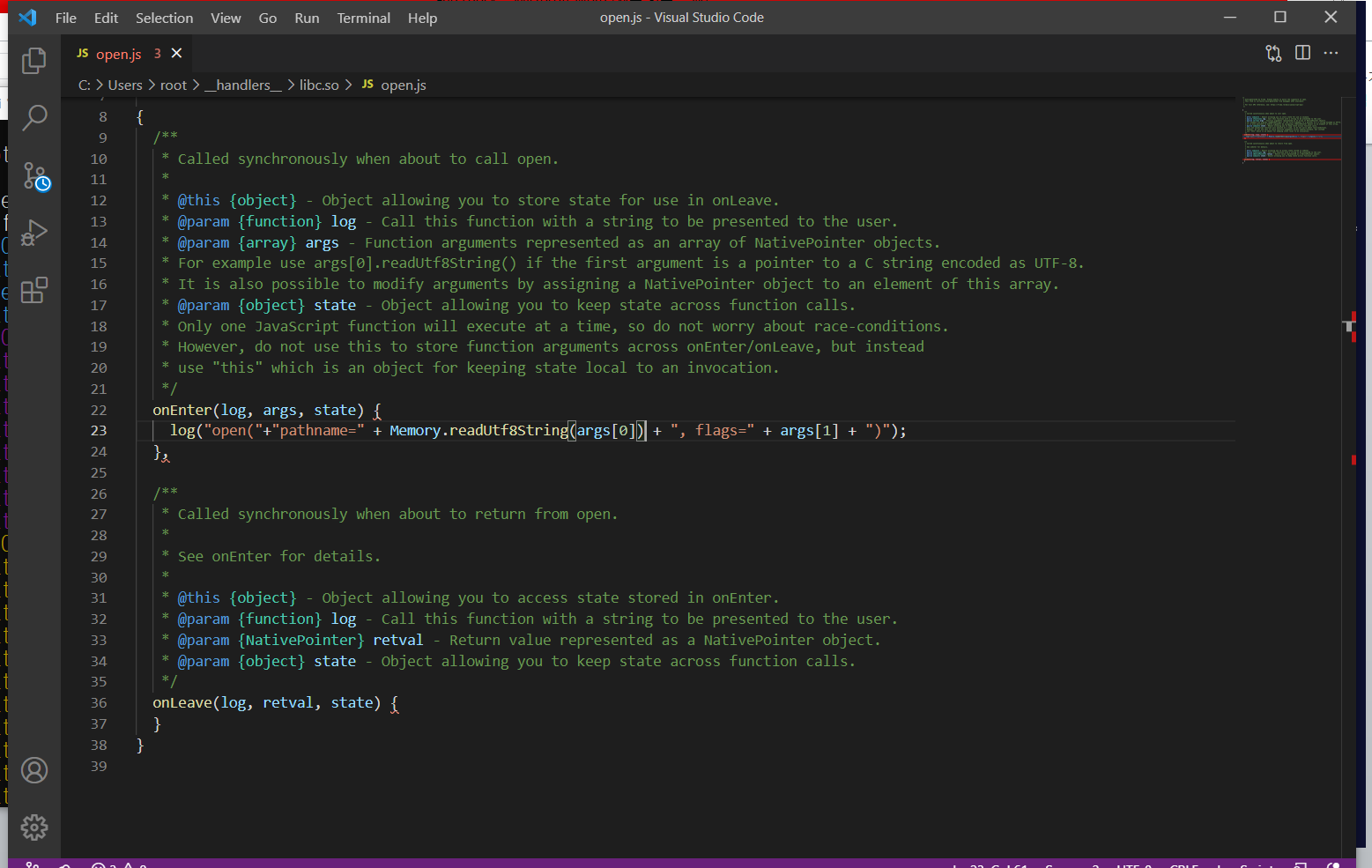


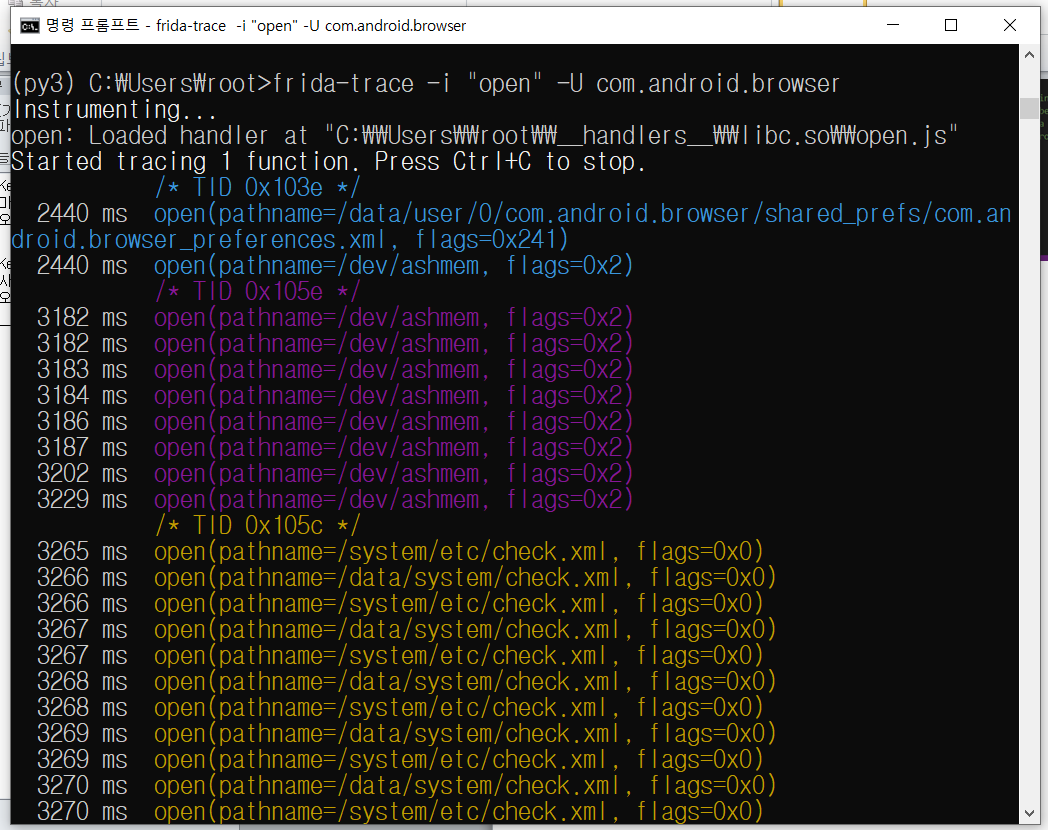






open 함수의 인자 값 확인 시, 첫 번째 전달되는 인자가 pathname 임을 알 수 있었음





onEnter 부분에서 frida API 함수(Memory.readUtf8String)를 이용해 소스코드를 수정해서 pathname 주소 값을 불러와 텍스트로 찍어 pathname을 구할 수 있음

이런 방식을 잘 사용한다면 앱 내 함수 역추적이 손쉽게 가능함