Forensic Study - 6
Windows Registry (1)

2017.11.14

KUICS

2014210009 주어진

목차

Registry?

원도우 레지스트리 : Windows 운영 체제의 설정과 선택 항목을 가지고 있는 DB.
하드웨어, 소프트웨어등등의 정보와 설정이 담겨 있다.

원래는 INI를 사용했으나, 파편화가 심해 Registry를 도입.

간단하게 말해서, 어떤 프로그램을 설치할 때도 Registry에 값이 추가되거나 수정되고,
하드웨어를 새로 장착했을 때도 Registry가 바뀔 수 있다.

Registry?

DOS : Autobat, Config.sys등에 저장

Win 95이후 : 레지스트리로 대체

Registry?

일부 레지스트리는 휘발성이며, 어떤 레지스트리는 비휘발성이다.

비휘발성은 파일형태로 존재
휘발성은 시스템 시작시 생성, 종료시 삭제

Registry?

보통은 C:₩Windows₩System32 하위 디렉토리에 파일형태로 존재한다. (64bit 환경에서도 System32 폴더이다.)
또는 C:₩Users₩$USERNAME₩

파일형태로 존재하는 경우 : System, SAM, Security, Softwate, User SID, Default
휘발성 : Hardware, Clone

Q. 그럼 어떻게 모든 레지스트리를 온전하게 보존?

Registry? (Advanced)

레지스트리는 UAC의 도입과 함께 가상화가 이루어진다.

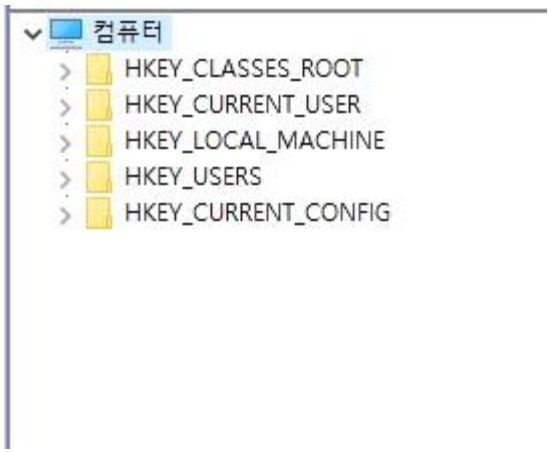
HKEY_MACHINE₩SOFTWARE -> HKEY_USER₩Software₩Classes₩VirtualStore₩Machine₩Software

다만,
HKEY_MACHINE₩SOFTWARE₩Classes, ₩Microsoft₩Windows는 가상화에서 제외

폴더가 가상화되는 위치에 레지스트리도 가상화 되므로

C:₩Users₩$USERNAME₩AppData₩Local₩Microsoft₩Windows₩UsrClass.dat로 존재.

Registry Hive



ROOT -> 어플리케이션 환경설정
CURRENT_USER -> 현재 접속한 유저 프로파일
MACHINE -> 시스템 HW & SW 환경설정
CURRENT_CONFIG -> 하드웨어 프로파일
USERS -> 모든 사용자의 프로파일

Registry Hive (Advanced)

S-1-5-18 : 로컬 시스템
S-1-5-19 : 로컬 서비스
S-1-5-20 : 네트워크 서비스
S-1-5-21-396... : 뭘까요?

Registry Hive (Advanced)

```
svchost.exe (528): S-1-5-21-285125983-2218342051-2926112896-1000 (Chobo)
svchost.exe (528): S-1-5-21-285125983-2218342051-2926112896-513 (Domain Users)
svchost.exe (528): S-1-1-0 (Everyone)
svchost.exe (528): S-1-5-114 (Local Account (Member of Administrators))
svchost.exe (528): S-1-5-32-544 (Administrators)
svchost.exe (528): S-1-5-32-545 (Users)
svchost.exe (528): S-1-5-4 (Interactive)
svchost.exe (528): S-1-2-1 (Console Logon (Users who are logged onto the physical console))
svchost.exe (528): S-1-5-11 (Authenticated Users)
svchost.exe (528): S-1-5-15 (This Organization)
svchost.exe (528): S-1-5-113 (Local Account)
svchost.exe (528): S-1-5-5-0-429020 (Logon Session)
svchost.exe (528): S-1-2-0 (Local (Users with the ability to log in locally))
```

참조 : Study 3 - Example 1

S-1-5-18 : 로컬 시스템
S-1-5-19 : 로컬 서비스
S-1-5-20 : 네트워크 서비스
S-1-5-21-396... : 아마도 현재 사용자, 도메인 유저를 의미할 것이다.

Registry Data Type

REG_DWORD : 데이터를 4byte로 표현
REG_BINARY : 이진 데이터
REG_SIZE : 고정 길이 문자열
REG_EXPAND_SZ : 가변 길이 데이터
REG_LINK : 심볼릭 링크 유니코드
...

이름 , 종류 , 데이터로 나뉜다.
ex) KUICS / REG_DWORD / 0x00000001 (1)

Registry Data Type

REG_DWORD : 데이터를 4byte로 표현
REG_BINARY : 이진 데이터
REG_SIZE : 고정 길이 문자열
REG_EXPAND_SZ : 가변 길이 데이터
REG_LINK : 심볼릭 링크 유니코드
...

이름 , 종류 , 데이터로 나뉜다.
ex) KUICS / REG_DWORD / 0x00000001 (1)

Registry Data Type

REG_DWORD : 데이터를 4byte로 표현
REG_BINARY : 이진 데이터
REG_SIZE : 고정 길이 문자열
REG_EXPAND_SZ : 가변 길이 데이터 -> REG_SZ는 EXPAND와 MULTI의 성격을 동시에 가지고 있다.
REG_LINK : 심볼릭 링크 유니코드

Registry Path

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

감사합니다

과제 : 없습니다.

다음주는 VM과 함께 실습입니다. VMWare Player 설치해오세요.
(약간의 구글링을 통해 WorkStation을 설치할 수도 있습니다.)