레지스트리 포렌식 & 보안

JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

개 요

1. 레지스트리 소개
2. 레지스트리 획득
3. 레지스트리 내부
4. 레지스트리 복구
5. 레지스트리 분석
6. 레지스트리 도구
7. 레지스트리 분석 예제
8. 레지스트리 보안

레지스트리 소개

Security is a people problem…

레지스트리 소개 및 분석의 필요성

- **윈도우 레지스트리 (Windows Registry)**
  - 마이크로소프트 윈도우 운영체제에서 운영체제와 응용프로그램 운영에 필요한 정보를 저장하기 위해 고안한 계층형 데이터베이스 (http://support.microsoft.com/kb/256986)
  - 부팅 과정부터 로그인, 서비스 실행, 응용프로그램 실행, 사용자 행위 등 모든 활동에 관여함
  - 윈도우 3.11, 9x, Me, NT, 2000, XP, 2003, Vista, 2008, 7 에서 사용

- **레지스트리 포렌식 분석의 필요성**
  - 윈도우 시스템 분석의 필수 요소
    - 운영체제 정보, 사용자 계정 정보, 시스템 정보, 응용프로그램 실행 흔적, 최근 접근 문서 등
    - 자동 실행 항목(Autoruns) 분석, 악성코드 탐지
    - 저장매체 사용 흔적 분석(하드디스크, CD-ROM, USB 등)
  - 사용자/시스템/저장매체 사용 흔적 분석 ➔ 추가적인 포렌식 분석 대상 선별

레지스트리 소개

레지스트리 분석의 포렌식 관점

- **온라인(On-line) 레지스트리 분석**
  - 활성시스템에서의 레지스트리 분석
  - RegEdit(regedit.exe), RegEdt32(regedt32.exe)를 통해 확인 가능 (http://support.microsoft.com/kb/141377)

- **오프라인(Off-line) 레지스트리 분석**
  - 비활성시스템(포렌식 복제 드라이브나 이미지)에서의 레지스트리 분석
  - 레지스트리 하이브(Hive) 파일의 수집이 필요
  - 운영체제 버전별 하이브 파일의 정확한 위치를 사전에 숙지
  - 포렌식 분석은 대부분 오프라인 레지스트리 분석을 대상으로 함

레지스트리 소개

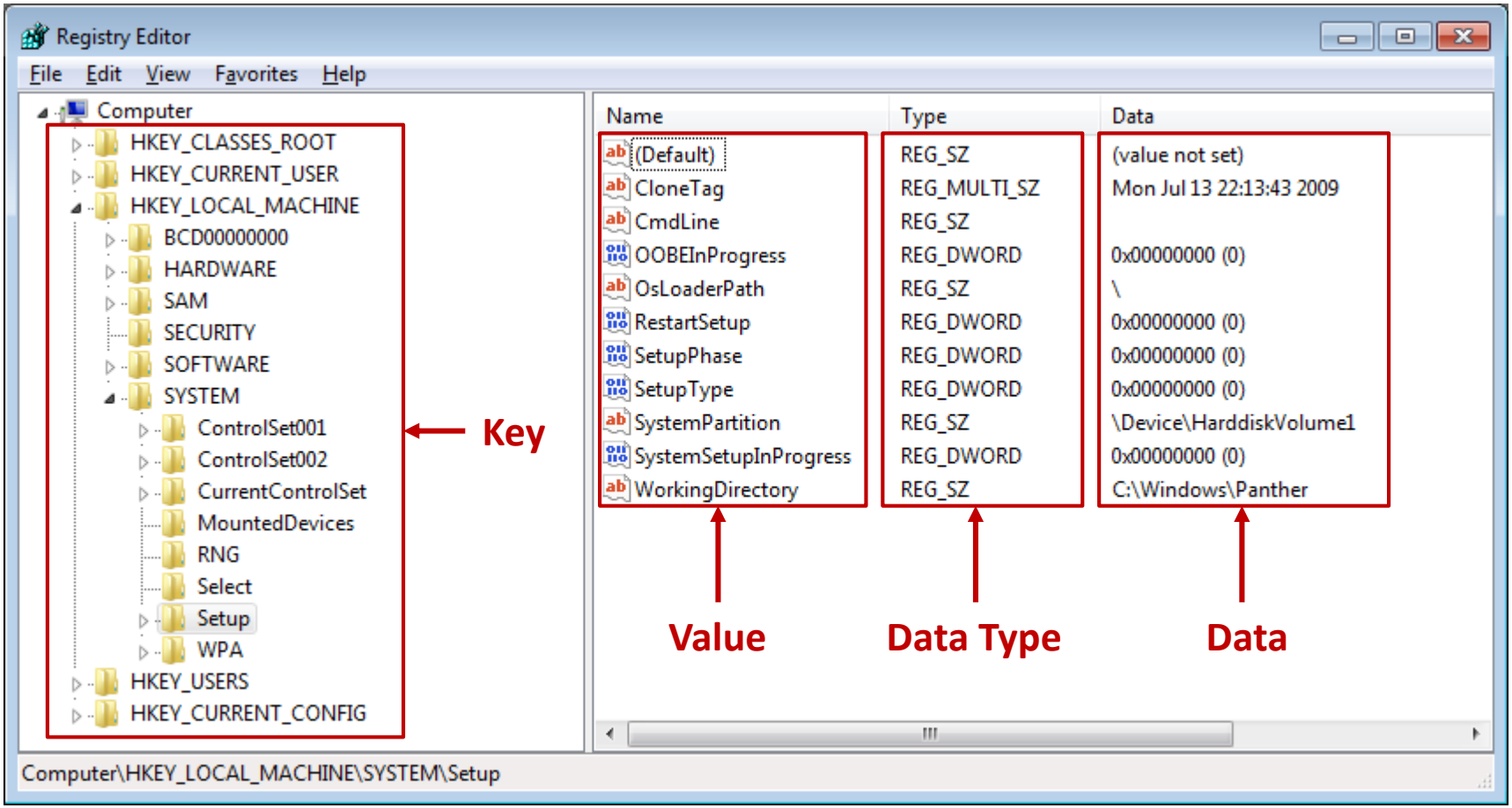
하이브(Hive) 파일이란?

- **하이브 파일**
  - 레지스트리 정보를 저장하고 있는 물리적인 파일
  - 키(Key) 값들이 논리적인 구조로 저장
  - 활성시스템의 커널에서 하이브 파일을 관리
    - 일반적인 방법으로는 접근 불가

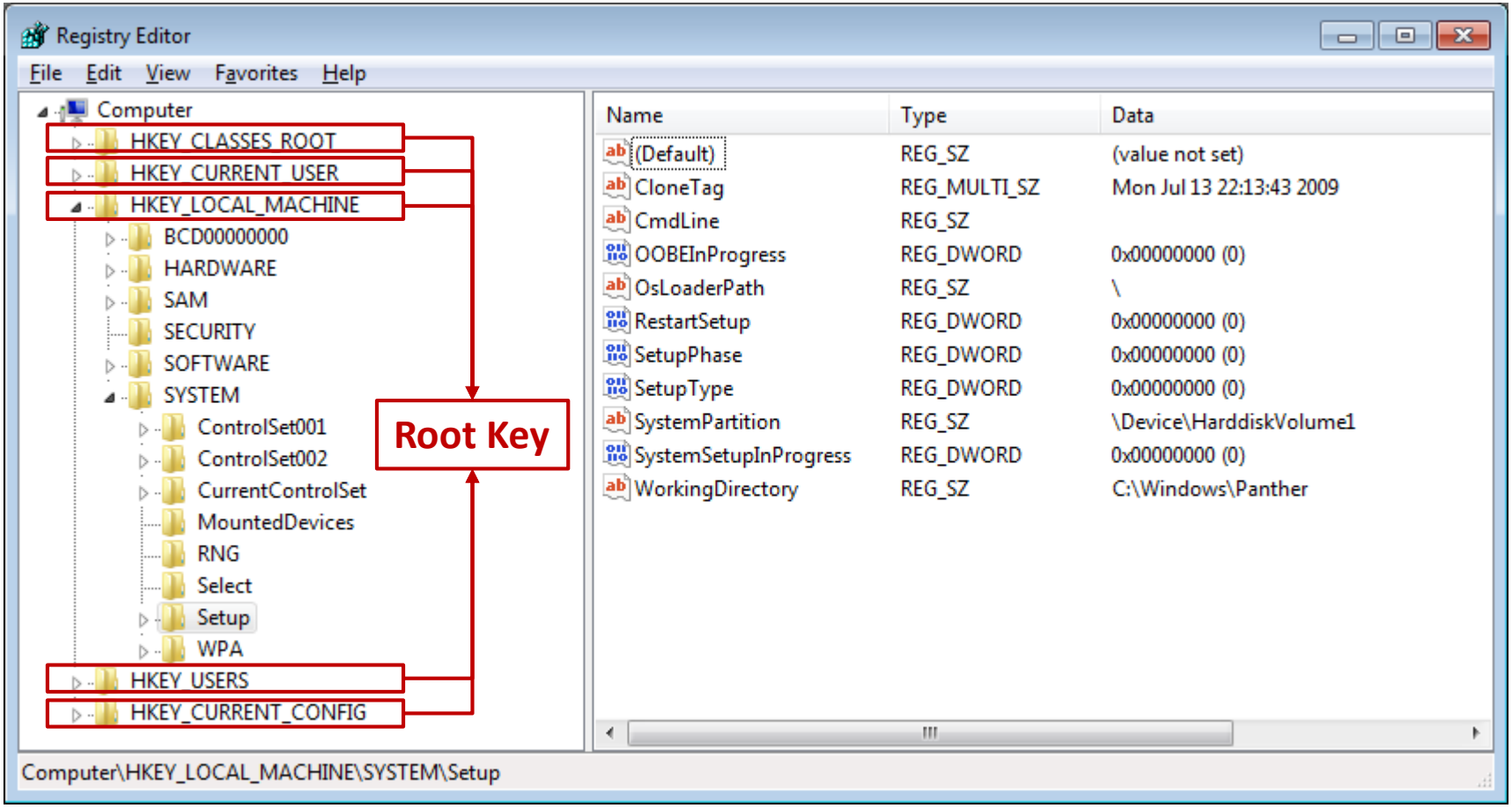
- **하이브 셋 (Hive Set)**
  - 활성시스템의 레지스트리를 구성하는 하이브 파일 목록
  - SAM, SECURITY, SYSTEM, SOFTWARE, Default, NTUSER.DAT, Usrclass.dat, BCD, COMPONENTS 등

레지스트리 소개

레지스트리 데이터 형식



레지스트리 루트키


Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
SYSTEM
ControlSet001
ControlSet002
CurrentControlSet
MountedDevices
RNG
Select
Setup
WPA
HKEY_USERS
HKEY_CURRENT_CONFIG
Root Key
Name
Type
Data
(Default) REG_SZ (value not set)
CloneTag REG_MULTI_SZ Mon Jul 13 22:13:43 2009
CmdLine REG_SZ
OOBEInProgress REG_DWORD 0x00000000 (0)
OsLoaderPath REG_SZ \
RestartSetup REG_DWORD 0x00000000 (0)
SetupPhase REG_DWORD 0x00000000 (0)
SetupType REG_DWORD 0x00000000 (0)
SystemPartition REG_SZ \Device\HarddiskVolume1
SystemSetupInProgress REG_DWORD 0x00000000 (0)
WorkingDirectory REG_SZ C:\Windows\Panther
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup

레지스트리 소개

레지스트리 루트키

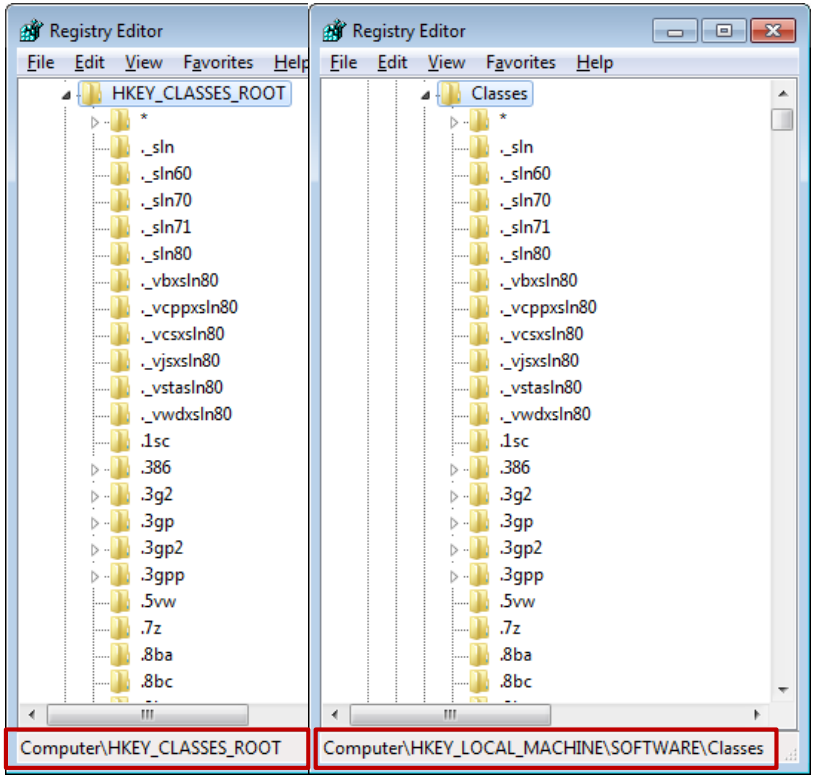
- **HKEY_CLASSES_ROOT**
  - 파일 연관성과 COM(Component Object Model) 객체 등록 정보
- **HKEY_CURRENT_USER**
  - 현재 시스템에 로그인된 사용자의 사용자 프로파일 정보
- **HKEY_LOCAL_MACHINE**
  - 시스템의 하드웨어, 소프트웨어 설정 및 다양한 환경 정보
- **HKEY_USERS**
  - 시스템의 모든 사용자와 그룹에 관한 프로파일 정보
- **HKEY_CURRENT_CONFIG**
  - 시스템이 시작할 때 사용되는 하드웨어 프로파일 정보
- **HKEY_PERFORMANCE_DATA**
  - 성능 정보를 저장

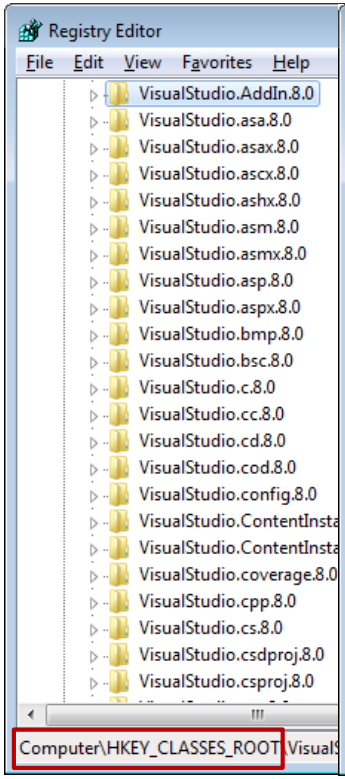
레지스트리 루트키 구성 정보

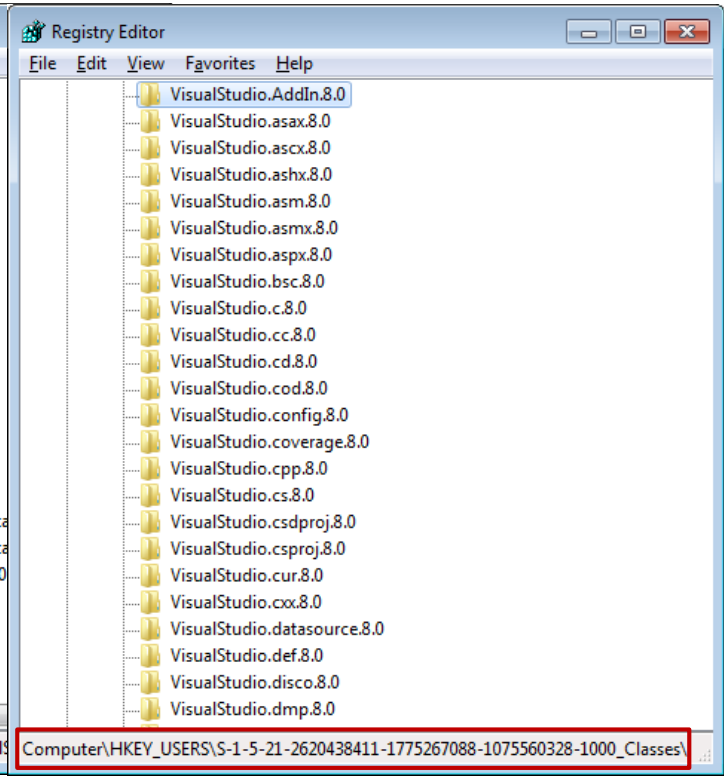
루트키	약어	설명
HKEY_CLASSES_ROOT	HKCR	HKLM\SOFTWARE\Classes와 HKU\<SID>\Classes 모음
HKEY_CURRENT_USER	HKCU	HKU 아래 사용자 프로파일 중 현재 로그인한 사용자의 하위키
HKEY_LOCAL_MACHINE	HKLM	시스템에 존재하는 하이브 파일과 메모리 하이브 모음
HKEY_USERS	HKU	사용자 루트 폴더에 존재하는 NTUSER.DAT 파일의 내용
HKEY_CURRENT_CONFIG	HKCC	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current의 내용
HKEY_PERFORMANCE_DATA	HKPD	성능 카운트 (레지스트리 편집기를 통해 접근 불가, 레지스트리 함수로만 접근)

HKEY_CLASSES_ROOT (HKCR)

- **하위키 구성**
  - 별도의 하이브를 가지지 않고 다른 루트키의 하위키로 구성됨
  - **HKLM₩SOFTWARE₩Classes + HKU₩<SID>_Classes**

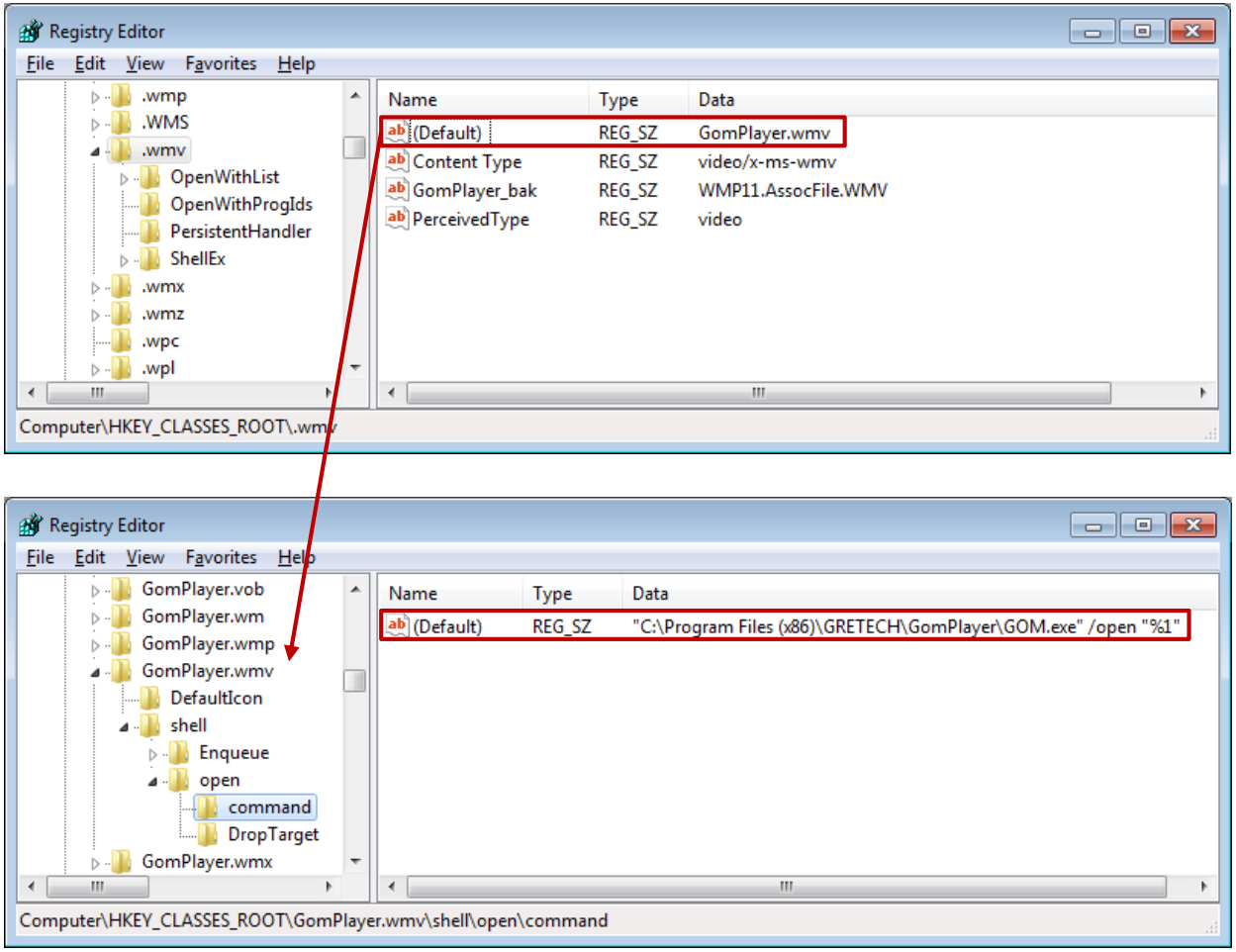






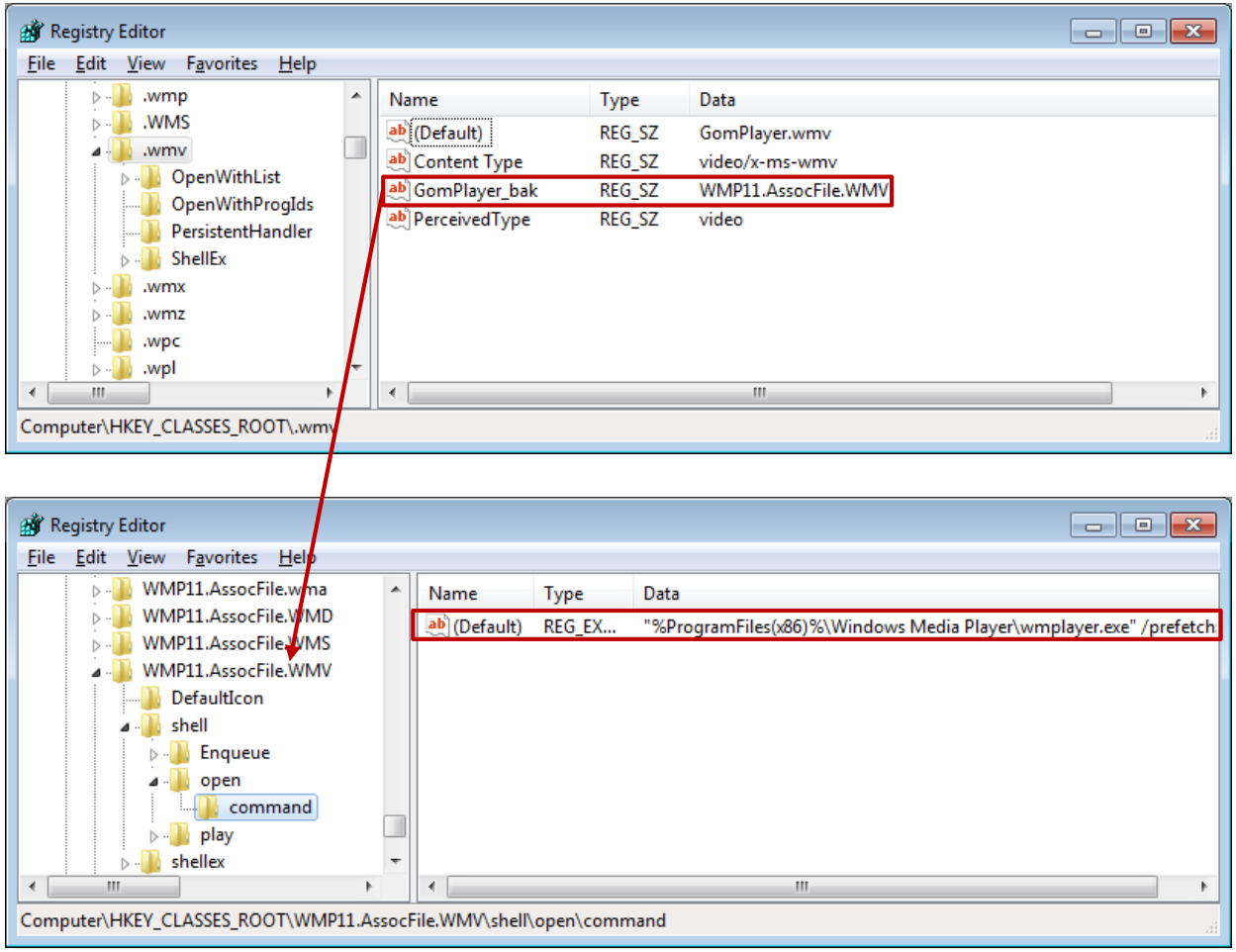
HKEY_CLASSES_ROOT (HKCR)

- 어플리케이션 바인딩 (http://forensic-proof.com/archives/294)



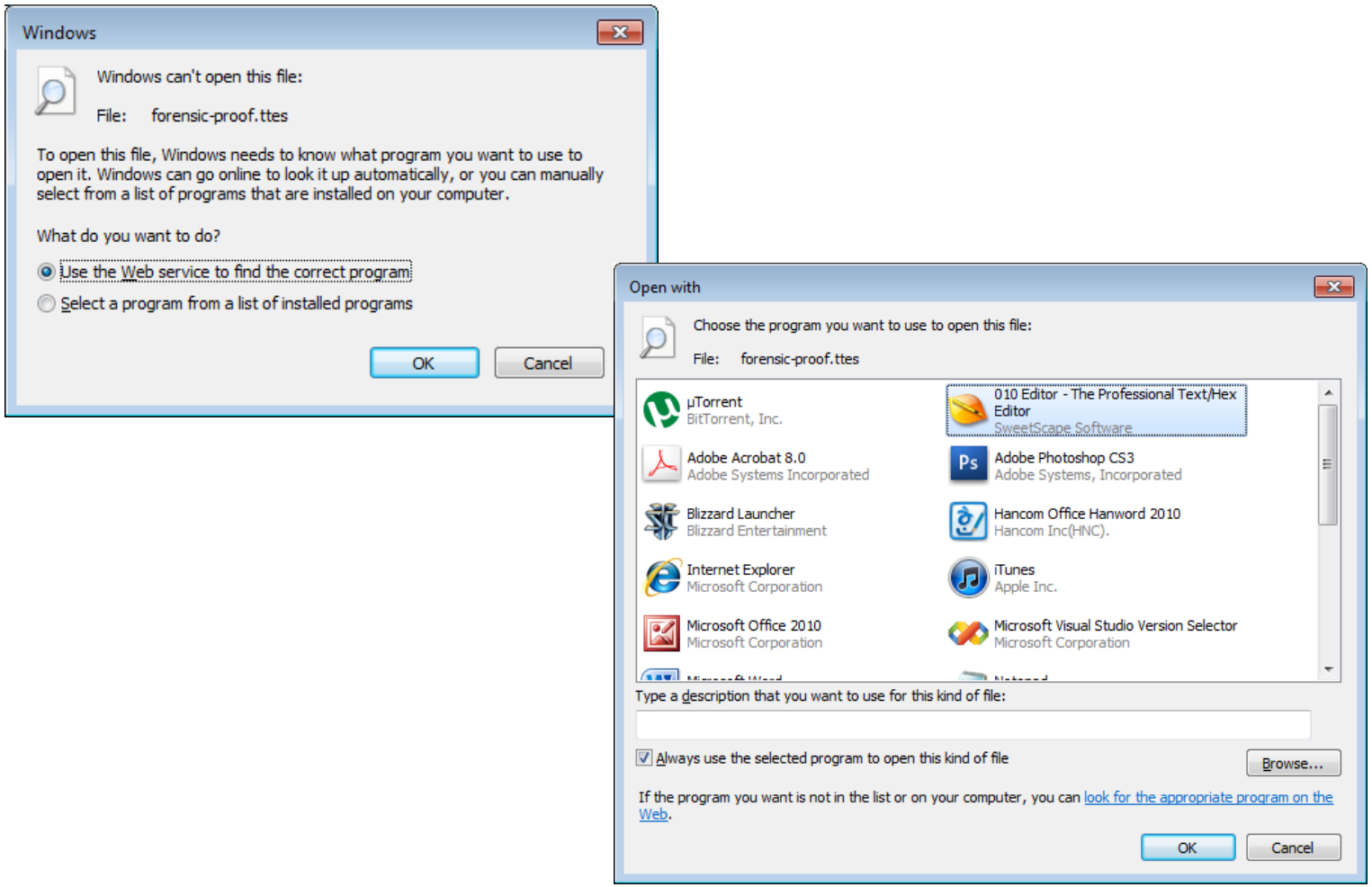
HKEY_CLASSES_ROOT (HKCR)

- 어플리케이션 바인딩 (http://forensic-proof.com/archives/294)



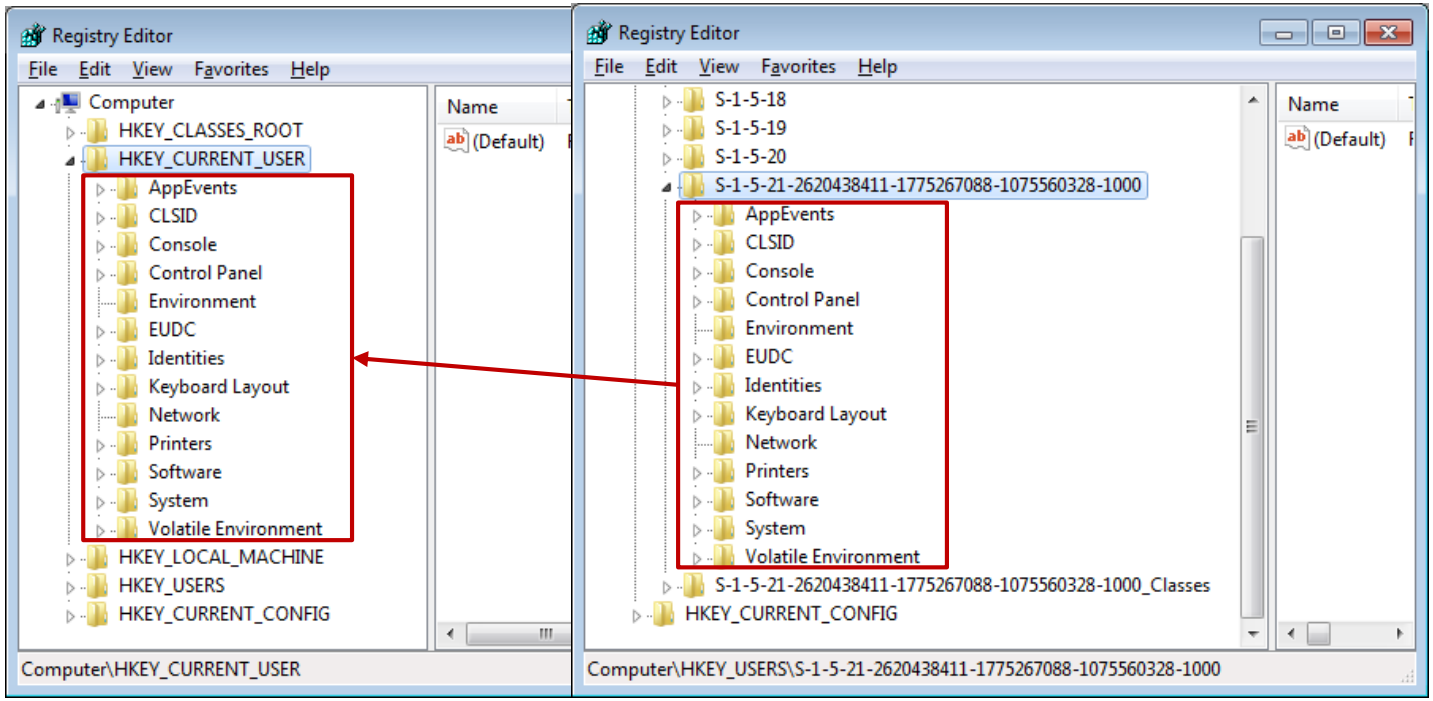
HKEY_CLASSES_ROOT (HKCR)

- 어플리케이션 바인딩 (http://forensic-proof.com/archives/294)



HKEY_CURRENT_USER (HKCU)

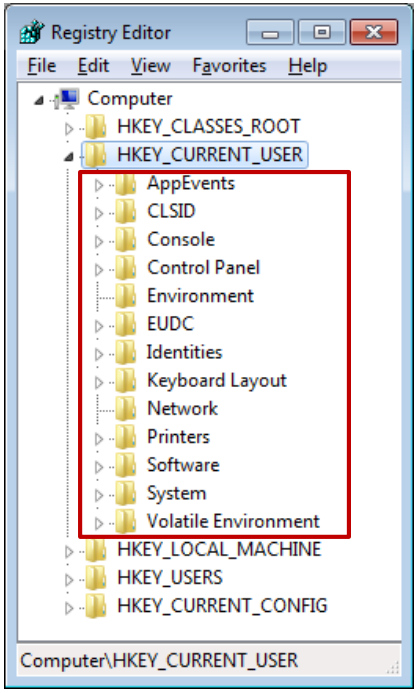
- **하위키 구성**
  - **HKU (HKEY_USERS)** 아래의 프로파일 중 현재 로그인한 사용자의 하위키



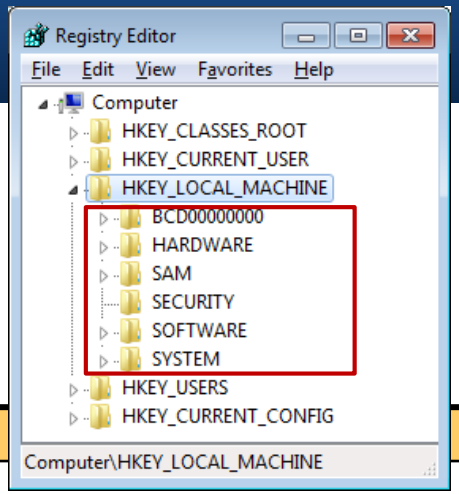
HKEY_CURRENT_USER (HKCU)

- **하위키 내용**

하위키	설명
AppEvents	사운드, 이벤트 관련 키
CLSID	COM 객체 연결 정보
Console	명령 프롬프트 윈도우 설정 정보 (가로, 세로 크기, 색상 등)
ControlPanel	데스크탑 테마, 키보드/마우스 세팅 등의 환경 설정 정보
Environment	환경 변수 정의
EUDC	최종 사용자가 정의한 문자 정보
Identities	윈도우 메일 계정 정보
Keyboard Layout	키보드 레이아웃 설정 정보
Network	네트워크 드라이브 매핑 정보, 환경 설정 값
Printers	프린트 연결 설정
Session Information	작업표시줄에 표시되는 현재 실행되는 프로그램 설정
Software	**로그인한 사용자 소프트웨어 목록**
System	HKLM/SYSTEM 하위키의 일부 (Control, Policies, Services)
UNICODE Program Groups	로그인한 사용자 시작 메뉴 그룹 정의
Volatile Environment	휘발성 환경 변수



레지스트리 소개

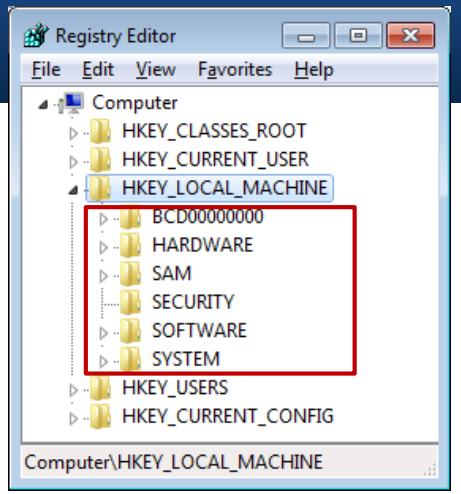


HKEY_LOCAL_MACHINE (HKLM)

- **하위키 구성**
  - 시스템의 다양한 하드웨어, 소프트웨어, 환경 설정 정보

HKLM 하위키	하이브 파일 위치
HKLM\BCD00000000 (Vista/7)	{Boot Partition}\Boot\BCD {Boot Partition}\Boot\BCD.LOG {Boot Partition}\Boot\BCD.LOG1 {Boot Partition}\Boot\BCD.LOG2
HKLM\COMPONENTS (Vista/7)	%SystemRoot%\System32\config\COMPONENTS %SystemRoot%\System32\config\COMPONENTS.LOG %SystemRoot%\System32\config\COMPONENTS.LOG1 %SystemRoot%\System32\config\COMPONENTS.LOG2
HKLM\HARDWARE	Volatile hive
HKLM\SAM	%SystemRoot%\System32\config\SAM %SystemRoot%\System32\config\SAM.LOG %SystemRoot%\System32\config\SAM.LOG1 %SystemRoot%\System32\config\SAM.LOG2
HKLM\SECURITY	%SystemRoot%\System32\config\SECURITY %SystemRoot%\System32\config\SECURITY.LOG %SystemRoot%\System32\config\SECURITY.LOG1 %SystemRoot%\System32\config\SECURITY.LOG2
HKLM\SOFTWARE	%SystemRoot%\System32\config\SOFTWARE %SystemRoot%\System32\config\SOFTWARE.LOG %SystemRoot%\System32\config\SOFTWARE.LOG1 %SystemRoot%\System32\config\SOFTWARE.LOG2
HLLM\SYSTEM	%SystemRoot%\System32\config\SYSTEM %SystemRoot%\System32\config\SYSTEM.LOG %SystemRoot%\System32\config\SYSTEM.LOG1 %SystemRoot%\System32\config\SYSTEM.LOG2

레지스트리 소개

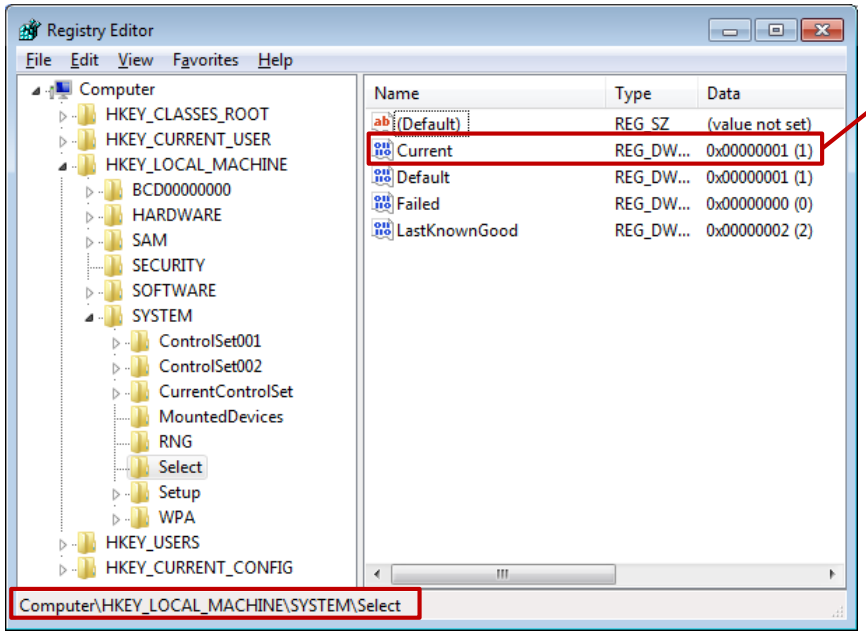


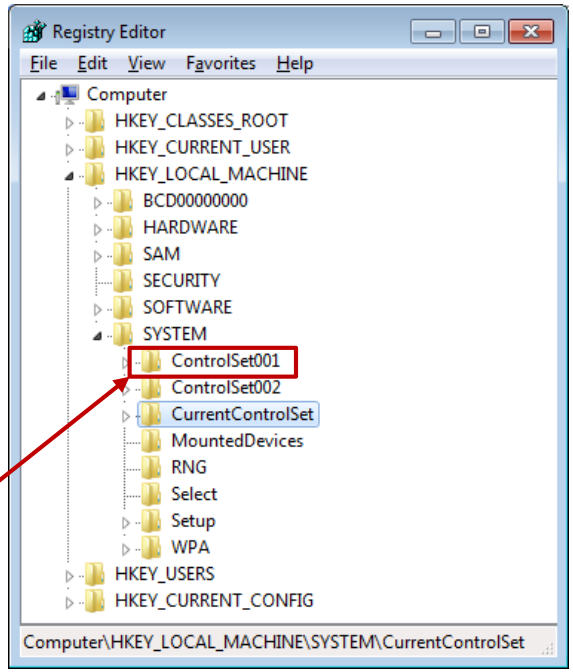
HKEY_LOCAL_MACHINE (HKLM)

- **하위키 내용**
  - **BCD00000000** – Boot Configuration Data 관리 (XP의 Boot.ini 대체)
  - **COMPONENTS** – 설치된 Components와 관련된 정보 관리
  - **HARDWARE** – 시스템 하드웨어 디스크립션과 모든 하드웨어의 장치 드라이버 매핑 정보 (Volatile hive)
  - **SAM** – 로컬 계정 정보와 그룹 정보 (시스템 계정만 접근 가능)
  - **SECURITY** – 시스템 보안 정책과 권한 할당 정보 (시스템 계정만 접근 가능)
  - **SOFTWARE** – 시스템 부팅에 필요없는 시스템 전역 구성 정보 (소프트웨어 정보)
  - **SYSTEM** – 시스템 부팅에 필요한 시스템 전역 구성 정보
    - 부팅 시 **HKLM₩SYSTEM** 하이브는 물리 메모리로 로드되기 때문에 하이브 파일 크기에 제한

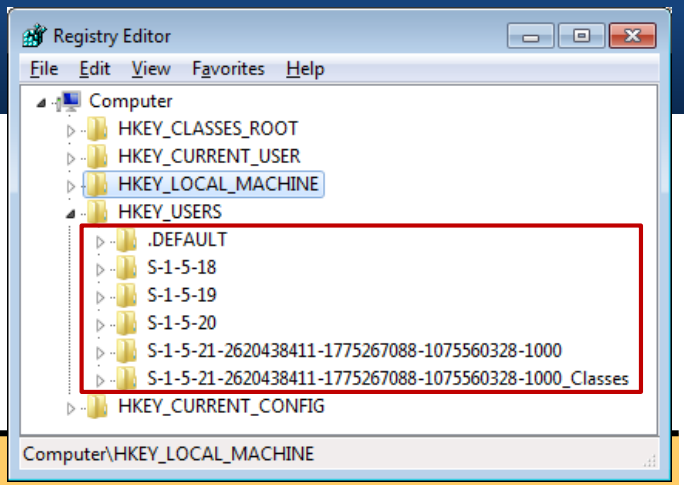
HKEY_LOCAL_MACHINE (HKLM)

- **HKLM₩SYSTEM₩CurrentControlSet**
  - 디바이스 드라이버와 서비스 등의 시스템 환경 설정 정보
  - ControlSet00**N**에 대한 링크
  - Select 키의 Current 값에 따라 현재 사용 중인 ControlSet 확인





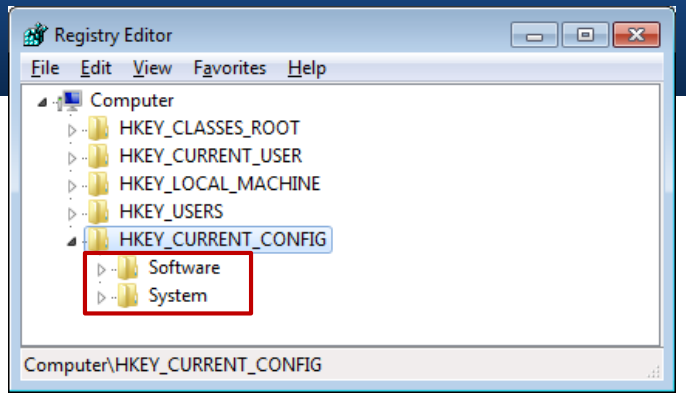
레지스트리 소개



HKEY_USERS (HKU)

- **하위키 구성**
  - 모든 사용자의 프로파일과 사용자 클래스 등록 정보

HKU 하위키	하이브 파일 위치
HKU\<LocalServices SID>	XP – %UserProfile%\LocalService\NTUSER.DAT Vista/7 - %SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT
HKU\<NetworkServices SID>	XP – %UserProfile%\NetworkService\NTUSER.DAT Vista/7 - %SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT
HKU\<User SID>	XP – %UserProfile%\<UserName>\NTUSER.DAT Vista/7 - %UserProfile%\NTUSER.DAT
HKU\<User SID>_Classes	XP – %UserProfile%\<UserName>\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat Vista/7 –%UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat
HKU\.DEFAULT	%SystemRoot%\System32\Config\DEFAULT



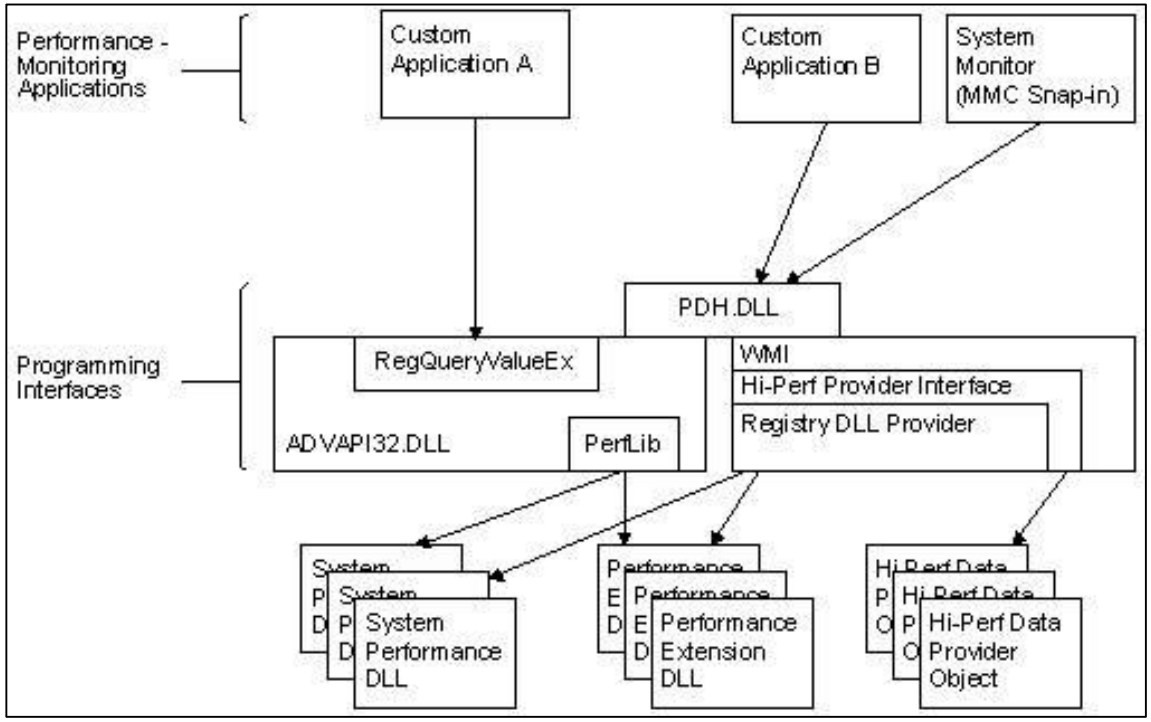
HKEY_CURRENT_CONFIG (HKCC)

- **하위키 구성**
  - 별도의 하이브 파일을 가지지 않음
  - 현재 활성화되어 있는 하드웨어 프로파일 정보 참조
  - **HKLM₩SYSTEM₩CurrentControlSet₩Hardware Profiles₩Current**의 링크

레지스트리 소개

HKEY_PERFORMANCE_DATA (HKPD)

- **HKPD 성능 카운터** (http://msdn.microsoft.com/en-us/library/aa371643(v=vs.85).aspx)
  - 시스템의 성능을 측정하여 관리하는 메커니즘 ➔ 운영체제, 응용프로그램에서 활용
  - 레지스트리 편집기를 통해 접근 불가
  - RegQueryValueEx() 와 같은 레지스트리 함수를 통해 접근 가능



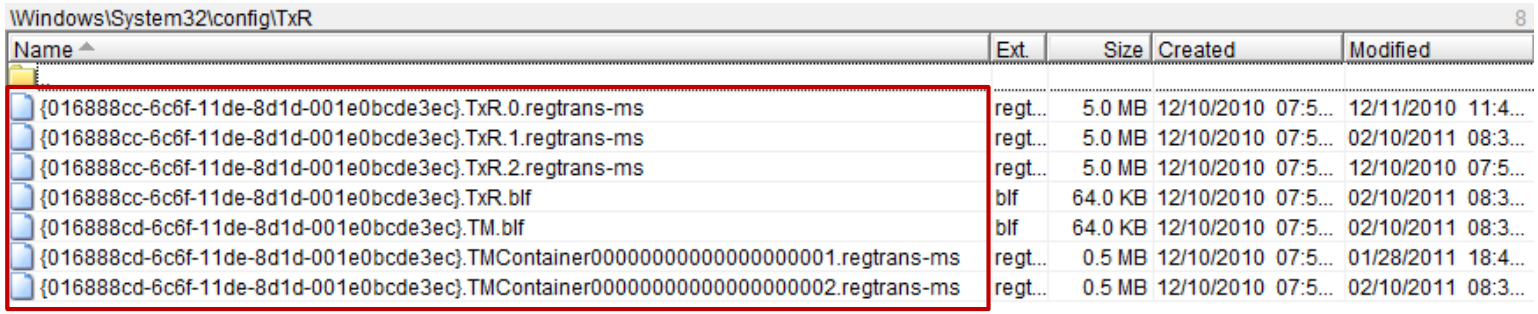
Transactional Registry (TxR)

- **트랜잭션 레지스트리 (TxR)** (http://forensic.korea.ac.kr/~webmaster/xe/?document_srl=2016)
  - Vista 이전 레지스트리에서는 트랜잭션 동작을 관리하기 어려웠음
  - Vista 부터 KTM(Kernel Transaction Manager)에 의해 오류 복구가 가능한 트랜잭션 기능 사용 가능

Not-Transaction API	Transaction API
RegOpenKey	RegOpenKeyTransacted
RegCreateKey	RegCreateKeyTransacted
RegDeleteKey	RegDeleteKeyTransacted

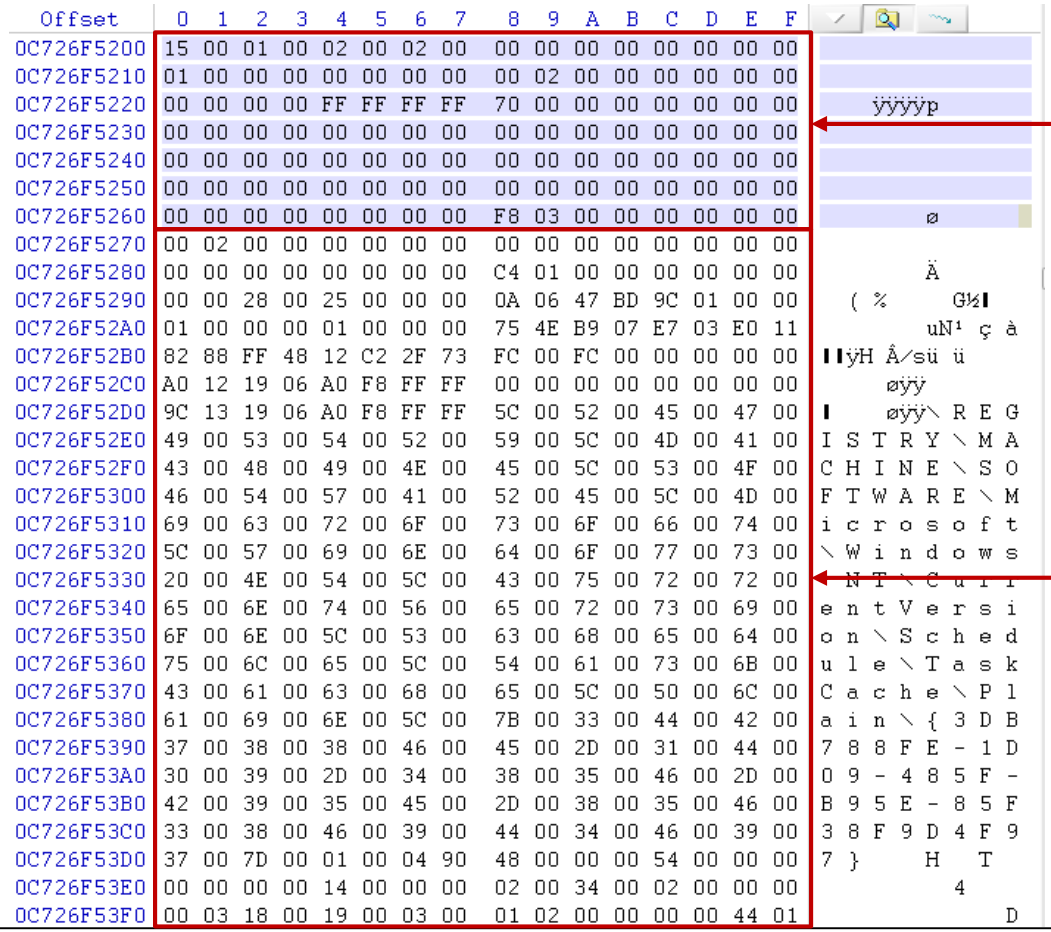
Transactional Registry (TxR)

- **트랜잭션 레지스트리 (TxR)**
  - 레지스트리 트랜잭션 정보는 파일로 저장
  - **%SystemRoot%₩System32₩config₩TxR**
    - %FILE%{%GUID%}.TM.blf
    - %FILE%{%GUID%}.TMContainer00000000000000000001.regtrans-ms
    - %FILE%{%GUID%}.TMContainer00000000000000000002.regtrans-ms
    - %FILE%{%GUID%}.TxR.blf
    - %FILE%{%GUID%}.TxR.0.regtrans-ms
    - %FILE%{%GUID%}.TxR.1.regtrans-ms
    - %FILE%{%GUID%}.TxR.2.regtrans-ms



Transactional Registry (TxR)

- **트랜잭션 레지스트리 (TxR)**
  - 로그 정보는 **TxR.{0|1|2}.regtrans-ms** 파일에 저장 (기본 5MB)



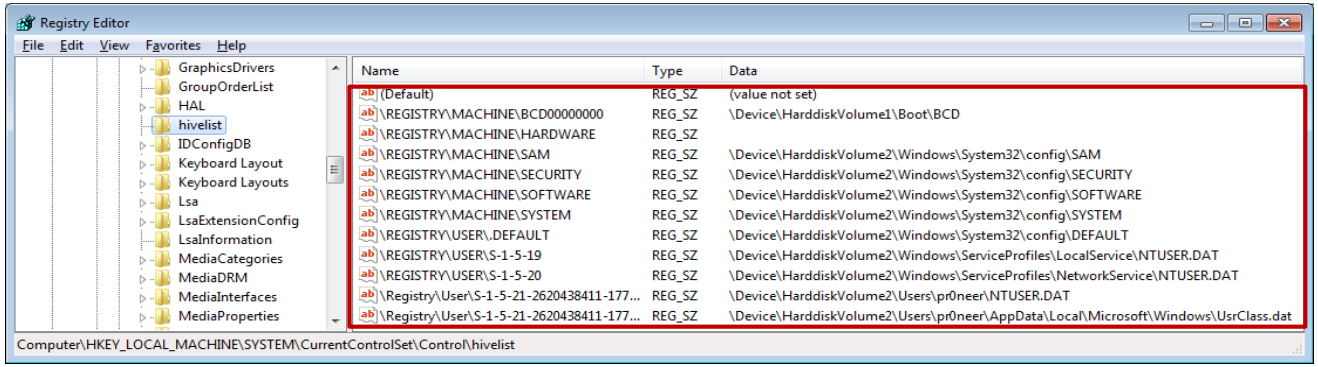
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0C726F5200	15	00	01	00	02	00	02	00	00	00	00	00	00	00	00	00
0C726F5210	01	00	00	00	00	00	00	00	00	02	00	00	00	00	00	00
0C726F5220	00	00	00	00	FF	FF	FF	FF	70	00	00	00	00	00	00	00
0C726F5230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C726F5240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C726F5250	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C726F5260	00	00	00	00	00	00	00	00	F8	03	00	00	00	00	00	00
0C726F5270	00	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0C726F5280	00	00	00	00	00	00	00	00	C4	01	00	00	00	00	00	00
0C726F5290	00	00	28	00	25	00	00	00	0A	06	47	BD	9C	01	00	00
0C726F52A0	01	00	00	00	01	00	00	00	75	4E	B9	07	E7	03	E0	11
0C726F52B0	82	88	FF	48	12	C2	2F	73	FC	00	FC	00	00	00	00	00
0C726F52C0	A0	12	19	06	A0	F8	FF	FF	00	00	00	00	00	00	00	00
0C726F52D0	9C	13	19	06	A0	F8	FF	FF	5C	00	52	00	45	00	47	00
0C726F52E0	49	00	53	00	54	00	52	00	59	00	5C	00	4D	00	41	00
0C726F52F0	43	00	48	00	49	00	4E	00	45	00	5C	00	53	00	4F	00
0C726F5300	46	00	54	00	57	00	41	00	52	00	45	00	5C	00	4D	00
0C726F5310	69	00	63	00	72	00	6F	00	73	00	6F	00	66	00	74	00
0C726F5320	5C	00	57	00	69	00	6E	00	64	00	6F	00	77	00	73	00
0C726F5330	20	00	4E	00	54	00	5C	00	43	00	75	00	72	00	72	00
0C726F5340	65	00	6E	00	74	00	56	00	65	00	72	00	73	00	69	00
0C726F5350	6F	00	6E	00	5C	00	53	00	63	00	68	00	65	00	64	00
0C726F5360	75	00	6C	00	65	00	5C	00	54	00	61	00	73	00	6B	00
0C726F5370	43	00	61	00	63	00	68	00	65	00	5C	00	50	00	6C	00
0C726F5380	61	00	69	00	6E	00	5C	00	7B	00	33	00	44	00	42	00
0C726F5390	37	00	38	00	38	00	46	00	45	00	2D	00	31	00	44	00
0C726F53A0	30	00	39	00	2D	00	34	00	38	00	35	00	46	00	2D	00
0C726F53B0	42	00	39	00	35	00	45	00	2D	00	38	00	35	00	46	00
0C726F53C0	33	00	38	00	46	00	39	00	44	00	34	00	46	00	39	00
0C726F53D0	37	00	7D	00	01	00	04	90	48	00	00	00	54	00	00	00
0C726F53E0	00	00	00	00	14	00	00	00	02	00	34	00	02	00	00	00
0C726F53F0	00	03	18	00	19	00	03	00	01	02	00	00	00	00	44	01

레지스트리 획득

Security is a people problem…

레지스트리 파일(하이브) 획득 방안

- **온라인 하이브 파일 획득**
  - 일반적으로 레지스트리 파일은 커널에서 열고 있기 때문에 획득 불가능
  - 직접 파일시스템을 해석하거나 DeviceIoControl() API를 이용하여 획득
  - 하이브 목록 확인 ➔ **HKLM₩SYSTEM₩CurrentControlSet₩Control₩hivelist**



- **오프라인 하이브 파일 획득**
  - 복제한 저장매체 혹은 이미징 데이터에서 하이브 파일 추출
  - 각 운영체제 버전별 하이브 파일 위치 확인 필요 ➔ %SystemRoot%₩System32₩Config
  - %UserProfile% 목록 확인 ➔ **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩ProfileList**

하이브 파일 위치

- **하이브 레지스트리 경로**

레지스트리 경로	하이브 파일 경로
HKEY_LOCAL_MACHINE\BCD00000000	{Boot Partition}\Boot\BCD
HEKY_LOCAL_MACHINE\COMPONENTS	%SystemRoot%\System32\Config\COMPONENTS
HEKY_LOCAL_MACHINE\SYSTEM	%SystemRoot%\System32\Config\SYSTEM
HEKY_LOCAL_MACHINE\SAM	%SystemRoot%\System32\Config\SAM
HEKY_LOCAL_MACHINE\SECURITY	%SystemRoot%\System32\Config\SECURITY
HEKY_LOCAL_MACHINE\SOFTWARE	%SystemRoot%\System32\Config\SOFTWARE
HEKY_LOCAL_MACHINE\HARDWARE	Volatile
HKEY_USERS\<SID of local service account>	%SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT
HKEY_USERS\<SID of network service account>	%SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT
HKEY_USERS\<SID of username>	%UserProfile%\NTUSER.DAT
HKEY_USERS\<SID of username>_Classes	%UserProfile%\AppData\Local\Microsoft\Windows\Usrclass.dat
HKEY_USERS\.DEFAULT	%SystemRoot%\System32\Config\DEFAULT

백업 및 로그 하이브

- **백업되거나 로그로 생성된 하이브 파일**
  - 운영체제에 의해 하이브 파일은 백업되거나 관련 로그가 생성됨
  - **백업 하이브** - %SystemRoot%₩System32₩config₩RegBack
  - **로그 하이브** – %SystemRoot%₩System32₩config (기본/백업 하이브 로그 (.LOG, .LOG1, .LOG2))
  - 로그 파일도 동일한 하이브 구조를 가짐
  - 백업이나 로그 하이브 파일은 기존 하이브 파일의 일부 정보만 저장

트랜잭션 레지스트리 로그 획득

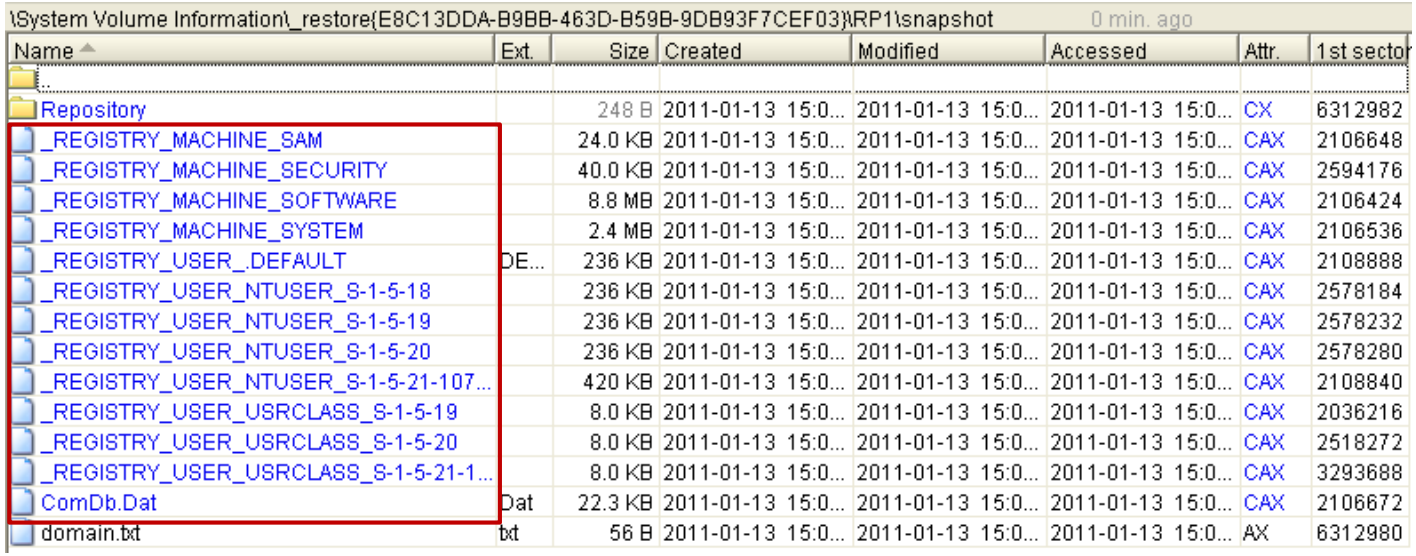
- **TxR 레지스트리 로그 획득**
  - **%SystemRoot%₩System32₩config₩TxR**

\Windows\System32\config\TxR

Name	Ext.	Size	Created	Modified
{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms	regt...	5.0 MB	12/10/2010 07:5...	12/11/2010 11:4...
{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms	regt...	5.0 MB	12/10/2010 07:5...	02/10/2011 08:3...
{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms	regt...	5.0 MB	12/10/2010 07:5...	12/10/2010 07:5...
{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf	blf	64.0 KB	12/10/2010 07:5...	02/10/2011 08:3...
{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf	blf	64.0 KB	12/10/2010 07:5...	02/10/2011 08:3...
{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms	regt...	0.5 MB	12/10/2010 07:5...	01/28/2011 18:4...
{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms	regt...	0.5 MB	12/10/2010 07:5...	02/10/2011 08:3...

XP 시스템 복원 지점

- **XP 시스템 복원 지점에서의 하이브 스냅샷**
  - 시스템 복원을 위해 레지스트리 하이브 파일 스냅샷 백업
  - 백업된 스냅샷 파일은 시스템 복원 정보 저장 시점의 사용자 흔적 파악에 큰 도움
  - **₩System Volume Information₩_restore{GUID}₩RP##₩snapshot**

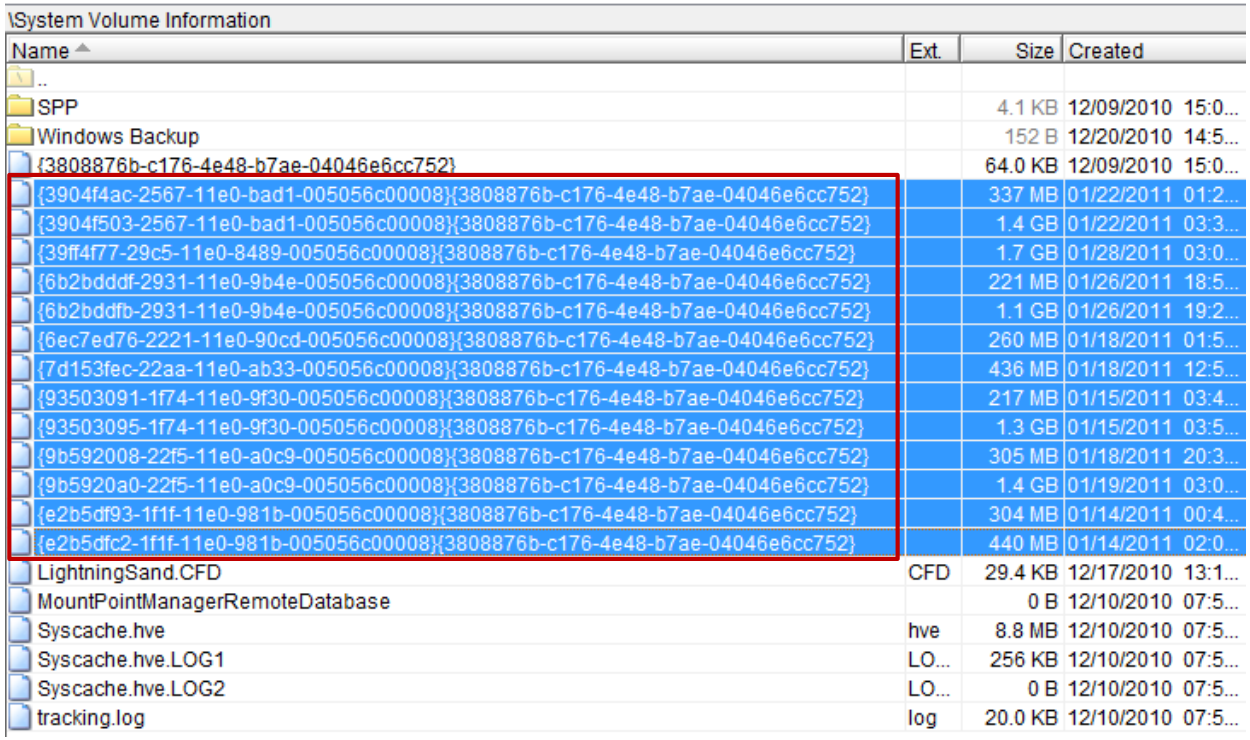


\System Volume Information_restore{E8C13DDA-B9BB-463D-B59B-9DB93F7CEF03}\RP1\snapshot 0 min. ago

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
..							
Repository		248 B	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CX	6312982
_REGISTRY_MACHINE_SAM		24.0 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2106648
_REGISTRY_MACHINE_SECURITY		40.0 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2594176
_REGISTRY_MACHINE_SOFTWARE		8.8 MB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2106424
_REGISTRY_MACHINE_SYSTEM		2.4 MB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2106536
_REGISTRY_USER_.DEFAULT	DE...	236 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2108888
_REGISTRY_USER_NTUSER_S-1-5-18		236 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2578184
_REGISTRY_USER_NTUSER_S-1-5-19		236 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2578232
_REGISTRY_USER_NTUSER_S-1-5-20		236 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2578280
_REGISTRY_USER_NTUSER_S-1-5-21-107...		420 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2108840
_REGISTRY_USER_USRCLASS_S-1-5-19		8.0 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2036216
_REGISTRY_USER_USRCLASS_S-1-5-20		8.0 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2518272
_REGISTRY_USER_USRCLASS_S-1-5-21-1...		8.0 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	3293688
ComDb.Dat	Dat	22.3 KB	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	CAX	2106672
domain.txt	txt	56 B	2011-01-13 15:0...	2011-01-13 15:0...	2011-01-13 15:0...	AX	6312980

Vista/7 시스템 복원 지점

- **VSS (Volume Shadow Copy) 내의 하이브 백업**
  - 비스타 이후부터는 시스템 복원 지점을 위해 VSS 사용
  - VSS 복사본에 하이브 데이터가 저장될 수 있음

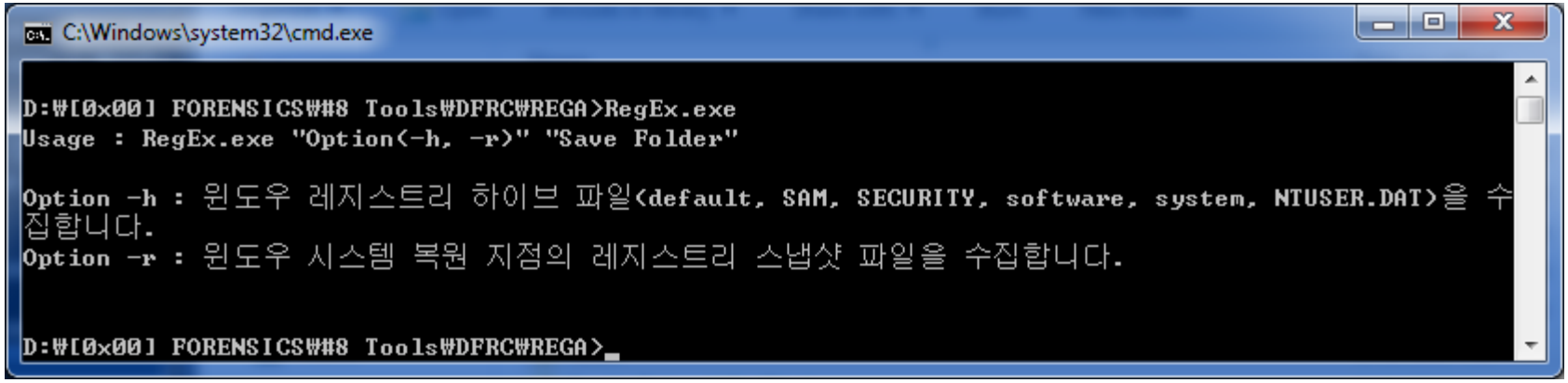


\System Volume Information

Name	Ext.	Size	Created
..			
SPP		4.1 KB	12/09/2010 15:0...
Windows Backup		152 B	12/20/2010 14:5...
{3808876b-c176-4e48-b7ae-04046e6cc752}		64.0 KB	12/09/2010 15:0...
{3904f4ac-2567-11e0-bad1-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		337 MB	01/22/2011 01:2...
{3904f503-2567-11e0-bad1-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.4 GB	01/22/2011 03:3...
{39ff4f77-29c5-11e0-8489-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.7 GB	01/28/2011 03:0...
{6b2bdddf-2931-11e0-9b4e-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		221 MB	01/26/2011 18:5...
{6b2bddfb-2931-11e0-9b4e-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.1 GB	01/26/2011 19:2...
{6ec7ed76-2221-11e0-90cd-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		260 MB	01/18/2011 01:5...
{7d153fec-22aa-11e0-ab33-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		436 MB	01/18/2011 12:5...
{93503091-1f74-11e0-9f30-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		217 MB	01/15/2011 03:4...
{93503095-1f74-11e0-9f30-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.3 GB	01/15/2011 03:5...
{9b592008-22f5-11e0-a0c9-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		305 MB	01/18/2011 20:3...
{9b5920a0-22f5-11e0-a0c9-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.4 GB	01/19/2011 03:0...
{e2b5df93-1f1f-11e0-981b-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		304 MB	01/14/2011 00:4...
{e2b5dfc2-1f1f-11e0-981b-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		440 MB	01/14/2011 02:0...
LightningSand.CFD	CFD	29.4 KB	12/17/2010 13:1...
MountPointManagerRemoteDatabase		0 B	12/10/2010 07:5...
Syscache.hve	hve	8.8 MB	12/10/2010 07:5...
Syscache.hve.LOG1	LO...	256 KB	12/10/2010 07:5...
Syscache.hve.LOG2	LO...	0 B	12/10/2010 07:5...
tracking.log	log	20.0 KB	12/10/2010 07:5...

레지스트리 온라인 하이브 획득 도구 – RegEx

- **RegEx – 활성시스템에서의 레지스트리 하이브 파일 수집 도구**



  - http://forensic.korea.ac.kr

레지스트리 내부

Security is a people problem…

하이브 구조

- **하이브 블록 (Hive Block)**
  - 파일시스템 클러스터와 같이 하이브에서 사용하는 논리적인 할당 단위
  - 블록 크기 : 4,096 바이트
  - 새로운 데이터가 하이브에 추가되면 항상 블록 단위로 증가
  - 하이브의 첫번째 블록은 베이스 블록 (base block)
    - 시그니처 (“regf”)
    - 갱신 순서 번호
    - 마지막 수정 시간
    - 레지스트리 복원/복구에 관한 정보
    - 하이브 포맷 버전 번호
    - 체크섬
    - 파일명

하이브 구조

- **하이브 빈 (Hive Bin)**
  - 레지스트리의 논리적인 크기는 블록 단위로 증가
  - 블록 내부적으로 데이터를 저장하기 위한 4,096 바이트의 구조
  - 레지스트리 로드시 하이브 빈 단위를 기준으로 로드
  - 모든 하이브 빈은 "hbin"이라는 시그니처 값으로 시작

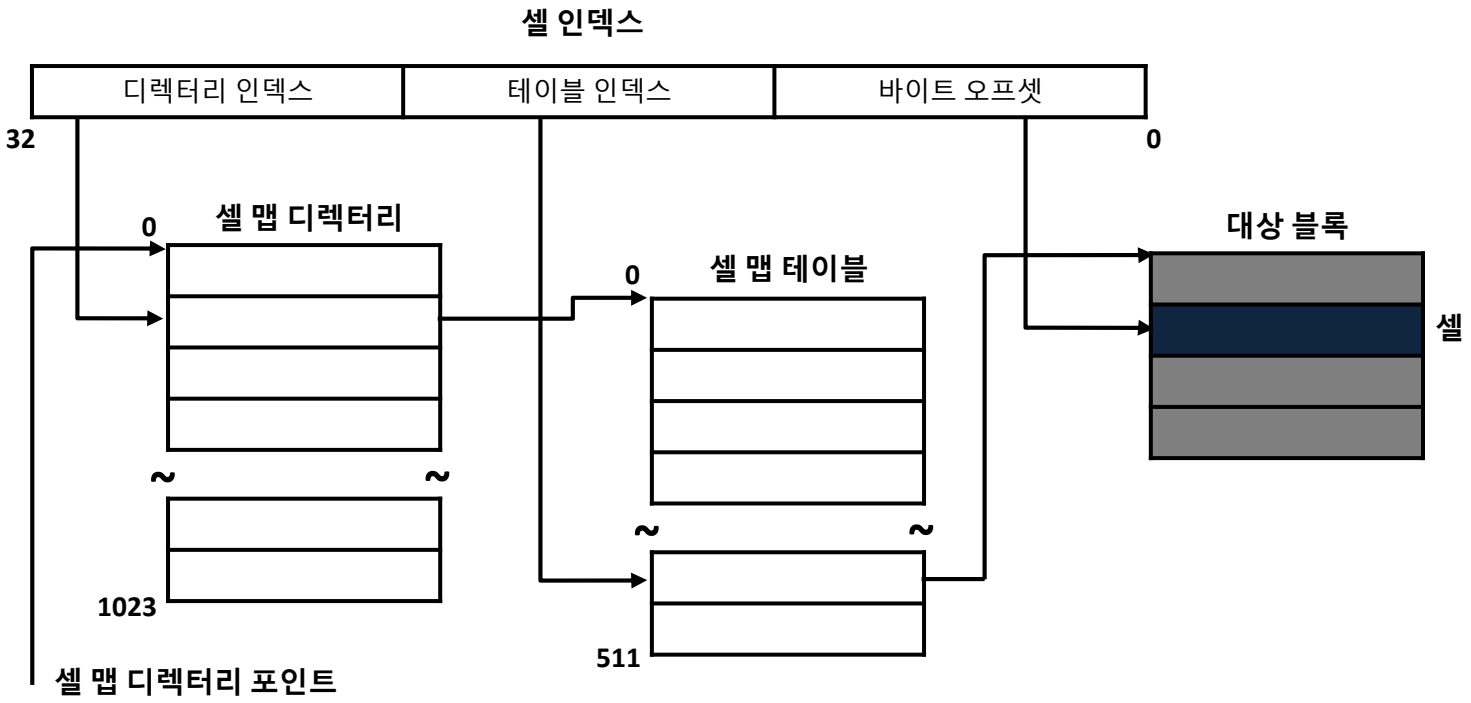
하이브 구조

- **셀 (Cell)**
  - 하이브 내의 다양한 데이터는 셀 구조로 저장 (8 바이트의 배수)

데이터 유형	설명
키 셀 (Key Cell)	레지스트리 키가 들어 있는 셀로 시그니처, 타임스탬프, 부모키 인덱스, 서브키 인덱스, 키 이름 등을 저장
값 셀 (Value Cell)	키에 대한 값이 들어있는 셀로 시그니처, 값 유형, 값 이름 등이 저장
하위키 목록 셀 (Subkey-list Cell)	부모키의 모든 하위키 셀의 인덱스 목록 저장
값 목록 셀 (Value-list Cell)	부모키의 모든 값 셀의 인덱스 목록 저장
데이터 셀 (Data Cell)	데이터를 저장하는 셀 (Big Data Cell, Normal Data Cell)
보안 기술자 셀 (Security-descriptor Cell)	보안 기술자 저장

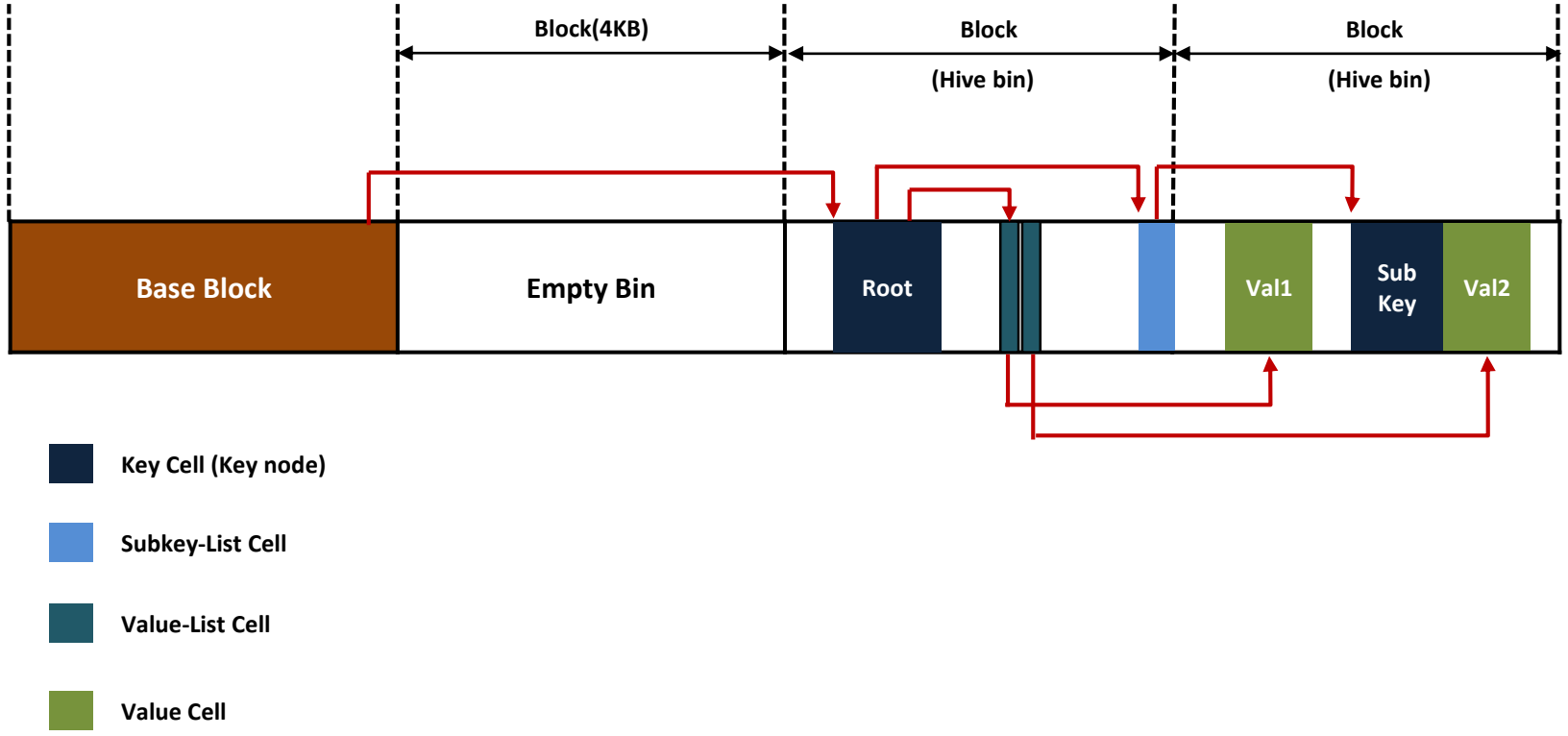
하이브 구조

- **셀 맵 (Cell Map)**
  - 레지스트리 접근시 매번 하이브 파일에 접근하지 않음
  - 하이브 접근을 위해 하이브 일부분을 메모리에 매핑
  - 메모리 내의 불연속적인 하이브 데이터를 참조하기 위해 셀 맵을 이용한 셀 인덱스 사용

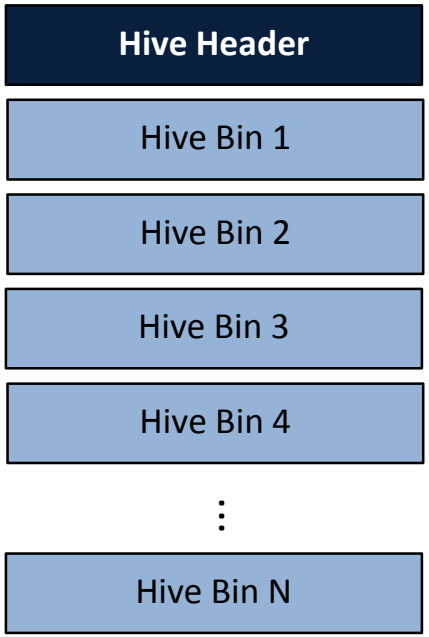


레지스트리 내부

하이브 구조 (http://technet.microsoft.com/en-us/library/cc750583.aspx)



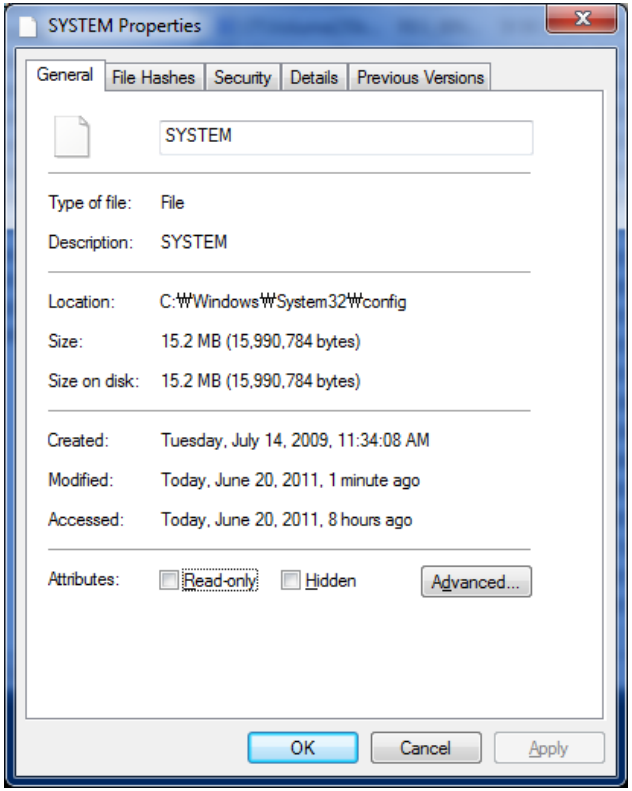
하이브 구조

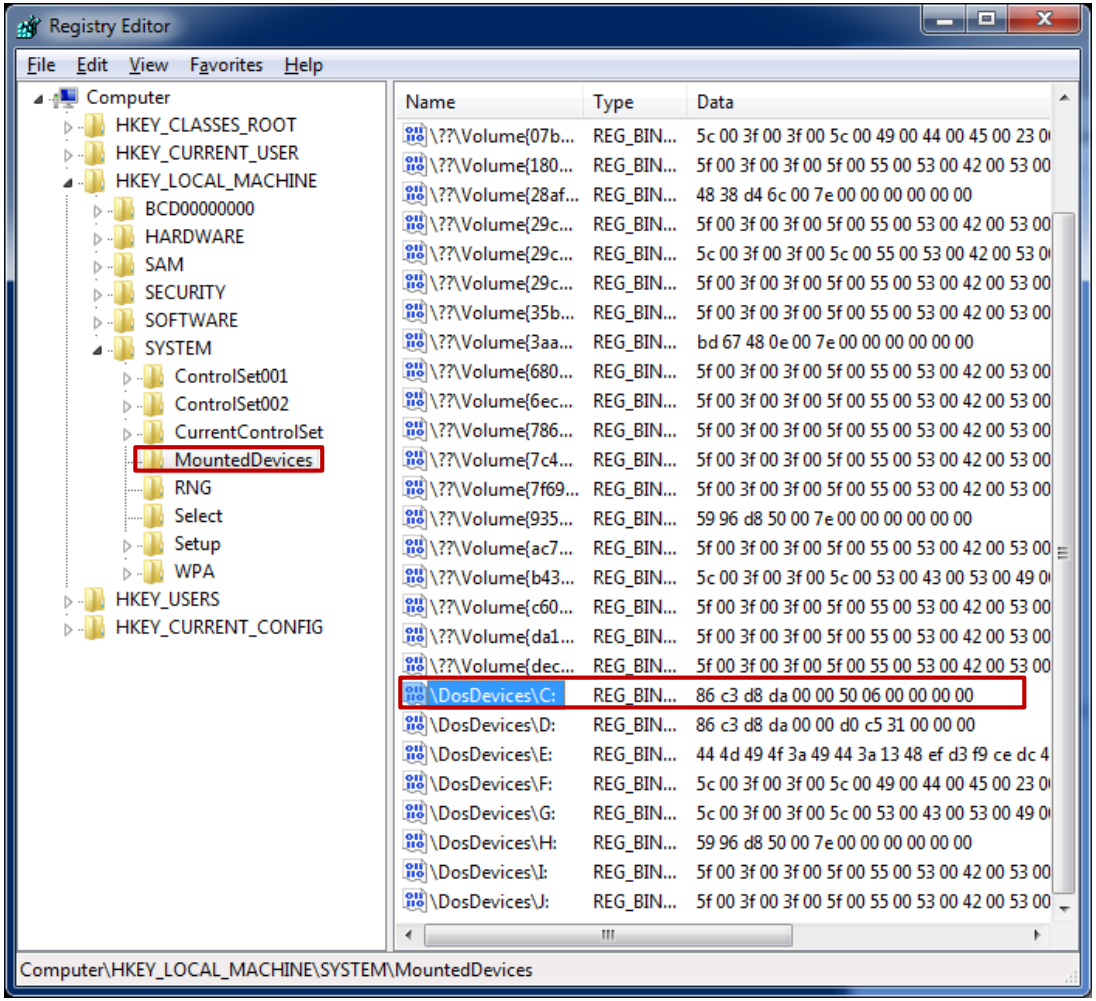


- **블록 크기**
  - 4,096 bytes
- **하이브 헤더(Hive Header)**
  - 1 블록
- **하이브 빈 (Hive Bin)**
  - 셀(Cell)을 포함하는 컨테이너
  - 가변 길이의 블록
  - 모든 하이브 빈은 "hbin"이라는 시그니처 값으로 시작
  - 레지스트리 로드시 하이브 빈 단위를 기준함
- **셀 (Cell)**
  - 실제 데이터를 저장하는 단위 (8 바이트의 배수)
  - 키(key), 하위키 목록(subkey-list), 값(value), 값 목록(value list), 데이터(data), 보안 기술자(security descriptor) 등의 유형이 있음

레지스트리 내부

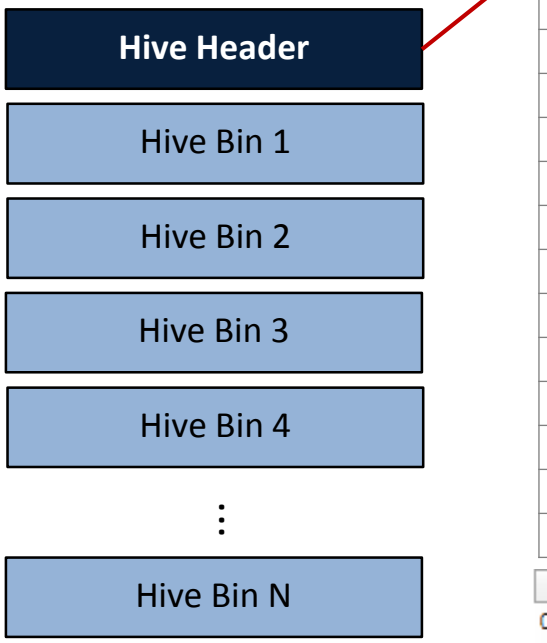
예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석





레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	r	e	g	f	seq num 1				seq num 2				**Timestamp**			
0010	(FILETIME)				major ver				minor ver				Type (?)			
0020	Format (?)				Start of Root Cell				Start of last hbin				Always 1			
0030	**Hive file path or name (Unicode, 64 bytes)**															
0040																
0050																
0060																
0070	GUID															
0080	GUID															
0090	Unknown				GUID											
00A0					Unknown											
...																
01F0													Checksum			

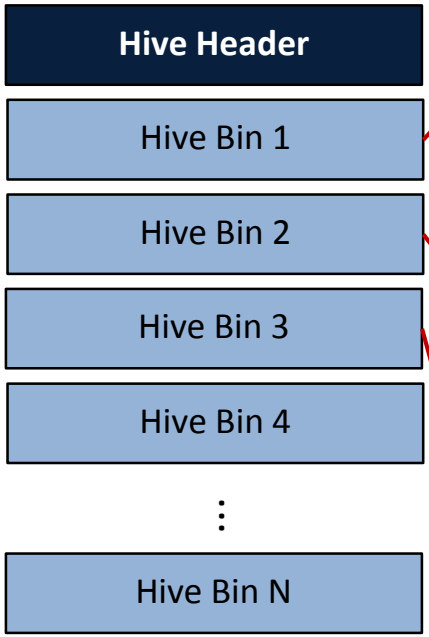
0x20 + 0x1000 = 0x1020

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 72 65 67 66 5A 31 01 00 5A 31 01 00 9D 70 55 36  regfZ1..Z1...pU6
0010h: 37 2F CC 01 01 00 00 00 05 00 00 00 00 00 00 00  7/Ì.............
0020h: 01 00 00 00 20 00 00 00 00 F0 F2 00 01 00 00 00  .... ....ðò.....
0030h: 53 00 59 00 53 00 54 00 45 00 4D 00 00 00 00 00  S.Y.S.T.E.M.....
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0070h: CC 88 68 01 6F 6C DE 11 8D 1D 00 1E 0B CD E3 EC  Ì^h.olÞ......Íãì
0080h: CC 88 68 01 6F 6C DE 11 8D 1D 00 1E 0B CD E3 EC  Ì^h.olÞ......Íãì
0090h: 01 00 00 00 CD 88 68 01 6F 6C DE 11 8D 1D 00 1E  ....Í^h.olÞ.....
00A0h: 0B CD E3 EC 72 6D 74 6D 00 00 00 00 00 00 00 00  .Íãìrmtm........

01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0h: 00 00 00 00 00 00 00 00 00 00 00 00 EE 93 6D DE  ............î"mÞ
```

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



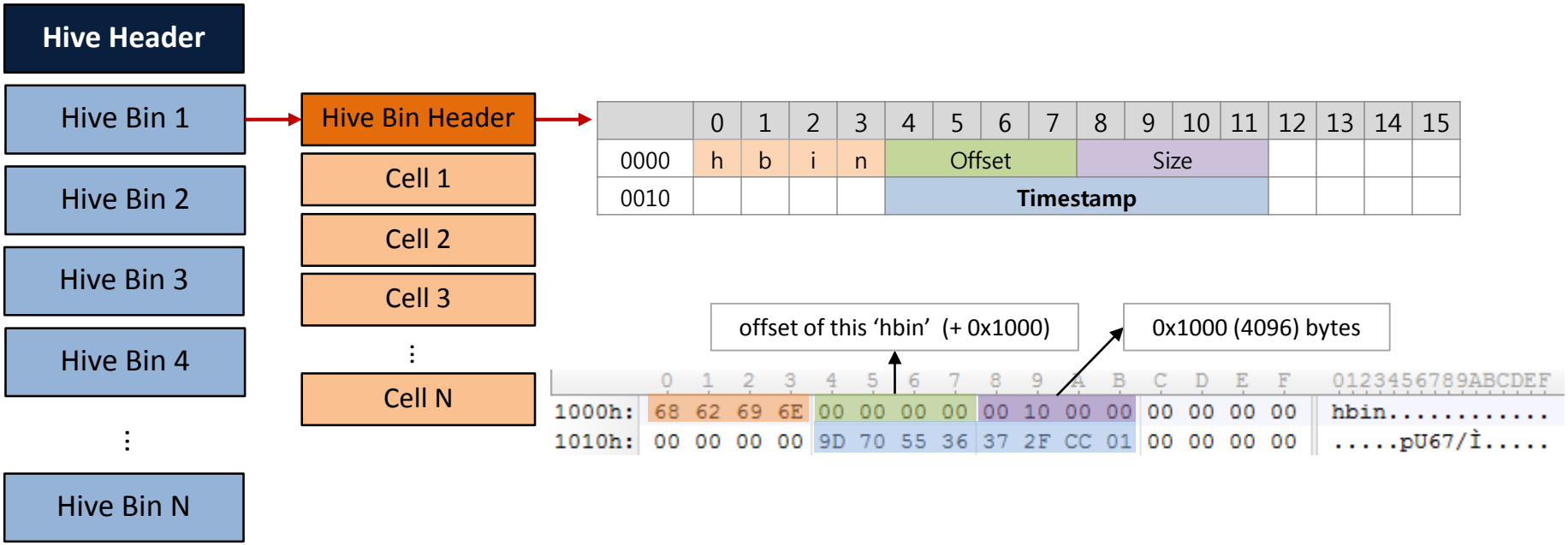
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1000h:	68	62	69	6E	00	00	00	00	00	10	00	00	00	00	00	00	hbin.....
1010h:	00	00	00	00	9D	70	55	36	37	2F	CC	01	00	00	00	00	.....pU67/Ì.....
1020h:	78	FF	FF	FF	6E	6B	2C	00	41	C9	38	BC	13	2F	CC	01	xÿÿÿnk,.AÉ8¼./Ì.
1030h:	00	00	00	00	78	02	00	00	07	00	00	00	01	00	00	00	....x.....
1040h:	B8	C0	11	00	78	01	00	80	00	00	00	00	FF	FF	FF	FF	¸À..x..€....ÿÿÿÿ
1050h:	00	FD	00	00	FF	FF	FF	FF	22	00	00	00	00	00	00	00	.ý..ÿÿÿÿ".....
1060h:	00	00	00	00	00	00	00	00	00	00	00	00	34	00	00	00	............4...

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2000h:	68	62	69	6E	00	10	00	00	00	10	00	00	00	00	00	00	hbin.....
2010h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
2020h:	C0	FF	FF	FF	76	6B	24	00	34	02	00	00	60	10	00	00	Àÿÿÿvk$.4...`...
2030h:	03	00	00	00	01	00	00	00	31	61	39	34	34	33	64	34	........1a9443d4
2040h:	2D	62	30	39	39	2D	34	34	64	36	2D	38	65	62	31	2D	-b099-44d6-8eb1-
2050h:	38	32	39	62	39	63	32	66	65	32	39	30	00	00	00	00	829b9c2fe290....
2060h:	C8	FD	FF	FF	01	00	04	80	14	00	00	00	24	00	00	00	Èýÿÿ...€....$...

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
3000h:	68	62	69	6E	00	20	00	00	00	10	00	00	00	00	00	00	hbin. .....
3010h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
3020h:	A8	FF	FF	FF	6E	6B	20	00	3E	0B	02	6B	3E	04	CA	01	¨ÿÿÿnk .>..k>.Ê.
3030h:	00	00	00	00	58	1F	00	00	02	00	00	00	00	00	00	00	....X.....
3040h:	78	9B	00	00	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	x›..ÿÿÿÿ....ÿÿÿÿ
3050h:	28	14	30	00	FF	FF	FF	FF	0E	00	01	00	00	00	00	00	(.0.ÿÿÿÿ.....
3060h:	00	00	00	00	00	00	00	00	01	00	00	00	05	00	00	00	.....

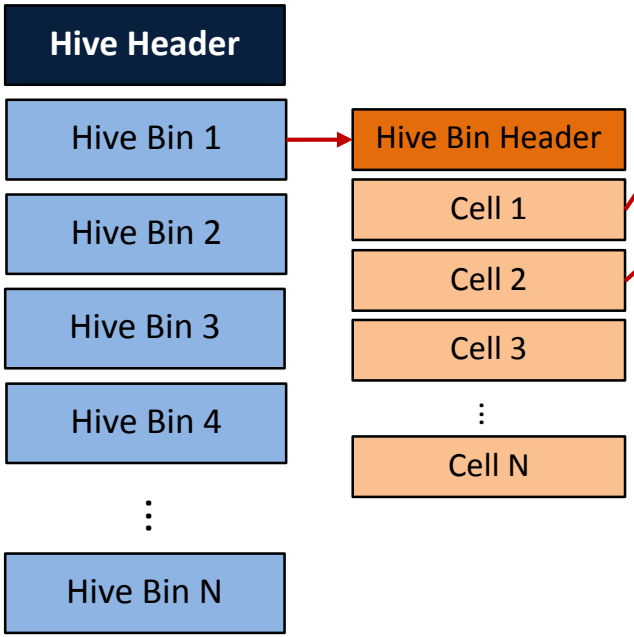
레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size															
0010	One of the Key (nk), Subkey-list (lf, lh, ri, li), Value (vk), Value-list, Security (sk), and Data															
...																
00XX	Cell Size															
00XX	One of the Key (nk), Subkey-list (lf, lh, ri, li), Value (vk), Value-list, Security (sk), and Data															
...																

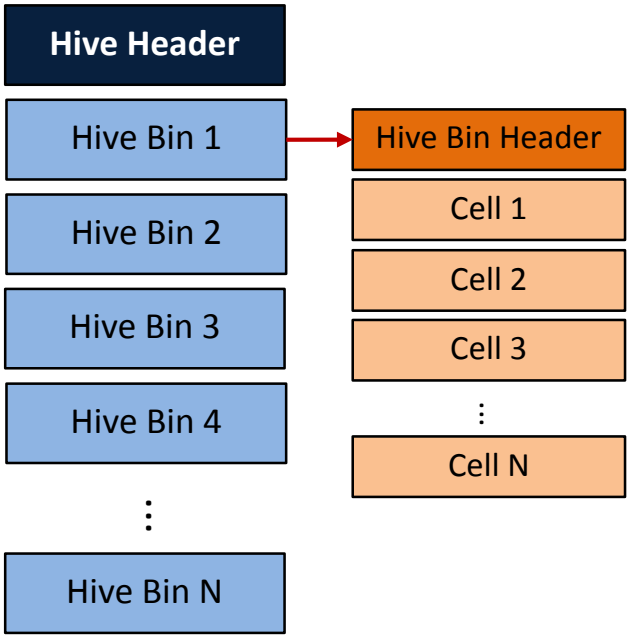
Negative if allocated
0xFFFFFF78 = -136

136

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1000h:	68	62	69	6E	00	00	00	00	00	10	00	00	00	00	00	00	hbin.....
1010h:	00	00	00	00	9D	70	55	36	37	2F	CC	01	00	00	00	00	.....pU67/Ì.....
1020h:	78	FF	FF	FF	6E	6B	2C	00	41	C9	38	BC	13	2F	CC	01	xÿÿÿnk,.AÉ8¼./Ì.
1030h:	00	00	00	00	78	02	00	00	07	00	00	00	01	00	00	00	....x.....
1040h:	B8	C0	11	00	78	01	00	80	00	00	00	00	FF	FF	FF	FF	¸À..x..€....ÿÿÿÿ
1050h:	00	FD	00	00	FF	FF	FF	FF	22	00	00	00	00	00	00	00	.ý..ÿÿÿÿ".....
106			00	00	00	00	00	00	00	00	00	00	34	00	00	00	.....4...
1070h:	43	4D	49	2D	43	72	65	61	74	65	48	69	76	65	7B	32	CMI-CreateHive{2
1080h:	41	37	46	42	39	39	31	2D	37	42	42	45	2D	34	46	39	A7FB991-7BBE-4F9
1090h:	44	2D	42	39	31	45	2D	37	43	42	35	31	44	34	37	33	D-B91E-7CB51D473
10A0h:	37	46	35	7D	FC	03	CA	01	A8	FF	FF	FF	6E	6B	20	00	7F5}ü.Ê.¨ÿÿÿnk .
10B0h:	09	82	22	68	3E	04	CA	01	00	00	00	00	30	06	00	00	.,"h>.Ê.....0...
10C0h:	0A	00	00	00	00	00	00	00	E0	C0	08	00	FF	FF	FF	FF	........àÀ..ÿÿÿÿ
10D0h:	00	00	00	00	FF	FF	FF	FF	10	FC	00	00	FF	FF	FF	FF	....ÿÿÿÿ.ü..ÿÿÿÿ

레지스트리 내부

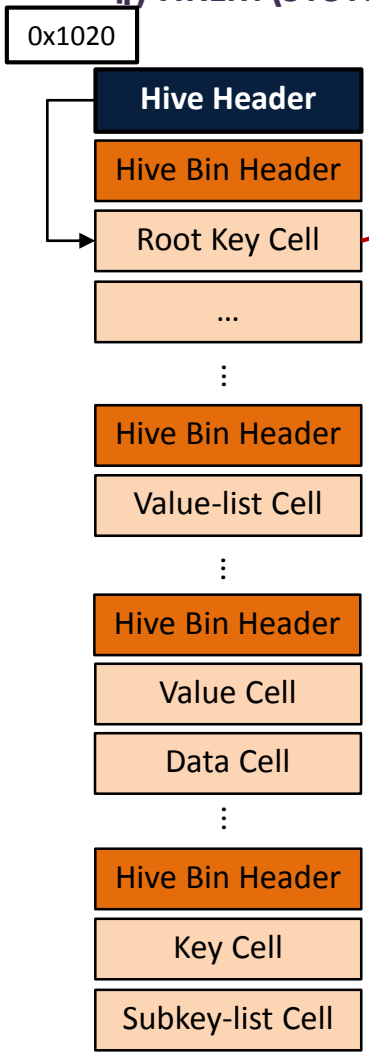
예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1000h:	68	62	69	6E	00	00	00	00	00	10	00	00	00	00	00	00	hbin.....
1010h:	00	00	00	00	9D	70	55	36	37	2F	CC	01	00	00	00	00	.....pU67/Ì.....
1020h:	78	FF	FF	FF	6E	6B	2C	00	41	C9	38	BC	13	2F	CC	01	xÿÿÿnk,.AÉ8¼./Ì.
1030h:	00	00	00	00	78	02	00	00	07	00	00	00	01	00	00	00	....x.....
1040h:	B8	C0	11	00	78	01	00	80	00	00	00	00	FF	FF	FF	FF	¸À..x..€....ÿÿÿÿ
1050h:	00	FD	00	00	FF	FF	FF	FF	22	00	00	00	00	00	00	00	.ý..ÿÿÿÿ".....
1060h:	00	00	00	00	00	00	00	00	00	00	00	00	34	00	00	00	............4...
1070h:	43	4D	49	2D	43	72	65	61	74	65	48	69	76	65	7B	32	CMI-CreateHive{2
1080h:	41	37	46	42	39	39	31	2D	37	42	42	45	2D	34	46	39	A7FB991-7BBE-4F9
1090h:	44	2D	42	39	31	45	2D	37	43	42	35	31	44	34	37	33	D-B91E-7CB51D473
10A0h:	37	46	35	7D	FC	03	CA	01	A8	FF	FF	FF	6E	6B	20	00	7F5}ü.Ê.¨ÿÿÿnk .
10B0h:	09	82	22	68	3E	04	CA	01	00	00	00	00	30	06	00	00	.,"h>.Ê.....0...
10C0h:	0A	00	00	00	00	00	00	00	E0	C0	08	00	FF	FF	FF	FF	........àÀ..ÿÿÿÿ
10D0h:	00	00	00	00	FF	FF	FF	FF	10	FC	00	00	FF	FF	FF	FF	....ÿÿÿÿ.ü..ÿÿÿÿ
10E0h:	1E	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	....
10F0h:	2F	00	00	00	03	00	00	00	4E	6C	73	0B	95	0A	2F	00	/.......Nls.•./.
1100h:	A0	FF	FF	FF	6E	6B	20	00	0E	A2	29	73	3E	04	CA	01	ÿÿÿnk ..¢)s>.Ê.
1110h:	00	00	00	00	F8	C2	01	00	02	00	00	00	00	00	00	00	....øÂ..........
1120h:	48	C6	01	00	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	HÆ..ÿÿÿÿ....ÿÿÿÿ
1130h:	E0	54	2C	00	FF	FF	FF	FF	1C	00	01	00	00	00	00	00	àT,.ÿÿÿÿ........
1140h:	00	00	00	00	00	00	00	00	00	00	00	00	0D	00	00	00	....
1150h:	4E	6F	74	69	66	69	63	61	74	69	6F	6E	73	DC	01	00	NotificationsÜ..
1160h:	A0	FF	FF	FF	6E	6B	20	00	FF	A4	E1	E0	A0	9D	CB	01	ÿÿÿnk .ÿ¤áà .Ë.
1170h:	00	00	00	00	20	00	00	00	05	00	00	00	00	00	00	00	....
1180h:	60	86	2C	00	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	`†,.ÿÿÿÿ....ÿÿÿÿ
1190h:	10	FC	00	00	FF	FF	FF	FF	24	00	01	00	00	00	00	00	.ü..ÿÿÿÿ$.....
11A0h:	00	00	00	00	00	00	00	00	00	00	00	00	0D	00	00	00	....
11B0h:	43	6F	6E	74	72	6F	6C	53	65	74	30	30	31	00	00	00	ControlSet001...
11C0h:	F0	FF	FF	FF	88	AB	01	00	F0	AB	01	00	18	AC	01	00	ðÿÿÿˆ«..ð«...¬..
11D0h:	A8	FF	FF	FF	6E	6B	20	00	D8	BC	00	BD	13	2F	CC	01	¨ÿÿÿnk .Ø¼.½./Ì.
11E0h:	00	00	00	00	60	01	00	00	0F	02	00	00	01	00	00	00	....`...........

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



Key Cell

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	Cell Size				n	k	Flag		Timestamp							
0010	Unknown				Parent key offset				Num of subkeys (stable)				Num of subkeys (volatile)			
0020	Subkey-list offset				Subkey-list offset				Num of values				Value-list offset			
0030	Security offset				Classname offset				Max name length of subkeys				Max classname length of subkeys			
0040	Max name length of values				Max value data size				Unknown				Keyname len		Classname len	
0050	Key name															
0060																
...																

0x0004 : Root, 0x0008 : cannot be deleted
0x0020 : key name is stored in ASCII

0x0011C0B8
+
0x1000
=
0x0011D0B8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1000h:	68	62	69	6E	00	00	00	00	00	10	00	00	00	00	00	00	hbin.....
1010h:	00	00	00	00	9D	70	55	36	37	2F	CC	01	00	00	00	00	.....pU67/Ì....
1020h:	78	FF	FF	FF	6E	6B	2C	00	41	C9	38	BC	13	2F	CC	01	xÿÿÿnk,.AÉ8¼./Ì.
1030h:	00	00	00	00	78	02	00	00	07	00	00	00	01	00	00	00	....x.....
1040h:	B8	C0	11	00	78	01	00	80	00	00	00	00	FF	FF	FF	FF	¸À..x..€....ÿÿÿÿ
1050h:	00	FD	00	00	FF	FF	FF	FF	22	00	00	00	00	00	00	00	.ý..ÿÿÿÿ".....
1060h:	00	00	00	00	00	00	00	00	00	00	00	00	34	00	00	00	.....4...
1070h:	43	4D	49	2D	43	72	65	61	74	65	48	69	76	65	7B	32	CMI-CreateHive{2
1080h:	41	37	46	42	39	39	31	2D	37	42	42	45	2D	34	46	39	A7FB991-7BBE-4F9
1090h:	44	2D	42	39	31	45	2D	37	43	42	35	31	44	34	37	33	D-B91E-7CB51D473
10A0h:	37	46	35	7D	FC	03	CA	01	A8	FF	FF	FF	6E	6B	20	00	7F5}ü.Ê.¨ÿÿÿnk .
10B0h:	09	82	22	68	3E	04	CA	01	00	00	00	00	30	06	00	00	.,"h>.Ê.....0...
10C0h:	0A	00	00	00	00	00	00	00	E0	C0	08	00	FF	FF	FF	FF	........àÀ..ÿÿÿÿ
10D0h:	00	00	00	00	FF	FF	FF	FF	10	FC	00	00	FF	FF	FF	FF	....ÿÿÿÿ.ü..ÿÿÿÿ

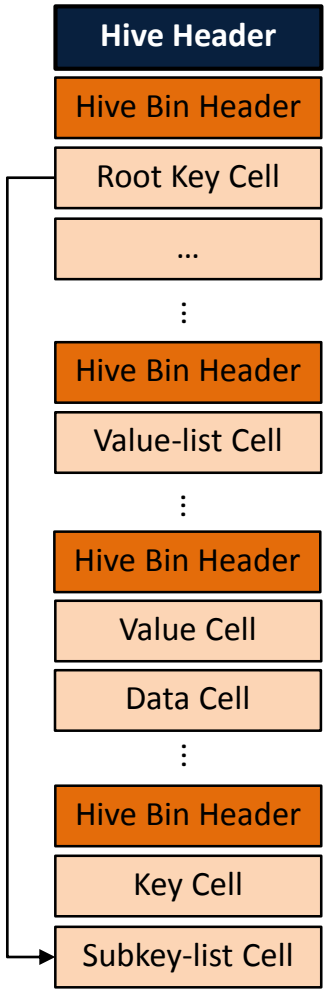
예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석

- **키 플래그 (Key Flags)**

플래그	설명
0x0001	휘발성 키
0x0002	다른 하이브의 마운트 지점
0x0004	루트키
0x0008	삭제할 수 없는 키
0x0010	링크된 키
0x0020	키 이름을 ASCII로 저장 (보통은 UTF-16LE로 저장)
0x0040	미리 정의된 키
0x0080	알 수 없음
0x1000	알 수 없음
0x4000	알 수 없음

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



Subkey-list Cell (ri : Index Root, li: Index Leaf)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size				r	i	Num		Subkey-list offset				Subkey-list offset			
0010	Subkey-list offset				Subkey-list offset				Subkey-list offset							
...																

Subkey-list Cell (lf: Fast Leaf, lh: Hash Leaf)

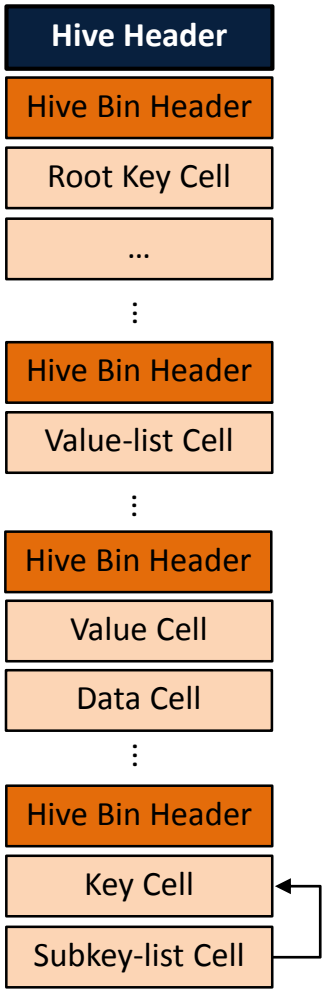
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size				l	f	Num		Key (nk) offset				hash value			
0010	Key (nk) offset				hash value				Key (nk) offset				hash value			
...																

0x2DD398 + 0x1000 = 0x2DE398

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
11:D0B0h: 57 50 41 00 00 00 00 00 C0 FF FF FF 6C 68 07 00 WPA.....Àÿÿÿlh..
11:D0C0h: 60 01 00 00 A2 A9 3B 8F B8 A3 3F 00 A3 A9 3B 8F `...¢©;.¸£?.£©;.
11:D0D0h: 98 D3 2D 00 2B 07 7A FC 40 1A 09 00 0F C2 01 00 ˜Ó-.+.zü@....Â..
11:D0E0h: A8 F8 08 00 A0 24 00 5F C8 A9 01 00 81 B8 7C 09 ¨ø.. $._È©...¸|.
11:D0F0h: 60 C0 11 00 10 DD 01 00 98 FF FF FF 6E 6B 20 00 `À...Ý..˜ÿÿÿnk .
11:D100h: 4B CA 30 68 3E 04 CA 01 00 00 00 00 50 1B 00 00 KÊ0h>.Ê.....P...
11:D110h: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF ........ÿÿÿÿÿÿÿÿ
11:D120h: 02 00 00 00 48 A7 01 00 40 F8 01 00 FF FF FF FF ....H§..@ø..ÿÿÿÿ
11:D130h: 00 00 01 00 00 00 00 00 20 00 00 00 3C 00 00 00 ........ ...<...
```

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



Key Cell

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	Cell Size				n	k	Flag		Timestamp							
0010	Unknown				Parent key offset				Num of subkeys (stable)				Num of subkeys (volatile)			
0020	Subkey-list offset				Subkey-list offset				Num of values				Value-list offset			
0030	Security cell offset				Classname offset				Max name length of subkeys				Max classname length of subkeys			
0040	Max name length of values				Max value data size				Unknown				Keyname len		Classname len	
0050	Key name															
0060																

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
553:E300h: A8 FF FF FF 6E 6B 20 00 F3 C5 22 B8 E7 41 CB 01  ¨ÿÿÿnk .óÅ",çAË.
553:E310h: 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00  .... ............
553:E320h: FF FF FF FF FF FF FF FF 02 00 00 00 58 E2 D3 01  ÿÿÿÿÿÿÿÿ....XâÓ.
553:E330h: D0 EE 22 01 FF FF FF FF 00 00 00 00 00 00 00 00  Ðî".ÿÿÿÿ........
553:E340h: 0C 00 00 00 2E 00 00 00 39 36 38 46 04 00 00 00  ........968F....
553:E350h: 50 65 72 6C 44 37 46 33 B8 FE FF FF 6C 68 1E 00  PerlD7F3¸þÿÿlh..
```

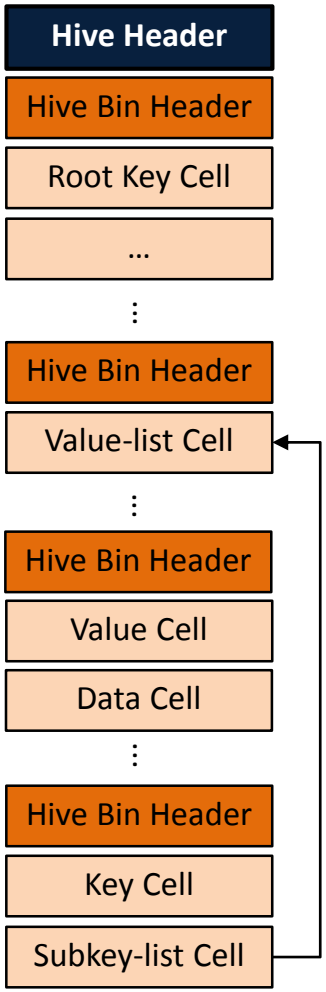
0x00D57918 + 0x1000 = 0x00D58918

0x0020 : key name is stored in ASCII

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2D:E390h: 53 59 53 54 45 4D 7F 00 A0 FF FF FF 6E 6B 20 00  SYSTEM.. ÿÿÿnk .
2D:E3A0h: 34 98 18 15 27 2F CC 01 00 00 00 00 20 00 00 00  4˜..'/Ì..... ...
2D:E3B0h: 00 00 00 00 00 00 00 00 FF FF FF FF FF FF FF FF  ........ÿÿÿÿÿÿÿÿ
2D:E3C0h: 1E 00 00 00 18 79 D5 00 10 46 13 00 FF FF FF FF  .....yÕ..F..ÿÿÿÿ
2D:E3D0h: 00 00 00 00 00 00 00 00 60 00 00 00 F6 00 00 00  ........`...ö...
2D:E3E0h: 02 00 00 00 0E 00 00 00 4D 6F 75 6E 74 65 64 44  ........MountedD
2D:E3F0h: 65 76 69 63 65 73 77 6E D8 FF FF FF 76 6B 0E 00  eviceswnØÿÿÿvk..
```

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



Value-list Cell

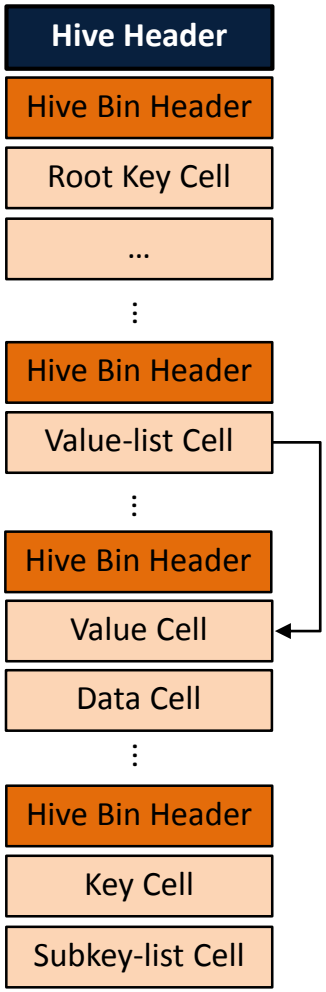
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size				Value offset				Value offset				Value offset			
0010	Value offset				Value offset				Value offset							
...																

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
D5:8910h: 7D 00 FF FF FF FF FF FF 80 FF FF FF F8 D3 2D 00  }.ÿÿÿÿÿÿ€ÿÿÿøÓ-.
D5:8920h: A0 94 34 00 68 98 34 00 C0 98 34 00 18 49 35 00   "4.h˜4.À˜4..I5.
```

0x002DD3F8 + 0x1000 = 0x002DE3F8

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



Value Cell

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000	Cell Size				v	k	Name len		Data length				Data offset			
0010	Data Type				Flag		Unknown									
0020	Value Name															
...																

0x002DD420 + 0x1000 = 0x002DE420

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
2D:E3F0h:	65	76	69	63	65	73	77	6E	D8	FF	FF	FF	76	6B	0E	00	eviceswnØÿÿÿvk..
2D:E400h:	0C	00	00	00	20	D4	2D	00	03	00	00	00	01	00	00	00	.... Ô-........
2D:E410h:	5C	44	6F	73	44	65	76	69	63	65	73	5C	43	3A	00	05	\DosDevices\C:..

0x0001 : value name is stored in ASCII, otherwise it is in Unicode

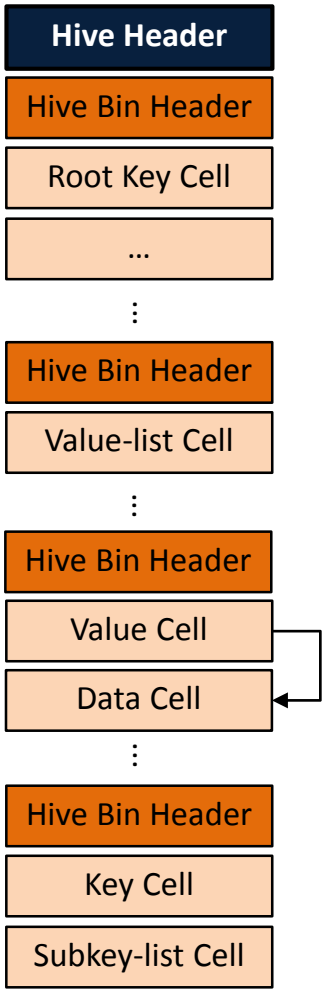
예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석

- **데이터 형식 (Data Type)**

값	이름	설명
0x00	REG_NONE	형식 없음
0x01	REG_SZ	UTF-16 문자열
0x02	REG_EXPAND_SZ	시스템 경로로 사용하는 UTF-16 문자열 (예, “%SYSTEMROOT%”)
0x03	REG_BINARY	이진 데이터
0x04	REG_DWORD	32비트 정수
0x04	REG_DWORD_LITTLE_ENDIAN	32비트 정수
0x05	REG_DWORD_BIG_ENDIGN	32비트 빅엔디안 정수
0x06	REG_LINK	심볼릭 링크
0x07	REG_MULTI_SZ	NULL로 끝나는 유니코드 문자열 배열
0x08	REG_RESOURCE_LIST	하드웨어 리소스 설명
0x09	REG_RESOURCE_DESCRIPTOR	하드웨어 리소스 설명
0x0A	REG_RESOURCE_REQUIREMENTS_LIST	리소스 요구사항
0x0B	REG_QWORD	64비트 정수
0x0B	REG_QWORD_LITTTLE_ENDIAN	64비트 정수

레지스트리 내부

예) HKLM\SYSTEM\MountedDevices (\DosDevices\C:) 분석



Big Data Cell → Version 1.4 or later, Data size > 16344 bytes

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size				d	b	Num of frag		Indirect cell offset				Unknown			

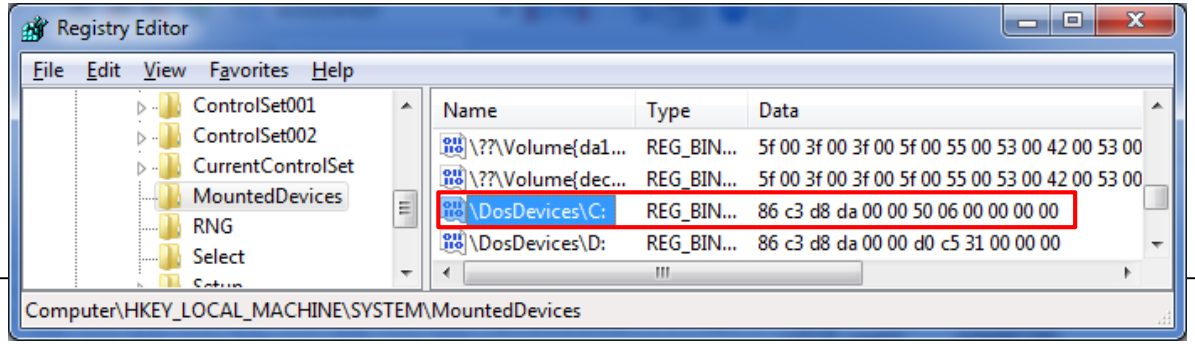
Big Data Indirect Cell

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size				Data offset				Data offset				Data offset			
...	Data offset															

(Normal) Data Cell

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0000	Cell Size				Data											
...																

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
2D:E420h: F0 FF FF FF 86 C3 D8 DA 00 00 50 06 00 00 00 00 ðÿÿÿ†ÃØÚ..P.....
2D:E430h: A8 FF FF FF 6E 6B 20 00 83 11 47 BC 13 2F CC 01 ¨ÿÿÿnk .ƒ.G¼./Ì.
2D:E440h: 00 00 00 00 D8 A3 2E 00 00 00 00 00 01 00 00 00 ....Ø£..........
```



레지스트리 복구

Security is a people problem…

레지스트리 복구 분류

- **삭제된 레지스트리 복구**
  - **레지스트리 하이브 내부로부터 삭제된 레지스트리 복구**
    - 윈도우 레지스트리 API를 이용해서 키(key)를 삭제하는 경우 해당 키와 관련된 링크 정보만 삭제
    - 해당 키와 관련된 실제 데이터는 하이브 파일 내의 비할당 영역에 그대로 유지됨
- **레지스트리 데이터 카빙**
  - **물리 메모리로부터 레지스트리 데이터 카빙**
    - 커널 영역에 레지스트리 데이터에 대한 캐쉬 영역 존재 ➔ 물리적인 하이브 파일과 매핑되어 있음
    - 응용프로그램 수행 과정에서 사용된(생성/읽기/쓰기/삭제) 레지스트리 정보는 레지스트리에 존재
    - 각 프로세스 영역을 통해 특정 프로세스가 사용한 레지스트리 정보 확인
  - **저장 매체의 비할당 영역으로부터 레지스트리 데이터 카빙**
    - 파일시스템 포맷으로 인해 이전 시스템의 레지스트리 데이터가 저장 매체의 비할당 영역에 존재할 가능성
    - 시스템 복원지점 생성시 레지스트리 복사 후 폴더 압축에 의해 비할당 영역에 존재할 가능성 (2000/XP)

레지스트리 복구

물리 메모리 카빙

- **CMHIVE 카빙** (http://www.dfrws.org/2008/proceedings/p26-dolan-gavitt.pdf)
  - 레지스트리 하이브는 메모리에서 CMHIVE 구조로 표현 (http://www.nirsoft.net/kernel_struct/vista/CMHIVE.html)
  - CHHIVE 구조를 카빙하여 레지스트리 정보를 획득
  - **Volatility Plugin** (http://moyix.blogspot.com/2009/01/memory-registry-tools.html) (1.4 버전부터 포함)
    - hivescan
    - hivelist
    - printkey
    - hashdump
    - lasdump
    - cachedump

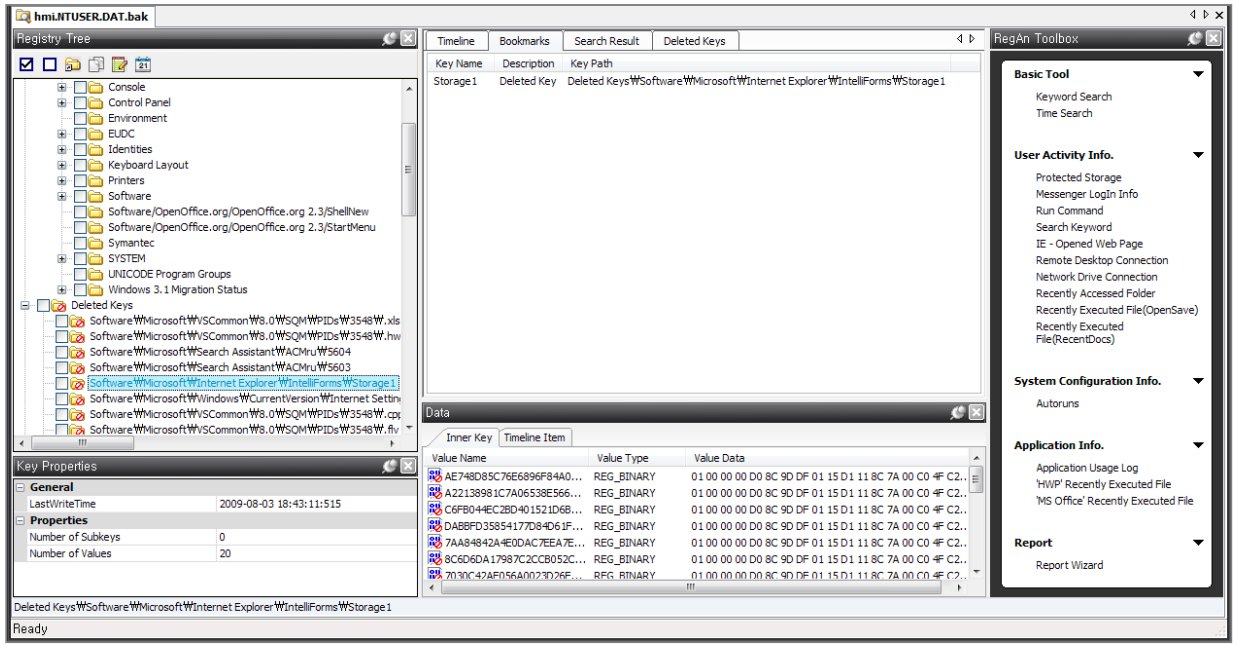
파일 시스템 비할당 영역 카빙

- **레지스트리 시그니처 카빙** (http://seclab.hdu.edu.cn/%E5%AE%9E%E9%AA%8C%E5%AE%A4%E8%AE%BA%E6%96%87/2009/Carving%20the%20windows%20registry%20files%20based%20on%20the%20internal%20structure.PDF)
  - 레지스트리를 구성하는 블록, 빈, 셀 등은 고유한 시그니처를 가짐
  - 비할당영역으로부터 시그니처를 카빙 후 레지스트리 구조 재구성

레지스트리 구조	시그니처
Hive	regf
Hive Bin	hbin
Key Node	nk
Key Link	lk
Key Value	vk
Key Security	sk
Folder List	lf
Hash List	lh
Index List	li
Index recursive	ri

레지스트리 하이브 내의 비할당 영역 카빙

- **레지스트리 시그니처 카빙**
  - 레지스트리를 구성하는 셀 (key, key-list, value, value-list, data 등) 은 고유한 시그니처를 가짐
  - 하이브 파일 내의 비할당 영역에 대해서 레지스트리 시그니처 카빙
  - 정상적으로 존재하는 데이터와의 연결 관계를 분석하여, 삭제된 항목 연결
  - **REGA** (http://forensic.korea.ac.kr)



레지스트리 분석

Security is a people problem…

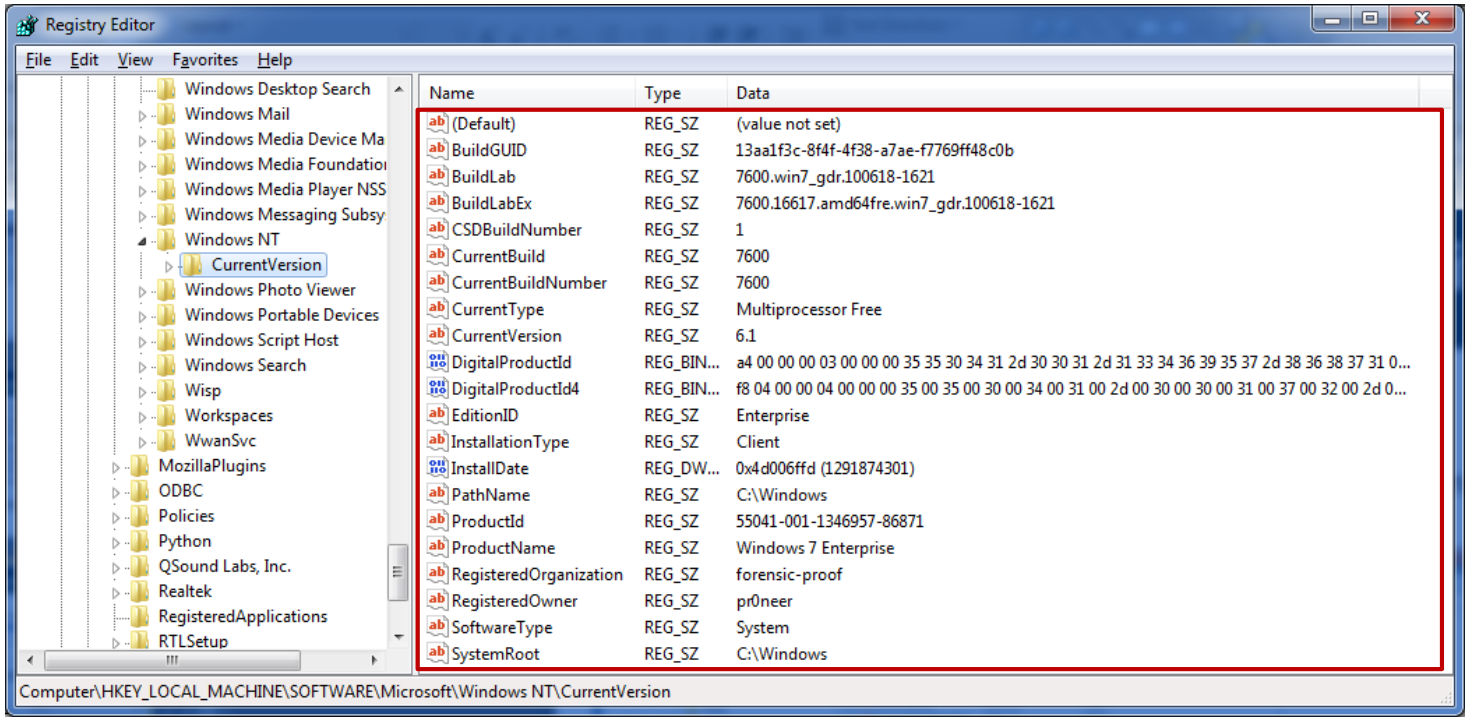
레지스트리 디지털 포렌식 분석

- **레지스트리 분석의 디지털 포렌식적 의미**
  - 윈도우 설치 정보와 계정 정보 등 확인 가능
  - 윈도우 부팅 시 자동 실행되는 응용프로그램 목록 확인 가능 ➔ 악성 코드 분석
  - 최근 사용한 파일, 실행 프로그램 등의 사용자 활동 내역 확인 가능
  - 응용프로그램 설치 정보와 사용 내역 등 확인 가능
  - 시스템에 사용한 하드웨어 정보 확인 가능
  - 추가적인 포렌식 분석 대상 선별 가능

➔ 윈도우 포렌식 분석의 필수 요소

시스템 정보 (1/5)

- **기본 시스템 정보**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion**



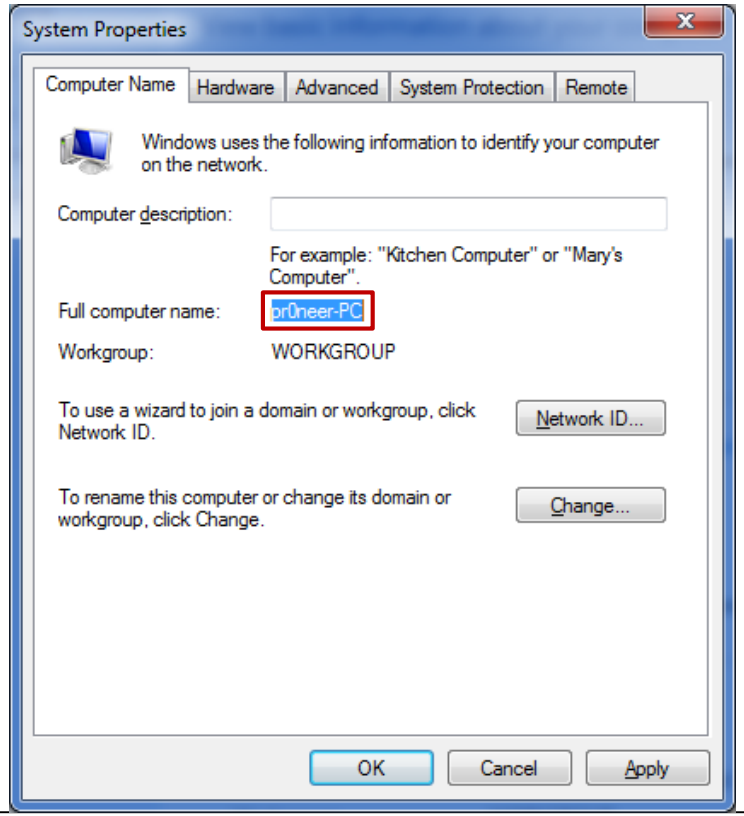
  - 활성정보 수집 시 **systeminfo** 명령을 사용
    - **C:₩>** systeminfo

시스템 정보 (2/5)

- **기본 시스템 정보**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion**
    - **ProductName** – 운영체제 이름
    - **Owner** – 사용자 이름
    - **Organization** – 조직 이름
    - **ProductId** – 운영체제 식별자
    - **BuildLab(Ex)** – 운영체제 세부 버전
    - **InstallDate** – 운영체제 설치 날짜 (유닉스 시간 형식)
    - **SystemRoot** – 운영체제 설치 루트 폴더

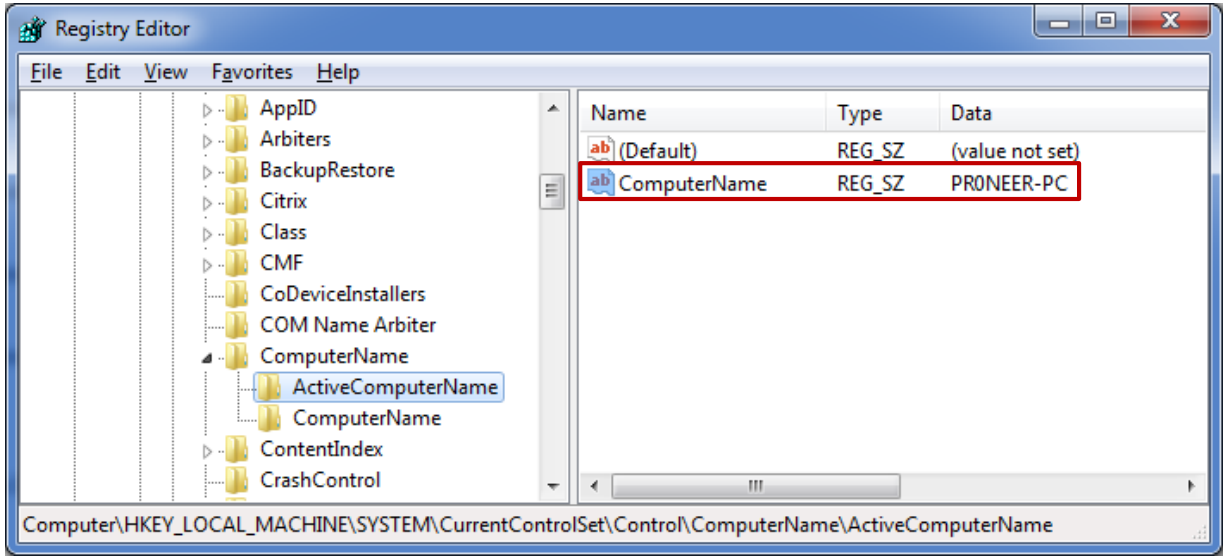
시스템 정보 (3/5)

- **컴퓨터 이름**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩ComputerName₩ActiveComputerName**
  - **ComputerName** – 시스템 등록 정보에 등록된 컴퓨터 이름



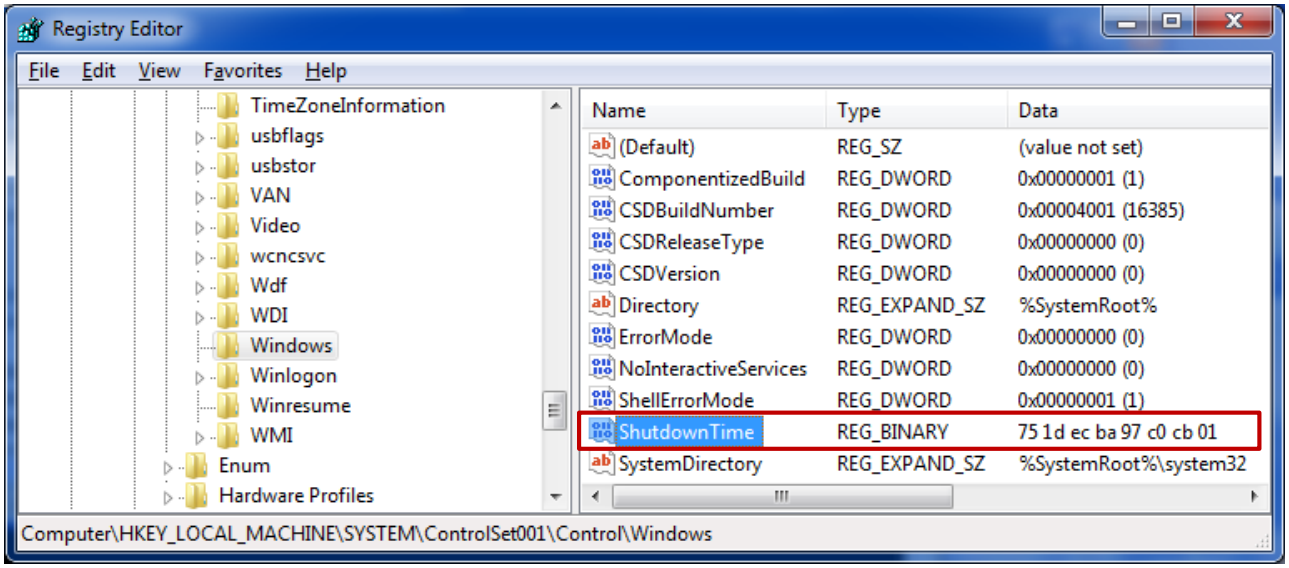
시스템 정보 (4/5)

- **컴퓨터 이름**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩ComputerName₩ActiveComputerName**
  - **ComputerName** – 시스템 등록 정보에 등록된 컴퓨터 이름



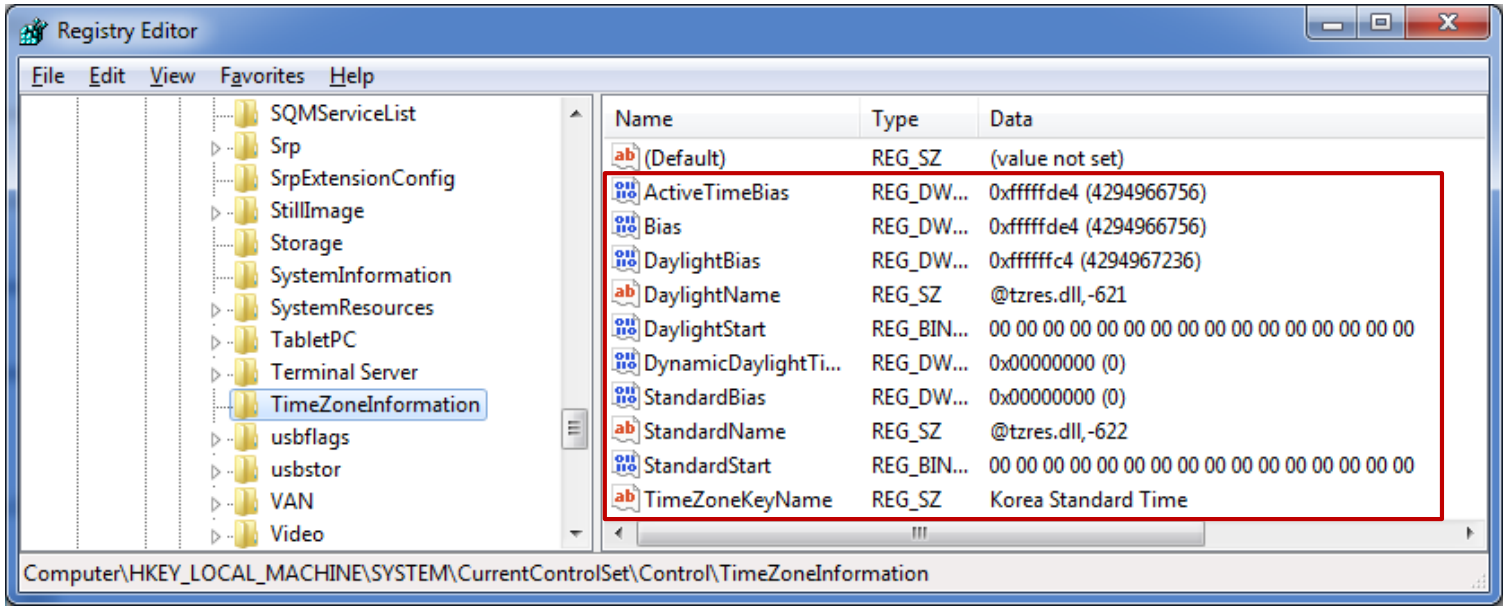
시스템 정보 (5/5)

- **시스템 마지막 종료 시각**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩Windows**
  - **ShutdownTime** – 마지막 종료 시각 저장
    - http://www.digital-detective.co.uk/freetools/decode.asp



표준 시간대와 날짜 변경 흔적

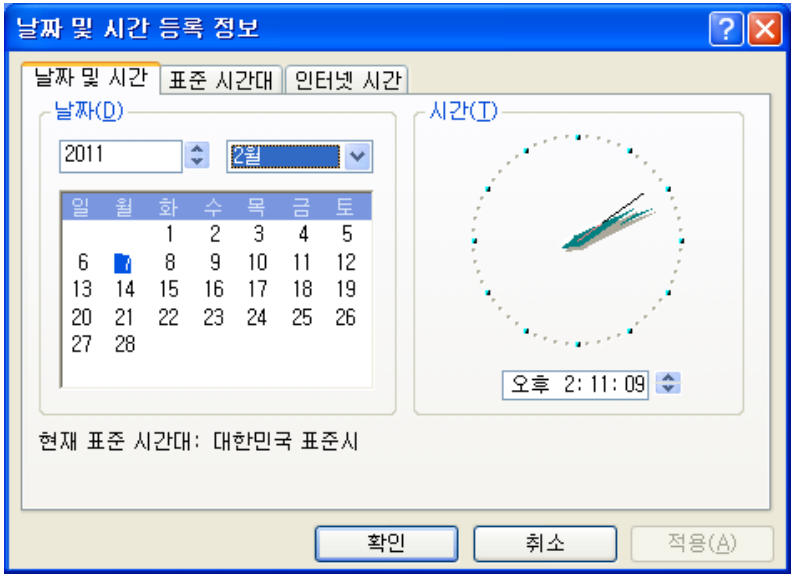
- **표준 시간대**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩TimeZoneInformation**



  - UTC/GMT 표준 시간대
  - 썸머 타임 관련 정보

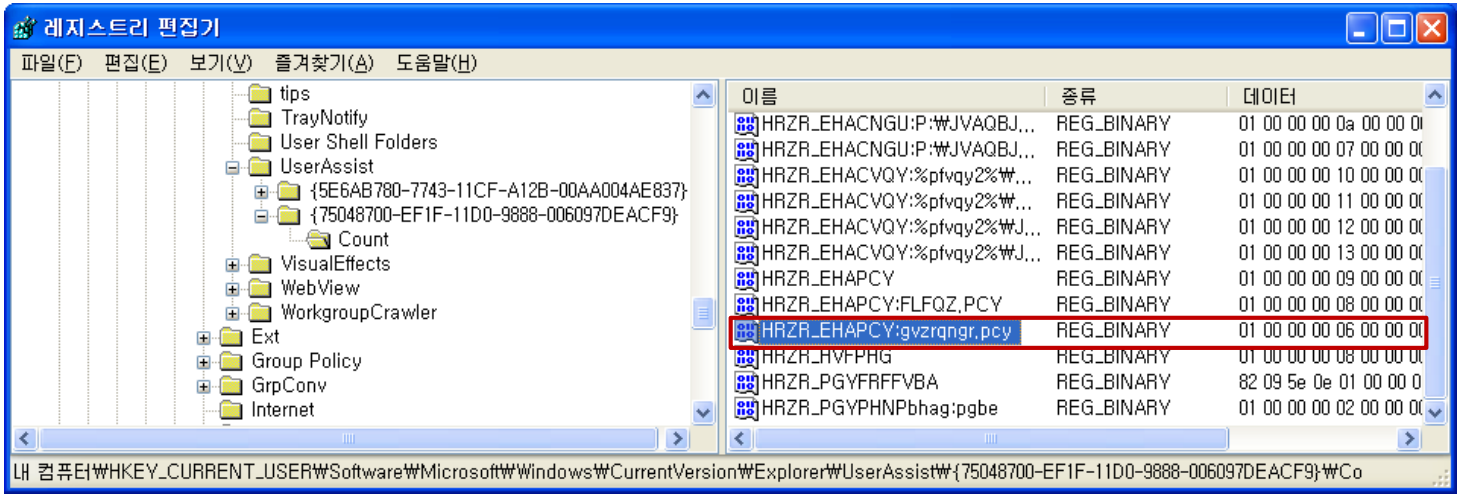
표준 시간대와 날짜 변경 흔적

- **날짜 변경 흔적 (2000/XP/Vista)**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{75048700-EF1F-11D0-9888-006097DEACF9}₩Count**
    - 날짜 및 시간 등록 정보 대화상자가 활성화된 횟수



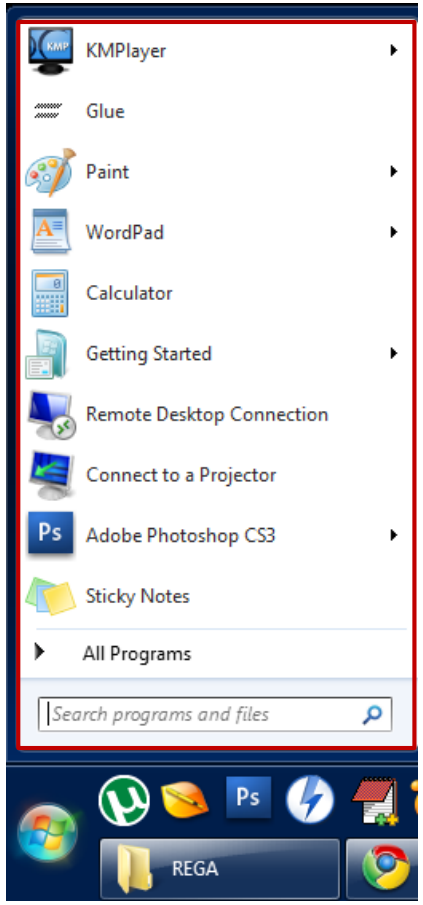
표준 시간대와 날짜 변경 흔적

- **날짜 변경 흔적 (2000/XP/Vista)**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{75048700-EF1F-11D0-9888-006097DEACF9}₩Count**
    - HRZR_EHAPCY:gvzrqngr.pcy ➔ ROT-13: **UEME_RUNCPL:timedata.cpl**
    - **4 – 7** : 작업 표시줄을 통해 대화상자를 연 횟수 (초기값 5)
    - **8 – 15** : 대화상자가 마지막으로 열린 시각 (변경된 시각을 의미하지는 않음)



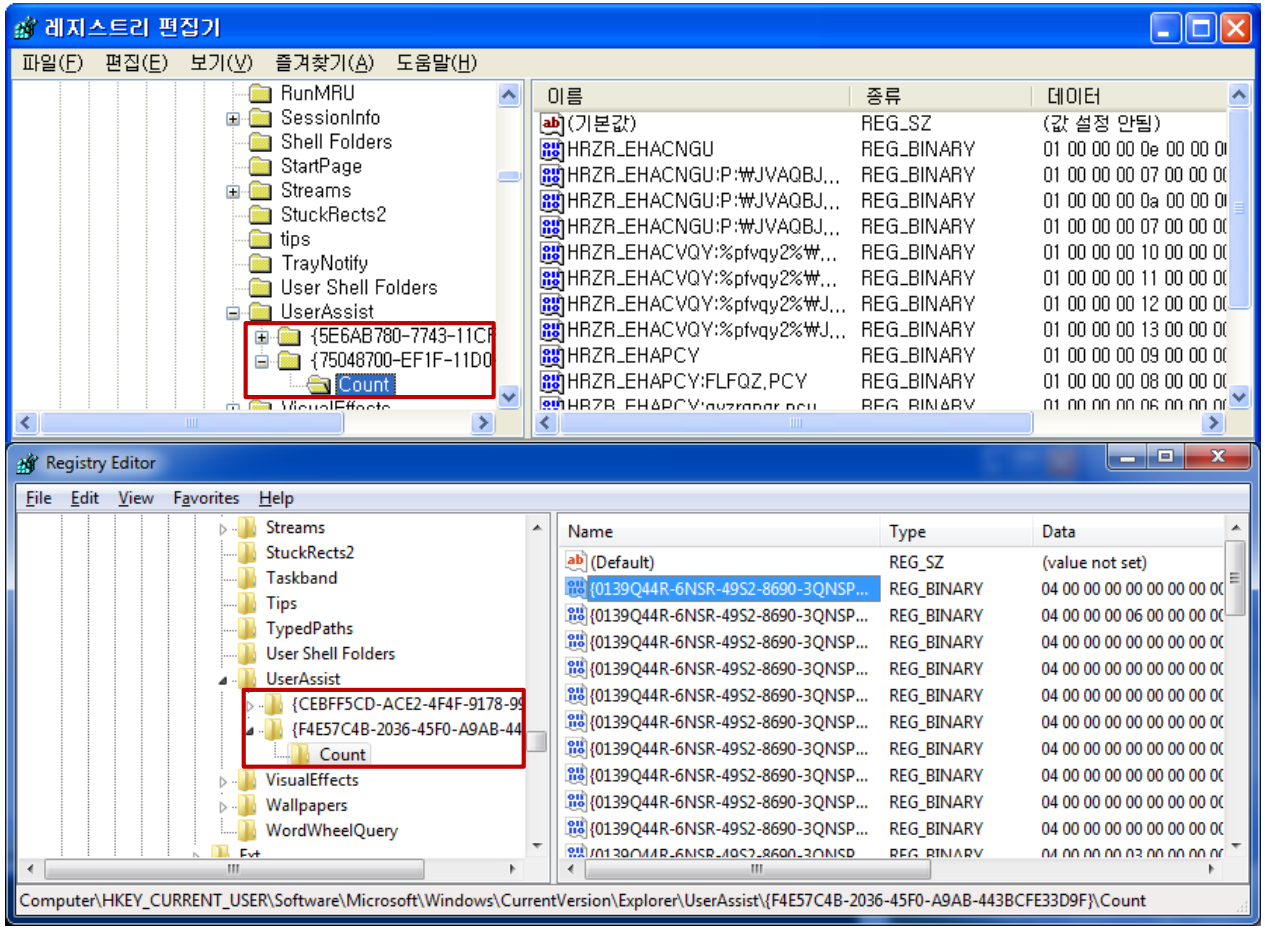
응용프로그램 정보 (1/12)

- **응용프로그램 사용 로그**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist**
  - **2000/XP/Vista**
    - {5E6AB780-7743-11CF-A12B-00AA004AE837}₩Count
    - {75048700-EF1F-11D0-9888-006097DEACF9}₩Count
  - **7**
    - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}₩Count
    - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}₩Count



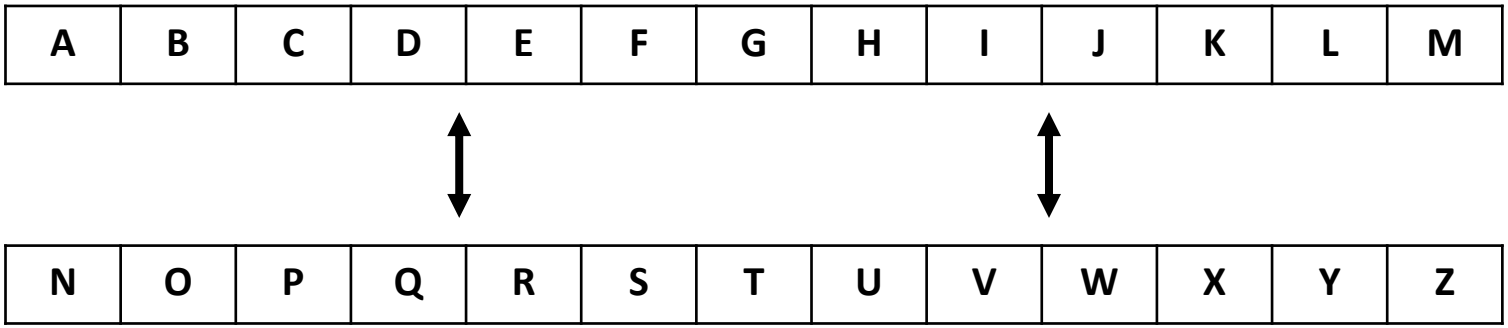
응용프로그램 정보 (2/12)

- **응용프로그램 사용 로그 (ROT-13 인코딩 – http://web.forret.com/tools/rot13.asp)**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{GUID}₩Count**



응용프로그램 정보 (3/12)

- 응용프로그램 사용 로그
  - ROT-13 인코딩



  - DFRC ➔ QSEP

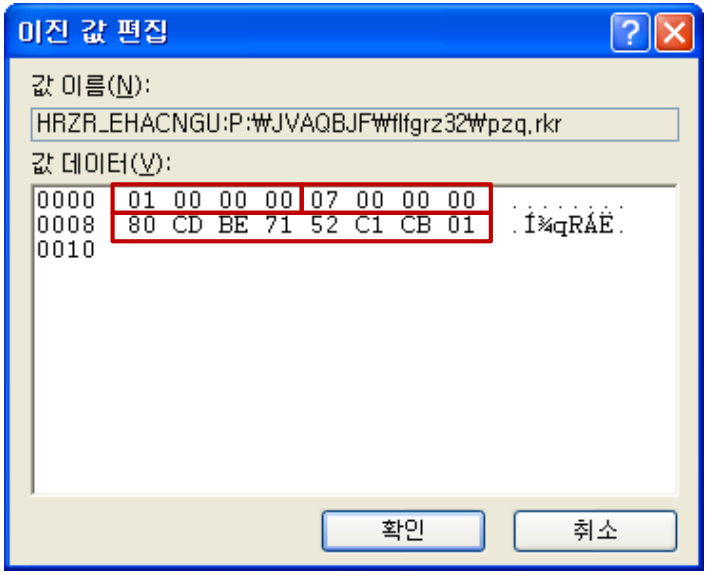
응용프로그램 정보 (4/12)

- **응용프로그램 사용 로그**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{GUID}₩Count**
  - 응용프로그램 종류, 최종 실행 시각, 실행 횟수, 세션 아이디 확인 가능

계정명	이름	종류	최종실행시각 (UTC+09:00)	실행횟수	세션아이디
pr0neer	{6D809377-6AF0-444B-8957-A3773F02200E}₩Microsoft Office₩Office14₩POWERPNT.EXE	CTLSESSION	2011-01-31 14:55:24 Mon	36	0
pr0neer	{F38BF404-1D43-42F2-9305-67DE0B28FC23}₩regedit.exe	CTLSESSION	2011-01-31 15:13:44 Mon	3	0
pr0neer	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}₩spool₩drivers₩x64₩3₩HNCE2PPRCONV8...	CTLSESSION	설정안됨	0	0
pr0neer	₩Autoplay.exe	CTLSESSION	설정안됨	0	0
pr0neer	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩Adobe₩Acrobat 8.0₩Acrobat₩Acrobat.exe	CTLSESSION	2011-01-31 14:58:34 Mon	26	0
pr0neer	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩Adobe₩Adobe Photoshop CS3₩Photosho...	CTLSESSION	2011-01-07 21:33:32 Fri	0	0
pr0neer	₩Users₩pr0neer₩AppData₩Local₩Temp₩WZSE0.TMP₩XEISetup2.exe	CTLSESSION	설정안됨	0	0
pr0neer	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩Hnc₩Hwp80₩Hwp.exe	CTLSESSION	2011-01-23 19:01:07 Sun	0	0
pr0neer	{6D809377-6AF0-444B-8957-A3773F02200E}₩Microsoft Office₩Office14₩WINWORD.EXE	CTLSESSION	2011-01-29 22:03:42 Sat	3	0
pr0neer	₩Users₩pr0neer₩AppData₩Local₩SK Communications₩NATEON₩Addin₩AAEB33C8-3...	CTLSESSION	설정안됨	0	0
pr0neer	₩Users₩pr0neer₩AppData₩Local₩SK Communications₩NATEON₩Addin₩AAEB33C8-3...	CTLSESSION	설정안됨	0	0
pr0neer	₩Users₩pr0neer₩AppData₩Local₩SK Communications₩NATEON₩Addin₩AAEB33C8-3...	CTLSESSION	설정안됨	0	0
pr0neer	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩Common Files₩Adobe₩Updater5₩Adobe...	CTLSESSION	설정안됨	0	0
pr0neer	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}₩Common Files₩Adobe₩Updater5₩Adobe...	CTLSESSION	설정안됨	0	0
pr0neer	{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}₩taskmgr.exe	CTLSESSION	설정안됨	0	0
pr0neer	₩Users₩pr0neer₩Desktop₩iTunesSetup.exe	CTLSESSION	2010-12-11 20:31:50 Sat	0	0
pr0neer	₩[0x01] PRONEER₩#3 Lecture₩È£¼-Àü¹®´ëÇÐ₩[2010-2] WEB HACKING₩Tools₩Web...	CTLSESSION	2010-12-11 21:50:07 Sat	0	0

응용프로그램 정보 (5/12)

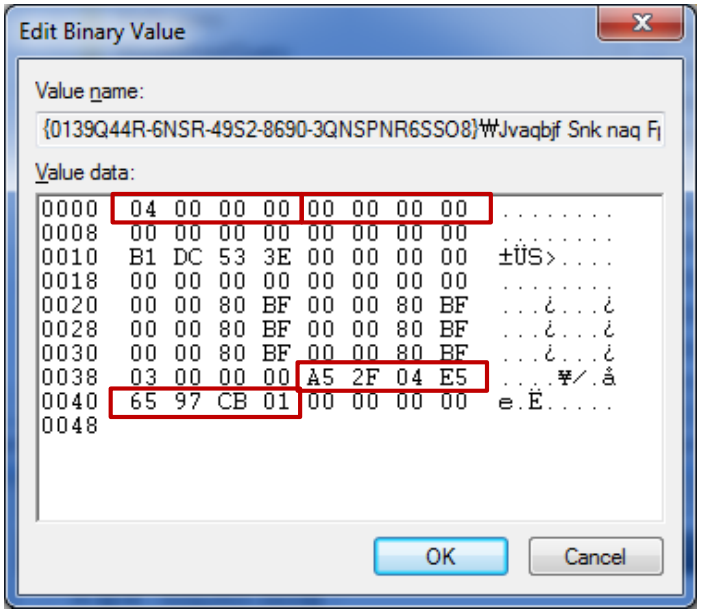
- **응용프로그램 사용 로그**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{GUID}₩Count**
  - **2000/XP/Vista 로그 포맷**
    - **0 – 3** : 세션 번호
    - **4 – 7** : 응용프로그램 실행 횟수 (초기값 5)
    - **8 – 15** : 응용프로그램 마지막 실행 시간



응용프로그램 정보 (6/12)

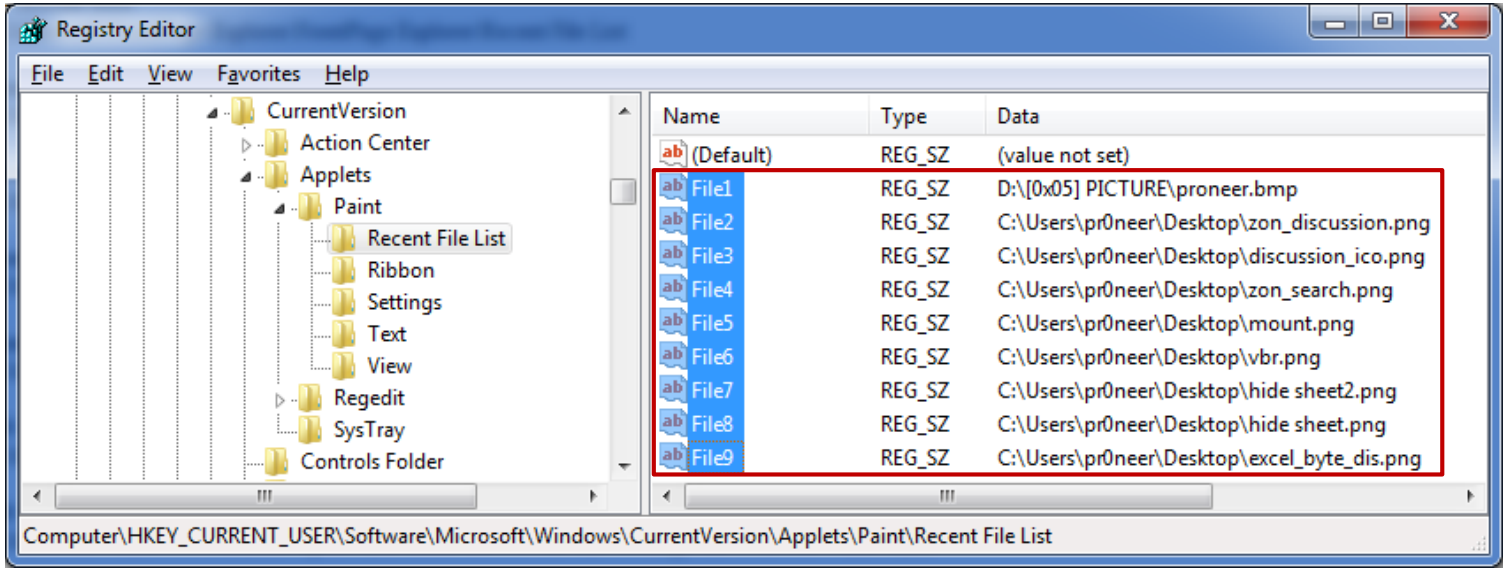
- **응용프로그램 사용 로그**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{GUID}₩Count**
  - **7 로그 포맷**
    - **0 – 3** : 세션 번호
    - **4 – 7** : 응용프로그램 실행 횟수

      (초가값은 응용프로그램에 따라 다름)
    - **60 – 67** : 응용프로그램 마지막 실행 시간



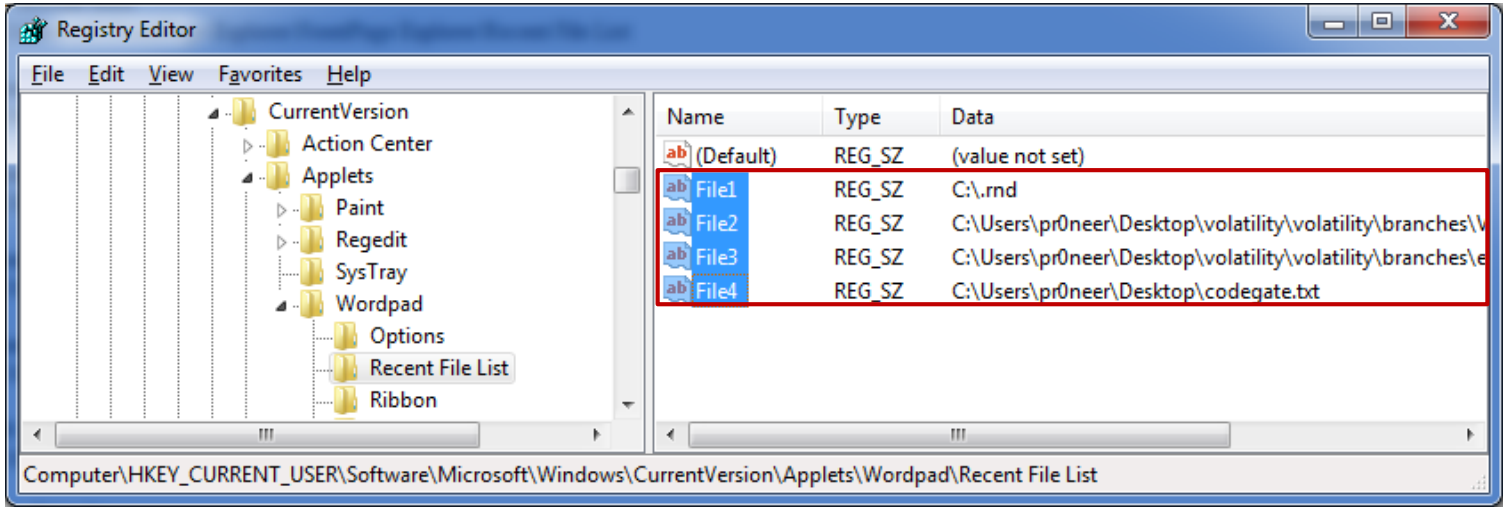
응용프로그램 정보 (7/12)

- **그림판에서 열어본 파일 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Applets₩Paint₩Recent File List**
  - **File#** – 숫자가 낮을 수록 최근에 열어본 파일 (그림판을 종료하는 시점에 값 저장)



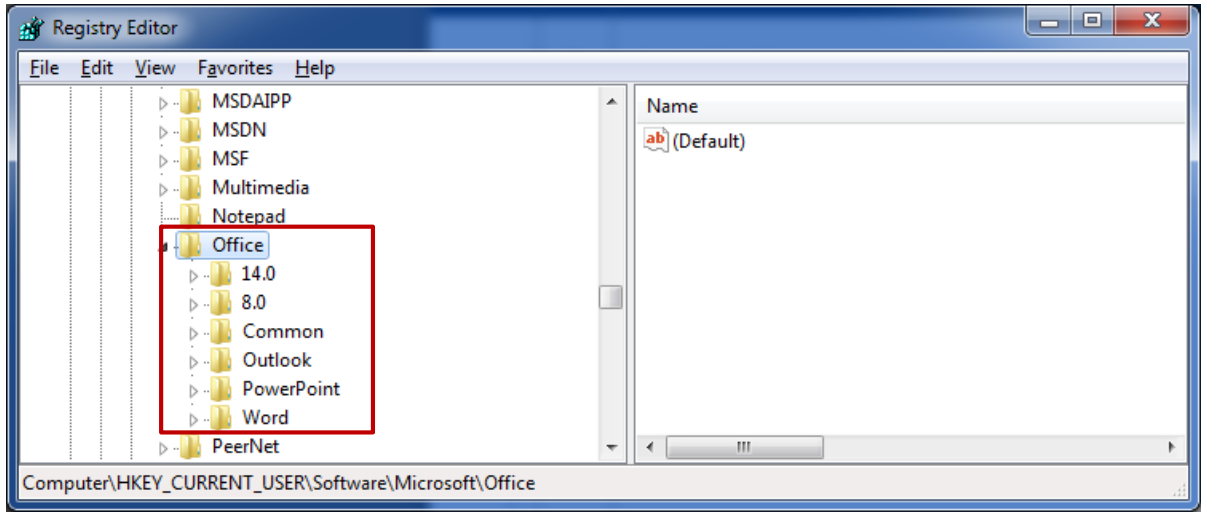
응용프로그램 정보 (8/12)

- **워드패드에서 열어본 파일 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Applets₩wordpad₩Recent File List**
  - **File#** – 숫자가 낮을 수록 최근에 열어본 파일 (워드패드를 종료하는 시점에 값 저장)



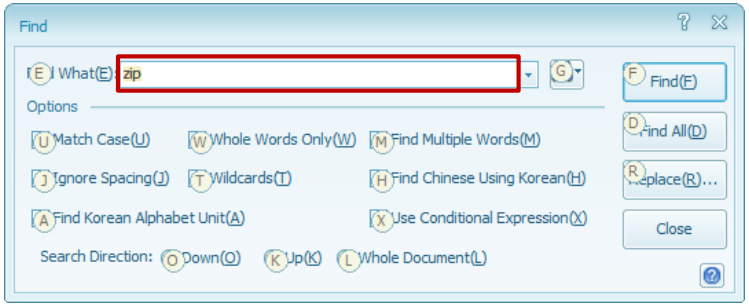
응용프로그램 정보 (9/12)

- **MS OFFICE 사용 흔적** (http://accessdata.com/downloads/media/Microsoft_Office_2007-2010_Registry_ArtifactsFINAL.pdf)
  - **최근 열린 폴더 – HKU₩{USER}₩SOFTWARE₩Microsoft₩Office₩{VERSION}₩{APP}₩Place MRU**
  - **최근 사용한 파일 – HKU₩{USER}₩SOFTWARE₩Microsoft₩Office₩{VERSION}₩{APP}₩File MRU(Recent Files)**
  - 각 응용프로그램 및 버전 별로 다양한 흔적 저장
  - 최근 열린 폴더, 최근 사용한 파일, 최근 사용한 페이지, 최근 접근한 URL 등등



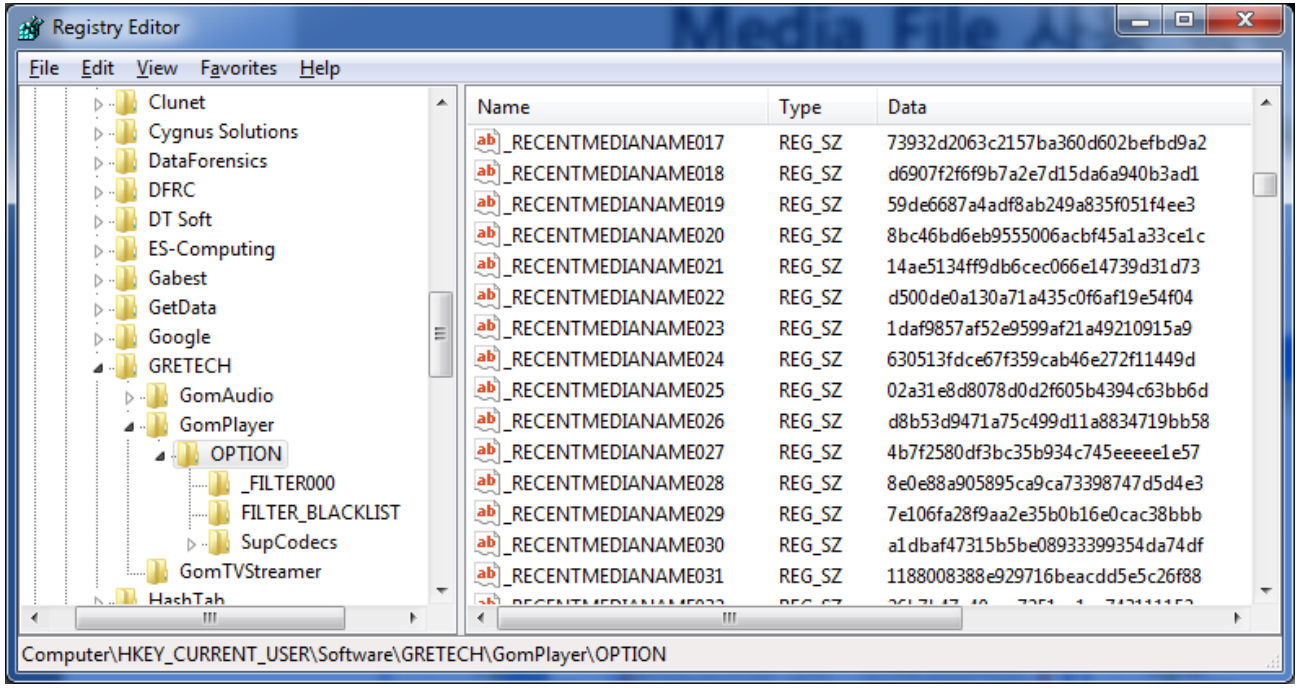
응용프로그램 정보 (10/12)

- 한글 사용 흔적
  - 최근 사용한 파일
    - 한글 2005 – HKU₩{USER}₩SOFTWARE₩HNC₩Hwp₩6.5₩RecentFile
    - 한글 2007 – HKU₩{USER}₩SOFTWARE₩HNC₩Hwp₩7.0₩HwpFrame₩RecentFile
    - 한글 2010 – HKU₩{USER}₩SOFTWARE₩HNC₩Hwp₩8.0₩HwpFrame₩RecentFile
  - 찾기/바꾸기 목록
    - HKU₩{USER}₩SOFTWARE₩HNC₩Hwp₩FindReplace₩Find



응용프로그램 정보 (11/12)

- **곰플레이어 사용 흔적**
  - **HKU₩{USER}₩SOFTWARE₩GRETECH₩GomPlayer₩OPTION**
  - 최근 열린 폴더, 최근 사용한 파일 목록, 다양한 설정 정보 저장

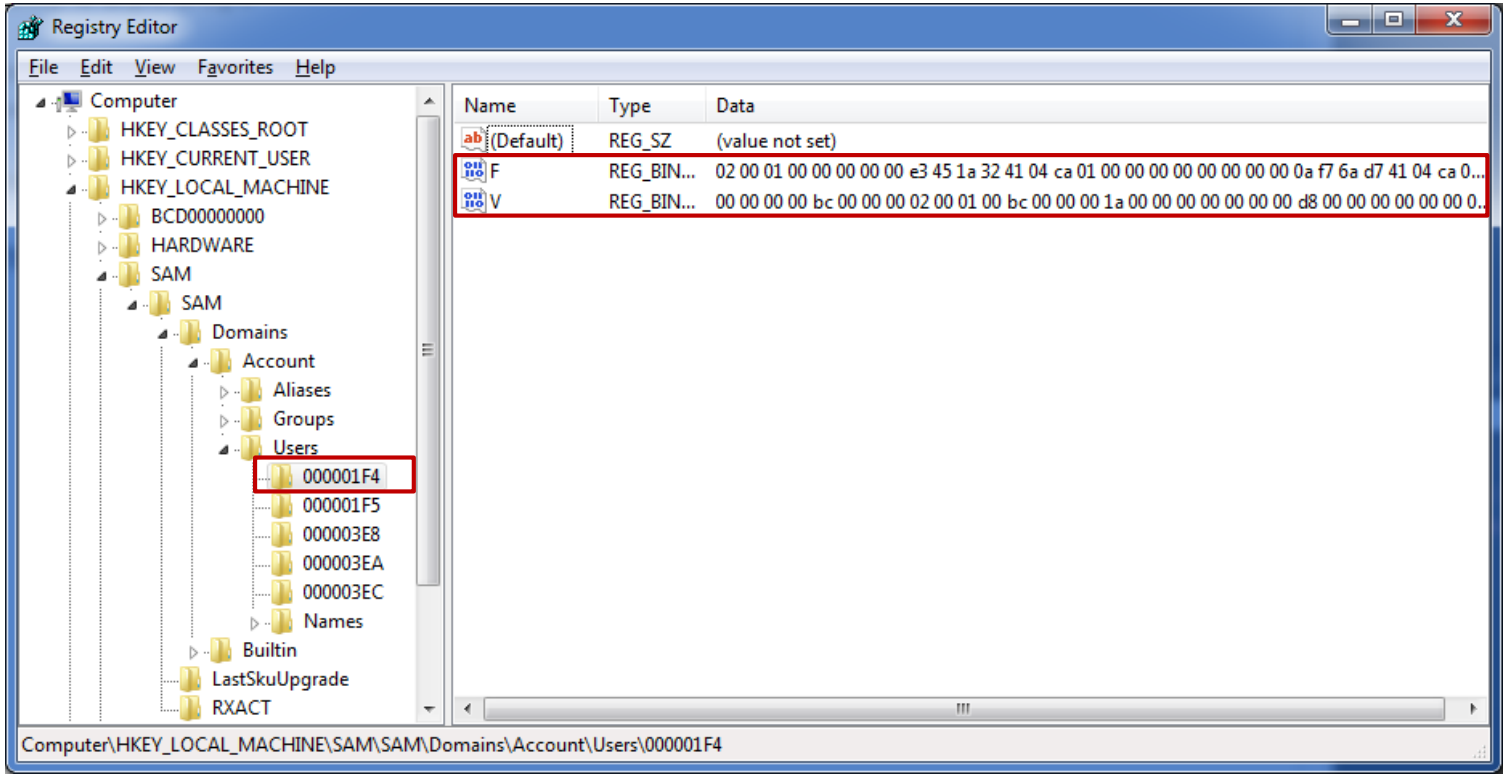


응용프로그램 정보 (12/12)

- **다양한 응용프로그램 사용 흔적**
  - **WinRAR Archive History**
    - HKU₩{USER}₩SOFTWARE₩WinRAR₩ArcHistory
    - HKU₩{USER}₩SOFTWARE₩WinRAR₩DialogEditHistory₩ArcName
  - **XP MediaPlayer Recent Files**
    - HKU₩{USER}₩SOFTWARE₩Microsoft₩MediaPlayer₩Player₩RecentFileList
  - **XP MediaPlayer Recent URLs**
    - HKU₩{USER}₩SOFTWARE₩Microsoft₩MediaPlayer₩Player₩RecentURLList
  - **Adobe Acrobat | Reader**
    - HKU₩{USER}₩SOFTWARE₩Adobe₩Adobe Acrobat₩{version}₩AVGeneral₩cRecentFiles
    - HKU₩{USER}₩SOFTWARE₩Adobe₩Acrobat Reader₩{version}₩AVGeneral₩cRecentFiles

사용자 계정 정보 (1/7)

- **시스템 사용자 목록**
  - **HKLM₩SAM₩SAM₩Domains₩Account₩Users₩{RID}**
  - 각 사용자의 계정 정보는 Users의 하위키인 **{RID}(R = Relative, ID = ID)** 폴더의 F, V 값에 저장



사용자 계정 정보 (2/7)

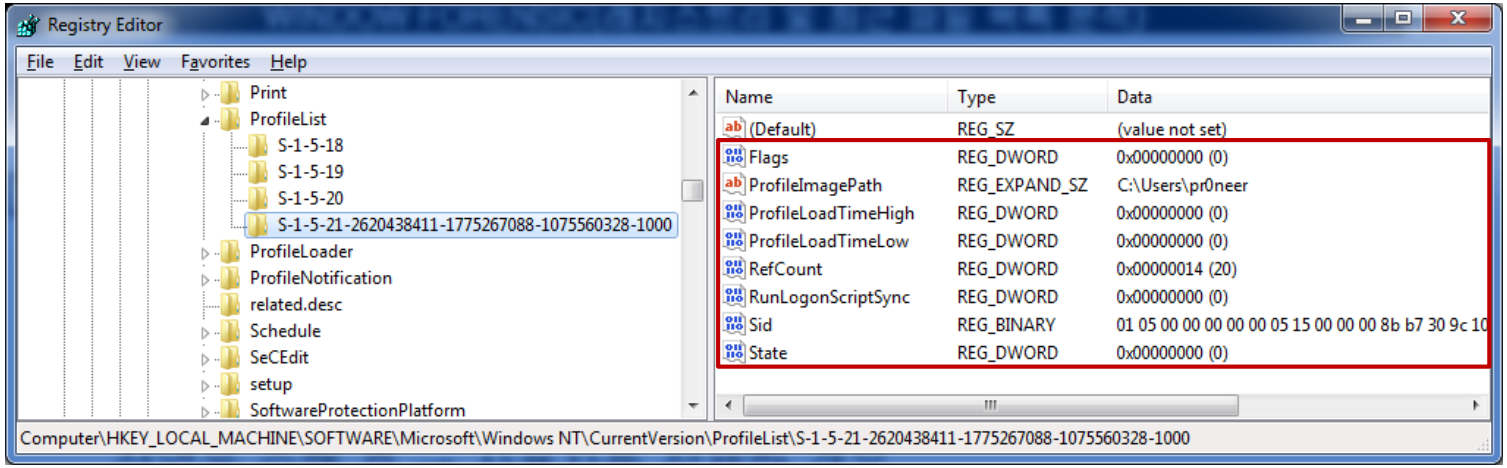
- **시스템 사용자 목록**
  - **HKLM₩SAM₩SAM₩Domains₩Account₩Users₩{RID}**
  - **F 값에 저장되는 계정 정보**
    - 최종 로그인 시각
    - 패스워드 재설정 시각
    - 계정 만료 시각
    - 로그인 실패 시각
    - RID (SID의 마지막 식별부분)
    - 계정 상태 정보 (활성화/비활성, 패스워드 설정/비설정)
    - 국가 코드 (국제 전화에 사용되는 코드)
    - 로그인 실패 횟수
    - 로그인 성공 횟수

사용자 계정 정보 (3/7)

- **시스템 사용자 목록**
  - **HKLM₩SAM₩SAM₩Domains₩Account₩Users₩{RID}**
  - **V 값에 저장되는 계정 정보**
    - 로그인 계정 이름
    - 전체 이름
    - 계정 설명
    - LM 해쉬
    - NT 해쉬

사용자 계정 정보 (4/7)

- **시스템 사용자 프로필 목록**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩ProfileList₩{SID}**
  - 하위키인 사용자 {SID}별로 사용자 프로필 정보 저장



사용자 계정 정보 (5/7)

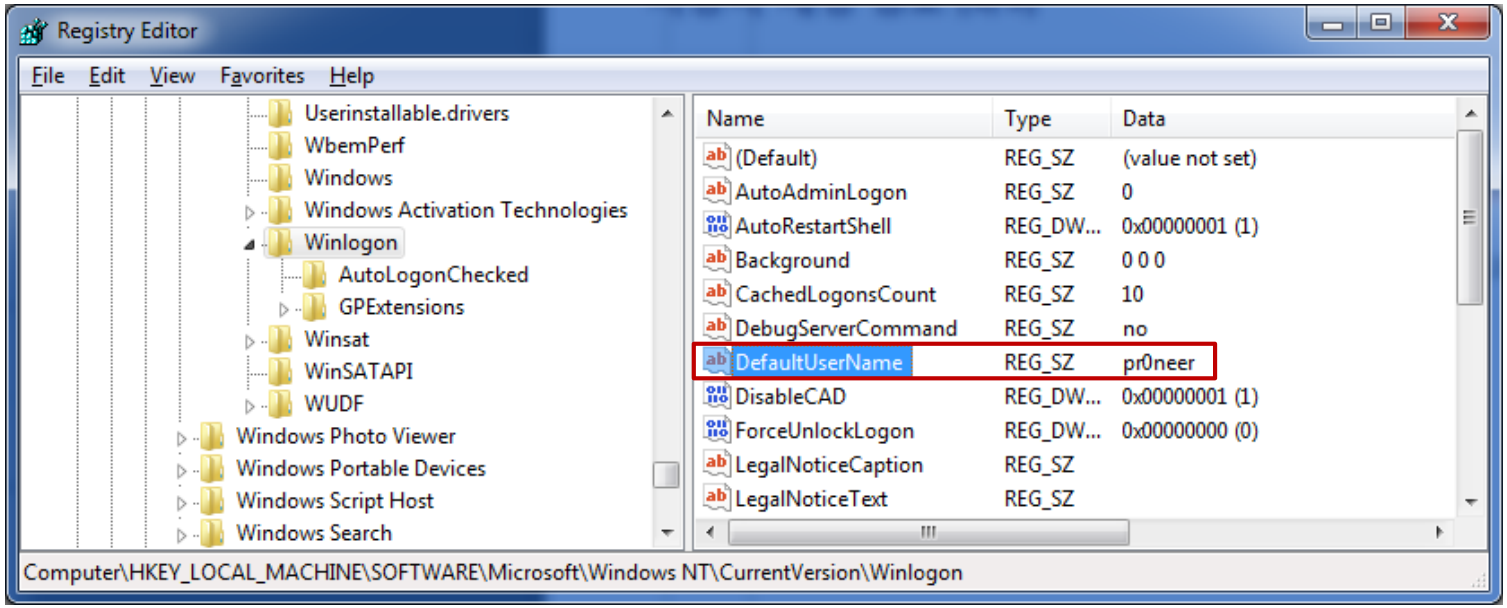
- **시스템 사용자 프로필 목록 – SID(Security Identifier, 보안 식별자)**
  - **S – 1 – 5 – 21 – 2620438411 – 1775267088 – 1075560328 – 1000**

SID 구분	설명
S	SID를 나타내는 식별자
1	SID 세부 버전
5	권한 식별자
21–2620438411–1775267088–1075560328	도메인이나 로컬 컴퓨터 식별자
1000	RID(Relative ID)로 관리자 계정은 500, 사용자 계정은 1000번 이상의 값을 가짐

  - **권한 식별자(Authority Identifier)**
    - 0 – Null Authority
    - 1 – World Authority
    - 2 – Local Authority
    - 3 – Creator Authority
    - 4 – Non-unique Authority
    - 5 – NT Authority
    - 9 – Resource Manager Authority

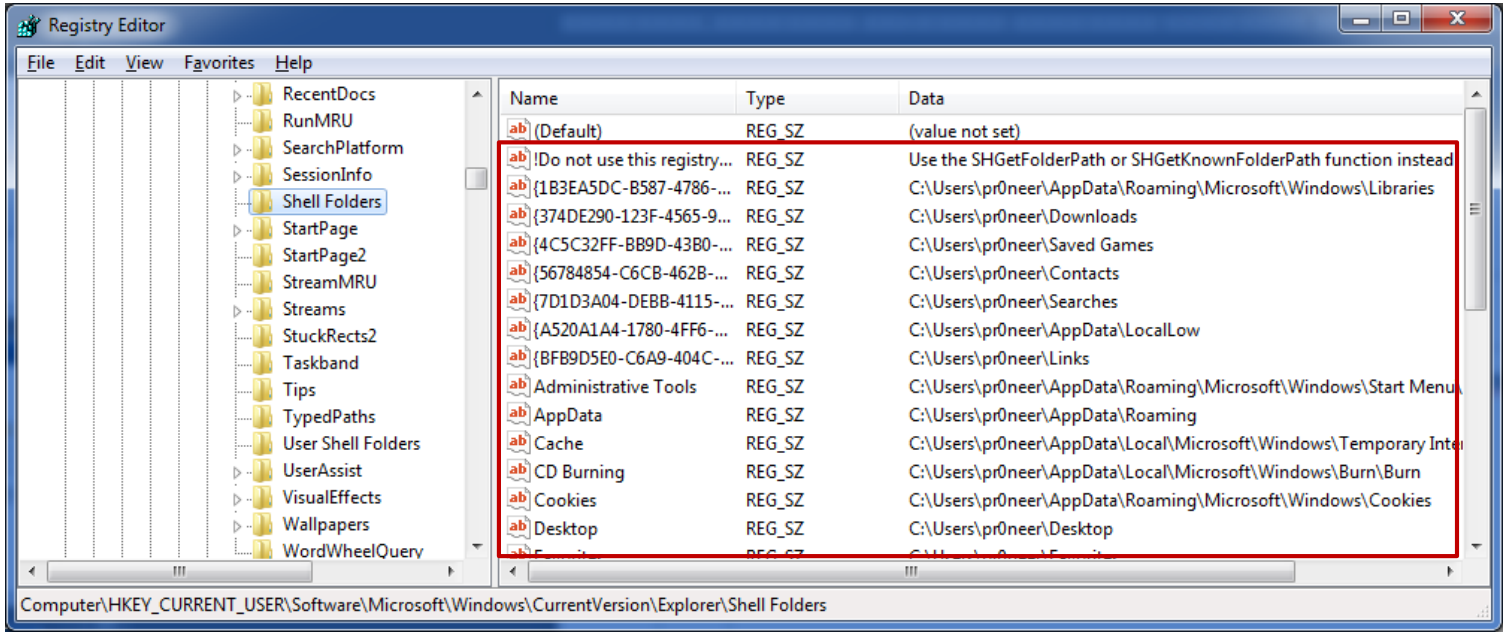
사용자 계정 정보 (6/7)

- **마지막으로 로그인한 사용자**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon**
  - **DefaultUserName** 값이 마지막으로 로그인한 사용자를 나타냄



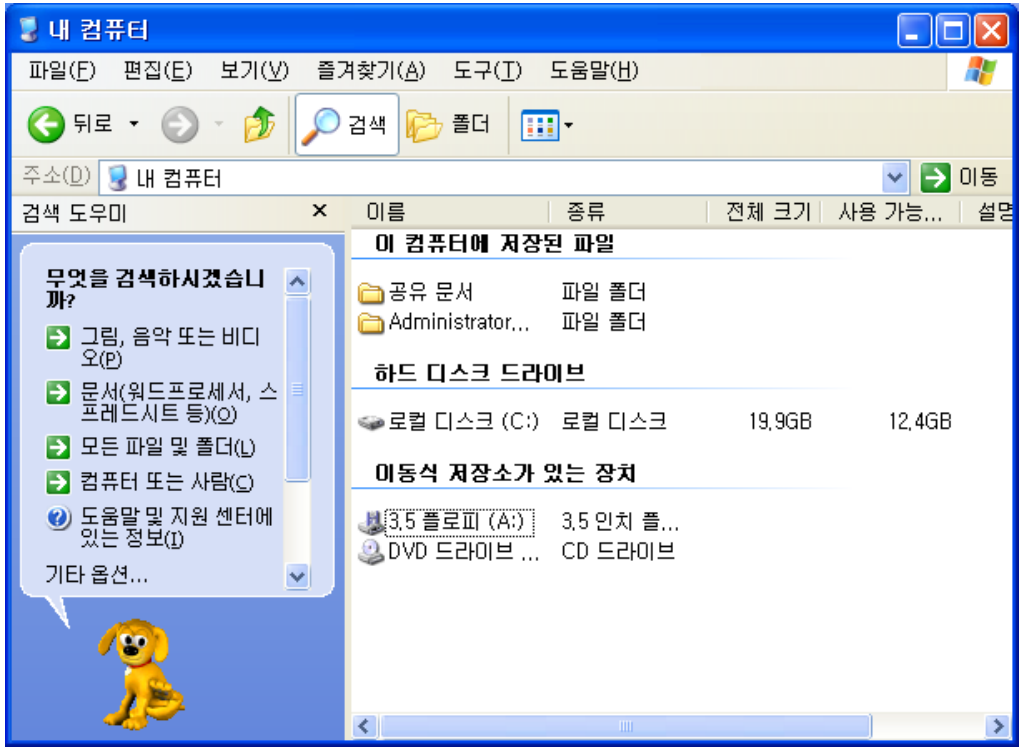
사용자 계정 정보 (7/7)

- **사용자별 기본 경로**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Shell Folders**
  - 각 사용자별 기본 경로 저장



윈도우 검색 정보 (1/5)

- **2000/XP 검색어 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩####**
  - 윈도우 2000/XP 탐색기에서 검색을 사용할 경우 검색어 목록

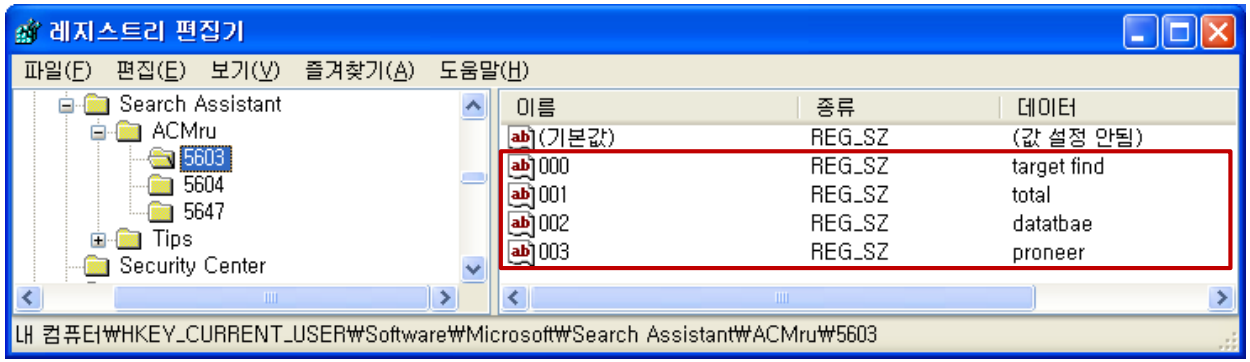


윈도우 검색 정보 (2/5)

- **2000/XP 검색어 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩####**
  - 인터넷 검색
    - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩5001**
  - 모든 파일 및 폴더 검색
    - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩5603**
  - 파일에 들어있는 단어나 문장/그림, 음악 또는 비디오 검색
    - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩5604**
  - 프린터, 컴퓨터 또는 사람/네트워크에 있는 컴퓨터/컴퓨터 찾기 검색
    - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩5647**

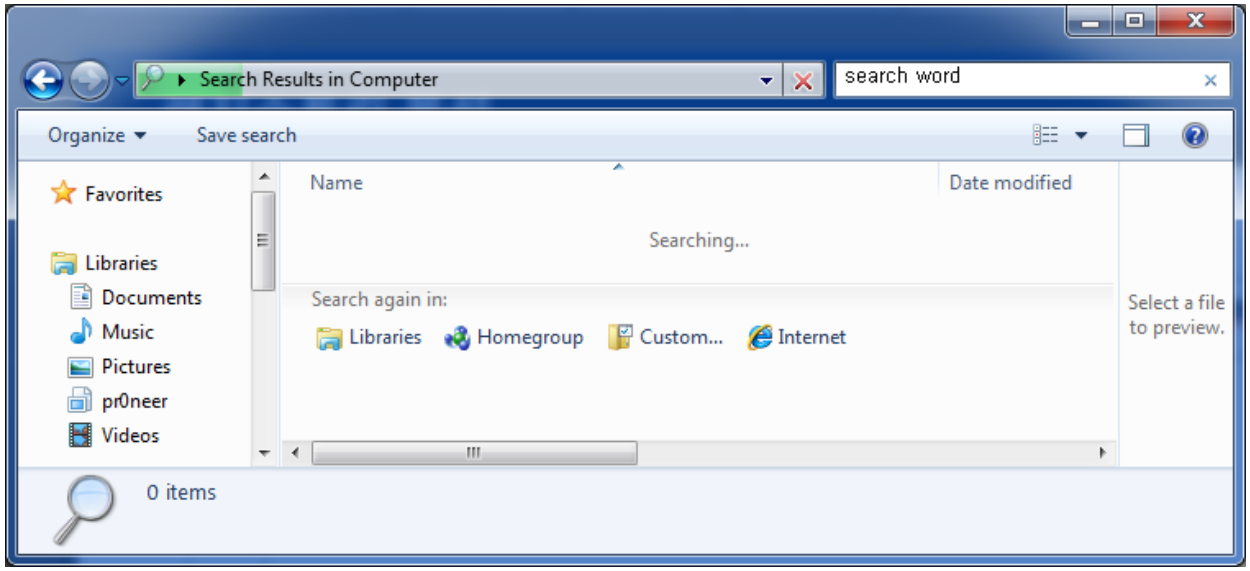
윈도우 검색 정보 (3/5)

- **2000/XP 검색어 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Search Assistant₩ACMru₩5603**
  - 번호가 낮을 수록 최근에 검색한 검색어



윈도우 검색 정보 (4/5)

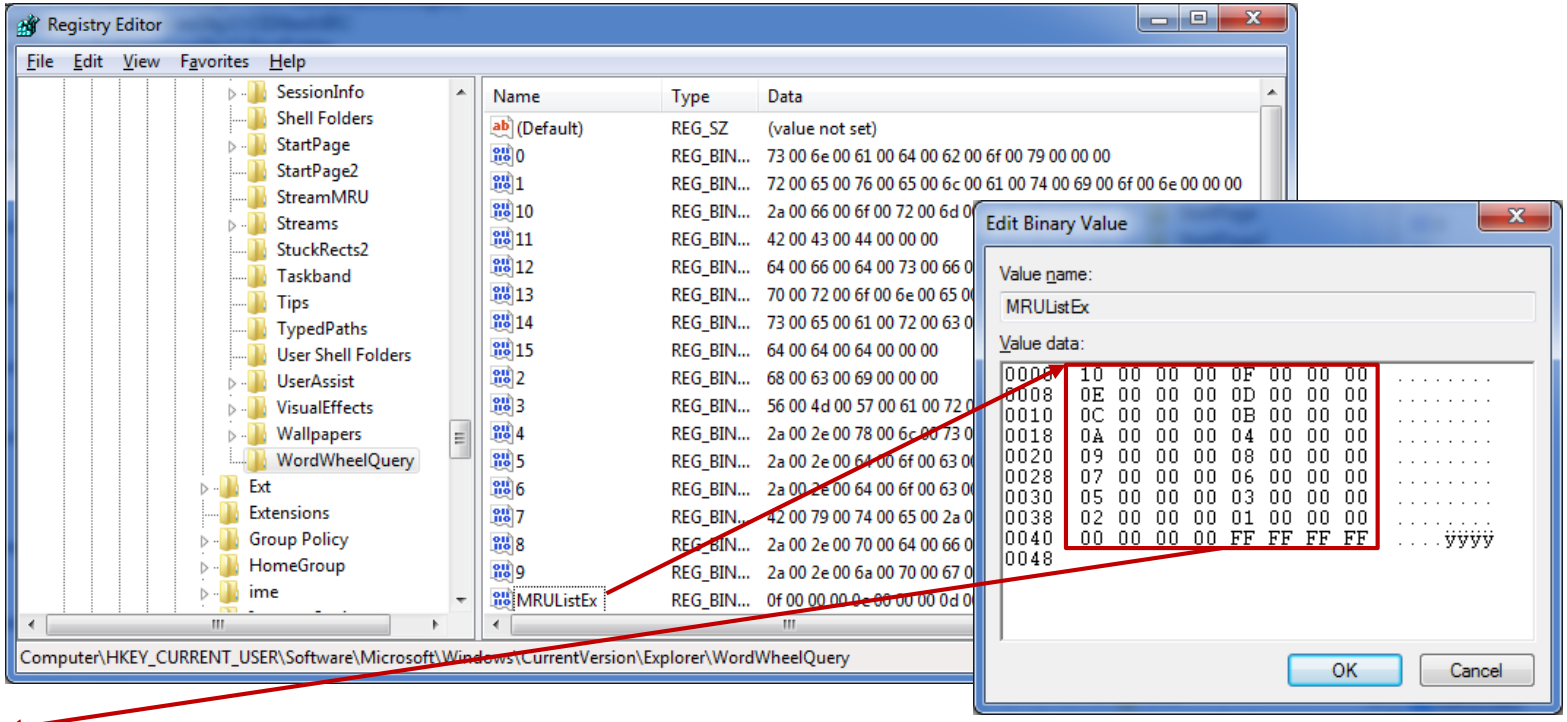
- **7 검색어 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩WordWheelQuery**
  - 윈도우 7 탐색기에서 검색을 사용할 경우 검색어 목록



  - 참고로 Vista의 경우 검색어 목록을 레지스트리에 저장하지 않음

윈도우 검색 정보 (5/5)

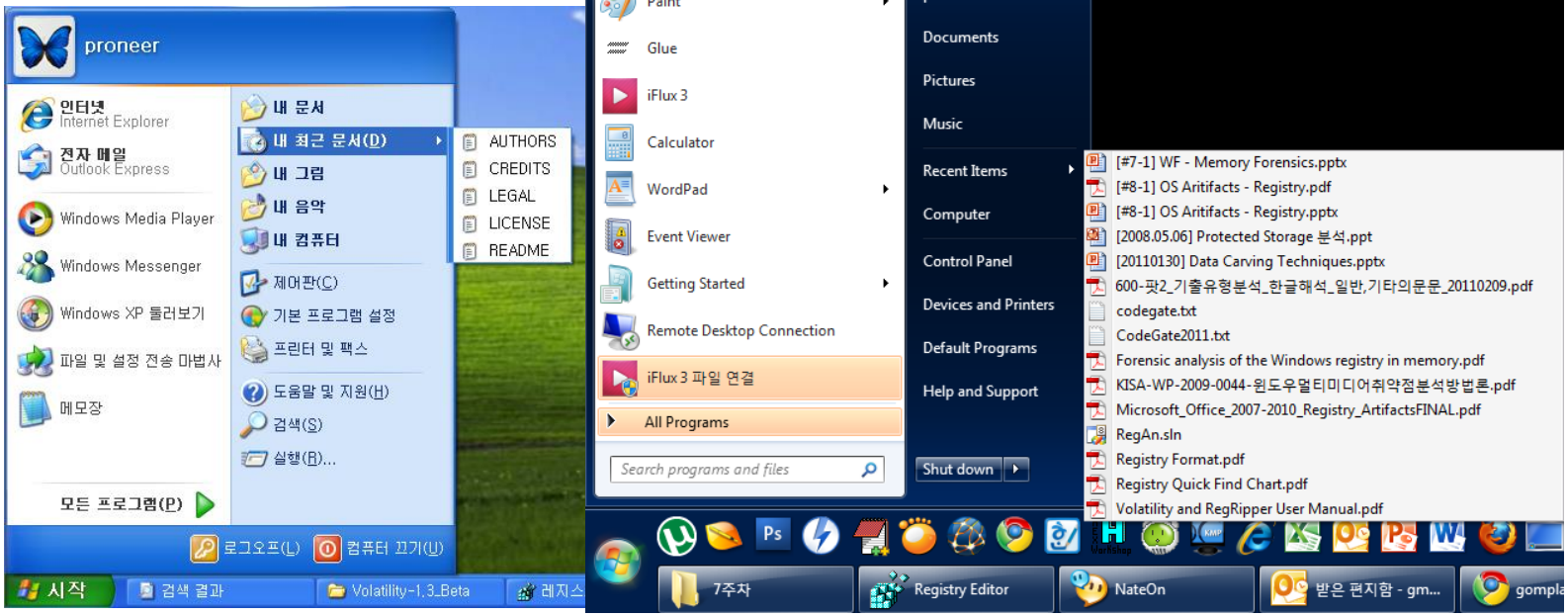
- **7 검색어 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩WordWheelQuery**
  - **MRUListEx** 키값을 통해 검색어 사용 순서 확인



  - 10 → 0F → 0E → 0D → 0C → 0B → 0A → 04 → 09 → 08 → 07 → 06 → 05 → 03 → 02 → 01 → 00

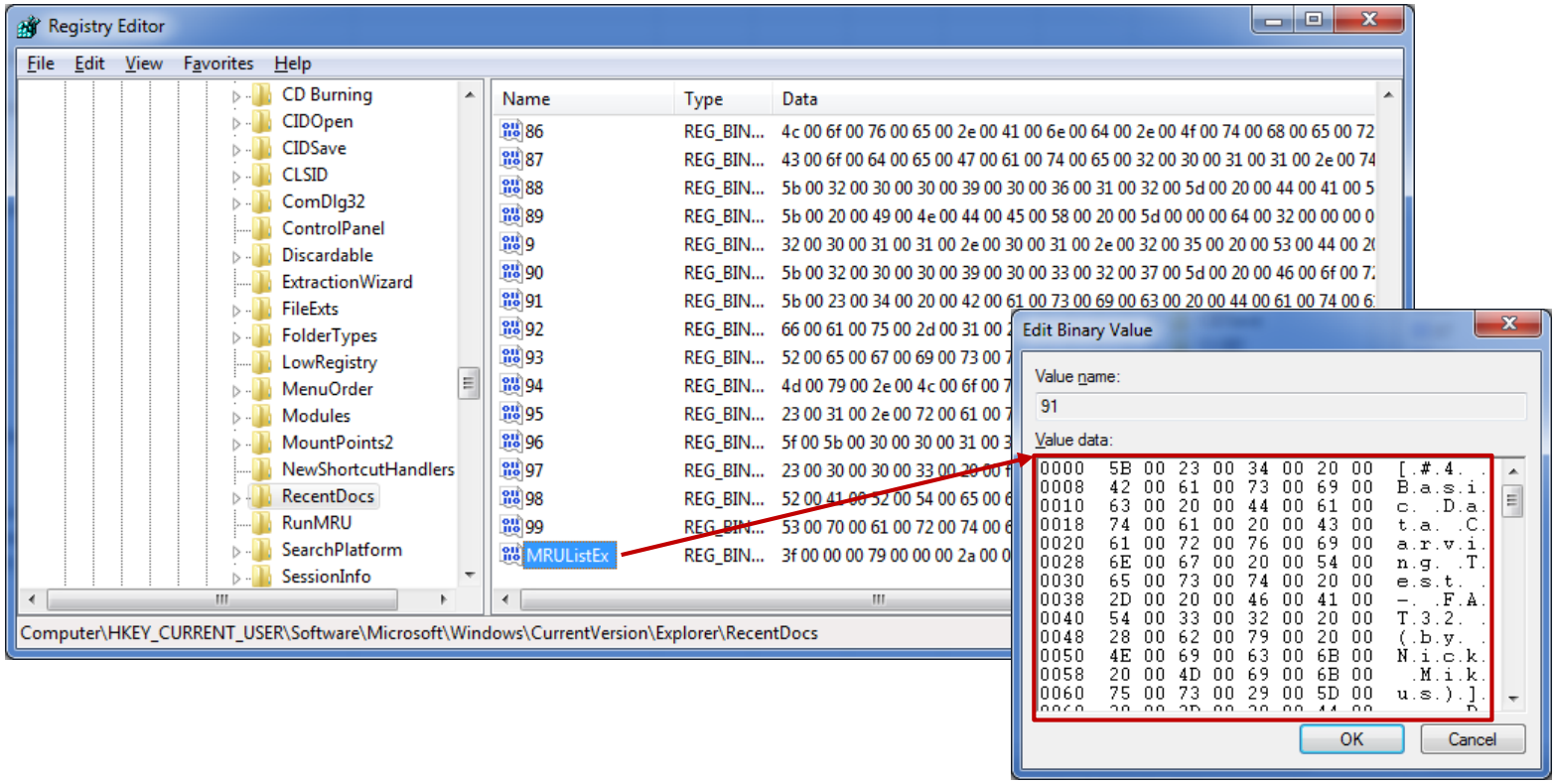
최근 접근 흔적 (1/2)

- **최근에 열어본 파일**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RecentDocs**
  - 최근에 열었던 문서, 그림, 음악, 동영상 등의 파일
  - **2000/XP** – My Recent Documents
  - **Vista/7** – Recent Items



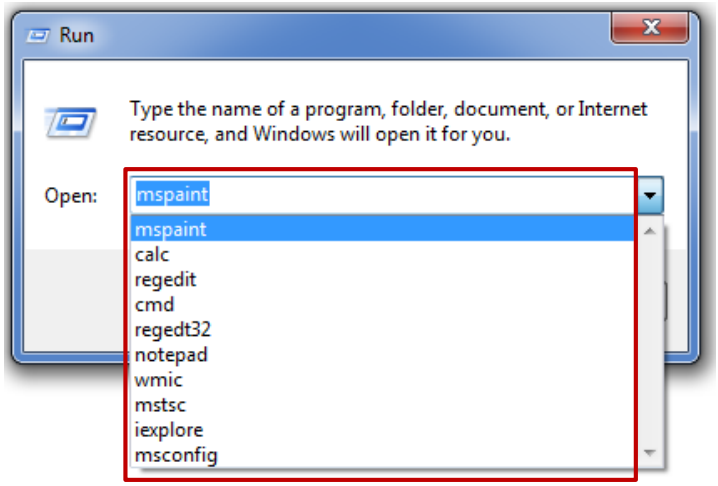
최근 접근 흔적 (2/2)

- **최근에 열어본 파일**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RecentDocs**
  - **MRUListEx** 키값을 통해 열어본 순서 확인



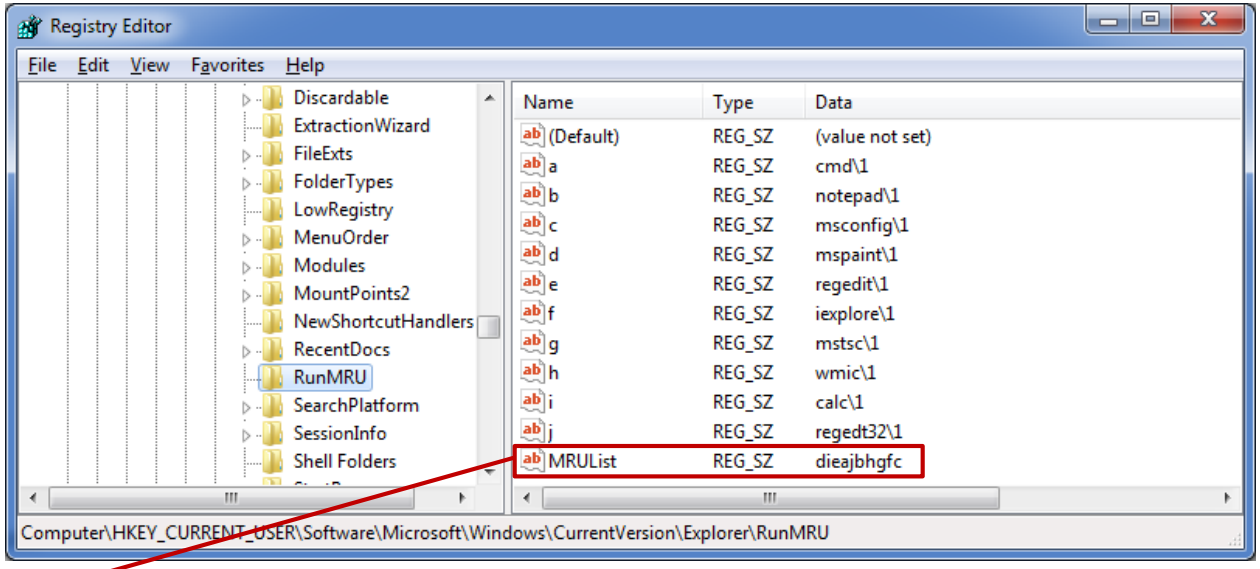
최근 실행 흔적 (1/2)

- **최근에 실행한 명령**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RunMRU**
  - "시작 ➔ 실행" 또는 "Ctrl + R" 를 통해 실행한 명령 목록



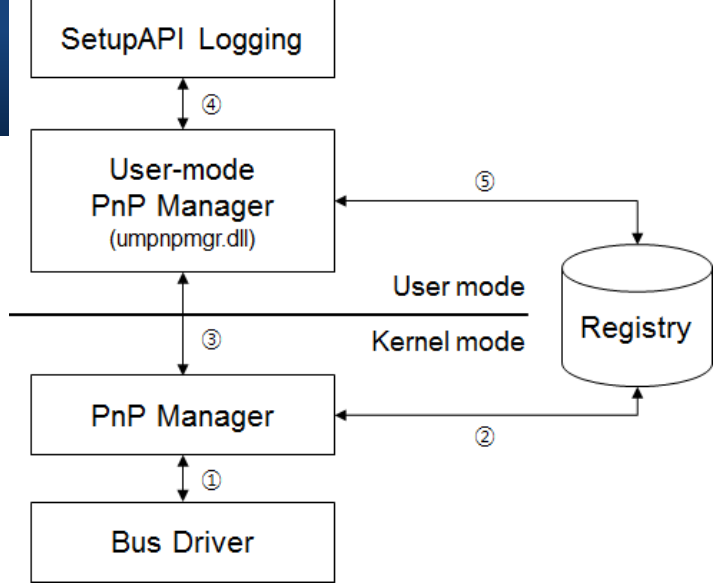
최근 실행 흔적 (2/2)

- **최근에 실행한 명령**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RunMRU**
  - 최근 실행한 명령 순서는 MRUList의 알파벳 순서



  - **dieajbhgfc**
    - Mspaint → calc → regedit → cmd → regedt32 … …

USB 장치 연결 정보 (1/12)



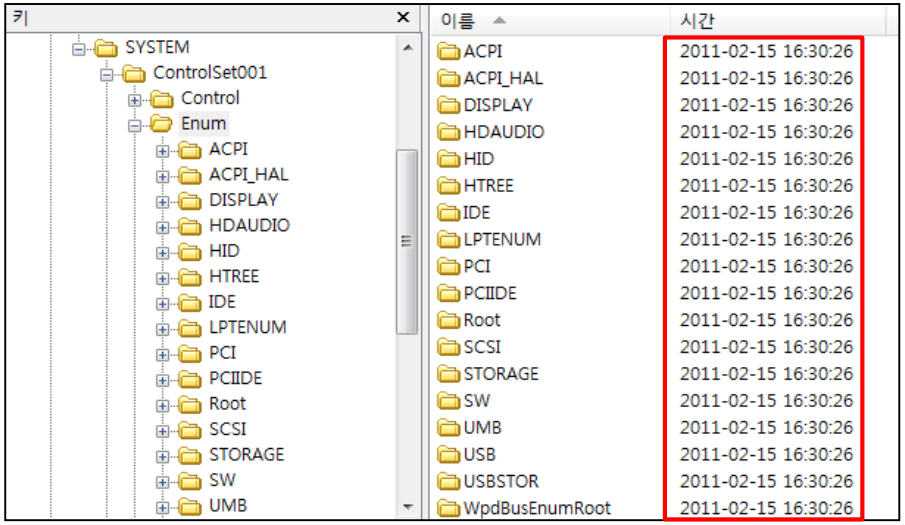
- **USB 저장매체 인식 절차**

1. USB 저장매체가 연결되면 버스 드라이버는 PnP 관리자에게 장치의 고유한 식별번호(device descriptor)를 사용하여 연결 알림
   - **device descriptor** – 제조사, 일련번호, 드라이버 정보 등을 포함
2. PnP 관리자는 받은 정보를 기반으로 Device Class ID를 설정하고 적절한 드라이버 검색
3. 드라이버가 없을 경우 사용자 모드의 PnP 관리자는 해당 장치의 펌웨어로부터 드라이버를 전달받아 로드하고 레지스트리에 기록
   - **HKLM₩SYSTEM₩ControlSet00X₩Enum₩USBSTOR₩{DID, device class identifier}**
   - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{GUID}**
4. 장치 드라이버 설치과정은 로그 파일에 저장

▪ 결과적으로 **로그 파일(setupapi.log) 및 레지스트리를** 통해 USB 장치의 흔적 파악 가능

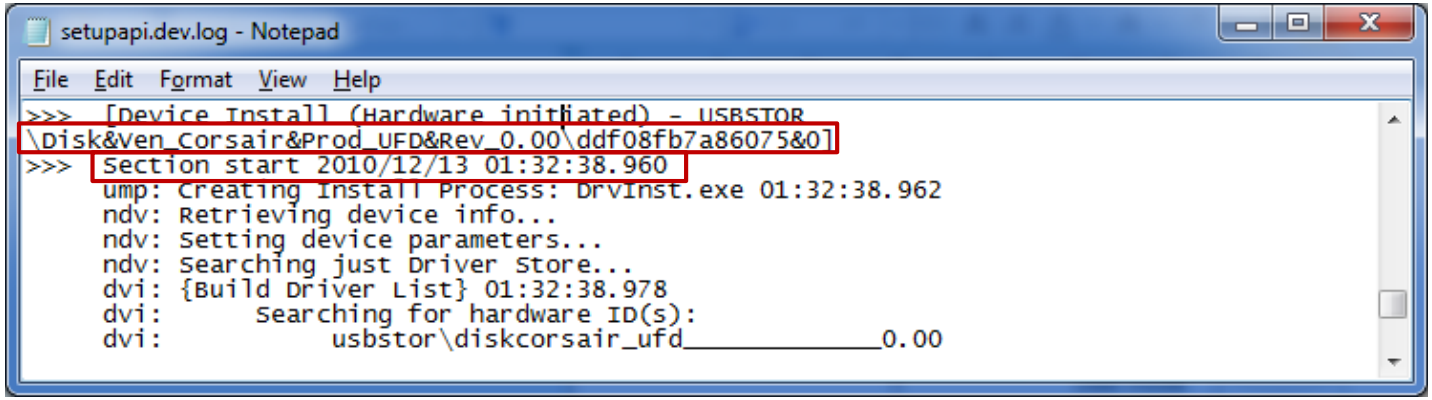
USB 장치 연결 정보 (2/12)

- **레지스트리 키 마지막 수정 시간 정보 확인시 주의사항**
  - 각 레지스트리 키에는 해당 키의 마지막 수정 시간이 저장
  - 마지막 수정 시간 정보를 활용하여 USB의 다양한 흔적 파악 가능
  - 단, **Enum₩USB, Enum₩USBSTOR** 하위키의 시간은 고려되지 않아야 함
  - 보안 정책에 의해 (윈도우 Vista/7) PnP 관리자가 하위키 보안 토큰 설정을 위해 수시로 접근
    - RegSetKeySecurity API 호출 ➔ 마지막 수정 시간 변경



USB 장치 연결 정보 (3/12)

- **SetupAPI Logging**
  - **2000/XP – %SystemRoot%₩Setupapi.log**
  - **Vista/7 – %SystemRoot%₩Inf₩Setupapi.dev.log**



  - **Device Class ID** – Disk&Ven_Corsair&Prod_UFD&Rev_0.00
  - **Unique Instance ID** – ddf08fb7a86075&0
  - **Section Start** – 2010/12/13 01:32:38.960

USB 장치 연결 정보 (4/12)

- **DID(Device class ID), UID(Unique Instance ID) 형식**
  - **Device Class ID** – Disk&Ven_Corsair&Prod_UFD&Rev_0.00

Disk & Ven_????? & Prod_????? & Rev_????

↓

Disk & Ven_{제조사명} & Prod_{제품명} & Rev_{버전번호}

  - **Unique Instance ID** – ddf08fb7a86075&0

?????????????? & #

↓ 시리얼번호가 있는 경우

{시리얼번호} & #

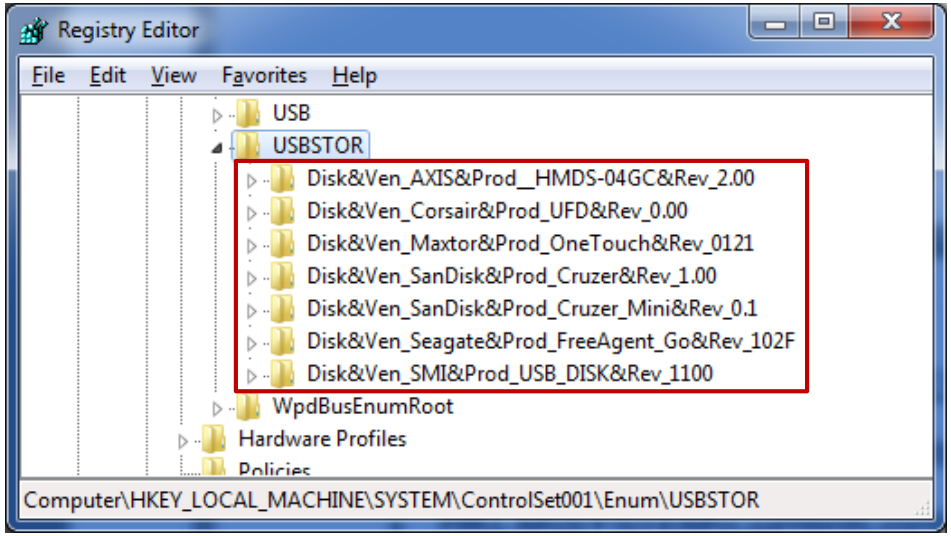
& ??????????? &

↓ 시리얼번호가 없는 경우

& {PnP 관리자 생성 번호} &

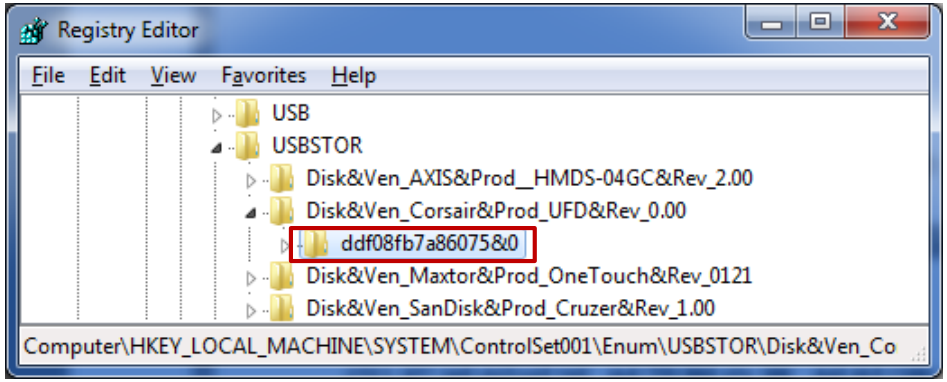
USB 장치 연결 정보 (5/12)

- **저장매체 정보**
  - **HKLM₩SYSTEM₩ControlSet00X₩Enum₩USBSTOR**
  - Device Class ID 형식을 통해 제조사, 제품명, 버전 정보 확인



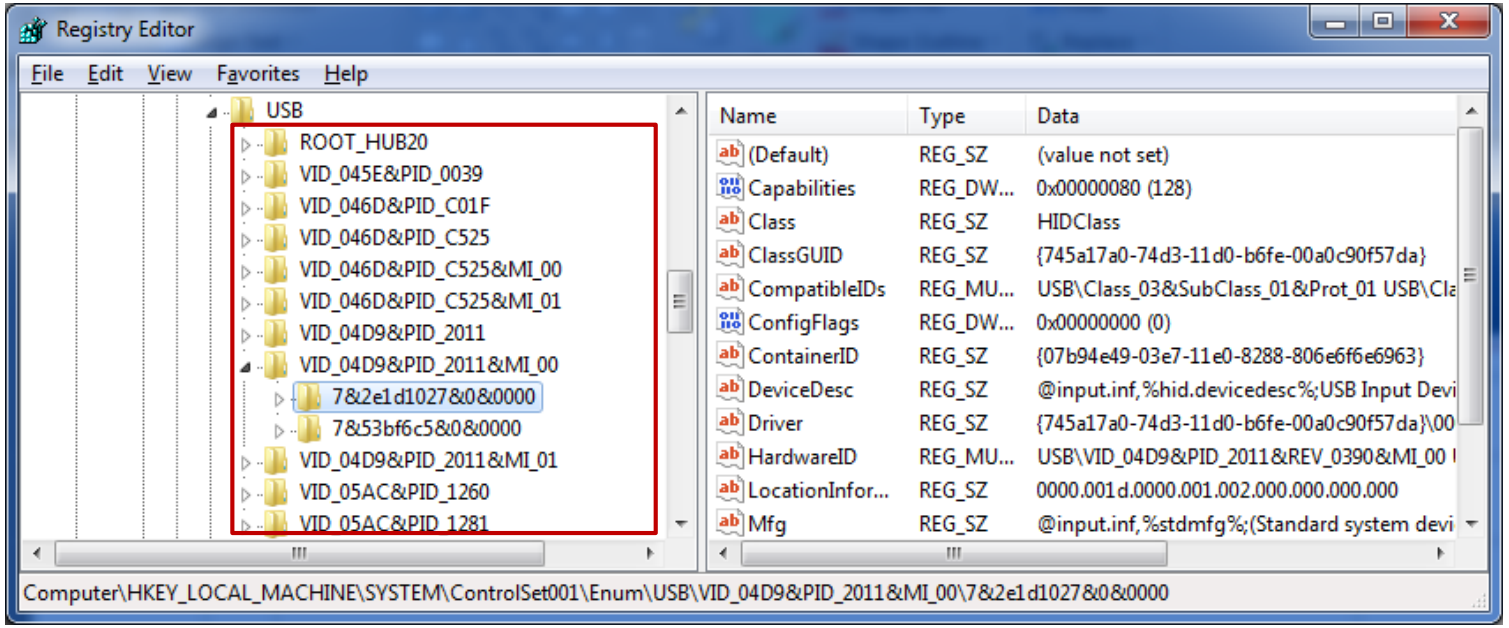
USB 장치 연결 정보 (6/12)

- **시리얼번호**
  - **HKLM₩SYSTEM₩ControlSet00X₩Enum₩USBSTOR₩{Device Class ID}**
  - Device Class ID 하위키의 Unique Instance ID 형식을 통해 시리얼번호 확인



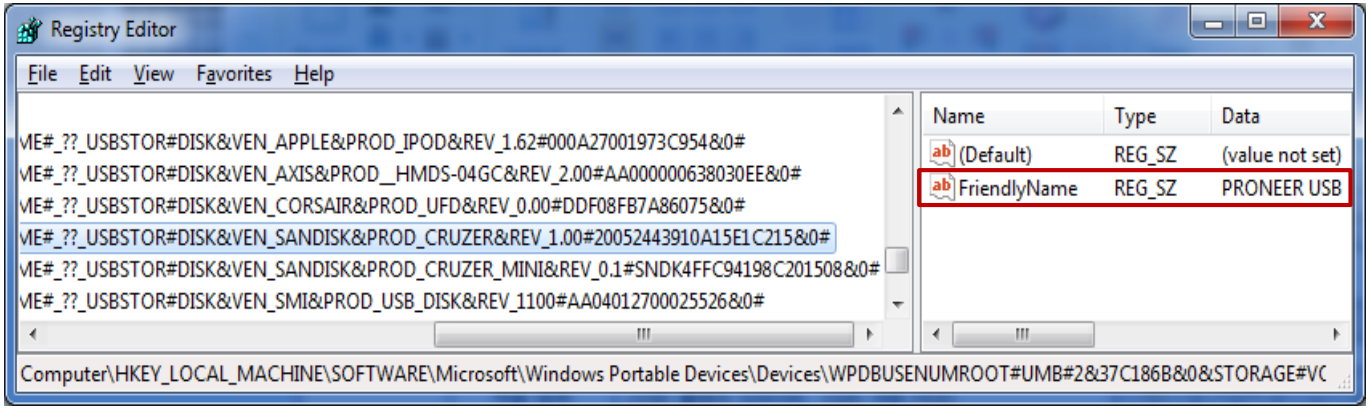
USB 장치 연결 정보 (7/12)

- **제조사 ID, 제품 ID**
  - **HKLM₩SYSTEM₩ControlSet00X₩Enum₩USB**
  - VID_####&PID_#### ➔ 제조사 ID, 제품 ID



USB 장치 연결 정보 (8/12)

- **연결된 볼륨명**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩Devices**
  - 하위키 중 제품명 또는 시리얼번호를 포함하는 키 검색
  - **FriendlyName**
    - 장치명이 설정된 경우 – 설정한 장치명
    - 장치명이 설정되지 않은 경우 – 연결된 볼륨명



USB 장치 연결 정보 (9/12)

- **최초 연결 시각**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows Portable Devices₩Devices**
  - 하위키 중 제품명 또는 시리얼번호를 포함하는 키 검색
  - 해당 키의 마지막 수정 시간 (Last Written Time)
    - 장치명이 설정된 경우 – 장치명을 변경하지 않는다면 최초 연결시간 유지
    - 장치명이 설정되지 않은 경우 – 연결된 볼륨명이 변경되지 않고 계속 사용되면 최초 연결시간 유지

USB 장치 연결 정보 (10/12)

- **부팅 이후 최초 연결 시각**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}**
    - **GUID for Disk**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}**
    - **GUID for Volume**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{A5DCBF10-6530-11D2-901F-00C04FB951ED}**
    - **GUID for USB**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{6AC27878-A6FA-4155-BA85-F98F491D4F33}**
    - **GUID for Windows Portable Device (Vista or later)**
  - **HKLM₩SYSTEM₩ControlSet00X₩Enum₩USBSTOR₩[Device Class ID]**
  - 하위키 중 제품명이나 시리얼번호를 포함하는 키 검색
  - 해당 키의 마지막 수정 시간 (Last Written Time)
  - **Enum₩USBSTOR**를 통해서도 확인이 가능하지만 보안정책에 의한 시간정보 임의 갱신으로 바람직하지 않음

USB 장치 연결 정보 (11/12)

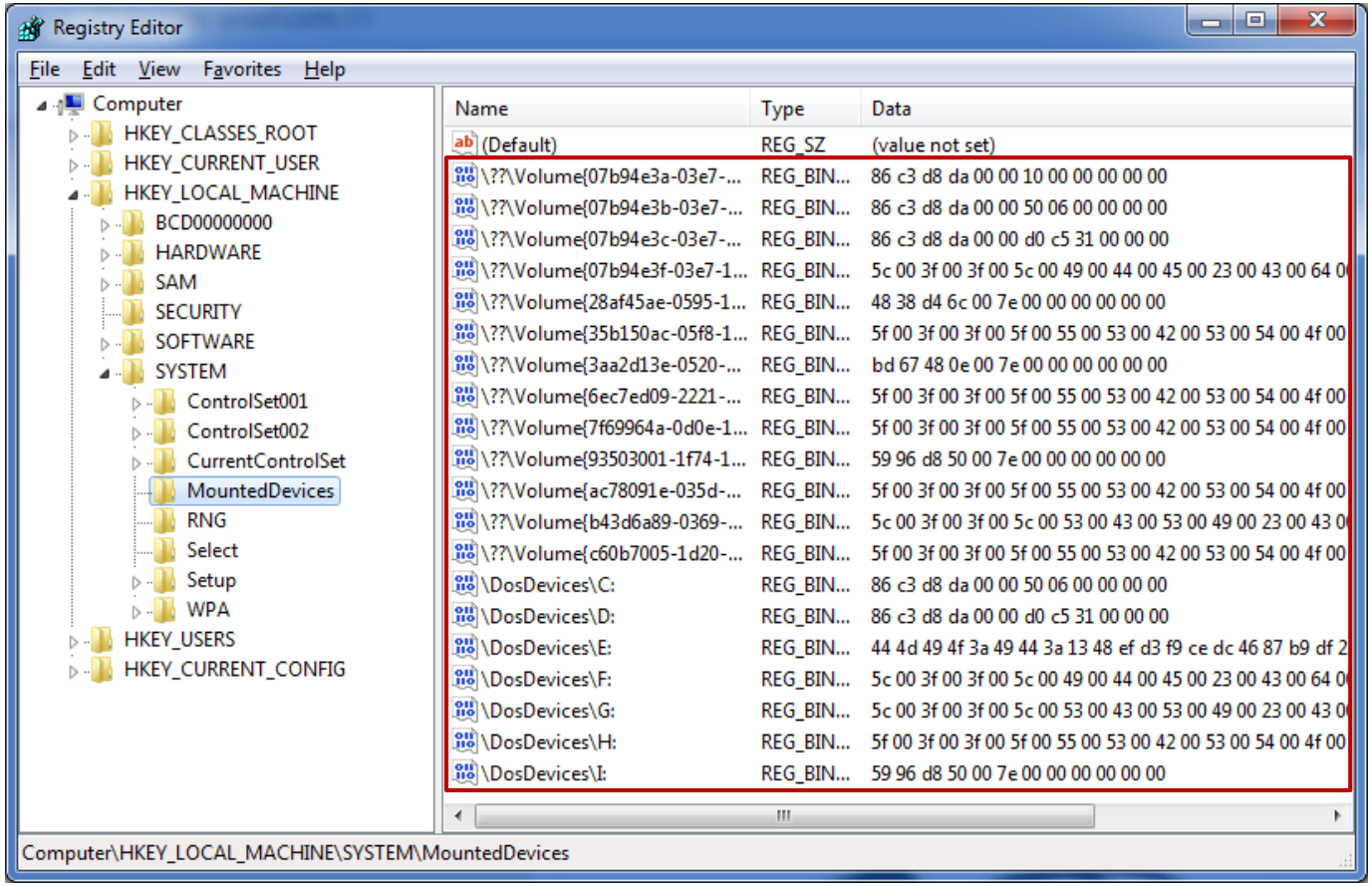
- **마지막 연결 시각**
  - **HKU₩{USER}₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩MountPoint2**
  - **HKLM₩SYSTEM₩ControlSetXXX₩Enum₩USB₩VID_####&PID_####**
  - 하위키 중 Volume GUID 또는 시리얼번호를 포함하는 키 검색
  - 해당 키의 마지막 수정 시간 (Last Written Time)
  - **Enum₩USB**를 통해서도 확인이 가능하지만 보안정책에 의한 시간정보 임의 갱신으로 바람직하지 않음

USB 장치 연결 정보 (12/12)

- **마지막 연결/해제 시간**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{53F56307-B6BF-11D0-94F2-00A0C91EFB8B}₩###?#USBSTOR#....[Serial Number]....{₩|₩#₩}Control**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{53F5630D-B6BF-11D0-94F2-00A0C91EFB8B}₩###?#USBSTOR#....[Serial Number]....{₩|₩#₩}Control**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{A5DCBF10-6530-11D2-901F-00C04FB951ED}₩###?#USBSTOR#....[Serial Number]....{₩|₩#₩}Control**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩DeviceClasses₩{6AC27878-A6FA-4155-BA85-F98F491D4F33}₩###?#USBSTOR#....[Serial Number]....{₩|₩#₩}Control**
  - 장치가 연결/해제되면 Control 키의 시간이 변경됨
  - Control 키의 마지막 수정 시간 (Last Written Time)
    - USB 연결 상태 – USB의 마지막 연결 시간
    - USB 해제 상태 – 마지막 연결 연결 해제 시간
  - 단, Control 키는 활성 상태에서만 유지되므로 오프라인 레지스트리 분석은 불가능

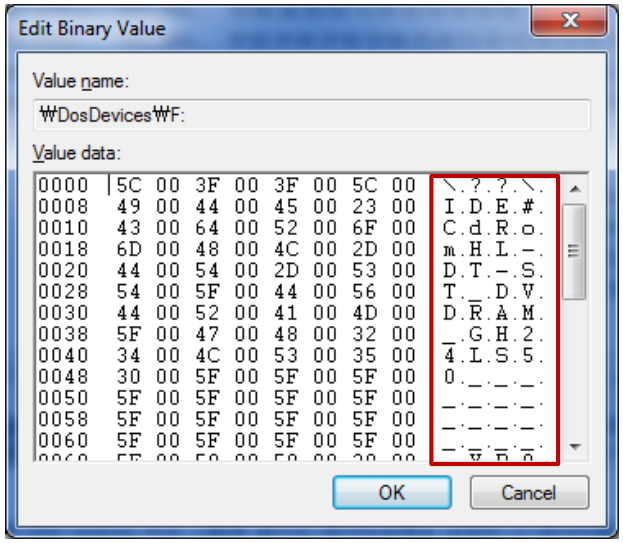
연결된 저장장치 정보 (1/5)

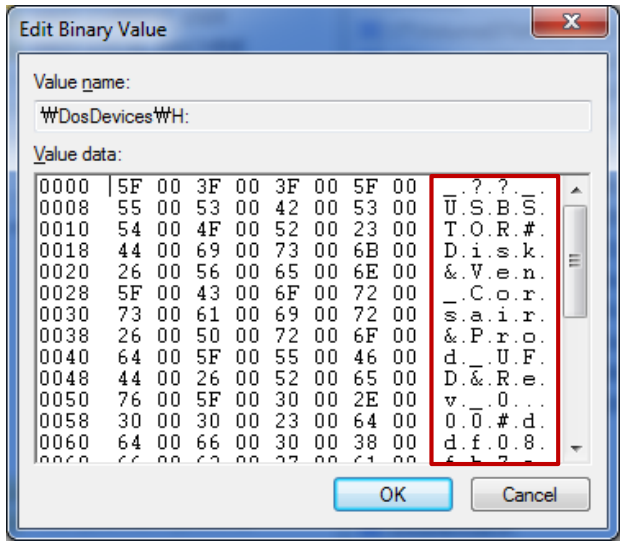
- **마운트된 저장장치**
  - **HKLM₩SYSTEM₩MountedDevices**



연결된 저장장치 정보 (2/5)

- **마운트된 저장장치**
  - **HKLM₩SYSTEM₩MountedDevices**

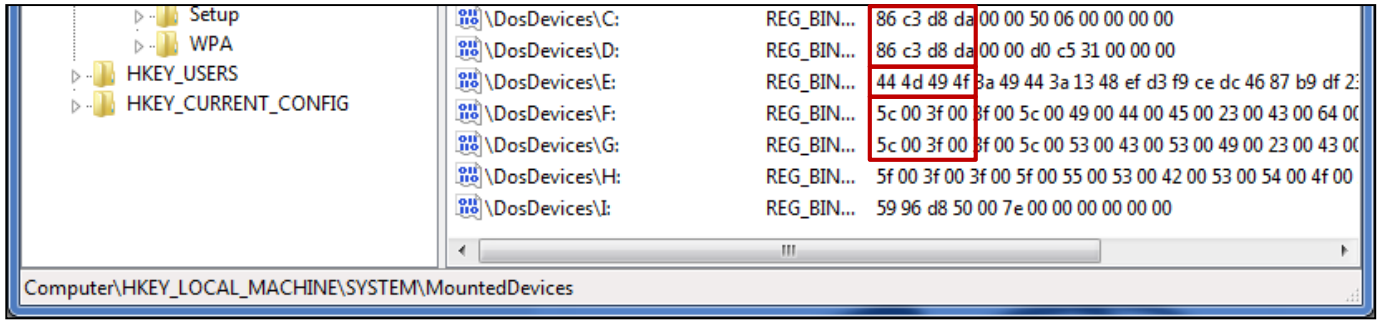




  - 데이터를 통해 해당 드라이브에 마운트된 장치 형식 확인 가능

연결된 저장장치 정보 (3/5)

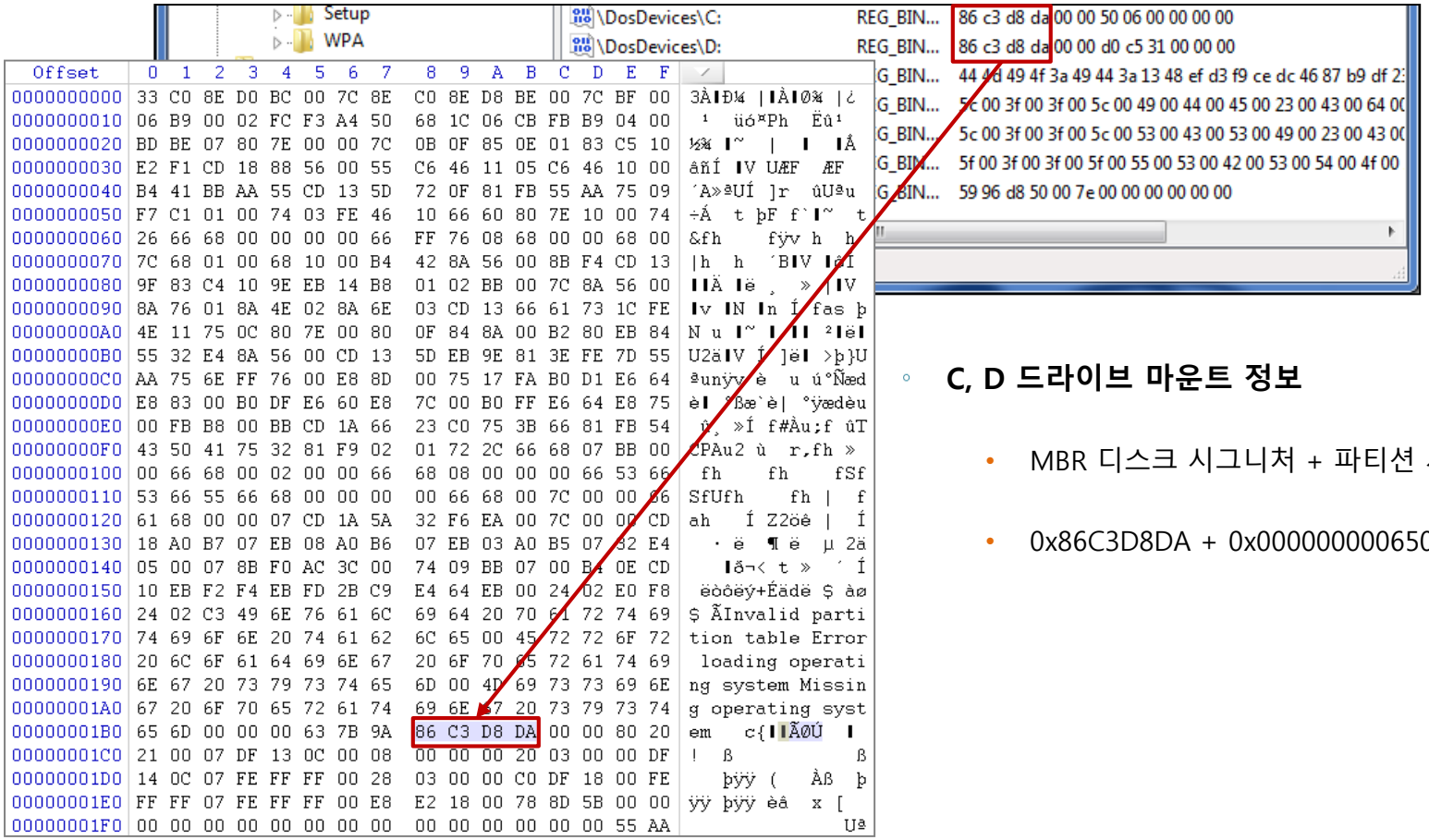
- **마운트된 저장장치**
  - **디스크 시그니처 (Disk Signature)**



  - 시스템에는 총 3개의 디스크가 마운트
    - 디스크 1 – C, D 드라이브(파티션) 사용
    - 디스크 2 – E 드라이브(파티션) 사용
    - 디스크 3 – F, G 드라이브(파티션) 사용

연결된 저장장치 정보 (4/5)

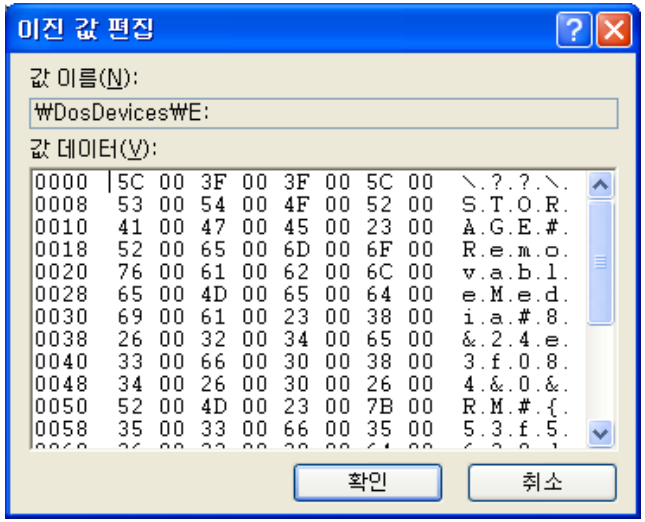
- **마운트된 저장장치**
  - **디스크 시그니처 (Disk Signature)**

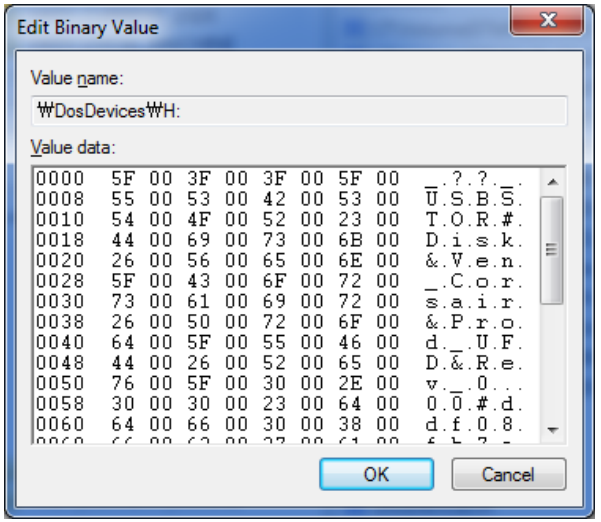


- **C, D 드라이브 마운트 정보**
  - MBR 디스크 시그니처 + 파티션 시작 위치
  - 0x86C3D8DA + 0x0000000006500000

연결된 저장장치 정보 (5/5)

- **마운트된 저장장치**
  - **외장형 저장장치 마운트 정보**

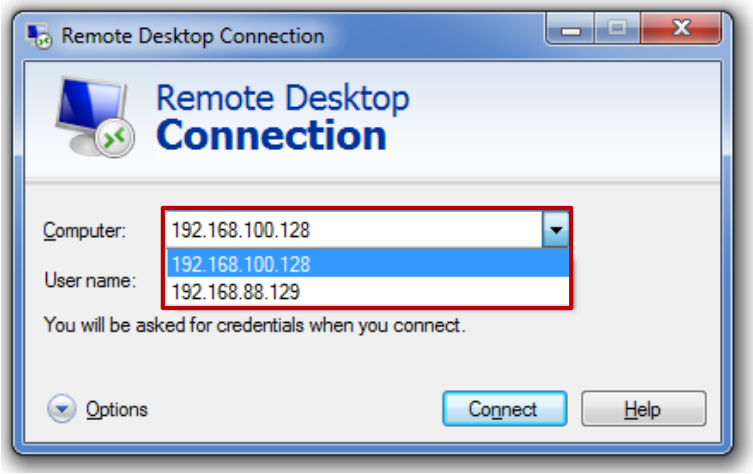




- **2000/XP –** ₩??₩STORAGE#RemovableMedia#**8&24e3f084&0**&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  - ₩??₩STORAGE#RemovableMedia#**{ParentIdPrefix}**&RM#{GUID}
- **Vista/7 –** _??_USBSTOR#Disk&Ven_Corsair&Prod_UFD&Rev_0.0.0#**ddf08fb7a86075&0**#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  - _??_USBSTOR#Disk&Ven_{제조사명}&Prod_{제품명}&Rev_0.0.0#**{시리얼번호}**#{GUID}

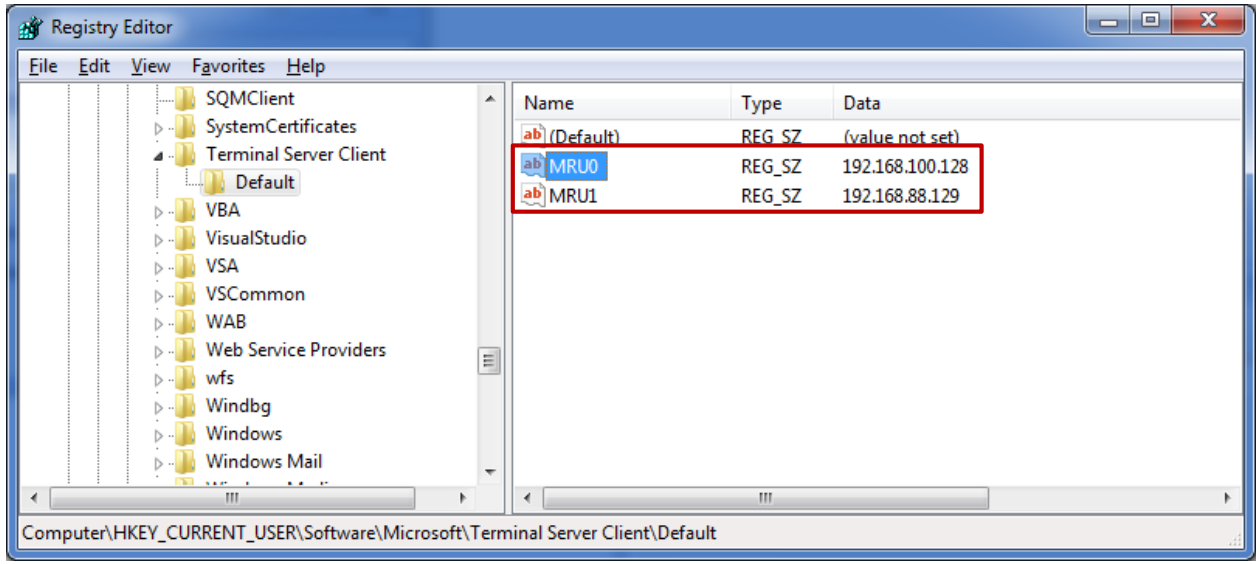
외부 시스템 연결 정보 (1/5)

- **원격 데스크탑 연결 정보 (RDP)**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Terminal Server Client₩Default**
  - 원격 데스크탑 연결(시작 → 실행 → "mstsc")을 수행한 이전 컴퓨터 IP



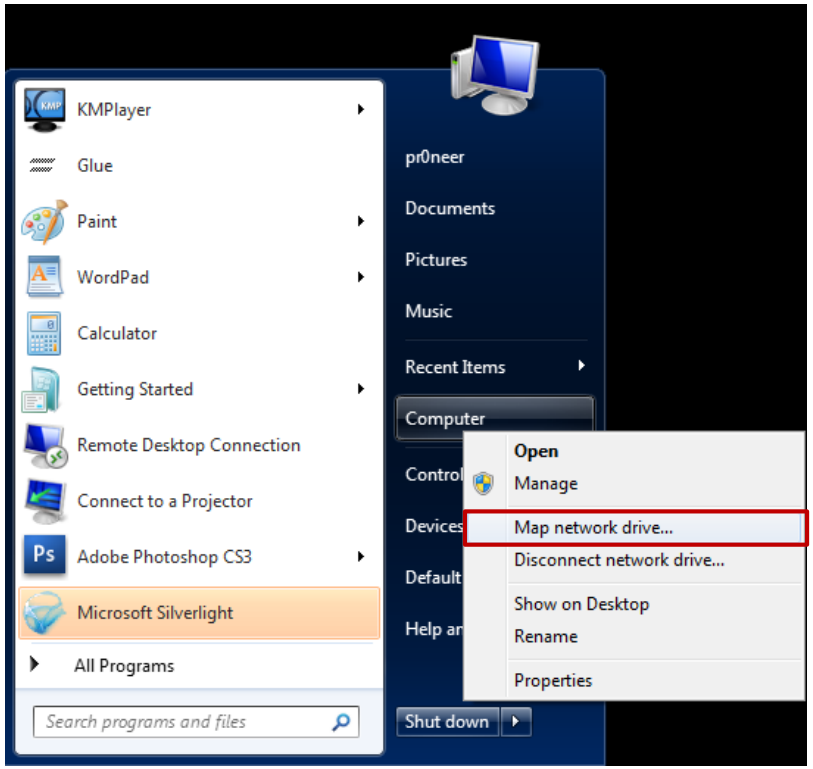
외부 시스템 연결 정보 (2/5)

- **원격 데스크탑 연결 정보 (RDP)**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Terminal Server Client₩Default**
  - **MRU#** – 숫자가 적을 수록 최근에 수행한 원격 데스크탑 연결 IP



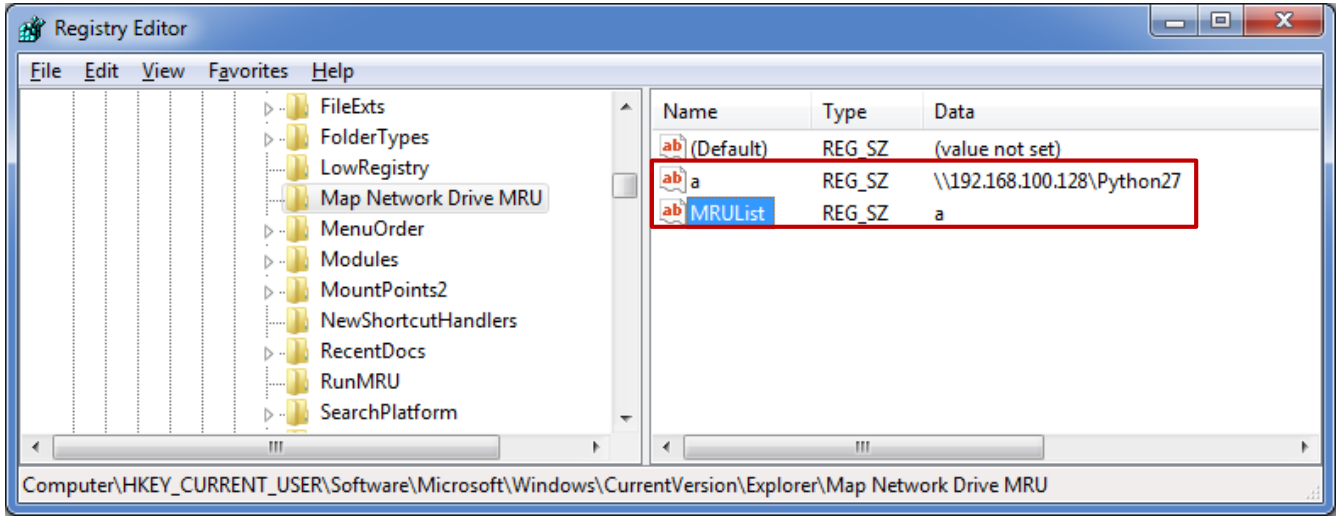
외부 시스템 연결 정보 (3/5)

- **네트워크 드라이브 연결**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Map Network Drive MRU**
  - 내컴퓨터 → 네트워크 드라이브 연결 (Map network drive....) 시 연결 정보



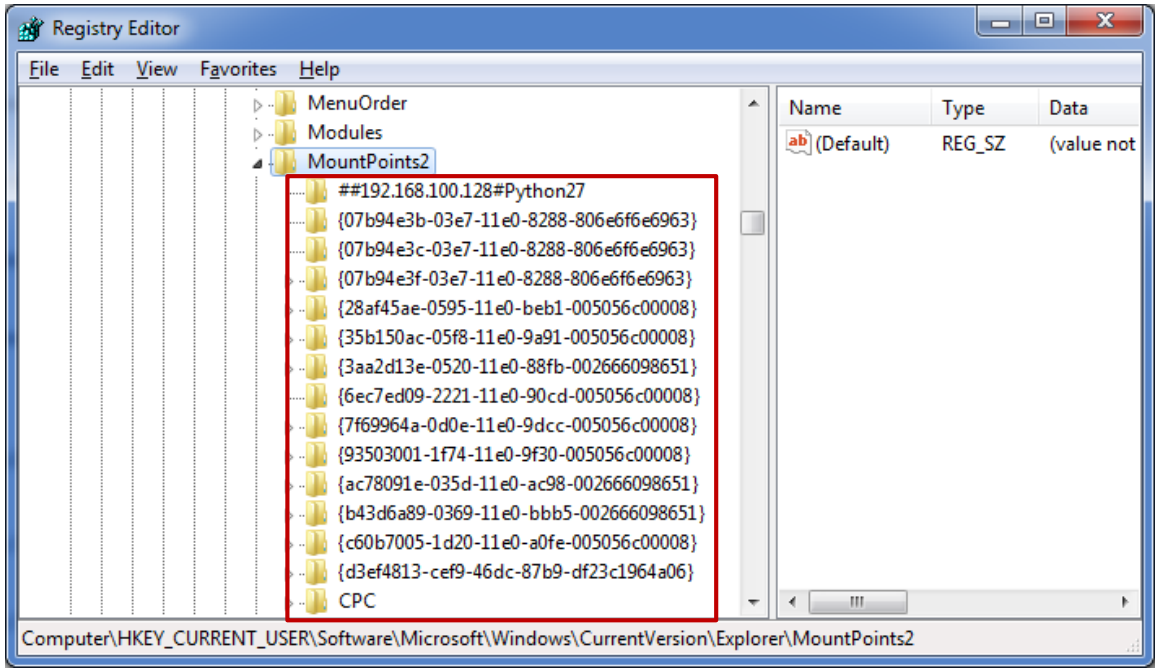
외부 시스템 연결 정보 (4/5)

- **네트워크 드라이브 연결**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Map Network Drive MRU**
  - **MRUList** – 네트워크 드라이브 연결 순서 확인



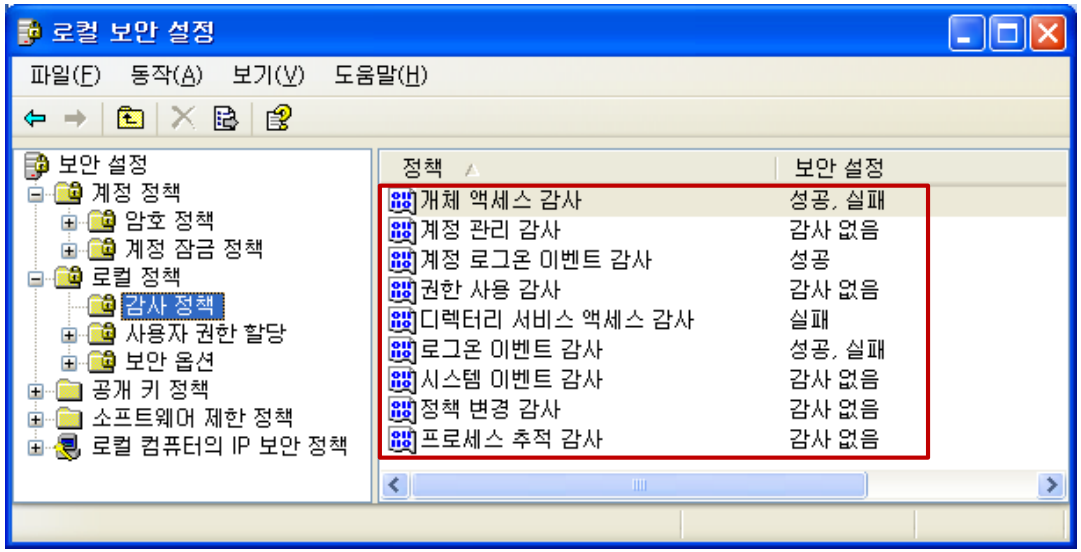
외부 시스템 연결 정보 (5/5)

- **마운트 포인트**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩MountPoints2₩{GUID}**
  - CPC₩Volume의 하위키와 연결하여 마운트된 볼륨 확인
  - 마운트된 저장장치(HKLM₩SYSTEM₩MountedDevices) 정보와 연결하여 마운트한 사용자 확인



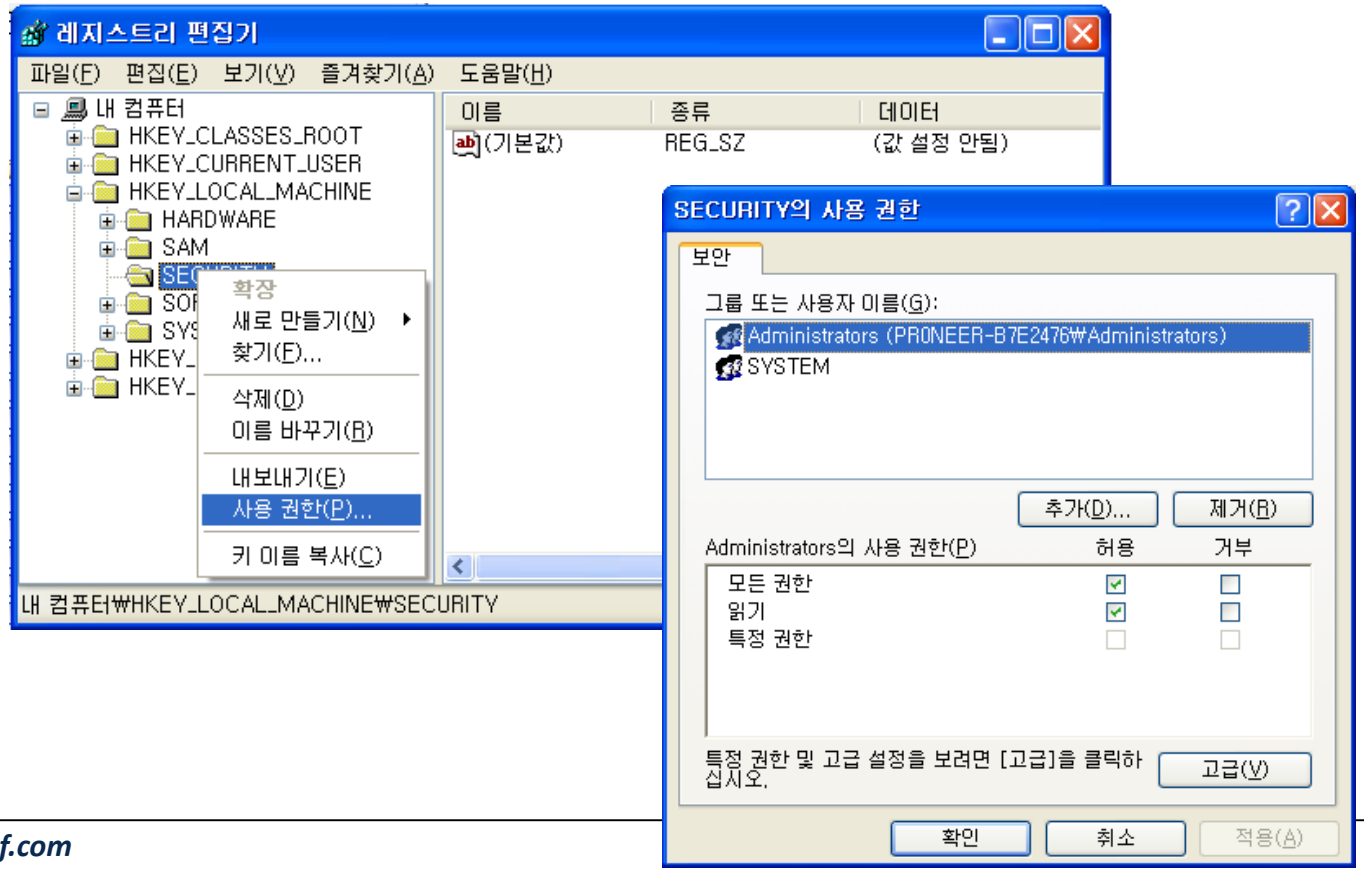
감사 정책 (1/8)

- **2000/XP 감사 정책**
  - 제어판 → 관리도구 → 로컬 보안 설정 → 로컬 정책 → 감사 정책



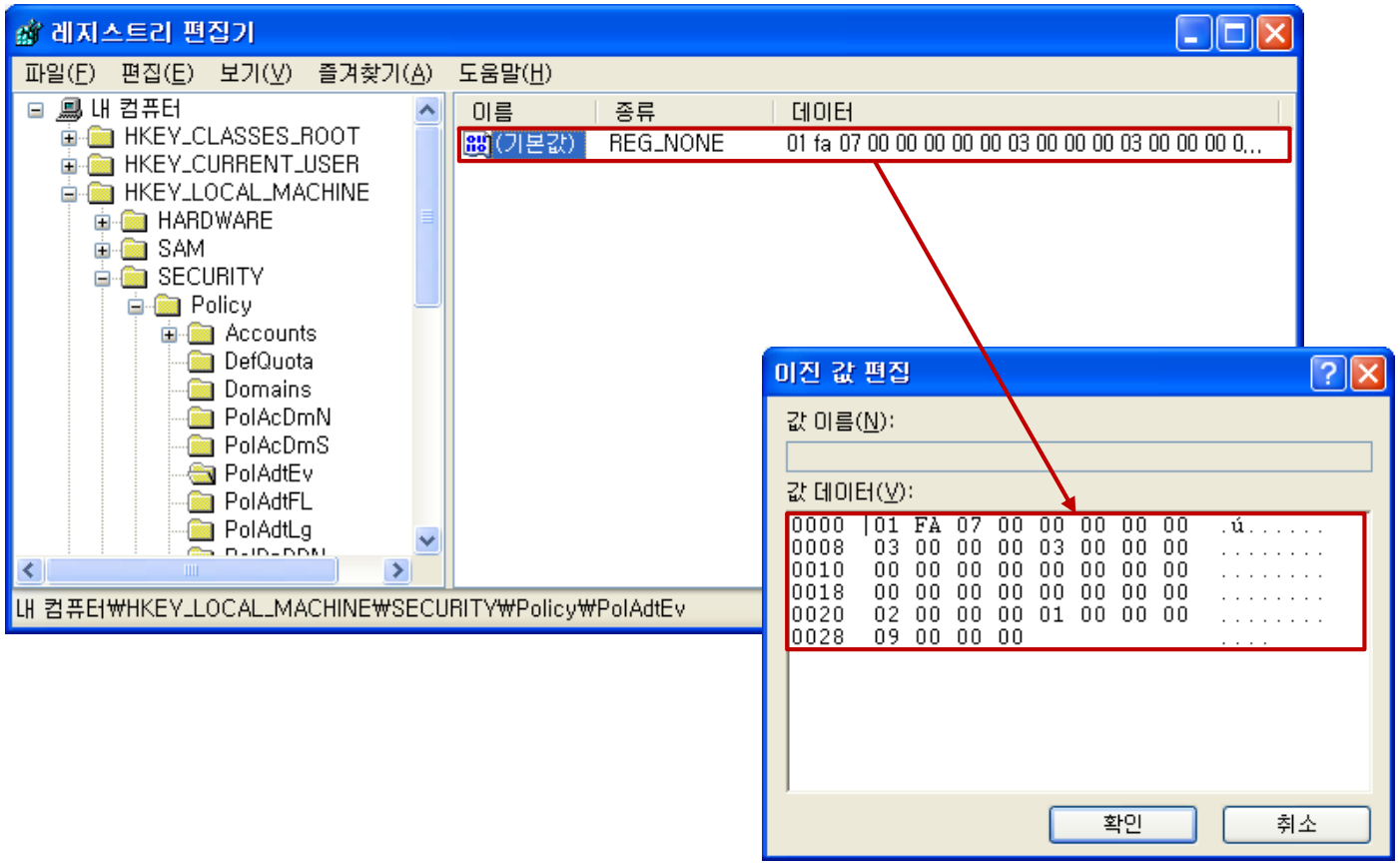
감사 정책 (2/8)

- **2000/XP 감사 정책**
  - **HKLM₩SECURITY₩Policy₩PolAdtEv**
  - 레지스트리 값 확인을 위해 해당 사용자에게 읽기 또는 모든 권한 부여



감사 정책 (3/8)

- **2000/XP 감사 정책**
  - **HKLM₩SECURITY₩Policy₩PolAdtEv**

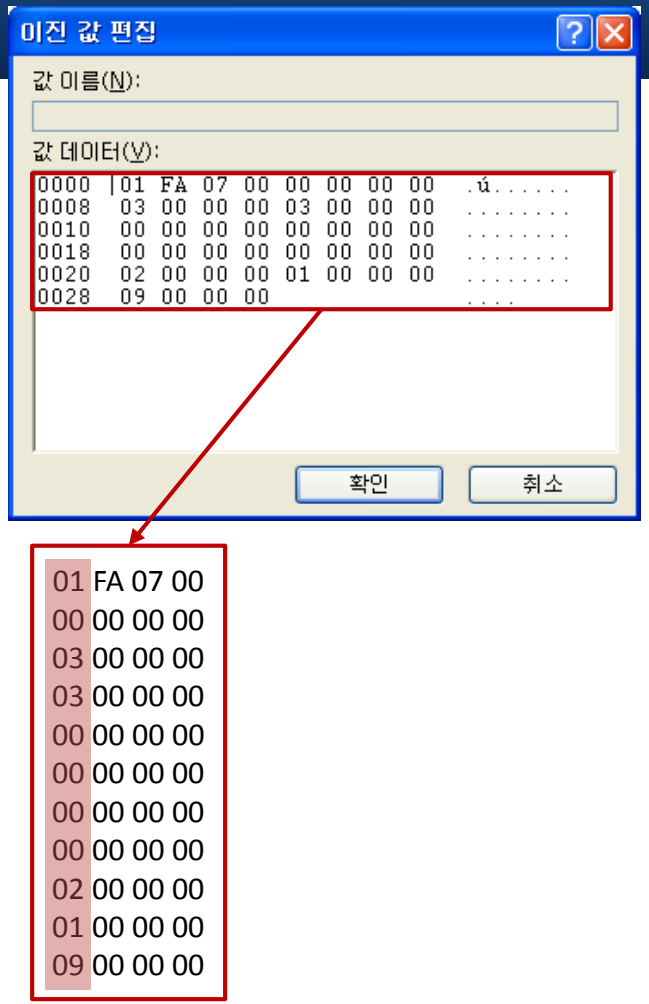


레지스트리 분석

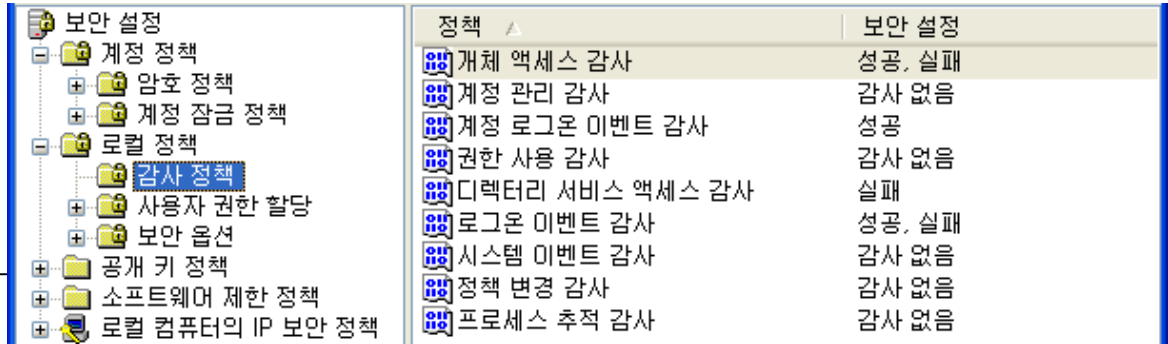
감사 정책 (4/8)

- **2000/XP 감사 정책**
  - **HKLM₩SECURITY₩Policy₩PolAdtEv**

위치 (Dec)	값 (Hex)	설명
0 – 0	**01**	0 : 감사정책 없음 1 : 1개 이상의 감사정책이 설정되어 있음
4 – 7	**00** 00 00 00	시스템 이벤트 감사
8 – 11	**03** 00 00 00	로그온 이벤트 감사
12 – 15	**03** 00 00 00	개체 액세스 감사
16 – 19	**00** 00 00 00	권한 사용 감사
20 – 23	**00** 00 00 00	프로세스 추적 감사
24 – 27	**00** 00 00 00	정책 변경 감사
28 – 31	**00** 00 00 00	계정 관리 감사
32 – 35	**02** 00 00 00	디렉터리 서비스 액세스 감사
36 – 39	**01** 00 00 00	계정 로그온 이벤트 감사

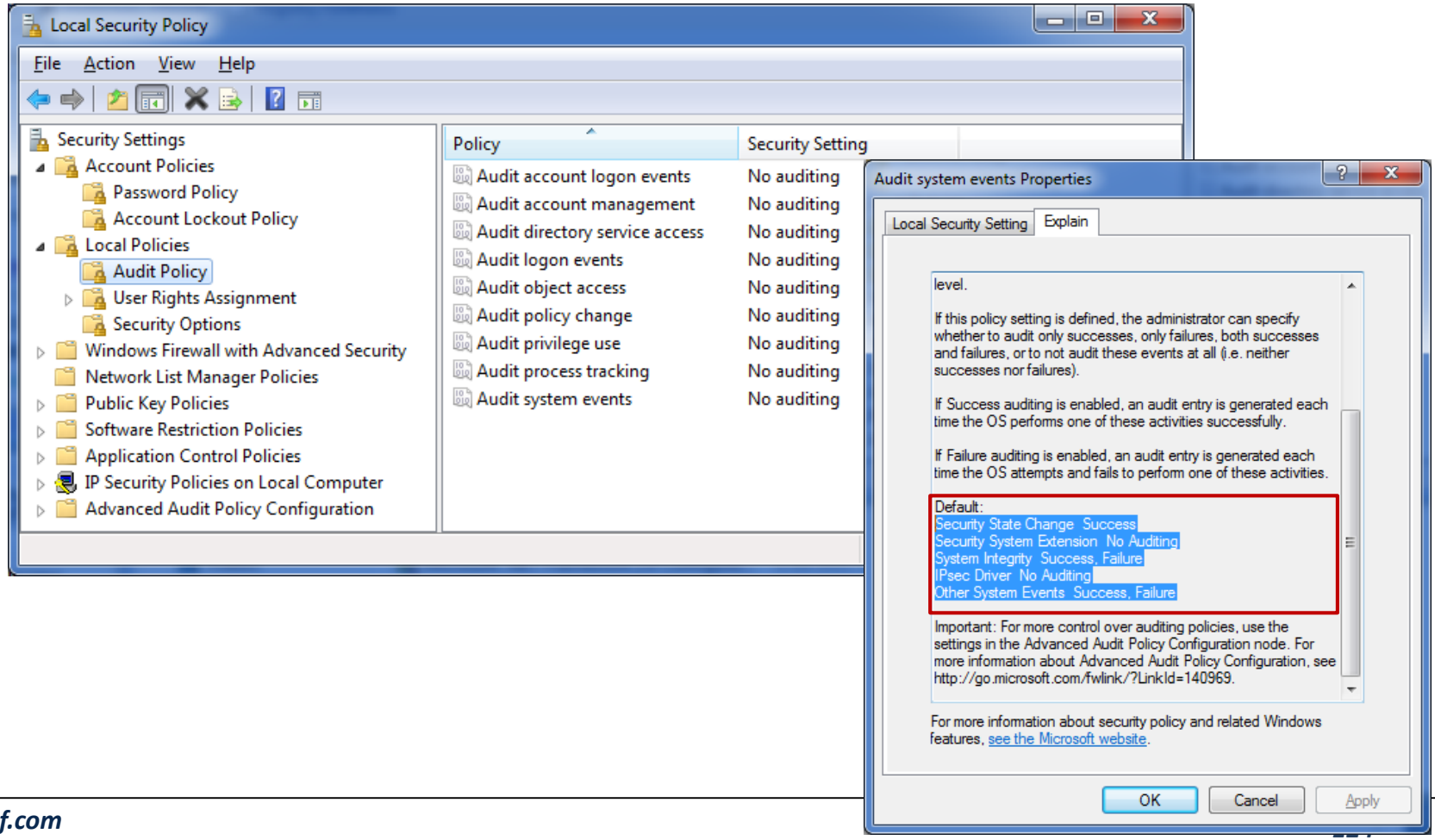


- **0x00 :** 감사 없음
- **0x01 :** 성공 이벤트 감사
- **0x02 :** 실패 이벤트 감사
- **0x03 :** 성공, 실패 이벤트 감사



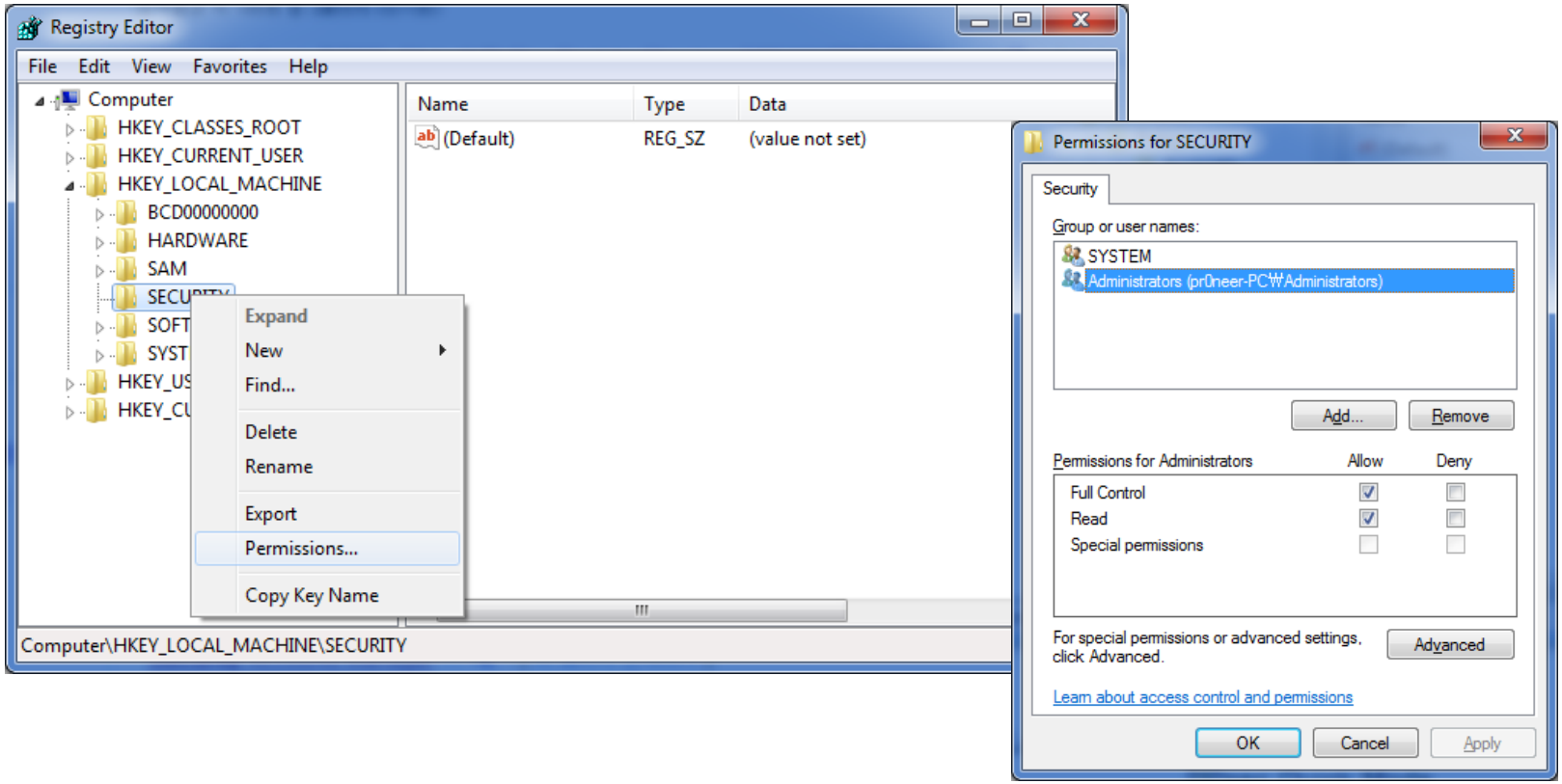
감사 정책 (5/8)

- **Vista/7 감사 정책**
  - 제어판 → 관리도구 → 로컬 보안 설정 → 로컬 정책 → 감사 정책



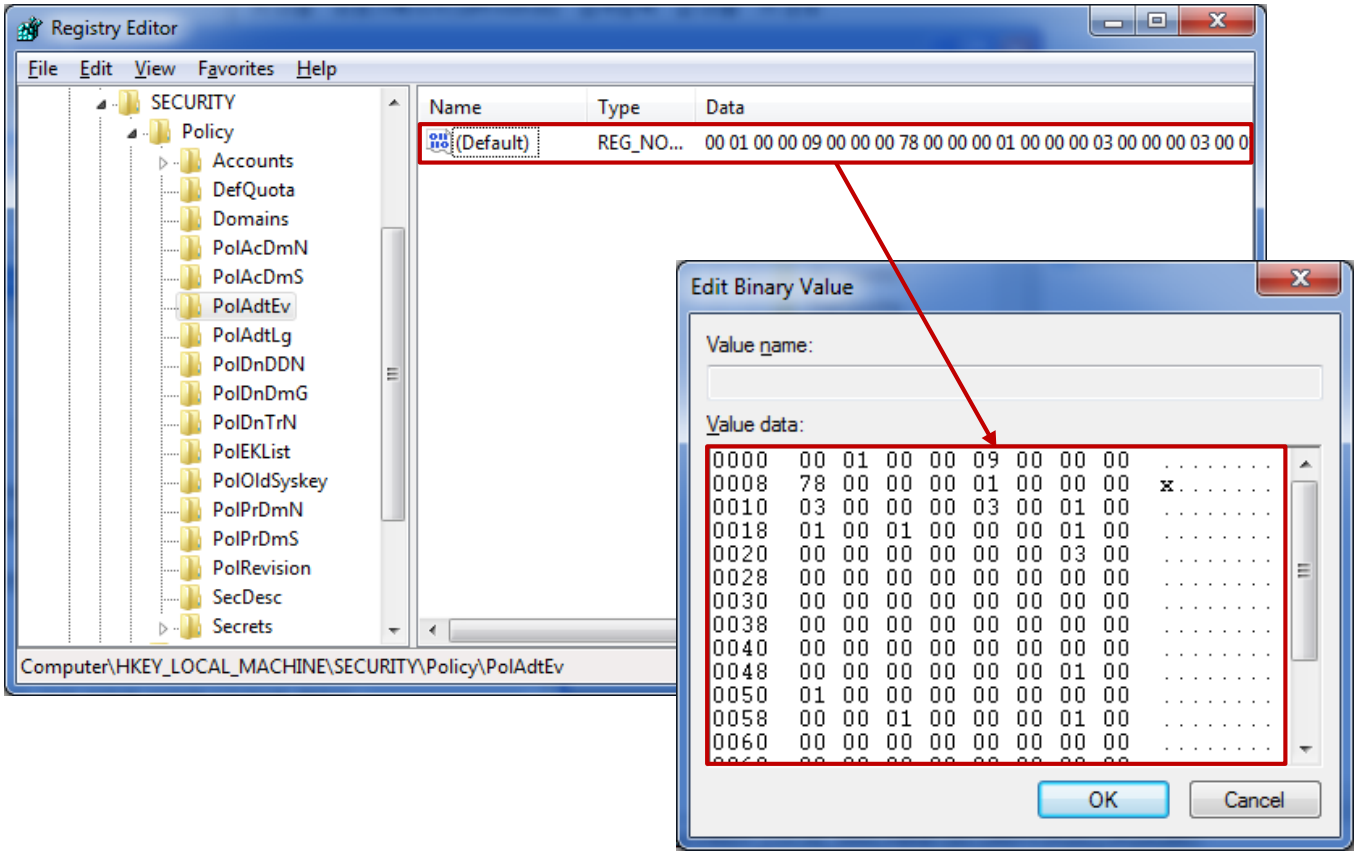
감사 정책 (6/8)

- **Vista/7 감사 정책**
  - **HKLM₩SECURITY₩Policy₩PolAdtEv**
  - 레지스트리 값 확인을 위해 해당 사용자에게 읽기 또는 모든 권한 부여



감사 정책 (7/8)

- **Vista/7 감사 정책**
  - **HKLM₩SECURITY₩Policy₩PolAdtEv**



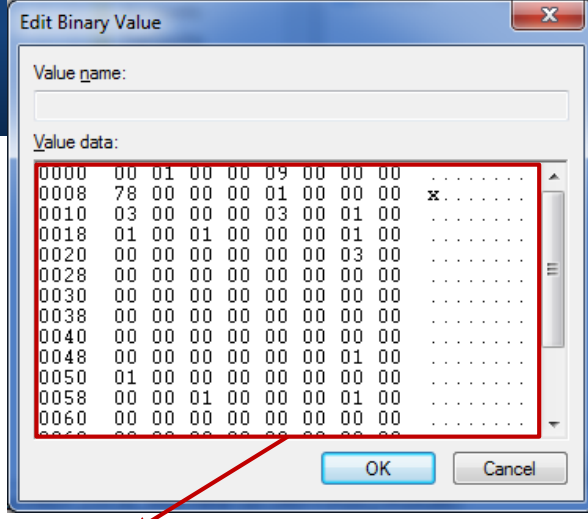
레지스트리 분석

감사 정책 (8/8) http://www.kazamiya.net/files/PolAdtEv_Structure_en_rev2.pdf

- **Vista/7 감사 정책**
  - **HKLM₩SECURITY₩Policy₩PolAdtEv**

위치 (Dec)	값 (Hex)	설명
0 – 0	**01**	0 : 감사정책 없음 1 : 1개 이상의 감사정책이 설정되어 있음
12 – 21	**01** 00 00 00 … ….	시스템 이벤트 감사
22 – 39	**03** 00 01 00 … …	로그온 이벤트 감사
40 – 61	**00** 00 00 00 … …	개체 액세스 감사
62 – 67	**00** 00 00 00 … …	권한 사용 감사
68 – 75	**00** 00 00 00 … …	프로세스 추적 감사
76 – 87	**01** 00 01 00 … …	정책 변경 감사
88 – 99	**01** 00 01 00 … …	계정 관리 감사
100 – 107	**01** 00 00 00 … …	디렉터리 서비스 액세스 감사
108 – 115	**01** 00 01 00 … …	계정 로그온 이벤트 감사

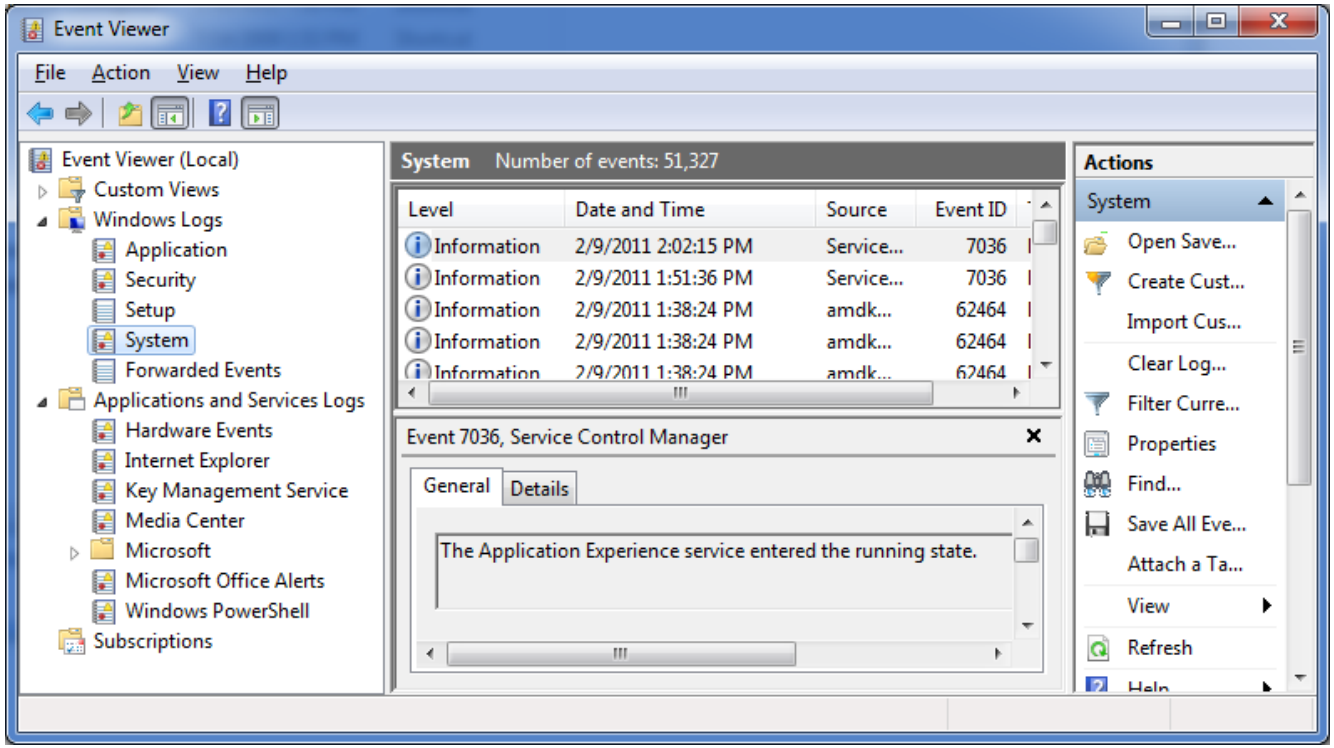
- **0x00 :** 감사 없음
- **0x01 :** 성공 이벤트 감사
- **0x02 :** 실패 이벤트 감사
- **0x03 :** 성공, 실패 이벤트 감사



00 01
00 00
09 00
00 00
78 00
00 00
01 00
00 00
03 00
00 00
03 00
01 00
01 00
01 00
00 00
01 00
00 00
… ….

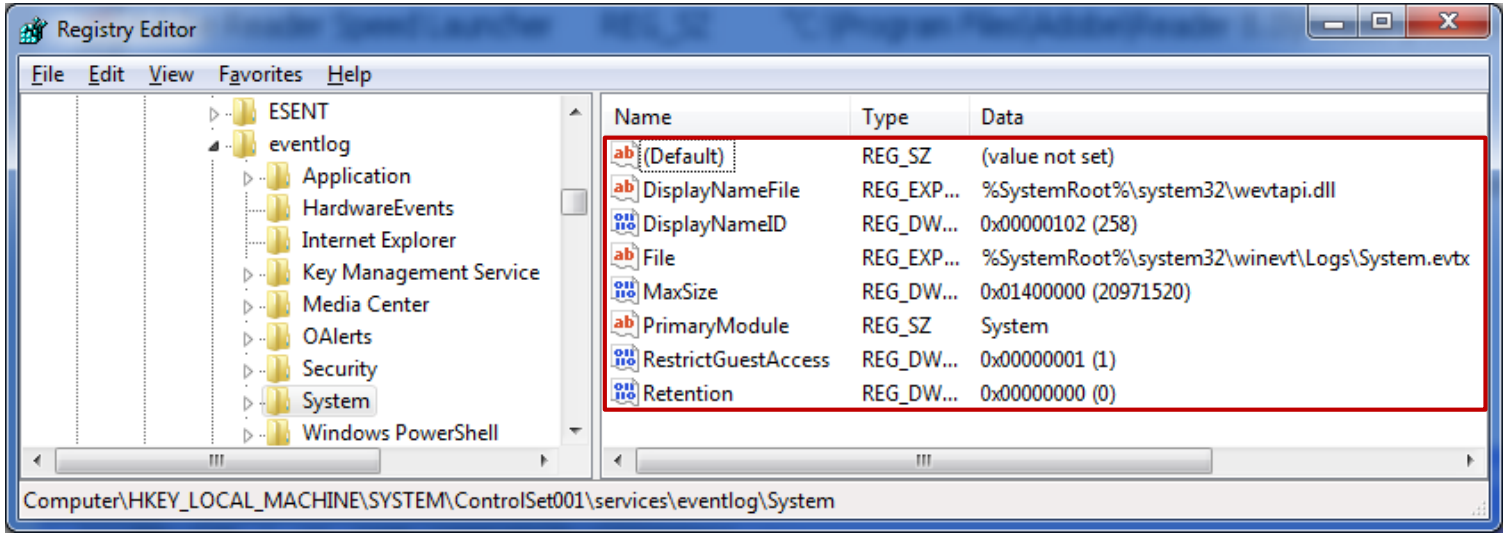
이벤트 로그 (1/2)

- **이벤트 로그 설정 정보**
  - 제어판 → 관리도구 → 이벤트 뷰어



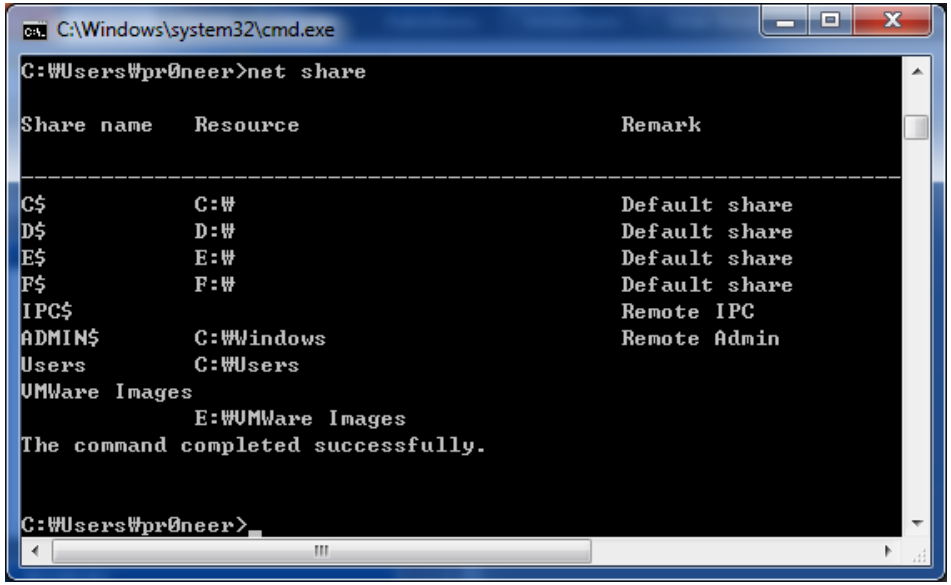
이벤트 로그 (2/2)

- **이벤트 로그 설정 정보**
  - **HKLM₩System₩ControlSet00X₩Services₩eventlog**
    - **Application, Security, System …**
  - 로그 파일 경로, 로그 파일 최대 크기, 로그 유지 기간 등의 정보 확인



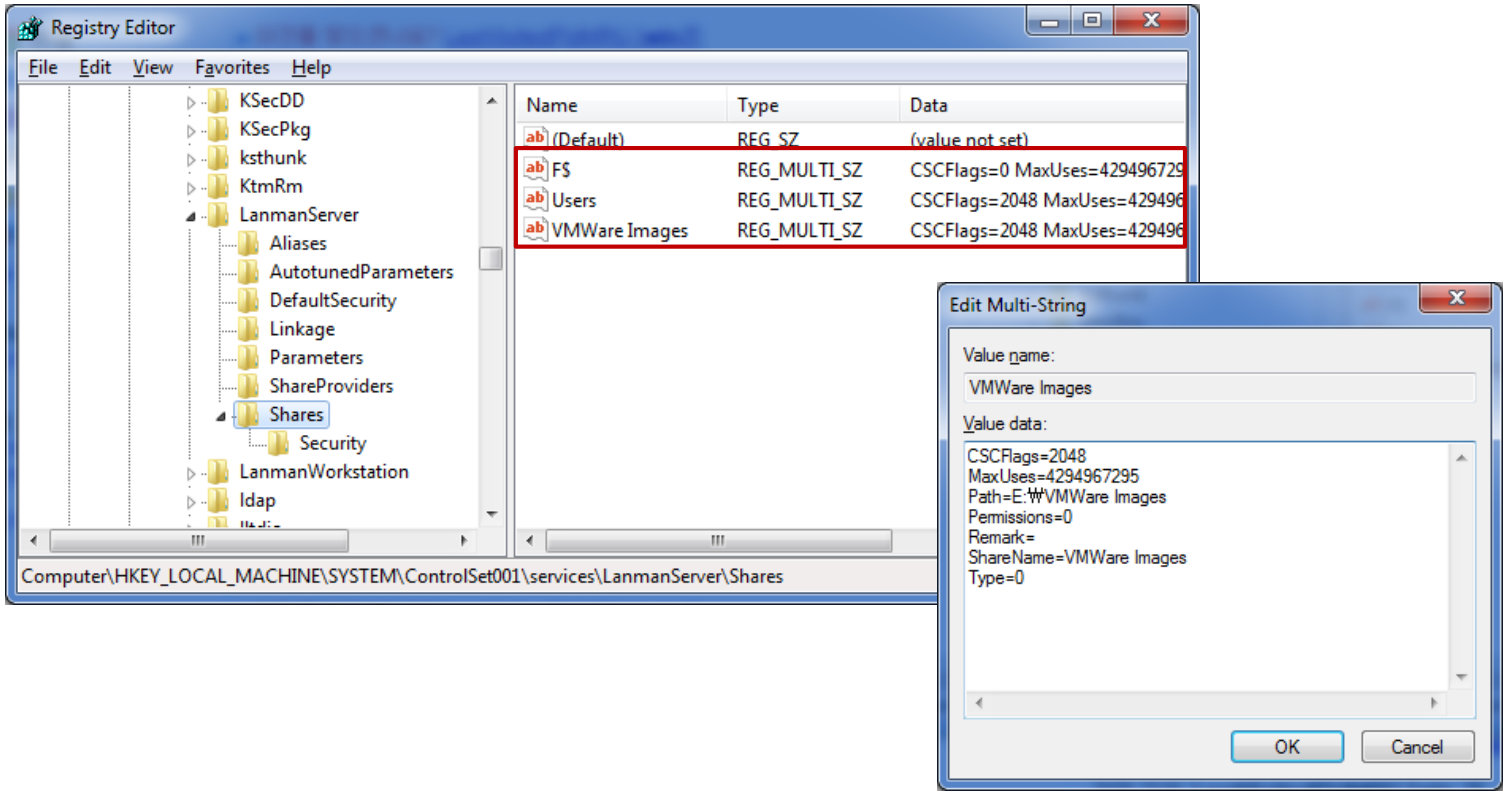
공유 목록 (1/2)

- **공유 폴더 목록**
  - **HKLM₩SYSTEM₩ContolSet00X₩Services₩LanmanServer₩Shares**
  - "net share" 명령을 통해 공유 폴더 확인
  - 기본적인 공유 목록이 아닌 사용자가 직접 추가한 항목만 관리



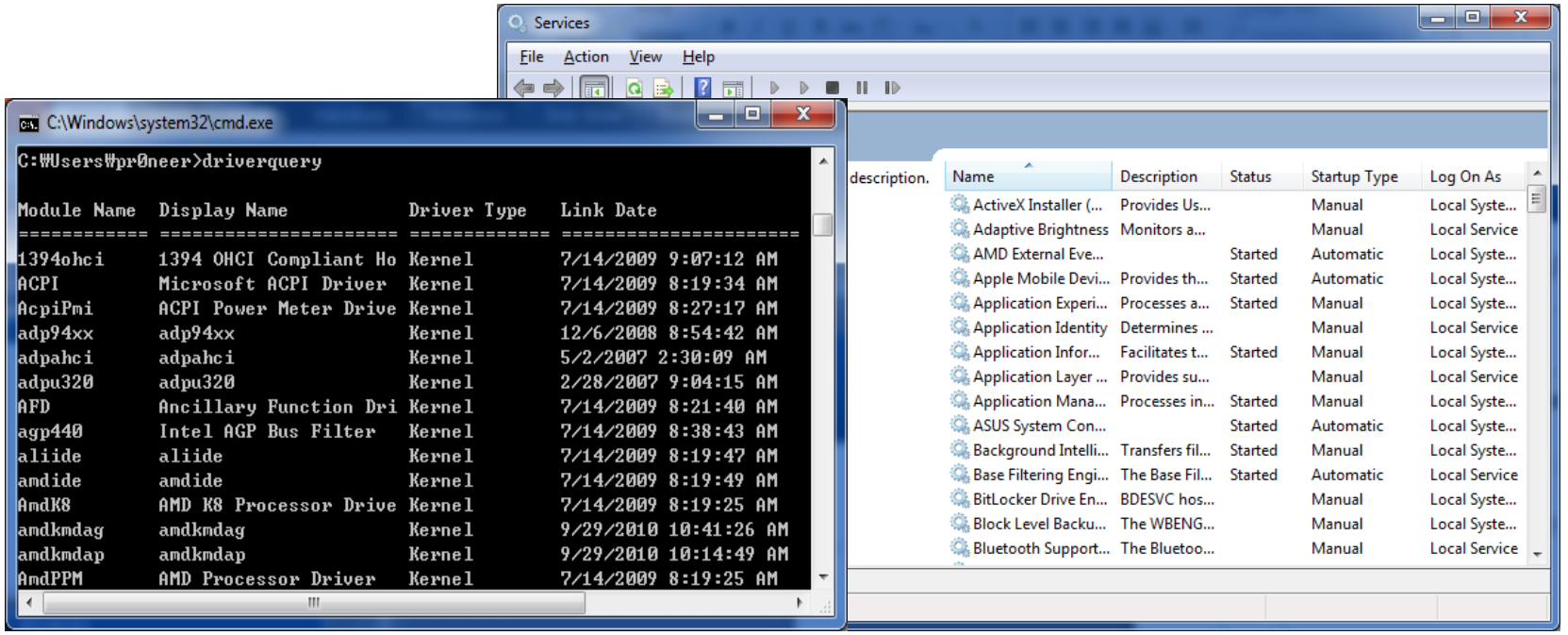
공유 목록 (2/2)

- **공유 폴더 목록**
  - **HKLM₩SYSTEM₩ContolSet00X₩Services₩LanmanServer₩Shares**
  - 공유 폴더 경로, 권한, 공유 이름 등의 정보 확인



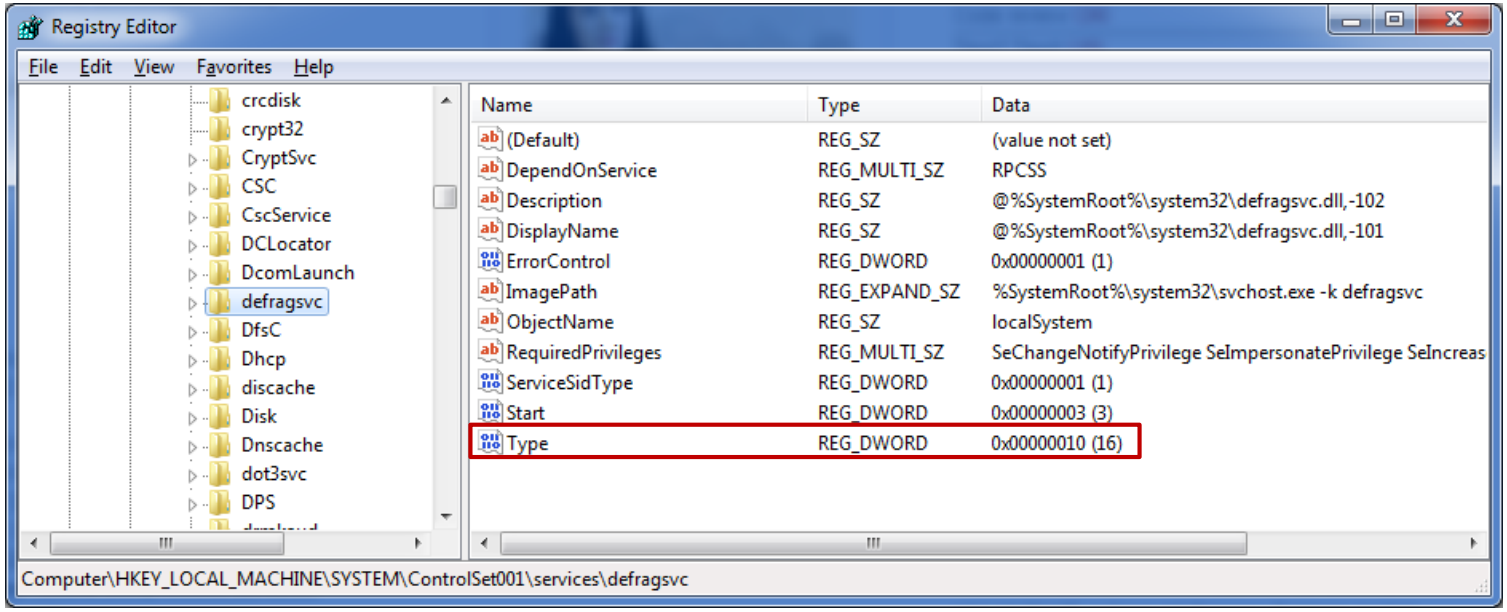
시스템 설정 정보 (1/3)

- **서비스 및 드라이버 목록**
  - **HKLM₩SYSTEM₩ContolSet00X₩Services₩{sub folder}**
  - "제어판 → 관리도구 → 서비스" 또는 "시작 → 실행 → msconfig → 서비스 탭"에서 확인 가능한 서비스 목록
  - "**driverquery**" 명령으로 확인 가능한 드라이버 목록



시스템 설정 정보 (2/3)

- **서비스 및 드라이버 목록**
  - **HKLM₩SYSTEM₩ContolSet00X₩Services₩{sub folder}**
  - 각각의 서비스 및 드라이버를 가리키는 세부키 값 중 "Type" 값에 따라 특성 정의
  - 자세한 세부키 값 의미 : http://support.microsoft.com/kb/103000



시스템 설정 정보 (3/3)

- **서비스 및 드라이버 목록**
  - **HKLM₩SYSTEM₩ContolSet00X₩Services₩{sub folder}**
  - Type 값의 의미
    - 0x1 – 커널 장치 드라이버
    - 0x2 – 파일시스템 드라이버 (커널 장치 드라이버에도 해당)
    - 0x04 – 어댑터에 대한 인수 집합
    - 0x10 – 서비스 컨트롤러에 의해 시작되는 Win32 프로그램 (프로세스로 동작)
    - 0x20 – 다른 Win32 서비스 프로세스와 공유 가능한 Win32 서비스

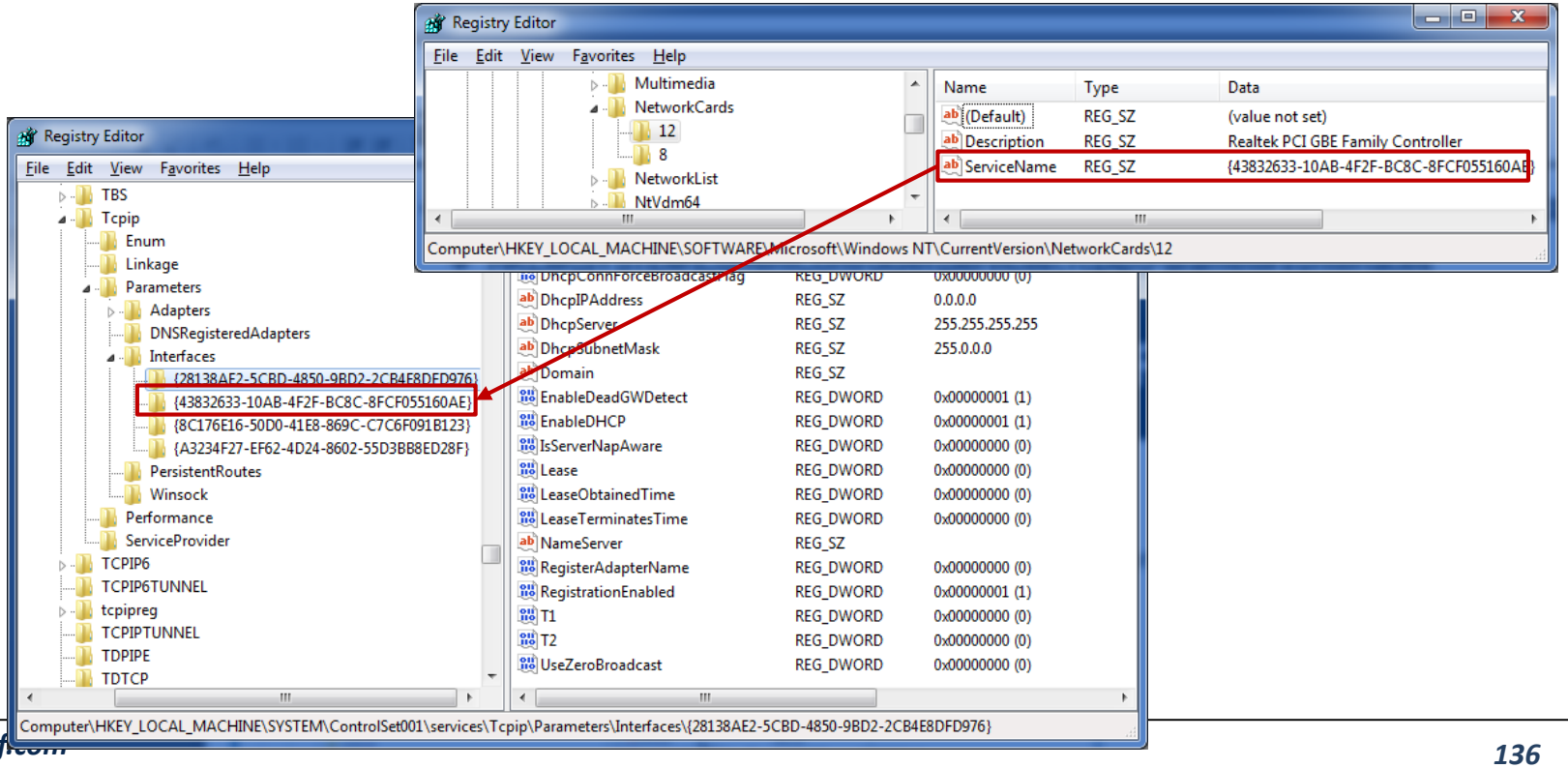
네트워크 정보 (1/8)

- **네트워크 인터페이스 정보**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkCards**
  - **HKLM₩SYSTEM₩ControlSet00X₩Services₩Tcpip₩Parameter₩Interfaces₩{GUID}**
  - **"ipconfig /all"** 명령으로 확인 가능한 정보 (추가적인 정보 포함)

Local Area Connection 2	
장치명	Realtek PCI GBE Family Controller
IP 주소	192.168.200.101
서브넷 마스크	255.255.255.0
네임 서버	203.246.162.253 164.124.101.2
도메인	
기본 게이트웨이	192.168.200.254
허가된 TCP 포트	
허가된 UDP 포트	
IP의 ContextList 번호	
IP 자동할당을 위한 DHCP 사용 여부	사용
DHCP 서버 주소	192.168.200.254
IP 할당 유효 시간 (만료시각 - 할당시각)	3600 sec
IP 할당 시각	1296455876 sec
IP 만료 시각	1296459476 sec
DHCP의 첫 IP 주소 할당 시각	1296457676 sec
IP 주소 갱신 실패 시각	1296459026 sec
IP 주소 (IP가 자동으로 할당된 경우)	
서브넷 마스크 (IP가 자동으로 할당된 경우)	
브로드캐스트	0.0.0.0

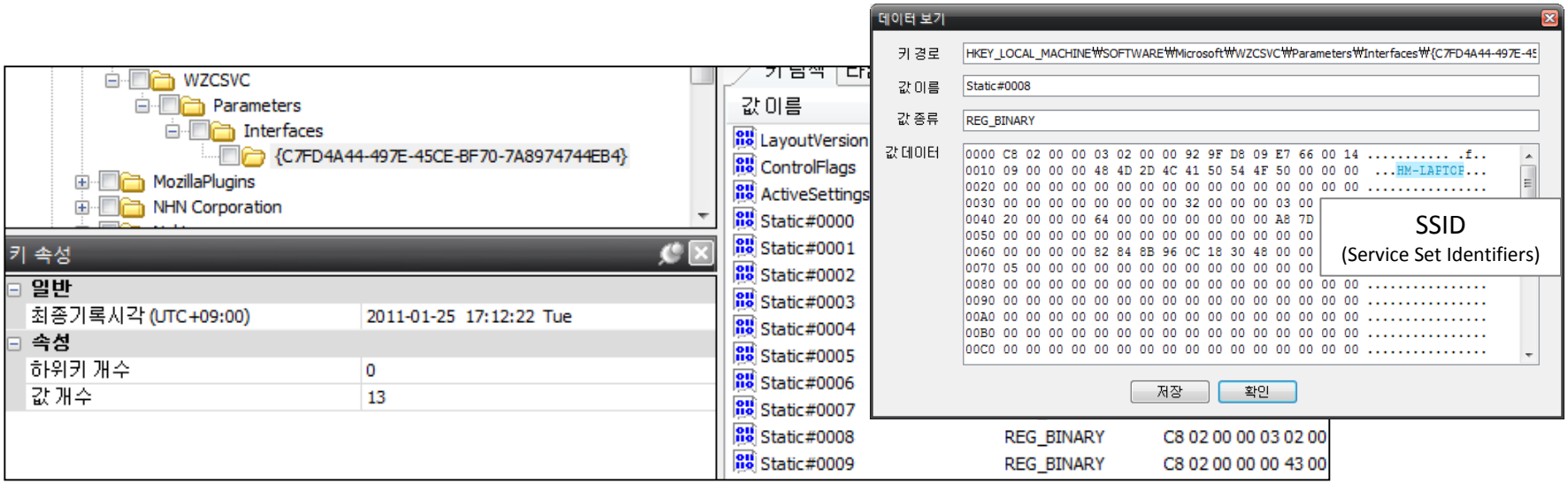
네트워크 정보 (2/8)

- **네트워크 인터페이스 정보**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkCards**
  - **HKLM₩SYSTEM₩ControlSet00X₩Services₩Tcpip₩Parameter₩Interfaces₩{GUID}**
  - **NetworkCards** 하위키를 통해 인터페이스 **ServiceName(GUID)** 확인 후 **Interfaces** 하위키의 값 확인



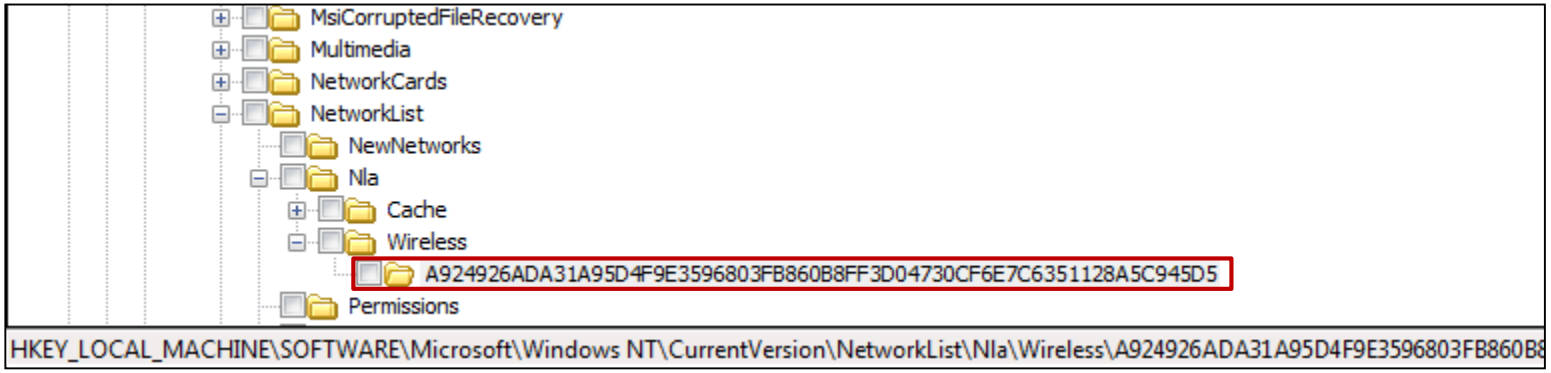
네트워크 정보 (3/8)

- **무선랜 접속 정보**
  - **2000/XP – HKLM₩SOFTWARE₩Microsoft₩WZCSVC₩Parameters₩Interface₩{GUID}**
  - 802.11 무선 랜에서 사용하는 AP(Access Point)
  - 하위키 중 **Static#00x** 데이터가 Wireless SSID (Service Set Identifier)
  - SSID와 함께 무선 인터페이스에 할당된 IP 정보를 함께 활용



네트워크 정보 (4/8)

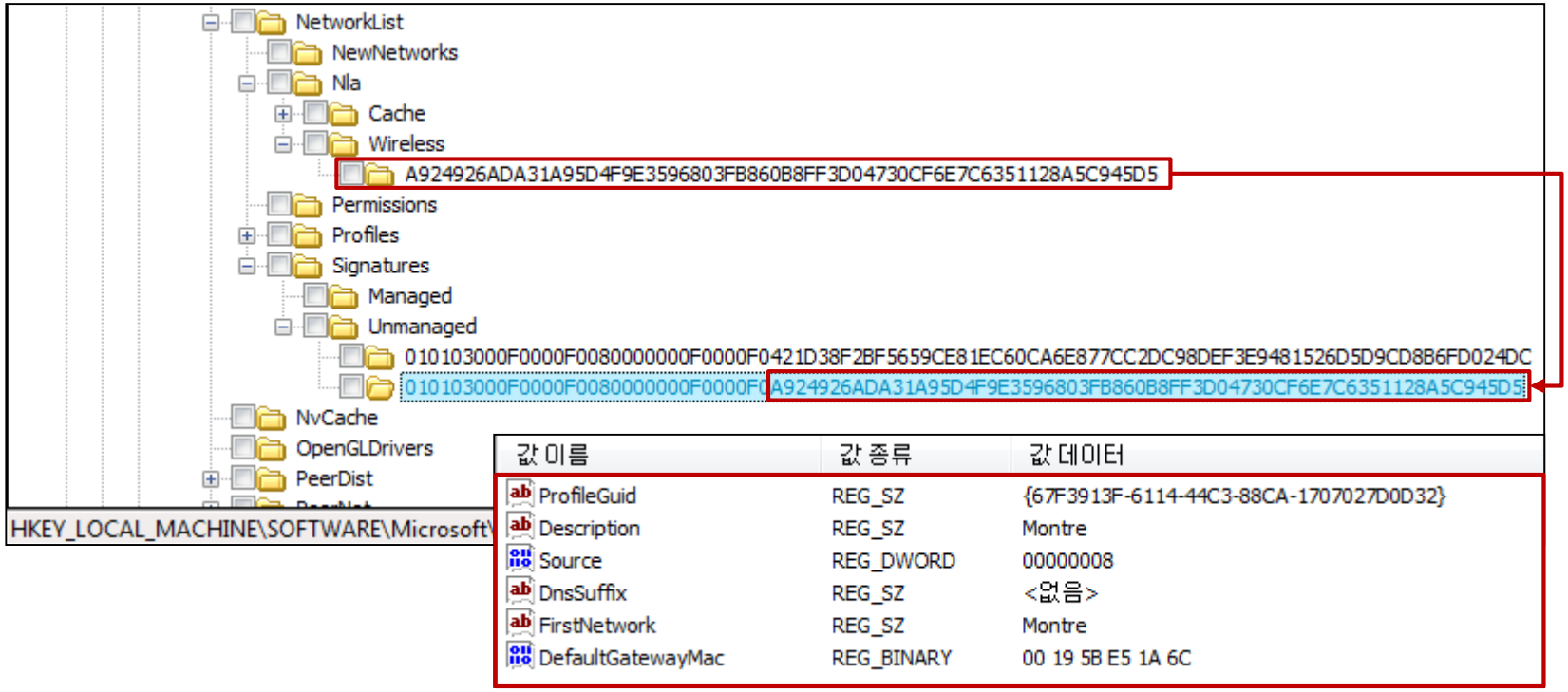
- **무선랜 접속 정보**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Nla₩Wireless**
  - 하위키에서 무선 네트워크 식별자(Wireless Identifier) 확인 가능
  - Signature₩Unmanaged 하위키와 연결하여 다양한 무선랜 접속 정보 확인 가능



네트워크 정보 (5/8)

- **무선랜 접속 정보**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Nla₩Wireless**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Signature₩**

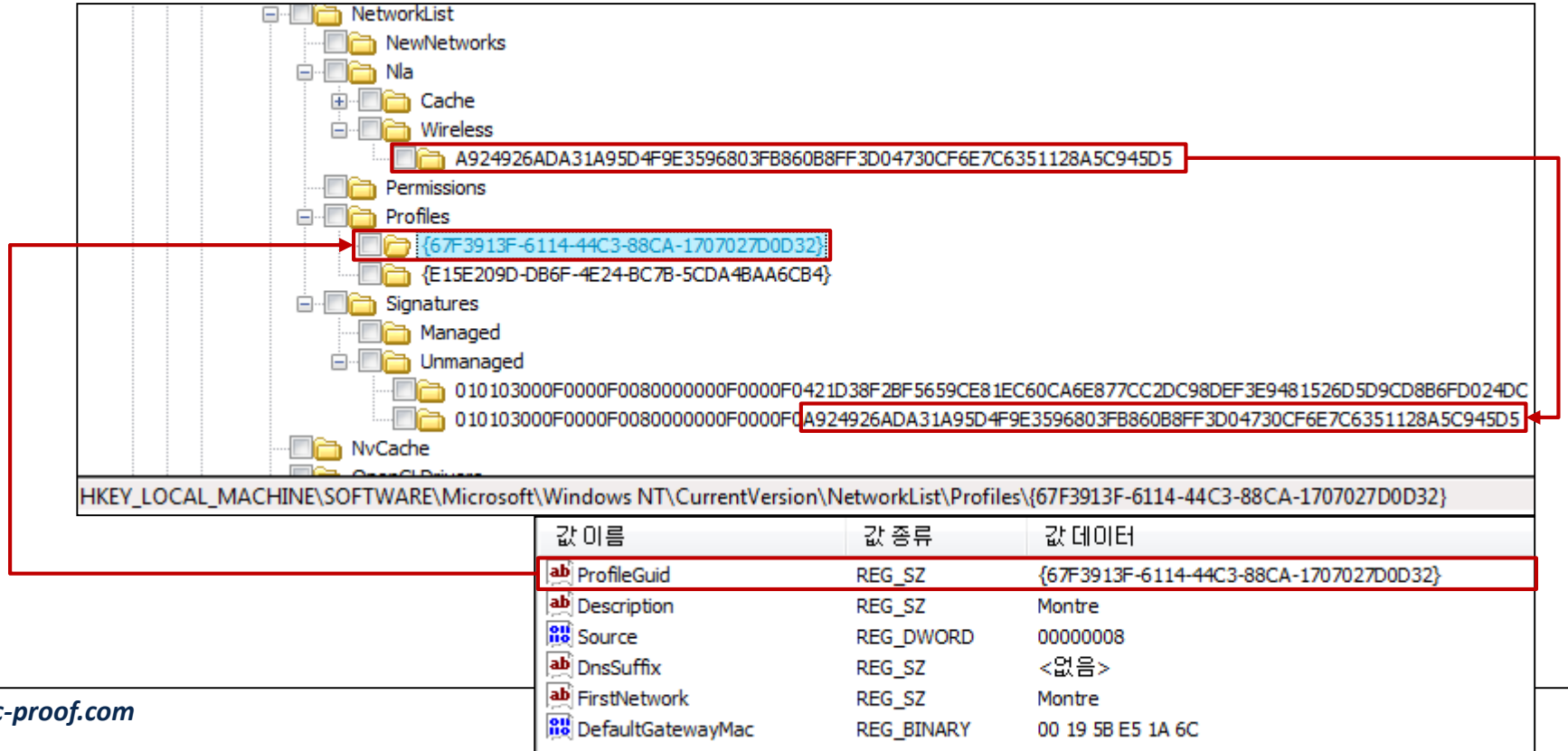
Unmanaged



레지스트리 분석

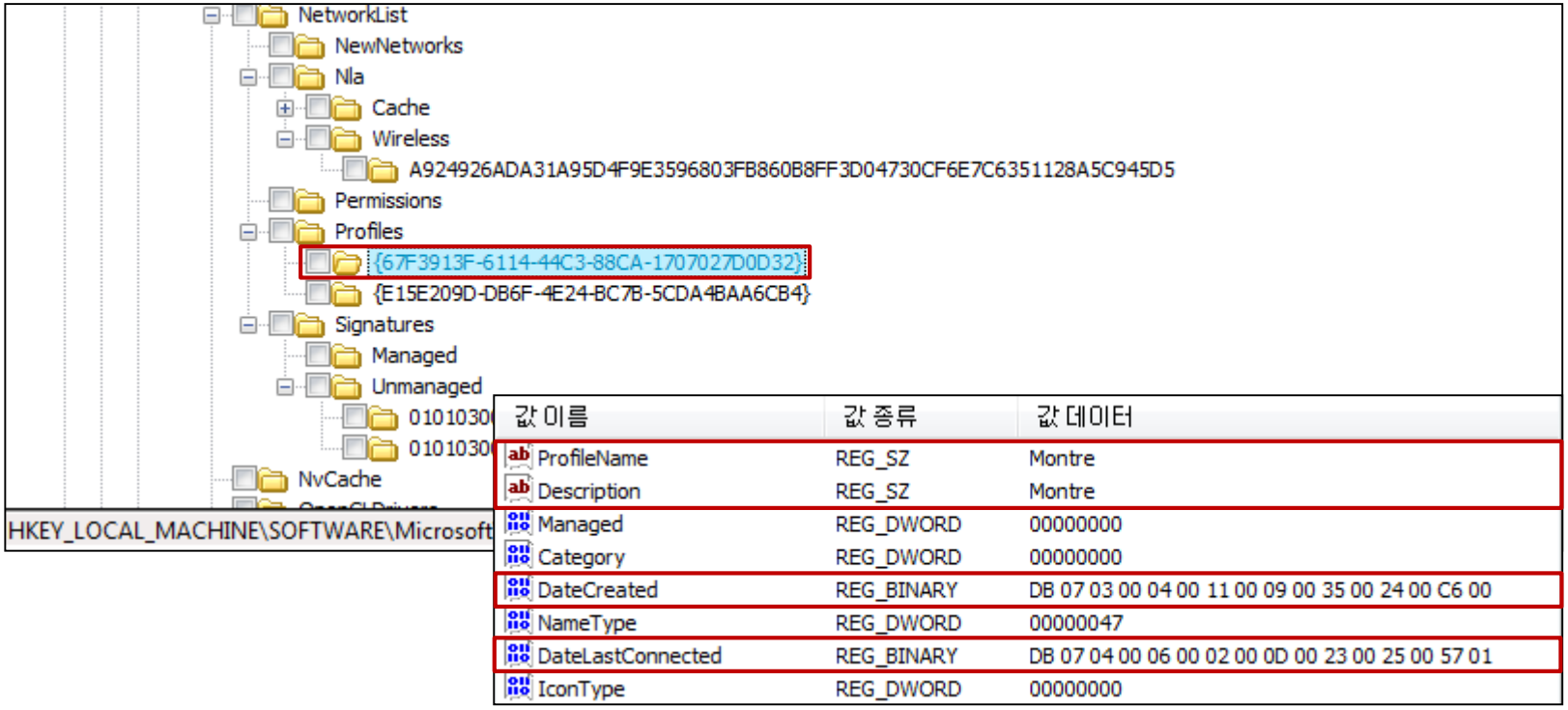
네트워크 정보 (6/8)

- **무선랜 접속 정보**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Signature₩ Unmanaged**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Profile₩{GUID}**



네트워크 정보 (7/8)

- **무선랜 접속 정보**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Signature₩Unmanaged**
  - **Vista/7 – HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩NetworkList₩Profile₩{GUID}**



네트워크 정보 (8/8)

- **무선랜 접속 정보**
  - 무선 AP 마지막 접속 시간

값 이름	값 종류	값 데이터
ProfileName	REG_SZ	Montre
Description	REG_SZ	Montre
Managed	REG_DWORD	00000000
Category	REG_DWORD	00000000
DateCreated	REG_BINARY	DB 07 03 00 04 00 11 00 09 00 35 00 24 00 C6 00
NameType	REG_DWORD	00000047
DateLastConnected	REG_BINARY	DB 07 04 00 06 00 02 00 0D 00 23 00 25 00 57 01
IconType	REG_DWORD	00000000

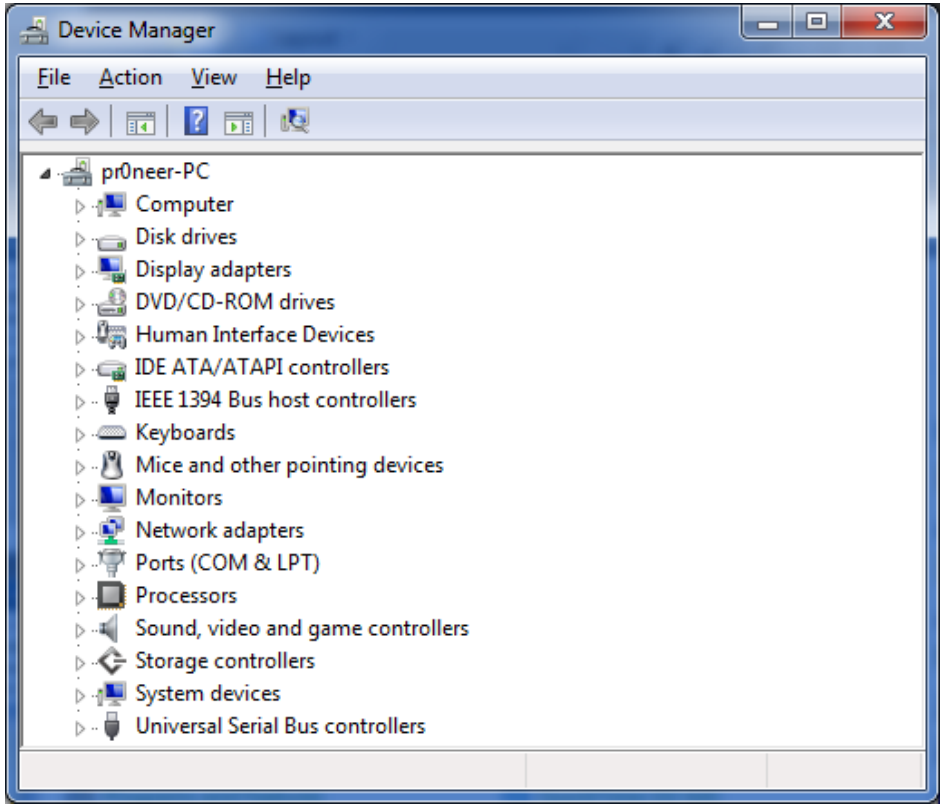
DB 07	04 00	06 00	02 00	0D 00	23 00	25 00	57 01
07 DB	00 04	00 06	00 02	00 0D	00 23	00 25	01 57
year	**month**	**weekday**	**day**	**hour**	**min.**	**sec.**	**ms.**
2011	**04**	**Sat**	**02**	**13**	**23**	**25**	**343**

엔디안 변환

  - **2011년 04월 02일 토요일 13:23:25 343ms**

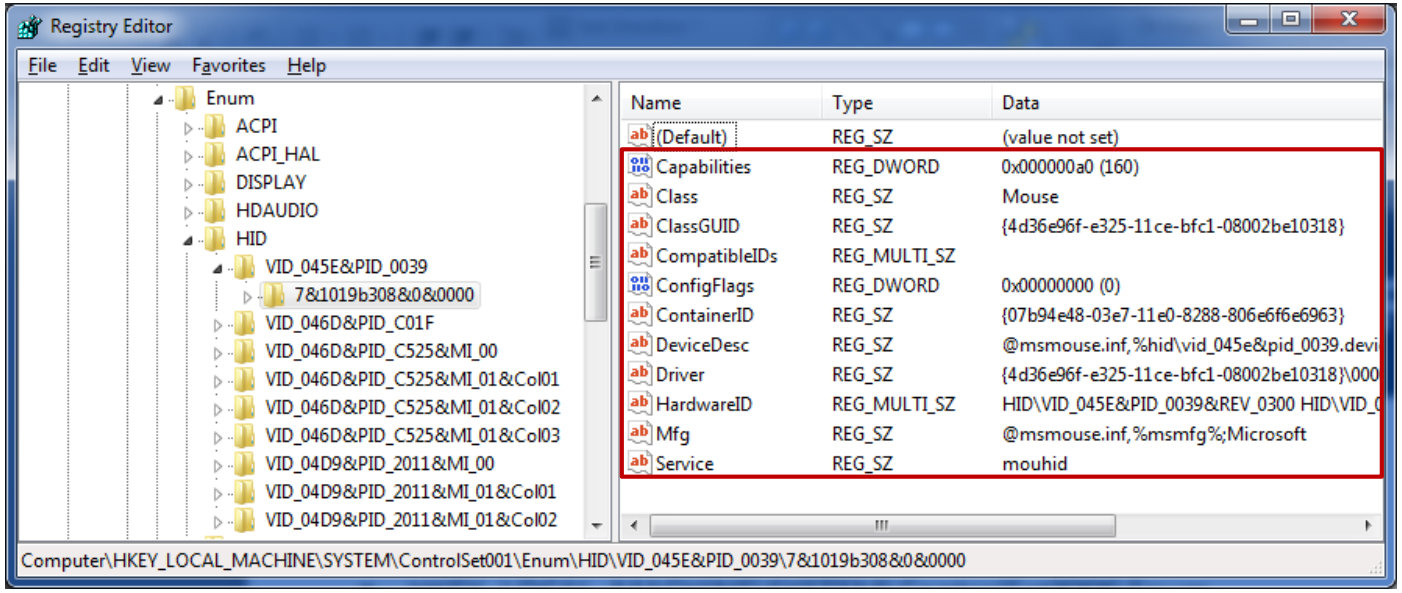
하드웨어 정보 (1/2)

- 하드웨어 목록
  - HKLM₩SYSTEM₩ControlSet00X₩Control₩Class
  - HKLM₩SYSTEM₩ControlSet00X₩Enum



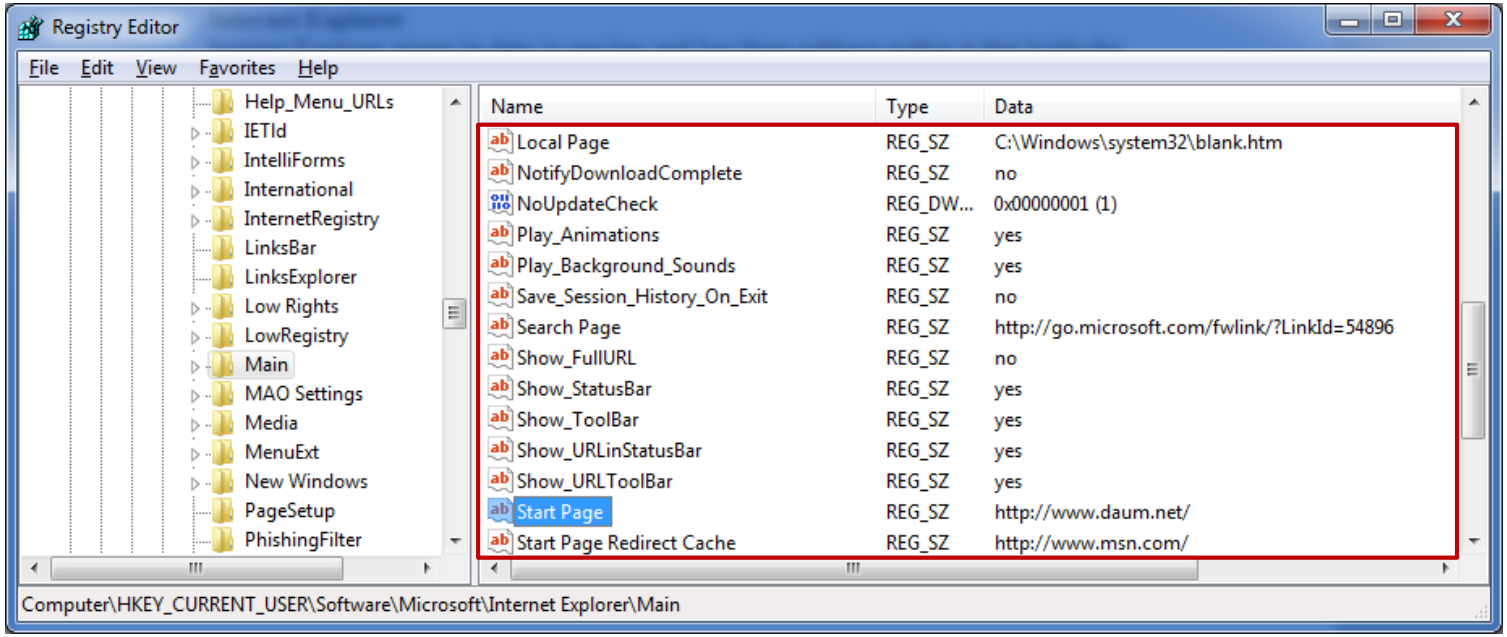
하드웨어 정보 (2/2)

- 하드웨어 목록
  - HKLM₩SYSTEM₩ControlSet00X₩Control₩Class
  - HKLM₩SYSTEM₩ControlSet00X₩Enum



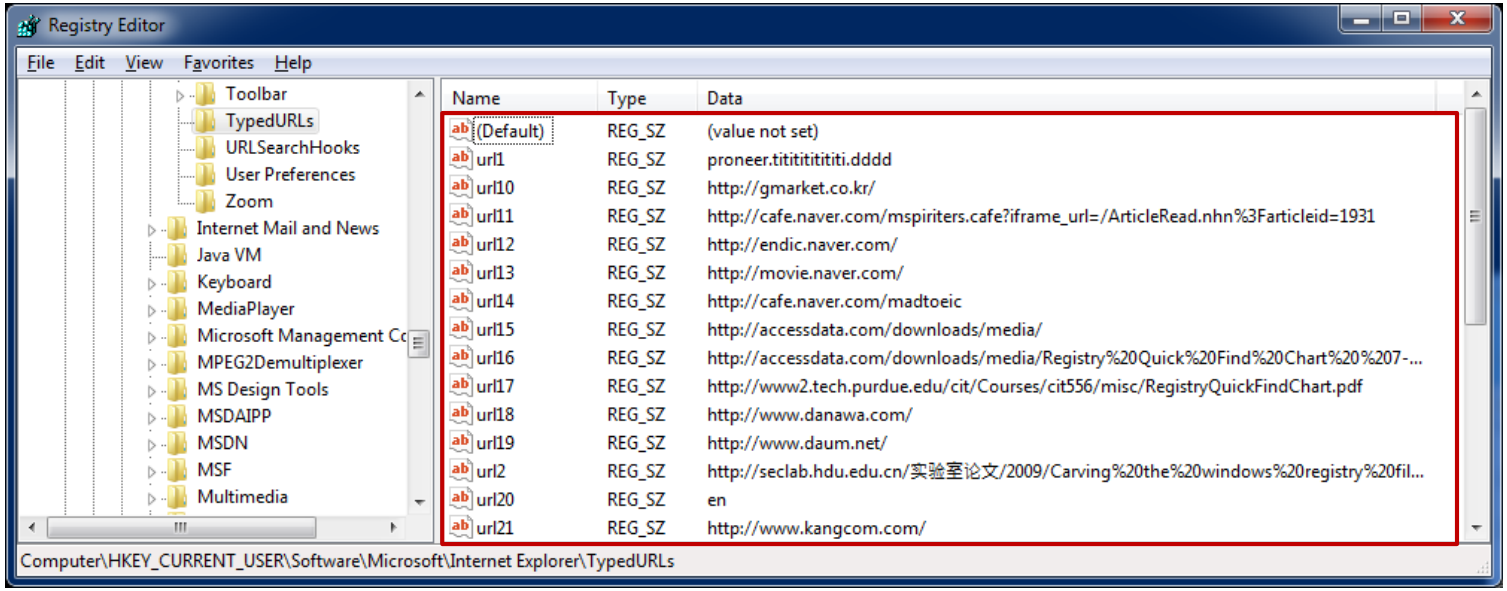
인터넷 사용 흔적 (1/11)

- **Internet Explorer 설정 정보**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer₩Main**
  - 시작 페이지, 동작 시간 정보, 검색 페이지 정보 등 다양한 설정 정보 저장



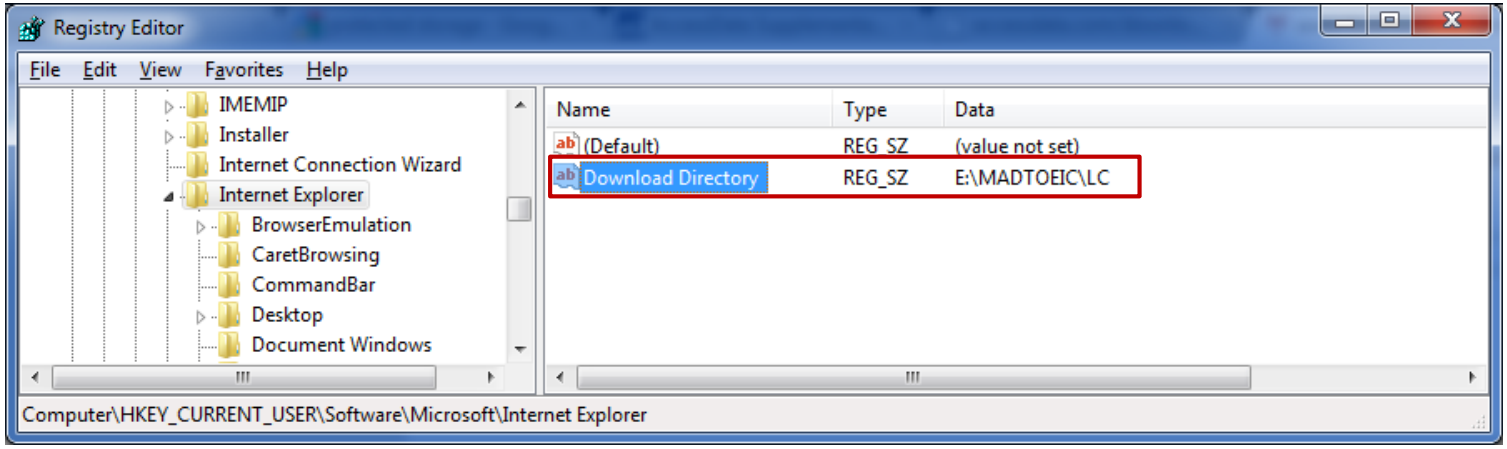
인터넷 사용 흔적 (2/11)

- **Internet Explorer 타이핑한 URL 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer₩TypedURLs**
  - 사용자가 익스플로러 주소창에 직접 타이핑하여 이동된 페이지 목록
  - "인터넷 옵션 ➔ 히스토리 항목 삭제"를 할 경우 해당 내용도 삭제됨



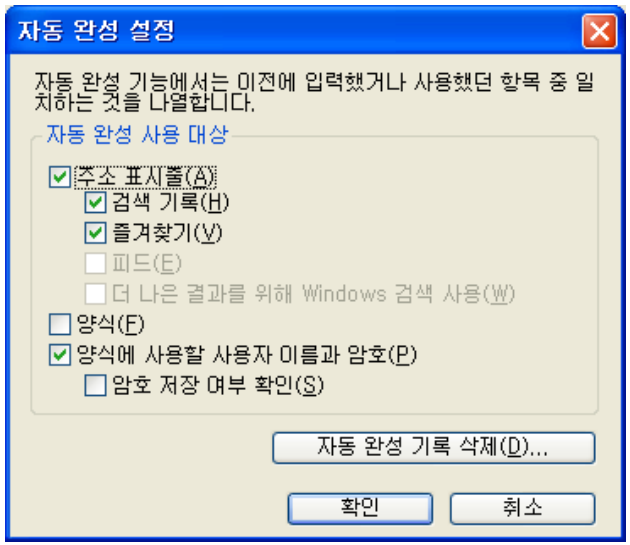
인터넷 사용 흔적 (3/11)

- **Internet Explorer 다운로드 경로**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer**
  - Download Directory – 익스플로러를 통해 파일을 다운로드 했을 경우 최종 다운로드 경로



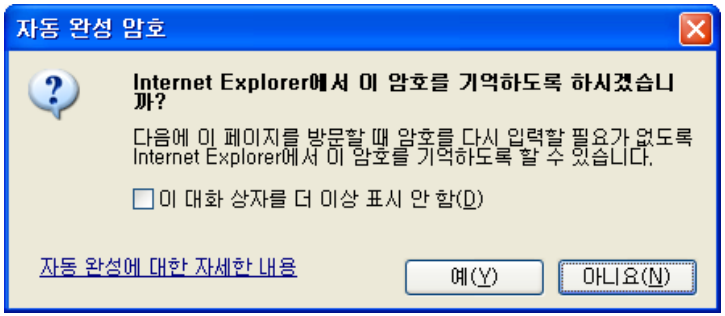
인터넷 사용 흔적 (4/11)

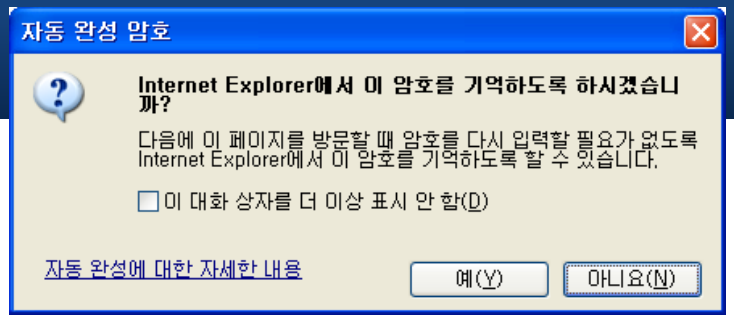
- **Internet Explorer 자동 완성**
  - 인터넷 익스플로러에는 작성한 글이나 패스워드를 기억해주는 자동완성 기능이 존재
  - 인터넷 옵션 → 내용 → 자동 완성



인터넷 사용 흔적 (5/11)

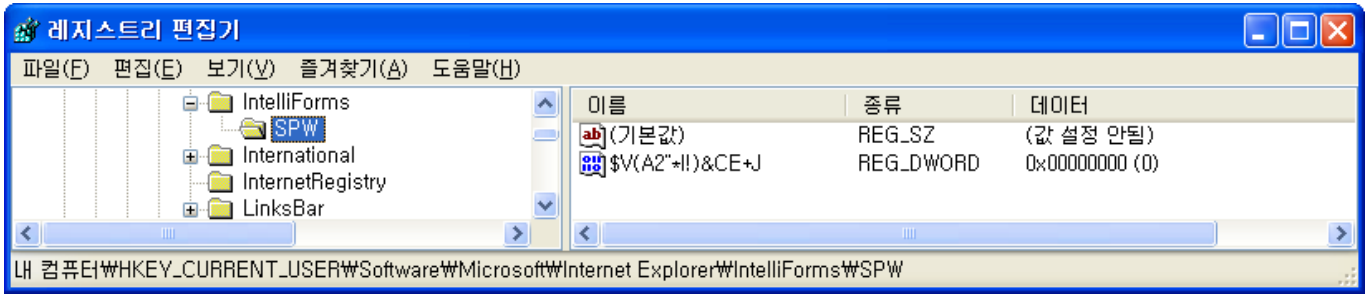
- **Internet Explorer 자동 완성**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer₩Main**
  - **FormSuggest PW Ask** – 자동 완성 대화상자를 표시할 것인지 아닌 여부
    - "yes" – 대화상자 표시 (사용자가 체크 박스에 체크하지 않을 경우)
    - "no" – 대화상자 표시하지 않음 (사용자가 표시 안함 체크박스에 체크한 경우)





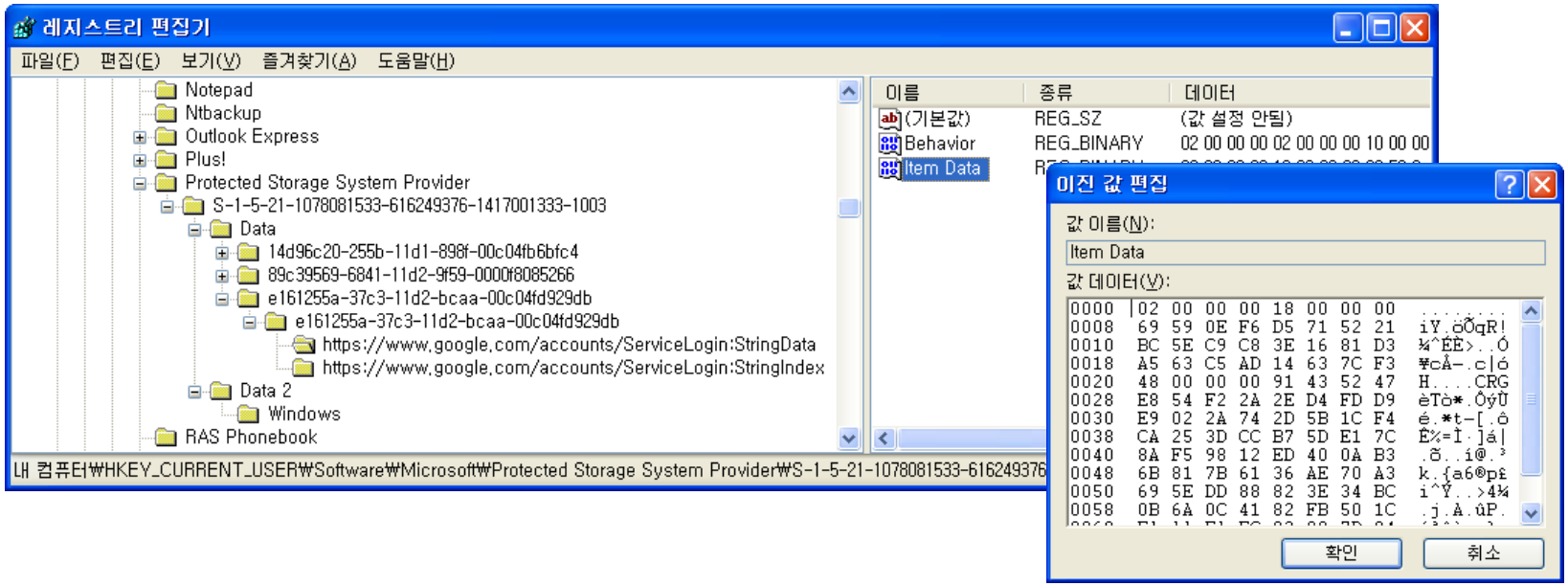
인터넷 사용 흔적 (6/11)

- **Internet Explorer (4.x – 6.x) 자동 완성**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer₩IntelliForms₩SPW**
  - **SPW(SavePassWords)** – 사이트의 자동완성 정보가 저장되어 있는지 여부
    - 대화상자에서 "예" 또는 "아니요" 어느 것을 선택하더라도 해당 값 저장
    - 방문한 사이트 URL이 해쉬되어 저장
  - **"예(Yes)" 를 선택**
    - HKEY₩{USER}₩SOFTWARE₩Microsoft₩Protected Storage System Provider – 아이디/패스워드 저장
  - **"아니요(No)"를 선택**
    - HKEY₩{USER}₩SOFTWARE₩Microsoft₩Protected Storage System Provider – 아이디 저장



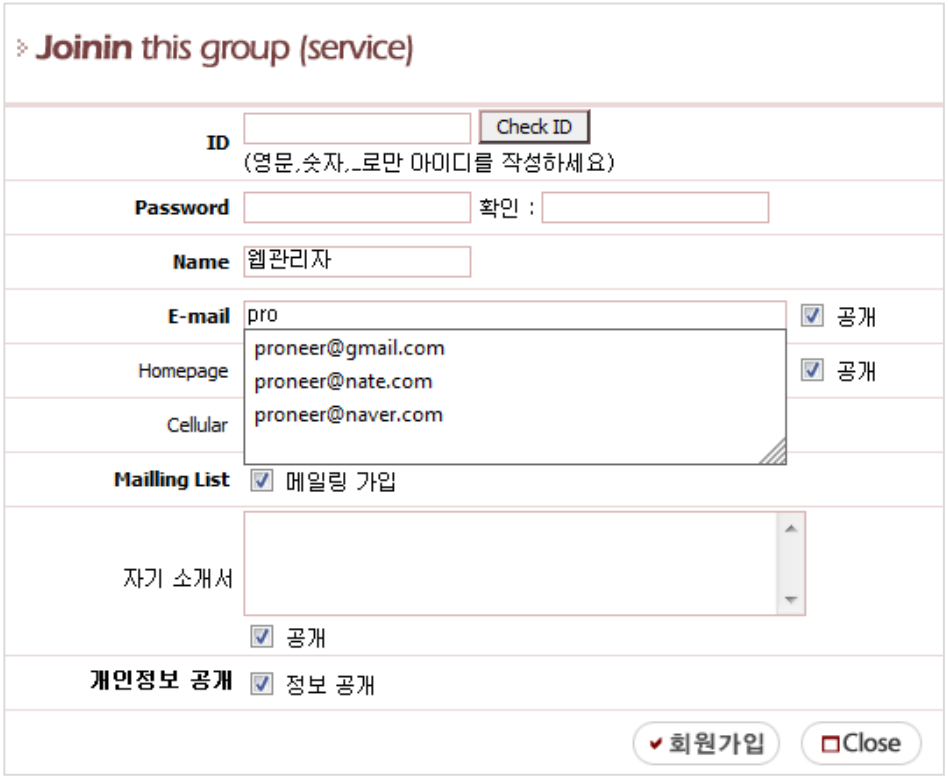
인터넷 사용 흔적 (7/11)

- **Internet Explorer (4.x – 6.x) 자동 완성**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Protected Storage System Provider₩{SID}₩{subkey}**
  - 저장한 아이디 패스워드는 암호화(Triple DES) 되어 저장
  - ₩Data2 하위키에 키와 salt가 저장
  - 다양한 복구 도구로 복호화 가능 (http://www.nirsoft.net/utils/internet_explorer_password.html)



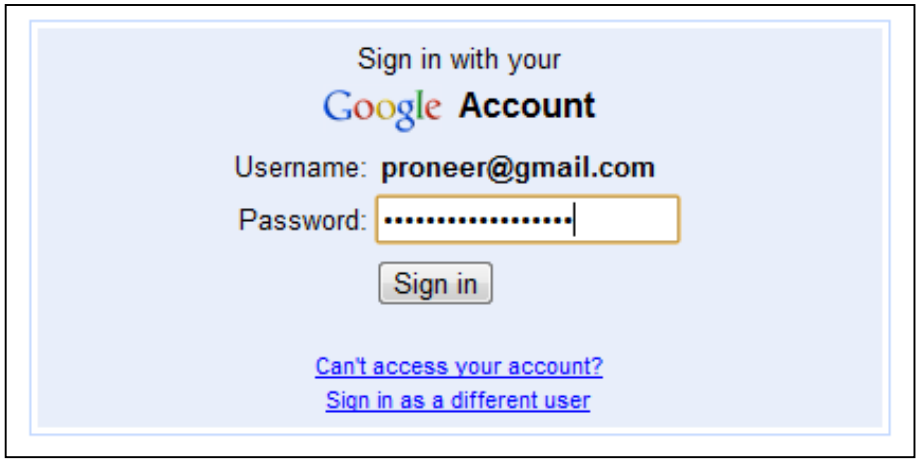
인터넷 사용 흔적 (8/11)

- **Internet Explorer (7.x – 8.x) 자동 완성**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer₩IntelliForms₩Storage1**
  - 사이트 URL을 키로 사용하여 폼(Form) 데이터를 암호화



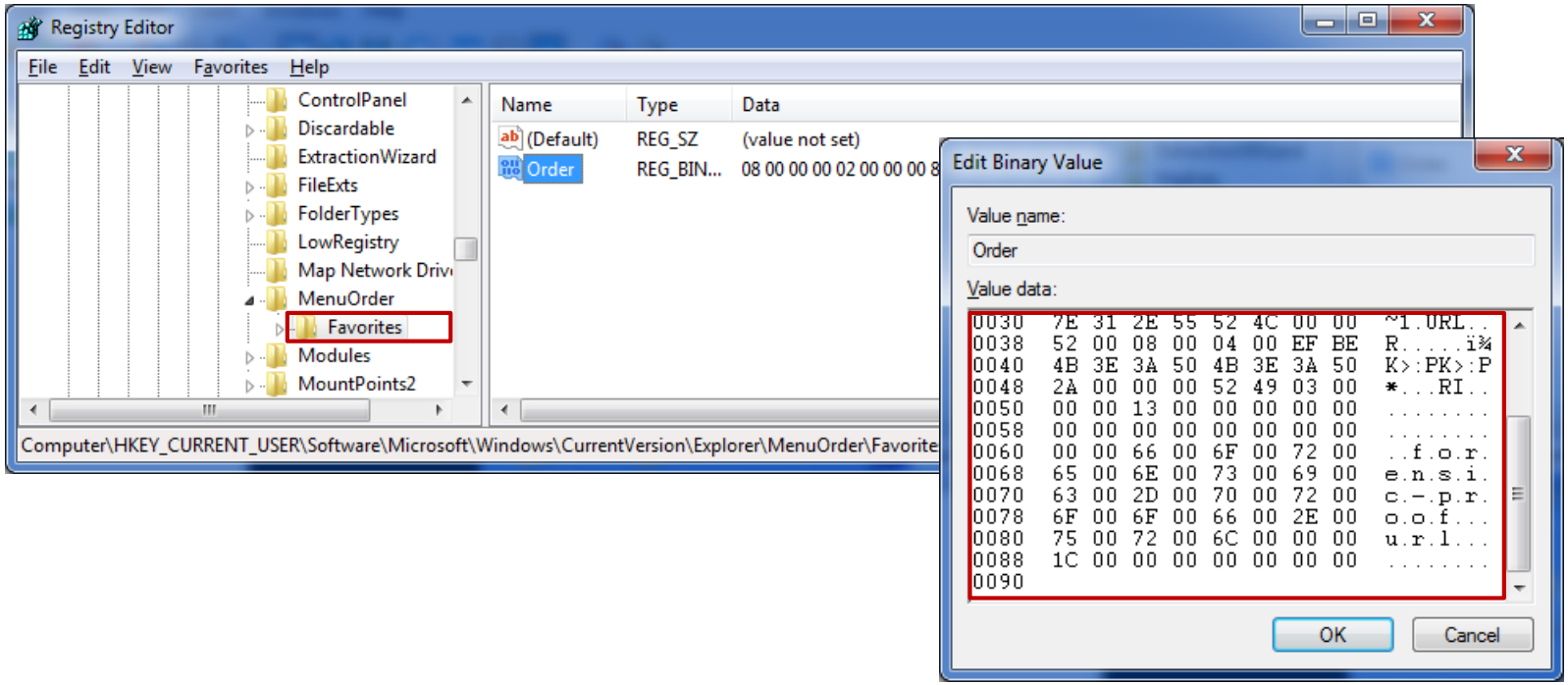
인터넷 사용 흔적 (9/11)

- **Internet Explorer (7.x – 8.x) 자동 완성**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Internet Explorer₩IntelliForms₩Storage2**
  - 사이트 URL을 키로 사용하여 아이디/패스워드를 암호화



인터넷 사용 흔적 (10/11)

- **Internet Explorer 즐겨찾기(Favorite) 목록**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩MenuOrder₩Favorites**
  - **Order** – 즐겨찾기 목록 저장
  - **하위키** – 즐겨찾기 폴더 이름

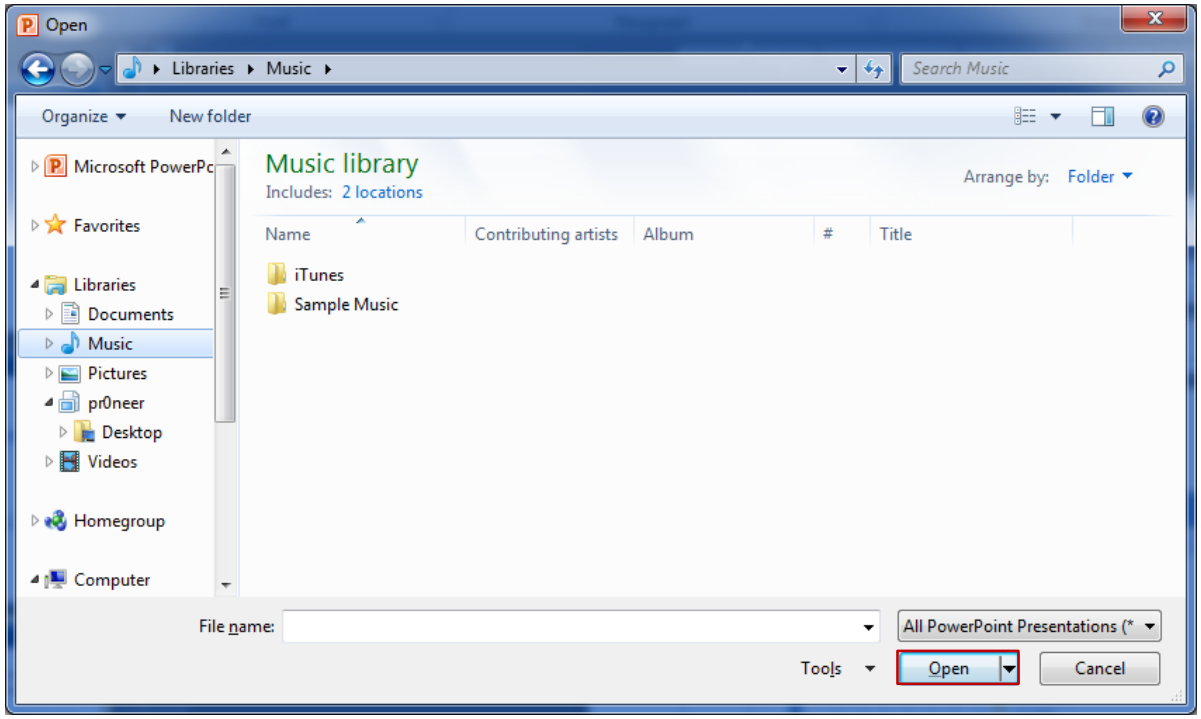


인터넷 사용 흔적 (11/11)

- **추가적인 분석**
  - 앞서 살펴본 내용 이외에도 다양한 인터넷 사용 흔적 존재
  - FireFox, Chrome, Safari, Opera 등의 브라우저에 대한 흔적 분석
  - 각 브라우저별 패스워드 저장 경로
    - http://hack-o-crack.blogspot.com/2009/10/applications-saved-password-location-in.html

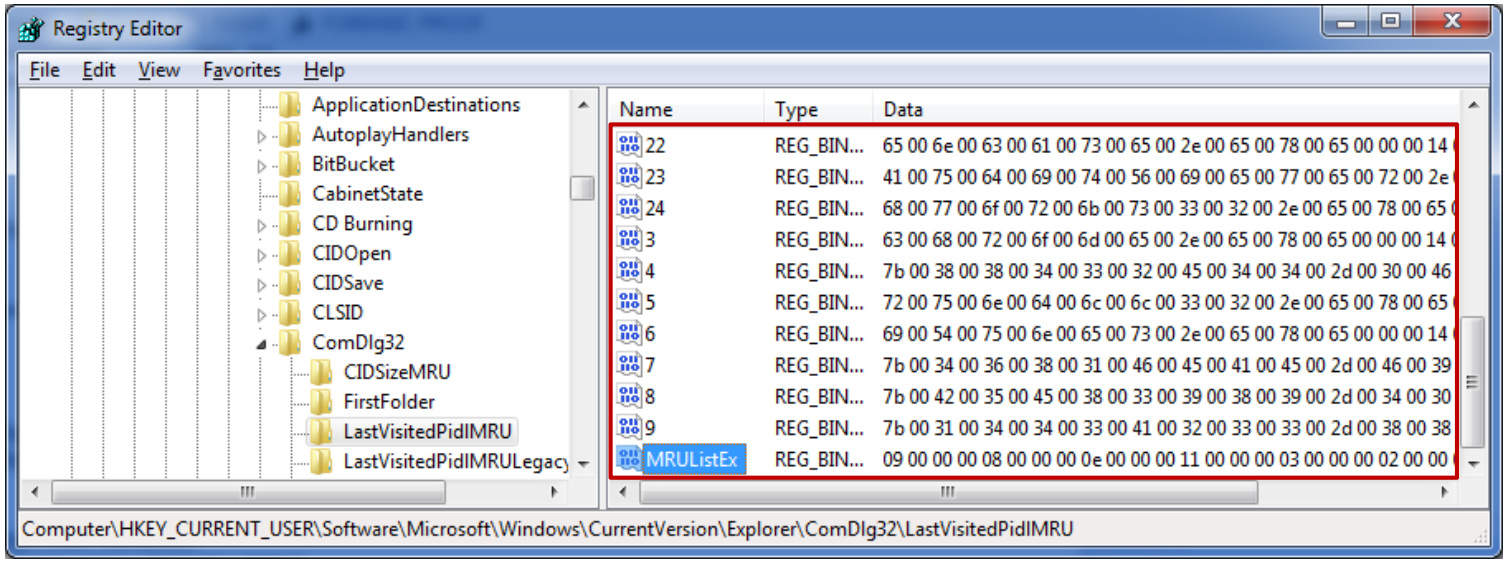
대화상자(Dialog) 사용 흔적 (1/5)

- **최근에 접근한 폴더 목록**
  - **2000/XP –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedMRU
  - **Vista/7 –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedPidMRU
  - 대화상자를 통해 "**Open**" 한 폴더 목록



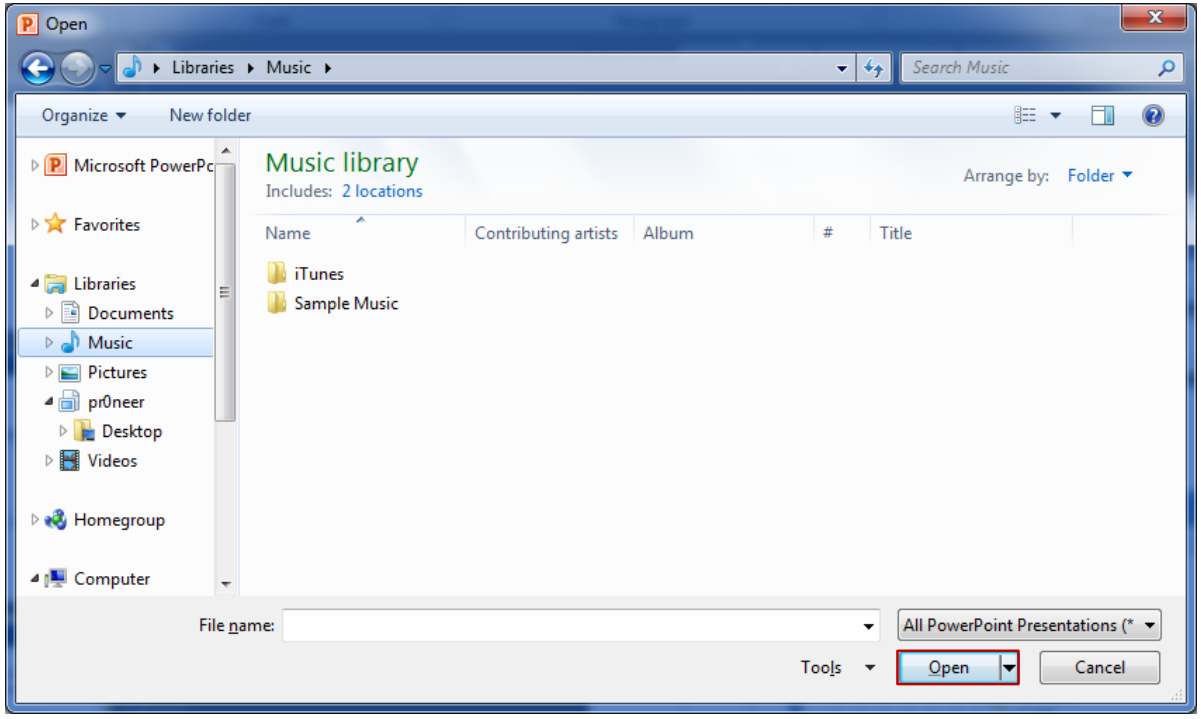
대화상자(Dialog) 사용 흔적 (2/5)

- **최근에 접근한 폴더 목록**
  - **2000/XP –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedMRU
  - **Vista/7 –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedPidMRU
  - **MRUListEx** 를 통해 최근 접근한 폴더 순서 확인



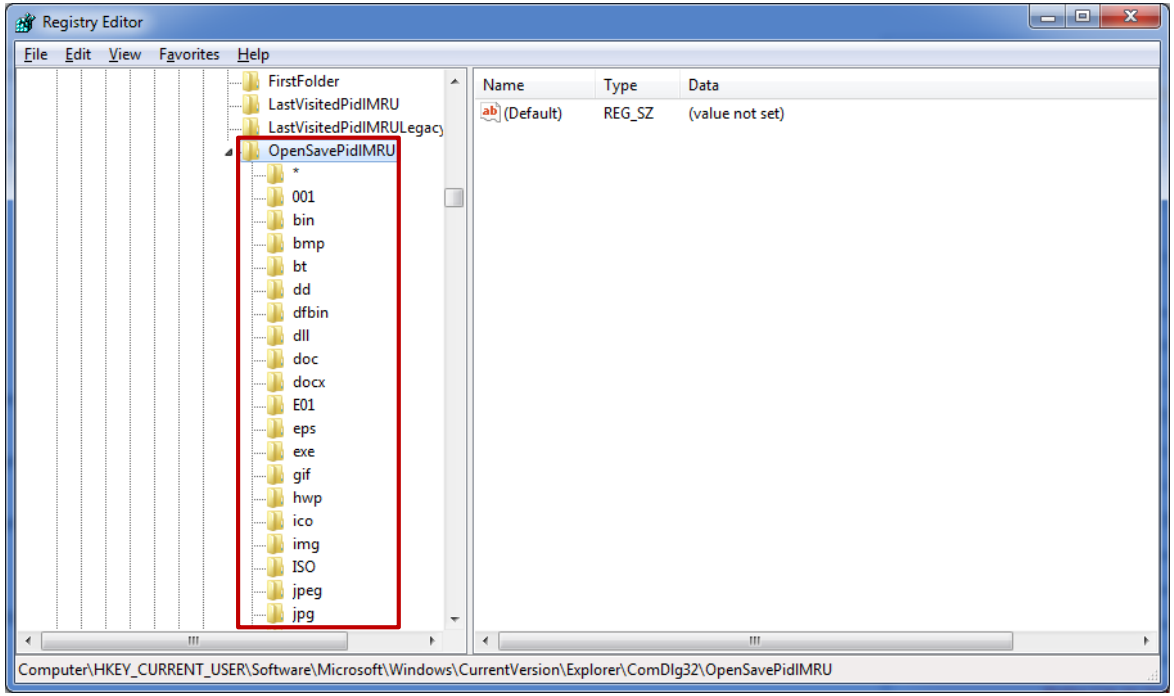
대화상자(Dialog) 사용 흔적 (3/5)

- **최근에 읽거나 저장한 파일 목록**
  - **2000/XP –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩OpenSaveMRU
  - **Vista/7 –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩OpenSavePidMRU
  - 대화상자를 통해 "**Open**"하거나 "**Save As**"한 파일 목록



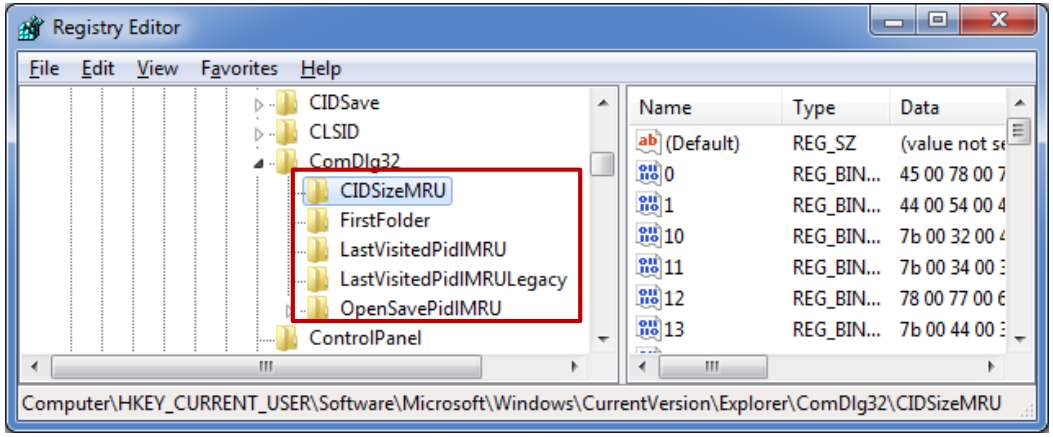
대화상자(Dialog) 사용 흔적 (4/5)

- **최근에 읽거나 저장한 파일 목록**
  - **2000/XP –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩OpenSaveMRU
  - **Vista/7 –** HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩OpenSavePidMRU
  - 확장자 서브키를 통해 최근 읽거나 저장한 파일 목록 관리



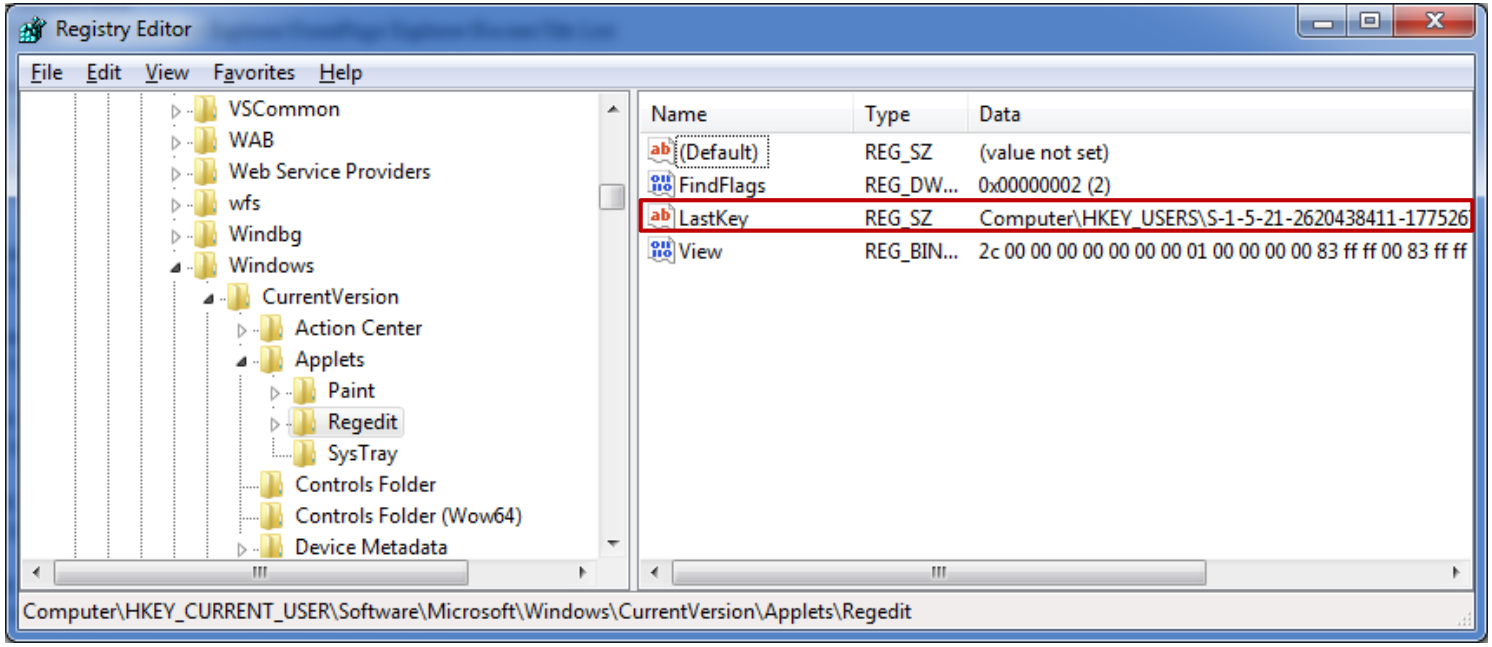
대화상자(Dialog) 사용 흔적 (5/5)

- **Vista/7에서 추가된 대화상자 흔적**
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩LastVisitedPidMRULegacy
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩CIDSizeMRU
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩ComDlg32₩FirstFolder



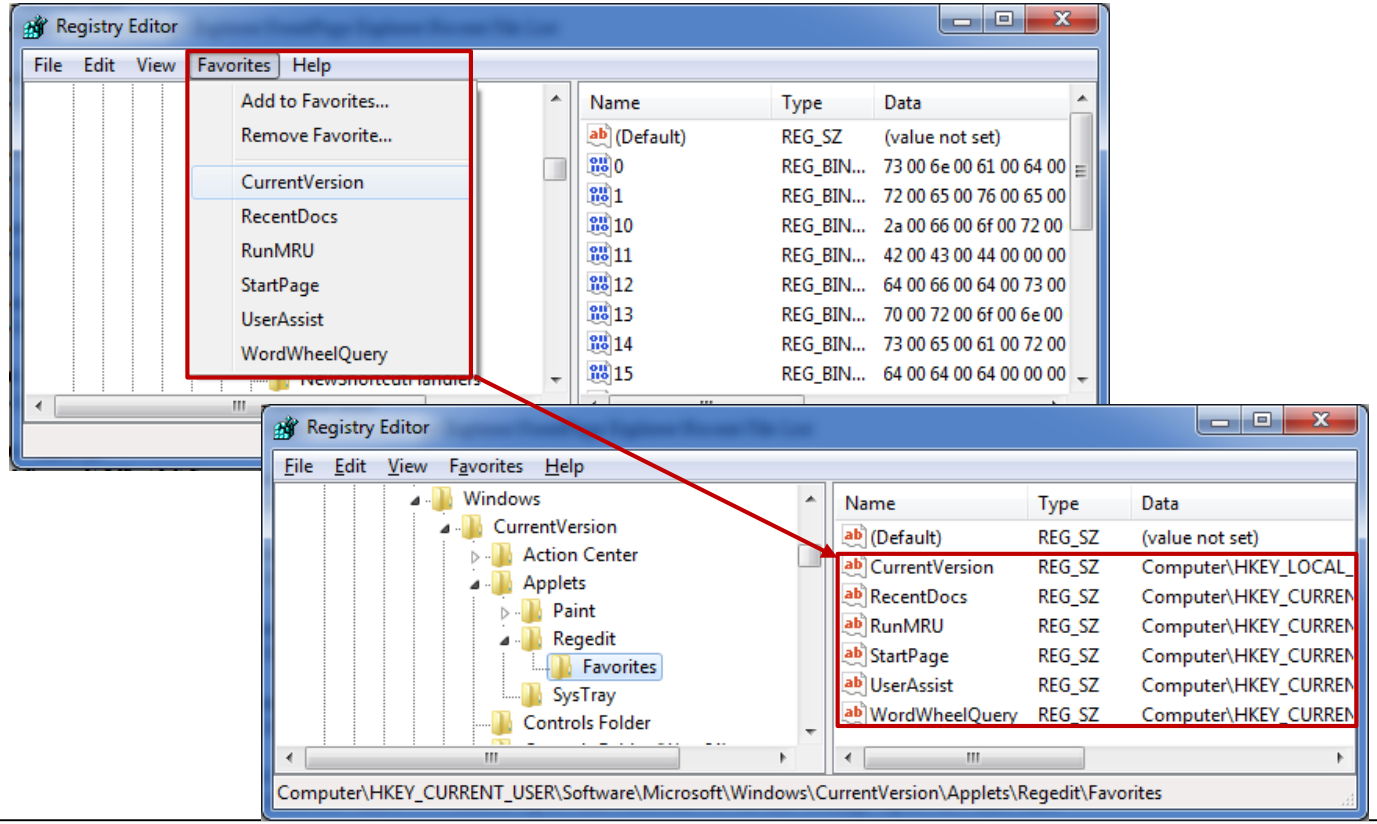
레지스트리 편집기 사용 흔적 (1/1)

- **레지스트리 편집기에서 마지막으로 접근한 키**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Applets₩Regedit**
  - **LastKey** 값에 마지막으로 접근한 키 경로 저장



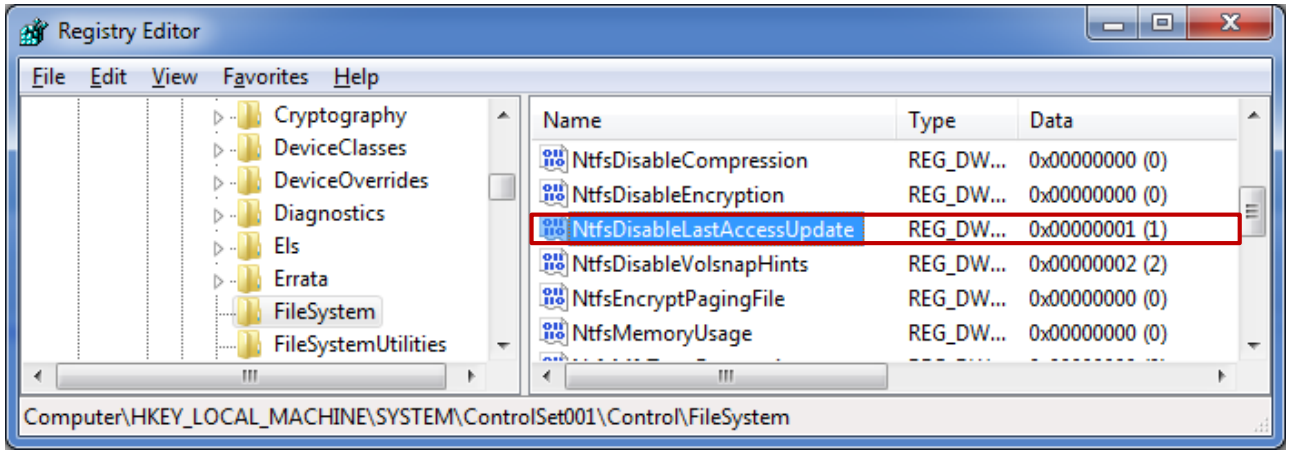
레지스트리 편집기 사용 흔적 (2/2)

- **레지스트리 편집기의 즐겨찾기에 추가한 키**
  - **HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Applets₩Regedit₩Favorites**
  - 즐겨찾기에 추가한 각 키 값과 경로 저장



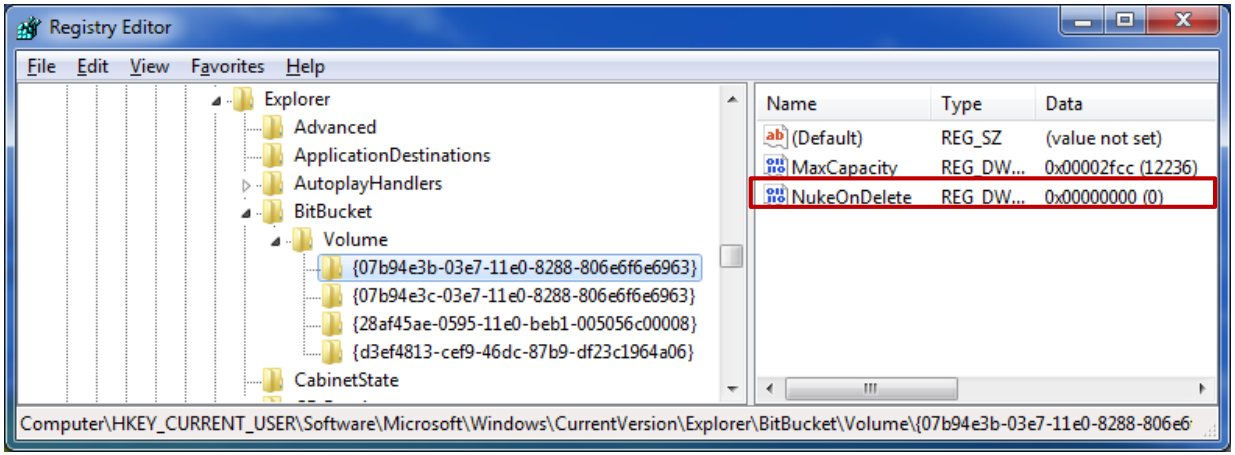
NtfsDisableLastAccessUpdate

- **파일 접근 시간 업데이트 여부 (Vista/7 에서만 사용)**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩FileSystem**
  - **NtfsDisableLastAccessUpdate**
    - 0 : 접근 시간을 업데이트 함
    - 1 : 접근 시간을 업데이트 하지 않음 (Default)
  - 디렉터리 리스팅 시 속도를 빠르게 하기 위한 목적으로 접근 시간을 업데이트 하지 않음



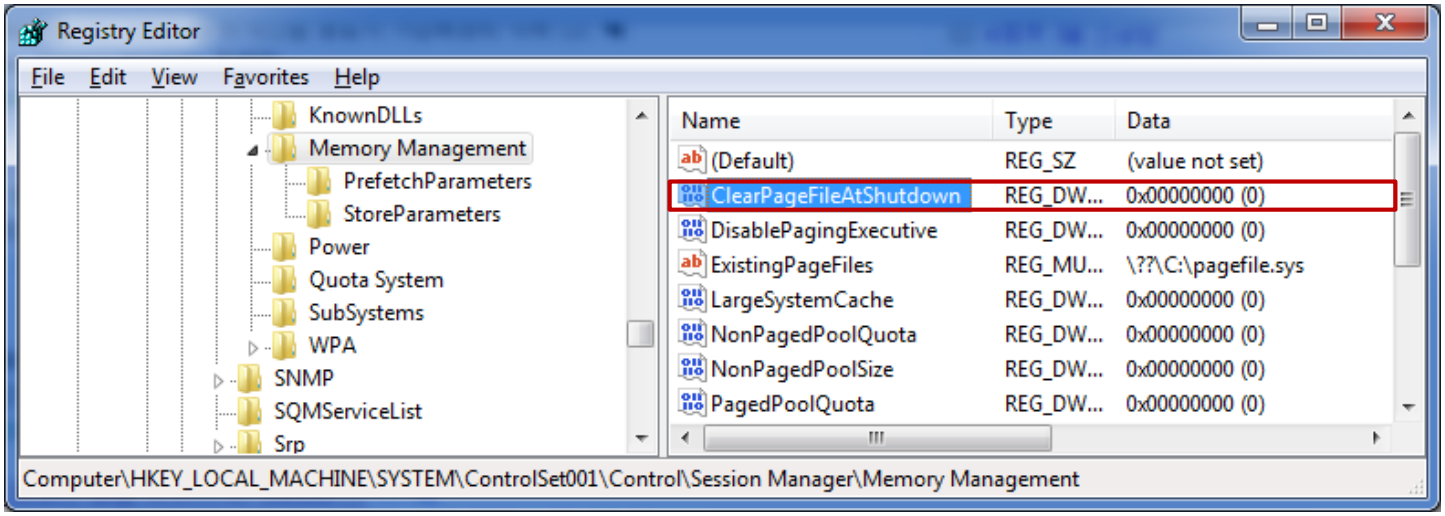
NukeOnDelete

- **휴지통 우회**
  - **2000/XP – HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩BitBucket**
  - **Vista/7 – HKU₩{USER}₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Bitbucket₩Volume₩{GUID}**
  - **NukeOnDelete**
    - 0 : 파일 삭제시 휴지통으로 이동 (Default)
    - 1 : 파일 삭제시 휴지통을 거치지 않고 바로 삭제
  - XP 이하에서는 단일 설정으로 전체 사용자에 적용, Vista 이상부터는 사용자와 볼륨마다 설정 가능



ClearPageFileAtShutdown

- **시스템 종료 시 페이지 파일 삭제**
  - **HKLM₩SYSTEM₩ControlSet00X₩Control₩Session Manager₩Memory Management**
  - **ClearPageFileAtShutdown**
    - 0 : 시스템 종료시 페이지 파일 유지 (Default)
    - 1 : 시스템 종료시 페이지 파일 삭제



추가적인 레지스트리 분석 정보

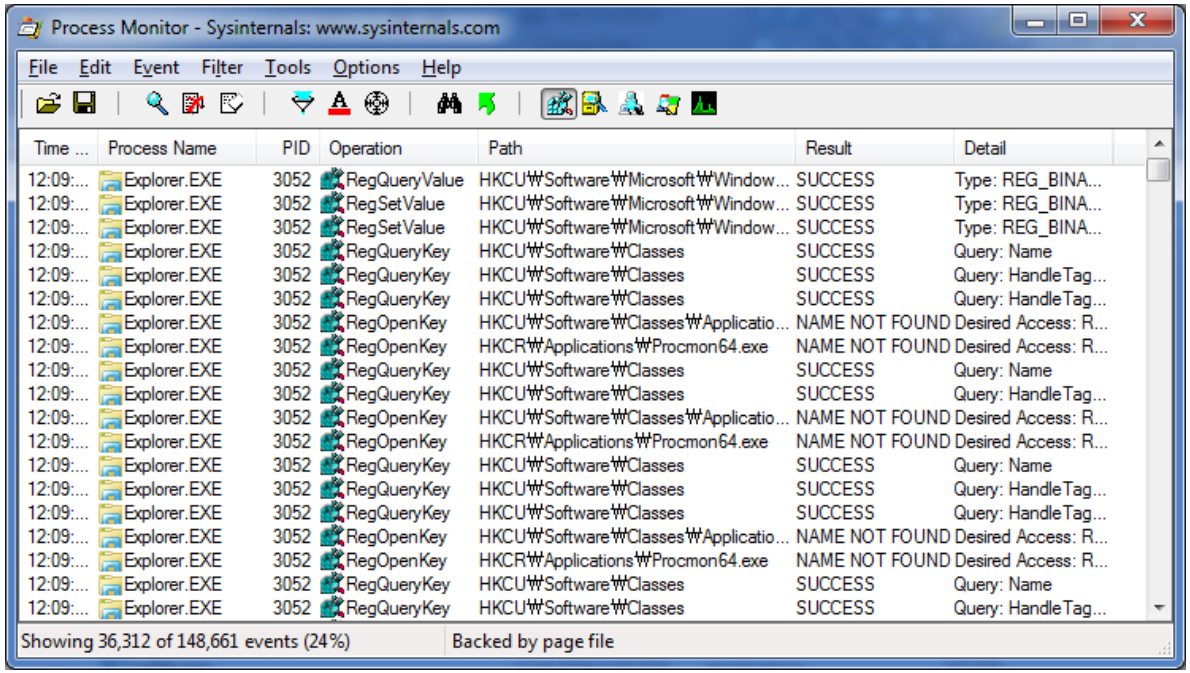
- **레지스트리 분석 체계화**
  - 앞서 언급한 레지스트리 흔적 이외에도 응용프로그램이나 사용자의 행위에 따라 다양한 흔적 존재
  - 매 사건마다 전체 레지스트리 흔적을 모두 찾는 것은 바람직하지 않음
  - 사건이 일어난 후 사전 조사를 통해 우선 분석이나 정밀 분석해야할 레지스트리 선정 필요
  - 따라서 사전에 응용프로그램이나 사용자 행위에 따른 레지스트리 흔적 변화의 체계적인 정리 필요
  - 국내에서 널리 사용되는 응용프로그램(한글, 곰플레이어, 알집 등)에 대한 레지스트리 흔적도 분석 필요

레지스트리 도구

Security is a people problem…

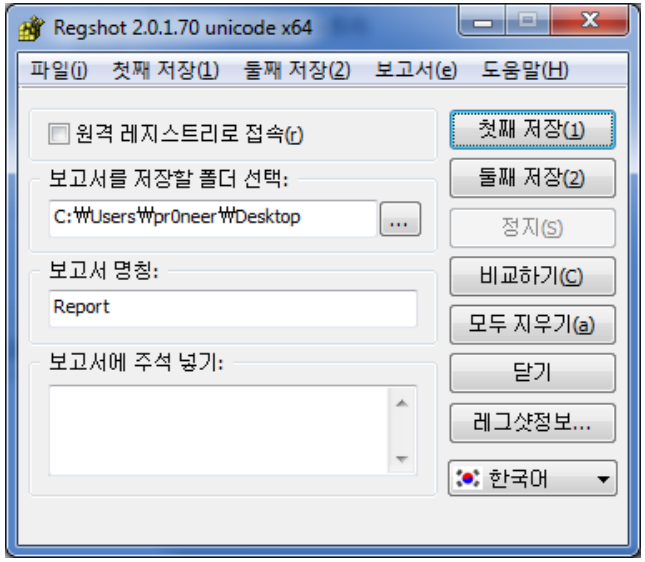
모니터링 도구

- **Process Monitor** (http://technet.microsoft.com/en-us/sysinternals/bb896645)
  - 레지스트리 실시간 모니터링 도구
  - 지원 운영체제
    - 클라이언트 : Windows XP SP2 이상
    - 서버 : Windows Server 2003 SP1 이상



모니터링 도구

- **Regshot** (http://sourceforge.net/projects/regshot/)
  - 레지스트리 스냅샷을 통해 두 시점간의 레지스트리 비교
  - 지원 운영체제 : Windows 2000, XP, Vista, 7



삭제된 키들 (0) 다음 저장에서 : 저장 A

생성된 키들 (3) 다음 저장에서 : 저장 B

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\InCtrl5]
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PC Magazine]
```

삭제된 값들 (0) 다음 저장에서 : 저장 A

생성된 값들 (3) 다음 저장에서 : 저장 B

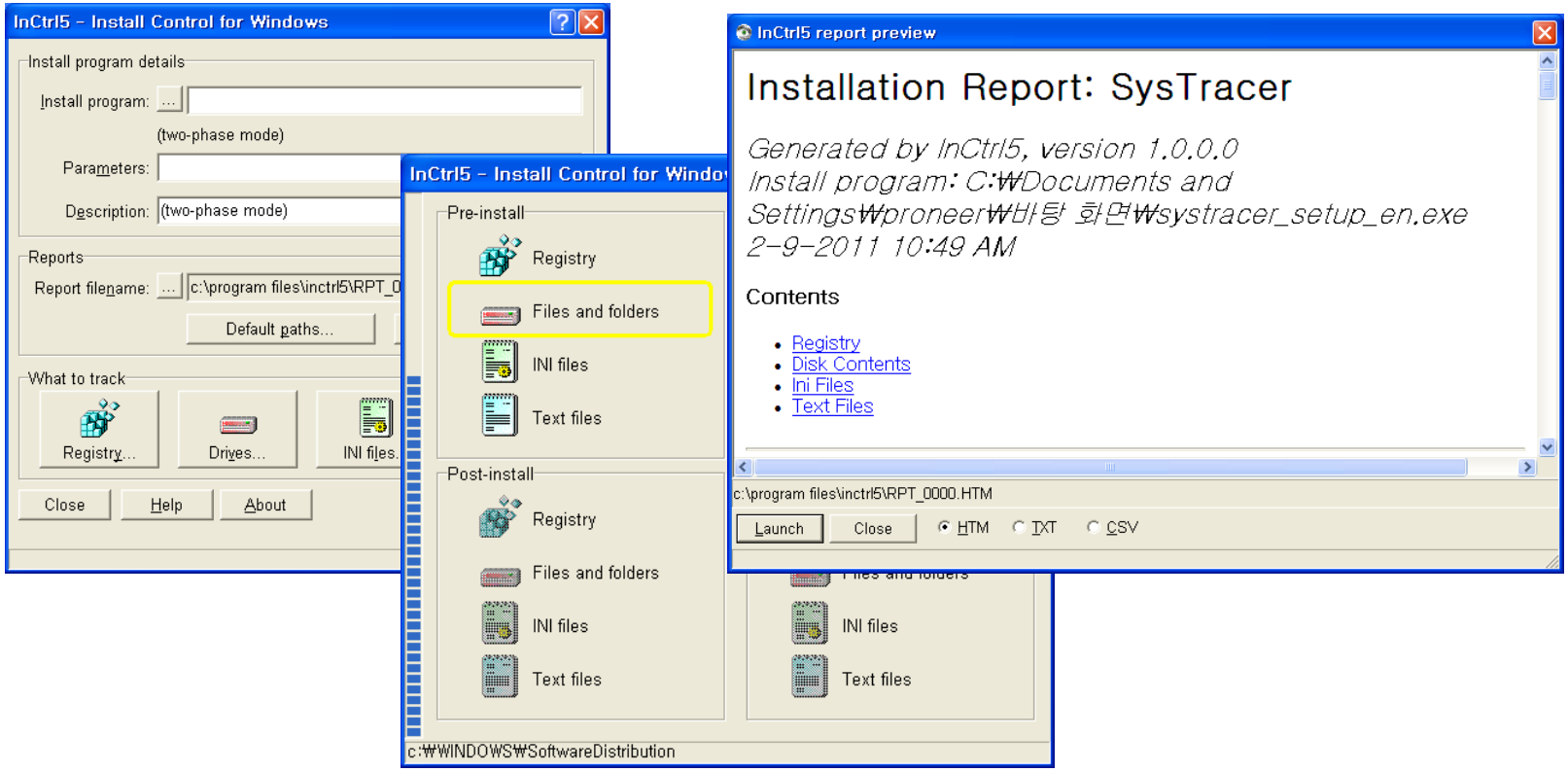
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\InCtrl5]
"DisplayName"="InCtrl5"
"UninstallString"="C:\\PROGRA~2\\InCtrl5\\UNWISE.EXE C:\\PROGRA~2\\InCtrl5\\INSTALL.LOG"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PC Magazine\InCtrl5]
"ProgramLocation"="C:\\Program Files (x86)\\InCtrl5"
```

변화된 값들 (18) 다음 저장에서 : 저장 A

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Reliability Analysis\RAC]
"WmiLastTime"=hex(b):f5,8b,cb,60,92,c7,cb,01
"WmiLastTime"=hex(b):cc,84,4e,02,99,c7,cb,01
"TransientValue"=hex:0f,bf,0e,ec,88,dc,1c,40
"TransientValue"=hex:a6,0b,8b,ec,4a,ee,1c,40
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]
"GlobalAssocChangedCounter"=dword:0000000b
"GlobalAssocChangedCounter"=dword:0000000c
```

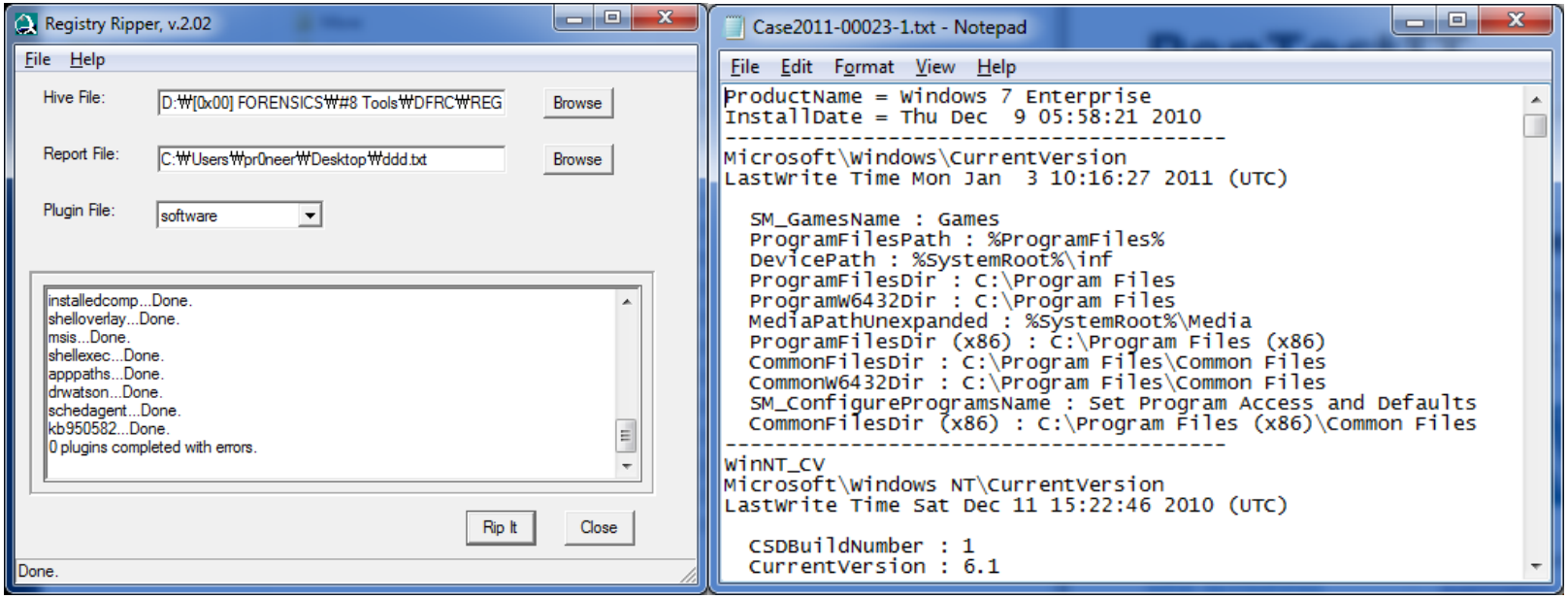
모니터링 도구

- **InCtrl5** (http://www.pcmag.com/article2/0,2817,25126,00.asp)
  - 레지스트리, 파일 스냅샷을 통해 두 시점간의 레지스트리, 파일 비교
  - 지원 운영체제 : Windows 95, 98, NT, 4.0, 2000, ME



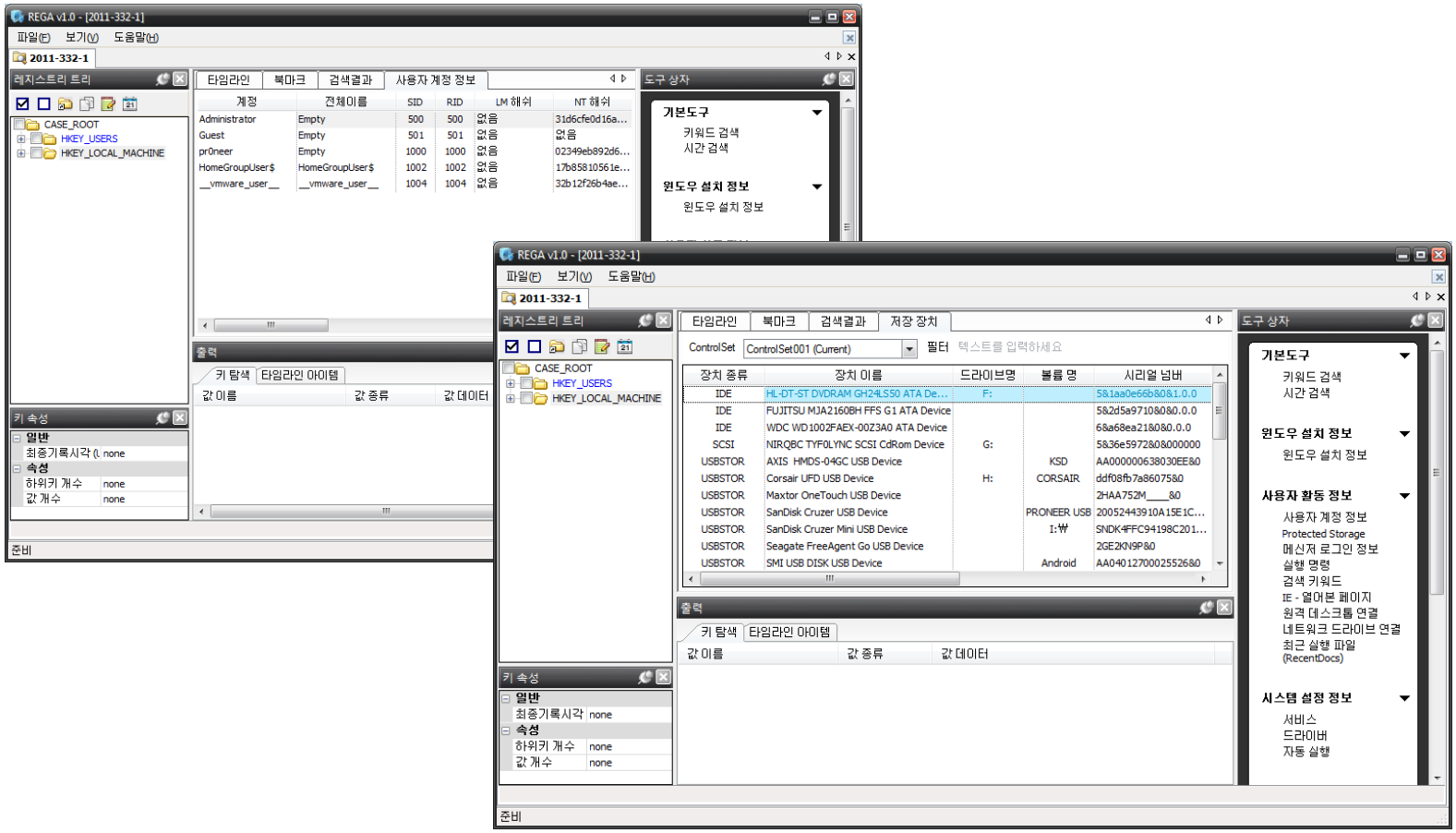
분석 도구

- **RegRipper** (http://regripper.net/)
  - 펄(Perl) 기반의 레지스트리 파일(하이브) 분석 도구
  - RegRipper를 포함한 포렌식 툴킷
    - PlainSight (http://www.plainsight.info)
    - SIFT(SANS Investigative Forensic Toolkit) (https://computer-forensics.sans.org/community/downloads)



분석 도구

- **REGA** (http://forensic.korea.ac.kr)
  - MFC 기반의 GUI 레지스트리 분석 도구



레지스트리 분석 예제

Security is a people problem…

Q) Forensics 300

- We are investigating the military secret's leaking.

  we found traffic with leaking secrets while monitoring the network.

  Security team was sent to investigate, immediately. But, there was no one present.

  It was found by forensics team that all the leaked secrets were completely deleted by wiping tool.

  And the team has found a leaked trace using potable device.

  Before long, the suspect was detained. But he denies allegations.

- Now, the investigation is focused on potable device.

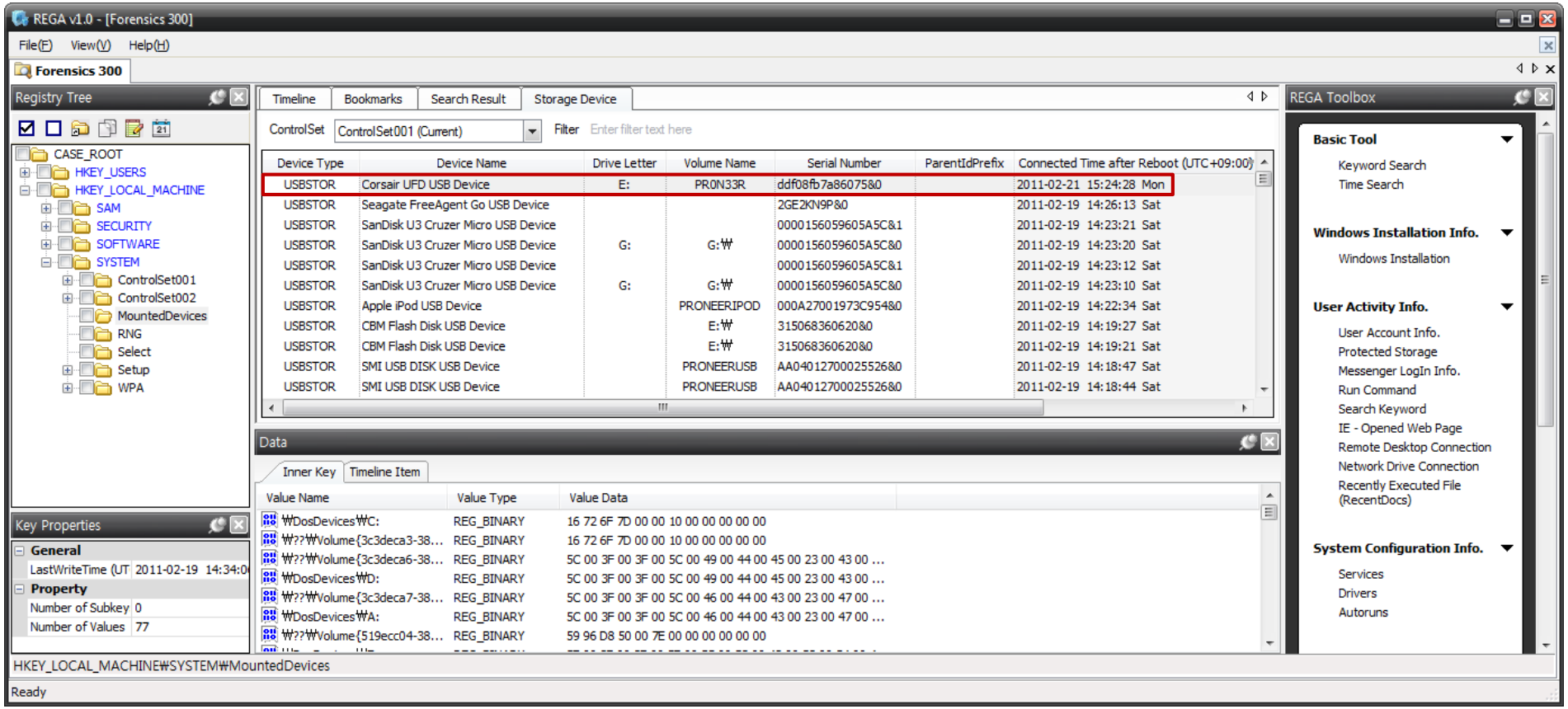
  The given files are acquired registry files from system.

  The estimated time of the incident is Mon, 21 February 2011 15:24:28(KST).

  Find a trace of portable device used for the incident.

- **The Key : "Vendor name" + "volume name" + "serial number" (please write in capitals)**

A) Forensics 300 Writeup



- The Key : "Vendor name" + "volume name" + "serial number" (please write in capitals)
- Vendor : Corsair, Volume name : PR0N33R, Serial number : ddf08fb7a86075&0
- Answer : CORSAIRPR0N33RDDF08FB7A86075

Q) Forensics 'GEOL' or 'YUT'

- we are investigating the military secret's leaking.
- It seems that the suspect used a portable device.

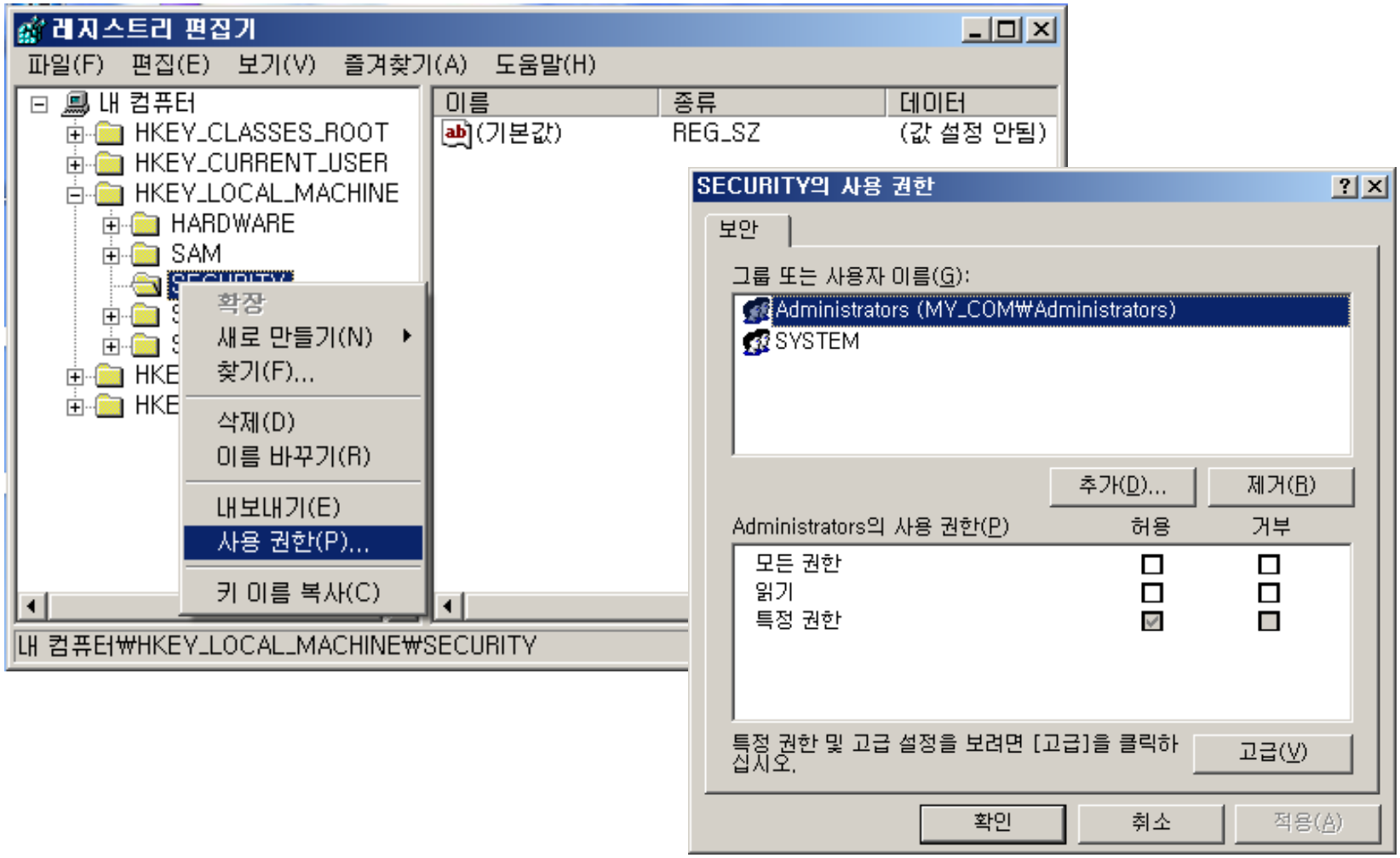
- **Find a signature of mounted E: drive. (please write in capitals)**

레지스트리 보안

Security is a people problem…

레지스트리 설정

- **키 권한 설정**



레지스트리 설정

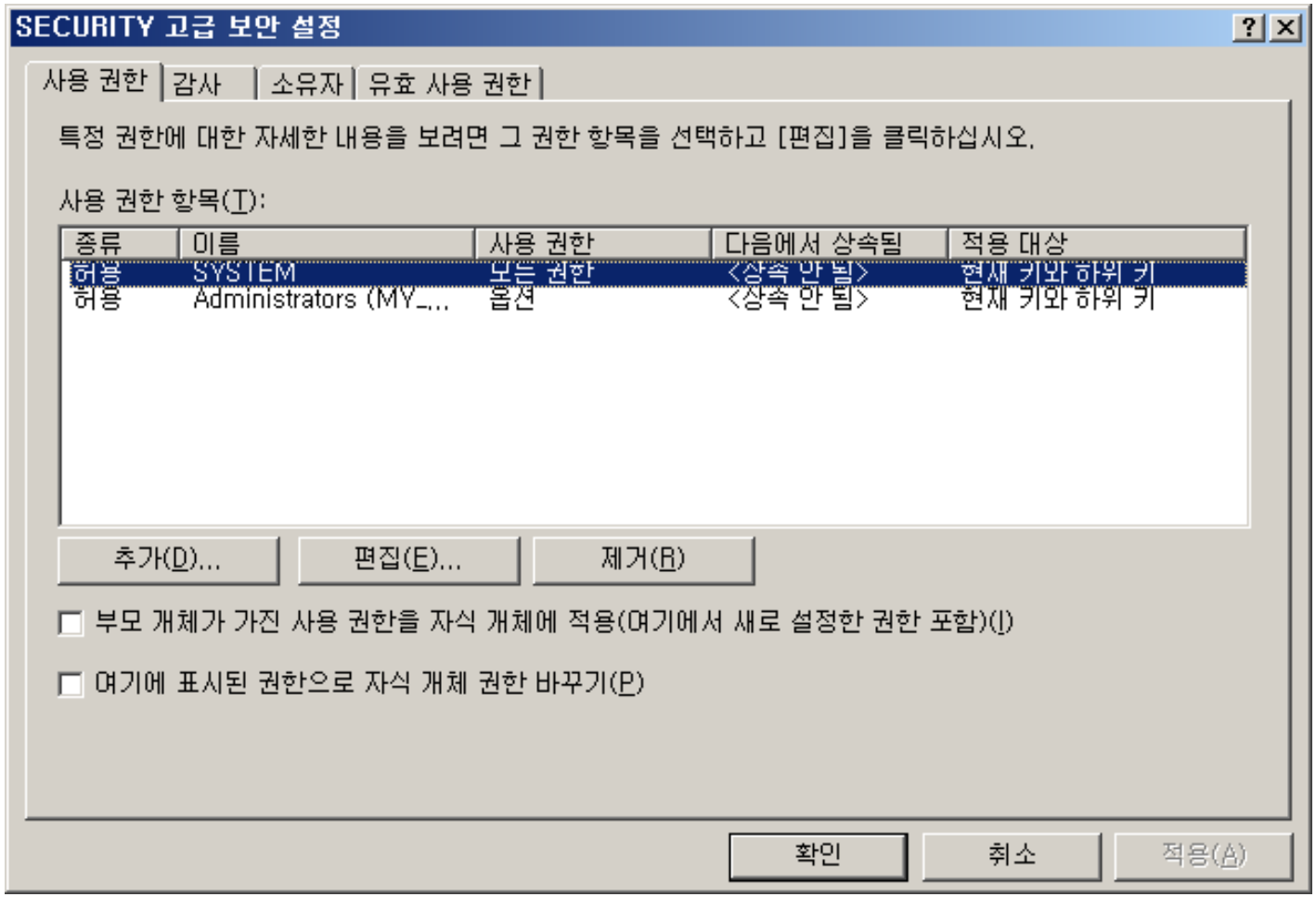
- 키 권한 설정
  - RegCreateKeyEx (

```
__in        HKEY hKey,
__in        LPCTSTR lpSubKey,
__reserved  DWORD Reserved,
__in_opt    LPTSTR lpClass,
__in        DWORD dwOptions,
__in        REGSAM samDesired,        /* 키 보안 및 접근 권한 mask 설정 */
__in_opt    LPSECURITY_ATTRIBUTES lpSecurityAttributes,
__out       PHKEY phkResult,
__out_opt   LPDWORD lpdwDisposition );
```

  - RegOpenKeyEx()
  - RegCreateKeyTransacted()
  - RegOpenKeyTransacted()

레지스트리 설정

- **고급 보안 설정 (사용 권한, 감사, 소유자, 유효 사용 권한)**

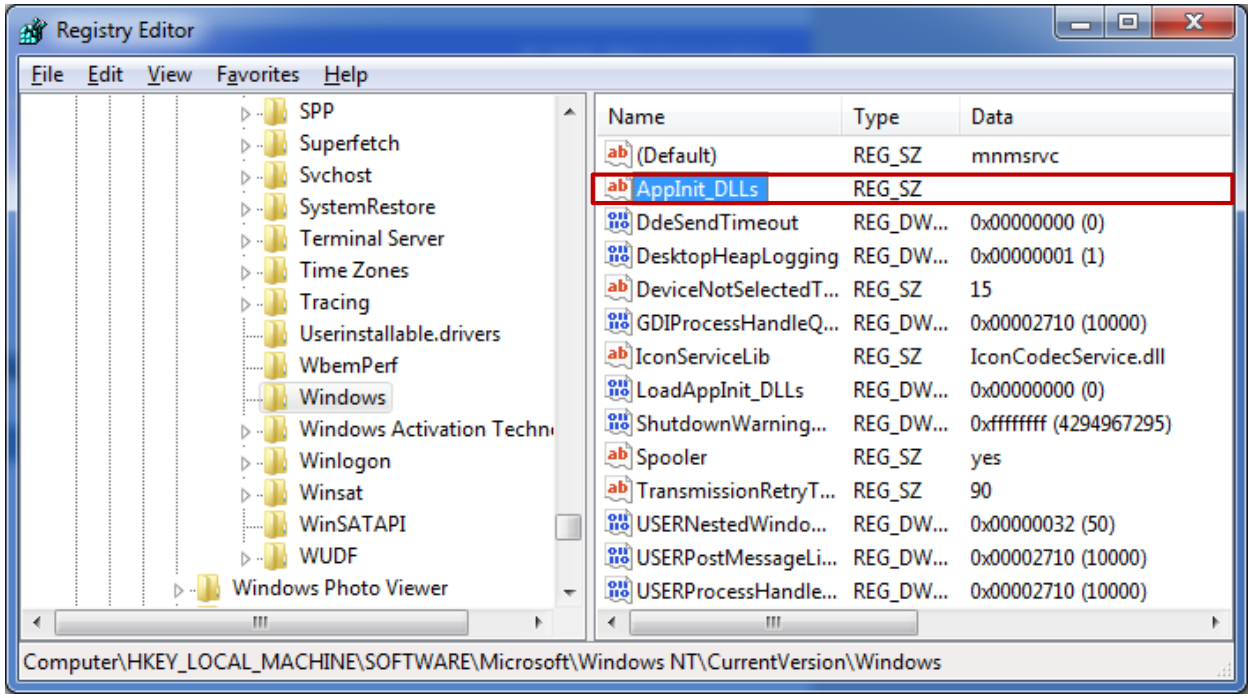


악성코드 (1/5)

- **자동 시작 목록 (약 130여개의 키가 확인 됨, Autoruns by Sysinternals.com, Microsoft)**
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnce
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnceEx
  - HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Windows₩Run
  - HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run
  - HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnce
  - HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩RunOnceEx
  - HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer₩Run
  - HKLM₩SYSTEM₩ControlSet00X₩Control₩Terminal Server₩Wds₩rdpwd₩StartupPrograms
  - … …

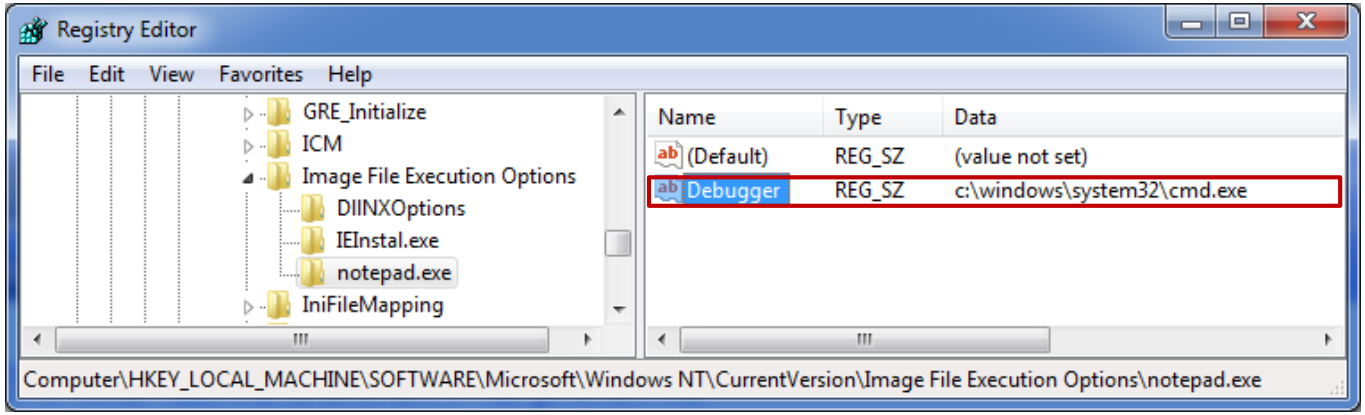
악성코드 (2/5)

- **Appinit_DLLs – GUI 응용프로그램에 의해 로드되는 DLL**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Windows**
  - **AppInit_DLLs** – GUI 응용프로그램 실행 시 (user32.dll에 의해) 자동으로 로드되는 DLL
  - 일반적으로 비어 있으며, 값이 존재한다면 악성코드일 가능성이 큼



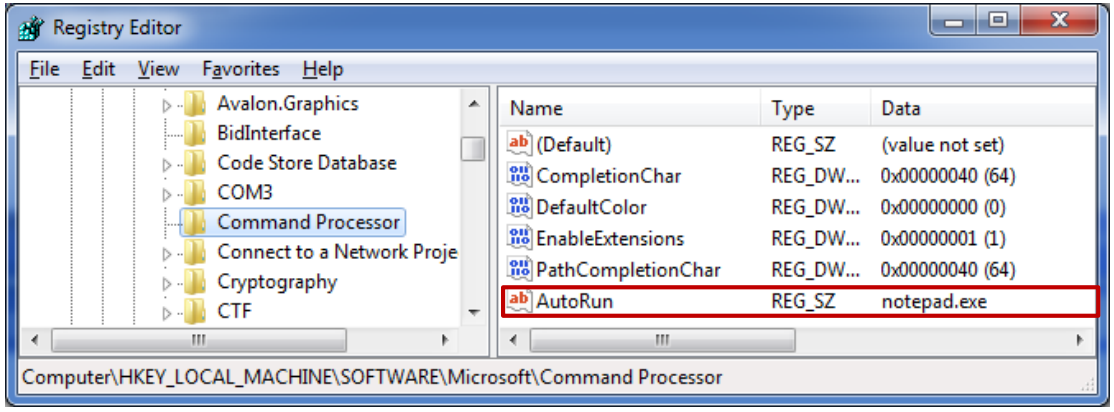
악성코드 (3/5)

- **Image File Execution Options – 자동 디버그 연결 정보**
  - **HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Image File Execution Options**
  - 하위 키로 디버깅하고자 하는 응용프로그램 추가
  - Debugger 값으로 해당 응용프로그램 실행 시 연결 시킬 디버거 지정 (디버거 검증 안함)
  - 특정 응용프로그램을 다른 프로그램으로 리다이렉트 가능



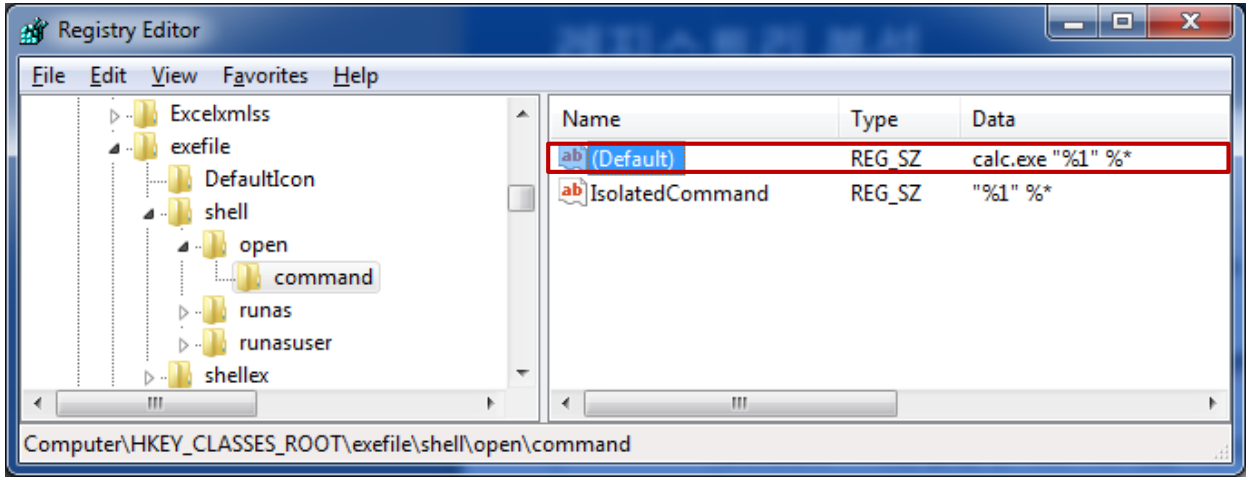
악성코드 (4/5)

- **Command Processor₩AutoRun – 명령프롬프트 실행 시 자동 시작되는 응용프로그램**
  - **HKLM(HKCU)₩SOFTWARE₩Microsoft₩Command Processor**
  - **AutoRun** – 값 생성 후 특정 응용프로그램을 지정하면 명령 프롬프트 실행 시 자동으로 함께 실행



악성코드 (5/5)

- **exefile₩shell₩open₩command – 실행 파일 실행 시 정상적인 매개변수**
  - **HKLM₩SOFTWARE₩Classes₩exefile₩shell₩open₩command**
  - **Default** – 기본값은 ["%1" %*]를 가져야 함
  - 악성 코드에 의해 실행 파일 실행 시 다른 프로그램 수행
  - exefile 외에 comfile, batfile, htafile 등에도 동일하게 적용



완전 삭제 (wiping)

- **삭제된 레지스트리 개체를 복구 불가능하도록 완전 삭제**
  - 레지스트리 직접 삭제나 API를 이용해서는 안됨
  - 삭제 동작 시 하이브 파일 내에서 해당 레지스트리 데이터 완전 삭제

참고자료

추가적인 내용은 다음 자료 참고

- **AccessData – Registry Offsets**
  - http://accessdata.com/downloads/media/Registry%20Offsets%209-8-08.pdf
- **AccessData – Registry Quick Find Chart**
  - http://accessdata.com/downloads/media/Registry%20Quick%20Find%20Chart%20%207-22-08.pdf
- **AccessData – Microsoft Office 2007, 2010 – Registry Artifacts**
  - http://accessdata.com/downloads/media/Microsoft_Office_2007-2010_Registry_ArtifactsFINAL.pdf
- **AccessData – UserAssist Registry Key**
  - http://accessdata.com/downloads/media/UserAssist%20Registry%20Key%209-8-08.pdf
- **A Windows Registry Quick Reference : For the Everyday Examiner**
  - http://www.forensicfocus.com/downloads/windows-registry-quick-reference.pdf

질문 및 답변