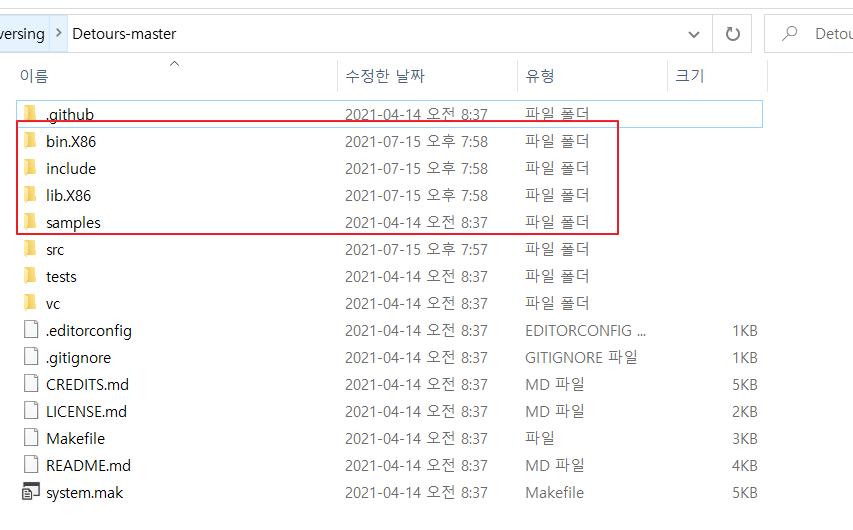
Detours는 Microsoft사에서 공개한 매우 강력한 Windows API 후킹 라이브러리이다.

컴파일을 하게되면 bin.X86, lib.X86 파일이 생기는 것을 확인할 수 있다.

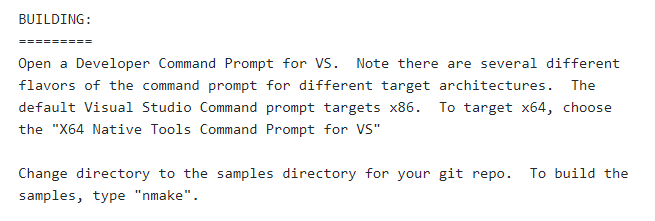
디렉토리별 설명은 아래와 같다.

bin.X86 : samples에 있는 소스코드들이 컴파일 되어서 exe, dll파일로 저장되는 디렉터리이다. 앞으로 예제에서 사용하게 될 setdll.exe 파일도 해당 경로에 존재한다.

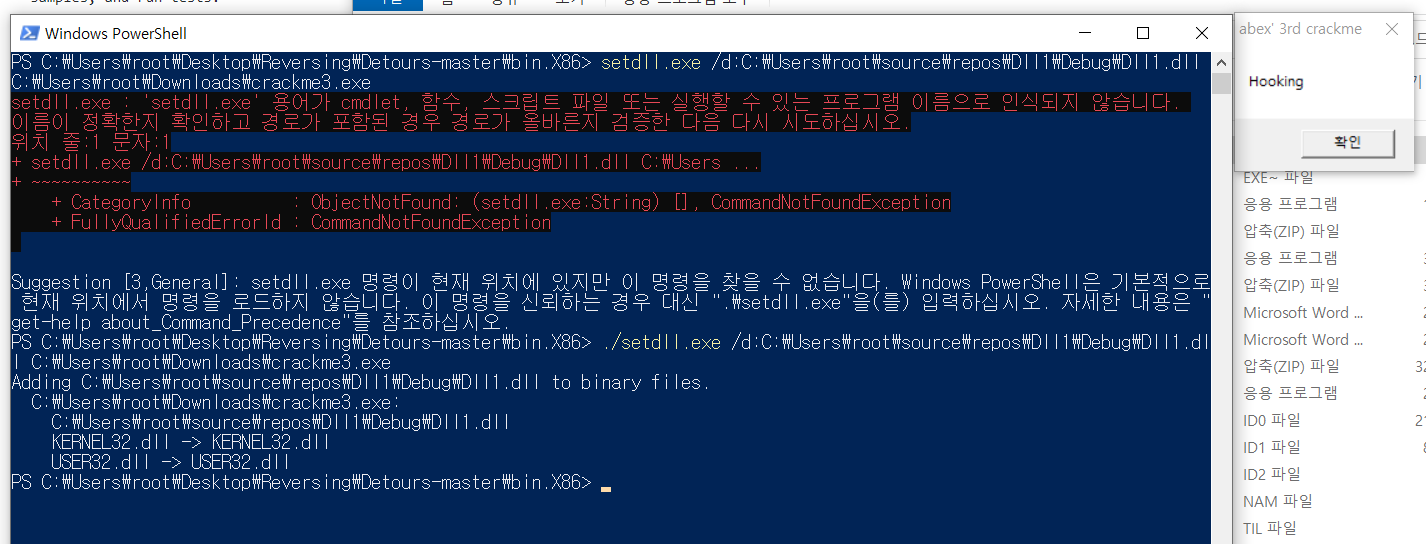
include : 내가 직접 dll 코드를 작성하게 될 때 사용해야 할 헤더파일이 존재하는 디렉터리이다.

lib.X86 : 내가 직접 dll 코드를 작성하게 될 때 사용해야 할 라이브러리 파일이 존재하는 디렉터리이다.

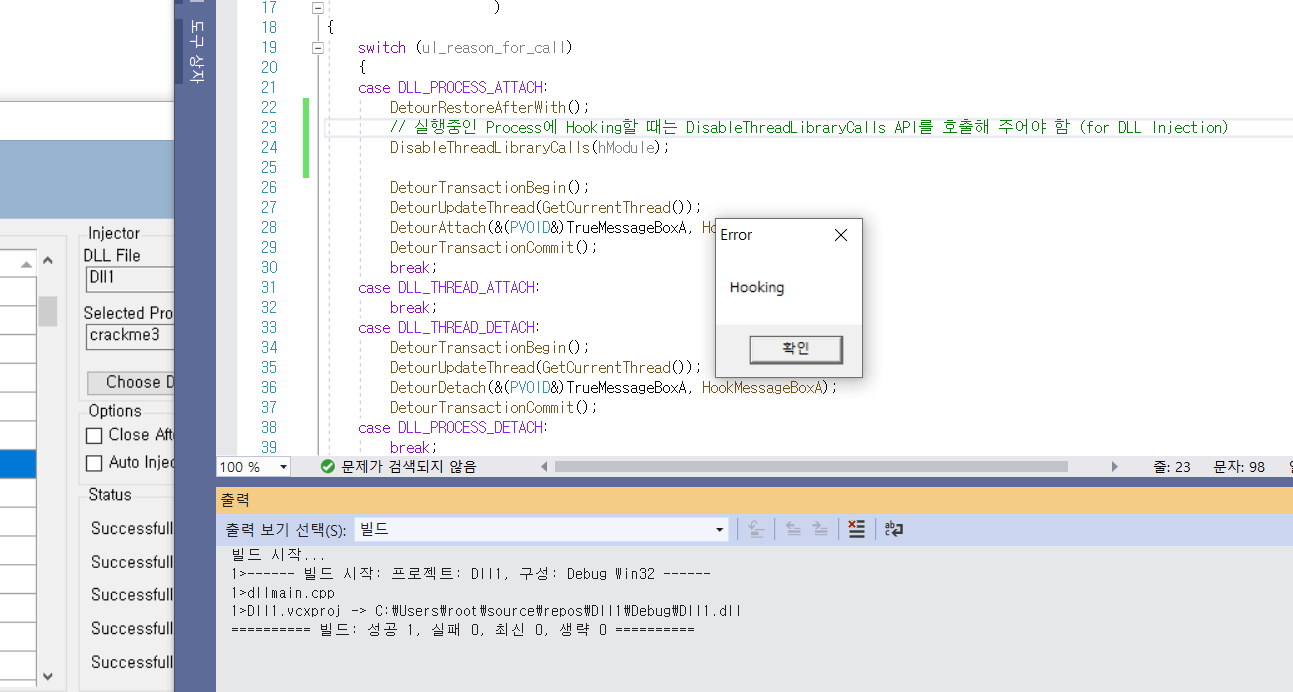
samples : Detours Library에 적응하기 위해 테스트해볼 수 있는 예제 코드들이 존재하는 디렉터리이다. setdll.exe와 같이 실제 사용하기 좋은 소스코드도 많이 존재하는 것 같다. (공부필요…)



Detours X64 Build 방법



setdll.exe를 이용한 케이스 (원본 바이너리가 패치됨)



DLL Injection을 이용한 케이스 (원본 바이너리 실행 시 후킹)