문서파일 포렌식

화이트햇 스쿨 보고서

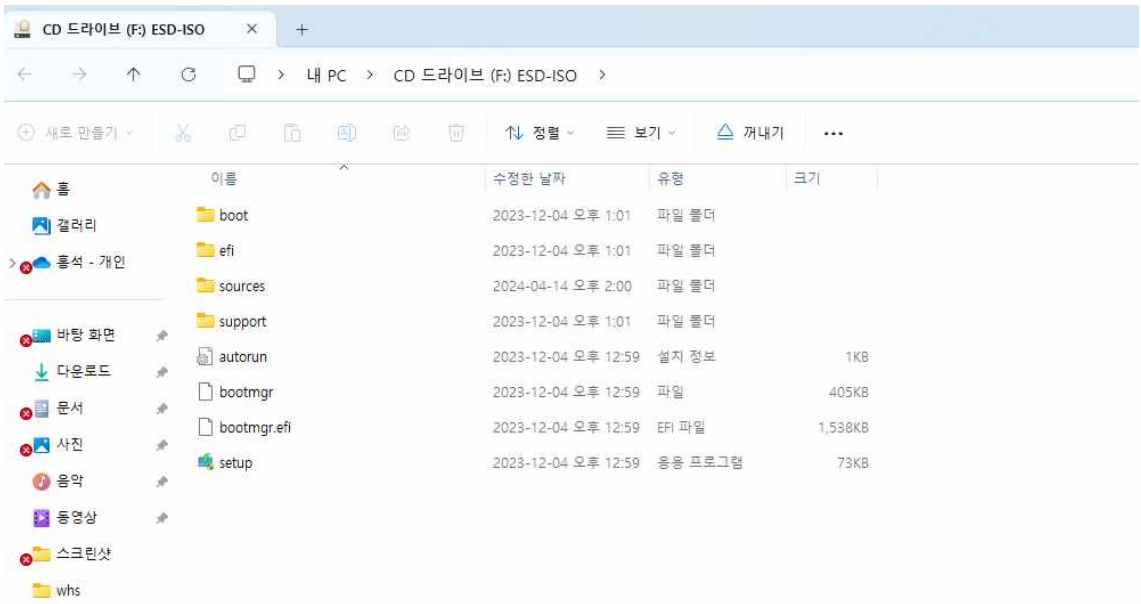
2024 화이트햇 스쿨 2기
[15반] 최홍석_9246

1. 바탕화면에 Windows.iso 파일을 다운로드한다.

2. Windows.iso 파일을 마운트한다.

Windows.iso 파일을 가상 드라이브에 마운트를 하면 해당 드라이브(F:)에 윈도우 설치 파일이 생성된다.

바탕화면 -〉 Windows.iso 파일에서 마우스 우클릭 -〉 가상 드라이브에 마운트 -〉 (F:)ESD-ISO 생성



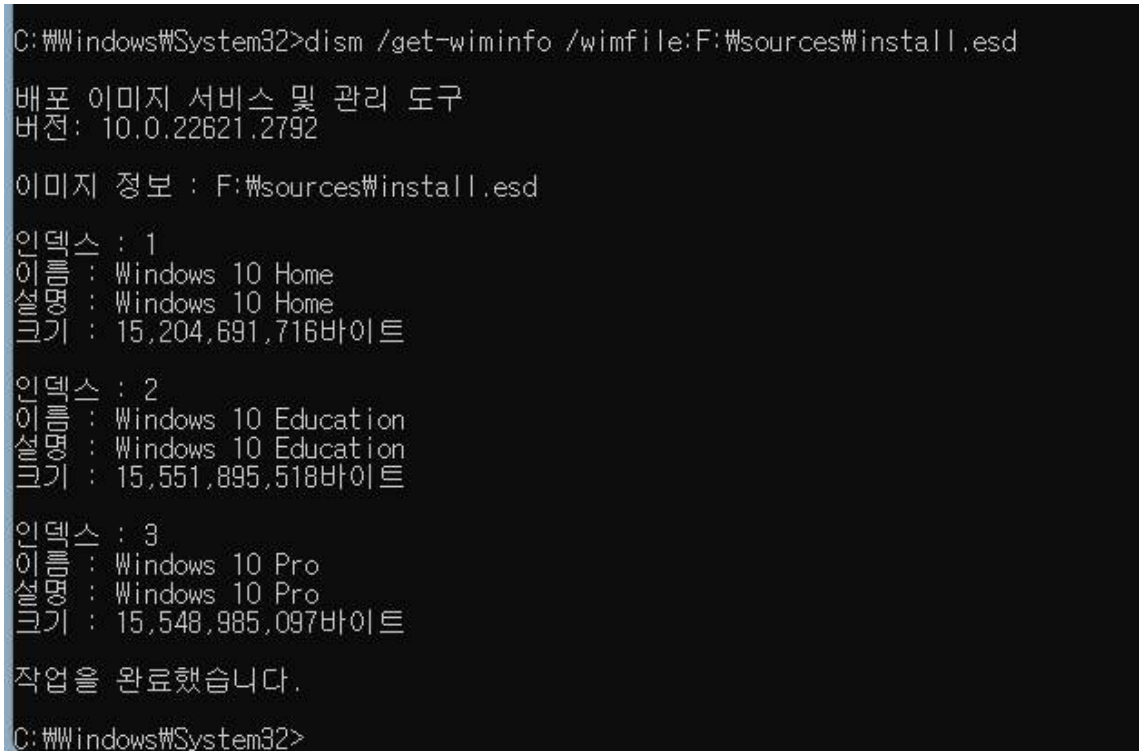
3) 원하는 윈도우 버전의 인덱스 번호를 확인한다.

3-1) install.esd 파일에서는 여러 가지 버전의 윈도우를 포함하기 때문에 추출하려는 윈도우 버전의 index 번호를 확인한다.

3-2) 명령 프롬프트를 권리자 권한으로 실행시킨다.

3-3) 윈도우 버전의 인덱스 번호를 확인한다.

dism /get-wiminfo/wimfile:F:₩sources₩install.esd



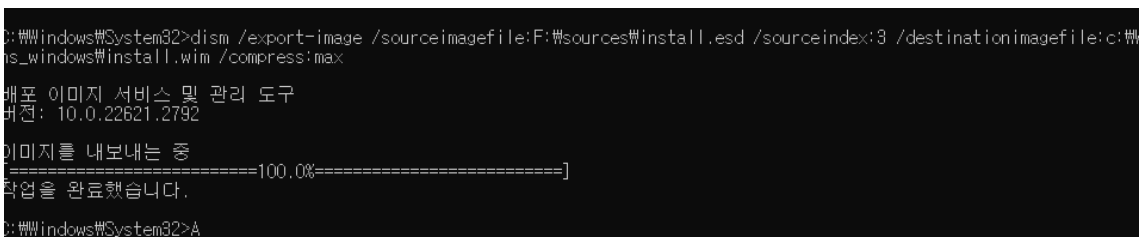
4. wim 파일을 추출한다.

4-1)사전에 wim 파일을 생성할 임의의 폴더 (c:₩whs_windows)를 만들어준다.

4-2)인덱스: 3(windows 10 pro)를 추출한다.

4-3)wim 파일을 추출한다.

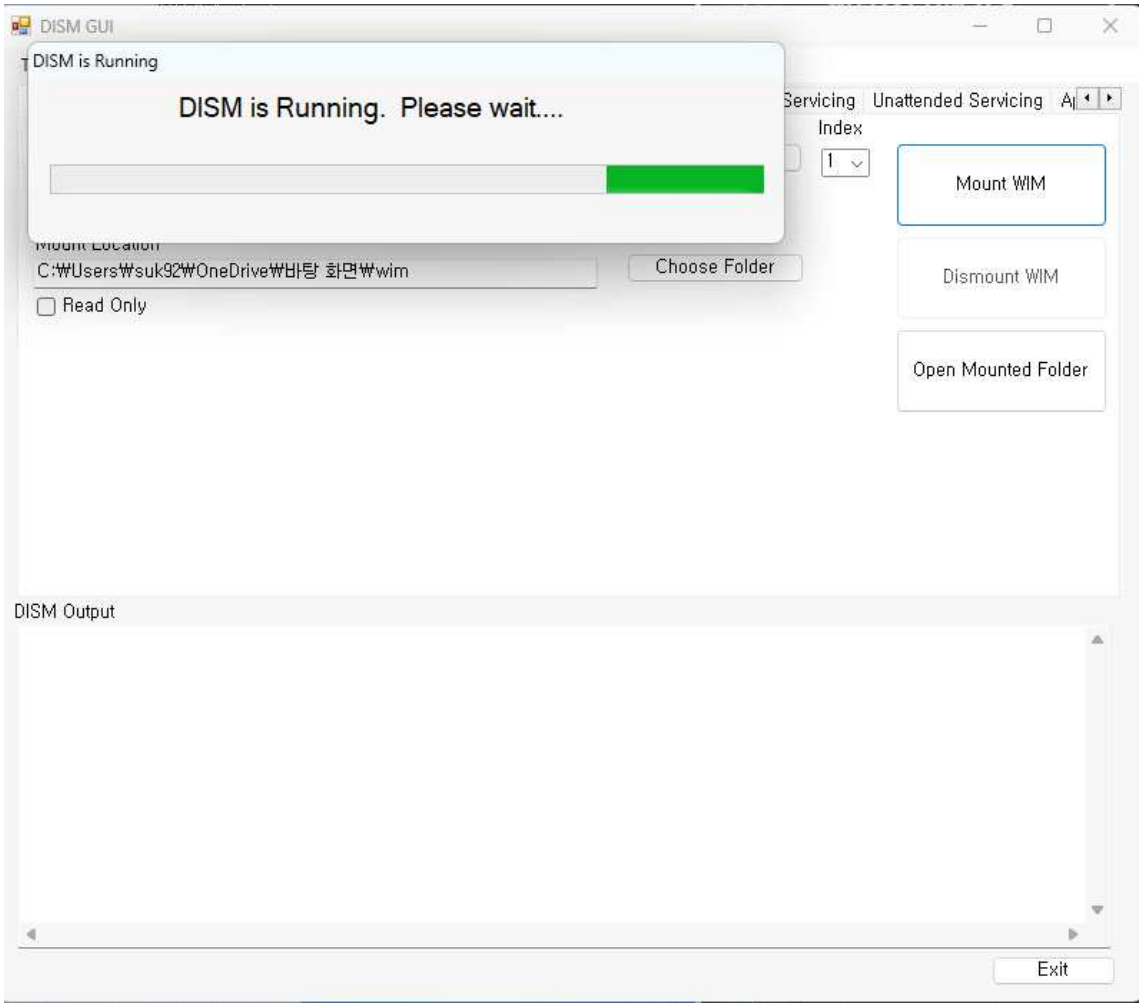
dism/export0image /sourceimagefile:F:₩sources₩install.esd /sourceindex:3
/destinationimagefile:c:₩whs_windows₩install.wim /compress:max



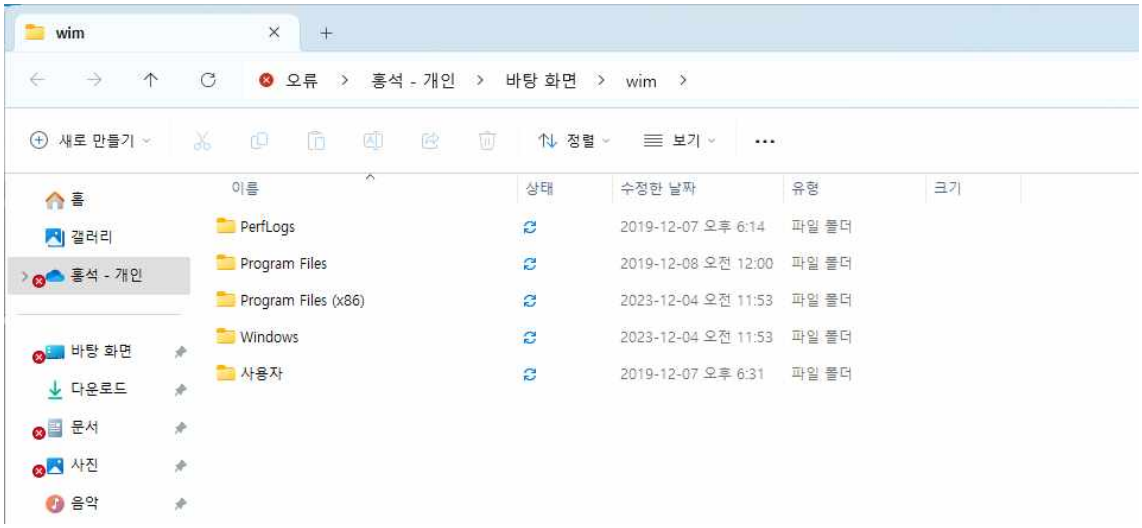
4-4) 탐색기를 통해 확인한다.

- 탐색기에서 확인하면 whs_windows 폴더에 install.wim 파일이 잘 추출되었음을 알 수 있다. wim 파일도 압축 이미지 파일이고, 추출된 install.wim 파일의 크기는 4.55GB이다.

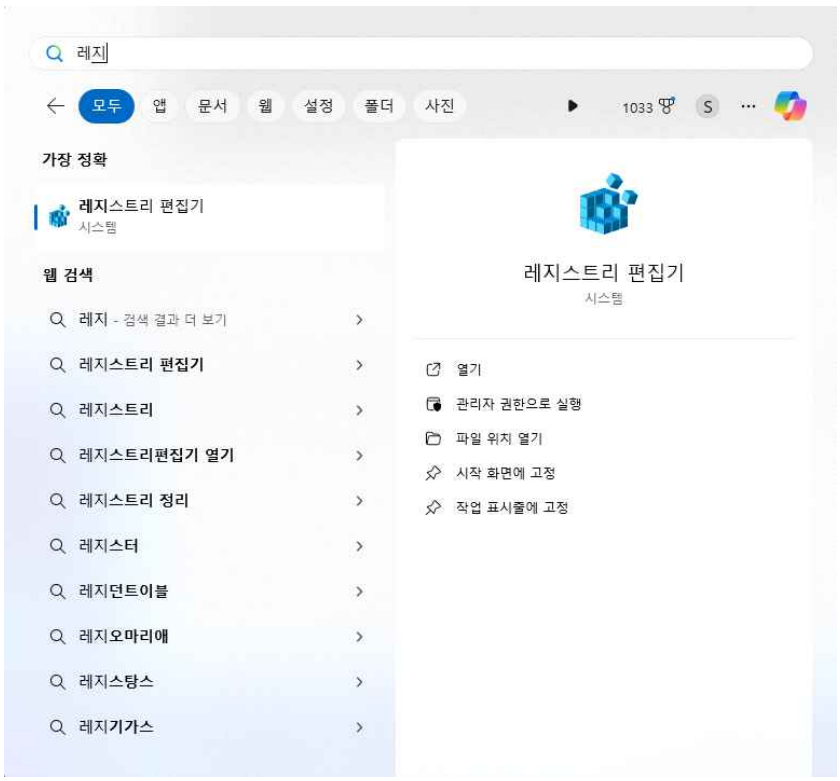
5) 설치한 dism gui를 통해 wim을 마운트한다.



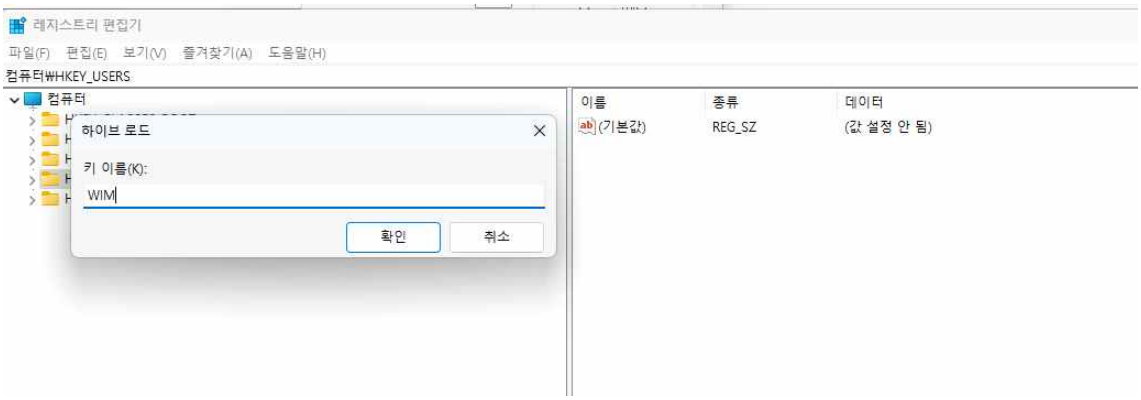
6) mount해 놓은 wim 파일을 열어보면 windows에서 자주 보았던 디렉토리 구조들을 확인할 수 있다.



7)레지스토리 편집기를 연다.

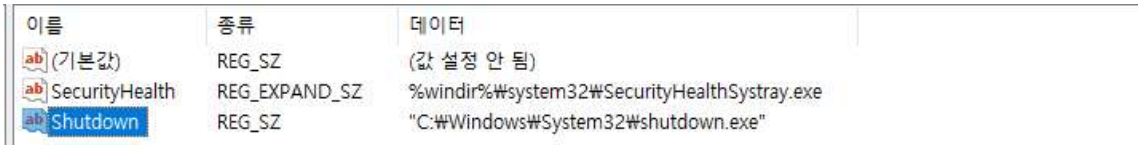


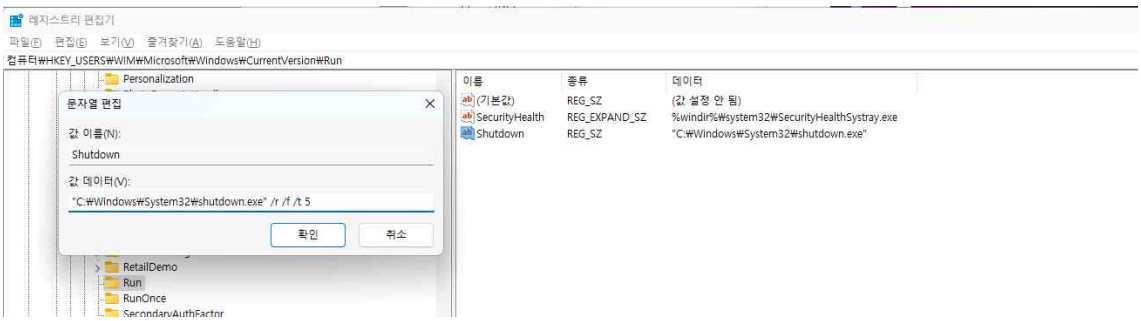
8) 악성코드를 심는다면 주로 HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run에 심는다. 그래서 HKEY_CURRENT_USER에 wim파일의 software파일을 하이브로드한다.



9)cmd에서 where명령을 통해 shutdown.exe 위치를 찾는다.

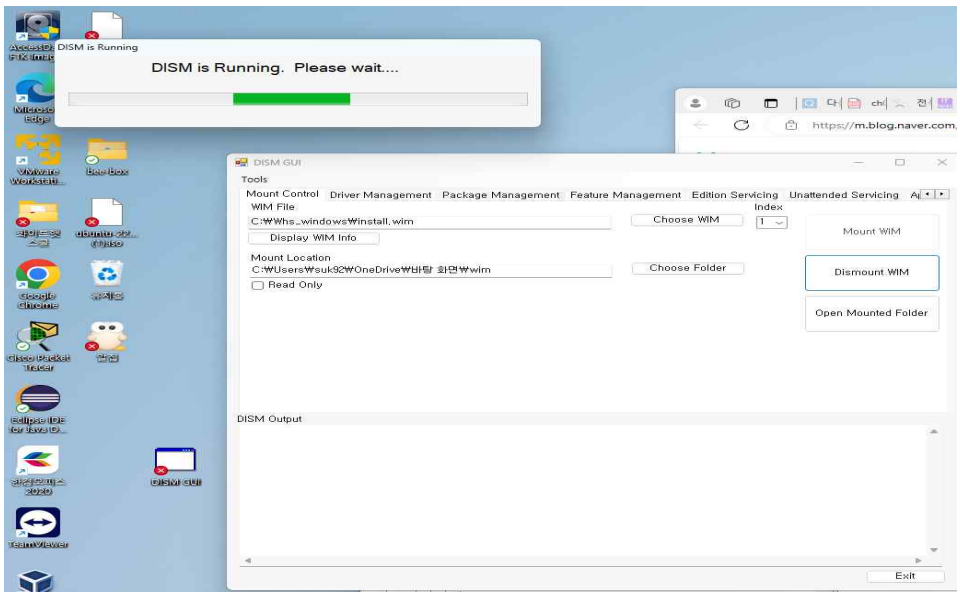
10) 레지스토리 편집기(레지스토리 값 변조)를 통해 HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run에 shutdown 문자열값을 생성한다.



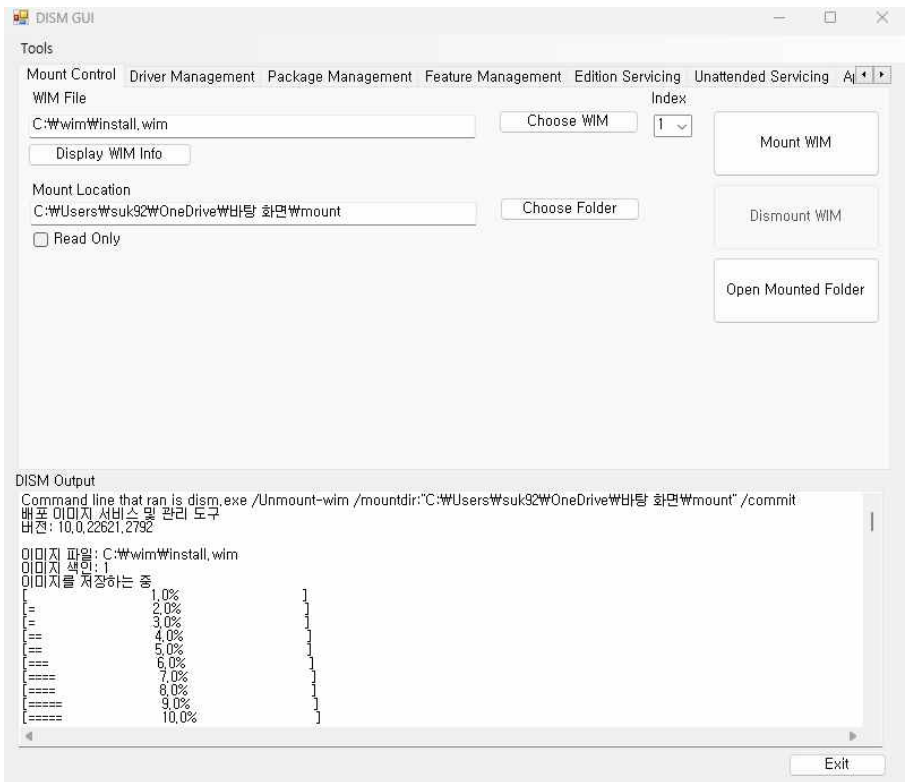


-windows로그인 했을 때, 5초 후 시스템이 무한 재부팅되는 악성코드를 제작해야 되기 때문에 기준과 알맞은 데이터를 작성한다.
“C:₩Windows₩System32₩shutdown.exe” /r /f /t 5

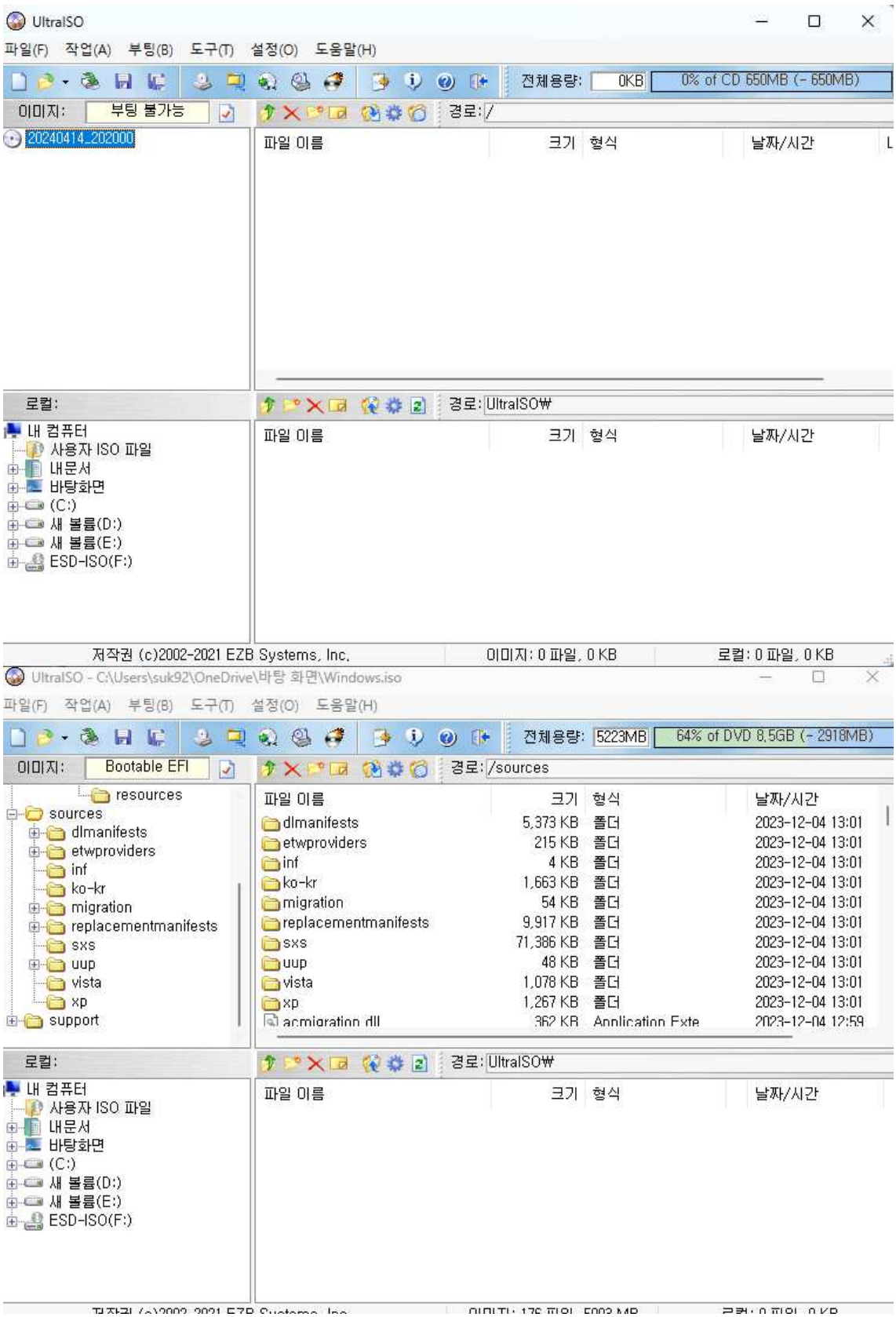
11) 하이브 언로드를 한 뒤 dismout wim을 한다.



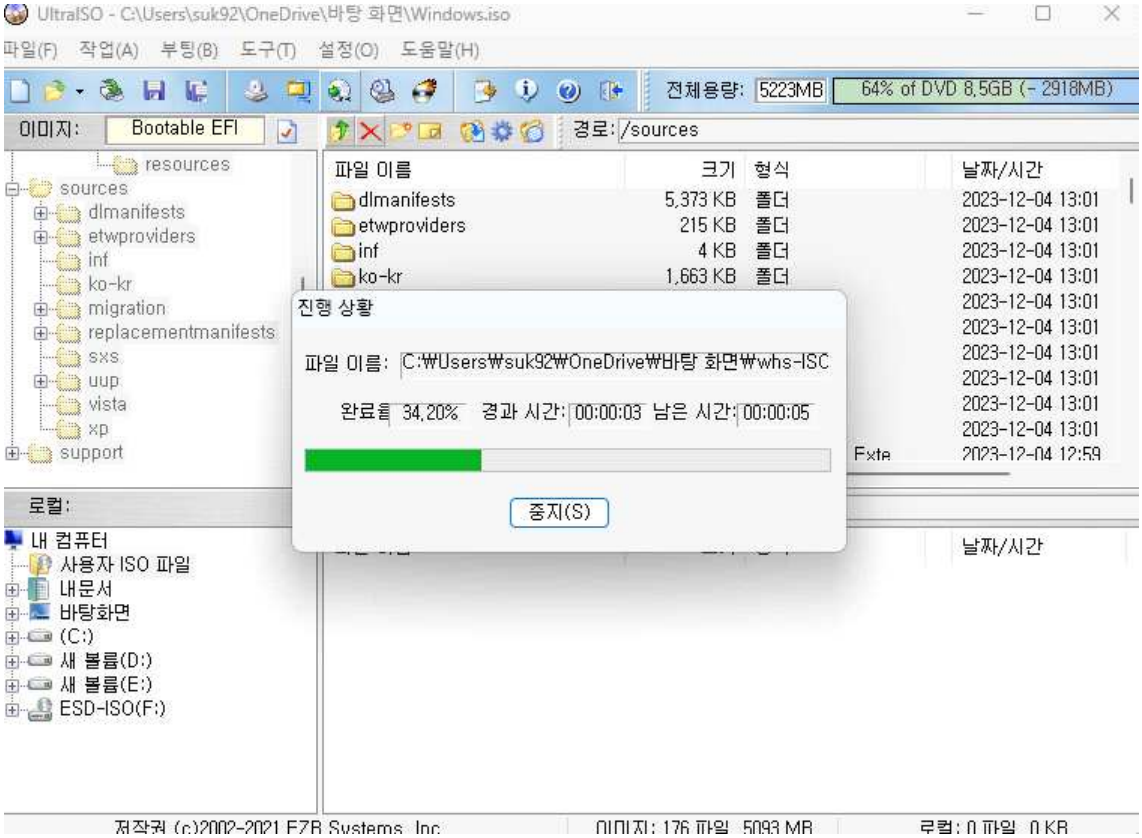
- 과제 실습 중에 dism gui를 닫아버려서 다시 실습하느라 whs_windows 폴더 대신 wim 폴더로 대체했다.



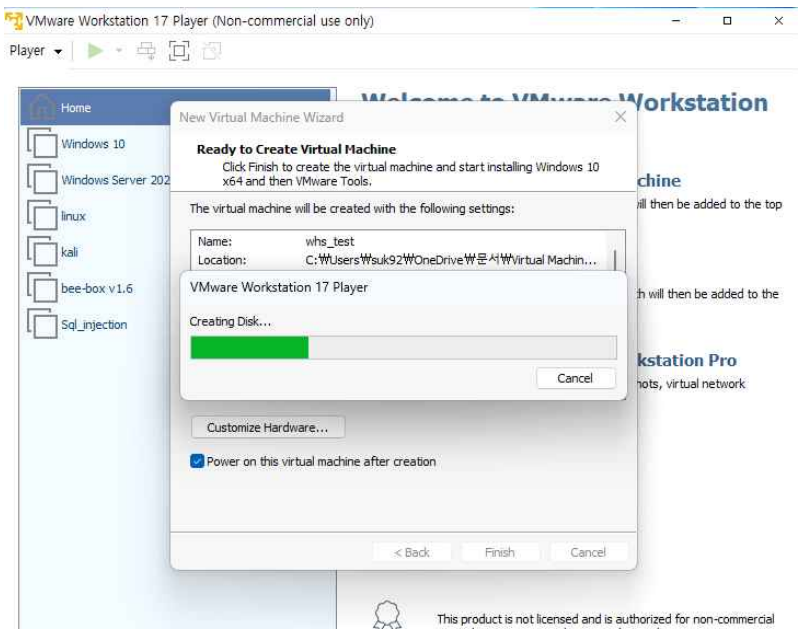
12)UltraISO로 아까 다운로드 받은 windows.iso를 연다.



13)해당 iso 파일에서 install.esd 파일을 삭제하고 dismount했던 install.esd를 추가한 뒤 파일을 다른 이름으로 저장한다.



14) 해당 iso 파일을 가상 머신으로 실행시킨다.



15) 과제 조건과 마찬가지로 windows 로그인을 했을 대, 5초 뒤 시스템이 무한 재부팅됨을 확인할 수 있었다.