

# 1주차 스터디

스터디 계획 및 레지스트리 포렌식 설명

# 앞으로 배우게 될 내용들

- 윈도우 포렌식
  - 레지스트리 포렌식
  - 이벤트 로그 분석
  - 브라우저 포렌식
  - Ink (링크파일), Prefetch 분석
  - 파일시스템 포렌식
  - ...
- 메모리 포렌식
- 침해사고 분석 (KEEPER CTF - IR-1, IR-2, IR-3, IR-4)
- ...

# 아티팩트

- 운영체제나 애플리케이션을 사용하면서 생성되는 흔적
- 생성 증거
  - 시스템이나 애플리케이션이 자동으로 생성한 데이터
  - 예:) 레지스트리, 프리/슈퍼패치, 이벤트 로그
- 보관 증거
  - 사람의 사상이나 감정을 표현하기 위해 작성한 데이터
  - 예:) 직접 작성한 메일 내용, 블로그 및 소셜 네트워크 작성 내용, 직접 작성한 문서
- 컴퓨터를 사용할 때 편리하다. → 그만큼 많은 정보가 저장되어 있다.
  - 최근 열람 문서, 파일, 브라우저 즐겨찾기 등

# 아티팩트

새로운 버전의 윈도우가 출시됨에 따라 마이크로소프트는 '사용자 경험'을 향상시키려고 노력해왔고, 그렇게 함으로써 어떤 면에서는 점점 더 많은 사용자 활동을 기록하고 추적할 필요가 생겼다. 그 결과 디지털 분석가가 활용할 수 있는 정보는 점점 늘어났다. 윈도우 7에서는 윈도우 XP에 비해 윈도우 이벤트 로그 파일뿐만 아니라 운영체제와 애플리케이션에 의해 기록되는 사용자별 행위 관련 정보 또한 현저하게 증가했다. 윈도우 10에서는 이보다 더 많이 증가했다.

[Windows 환경에서 침해 시스템 분석하기 - p89, Eng](#)

# 법 이야기

- 형사소송법 제106, 107, 109조 개정 2011. 7. 18

## 제10장 압수와 수색

- 제106조(압수) ①법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. <개정 2011. 7. 18.>
- ②법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.
- ③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 “정보저장매체등”이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다. <신설 2011. 7. 18.>
- ④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011. 7. 18.>
- 제107조(우체물의 압수) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 우체물 또는 「통신비밀보호법」 제2조제3호에 따른 전기통신(이하 “전기통신”이라 한다)에 관한 것으로서 체신관서, 그 밖의 관련 기관 등이 소지 또는 보관하는 물건의 제출을 명하거나 압수를 할 수 있다. <개정 2011. 7. 18.>
- ② 삭제 <2011. 7. 18.>
- ③제1항에 따른 처분을 할 때에는 발신인이나 수신인에게 그 취지를 통지하여야 한다. 단, 심리에 방해될 염려가 있는 경우에는 예외로 한다. <개정 2011. 7. 18.>
- 제108조(임의 제출물 등의 압수) 소유자, 소지자 또는 보관자가 임의로 제출한 물건 또는 유류한 물건은 영장없이 압수할 수 있다.
- 제109조(수색) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 피고인의 신체, 물건 또는 주거, 그 밖의 장소를 수색할 수 있다. <개정 2011. 7. 18.>
- ②피고인 아닌 자의 신체, 물건, 주거 기타 장소에 관하여는 압수할 물건이 있음을 인정할 수 있는 경우에 한하여 수색할 수 있다.

# 법 이야기

- 형사소송법 제313조 개정 2016. 5. 29

**제313조(진술서등)** ① 전2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태하에서 행하여진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다. <개정 2016.5.29.>

② 제1항 본문에도 불구하고 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다. <개정 2016.5.29.>

# 디지털 포렌식 5대 원칙

이름	내용
정당성의 원칙	적법한 절차에 따르지 아니하고 수집한 증거는 법적 효력을 상실한다. (위법수집증거배제법칙, 독수독과이론)
재현의 원칙	동일한 조건에서 반복 시에도 같은 결과가 도출되어야 한다.
무결성의 원칙	디지털 데이터를 수집한 이후에도 변조되지 않았음을 입증할 수 있어야 한다. 부득이하게 다른 확장자로 저장해야 한다면 동일성을 입증해야 한다.
연계 보관성의 원칙	증거 획득, 이송, 분석, 보관, 법정제출의 각 단계의 담당자 및 책임자가 명확해야 한다.
신속성의 원칙	휘발성 증거 수집의 경우 신속한 조치를 통해 지체 없이 진행되어야 한다.

# 필요한 선수 지식

- Python

- 스터디에서 배운 내용들을 활용하여 간단한 도구 개발 예정
- 이미 개발되어 있는 라이브러리를 활용
  - 레지스트리 - winreg
  - 이벤트 로그 - python-evtx, libevtx
  - ...
- Ink, Prefetch의 경우 직접 파서를 제작할 예정



# 왜 도구를 만들어보는거지?

- 사실 이미 웬만한 도구는 이미 구현되어 있다.
  - 스터디에서도 이런 도구들을 활용하여 실습할 예정
- 그러나 어떤 구조를 파싱해서 어떻게 동작하는지 간단하게 알 필요는 있다.
  - 이를 아는 사람과 모르고 그저 도구 사용법만 숙지하는 사람의 차이는 존재한다.
  - 추후에 자기만의 도구가 필요할 수도 있다.
- 도구화되어 있지 않은 구조는 어떻게 분석해야 할까?
  - 직접 개발해야한다.
  - 디지털 포렌식 챌린지 문제의 경우 파서, 도구 개발 등의 문제도 나온다.  
(영상 복구, 손상된 파일 복구 등) → 도구 개발 역량이 필요하다.

# 레지스트리 포렌식

- 레지스트리는 윈도우 운영체제에서 설정과 관련된 정보를 담고있는 데이터베이스

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY\_CURRENT\_USER\Software\Bandizip

이름	종류	데이터
RecentArchive0	REG_SZ	C:\Users\hyuunnnn\Downloads\63dcc786c3bd817a6f3e61cbb6a4e3fd (2).zip
RecentArchive1	REG_SZ	C:\Users\hyuunnnn\Downloads\63dcc786c3bd817a6f3e61cbb6a4e3fd.zip
RecentArchive2	REG_SZ	C:\Users\hyuunnnn\Desktop\sp12.zip

반디집 (스탠더드)

파일(F) 편집(E) 찾기(I) 설정(S) 보기(V) 도구(T) 도움말(A)

압축 파일 열기 Ctrl+O

최근 파일

새로 압축 Ctrl+N

압축 파일 닫기 F4

다른 이름으로 저장

압축 파일 삭제 Ctrl+Del

압축 파일 완전 삭제 Shift+Ctrl+Del

압축 파일이 있는 폴더 열기

압축 파일 테스트 Ctrl+T

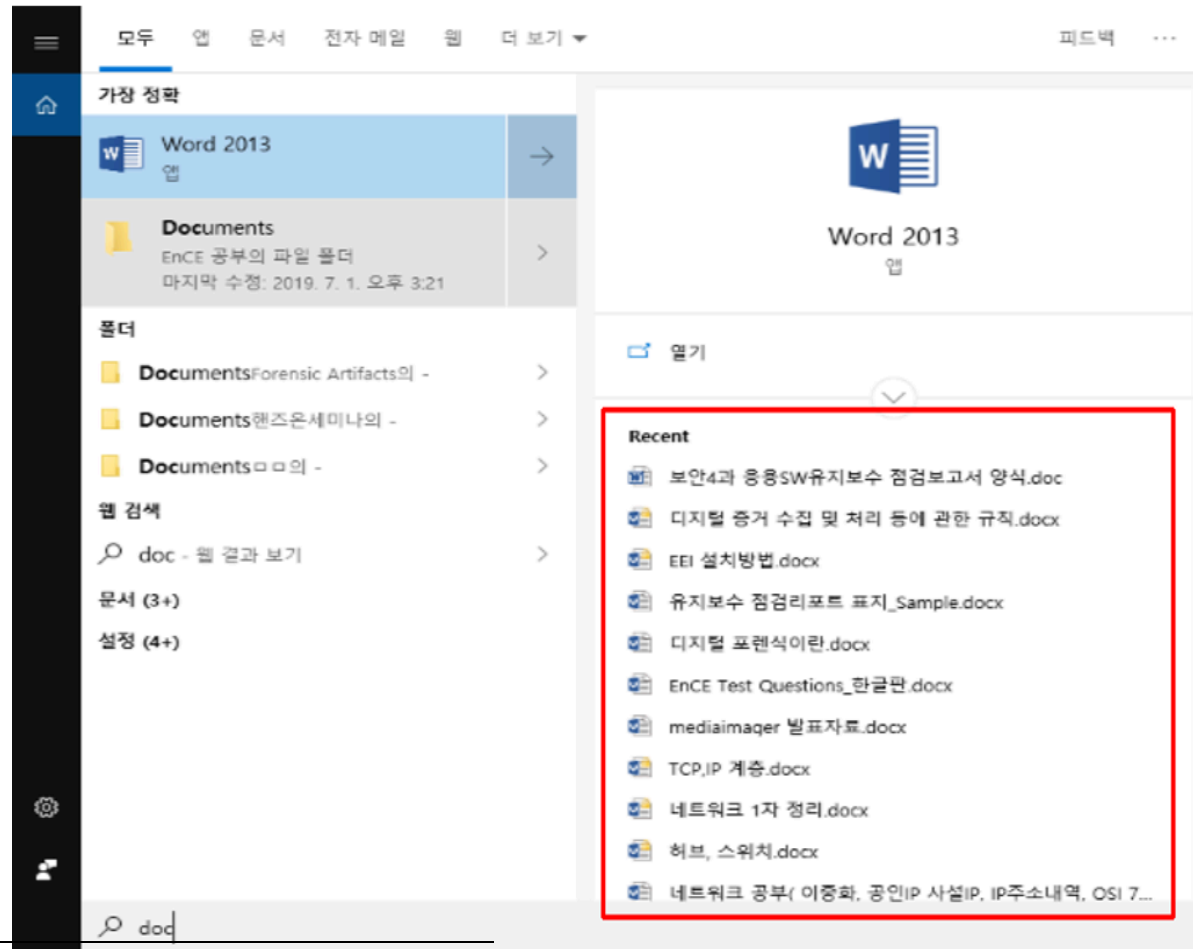
압축 파일 악성코드 검사 Ctrl+I

압축 풀기 Ctrl+E

C:\Users\hyuunnnn\Downloads\63dcc786c3bd817a6f3e61cbb6a4e3fd (2).zip  
C:\Users\hyuunnnn\Downloads\63dcc786c3bd817a6f3e61cbb6a4e3fd.zip  
C:\Users\hyuunnnn\Desktop\sp12.zip  
C:\Users\hyuunnnn\Downloads\Nespa-master.zip  
C:\Users\hyuunnnn\Downloads\sample.zip  
C:\Users\hyuunnnn\Desktop\22년 2학기#공학작문및발표#공학작문 과제 2번.zip  
C:\Users\hyuunnnn\Desktop\22년 2학기#공학작문및발표#과제 2번 - 나쁜글 revi...  
C:\Users\hyuunnnn\Downloads\과제 2번 - 나쁜글 review.zip  
C:\Users\hyuunnnn\Downloads\공학작문 과제 2번.zip  
C:\Users\hyuunnnn\Downloads\volatility3-2.0.1.zip  
C:\Users\hyuunnnn\Desktop#  
C:\Users\hyuunnnn\Downloads#  
C:\Users\hyuunnnn\Desktop\22년 2학기#자료구조#code#별보기#  
C:\Users\hyuunnnn\Desktop\test#a#  
C:\Windows\System32\cmd.exe#  
C:\Users\hyuunnnn\Desktop\302#templates#

# 레지스트리 포렌식

- 레지스트리는 윈도우 운영체제에서 설정과 관련된 정보를 담고있는 데이터베이스

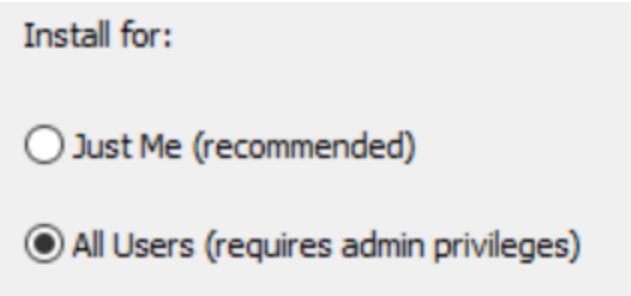


<sup>1</sup> <http://www.forensic-artifacts.com/windows-forensics/recentfiles>

# 레지스트리 구조

- 키와 값의 조합으로 구성되어 있다. (키는 폴더, 값은 파일과 비슷한 개념)

하이버	내용
HKEY_CLASSES_ROOT	확장자와 연결된 응용프로그램 정보
HKEY_CURRENT_USER	현재 로그인한 사용자의 설정 정보
HKEY_LOCAL_MACHINE	모든 사용자에게 적용되는 설정 정보 및 시스템 정보
HKEY_USERS	각 사용자에 대한 설정 정보를 담고 있다. HKEY_USERS가 HKEY_CURRENT_USER 보다 상위 개념



← 프로그램 설치 과정에서 유형을 선택하는 화면 (Anaconda)

# 레지스트리 구조

- 해당 파일들이 모여서 레지스트리 구조를 구성한다.

레지스트리 경로	파일 경로
HKLM\SYSTEM	%WINDIR%\SYSTEM32\Config\SYSTEM
HKLM\SAM	%WINDIR%\SYSTEM32\Config\SAM
HKLM\SECURITY	%WINDIR%\SYSTEM32\Config\SECURITY
HKLM\SOFTWARE	%WINDIR%\SYSTEM32\Config\SOFTWARE
HKEY_USERS\{User SID}	%UserProfile%\NTUSER.DAT
HKEY_USERS\{User SID}_Classes	%UserProfile%\AppData\Local \Microsoft\Windows\UsrClass.dat

- NTUSER.DAT , UsrClass.dat 파일은 각 유저마다 별도의 파일로 존재

# 레지스트리 분석

- Timezone 설정 확인
  - HKLM\SYSTEM\ControlSet00?\Control\TimeZoneInformation

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
ActiveTimeBias	REG_DWORD	0xffffffff (4294966756)
Bias	REG_DWORD	0xffffffff (4294966756)
DaylightBias	REG_DWORD	0xffffffff (4294967236)
DaylightName	REG_SZ	@tzres.dll,-621
DaylightStart	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DynamicDaylightT...	REG_DWORD	0x00000000 (0)
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-622
StandardStart	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Korea Standard Time













## Bias

The current bias for local time translation on this computer, in minutes. The bias is the difference, in minutes, between Coordinated Universal Time (UTC) and local time. All translations between UTC and local time are based on the following formula:

UTC = local time + bias

# 레지스트리 분석

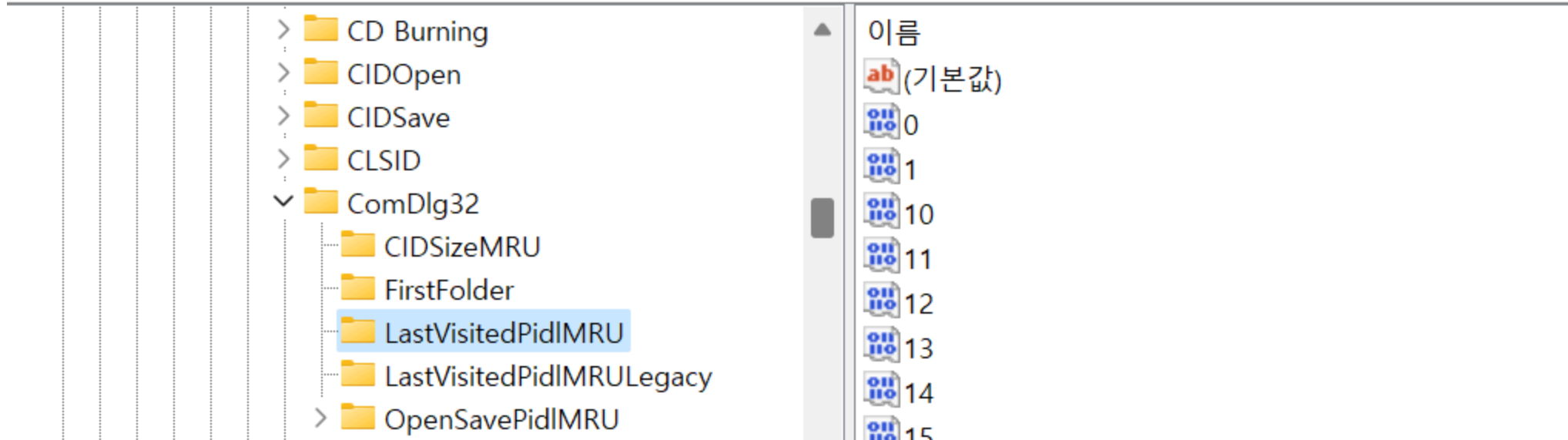
- Autorun
  - HKLM, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    - 컴퓨터가 부팅될 때마다 실행된다.
  - HKLM, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
    - 윈도우 시작 시 1번만 실행되며 실행 후에는 레지스트리에서 자동으로 삭제된다. (일회성)

이름	종류	데이터
 (기본값)	REG_SZ	(값 설정 안 됨)
 com.squirrel.slack.slack	REG_SZ	"C:\Users\Whyuunnnn\AppData\Local\slack\slack.exe" --process-start-args --startup
 Discord	REG_SZ	"C:\Users\Whyuunnnn\AppData\Local\Discord\Update.exe" --processStart Discord.exe
 Docker Desktop	REG_SZ	C:\Program Files\Docker\Docker\Docker Desktop.exe -Autostart
 electron.app.Notion	REG_SZ	C:\Users\Whyuunnnn\AppData\Local\Programs\Notion\Notion.exe --open-at-login
 flemozi	REG_SZ	C:\Users\Whyuunnnn\Downloads\Flemozi\Flemozi.exe --headless
 JetBrains Toolbox	REG_SZ	"C:\Users\Whyuunnnn\AppData\Local\JetBrains\Toolbox\bin\jetbrains-toolbox.exe" --minimize
 KakaoTalk	REG_SZ	"C:\Program Files (x86)\Kakao\KakaoTalk\KakaoTalk.exe" -bystartup
 MicrosoftEdgeAutoLau...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start
 Parsec.App.0	REG_SZ	C:\Program Files\Parsec\parsecd.exe app_silent=1
 Sync On Mobile	REG_SZ	
 Windows Cleaner	REG_SZ	"C:\Users\Whyuunnnn\AppData\Roaming\SubDir\Client.exe"

# 레지스트리 분석

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\
  - OpenSavePidlMRU: 열기/저장 기능에 사용된 파일
  - LastVisitedPidlMRU: 열기/저장 기능을 사용한 응용 프로그램

컴퓨터\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU





# 레지스트리 분석

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\
  - OpenSavePidIMRU: 열기/저장 기능에 사용된 파일
  - LastVisitedPidIMRU: 열기/저장 기능을 사용한 응용 프로그램
- RegistryExplorer 도구를 사용한 결과

Extension	Value Name	Mru Position	Absolute Path
Ⓜc	Ⓜc	=	Ⓜc
a	0		0 This PC\Documents\GitHub\java-lotto-game\whyunnn.zip.a
a60	0		0 Desktop\test.a60
bas	0		0 Documents\GitHub\CB2600105-061\과제 3\I
bdf	12		0 Documents\GitHub\CB2600778-002\week11(2)\logiccircuit\nine_week_2.bdf
bin	0		0 Desktop\maum.bin
bsf	1		0 Downloads\Automatic-Traffic-System-main\Automatic_Traffic_System\2seg.bsf
bt	0		0 Desktop\PDF.bt
c	19		0 Desktop\wylex.c

OpenSavePidIMRU

Value Name	Mru Position	Executable	Absolute Path
Ⓜc	=	Ⓜc	Ⓜc
4	0	chrome.exe	Desktop
3	1	Code.exe	Documents\GitHub\2024-Forensic-Study\marp
0	2	KakaoTalk.exe	Desktop
6	3	PickerHost.exe	Desktop\kaspersky_course\07.DRIVER
2	4	brave.exe	Desktop
17	5	AFFINE.exe	Downloads
7	6	{479C25C7-4E3C-4C5E-B7B4-127531CE09FC}	This PC\C:\whyunnn\
22	7	Notion.exe	Documents\GitHub\KEEPER_CTF\2024\IR
16	8	RegistryExplorer.exe	E:\240103
19	9	NTFS Log Tracker v1.71.exe	E:\240103

LastVisitedPidIMRU

# 레지스트리 분석

- UserAssist
  - HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
    - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count: 실행파일 기록
    - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count: 링크파일 기록



컴퓨터\WHKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count

이름	이름
Substrate	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\WCvpixeUbfgr.rkr
TabletMode	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wehaqyy32.rkr
Taskband	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\WFlgrzCebcregvrNqinaprq.rkr
TwInUI	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wgnfxubfgj.rkr
TypedPaths	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\WJfpevcg.rkr
User Shell Folders	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wjvaire.rkr
UserAssist	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wpbzrkczfp
{9E04CAB2-CC14-11DF-BB8C-A2F}	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wpzq.rkr
{A3D53349-6E61-4557-8FC7-002}	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wqpbzpast.rkr
{B267E3AD-A825-4A09-82B9-EEC}	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wriragije.rkr
Count	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\WRnfrBsNpprrffQvnybt.rkr
{BCB48336-4DDD-48FF-BB0B-D3}	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wsbagivrj.rkr
Count	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\WSbaqhr.rkr
{CAA59E3C-4792-41A5-9909-6A6}	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wzfvkrp.rkr
{CEBFF5CD-ACE2-4F4F-9178-992}	{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Wzntavsl.rkr
Count	{6Q809377-6NS0-4440-8957-N3773S02200R}\W010 RqvgbeW010Rqvgbe.rkr
{F2A1CB5A-E3CC-4A2E-AF9D-505}	{6Q809377-6NS0-4440-8957-N3773S02200R}\WAhibgba GbbyfWAh-Yvax_HFO_QevireWQCvafgWnzq64WQCvafg.rkr
Count	{6Q809377-6NS0-4440-8957-N3773S02200R}\WBenpyrWlveghnyObkWlveghnyObk.rkr
{F4E57C4B-2036-45F0-A9AB-443}	{6Q809377-6NS0-4440-8957-N3773S02200R}\WBenpyrWlveghnyObkWlveghnyObkIZ.rkr
{FA99DFC7-6AC2-453A-A5E2-5E2}	{6Q809377-6NS0-4440-8957-N3773S02200R}\WCbfgterFDYW15WfpevcgfWhehacdy.ong
VirtualDesktops	
VisualEffects	

- ROT13 인코딩이 적용되어 있어 디코딩 작업을 진행해야 한다.

# 레지스트리 분석

- UserAssist
  - 두 기록 중에서 실행파일을 확인한 결과 실행 횟수, 마지막 실행 시간 등 확인 가능

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
 c	=	=	 c	=
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	0	0	0d, 0h, 00m, 00s	2024-01-05 09:59:33
Microsoft.Paint_8wekyb3d8bbwe!App	0	0	0d, 0h, 00m, 00s	2024-01-09 11:58:30
Microsoft.WindowsNotepad_8wekyb3d8bbwe!App	4	3	0d, 0h, 00m, 50s	2024-01-09 15:13:43
MicrosoftWindows.Client.CBS_cw5n1h2txyewy!CortanaUI	0	1	0d, 0h, 00m, 12s	
MSEdge	0	0	0d, 0h, 00m, 00s	2024-01-09 06:02:36
windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	0	0	0d, 0h, 00m, 00s	2023-12-18 11:48:06
{System}!cmd.exe	0	0	0d, 0h, 00m, 00s	2024-01-09 04:32:21
Microsoft.Windows.Explorer	2	8	0d, 0h, 01m, 00s	2024-01-09 14:41:17
{ProgramFilesX64}!Bandizip!Bandizip.exe	0	1	0d, 0h, 00m, 08s	2024-01-08 05:32:17
Microsoft.VisualStudioCode	0	179	0d, 1h, 14m, 04s	2024-01-09 03:05:02
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App	0	0	0d, 0h, 00m, 08s	2024-01-09 09:26:38
Brave	0	0	0d, 0h, 00m, 00s	2024-01-09 01:05:53




# 레지스트리 분석

- USB: PC에 연결된 USB 장치의 기록 확인 가능
  - HKLM\SYSTEM\ControlSet001\Enum\USB

Timestamp	Key Name	Serial Number	Parentid Prefix	Service	Device Name
=	ABC	ABC	ABC	ABC	ABC
2023-10-17 10:54:51	VID_03FD&PID_0013	5&11fcb04&0&1		WINUSB	Xilinx Platform Cable USB II Firmware Loader
2023-10-17 10:57:40	VID_03FD&PID_0008	5&11fcb04&0&1		WINUSB	Xilinx USB Cable
2023-10-31 09:37:50	VID_03FD&PID_0013	5&11fcb04&0&3		WINUSB	Xilinx Platform Cable USB II Firmware Loader
2023-10-31 09:45:24	VID_03FD&PID_0008	5&11fcb04&0&3		WINUSB	Xilinx USB Cable
2023-11-21 10:19:43	VID_346D&PID_5678	8068771311214676951		USBSTOR	USB Mass Storage Device
2023-12-11 17:33:13	VID_05AC&PID_12A8	00008101001338863801401E	6&2965a859&1	usbccgp	Apple Mobile Device USB Composite Device
2023-12-11 17:33:14	VID_05AC&PID_12A8&MI_00	6&2965a859&1&0000		WUDFWpdMtp	Apple iPhone
2023-12-20 14:40:09	VID_04FE&PID_0021	5&11fcb04&0&1	6&2bcafd6&0	usbccgp	USB Composite Device
2023-12-20 14:40:09	VID_04FE&PID_0021&MI_00	6&2bcafd6&0&0000	7&1f99e0eb&0	HidUsb	USB Input Device
2023-12-20 14:40:09	VID_04FE&PID_0021&MI_01	6&2bcafd6&0&0001	7&43d5cd7&0	HidUsb	USB Input Device
2023-12-20 14:40:09	VID_04FE&PID_0021&MI_02	6&2bcafd6&0&0002	7&28149a99&0	HidUsb	USB Input Device
2023-12-21 15:36:47	VID_0403&PID_6001	B000KUC6		FTDIBUS	USB Serial Converter
2023-12-21 20:41:29	VID_1366&PID_0101	000261014326		jlink	J-Link driver

# 레지스트리 분석



- USBSTOR: PC에 연결된 USB 저장장치의 기록 확인 가능
  - HKLM\SYSTEM\ControlSet001\Enum\USBSTOR

Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Installed	First Installed	Last Connected	Last Removed
=						=	=	=	=
2023-12-14 23:17:07	Ven_VendorCo	Prod_ProductCode	Rev_2.00	8068771311214676951&0	VendorCo ProductCode USB Device	2023-11-21 10:19:43	2023-11-21 10:19:43	2023-11-21 10:19:43	2023-11-21 10:20:09





- 최초 연결 시간, 마지막 연결 시간, 마지막 해제 시간 등 자세한 시간 정보 확인 가능

# 레지스트리 분석

- MountedDevices: 시스템에 연결된 저장장치를 식별하는 용도
  - HKLM\SYSTEM\MountedDevices




Device Name	Device Data
	
\\DosDevices\\C:	DMIO:ID:Á—cØ«L·L'€™Î²8•B
\\DosDevices\\D:	DMIO:ID: s†Ê2orB·ÔÚN ÝÈÈ
\\DosDevices\\E:	sæzº †
\\??\\Volume{3a81a064-512f-11ed-a41f-005056c00008}	\\??\\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROI
\\DosDevices\\F:	_??_USBSTOR#Disk&Ven_VendorCo&Prod_ProductCo
\\??\\Volume{f2f53f1a-77d2-11ee-a489-3ce9f7bc5150}	_??_USBSTOR#Disk&Ven_VendorCo&Prod_ProductCo
\\??\\Volume{bc5d8e5a-7d44-11ee-a48c-3ce9f7bc5150}	_??_USBSTOR#Disk&Ven_VendorCo&Prod_ProductCo
\\??\\Volume{e36a7c13-8841-11ee-a496-3ce9f7bc5150}	_??_USBSTOR#Disk&Ven_VendorCo&Prod_ProductCo

- WindowsPortableDevices: 볼륨명 확인 용도
  - HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Deivces

Timestamp	Device	Serial Number	Guid	Friendly Name
=				
2023-11-21 10:19:44	DISK&VEN_VENDORCO&PROD_PRODUCTCO DE&REV_2.00	8068771311214676951&0	{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}	F:₩
2023-07-13 07:17:36			{16E4DE16-214D-11EE-A466-3CE9F7BC5150}	E:₩
2023-03-23 03:22:00				Apple iPhone
2023-11-03 05:41:59				Apple iPhone

# 레지스트리 분석

- NetworkList
  - 무선 네트워크 연결 정보 확인 가능

First Network	Network Name	Name Type	First Connect LOCAL	Last Connected L...	Managed	DNS Suffix
		=	=	=	<input checked="" type="checkbox"/>	
CellSpot_5GHz_6908	CellSpot_5GHz_6908	Wireless	2023-05-12 16:37:38	2024-01-09 12:26:29	<input type="checkbox"/>	T-mobile.com
PNU-WiFi	PNU-WiFi	Wireless	2022-10-21 22:53:46	2023-12-27 15:19:23	<input type="checkbox"/>	pusan.ac.kr
5G_LGWiFi_CDBC	5G_LGWiFi_CDBC	Wireless	2022-10-21 19:10:51	2023-12-27 05:55:14	<input type="checkbox"/>	<없음>
PNU-WiFi-2.4G	PNU-WiFi-2.4G	Wireless	2022-10-21 21:02:34	2023-12-26 10:06:16	<input type="checkbox"/>	pusan.ac.kr
6518_5G	6518_5G	Wireless	2022-11-09 10:04:54	2023-12-22 15:24:43	<input type="checkbox"/>	<없음>
PNU-WiFi 4	PNU-WiFi 4	Wireless	2023-02-09 14:39:38	2023-12-20 22:31:25	<input type="checkbox"/>	<없음>
6203-1_5G	6203-1_5G	Wireless	2023-09-27 15:30:29	2023-12-20 15:21:09	<input type="checkbox"/>	<없음>

# 레지스트리 분석

- Uninstall: 프로그램 설치 정보
  - HKLM, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Timestamp	Key Name	Display Name	Display Version	Publisher	Install Date
=	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
2023-12-20 17:54:31	JetBrains Toolbox (Fleet) 2d35fa0d-efde-454d-a613-f130d7d335cb	Fleet	1.28.117 Public Preview	JetBrains s.r.o.	20231221
2023-12-20 17:54:01	Toolbox	JetBrains Toolbox	2.1.3.18901	JetBrains	
2023-12-15 04:18:41	{771FD6B0-FA20-440A-A002-3B3BAC16DC50}_is1	Microsoft Visual Studio Code (User)	1.85.1	Microsoft Corporation	20231215
2023-12-15 04:18:09	661f0cc6-343a-59cb-a5e8-8f6324cc6998	Notion 3.1.0	3.1.0	Notion Labs, Inc	
2023-12-08 17:45:33	GitHubDesktop	GitHub Desktop	3.3.6	GitHub, Inc.	20231209
2023-12-04 09:06:54	Postman	Postman x86_64 10.20.0	10.20.0	Postman	20231204
2023-11-26 14:10:06	slack	Slack	4.35.126	Slack Technologies Inc.	20231126
2023-10-28 08:05:13	ZoomUMX	Zoom	5.16.2 (22807)	Zoom Video Communications, Inc.	
2023-09-14 06:14:48	DBeaver (current user)	DBeaver 23.2.0 (current user)	23.2.0	DBeaver Corp	



# 레지스트리 분석

- ShellBag - [Shellbags Explorer](#) 도구 활용하여 분석 가능
- VolumeInfoCache
- AppPaths
- HeapLeakDetection
- AppCompatFlags
- NetworkSetup2
- IconLayouts
- FirewallRules
- FeatureUsage
- BAM (Background Activity Moderator)
- ...

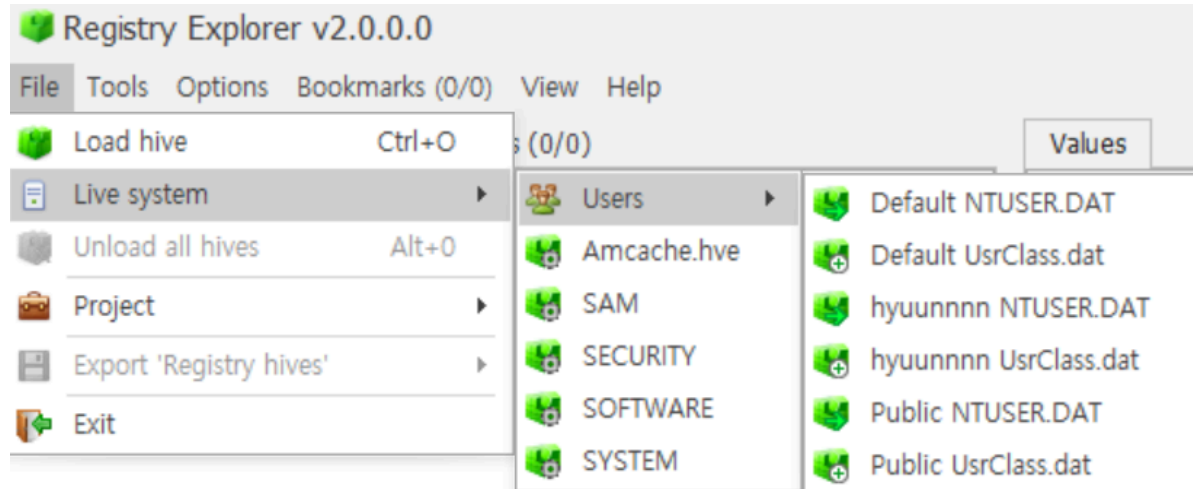
# 레지스트리 도구 실습

- [RegistryExplorer](#)
  - 지금까지 확인했던 것처럼 분석에 유용한 결과를 출력한다.
    - [RegistryPlugins](#)에 있는 플러그인들이 이를 수행한다.
  - 유의미한 아티팩트가 존재하는 경로들이 북마크에 등록되어 있다.
  - 북마크로 등록되지 않았다면 [RegistryExplorerBookmarks](#), 분석에 불편한 점이 있다면 플러그인을 개발해서 기여해보자. ([Registry Explorer Plugin 개발](#) 참고)
- [REGA](#), [RegRipper](#), ([yarp](#) - 레지스트리 하이브 카빙 도구) 등 다양한 도구 존재
  - 다양한 도구들을 사용하면서 어떤 장점, 강점이 있는지 확인하는 것도 좋은 경험
- [awesome-forensics](#), [ForensicsTools](#), [AboutDFIR](#) 등 정리된 사이트가 많이 있다.

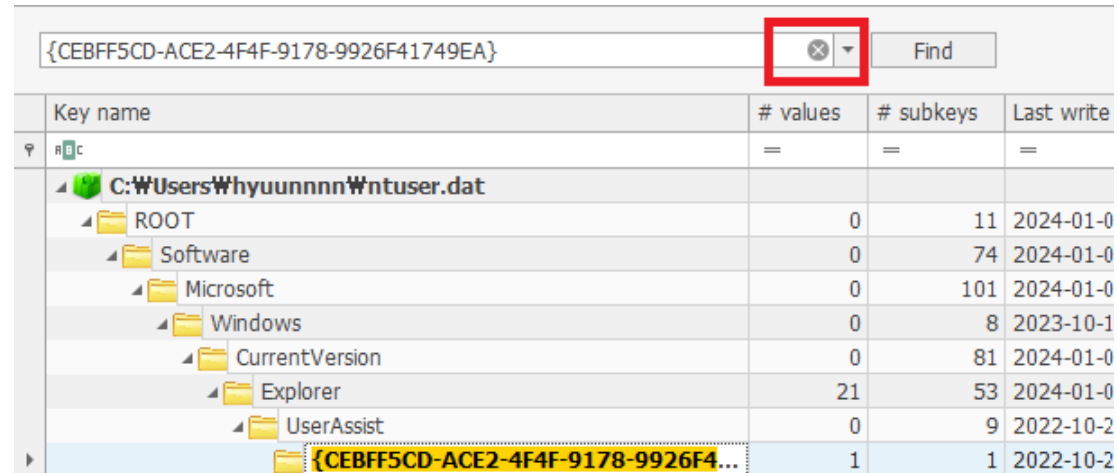
[1] The truth is that the Registry is a veriable gold mine of information for both the administrator and the forensic investigator.

<sup>1</sup> [Windows Forensic Analysis](#) - p158 (번역본)

# 레지스트리 도구 실습



- UserAssist 경로 검색 → 경로 클릭 → X 버튼 클릭



# 레지스트리 도구 실습

- 검색한 경로까지만 뜨기 때문에 경로 클릭 후 X 버튼 클릭
- 해당 경로 이후에 존재하는 Count 를 클릭하여 확인 가능

The screenshot shows the Registry Explorer v2.0.0.0 interface. The left pane displays the registry tree with the path `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced` expanded. The `Count` value is highlighted. The right pane shows the details of the `Count` value, which is a `DWORD` type with a value of `354`.

Key name	# values	# subkeys	Last write
<code>HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced</code>	354	0	2024-

# 레지스트리 도구 실습

- Available bookmarks 버튼을 누르면 현재 적용된 북마크 사용 가능

Registry hives (3)		Available bookmarks (95/0)	
<input type="text" value="Enter text to search..."/>		<input type="button" value="Find"/>	
Key name	# values	#	
HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainers\SystemAppData\Uninstall	=	^	
> HeapLeakDetection	0		
> Image File Execution Options	0		
> Internet Explorer	9		
> LogonUI	8		
> NetworkCards	0		
> NetworkList	3		
> Products	0		
> UserData	0		
> ProfileList	4		
Run	4		
RunOnce	0		
> App Paths	0		
> Uninstall	0		
> StartMenuInternet	1		
> System	21		
> System	21		
> TaskCache	0		
> Tracing	1		
> VolumeInfoCache	0		
> Windows Portable Devices	0		
> Winlogon	35		
> Tracing	1		
> Uninstall	0		

Registry hives (3)

Available bookmarks (95/0)

Enter text to search...

Find

Key name	# values	#
HKEY_CURRENT_USER	=	^
Tracing		1
Uninstall		0
C:\Windows\System32\config\SYSTEM		
{10497b1b-ba51-44e5-8318-a65c837b6661}		0
{4d36e972-e325-11ce-bfc1-08002be10318}		6
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}		0
{6bdd1fc6-810f-11d0-bec7-08002be2092f}		6
AppCompatCache		3
bam		7
Devices		0
ComputerName		2
CrashControl		11
DeviceClasses		0
Environment		21
EventLog		13
FilesNotToSnapshot		10
FileSystem		41
FirewallPolicy		4
Interfaces		0
Memory Management		16
MountedDevices		8
NetworkSetup2		0
PrefetchParameters		3
RDP-Tcp		85
SafeBoot		1
Services		0
Shares		0
Terminal Server		15
TimeZoneInformation		10
USB		0

Values

USB

Drag a column header here to group by that column

Timestamp	Key Name	Serial Number
=	HKEY_CURRENT_USER	HKEY_CURRENT_USER
2024-01-09 00:59:27	ROOT_HUB30	4&18d13c5b&0&0
2024-01-09 00:59:27	ROOT_HUB30	4&2a550402&0&0
2023-12-27 05:03:54	VID_0000&PID_0002	5&11fbc04&0&3
2023-10-17 10:57:40	VID_03FD&PID_0008	5&11fbc04&0&1
2023-10-31 09:45:24	VID_03FD&PID_0008	5&11fbc04&0&3
2023-10-17 10:54:51	VID_03FD&PID_0013	5&11fbc04&0&1
2023-10-31 09:37:50	VID_03FD&PID_0013	5&11fbc04&0&3
2023-12-21 15:36:47	VID_0403&PID_6001	8000KUC6
2024-01-07 01:14:04	VID_04E8&PID_61F5	MSFT301234567B8F
2024-01-09 00:59:29	VID_04F2&PID_B6FA	0001
2024-01-09 00:59:30	VID_04F2&PID_B6FA&M_I_00	6&13cee7cf&0&000
2023-12-20 14:40:09	VID_04FE&PID_0021	5&11fbc04&0&1
2023-12-22 07:37:46	VID_04FE&PID_0021	5&11fbc04&0&3
2023-12-20 14:40:09	VID_04FE&PID_0021&M_I_00	6&2bcafd6f&0&0000
2023-12-22 07:37:46	VID_04FE&PID_0021&M_I_00	6&6579cac&1&0000
2023-12-20 14:40:09	VID_04FE&PID_0021&M_I_01	6&2bcafd6f&0&0000
2023-12-22 07:37:46	VID_04FE&PID_0021&M_I_01	6&6579cac&1&0001
2023-12-20 14:40:09	VID_04FE&PID_0021&M_I_02	6&2bcafd6f&0&0000
2023-12-22 07:37:46	VID_04FE&PID_0021&M_I_02	6&6579cac&1&0002

# 레지스트리 도구 실습

- 확인하고자 하는 경로를 찾기 어렵다면 검색 기능을 활용하자.
- CTRL + F 를 통해 찾을 수도 있지만, 왼쪽 창에서 아래 사진과 같이 UserAssist 를 입력하여 바로 접근할 수 있다.

Registry Explorer v2.0.0.0

FileToolsOptionsBookmarks (32/0)ViewHelp

Registry hives (2)Available bookmarks (64/0)

Enter text to search...Find

Key name	# values	# subkeys	Last write timestamp
HKEY_CURRENT_USER	=	=	=
Substrate	3	0	2024-01-17 16
TabletMode	1	0	2022-10-21 10
Taskband	5	1	2024-01-13 17
TWinUI	0	1	2022-11-02 07
TypedPaths	26	0	2024-01-17 06
User Shell Folders	20	0	2022-10-21 10
UserAssist	0	9	2022-10-21 10
VirtualDesktops	3	1	2024-01-18 04
VisualEffects	0	19	2022-10-21 10
Wallpapers	7	0	2024-01-18 04
WordWheelQuery	18	1	2023-11-10 09

ValuesUserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
HKEY_CURRENT_USER	=	=	HKEY_CURRENT_USER	=
UEME_CTLSESSION	0	0	0d, 0h, 00m, 00s	
UEME_CTLSESSION	0	0	0d, 0h, 00m, 00s	
UEME_CTLSESSION	0	0	0d, 0h, 00m, 00s	
UEME_CTLSESSION	0	0	0d, 0h, 00m, 00s	
UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
UEME_CTLSESSION	450	4528	1d, 22h, 10m, 26s	
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	0	0	0d, 0h, 00m, 00s	2024-01-05 09:59:33
Microsoft.Paint_8wekyb3d8bbwe!App	3	3	0d, 0h, 00m, 23s	2024-01-17 08:20:42
Microsoft.WindowsNotepad_8wekyb3d8bbwe!App	35	167	0d, 0h, 40m, 38s	2024-01-17 16:25:44

# 과제

- 간단한 레지스트리 분석 도구 만들어보기
  - 파이썬에 내장되어 있는 **winreg** 라이브러리를 사용하여 쉽게 개발 가능
  - 위에서 설명했던 경로 혹은 추가로 찾아본 후 아래와 같이 자유롭게 만들어보기

*Registry Parser*

input command: hwplist

file0 : C:\Users\hy00u\Desktop\winreg.hwp

file1 : C:\Users\hy00u\OneDrive\문서\카카오톡 받은 파일\Ruzin.hwp

file2 : C:\Users\hy00u\Downloads\독서 활동 감상문.hwp

file3 : C:\Users\hy00u\Desktop\독서 활동 감상문.hwp

file4 : C:\Users\hy00u\Desktop\논문문의사결정나무.hwp

file5 : C:\Users\hy00u\Desktop\논문warm 커널 파일 시스템 연구.hwp

file6 : C:\Users\hy00u\Desktop\논문대각선 논법을 이용한 멈춤 문제의 증명.hwp

오늘

2024-1-10\_2-45-34\_MUICache.csv 2024-01-10 오전 2:45 Microsoft Excel 실행... 106KB

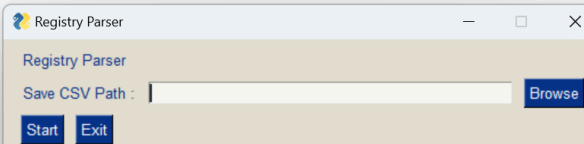
2024-1-10\_2-45-34\_UserAssist.csv 2024-01-10 오전 2:45 Microsoft Excel 실행... 59KB

2024-1-10\_2-45-34\_LastVisited.csv

2024-1-10\_2-45-34\_USBSTOR.csv

2024-1-10\_2-45-34\_Office.csv

2024-1-10\_2-45-34\_RecentDocs.csv



# 권한 문제

- HKEY\_LOCAL\_MACHINE 에 접근할 때 `PermissionError` 발생

```
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1>python winreg_analyzer.py
Traceback (most recent call last):
  File "C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1\winreg_analyzer.py", line 82, in <module>
    window['-TEXT-'].update('\n'.join(uninstall()))
                                ^^^^^^^^^^^^^^^
  File "C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1\winreg_analyzer.py", line 10, in uninstall
    varKey = winreg.OpenKey(varReg, path, 0, winreg.KEY_ALL_ACCESS)
            ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
PermissionError: [WinError 5] 액세스가 거부되었습니다
```

- 터미널을 관리자 권한으로 실행 후 사용하는 방법도 있지만, `gsudo`를 사용하면 리눅스의 `sudo` 명령어처럼 동작한다.

```
$ winget install gerardog.gsudo # gsudo 설치
$ sudo # 또는 gsudo
```

```
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1>sudo
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1# exit

C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1>gsudo
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1# exit
```



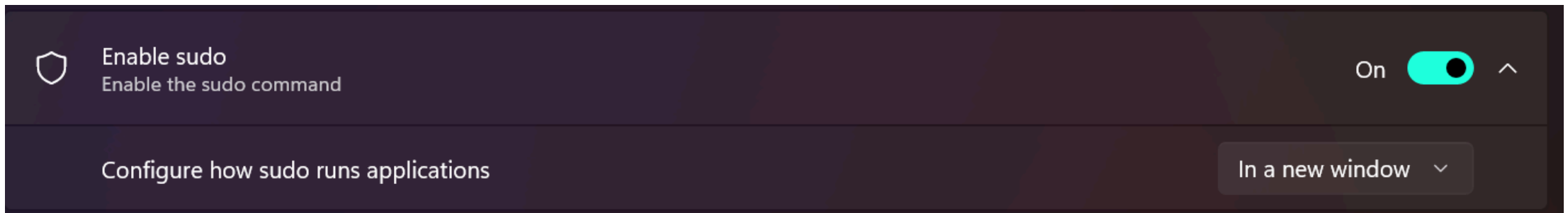
# 권한 문제

```
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1>gsudo python winreg_analyzer.py
```

```
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1>sudo python winreg_analyzer.py  
|
```

```
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1>sudo  
C:\Users\hyuunnnn\Documents\GitHub\forensic-study-2023winter\homework\1# python winreg_analyzer.py  
|
```

- Windows에서 **sudo** 기능을 공식적으로 지원할 예정이다.<sup>1 2</sup>
  - 현재 프리뷰 버전(26052)에 기능이 추가되어 있다.<sup>3</sup>



<sup>1</sup> <https://learn.microsoft.com/ko-kr/windows/sudo/>, [Introducing Sudo for Windows!](https://github.com/microsoft/sudo), <https://github.com/microsoft/sudo>

<sup>2</sup> <https://youtu.be/9y3mOUARQdE>

<sup>3</sup> [Announcing Windows 11 Insider Preview Build 26052 \(Canary and Dev Channels\)](#)

# 참고자료

- 국가법령정보센터 - 형사소송법
- casenote - 형사소송법
- forensic-proof - 아티팩트의 의미는?
- 윈도우 레지스트리 - wikipedia
- Ahnlab - 디지털 세상의 CSI, 범죄를 입증하라
- mandiant - Digging Up the Past: Windows Registry Forensics Revisited
- Exploring Registry Explorer
- Introducing AboutDFIR's Registry Explorer/RECmd Guide
- 기초부터 따라하는 디지털포렌식