문제3. 증거 사본에서 다음 각 항목에서 요구하는 정보를 찾고, 각 항목의 답안을 작성하시오.

1. MD5 값이 89d9ef6bedac8b82ac23b8e98ecceda8 인 파일을 찾고 파일명, 크기, 시간 정보를 구하라.

경로명	/vol_vol2/Users/forensic/Desktop/영화 시나리오/명량.pdf
파일명	명량.pdf
크기	1926536 Bytes
시간 정보	Modified : 2019-06-14 21:28:30 KST Accessed : 2019-06-15 10:16:26 KST Created : 2019-06-15 10:16:26 KST

2. 파일시스템이 생성된 날짜와 운영체제가 설치된 날짜를 구하라.

- NTFS 파일시스템이 생성된 날짜를 구하기 위해 '/vol_vol2/$MFT' 파일의 Created Time을 다음과 같이 참조함.

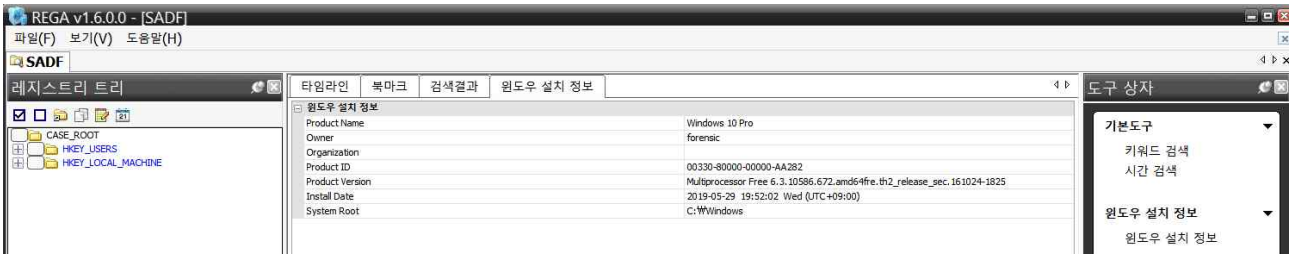
Metadata

Name:	/img_PBR복원_dd사본_vmdk.001/vol_vol2/$MFT
Type:	File System
MIME Type:	application/octet-stream
Size:	8650752
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-06-15 11:03:16 KST
Accessed:	2019-06-15 11:03:16 KST
Created:	2019-06-15 11:03:16 KST
Changed:	2019-06-15 11:03:16 KST
MD5:	3ee07c238a4f71b7a8fc1e1250bbb5d0
SHA-256:	64008de105ee8ce27be8b3eec892466dd7879062351d4fc8faee5e37e86be83a
Hash Lookup Results:	UNKNOWN
Internal ID:	10997

- 운영체제 설치된 날짜를 구하기 위해 레지스트리 파일을 추출함.

/vol_vol2/Users/forensic/NTUSER.DAT
/vol_vol2/Windows/System32/config/SYSTEM
/vol_vol2/Windows/System32/config/SAM
/vol_vol2/Windows/System32/config/SOFTWARE
/vol_vol2/Windows/System32/config/SECURITY

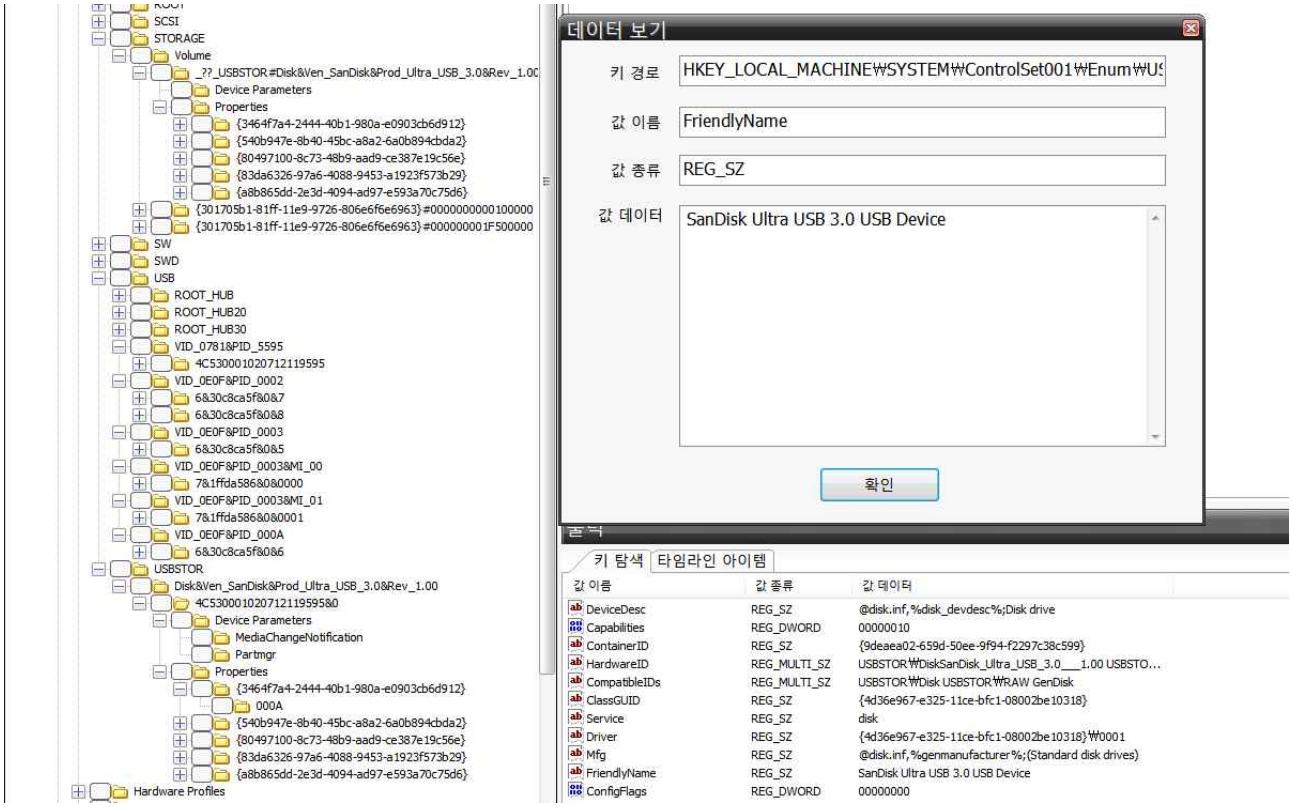
- REGA를 활용하여 추출한 레지스트리를 분석해 윈도우 운영체제가 설치된 날짜를 다음과 같이 확인함.



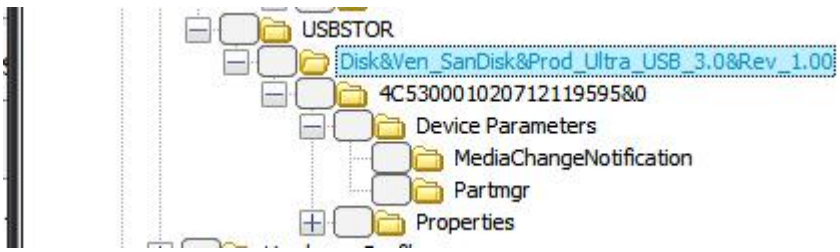
파일시스템이 생성된 날짜	2019-06-15 11:03:16 KST
운영체제가 설치된 날짜	2019-05-29 19:52:02 Wed (UTC+09:00)

3. 증거사본에 해당 시스템에 연결된 USB Drive Name, Vender, Serial Number를 구하라.

- REGA를 이용하여 'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00\4C530001020712119595&0' 키 내 'FriendlyName' 값 확인함.



'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00' 키 내 Ven_SanDisk로 Vender정보가 Sandisk임을 확인

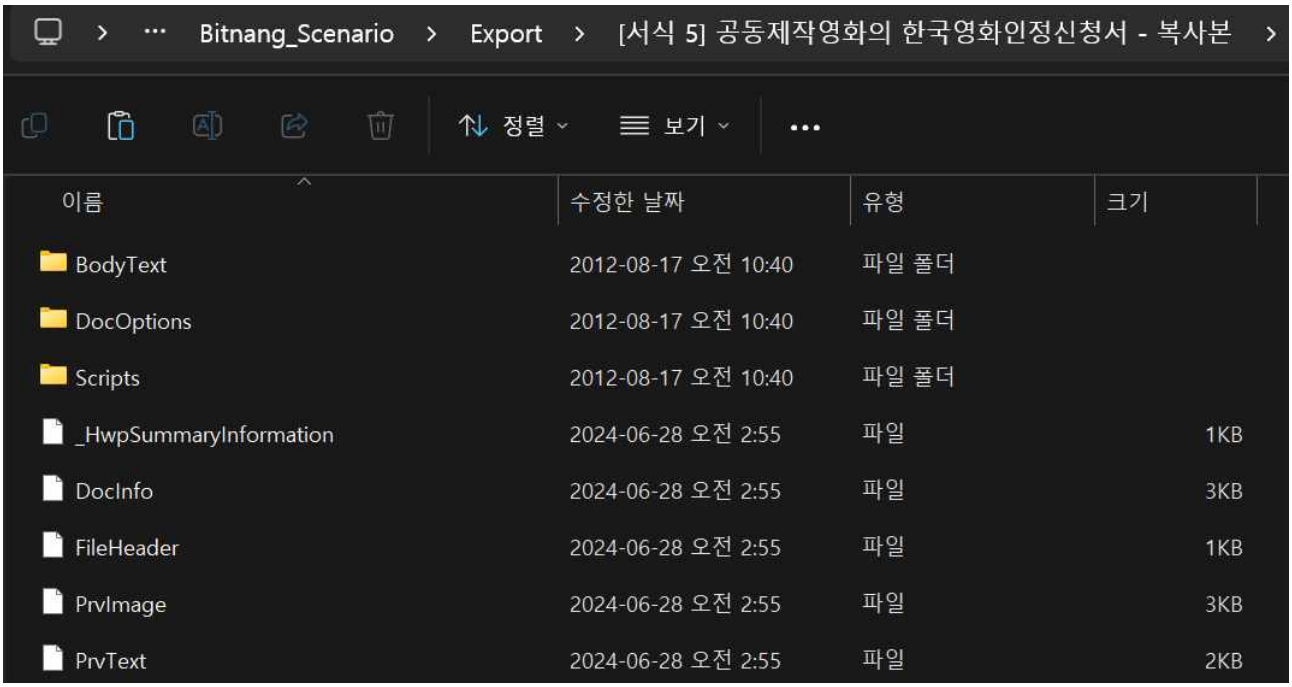


‘HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00\4C530001020712119595&0’의 키를 확인하여 Serial Number 구함.

USB Drive Name	SanDisk Ultra USB 3.0 USB Device (PID : 5595)
Vender	SanDisk (VID : 0781)
Serial Number	4C530001020712119595

4. “[서식 5] 공동제작영화의 한국영화인정신청서.hwp” 파일의 내부구조를 파악하고, 지은이(Author)을 파악하라.

- ‘/vol_vol2/Users/forensic/Desktop/영화 서식/[서식 5] 공동제작영화의 한국영화인정신청서.hwp’의 내부구조 파악을 위해 추출 후 .zip파일로 확장자 변환하여 압축 푼 결과 내부구조가 다음과 같음을 확인함.

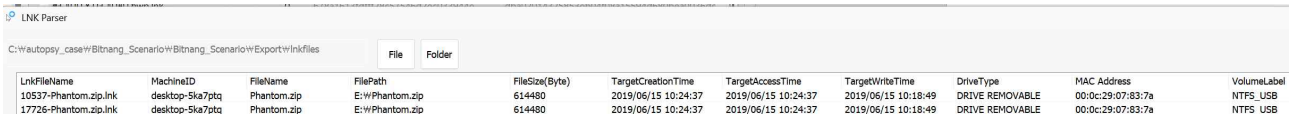


Metadata

Name:	/img_PBR복원_dd사본_vmdk.001/vol_vol2/Users/forensic/Desktop/영화 서식/[서식 5] 공동제작영화의 한국영화인정신청서.hwp
Type:	File System
MIME Type:	application/x-hwp-v5
Size:	18944
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2019-06-14 21:49:49 KST
Accessed:	2019-06-15 10:15:58 KST
Created:	2019-06-15 10:15:58 KST
Changed:	2019-06-15 11:05:13 KST
MD5:	68a143208e075ca63c6171553d628a5b
SHA-256:	b8c8e5c41d9c17b53b3c1735af288a32b39fb2d31bb1bf5af5576b8b8686c482
Hash Lookup Results:	UNKNOWN
Internal ID:	10683

5. 외부저장장치에 연결된 링크파일을 확인하고 외부저장장치의 MAC주소, 볼륨 시리얼 넘버, 대상파일 크기를 확인하라.

- LNKParser를 활용하여 링크파일들을 추출한 후 DriveType이 Removable인 '10537-Phantom.zip.lnk'와 '17726-Phantom.zip.lnk'를 확인함.



MAC주소	00:0c:29:07:83:7a
볼륨 시리얼 넘버	5c3da927
대상파일 크기	614480 Bytes