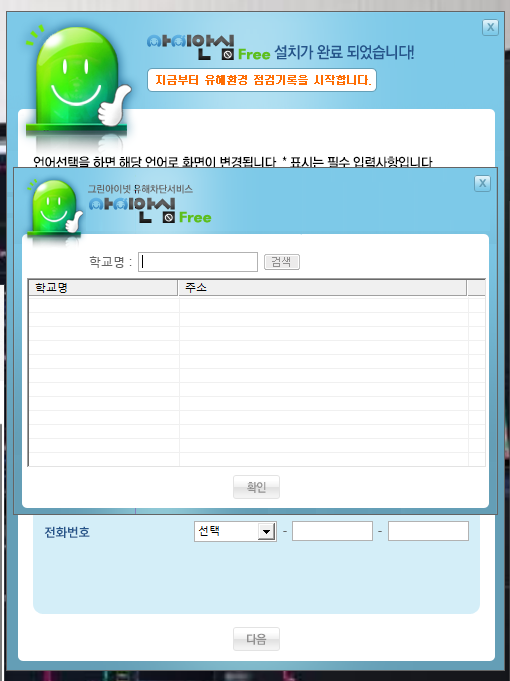
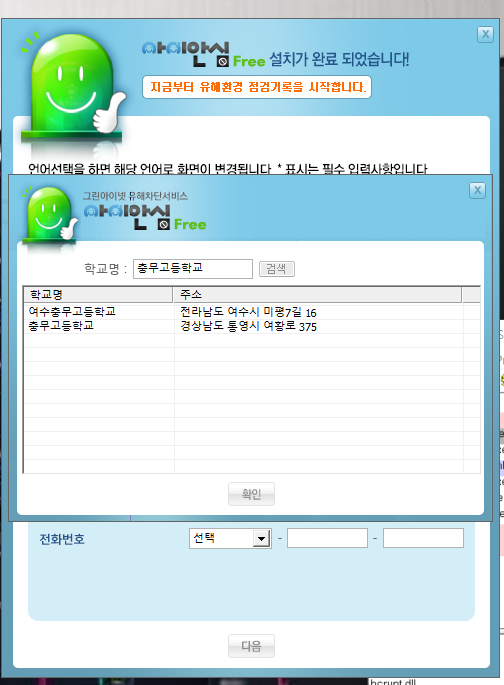
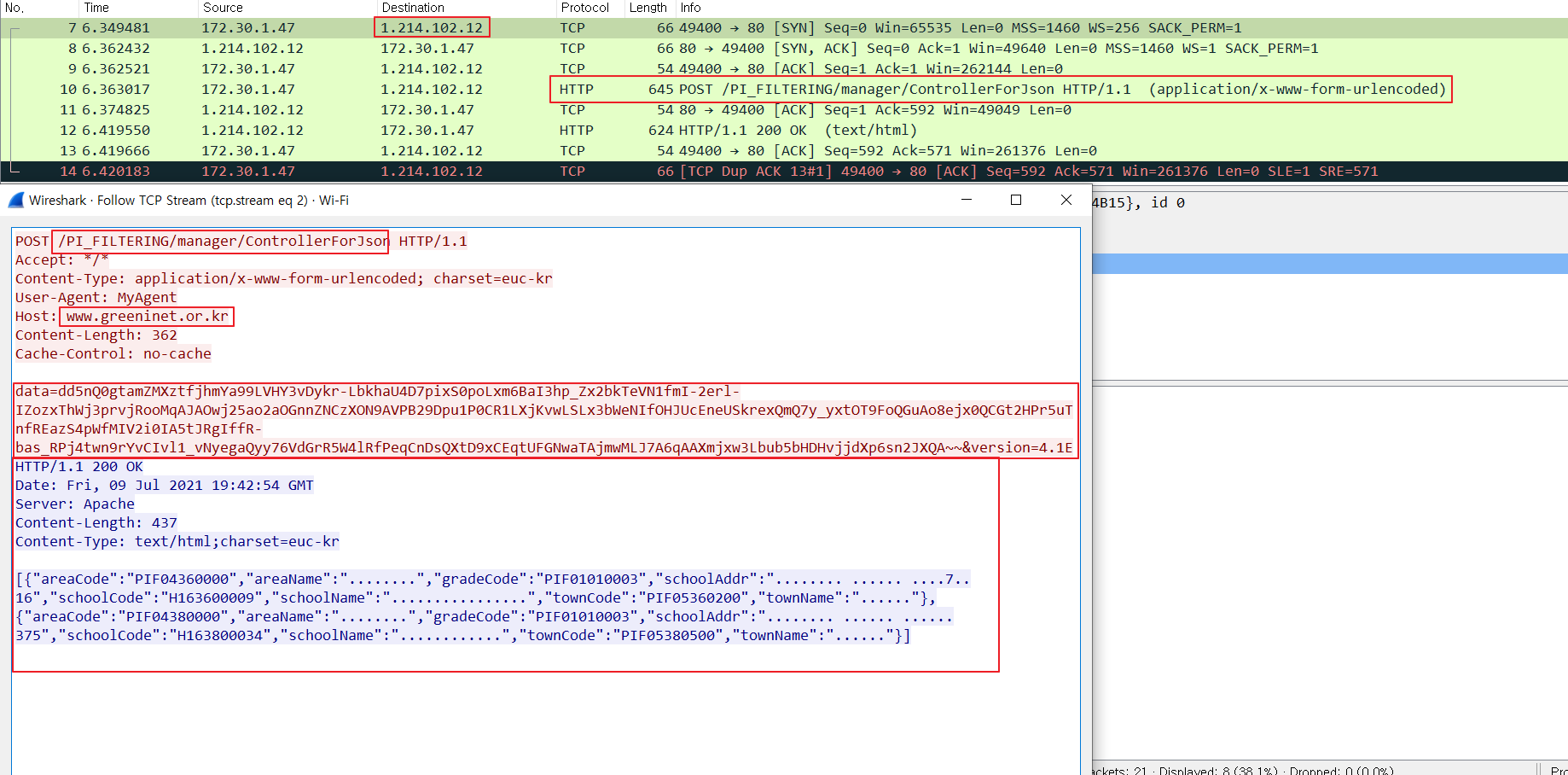


**Wireshark**

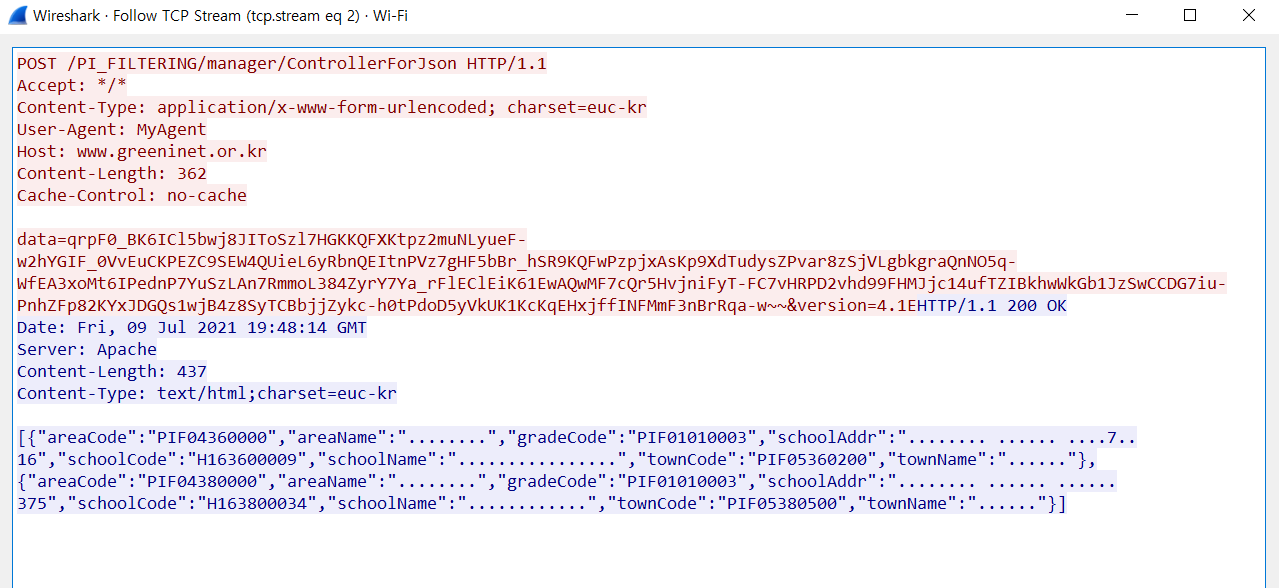




**1**

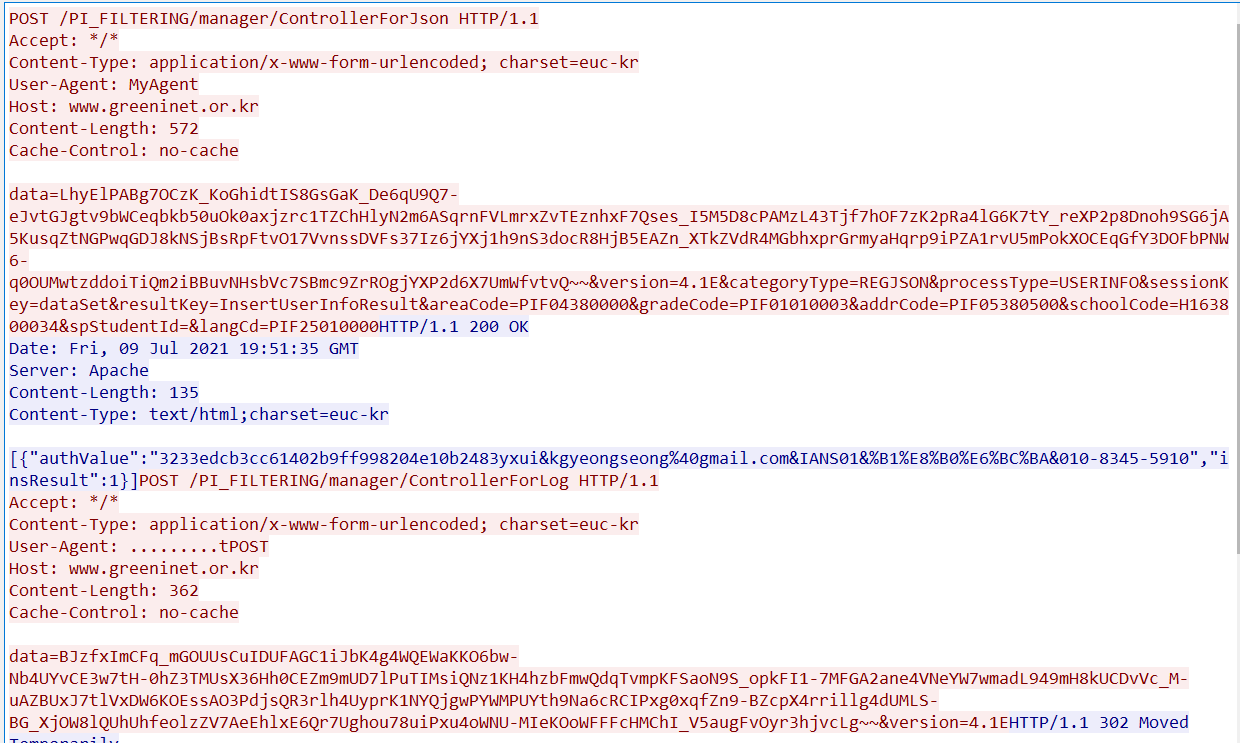


**2**



1과 2의 request data값이 다름. request data 암호화되고 서버측에서 복호화 하는 듯

학부모 정보 입력 후 [다음] 버튼 눌렀을 때

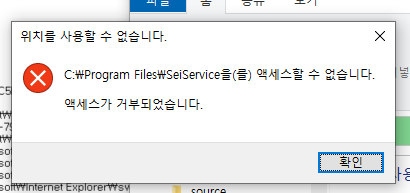




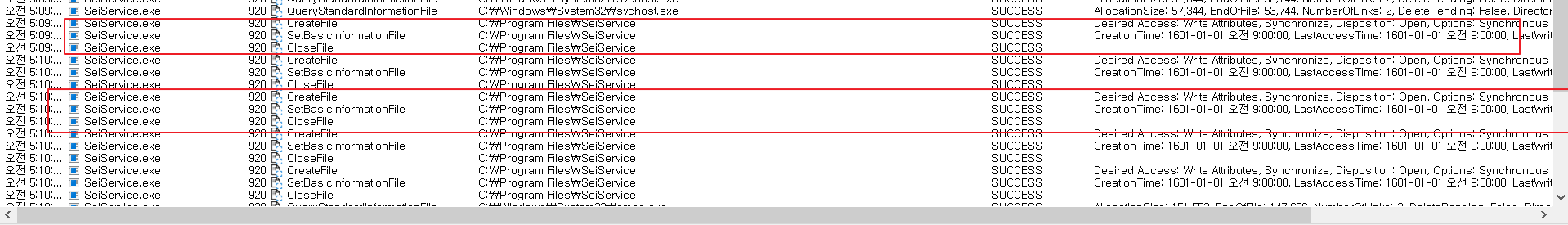
관리자 비밀번호: 123456

아이안심 특징

* 설치하면 자동으로 실행되고 해당 경로에서 폴더를 찾을 수 없으며
* 해당 폴더에 액세스 할 수 없다고 함

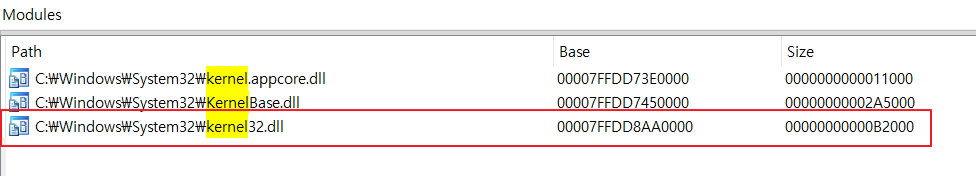


**폴더 숨기고 액세스 할 수 없게 하는 의심 루틴**

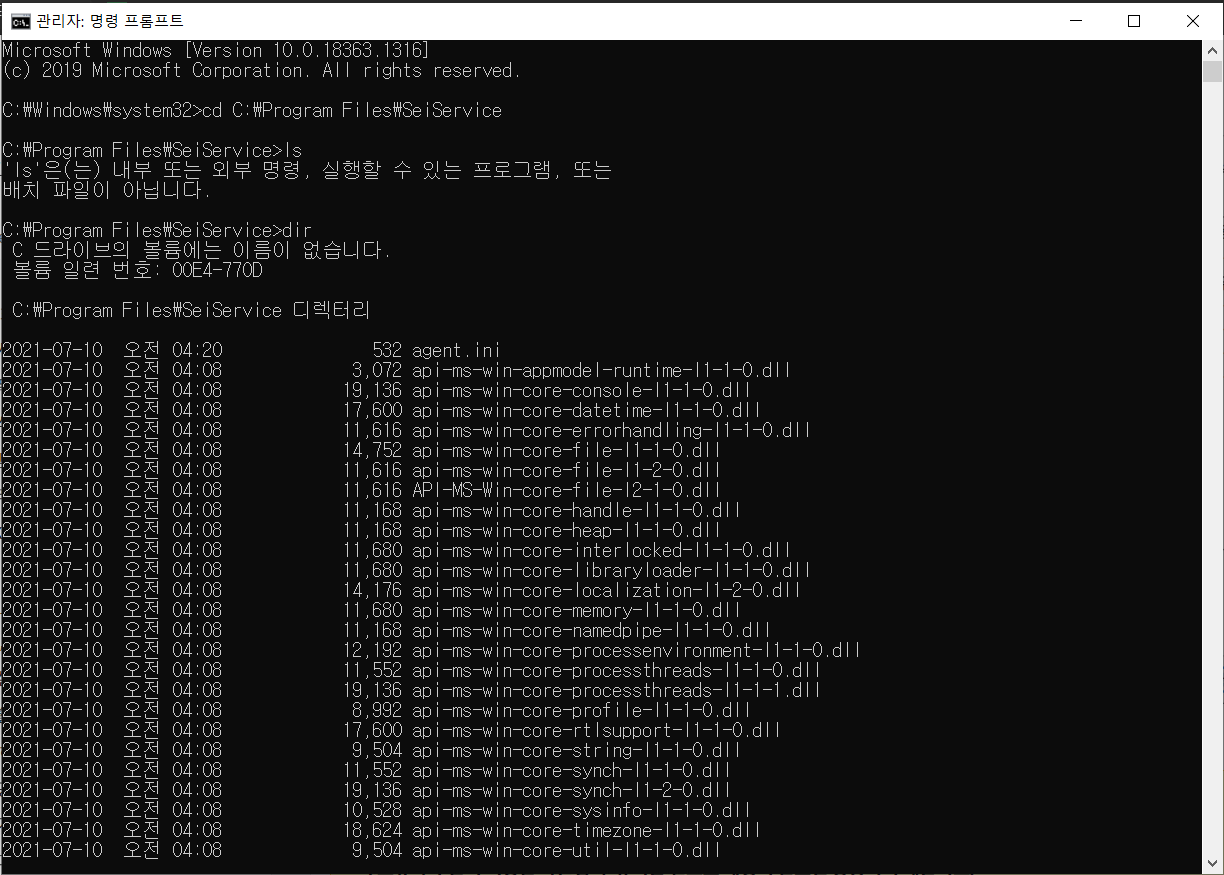


* CreateFile
* SetBasicInformationFile
* CloseFile

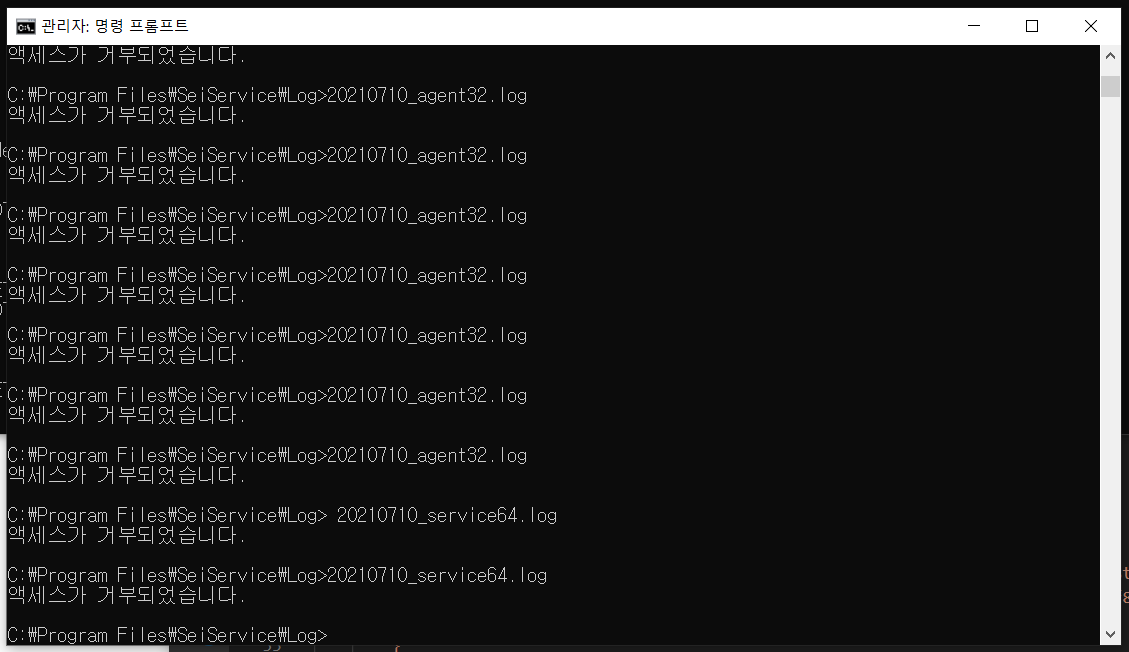
해야할 일 : 해당 함수들 후킹해서 확인해볼 것

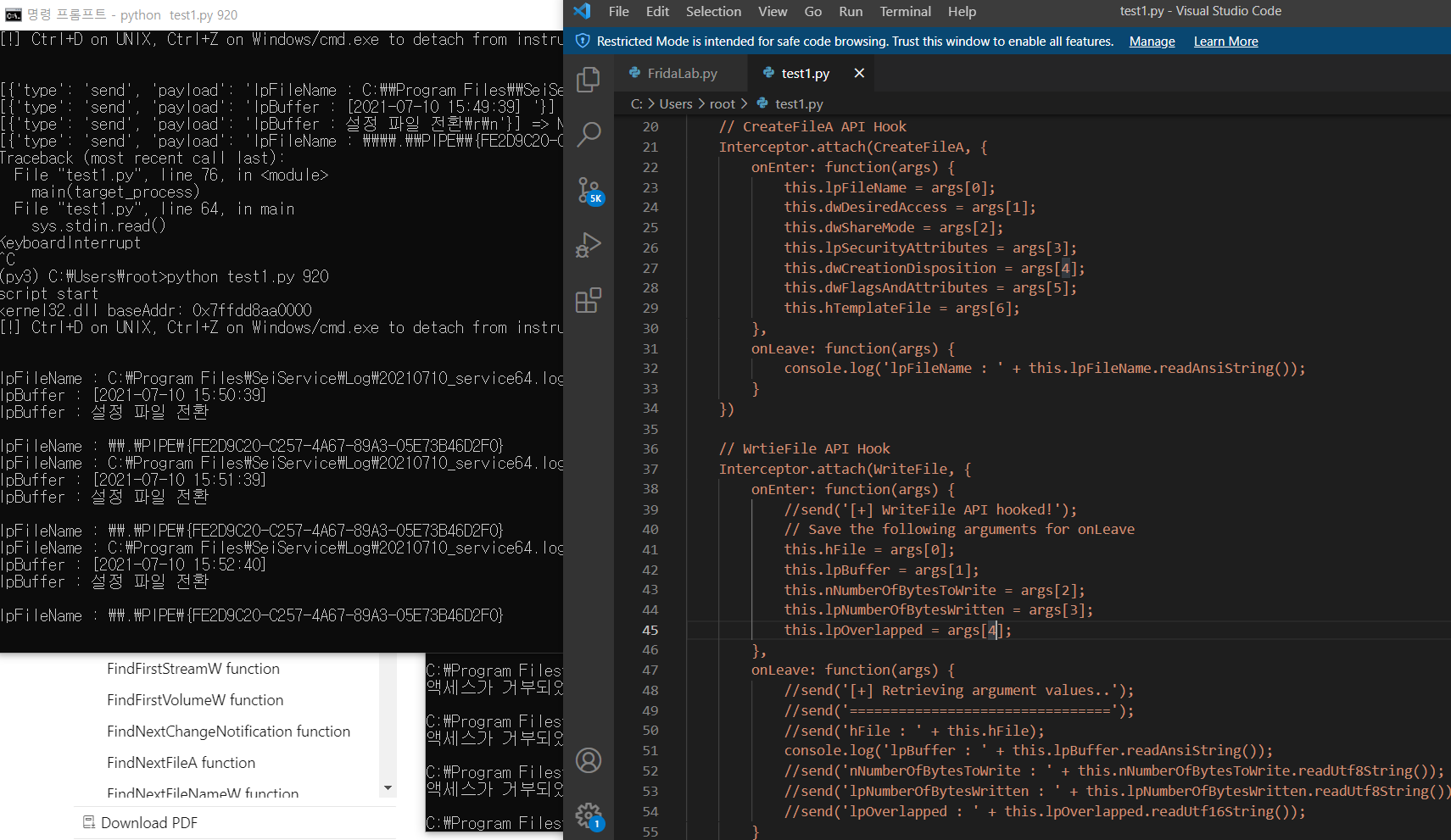


**해결1: CMD 관리자 권한으로 폴더 액세스 가능**



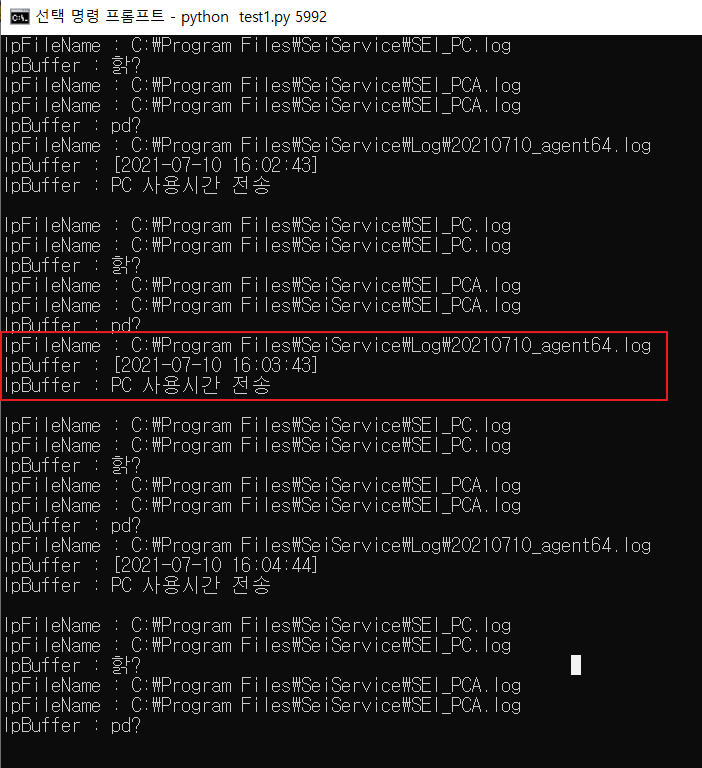
**Log 파일 분석**



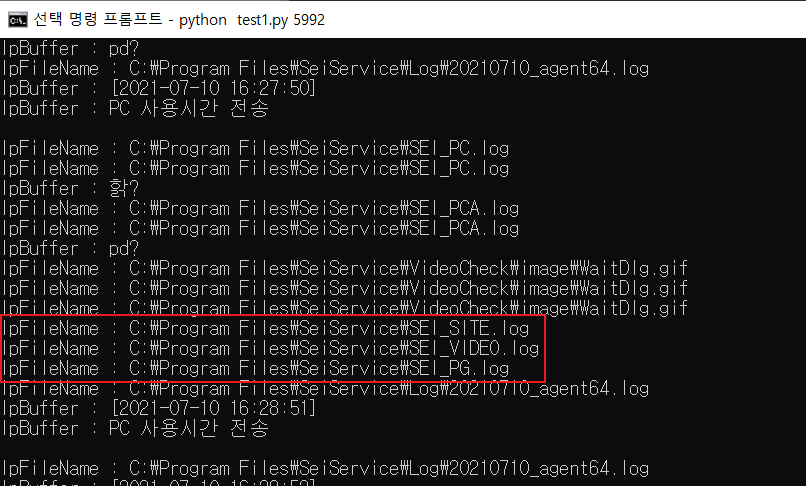


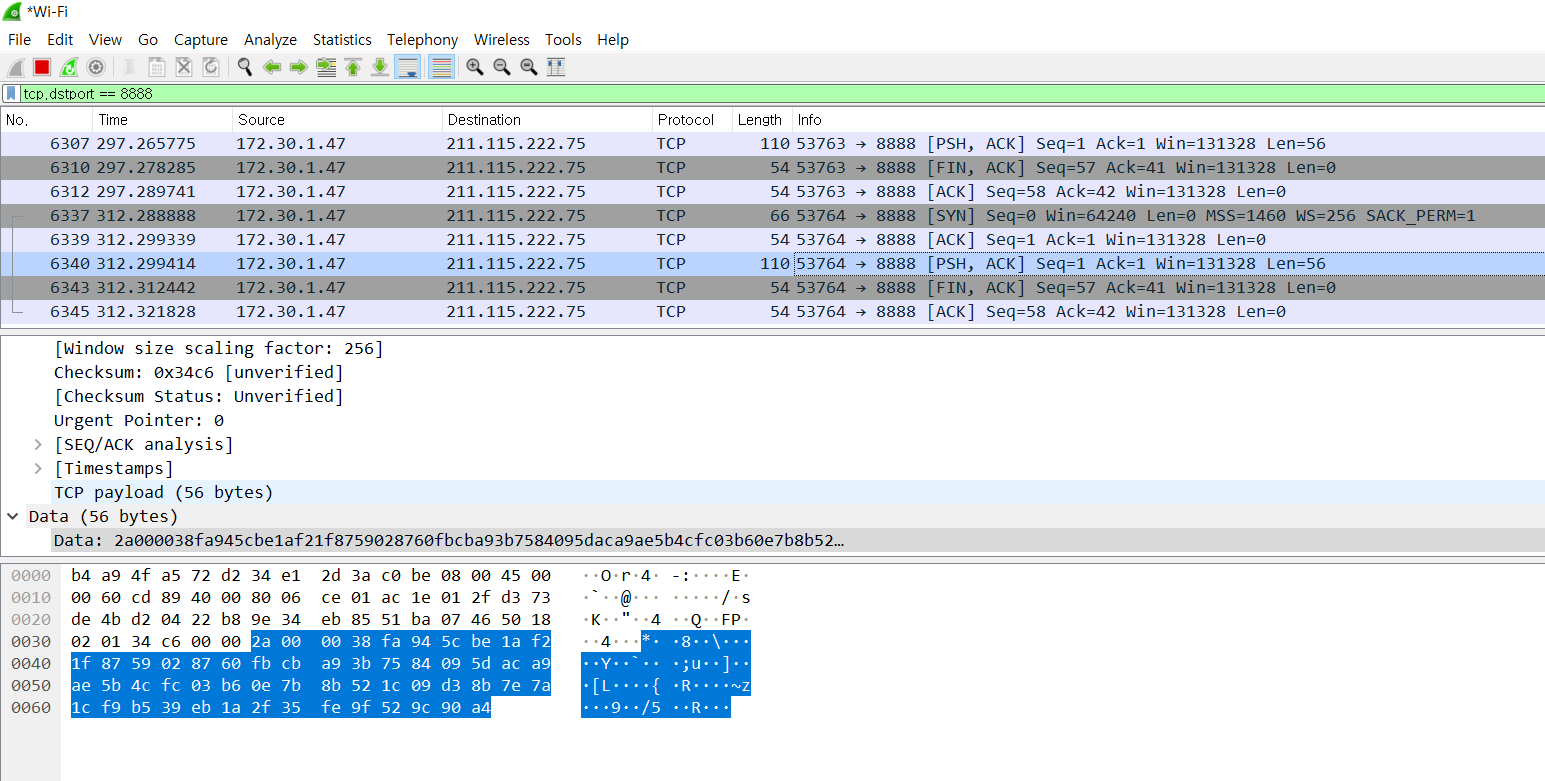
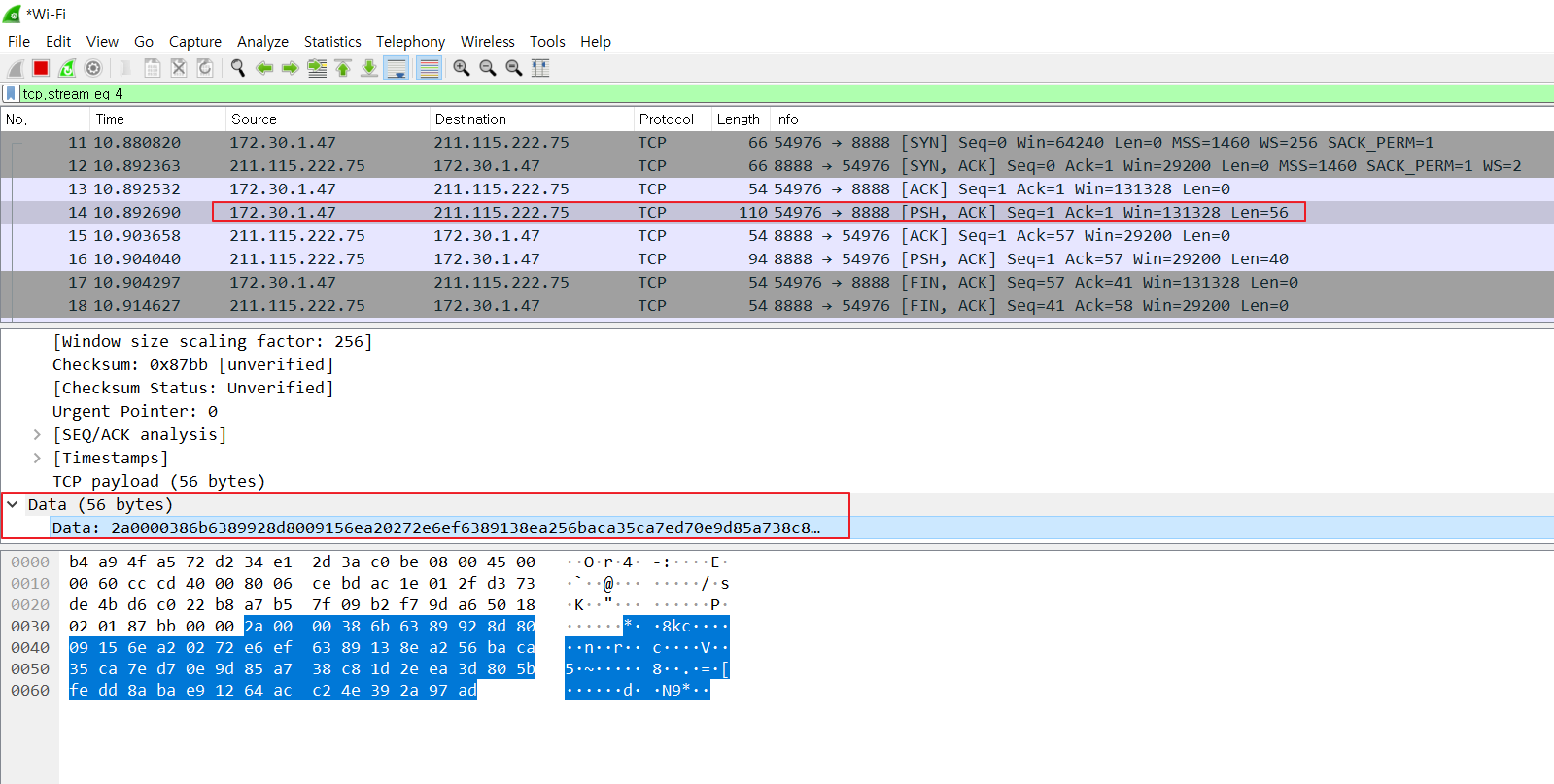
대상: SeiService.exe의 CreateFileA, WriteFile 후킹

대상: SeiAgent.exe의 CreateFileA, WriteFile 후킹



보호자 모드 실행 시





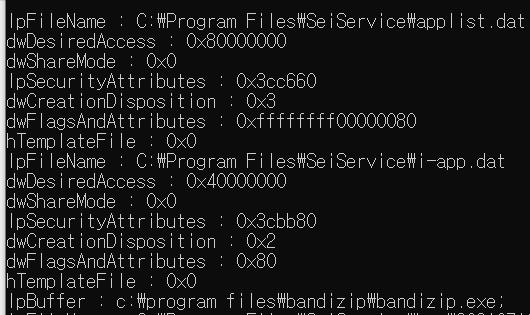
**지정 프로그램 차단 설정 후 어디에 쓰는지 확인**

차단 프로그램 설정



차단 프로그램 설정 해제





* CreateFileA
  + dwDesiredAccess
    - 0x80000000 (GENERIC\_READ)
    - 0x40000000 (GENERIC\_WRITE)

**파일 시스템 필터 드라이버로 액세스 거부한다면?**

* 커널 디버깅 해보기