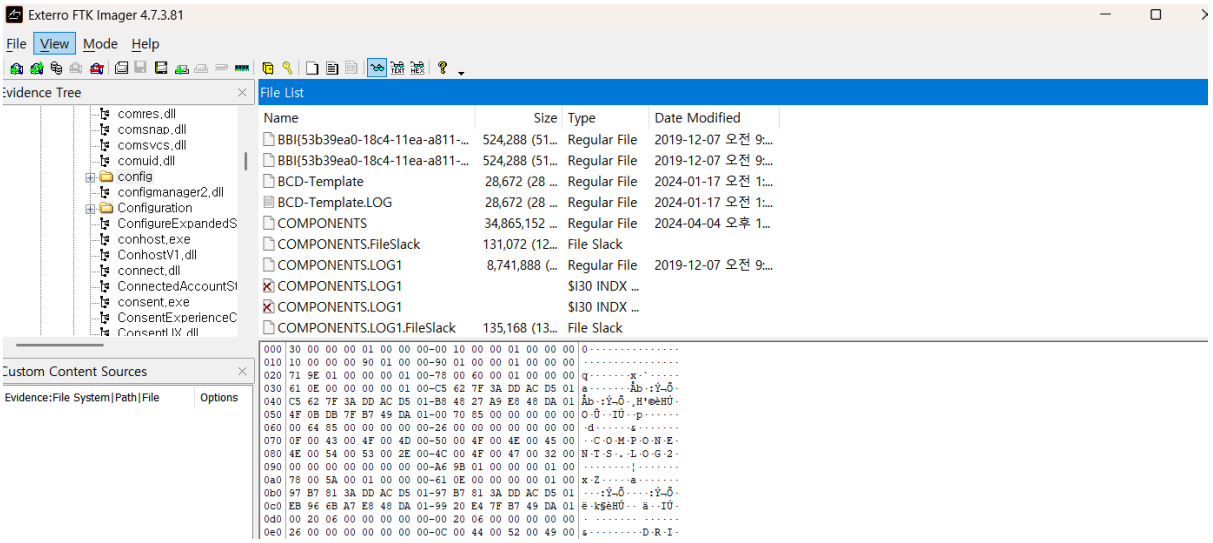
Dreamhack-Find The USB

먼저 드림핵에서 제공해주는 디스크 이미지 1 다운하고 ftk 이미지로 열면 루트가 보인다.

windows system 32에 들어가서 config에 들어가면, 다음과 같이 로그파일이 보인다



일단 디폴트랑 디폴트 로그 1 로그 2를 추출해서 임의적인 파일을 만들어서 구분하기 쉽게 registry를 만들고 저장을 한다.

sam이랑 sam로그1 로그 2도 추출해서 아까 만든 파일에 저장해준다.

시큐리티랑 시큐리티 로그1 로그2도 추출해서 아까 만든 파일에 저장

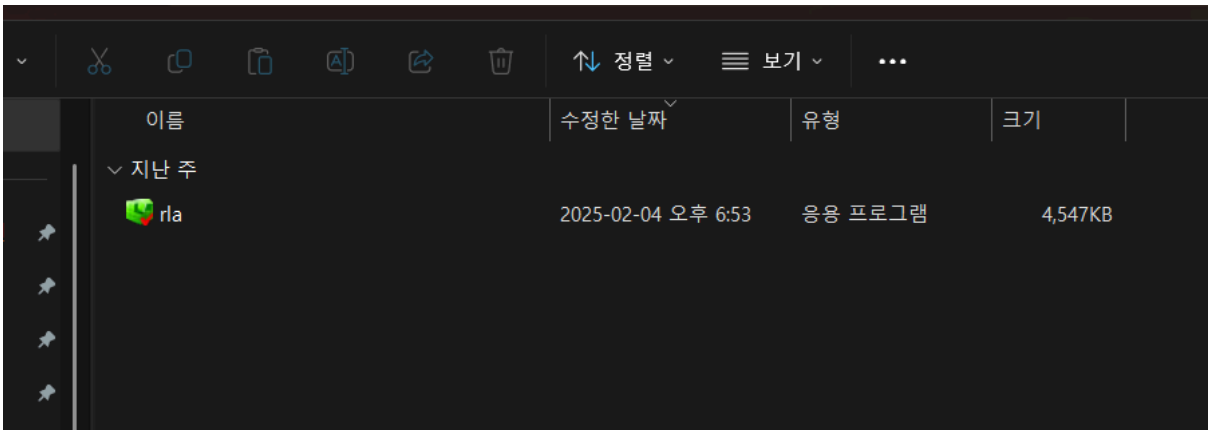
소프트웨어 소프트웨어 로그1 로그 2도 추출해서 동일하게 저장

시스템 시스템 로그 1 로그 2도 저장하는데 시스템 앞에 있는 엑스는 저장하면 안된다.

유저스에 들어가서 엔티유저 엔티유저 로그1 로그2도 저장한다 아까 그 파일에 저장

앱데이터 들어가서 userdat도 위와 동일하게 저장해준다.

이제 다운받은걸 다 클린해야한다!!



파워쉘 켜서 rla의 경로를 찾고 (툴위치) 파워쉘에 경로를 복사해서 붙이며 자동으로 실행이 된다

피피티에 있는 명령어 ./rla.exe를 입력하고

그 아까 만든 파일에 registry clean 폴더를 만들고

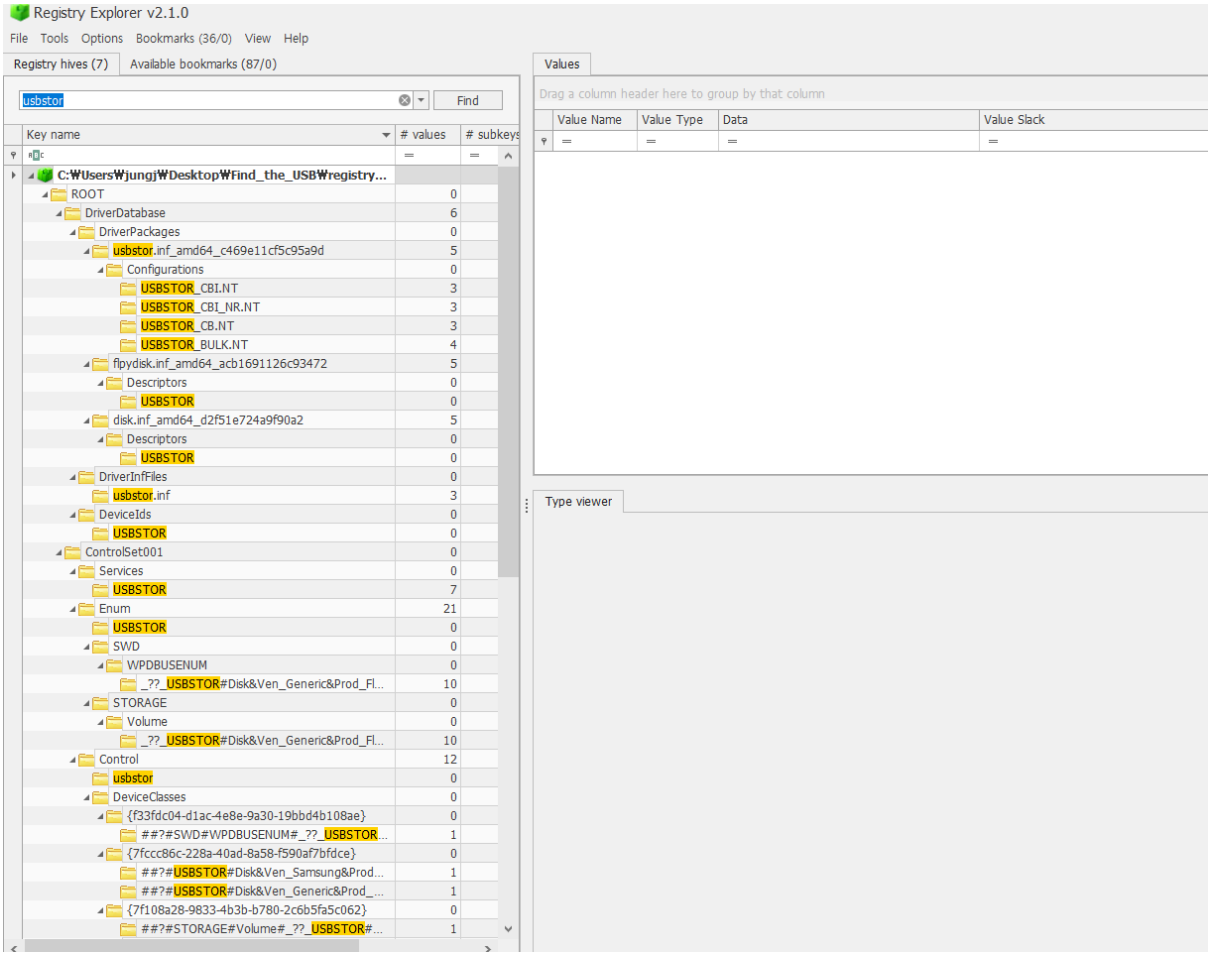
그 경로 하고 큰 따움표 없애고 -d registry\-out\registryclean 에 넣으면 된다

```
PS C:\Users\jungj>  C:\Users\jungj\Downloads\rla\rla.exe -d C:\Users\jungj\Desktop\Find_the_USB\registry\ --out C:\Users
\jungj\Desktop\Find_the_USB\registry_clean
```

```
Processing hive C:\Users\jungj\Desktop\Find_the_USB\registry\DEFAULT.LOG2.copy0
        Hive C:\Users\jungj\Desktop\Find_the_USB\registry\DEFAULT.LOG2.copy0 is not dirty, but --ca is True. Copying...
        Saving updated hive to C:\Users\jungj\Desktop\Find_the_USB\registry_clean\C_Users_jungj_Desktop_Find_the_USB_reg
istry_DEFAULT.LOG2.copy0

Processing hive C:\Users\jungj\Desktop\Find_the_USB\registry\ntuser.dat.LOG1.copy0
        Hive C:\Users\jungj\Desktop\Find_the_USB\registry\ntuser.dat.LOG1.copy0 is not dirty, but --ca is True. Copying.
..
        Saving updated hive to C:\Users\jungj\Desktop\Find_the_USB\registry_clean\C_jungj_ntuser.dat.LOG1.copy0

Processing hive C:\Users\jungj\Desktop\Find_the_USB\registry\ntuser.dat.LOG2.copy0
        Hive C:\Users\jungj\Desktop\Find_the_USB\registry\ntuser.dat.LOG2.copy0 is not dirty, but --ca is True. Copying.
..
        Saving updated hive to C:\Users\jungj\Desktop\Find_the_USB\registry_clean\C_jungj_ntuser.dat.LOG2.copy0

Processing hive C:\Users\jungj\Desktop\Find_the_USB\registry\SAM.LOG1.copy0
        Hive C:\Users\jungj\Desktop\Find_the_USB\registry\SAM.LOG1.copy0 is not dirty, but --ca is True. Copying...
        Saving updated hive to C:\Users\jungj\Desktop\Find_the_USB\registry_clean\C_Users_jungj_Desktop_Find_the_USB_reg
istry_SAM.LOG1.copy0

Processing hive C:\Users\jungj\Desktop\Find_the_USB\registry\SAM.LOG2.copy0
        Hive C:\Users\jungj\Desktop\Find_the_USB\registry\SAM.LOG2.copy0 is not dirty, but --ca is True. Copying...
        Saving updated hive to C:\Users\jungj\Desktop\Find_the_USB\registry_clean\C_Users_jungj_Desktop_Find_the_USB_reg
istry_SAM.LOG2.copy0

Total processing time: 0.306 seconds
```

레지스트리 익스플로어 실행 시켜서

로드 하이브를 눌러서 아까 그 파일의 레지스트리 클린 파일을 눌러서 싹 다 열어준다



그 다음에 system으로 들어가서

이제 유에스비 어쩌구를 봐야하는데 usbstor를 찾는다 검색 기능 이용하면된다.

우선, enum폴더에서 찾아야한다.

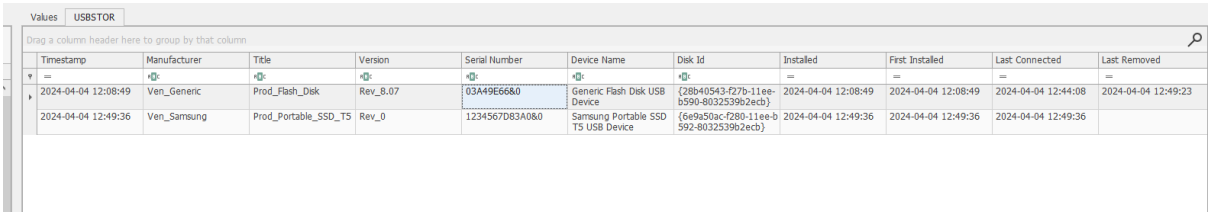
클릭해서 확대하면 시리얼 넘버가 보인다.

그리고 enum에 유에스비 폴더를 봐야한다.

폴더에 들어가면 아까 찾은 두개랑 같은거이다.

VID = 058F 이고 PID = 6387, 시리얼 넘버는 03A49E66이다.

다 더해서 플래그 제출하면 된다.


Values USBSTOR

Drag a column header here to group by that column

Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Disk Id	Installed	First Installed	Last Connected	Last Removed
=						=	=	=	=	
2024-04-04 12:08:49	Ven_Generic	Prod_Flash_Disk	Rev_8.07	03A49E66&0	Generic Flash Disk USB Device	{28b40543-f27b-11ee-b590-8032539b2ecb}	2024-04-04 12:08:49	2024-04-04 12:08:49	2024-04-04 12:44:08	2024-04-04 12:49:23
2024-04-04 12:49:36	Ven_Samsung	Prod_Portable_SSD_T5	Rev_0	1234567D83A0&0	Samsung Portable SSD T5 USB Device	{6e9a50ac-f280-11ee-b592-8032539b2ecb}	2024-04-04 12:49:36	2024-04-04 12:49:36	2024-04-04 12:49:36	

FLAG: DH{058F_6387_03A49E66}