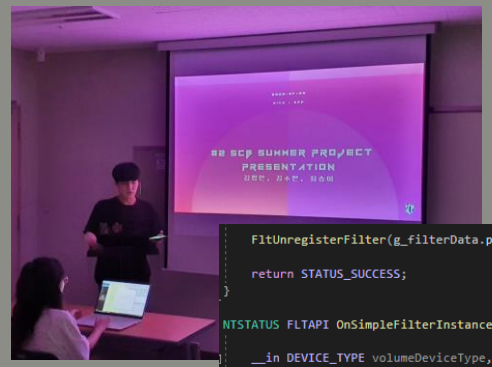
PERSONAL STUDY PRESENTATION

Contents




```
    FltUnregisterFilter(g_filterData.pFilter);

    return STATUS_SUCCESS;
}

NTSTATUS FLTAPI OnSimpleFilterInstanceSetup(__in PCFLT_RELATED_OBJECTS pFltObjects, __in FLT_INSTANCE_SETUP_FLAGS fla
    __in DEVICE_TYPE volumeDeviceType, __in FLT_FILESYSTEM_TYPE volumeFilesystemType)
{

    UNREFERENCED_PARAMETER(pFltObjects);

    UNREFERENCED_PARAMETER(flags);

    UNREFERENCED_PARAMETER(volumeDeviceType);

    PAGED_CODE();

    ASSERT(pFltObjects->Filter == g_filterData.pFilter);

    // 볼륨의 정보가 네트워크장치일경우에는 필터를 등록하지않는다.

    if (volumeDeviceType == FILE_DEVICE_NETWORK_FILE_SYSTEM)
    {

        return STATUS_FLT_DO_NOT_ATTACH;

    }
    return STATUS_SUCCESS;

}

BOOLEAN IsMyExtension(__in PUNICODE_STRING pExtension)
{

    const UNICODE_STRING* ext;

    // 비교할 대상의 문자열길이 가0이라면 아무것도없는 것 이다.

    if (pExtension->Length == 0)
    {

        return FALSE;

    }

    ext = g_myExtensions;
```

FILE SYSTEM

- File System?
- NTFS

REGISTRY

- Registry?

WINDOW EVENT LOG

- Window Event Log?
- 파일 및 폴더 감사정책 실습

PLUS

- FTZ Level1 ~ Level5
- OLLYDBG, Assembly

FILE SYSTEM

File System?

NTFS

FILE SYSTEM?

컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관
또는 조직하는 체제를 가리키는 말.


X


PPT


DOC


PDF


TXT

Function of File Systems

Create

Save

Search

Delete

Various File Systems

NTFS
New Technology File System

ExFAT
Extended File Allocation Table

FAT32
File Allocation Table

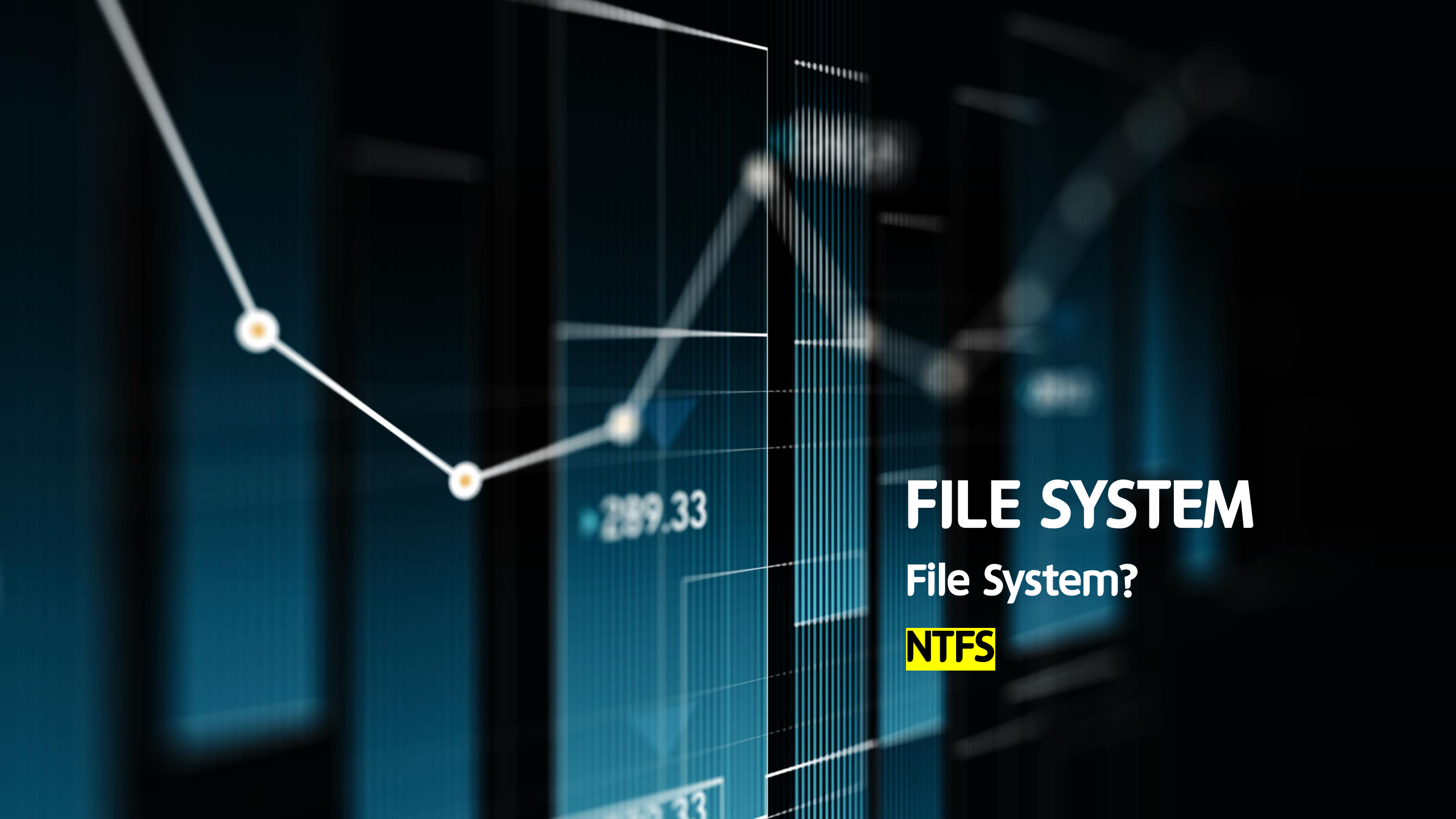
Ext4
Extended File Table

APFS
Apple File System

File System Structure

- 많은 파일을 관리할 수 있어야 함으로 파일시스템이라는 구조에 의존
- 파일시스템은 사용자 영역이 아닌 커널 영역에서 동작
- 사용자에게 하드디스크의 동작을 추상화 시켜주는 도구

File System Structure



FILE SYSTEM

File System?

NTFS

NTFS

NEW TECHNOLOGY FILE SYSTEM

FAT의 한계점을 개선한 파일 시스템

WINDOW NT 이후부터 사용

Structure of NTFS File System

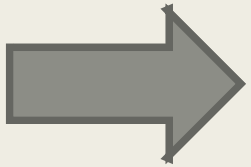

REGISTRY
Registry?

REGISTRY?

운영체제와 응용프로그램 운영에 필요한 정보들을 저장
하기 위해 고안된 계층형 데이터 베이스

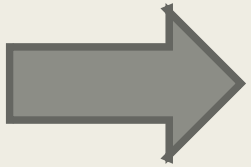
Registry

- HKEY_LOCAL_MACHINE(HKLM)
- HKEY_USERS(HKU)



Master Key

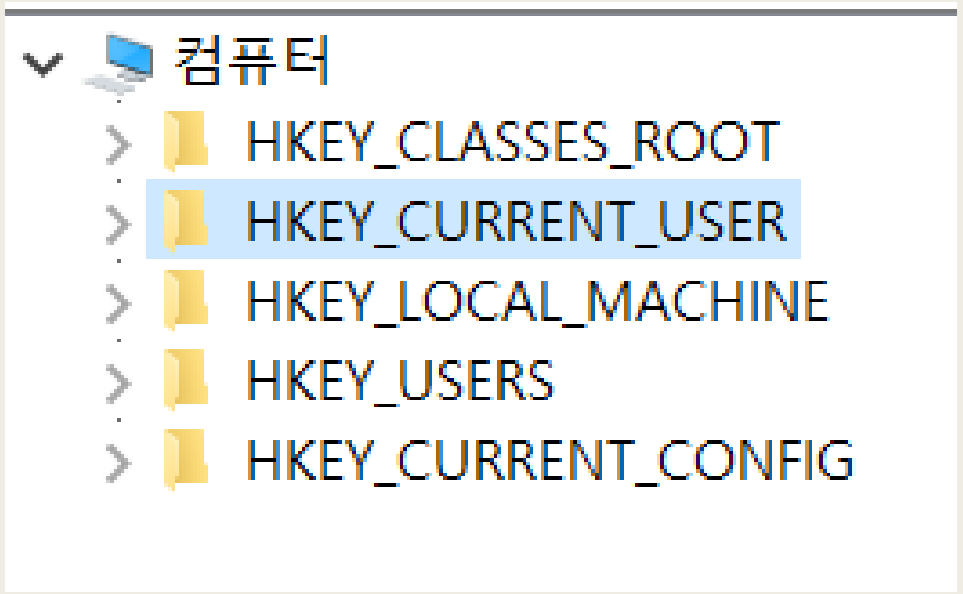
- HKEY_CURRENT_USER (HKCU)
- HKEY_CLASSES_ROOT(HKCR)
- HKEY_CURRENT_CONFIG(HKCC)



Derived Key

C:/windows/system32/config/
C:/users/account/NTUSER.dat

Registry hive



Use Case

Digital Forensic

Incident Response

Computer Setting

WINDOW EVENT LOG

Window Event Log?

파일 및 폴더 감사정책 실습

WINDOW EVENT LOG

Windows 시스템에서는 시스템의 로그가 이벤트 로그형식으로 관리되며, 이벤트 로그를 확인하기 위해 Event Viewer를 이용

WINDOW EVENT LOG

Window Event Log?

파일 및 폴더 감사정책 실습

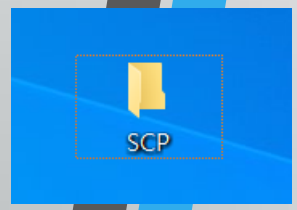
파일 및 폴더 감사정책

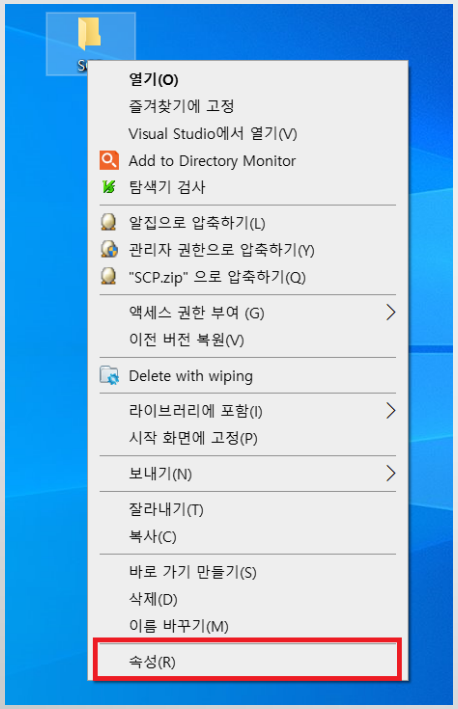
감사(Auditing)란 사용자와 운영체제의 활동을 추적하고 다음과 같은 것들을 기록 하는 것

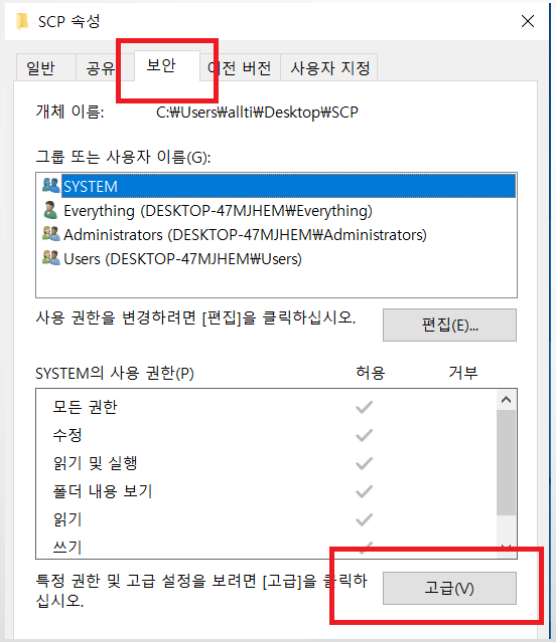
"무슨 일이 있었는지?", "누가 했는지?", "언제 있었는지?", "그래서 그 결과는?"

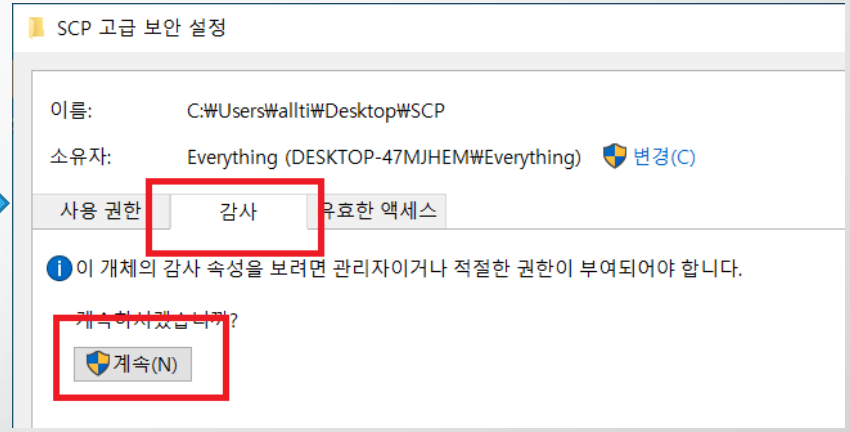
감사는 관리자의 가장 중요한 임무 중 하나

윈도우 파일 및 폴더 감사 정책 설정

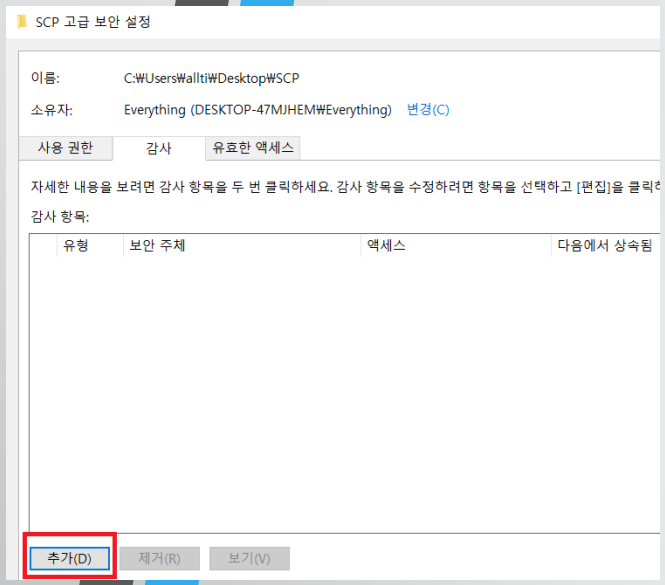


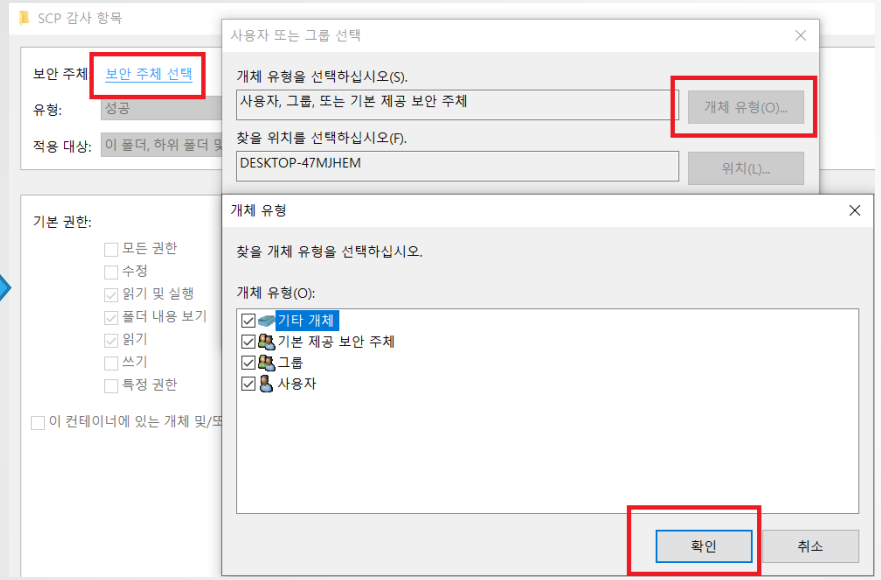


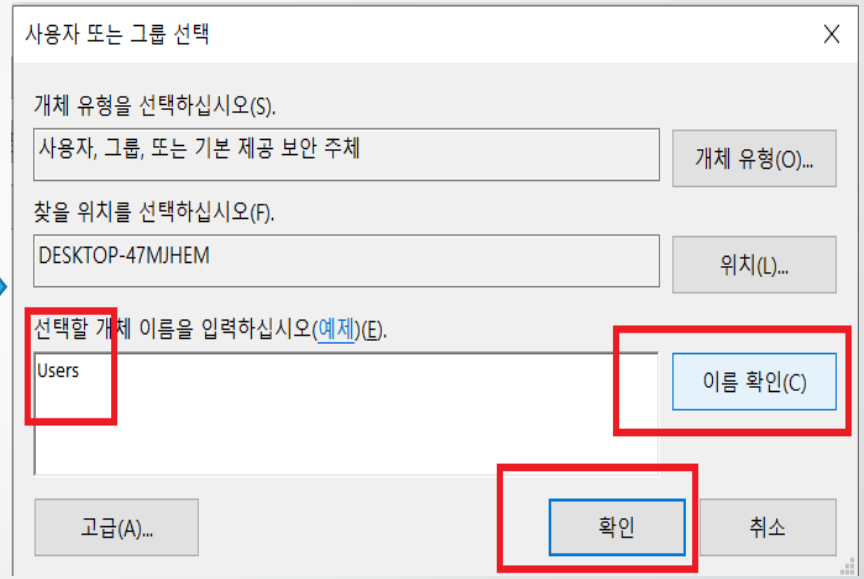


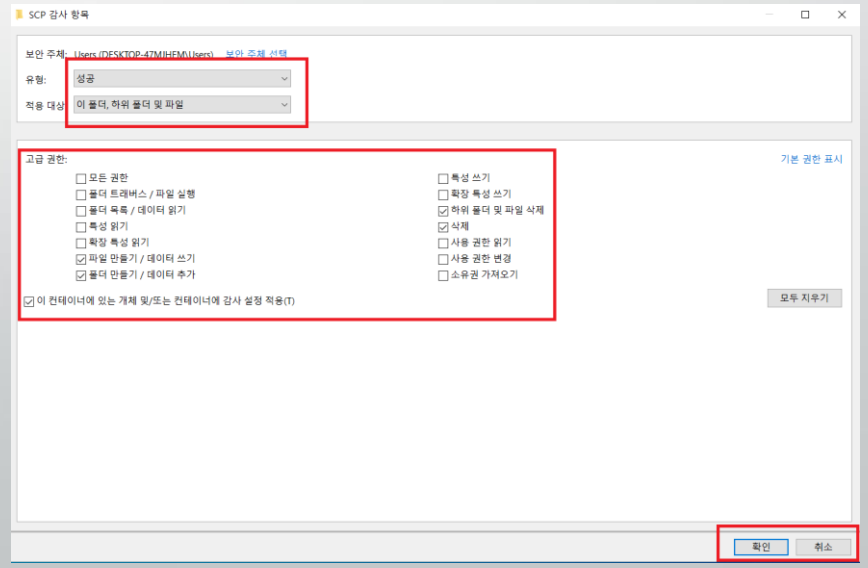


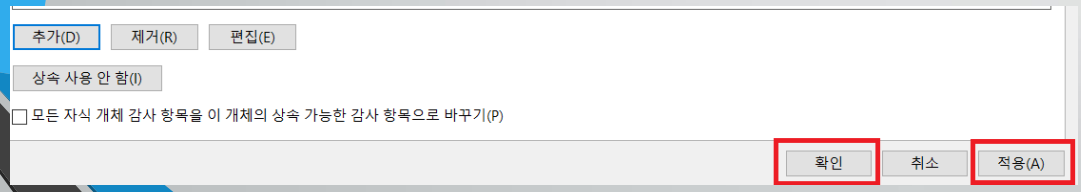
윈도우 파일 및 폴더 감사 정책 설정



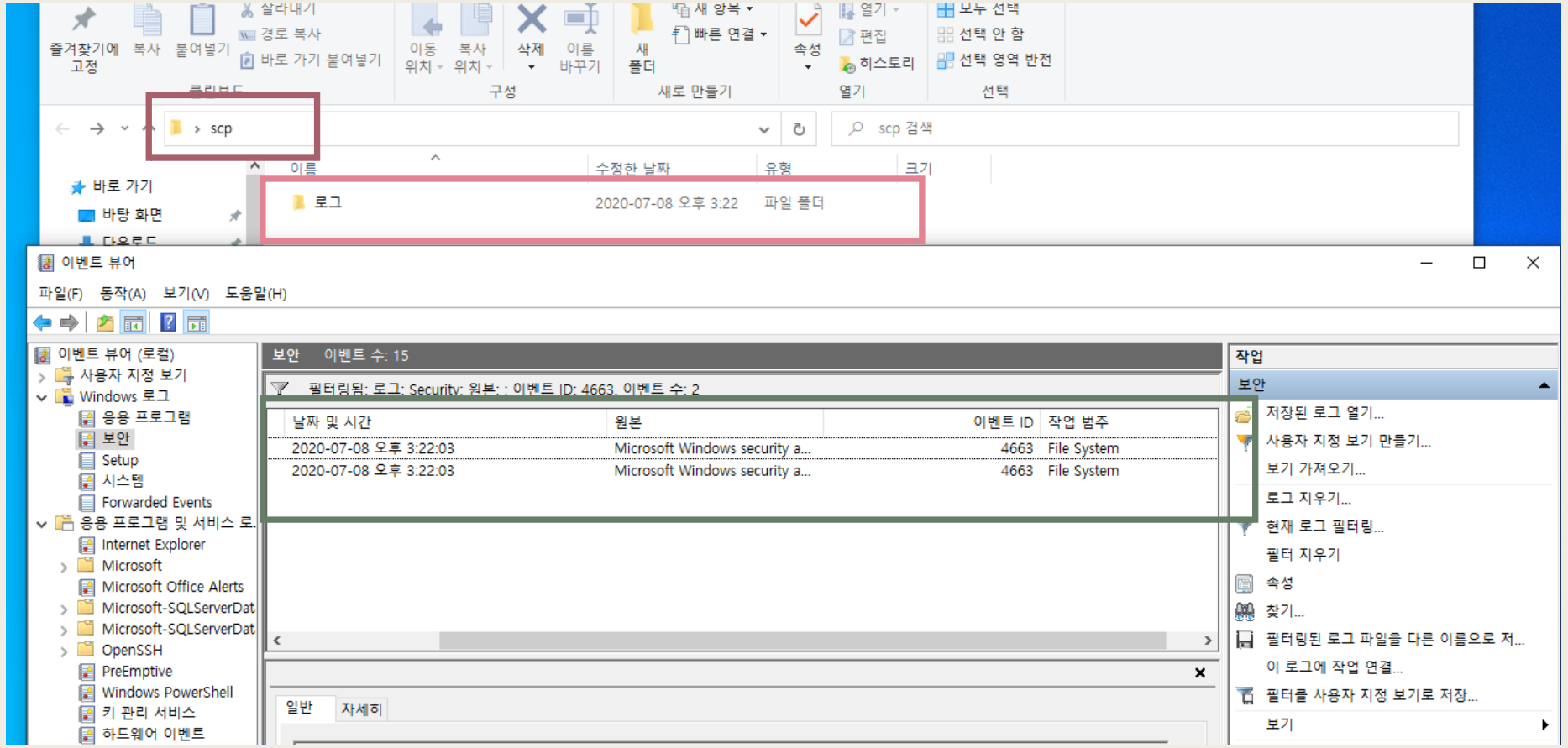




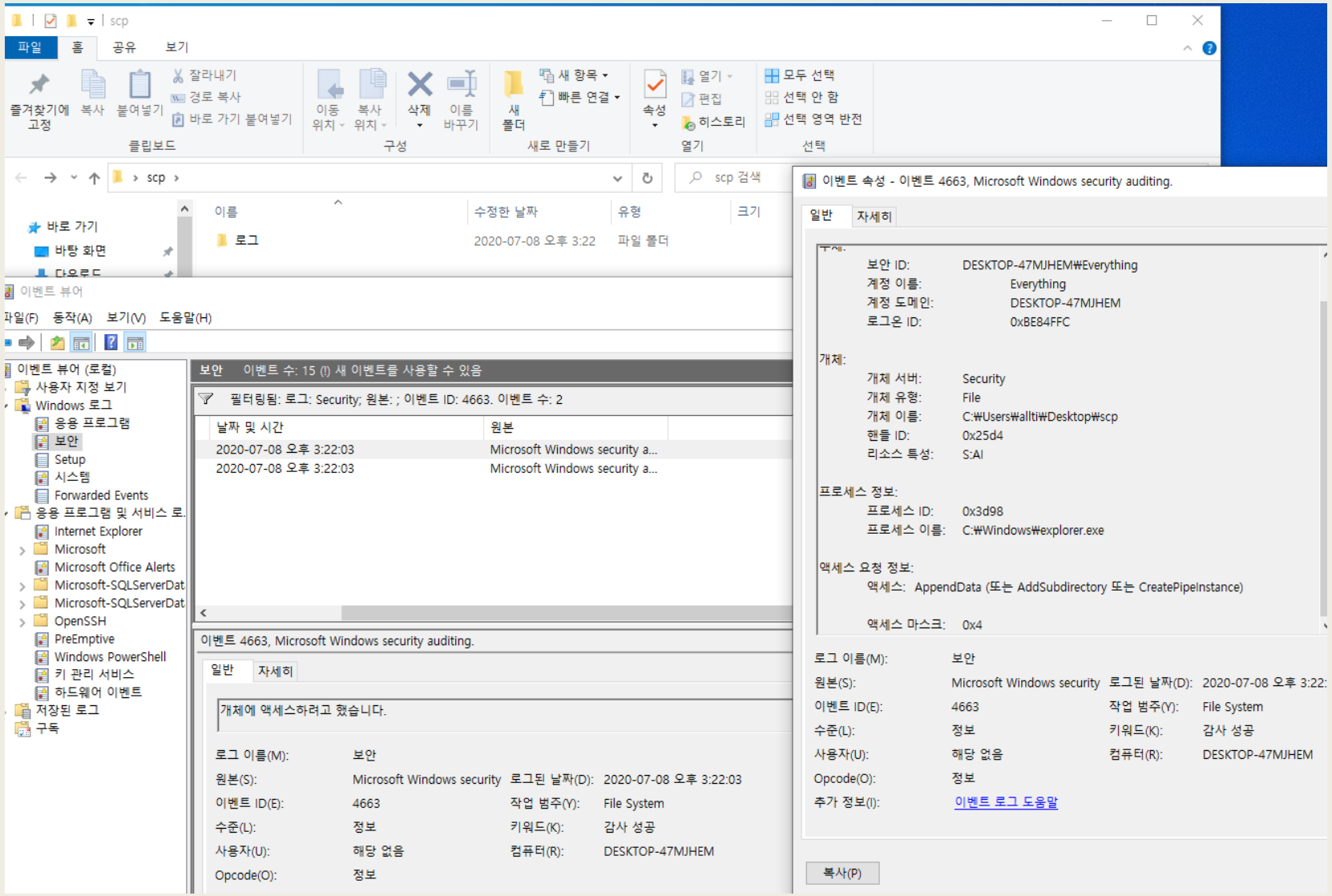




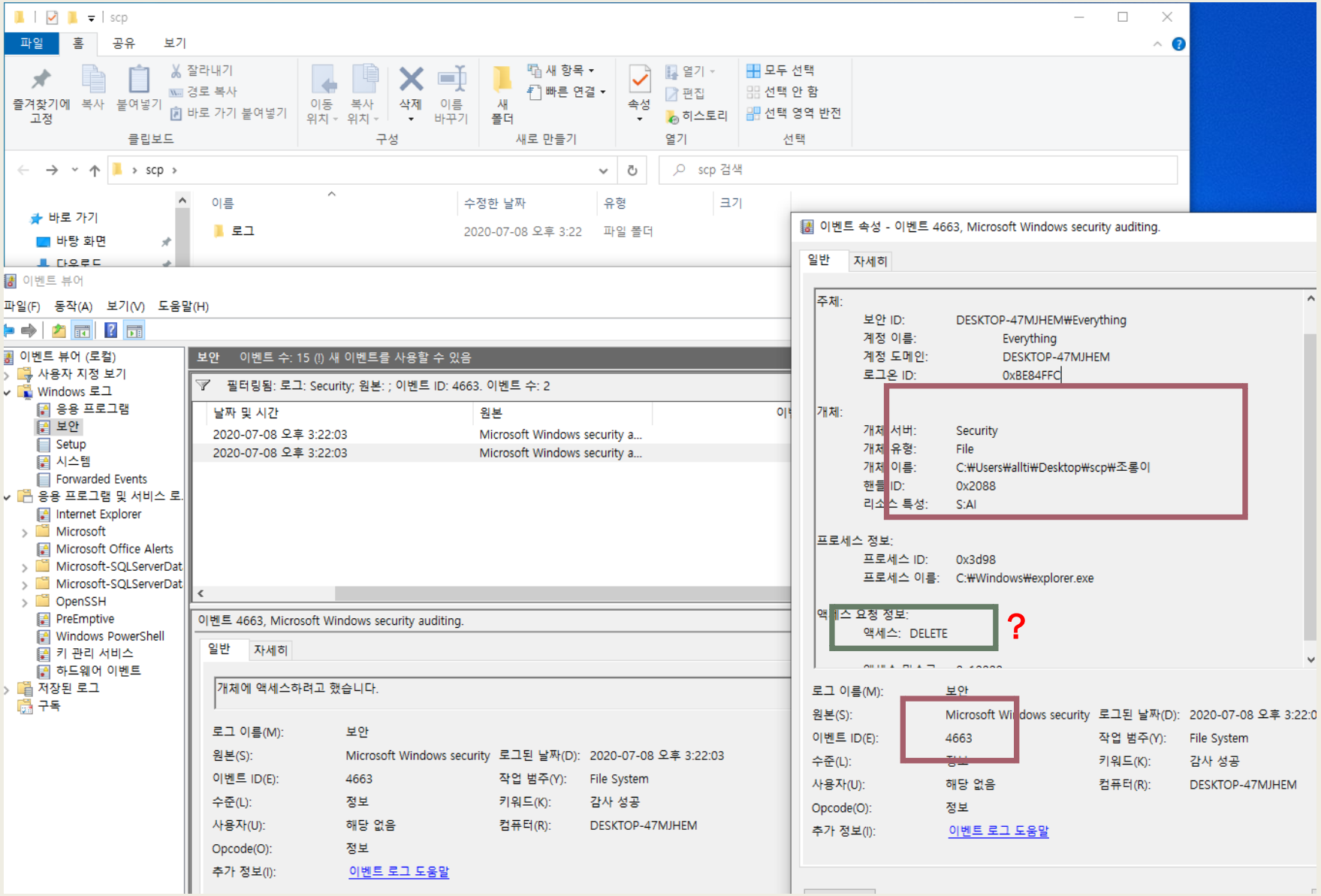
감사정책이 설정된 폴더에 파일 생성



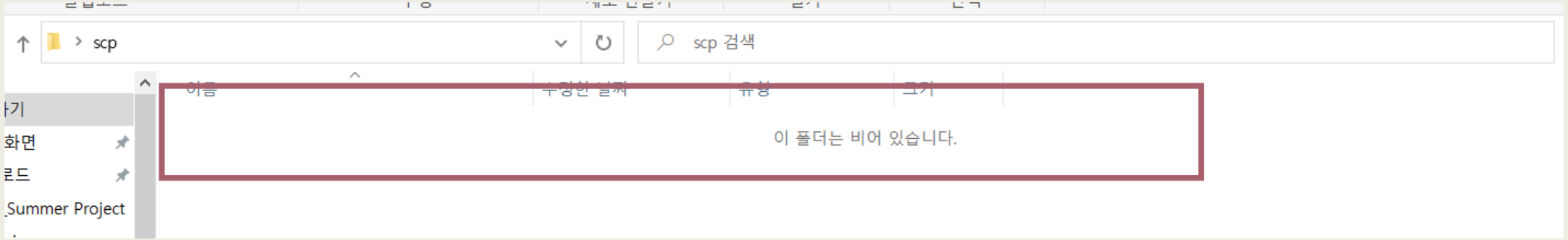
Window Event Log 01



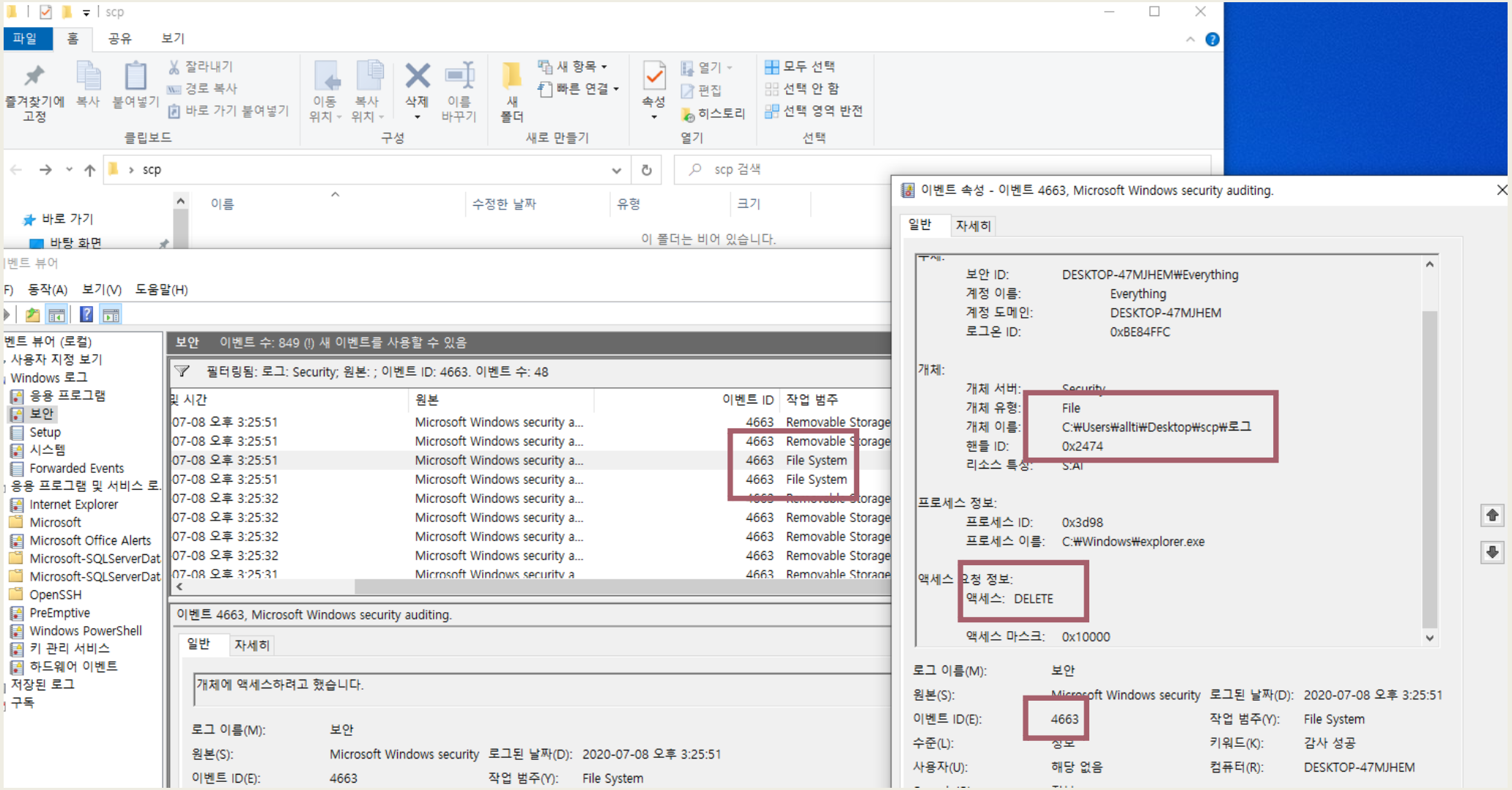
Window Event Log 02



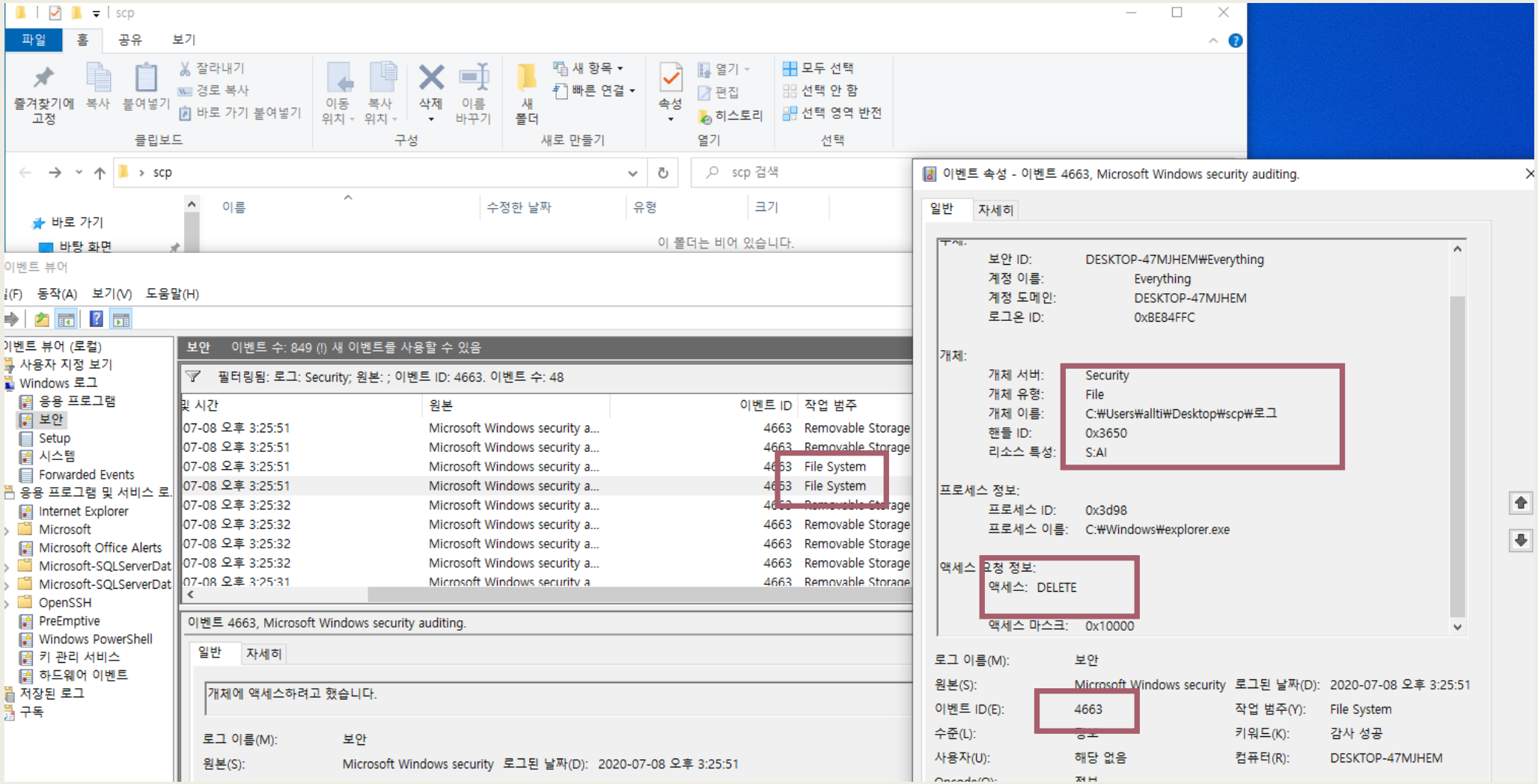
감사정책이 설정된 폴더에 파일 삭제



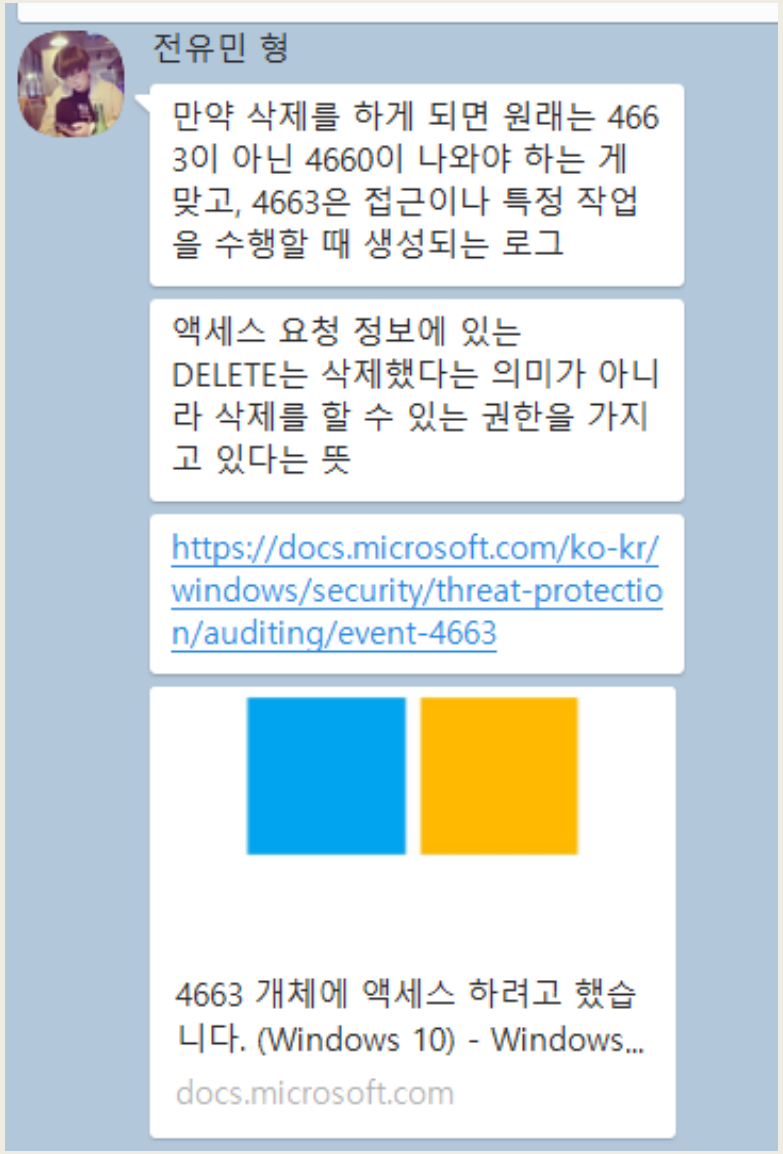
Window Event Log 01



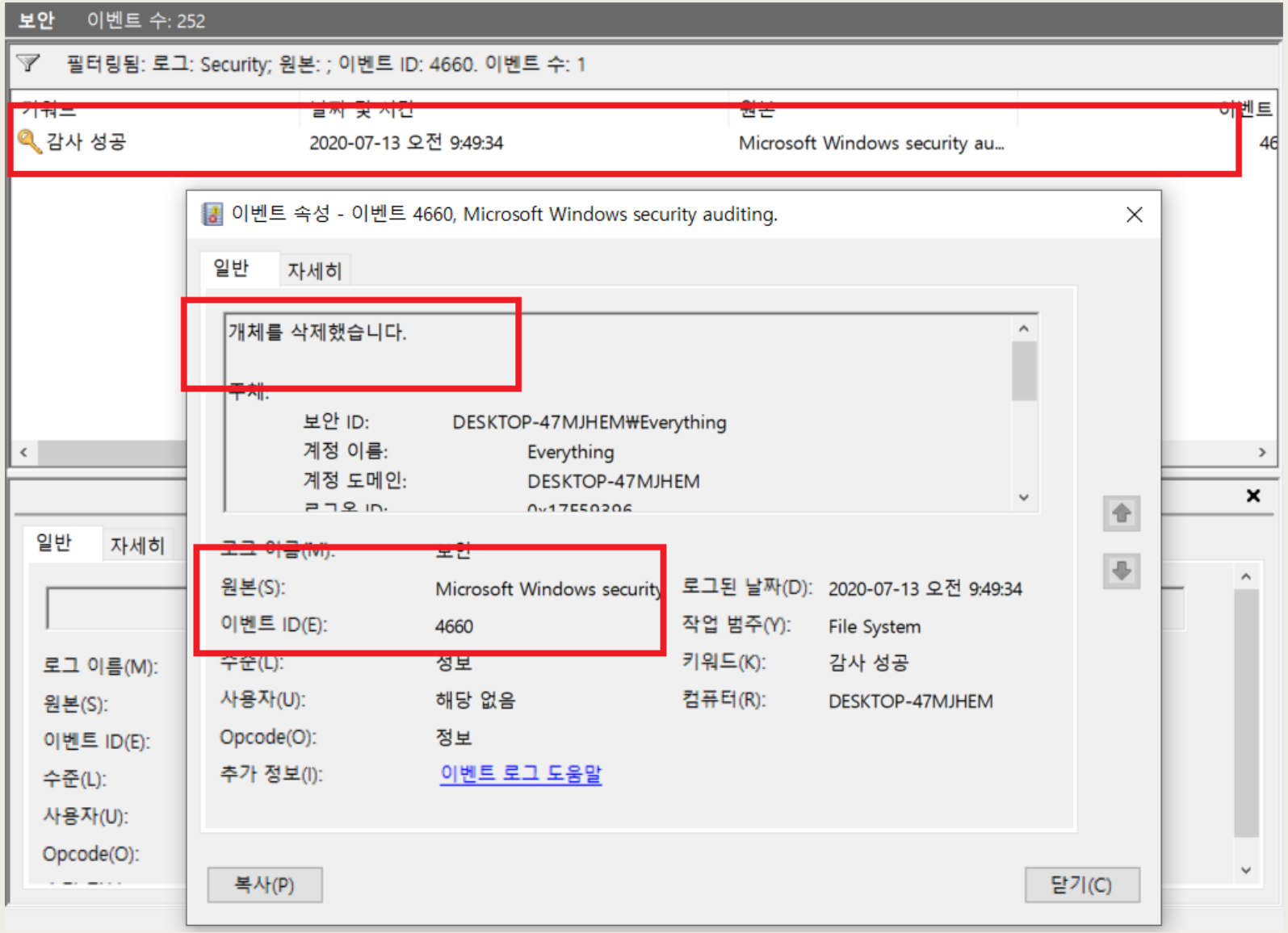
Window Event Log 02



전유민 PL님의 답변

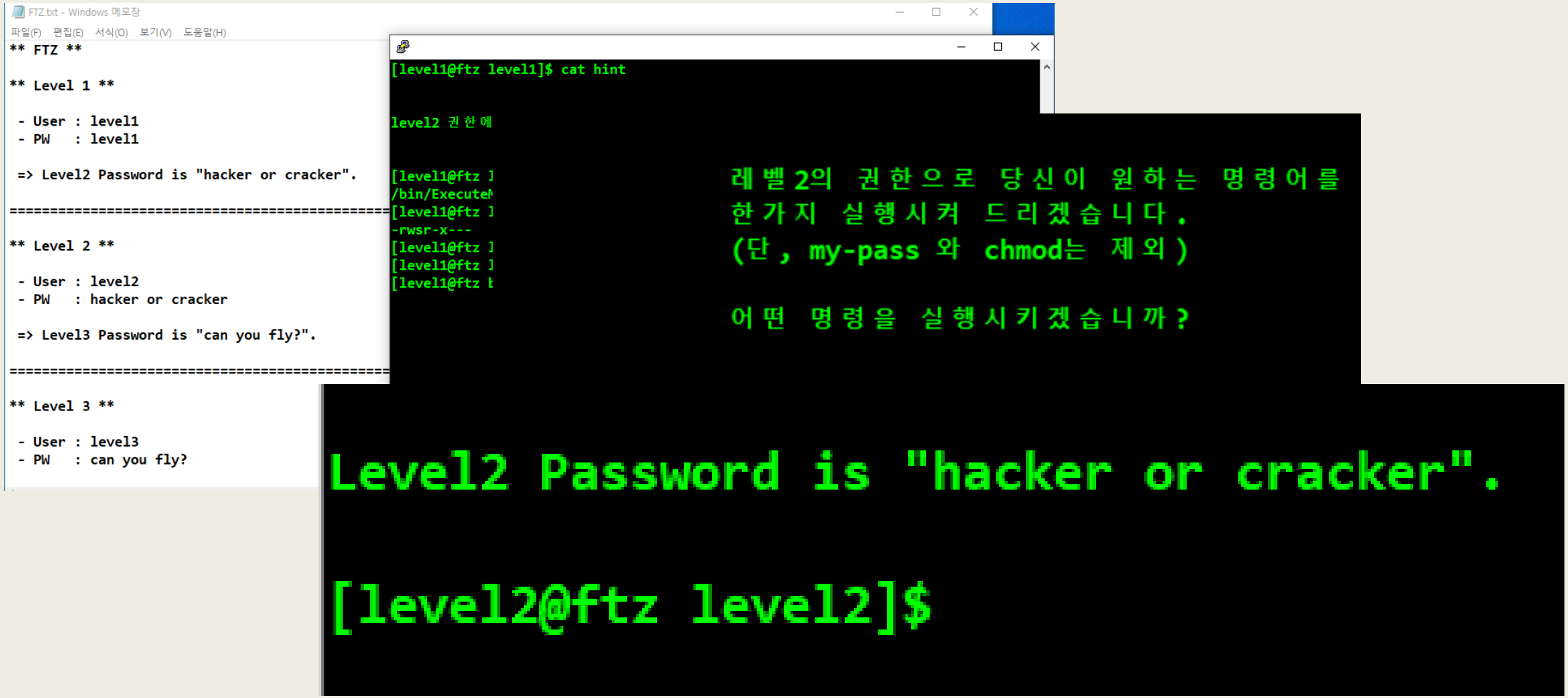

전유민 형
만약 삭제를 하게 되면 원래는 4663이 아닌 4660이 나와야 하는 게 맞고, 4663은 접근이나 특정 작업을 수행할 때 생성되는 로그
액세스 요청 정보에 있는 DELETE는 삭제했다는 의미가 아니라 삭제를 할 수 있는 권한을 가지고 있다는 뜻
https://docs.microsoft.com/ko-kr/windows/security/threat-protection/auditing/event-4663
4663 개체에 액세스 하려고 했습니다. (Windows 10) - Windows...
docs.microsoft.com

Window Event Log

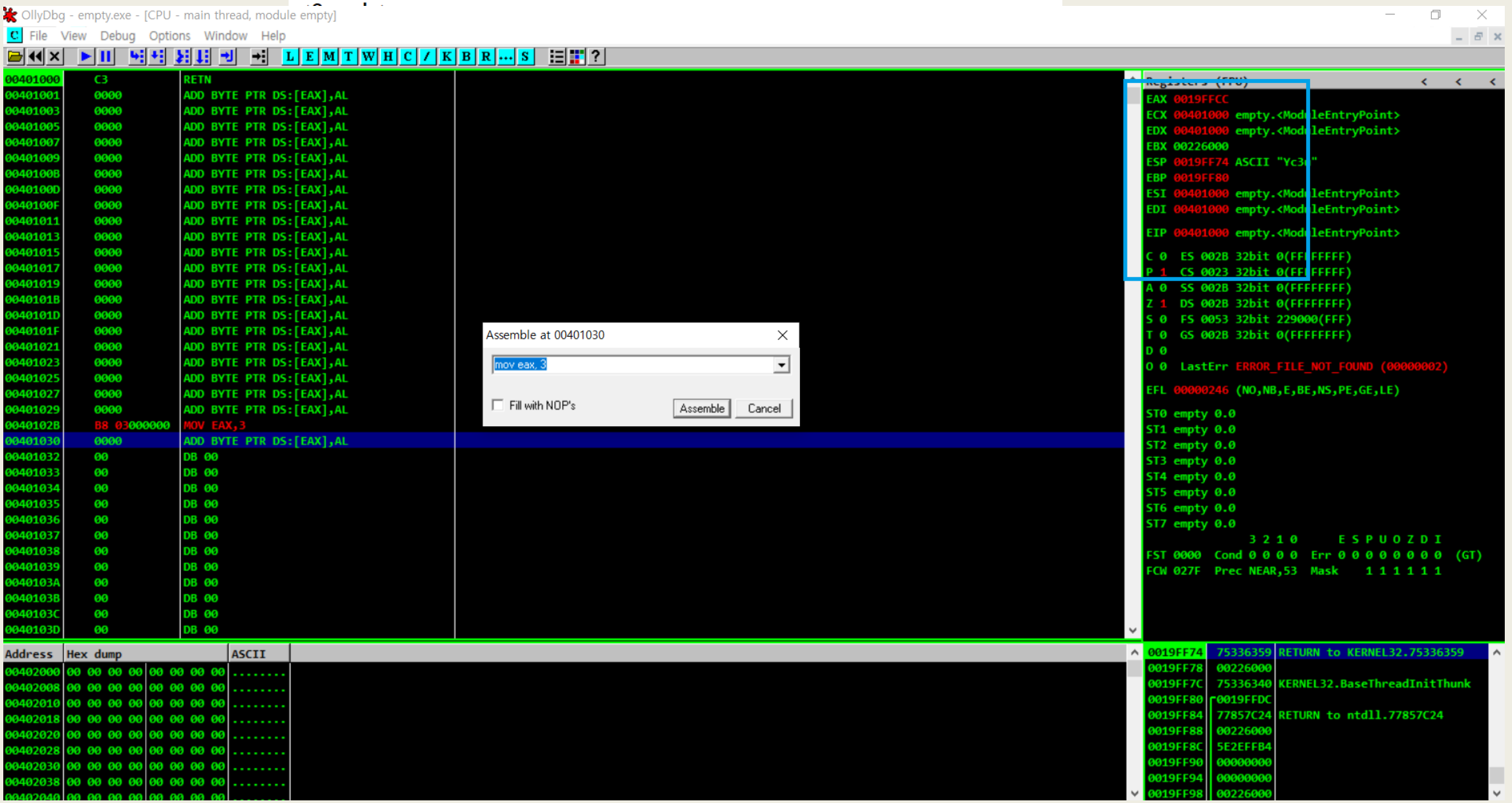



PLUS
FTZ Level1 ~ Level4
OLLYDBG, Assembly

FTZ Level1 ~ Level4



OLLYDBG, Assembly



도움주신

정재훈 형 (FTZ 공부 방법 및 IT 보안 분야 전반적인 질문답변)
조재현 형 (개인공부 방향 설정 도움)
서동훈 형 (FTZ 공부 방법)
전유민 형 (개인공부 방향 설정 도움 및 기타 자료 제공)
김우종 형 (리버싱 핵심원리 자료 제공)

분들께 감사드립니다.