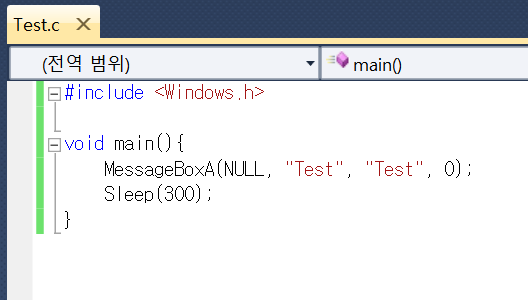
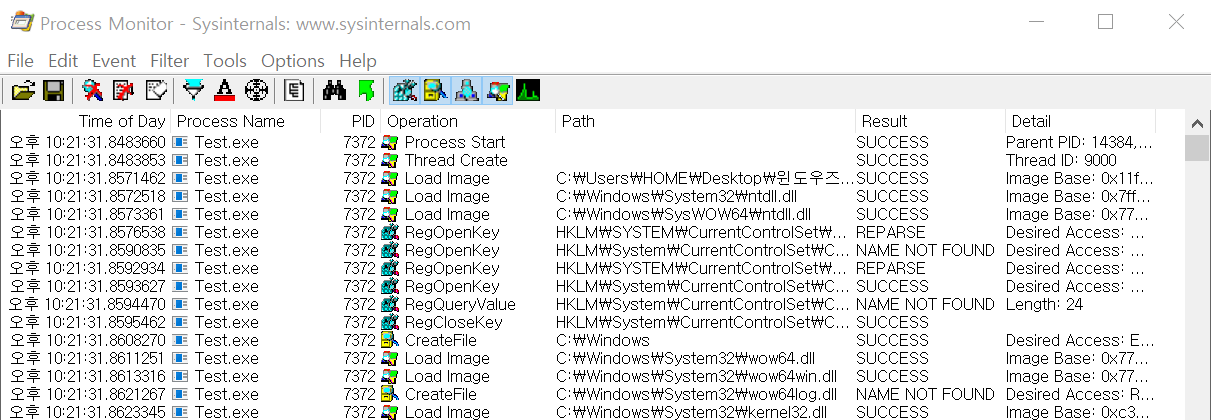
실습보고서3 2016111566 이나경

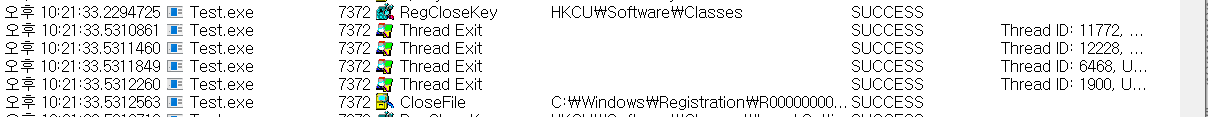
실습 1

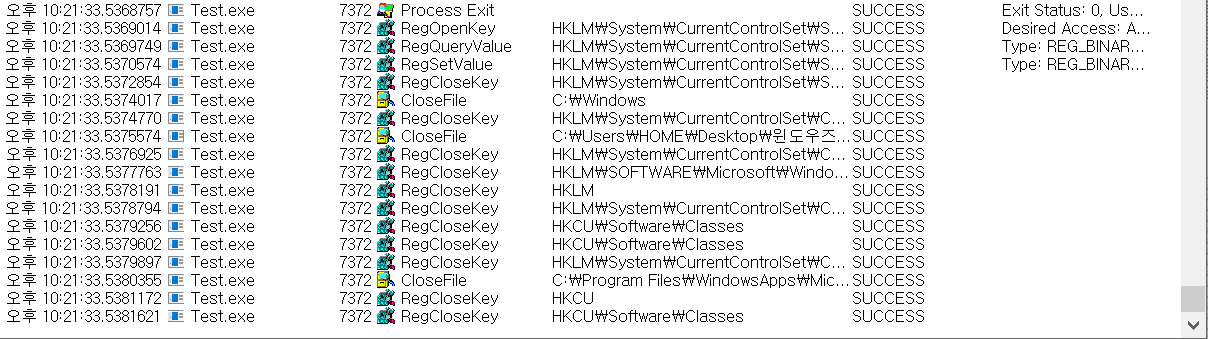
다음 프로그램을 작성하여 실행한 후 Procmon, Process Explorer, Decency Walker, Regshot 등을 통해 얻을 수 있는 모든 정보를 정리하라



위의 프로그램을 작성하여 실행한 후 Process Monitor로 분석하였다.

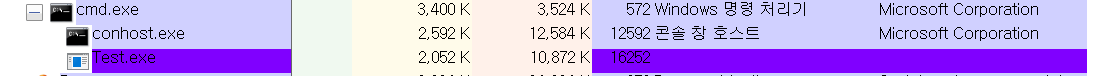


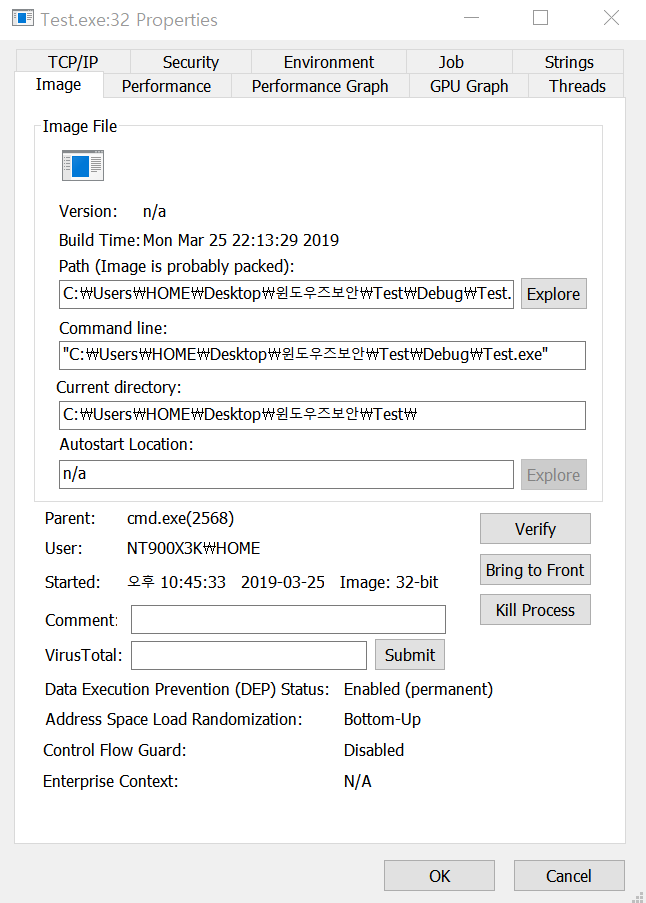
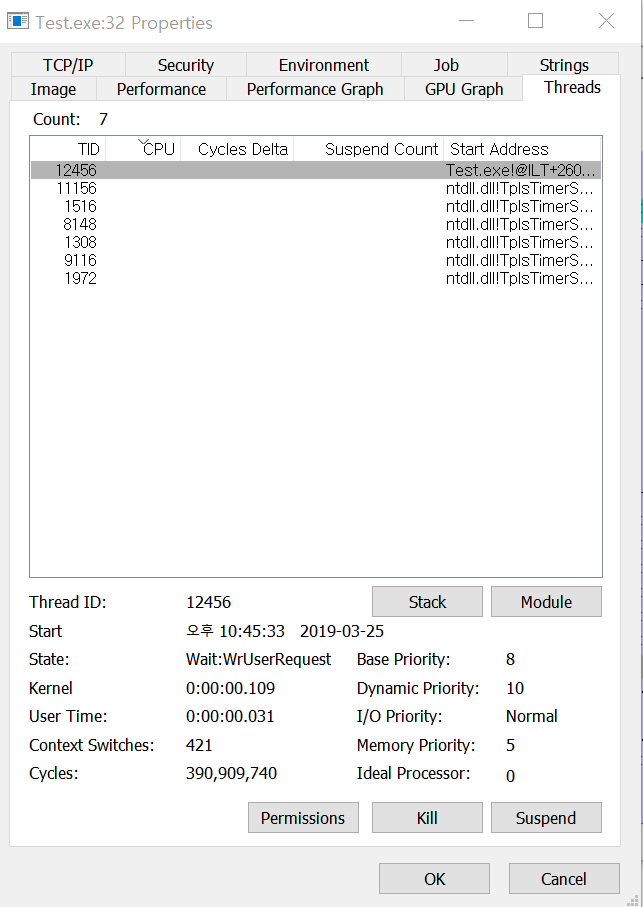


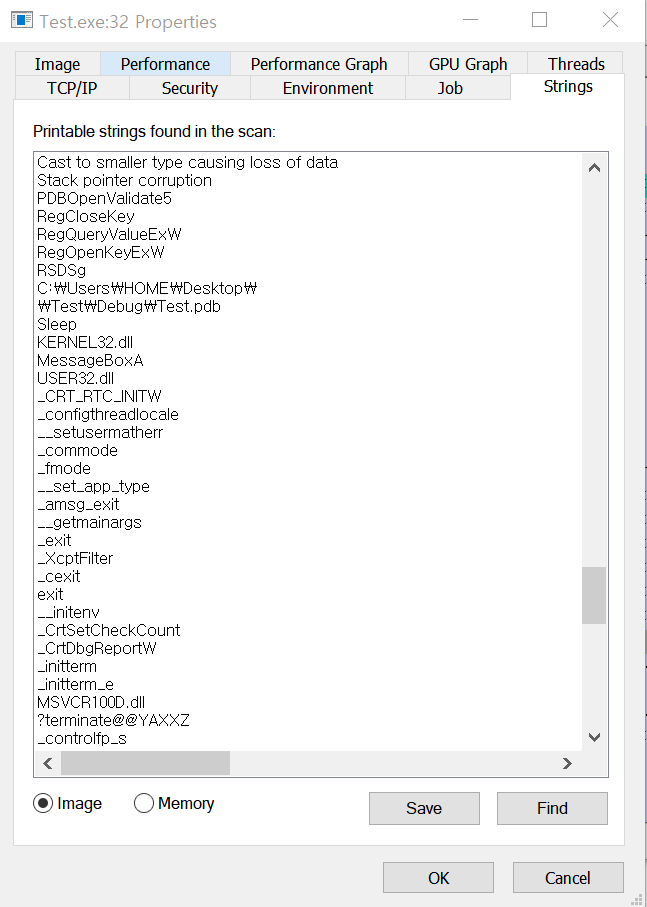


CreateFile, Thread Create, Load Image, CreateFileMapping, RegOpenKey, RegQueryValue 등의 행위를 감지할 수 있었다.

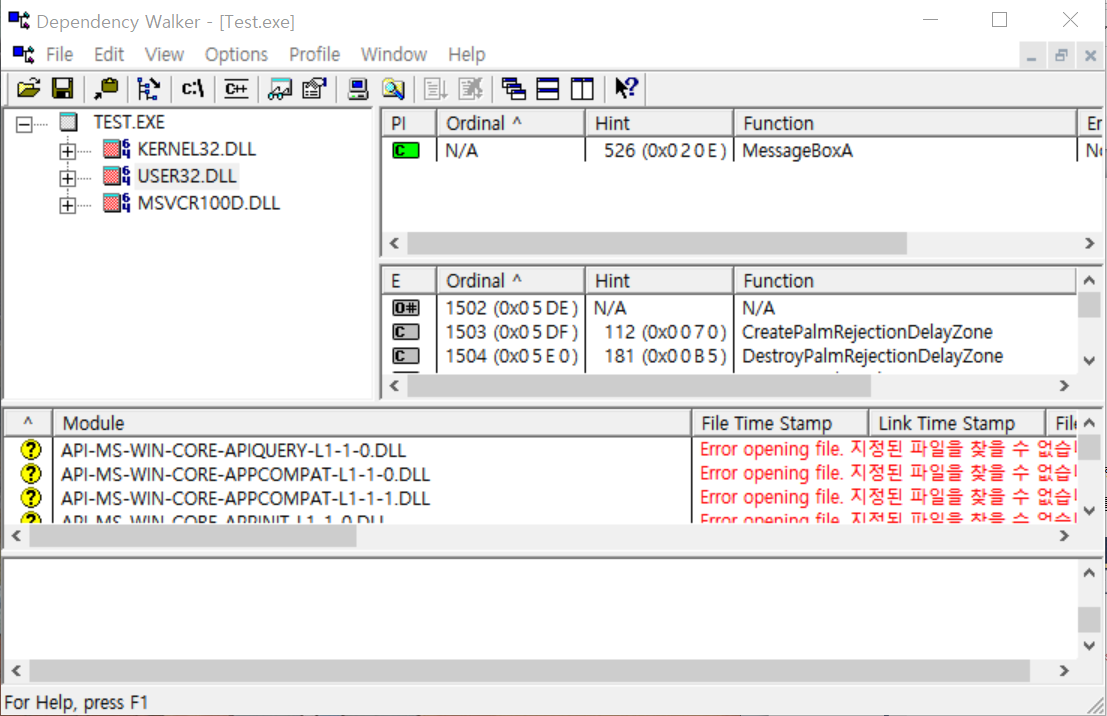
Process Explorer를 사용하여 분석한 결과



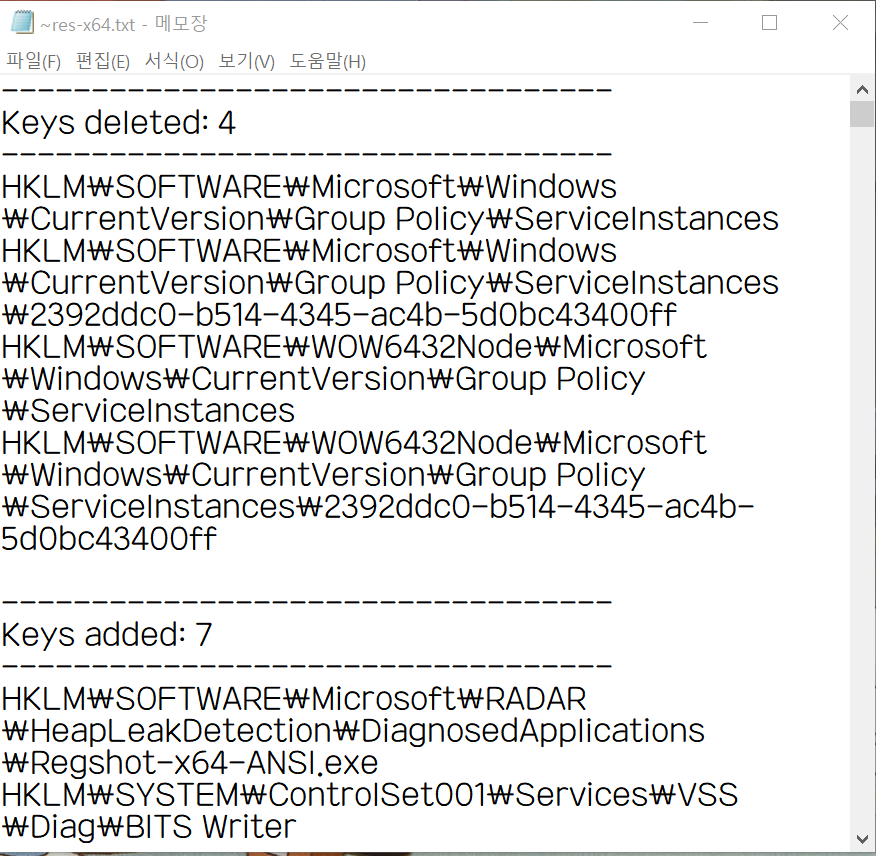
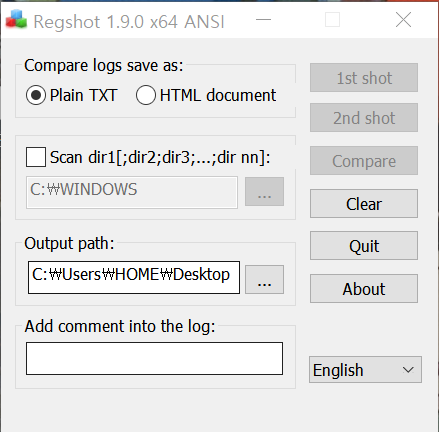
 



Test.exe는 cmd.exe와 함께 돌아가는 것을 확인하였고 ntdll.dll모듈을 링킹하고 있는 것을 알 수 있었다. 또한 Strings 정보를 확인한 결과 MessageBoxA함수를 사용하고 있는 것을 알 수 있다.



Dependency walker로 확인한 결과 kernel32.dll, user32.dll, msvcr100d.dll을 포함하는 것을 알 수 있고 user32.dll에서 MessageBoxA 함수를 임포트하는 것을 확인하였다.



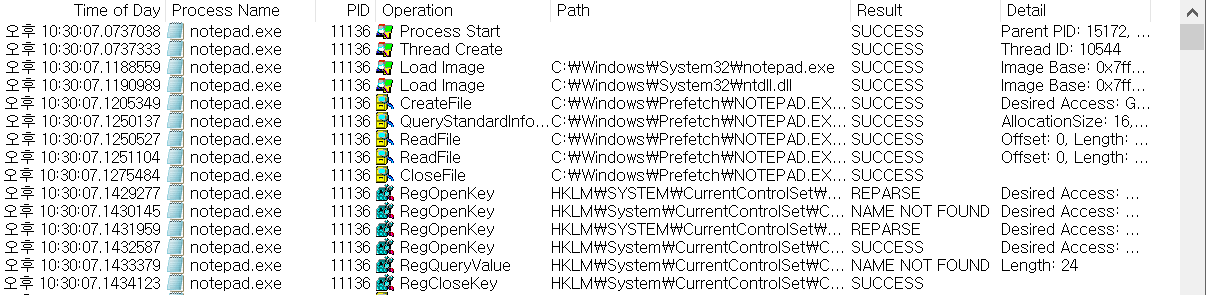
Regshot으로 프로그램 실행 전후를 비교한 결과 key가 4개 삭제되었고 7개가 추가되었다.

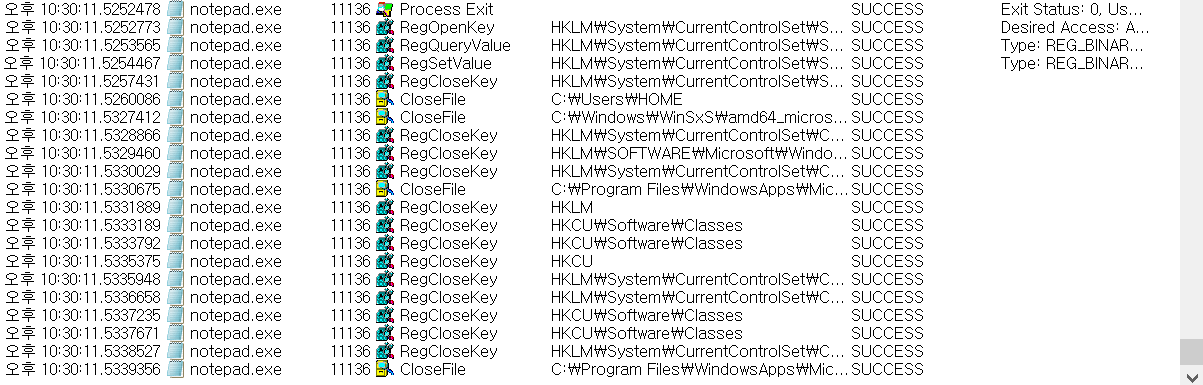
Value는 3개가 삭제되고 6개가 추가되었다.

실습 2

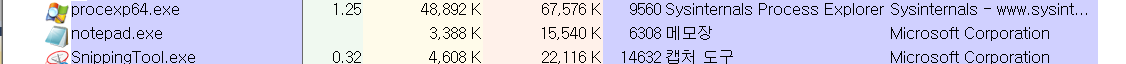
메모장 프로그램을 실행 한 후 Procmon, Process Explorer, Decency Walker, Regshot 등을 통해 얻을 수 있는 모든 정보를 정리하라

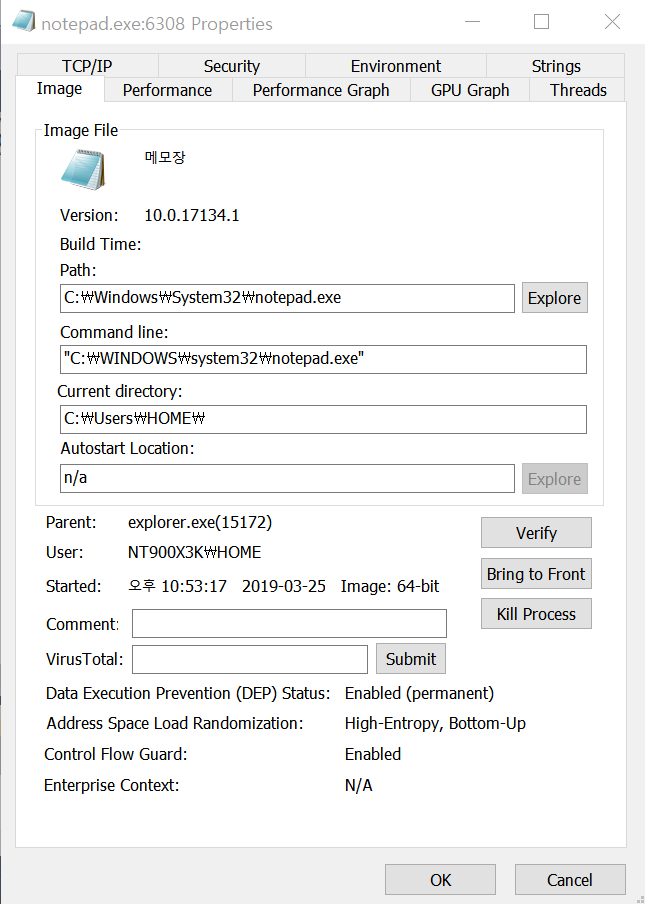
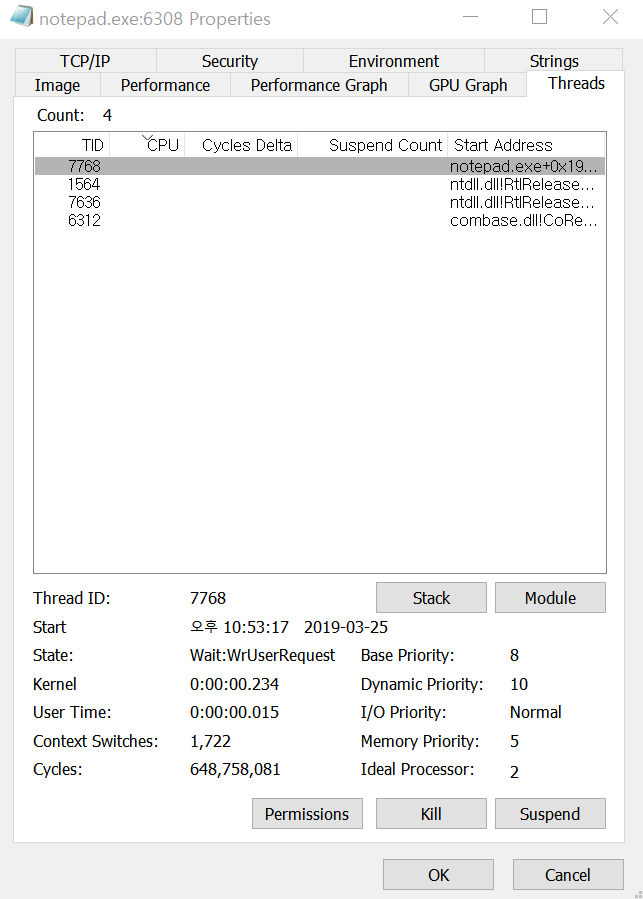
메모장 프로그램을 실행한 후 Process Monitor로 분석하였다.

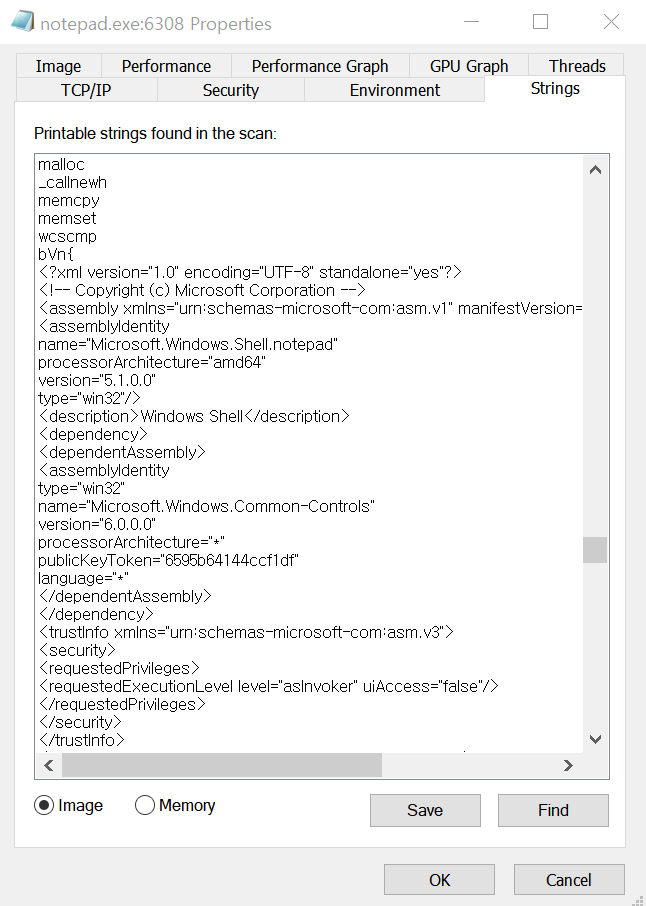




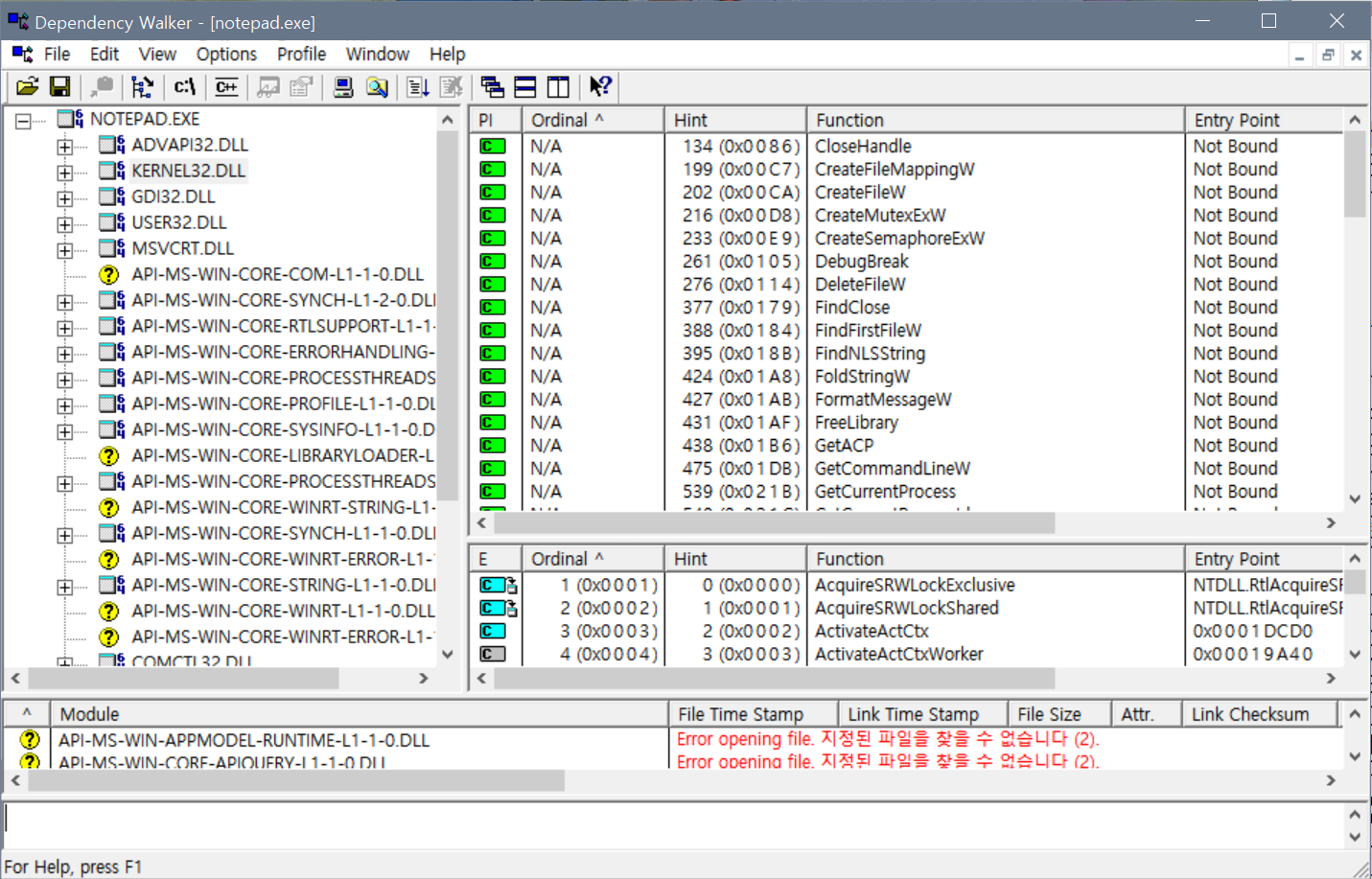
Thread Create, CreateFile, ReadFile, RegOpenKey, CreateFileMapping, RegQueryValue 등의 행위를 관찰할 수 있었다.



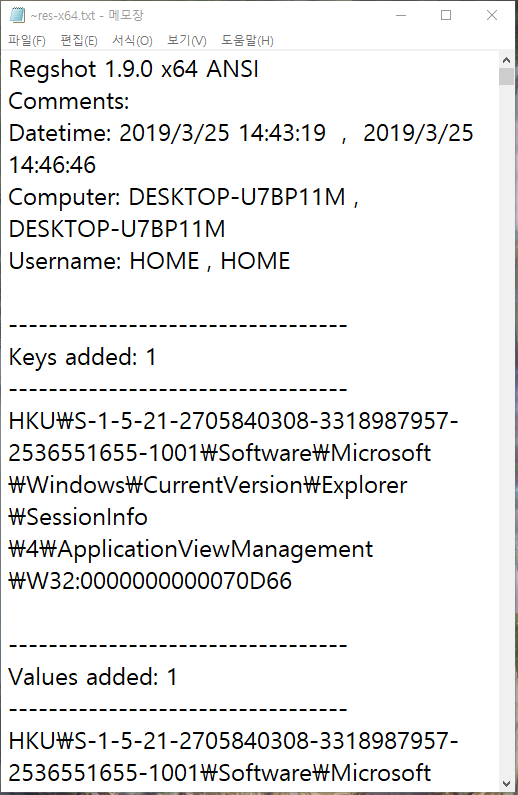
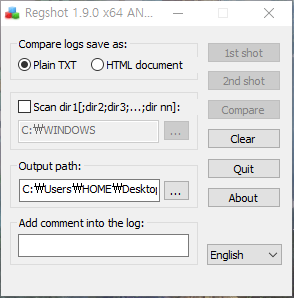
 



notepad.exe는 ntdll.dll, combase.dll모듈을 링킹하고 있는 것을 알 수 있었다.



Dependency walkwe로 확인한 결과 Notepad.exe가 kernel32.dll, user32.dll 등을 사용하고 있는 것을 알 수 있고 CreateFileMappingW, CreateFileW, CreateMutexExW, DeleteFileW, FindFirstFileW 등의 함수를 임포트하는 것을 확인할 수 있다.



Regshot으로 메모장 실행 전후를 비교한 결과 key가 1개 추가되었고 value 1개가 추가되었다.