Forensic Study - 8
Windows Registry Analysis

2017.12.07

KUICS

2014210009 주어진

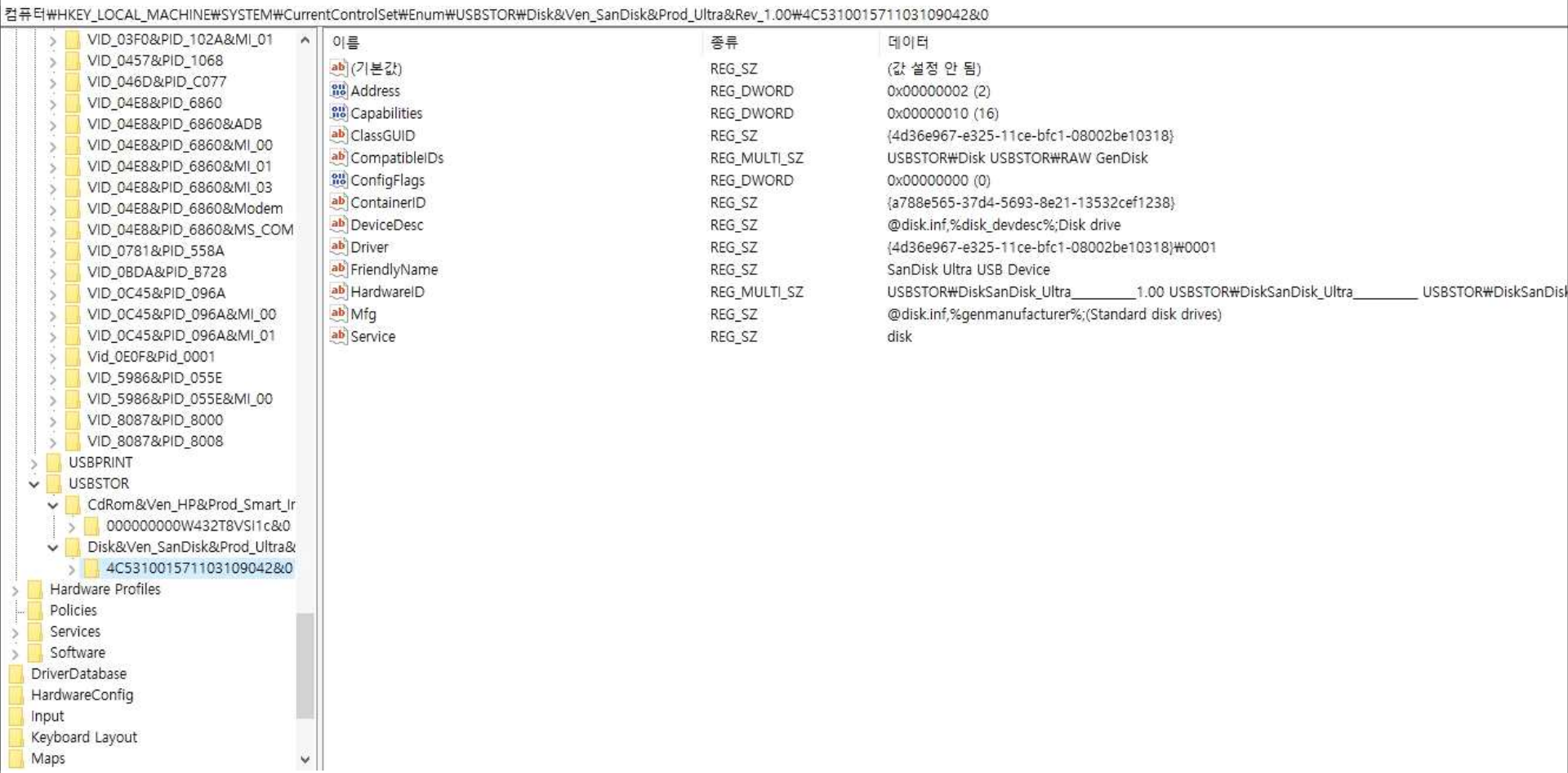
목차

Registry Path

HKLM₩SYSTEM₩CurrentControlSet₩Control₩hivelist : 하이브의 위치를 저장한다. (가장 먼저 봐야할 곳)

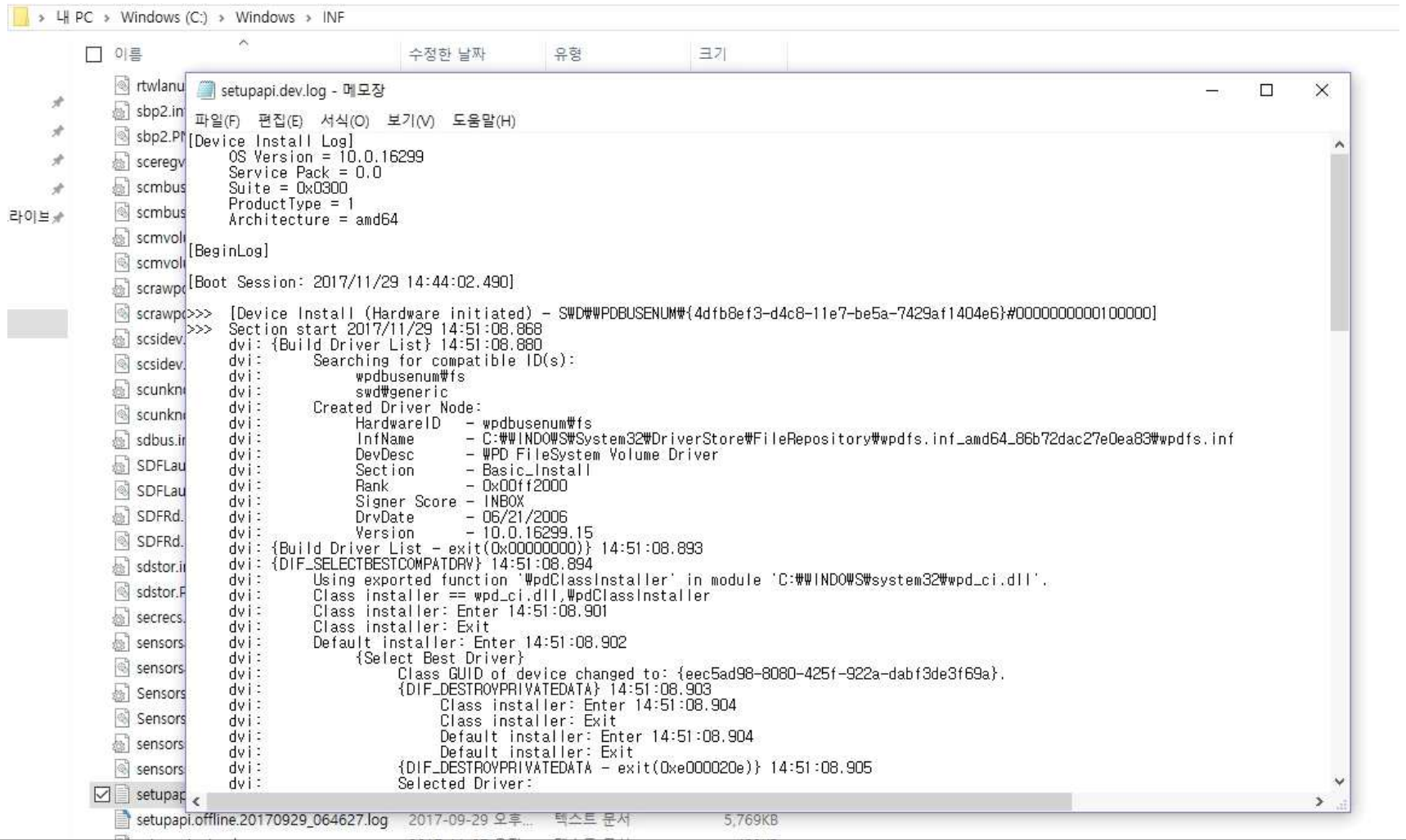
Registry Path

HKLM₩SYSTEM₩CurrentControlSet₩Enum₩USBSTOR₩... : 이 컴퓨터와 연결한 적이 있는 모든 USB Storage에 대한 정보 저장.



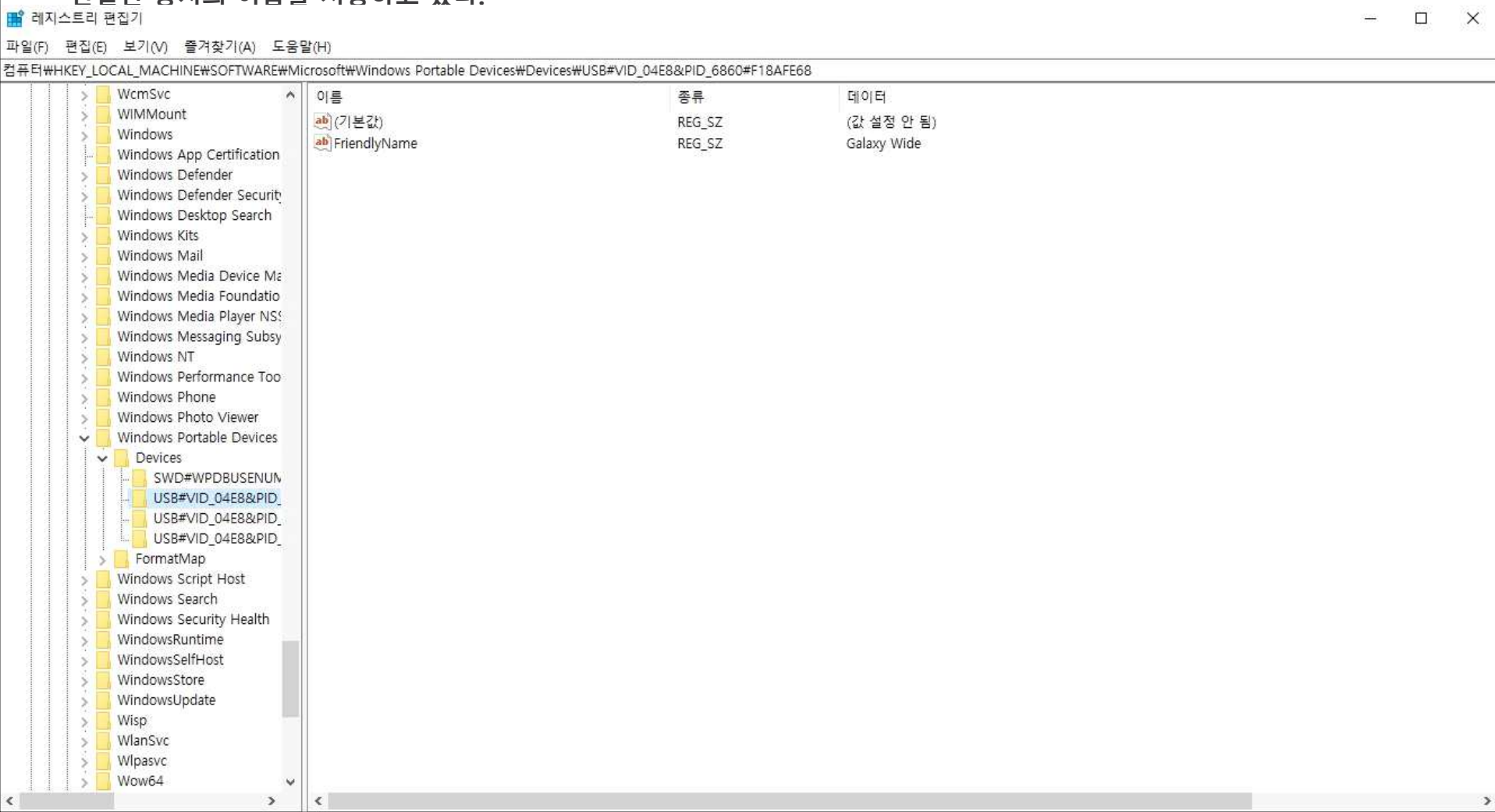
Registry Path (Additional)

C:₩Windows₩INF₩setupapi.dev.log에는 USB 관련한 정보가 저장되어 있다.



Registry Path

HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩USB₩... (VID : 회사 아이디, PID : 제품 아이디) : 연결된 장치의 이름을 저장하고 있다.

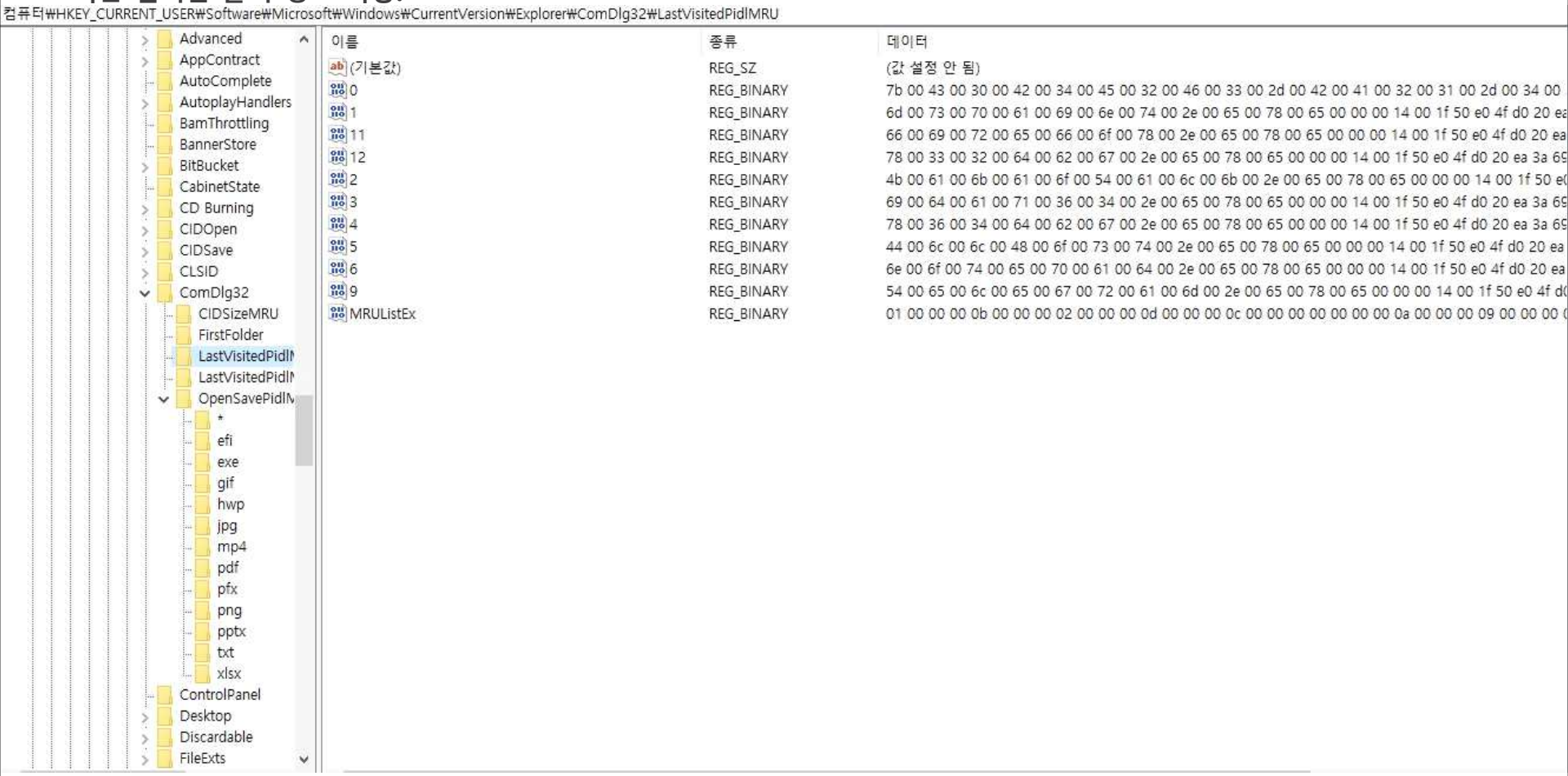


Registry Path

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RecentDocs : 최근 열어본 문서 목록 저장

Registry Path

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedPidlMRU :
최근 열어본 폴더 경로 저장.

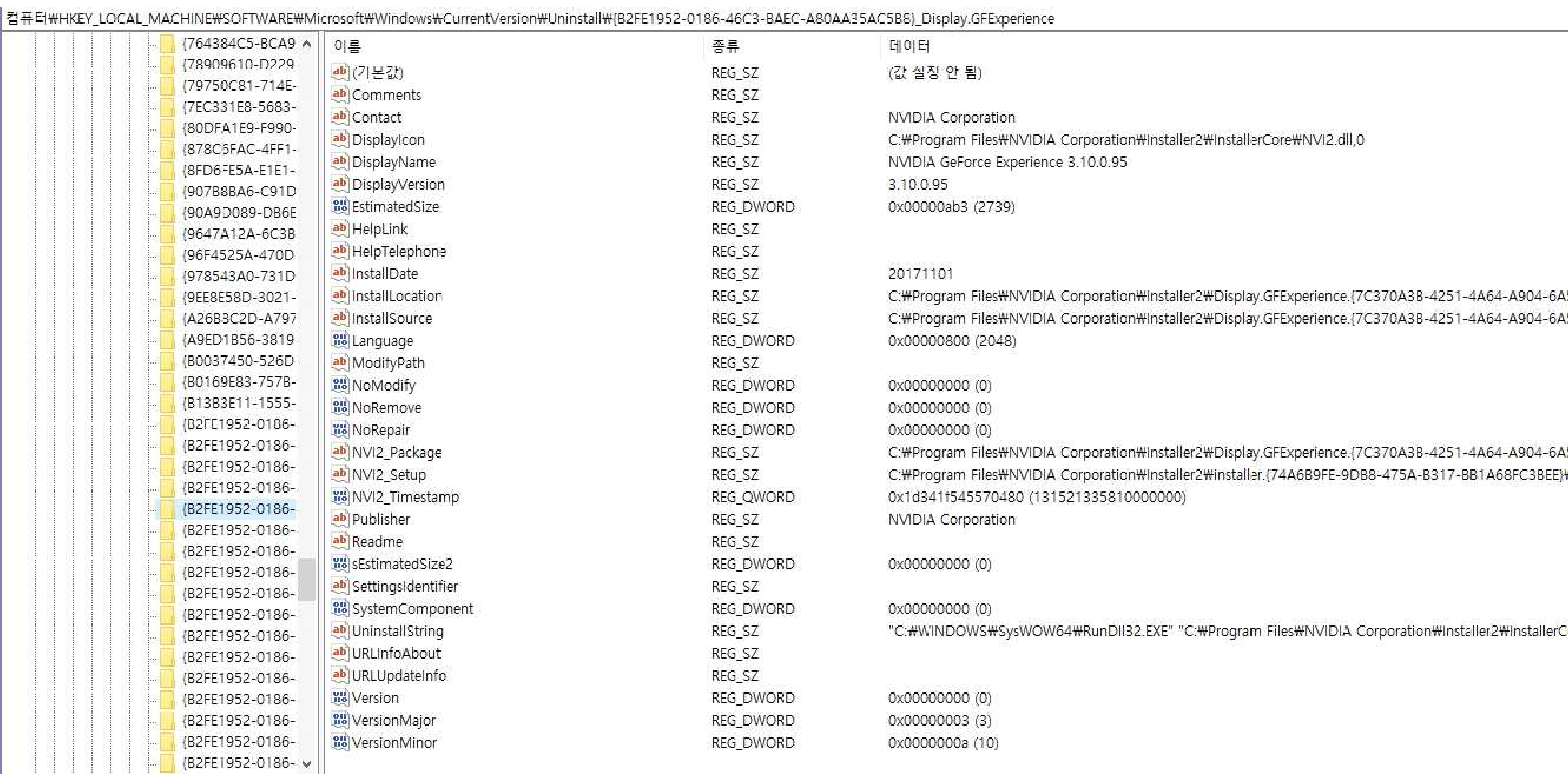


Registry Path

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩OpenSavePidlMRU :
최근 열어보거나 저장한 파일을 확장자마다 나누어서 저장.

Registry Path

HKLM₩SOFTWARE₩Microsof₩Windows₩CurrentVersion₩Uninstall :
프로그램 추가/제거 목록



컴퓨터₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Uninstall₩{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}_Display.GFExperience

{764384C5-BCA9
{78909610-D229-
{79750C81-714E-
{7EC331E8-5683-
{80DFA1E9-F990-
{878C6FAC-4FF1-
{8FD6FE5A-E1E1-
{907B8BA6-C91D
{90A9D089-DB6E
{9647A12A-6C3B
{96F4525A-470D-
{978543A0-731D
{9EE8E58D-3021-
{A26B8C2D-A797
{A9ED1B56-3819-
{B0037450-526D-
{B0169E83-757B-
{B13B3E11-1555-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-
{B2FE1952-0186-

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
Comments	REG_SZ	
Contact	REG_SZ	NVIDIA Corporation
DisplayIcon	REG_SZ	C:₩Program Files₩NVIDIA Corporation₩Installer2₩InstallerCore₩NVI2.dll,0
DisplayName	REG_SZ	NVIDIA GeForce Experience 3.10.0.95
DisplayVersion	REG_SZ	3.10.0.95
EstimatedSize	REG_DWORD	0x00000ab3 (2739)
HelpLink	REG_SZ	
HelpTelephone	REG_SZ	
InstallDate	REG_SZ	20171101
InstallLocation	REG_SZ	C:₩Program Files₩NVIDIA Corporation₩Installer2₩Display.GFExperience.{7C370A3B-4251-4A64-A904-6A
InstallSource	REG_SZ	C:₩Program Files₩NVIDIA Corporation₩Installer2₩Display.GFExperience.{7C370A3B-4251-4A64-A904-6A
Language	REG_DWORD	0x00000800 (2048)
ModifyPath	REG_SZ	
NoModify	REG_DWORD	0x00000000 (0)
NoRemove	REG_DWORD	0x00000000 (0)
NoRepair	REG_DWORD	0x00000000 (0)
NVI2_Package	REG_SZ	C:₩Program Files₩NVIDIA Corporation₩Installer2₩Display.GFExperience.{7C370A3B-4251-4A64-A904-6A
NVI2_Setup	REG_SZ	C:₩Program Files₩NVIDIA Corporation₩Installer2₩installer.{74A6B9FE-9DB8-475A-B317-BB1A68FC3BEE}₩
NVI2_Timestamp	REG_QWORD	0x1d341f545570480 (131521335810000000)
Publisher	REG_SZ	NVIDIA Corporation
Readme	REG_SZ	
sEstimatedSize2	REG_DWORD	0x00000000 (0)
SettingsIdentifier	REG_SZ	
SystemComponent	REG_DWORD	0x00000000 (0)
UninstallString	REG_SZ	"C:₩WINDOWS₩SysWOW64₩RunDll32.EXE" "C:₩Program Files₩NVIDIA Corporation₩Installer2₩InstallerC
URLInfoAbout	REG_SZ	
URLUpdateInfo	REG_SZ	
Version	REG_DWORD	0x00000000 (0)
VersionMajor	REG_DWORD	0x00000003 (3)
VersionMinor	REG_DWORD	0x0000000a (10)

Registry Path (Additional)

6주차때 써놓은 중요한 것들.

Network Interface : HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NerworkCards

MAC Address : HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Class₩{4d36e972-e325-11ce-bfc1-08002be10318}

WireLess SSID : HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WlanSvc₩Interfaces₩$ID₩Profiles

Auto Start
-> HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Run
-> HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩RunOnce
-> HKEY_LOCAL_MACHINE₩SOFTWARE₩WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩Run
-> HKEY_LOCAL_MACHINE₩SOFTWARE₩WOW6432Node₩Microsoft₩Windows₩CurrentVersion₩RunOnce
-> HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services

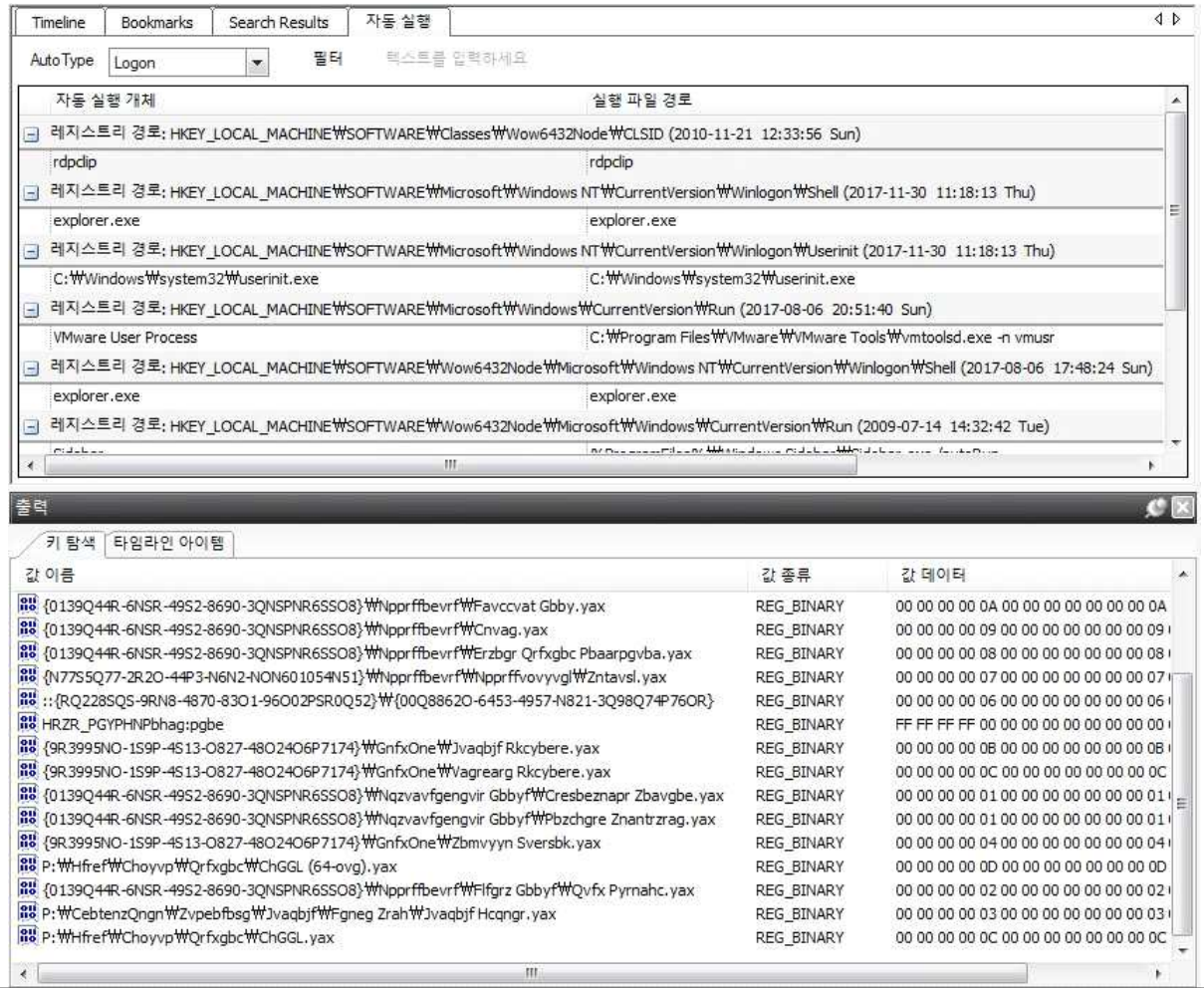
Practice With Tool - REGA

다운로드 : http://forensic.korea.ac.kr/tools/rega.html

예제 하이브 다운로드 : https://drive.google.com/file/d/1EvvKzoM78r38G1cdAuMyLbWXTA4cvWU8/view

Practice With Tool - REGA

제공한 하이브 파일을 로드해보자. Run도 알 수 있고, 저장장치 / 네트워크 드라이브 / 최근 열어본 문서등을 쉽게 알 수 있다.



Practice With Tool - REGA

제공한 하이브 파일을 로드해보자. Run도 알 수 있고, 저장장치 / 네트워크 드라이브 / 최근 열어본 문서등을 쉽게 알 수 있다.

(저장 장치의 경우 CODEGATE 2011 YUT 문제로도 출제 됐었고, 툴만 사용하면 쉽게 문제 해결이 가능했다.)

장치 종류	장치 이름	드라이브명	볼륨 명	시리얼 넘버	ParentIdPrefix	최초연결시각 (SetupAPI L...	부팅
FDC	플로피 디스크 드라이브	A:		6&3b4c39bd&0&0		2017-08-06 17:46:31 Sun	2017
IDE	NECVMWar VMware SATA CD01 ATA Device	D:		6&373888b8&0&...		2017-08-06 17:46:25 Sun	2017
SCSI	VMware, VMware Virtual S SCSI Disk Device			5&22be343f&0&...		2017-08-06 17:46:11 Sun	2017
USB	USB Root Hub			5&3bb57b&0	6&b77da92&0		
USB	USB Root Hub			5&299e1c9f&0			
USB	USB Composite Device (Port_#0001.Hub_#0002)			f18afe68	7&da5495d&0	2017-11-17 17:11:25 Fri	2017
USB	Galaxy Wide		Galaxy Wide	7&da5495d&0&0...		2017-11-17 17:11:25 Fri	2017
USB	CDC Serial (0002.0003.0000.001.000.000.000....			7&da5495d&0&0...			
USB	SAMSUNG_Android (0002.0003.0000.001.000.0...			7&da5495d&0&0...			
USB	Generic USB Hub (Port_#0002.Hub_#0001)			6&b77da92&0&2			
USB	USB Composite Device (Port_#0001.Hub_#0001)			6&b77da92&0&1	7&2a7d3009&0	2017-08-06 17:46:32 Sun	2017
USB	USB 입력 장치 (0002.0000.0000.001.000.000.0...			7&2a7d3009&0&...	8&17be0303&0		
USB	USB 입력 장치 (0002.0000.0000.001.000.000.0...			7&2a7d3009&0&...	8&2f818f48&0		

Practice With Tool - REGA

예시 문제.

Chobo는 윈도우 7을 설치하고 인터넷 서핑을 하는 도중, 바탕화면에 있는 이상한 프로그램 2개를 실행시켰다.
프로그램을 실행시키자 컴퓨터는 먹통이 되는 지경에 이르렀고, 다급히 레지스트리 하이브라도 복사해 성공적으로 클라우드에 업로드 할 수 있었다.

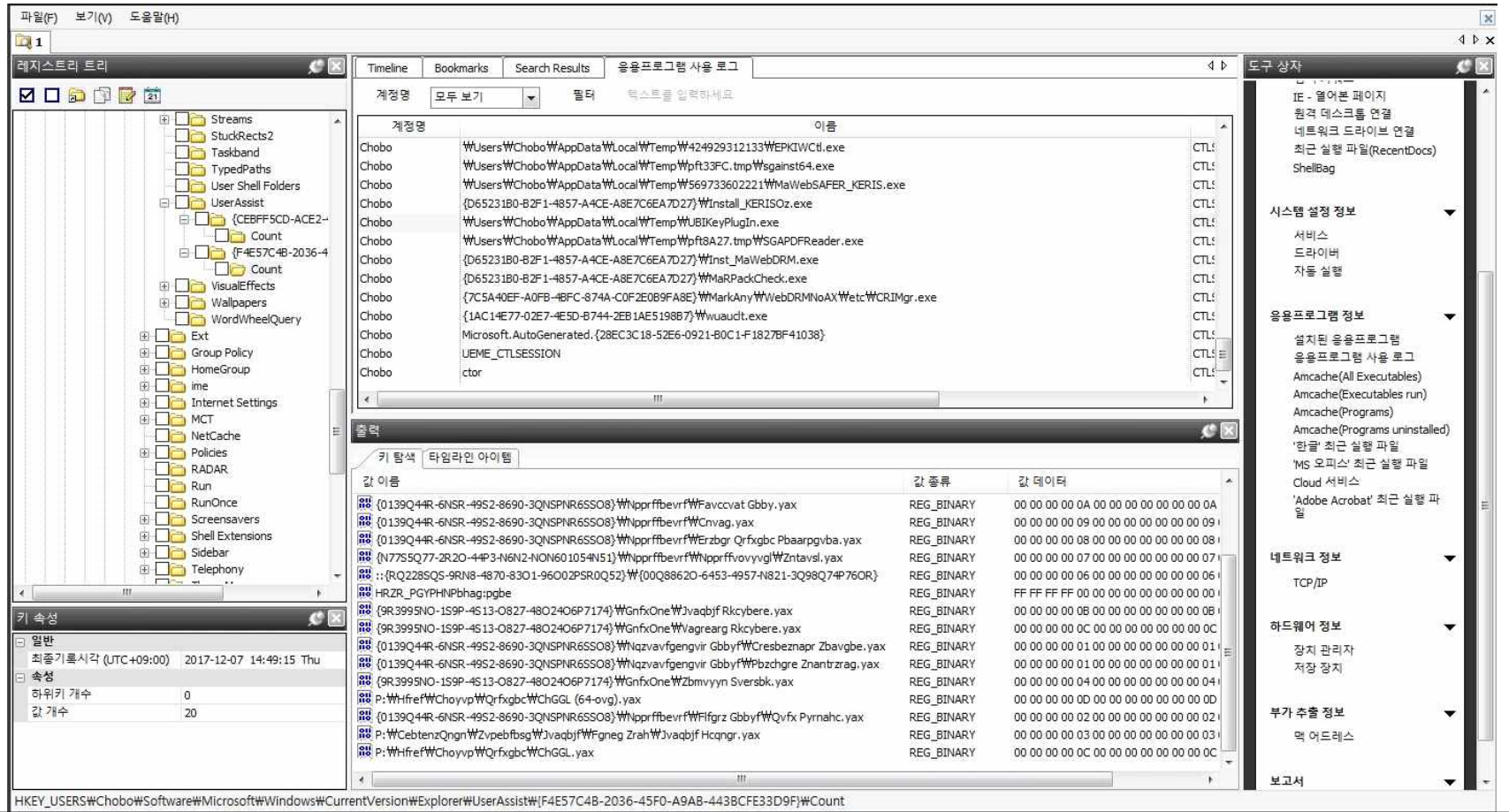
이 이상한 프로그램은 Windows 시스템에서 중요한 프로세스 이름과 비슷하거나 똑같이 네이밍됐으며, Chobo도 깜빡 속아 실행시켰다고 한다.

이 프로그램은 무엇일까?

Practice With Tool - REGA

답 : HKCU₩Software₩Windows₩CurrentVersion₩Explorer₩UserAssist에 존재한다.

P:₩Hfref₩Pubob₩Qrfxgbc₩ffzf.rkr -> ROT13이므로 해석하면 C:₩Users₩Chobo₩Desktop₩ssms.exe
P:₩Hfref₩Pubob₩Qrfxgbc₩fipubfg.rkr -> 역시 해석하면 C:₩Users₩Chobo₩Desktop₩svchost.exe



감사합니다

내부 CTF에 포렌식 스터디에서 배운 이론들을 활용한 문제를 출제할 예정.

마지막 스터디입니다.