

# A Forensic Analysis of the Windows Registry

국립경찰대학 사이버범죄연구회

Cybercrime Research Group

행정학과 3학년 김범연

2009. 11. 5.



## ○ 목 차 ○

### 1. 도입

### 2. 레지스트리

#### 2-1. 레지스트리 정의

#### 2-2. 레지스트리를 통해 알 수 있는 정보

#### 2-3. 레지스트리의 구성

##### 2-3.1. HKLM(HKEY\_LOCAL\_MACHINE)

##### 2-3.2. HKU(HKEY\_USERS)

##### 2-3.3. HKCU(HKEY\_CURRENT\_USER)

##### 2-3.4. HKCC(HKEY\_CURRENT\_CONFIG)

##### 2-3.5. HKCR(HKEY\_CLASS\_ROOT)

#### 2-4. 하이브 파일 (Hive File)

##### 2-4.1. 하이브 파일 (Hive File)의 정의

##### 2-4.2. 레지스트리 하이브 (Registry Hive)의 구성

##### 2-4.3. HKEY\_LOCAL\_MACHINE 의 4가지 Hive File

##### 2-4.4. HKEY\_USERS 의 2가지 Hive File

### 3. 레지스트리를 로그로 활용하기

#### 3-1. Offline System 레지스트리의 LastWrite time확인 (Encase 이용)

##### 3-1.1. 원하는 레지스트리에 해당하는 Hive File을 찾아간다.

##### 3-1.2. 해당 경로로 찾아가서 오른쪽 버튼 – View File Structure

##### 3-1.3. Hive File 익스포팅 후 별도의 툴 활용하기

#### 3-2. 어플리케이션 관련 최근 사용 흔적

##### 3-2.1. 최근 실행 목록(MRU lists, most recently used)

##### 3-2.2. 최근 삭제한 목록

##### 3-2.3. 특정 파일, 어플리케이션의 사용자 접근

### 3-3. 시스템 정보

- 3-3.1. USB 장치 (USB Memory, PDA, 핸드폰 등)
- 3-3.2. 마운트한 장치들
- 3-3.3. 기타 포렌식 관점으로 주시할 사항

### 3-4. 네트워크

- 3-4.1. 무선 네트워크
- 3-4.2. 로컬 네트워크
- 3-4.3. Intelliforms(자동완성기능)
- 3-4.4. 기타 포렌식 관점으로 주시할 사항

### 3-5. 웹 브라우저

- 3-5.1. 인터넷 익스플로러
- 3-5.2. Opera
- 3-5.3. Netscape, FireFox

### 3-6. P2P 클라이언트

- 3-6.1. Limewire
- 3-6.2. Kazaa
- 3-6.3. Morpheus
- 3-6.4. 기타 국내 P2P 및 웹 하드
- 3-6.5. 공통 레지스트리 키

### 3-7. Messenger

- 3-7.1. MSN Messenger
- 3-7.2. Nateon
- 3-7.3. Yahoo
- 3-7.4. AOL Instant Messenger (AIM)
- 3-7.5. Windows Messenger

### 3-8. Outlook and Outlook Express

#### 4. 레지스트리에서 공격자의 흔적 찾기

##### 4-1. 루트킷 탐지

- 4-1.1. 도입
- 4-1.2. 레지스트리 Hives (SYSTEM, SOFTWARE)
- 4-1.3. 로우 레벨 Data 획득
- 4-1.4. Helios 툴을 이용한 Cross-View 탐지
- 4-1.5. 한계

##### 4-2. 자동실행( Autoruns), 시작 프로그램(Startup) 관련

- 4-2.1. 일반적인 autuorun locations 목록
- 4-2.2. SharedTaskScheduler
- 4-2.3. ShellWOpenWCommand
- 4-2.4. ShellServiceObjectDelayLoad(SSODL)
- 4-2.5. SYTEM.INI / WIN.INI File
- 4-2.6. ShellExecute Hook
- 4-2.7. AppInit\_DLL 레지스트리 값 자동 실행
- 4-2.8. AppInit\_DLLs
- 4-2.9. Winlogon Notification Package
- 4-2.10. UserInit Key

##### 4-3. Internet Explorer 관련

- 4-3.1. Browser Helper Object (BHO)
- 4-3.2. IE Start page/search page/search bar/search assistant URL
- 4-3.3. Default URL Searchhook
- 4-3.4. IE Options access restricted by administrator
- 4-3.5. Extra Items in IE right-click menu

##### 4-4. 기타 포렌식 관점으로 주시할 사항

- 4-4.1. Windows Services
- 4-4.2. Hidden Resource configuration
- 4-4.3. Hosts 파일 (Domain Hijack)
- 4-4.4. Regedit access restricted by administrator

- 4-4.5. Event Log Restrictions
- 4-4.6. URL Default Prefix Hijack
- 4-4.7. WinSock LSP (Layered Service Provider)
- 4-4.8. 가상메모리 파일 자동삭제
- 4-4.9. 실행 파일을 다른 프로그램으로 연결
- 4-4.10. 임시 폴더 및 공유 폴더

## 5. 레지스트리 복구

- 5-1. Registry Key Recovery
  - 5-1.1. 레지스트리 키 복구 원리
  - 5-1.2. 레지스트리 키 삭제 매커니즘
  - 5-1.3. Reglookup-recover을 이용한 삭제된 키 복구
- 5-2. Restore Point (RP)
  - 5-2.1. 개요
  - 5-2.2. 설정 상태 확인
  - 5-2.3. Restore Point 위치
  - 5-2.4. 조사가 필요한 Restore Point 선택
  - 5-2.5. 백업 파일 조사
  - 5-2.6. 백업 레지스트리 조사

## 6. Registry Forensic 관련 툴 소개

- 6-1. Hijackthis
- 6-2. SysinternalsSuits 중 Autoruns
- 6-3. Registry Viewer
- 6-4. Paraben Registry Analyzer
- 6-5. Regripper
- 6-6. Regshot
- 6-7. Regmon

## 6. 결론

## 7. 참고문헌

## 1. 도입

오늘날 우리 사회에서, 온라인 메신저라든가 인터넷 쇼핑, 인터넷 은행계좌 거래에 이르기까지 컴퓨터와 인터넷의 사용은 일상생활이 되었다. 컴퓨터 범죄라고 하는 새로운 영역이 생겨났고 인터넷 사기, 주민등록번호 도용, 피싱, DoS 공격, 저작권 위반 등 다양한 유형을 보이며 그 수는 증가하기 시작했다. 법집행관과 디지털 포렌식 전문가는 컴퓨터 시스템을 완벽히 이해해야 하며, 효율적이고 효과적으로 디지털 증거를 수집 및 분석해야 할 필요성이 대두되었다. 이 중, 레지스트리는 Microsoft Windows 운영체제의 핵심적인 요소로서, 디지털 포렌식 관점에서 많은 정보를 얻을 수 있다. 컴퓨터를 사용한 모든 작업은 사용자의 의지와는 상관없이 레지스트리 키에 많은 흔적을 남기기 때문이다. 이 글에서는 Windows XP (서비스팩 2) 를 기반으로, 레지스트리에서 찾을 수 있는 유용한 수사 단서로서의 증거에 관하여 논하겠다.

## 2. 레지스트리

### 2-1. 레지스트리 정의

먼저 레지스트리란 무엇이며, 어떠한 정보가 그 안에 담겨있는지 이해하는 것이 중요하다. Windows에서 행해지는 거의 모든 작업은 레지스트리를 참고하며 또한 레지스트리에 기록된다.

Microsoft 지식 데이터베이스와 Microsoft Computer Dictionary(5판)에서는 레지스트리를 '한명 또는 다수의 사용자를 위한 시스템의 환경설정 정보와 어플리케이션, 하드웨어 장치 정보 등을 저장하기 위해 Windows 9x, CE, NT, 2000에서 사용하는 중앙 집중적이고 계층적인 데이터베이스'라고 정의하고 있다.

레지스트리는 Windows 95에서 처음 도입되었으며, 이후 많은 Microsoft 운영체제에 적용되었다. 버전마다 약간 상이하나, MSDOS에서 사용하던 config.sys(장치 드라이버를 load함)나 autoexec.bat(환경 변수와 실행 프로그램을 설정함) 파일과 같은 환경설정 파일을 대신하는 데이터베이스로서 그 역할과 구조는 동일하다. 레지스트리는 이 밖에도 Windows 3.0에서 도입된 텍스트 기반의 환경설정 파일(.ini)의 역할도 하고 있는데, .ini 파일 중 특히 win.ini와 system.ini 는 사용자 설정 정보와 운영체제의 매개변수들을 저장한다.

## 2-2. 레지스트리를 통해 알 수 있는 정보

Windows 레지스트리를 분석하여 최근에 열었거나, 실행, 수정한 문서에 대한 사용 흔적을 찾을 수 있고, Windows 2000 서버 같은 경우에는 불법계정생성 유무 확인을 할 수 있다. 특정 프로그램을 설치하고 삭제를 한 경우에도 그 흔적을 찾을 수 있으며, 바이러스 등 악성 프로그램에 의한 감염 여부와, 컴퓨터 정보 등의 유용한 정보들을 얻어낼 수 있다. (Chad Steel, 2006)

또한 Windows 에서 기본 제공하는 레지스트리 편집기에서는 보이지 않지만, 마지막 수정 시각(LastWritten time)이 기록되어 있어, 디지털 포렌식 관점에서 일종의 로그(언제, 누가, 무엇을 하였는지 기록)로서 유용하게 사용될 수 있다.

## 2-3. 레지스트리의 구성

레지스트리의 구성을 보면 레지스트리는 HKEY\_CLASSES\_ROOT를 비롯하여 5개의 가장 상위키를 갖는데, 이를 루트키라고 한다. 각 루트키 아래의 서브키 이하 트리구조를 하이브(Hive) 라고 하며, 각각의 하이브는 저마다 고유한 저장장소(파일)와 로그 파일을 갖고 있다. 다음에서는 각각의 Key 들을 통해 알 수 있는 정보에 대해 알아본다. HKLM과 HKU만이 Windows에서 파일 형태로 저장하고 있는 루트키이며, HKCU는 HKU에, HKCR과 HKCC는 HKLM 서브키의 심볼릭 링크이다. (Honeycutt, 2003, p. 26)

레지스트리의 구조와 관련한 많은 부분은 'Rusinovich and Solomon, 2004'에 잘 설명되어 있다.

※ 참고 : 각각의 루트키는 Master key 와 Derived key 로 나뉜다.

Master key : 대체로 대응하는 파일이 있다. 부팅시 CM(Configuration Manager)이 해당 하이브 파일을 읽어서 Master key 를 구성한다.

Derived key : Sybolic Link라고도 한다. Master key 로부터 그 값이 유도된다.

디스크 상에는 대응하는 파일이 없다. 메모리 상에만 존재한다.

Windows 운영체제 부팅 시 재설정된다.

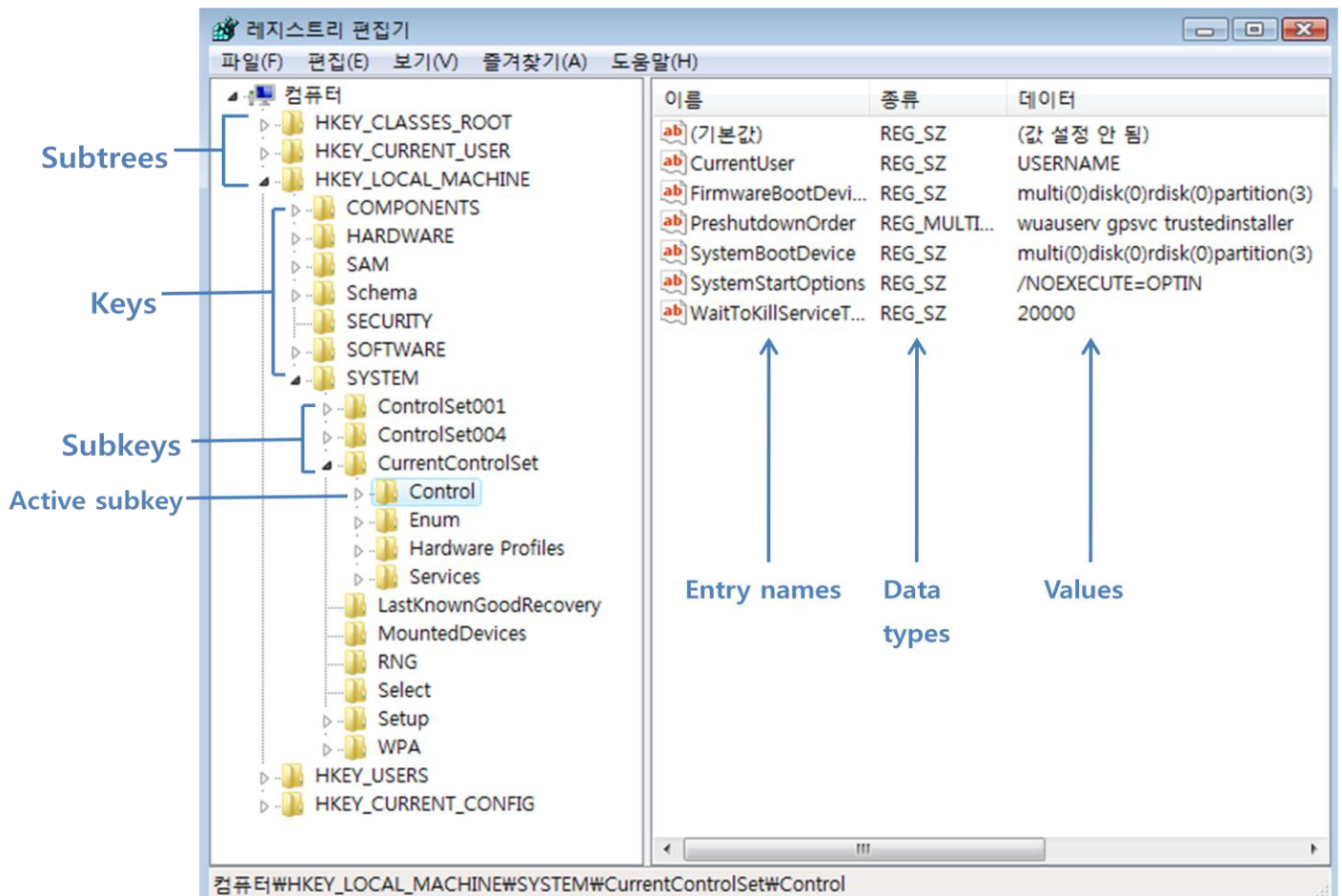


그림 1. Windows 레지스트리의 구성

### 2-3.1. HKLM(HKEY\_LOCAL\_MACHINE)

하드웨어 구성 초기화 파일, 시스템에 마운트한 드라이브와 설치된 하드웨어 및 어플리케이션의 일반적인 설정 정보 등이 존재한다. Key 대부분이 Master key로서, 해당 하이브 파일로부터 레지스트리 정보를 읽는다.

- i. System : 컴퓨터 이름, Time Zone, Last shutdown time, CD 오토런 세팅, 네트워크 연결정보(방화벽 설정, tcp/ip 설정), 프로세서 정보, 하드웨어 정보(플로피, 드라이브, 휴먼 인터페이스 장치, LPT 포트, 저장 장치, USB 메모리 장치, 마운트한 장치 등)
- ii. Software : USB 볼륨 시리얼 넘버(in Windows Vista), 휴지통 설정, 사용자 프로필, 무선연결정보, 프린터 정보, Autologon 세팅, 언인스톨된 소프트웨어 흔적, 어플리케이션 규제(eg. Winlogon), 감추어진 패스워드 설정정보 등
- iii. Security : SAM 서브키에 있는 Windows 로컬 security 데이터베이스. ACL 이 Administrator 가 이 서브키를 보지 못하도록 막는다.



별도의 툴을 활용하여, 현재 시스템의 패스워드, 마지막으로  
로그온한 사용자의 패스워드, 보관된 시스템 패스워드 확인 가능

iv. SAM : Security Accounts Manager.

시스템 사용자 계정, 사용자 정보와 속성(Linux 의 etc/pwd 와 유사),  
사용자 로그인 패스워드 정보, 사용자 프로필, 사용자 그룹 권한 등.  
ACL이 이 서브키를 보이지 않도록 하여, Live system에서는 그  
내용이 읽히지 않는다. 관련 크래킹 툴을 이용하여 파일을 강제로  
읽을 수 있다.

v. Hardware : 모니터, 포트 등 컴퓨터 구성 장치 정보

하이드 파일이 존재하지 않으나, Derived key 는 아니다.

시스템 시작시 동적으로 서브키가 생성된다.

vi. Components, bcd : Vista 에서만 존재한다.

### 2-3.2. HKU(HKEY\_USERS)

모든 사용자별의 어플리케이션 환경, 비주얼 설정정보 등의 프로필을 보관한다.

HKEY\_CURRENT\_USER 와 겹치면 HKCU 가 우선한다. HKU 는 Windows XP 에서  
잘 알려진 SID 를 가진다. S-1-5-18 은 로컬 시스템 계정을 의미하고, S-1-5-19 는  
로컬 서비스 계정, S-1-5-20 은 네트워크 서비스 계정을 의미한다. (Master key)

i. DEFAULT : 모든 사용자들에게 공통 적용되는 환경정보.

ii. SID : 각 사용자별 고유한 Security ID 를 가진다.

사용자별 설정정보들이 나열되어 있다.

(유닉스의 UID 와 유사, eg. S-1-5-18)

iii. SID\_CLASS

### 2-3.3. HKCU(HKEY\_CURRENT\_USER)

현재 시스템에 로그인 중인 사용자에 대한 설정 정보를 보관한다. 사용자  
데스크톱 설정, 네트워크 설정, 응용 프로그램 설정, 환경 설정, 프로그램 그룹  
등의 프로필 정보를 포함하며, 대부분의 정보는 HKU 로부터 파생된다.  
서브키로는 Identities, Network, Software, Volatile Environment 가 있다. 로그인  
담당 프로그램에서 호출시마다 갱신된다.

(Derived key : "HKUWSID " Master Key 로부터 유도되는 Symbolic link)

#### 2-3.4. HKCC(HKEY\_CURRENT\_CONFIG)

현재 사용중인 윈도의 디스플레이(화면글꼴이나 해상도) 정보와 프린터 정보 (Derived key : "HKLM의 SOFTWARE\_ FONTS, Microsoft" Master Key로부터 유도된다.)

#### 2-3.5. HKCR(HKEY\_CLASS\_ROOT)

각 사용자의 설정 유형, 파일의 확장자를 기준으로 한 타입별 연결 프로그램 정보, Component Object Model(COM)에 대한 클래스 등록 정보 등을 포함한다. 레지스트리의 대부분의 공간을 차지한다.

(Derived key : "HKLM\SOFTWARE\Classes와 HKCU\Software\Classes(HKU\SID\\_Classes로 링크됨) " 두 키를 통합하여 프로그램은 파일 연결 정보, 프로그램 클래스 등을 등록한다.)

### 2-4. 하이브 파일 (Hive File)

#### 2-4.1. 하이브 파일 (Hive File)의 정의

여러 정보를 안고 있는 레지스트리는 Directory의 계층 구조와 같은 트리 형태로 정보를 담으며, 키, 서브키 값과 같은 하이브 파일(Binary File)의 묶음 구조이다. 레지스트리 정보는 디스크에 존재하는 것이 아니라 Memory에만 존재한다. 하이브 파일이란, 레지스트리의 정보를 갖고 있는 디스크 상의 파일이다.

Live System 이 아닌 경우, Memory 를 덤프(dump)하여 레지스트리 관련정보를 확인할 수 없으므로, 하이브 파일을 찾아 필요한 정보를 확인하는 것이 중요하다. 또한 하이브 파일 조사/분석은 메모리가 아닌 디스크 상에서 행해지기 때문에, 루트킷의 영향을 받지 않는다는 장점이 있다. 파일을 직접 조사하기 때문이다

#### 2-4.2. 레지스트리 하이브 (Registry Hive)의 구성

레지스트리는 4096 바이트 사이즈인 블록(block)에 나누어 저장된다. 첫 번째 블록은 베이스 블록(base block)이라고 하고 첫 4바이트에 'regf(0x66676572)'라는 서명이 담겨 있다. 베이스 블록은 그 하이브의 루트키와 상응하는 것을 담고 있다. 실제 데이터는 셀(cell)이라는 저장 공간에 담겨 있다. 이 셀은 키, 값, 서브키 리스트나 값이나 데이터에 관한 리스트를 담는다. 이것들은 그 구조의 첫 두 바이트에 있는 시그니처로 구분된다. 각각의 셀의 헤더에는 시그니처와 해당 셀의

크기가 저장된다. (Dolan-Gavitt, 2008a).

레지스트리에 필요한 공간은 복수의 셀이 아닌 빈(bin)에 할당된다. 빈은 셀을 포함하는 개념으로 헤더에 'hbin'(0x6E696268)이라는 시그니처가 있다. 큰 데이터 필드는 복수의 빈에 나누어 저장시킬 수 있다. 각각의 셀은 레지스트리 하이브의 구조를 제공하기 위하여 서로 링크되어 있는데, 몇몇은 어미 셀(parent cell)에 몇몇은 자식 셀(child cell)에 링크되는 구조를 취하고 있다. 모든 링크는 같은 데이터 구조(eg. 같은 레지스트리 하이브 파일) 내의 오프셋 내에서 이루어지며, 오프셋은 현재 셀로부터의 상대적인 값이 아닌, 베이스 블록으로부터의 절대적인 값을 지닌다. 따라서, 모든 셀은 링크된 현 주소를 몰라도 오프셋을 통하여 접근하고 참조가 가능하다.

아래에서는 셀 타입(Types of Cells)에 대하여 간단히 알아본다. (Mihir Nanavati)

<b>키 셀(Key Cell) (NK)</b>	: 레지스트리 키를 포함한 셀. 헤더의 'nk'(0x6B6E)라는 시그니처로 구분된다. 가장 중요한 필드는 키의 이름과 그 길이라고 할 수 있으며, 서브 키의 개수, 각 키 내의 값의 개수를 저장하는 필드도 있다. 이 밖에도 두 개의 필드는 서브키 리스트 셀에 오프셋을 제공한다.
<b>서브키 리스트 셀(Sub-key List Cell) (RI/LH/LF)</b>	: 특정 키의 모든 서브 키에 대한 링크나 오프셋을 저장하는 셀. 시그니처 'lf'(0x686C), 'lh'(0x666C), 'ri'(0x6972)로 구분된다. LH와 LF 엔트리는 서로 유사하며 서브키를 구성하는 키 셀의 오프셋 리스트를 포함한다. RI 키는 다수의 서브키를 갖고 있는 키에 사용된다. 키 셀은 대개 LH나 LF 구조를 직접 가리키기 보다는, RI 구조체 한 세트를 가리키는데, RI 구조체가 몇몇 LH/LF 구조체에 대한 오프셋을 포함하기 때문이다. 오프셋은 리스트에 저장된다.
<b>Value-list Cell</b>	: 특정 키의 Value Cell의 오프셋 리스트를 포함하는 셀. 이를 구분하는 시그니처는 없다. 리스트 엔트리는 다른 것들과 유사하다.
<b>Value Cell (VK)</b>	: 키 값에 대한 정보가 있는 셀. 헤더의 'vk'(0x6B76) 시그니처로 구분된다. 이 필드에는 값의 이름, 이름의 길이, 데이터 등이 저장된다. unnamed Value는 레지스트리 편집기에 의해 Default로 표시된다. 데이터는 resident 또는 non-resident로 표기되며, Value가 데이터에 링크되어 있다면 데이터의 오프셋이 키에 저장된다. 오프셋 대신 Value가 직접 데이터를 그 자리에 저장하기도 한다.
<b>데이터 셀(Data Cell)</b>	: Value와 관련된 데이터가 저장된 셀. 헤더가 없다.

### 2-4.3. HKEY\_LOCAL\_MACHINE 의 4가지 Hive File

HKLM 의 **SYSTEM, SOFTWARE, SECURITY, SAM** 은 하이브 파일이 존재한다.

각각의 하이브 파일은 %systemroot%\system32\config\ 에 위치하며, 관련 로그 파일과 함께 존재한다. set 명령어를 사용하여 설정된 환경변수를 확인할 수 있다.

SYSTEM 과 SOFTWARE 하이브는 루트킷 탐지에 많이 사용된다. SYSTEM 은 시스템 상에 나타나 있는 모든 서비스와 드라이버의 리스트를 저장하고 있어, Hacker Defender 나 BadRkDemo 와 같은 커널 레벨 루트킷을 감지할 수 있다. 한편 DLL 인젝션을 사용하는 Vanquish 등은 SOFTWARE 에서 감지할 수 있다. (Dolan-Gavitt, 2007; Walters, 2006)

HKLM 의 HARDWARE 는 대응하는 하이브 파일이 없고, 컴퓨터 부팅시 윈도우 커널이 하드웨어 디바이스에 관한 정보를 읽은 후 구성한다. 따라서 오프라인 상에서는 이에 대한 조사가 불가능하나, Derived key 는 아니다.

```
C:\Documents and Settings\Forza>cd %systemroot%\system32\config
C:\WINDOWS\system32\config>ls
AppEvent.Evt  OSession.evt  SECURITY.LOG  system          userdiff
default       SAM           software     system.LOG      userdiff.LOG
default.LOG   SAM.LOG       software.LOG  system.sav
default.sav   SecEvent.Evt  software.sav  systemprofile
ODiag.evt     SECURITY      SysEvent.Evt TempKey.LOG
```

그림 2. HKLM의 4가지 Hive File 및 HKU의 Default Hive File

### 2-4.4. HKEY\_USERS 의 2가지 Hive File

HKEY\_USERS 의 DEFAULT, SID 는 하이브 파일이 존재한다.

**DEFAULT** 의 하이브 파일은 %systemroot%\system32\config\ 에 default 란 파일 형태로 존재한다.

**SID** 의 하이브 파일은 사용자별 home 폴더에 있다. 위치는 OS 별로 다르다.

(Windows XP) c:\users\wid\ntuser.dat,

(Windows Vista) c:\documents and settings\Administrator\ntuser.dat

```
C:\Documents and Settings\Forza>ls
?? ??      Favorites      NetHood        paros          Templates
?? ??      InstallAnywhere NTUSER.DAT     PrintHood     UserData
Application Data Local Settings  ntuser.dat.LOG Recent
Cookies     My Documents    ntuser.ini     SendTo
```

그림 3. NTUSER.DAT in Windows Vista

### 3. 레지스트리를 로그로 활용하기

모든 레지스트리 키는 LastWrite time 이라는 시간정보를 저장하고 있다. 이는 파일의 마지막 수정 시각과 매우 유사한 개념으로서, 해당 레지스트리키가 언제 마지막으로 수정되었는지를 FILETIME 구조체로 저장한다. Microsoft Knowledge Base 에 따르면, FILETIME 구조체는 1601-01-01 를 기점으로 100 나노초 단위로 시각을 표시한다고 한다. LastWrite time 은 레지스트리 키가 생성되거나 수정, 접근, 혹은 삭제될 경우에 업데이트된다. 이 때 LastWrite time 은 아쉽게도, 레지스트리 값(Value)이 아닌 레지스트리 키(Key)에 대한 시각 정보만 얻을 수 있다.

LastWrite time 분석 툴로는, Windwos Forensics and Incident Recovery 의 저자 Harlan Carvey 가 언급한 바 있는 Keytime.exe (<http://www.windowsir.com/tools.html>) 가 있다.

레지스트리 키의 LastWrite time 은, 포렌식 전문가에게 어떤 이벤트 발생의 대략적인 날짜와 시각 정보를 알려준다. 그러나 키의 last time 을 알더라도, 실제로 어떤 레지스트리 값이 변경되었는지를 아는 것은 어려운 일이다. 레지스트리를 훌륭한 로그로 활용하기 위해서는 레지스트리 키의 LastWrite time 과 함께 해당 파일시스템에서 발견한 MAC(modified, accessed, or created) time 등 다른 정보를 함께 조합하여 분석하는 능력이 필요하다.

### 3-1. Offline System 레지스트리의 LastWrite time 확인 (Encase 이용)

디스크 이미지는 레지스트리가 남아있지 않다. 레지스트리는 메모리상에 존재하기 때문이다. 레지스트리 편집기에서 보는 것은 메모리상의 데이터이며, 따라서 Live System 이 아닌 경우 디스크 상에는 하이브 파일밖에 없으므로, 하이브 파일을 찾는 것이 절대적으로 중요하다.

#### 3-1.1. 원하는 레지스트리에 해당하는 Hive File 을 찾아간다.

eg. HKLM-SOFTWARE : %systemroot%\system32\config\software 에 위치

#### 3-1.2. 해당 경로로 찾아가서 오른쪽 버튼 - View File Structure

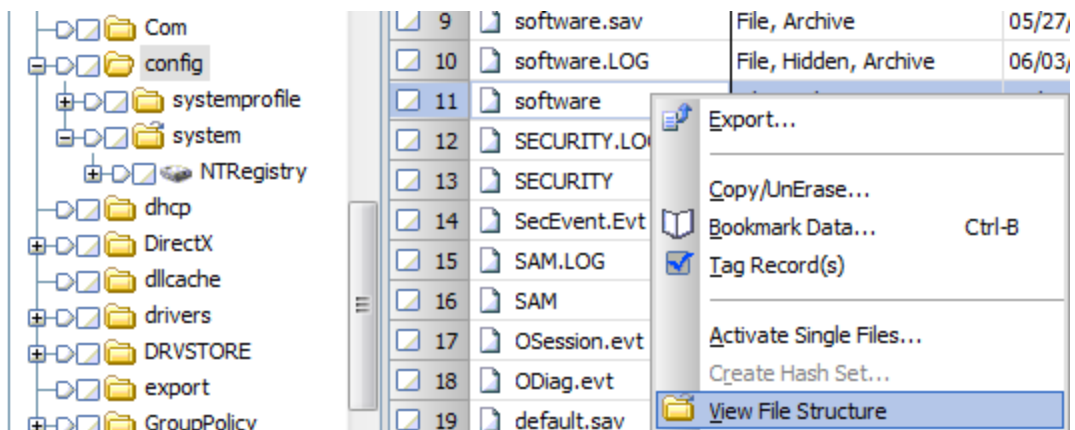


그림 4. SOFTWARE 하이브 파일을 마운트하여 레지스트리로 분석

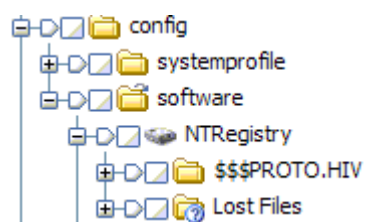
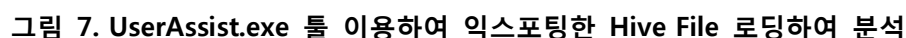
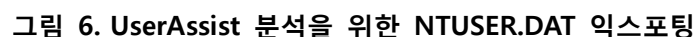


그림 5. 마운트 후 레지스트리로 보이는 모습

#### 3-1.3. Hive File 익스포팅 후 별도의 툴 활용하기

eg. UserAssist 툴을 활용하여 분석하기

Encase에서 UserAssist Key를 분석하기 위해서는 Enscript를 개발하여 사용해야 한다. 대안으로 하이브 파일을 직접 익스포팅한 후 별도의 툴(UserAssist.exe)을 이용하여 분석할 수 있다. UserAssist의 경우, Key, Index, Name, Session, Count, LastWrite time 등의 정보 분석이 가능하다.





## 3-2. 어플리케이션 관련 최근 사용 흔적

### 3-2.1. 최근 실행 목록(MRU lists, most recently used)

최근 실행 목록은 사용자의 구체적인 작업들로 인해 생성된 엔트리들을 포함하며, 사용자가 후에 이러한 목록을 다시 호출할 것을 대비하여 다양한 레지스트리 키에 보관된다. 이는 웹 브라우저에서 히스토리나 쿠키의 역할과 유사하다고 보면 되겠다.

하나의 예를 들자면, 레지스트리에 위치한 최근 실행 목록 중 하나는 RunMRU 키이다. 사용자가 실행창에 명령어를 입력하면, 해당 엔트리는 이 레지스트리 키에 추가된다. 이 키의 위치는 HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU이다. 실행창을 통해 실행된 어플리케이션이 그 실행순서대로 MRUList의 데이터 필드에 기록된다. 이를 통해 마지막으로 입력된 명령어를 알 수 있으며, RunMRU 키의 LastWrite time 을 통해 마지막으로 실행된 어플리케이션의 시각 정보를 얻을 수 있다. RunMRU 키로부터 사용자가 무슨 어플리케이션을 이용했는지, 언제 이용했는지 등의 정보를 이용할 수 있게 된 것이다. 예를 들어, 그림 8과 같은 경우 실행한 어플리케이션들(msconfig, cmd, sysedit, regedit 등)을 보면, 사용자가 Windows 운영체제에 대해 많은 지식이 있음을 추측할 수 있다.

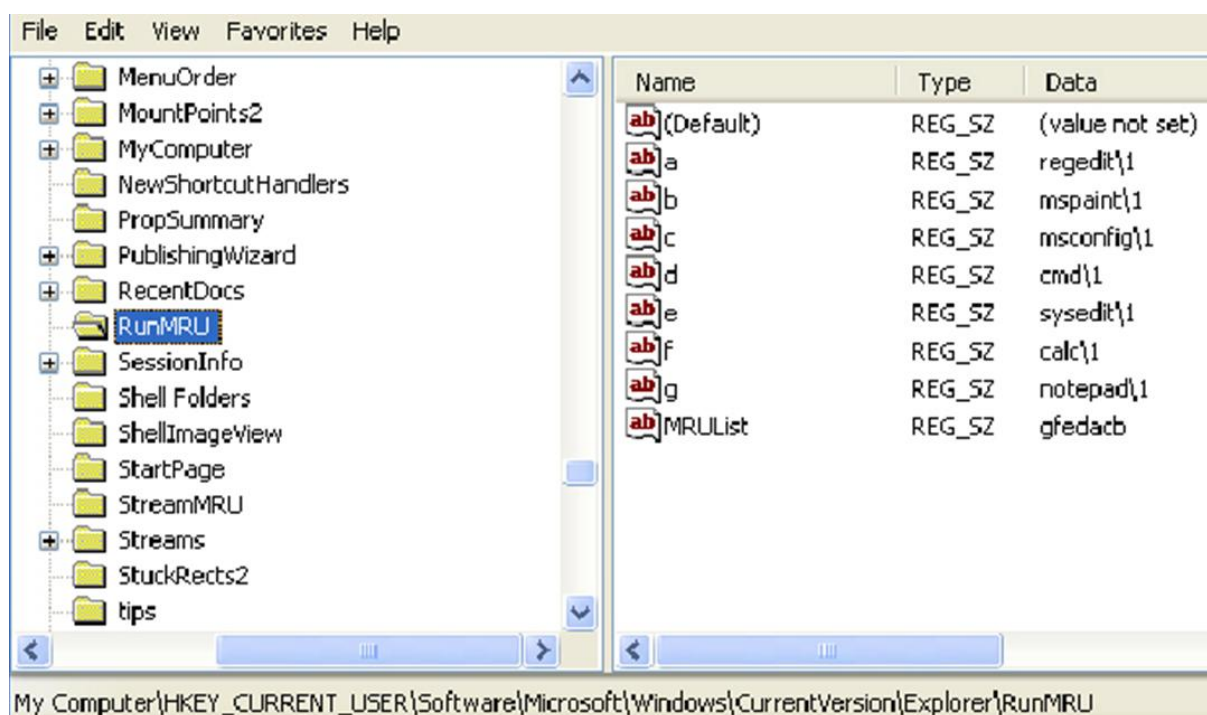


그림 8 . RunMRU Key



다음은 조사에 활용할 만한 MRU lists의 목록이다.

(참고 : <http://windowsxp.mvps.org/RegistryMRU.htm>)

XP 검색 폴더 및 파일	HKCU\Software\Microsoft\Search Assistant\ACMRU\5603
인터넷 검색 도구	HKCU\Software\Microsoft\Search Assistant\ACMRU\5001
프린터, 컴퓨터, 사람	HKCU\Software\Microsoft\Search Assistant\ACMRU\5647
파일 내 검색어	HKCU\Software\Microsoft\Search Assistant\ACMRU\5604
XP 시작메뉴-최근문서	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
R. Desktop - Connect	HKCU\Software\Microsoft\Terminal Server Client\Default [MRUnumber]
Run dialog box	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Regedit - Last accessed key	HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
Regedit- Favorites	HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites
MSPaint - Recent Files	HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
Mapped Network Drives	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
Computer searched via Windows Explorer	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FindComputerMRU
워드패드 - 최근에 사용한 파일	HKCU\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List
MRU – Last Visited	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU Windows 에서 가장 최근 열어본 어플리케이션과 파일 이름의 목록 저장
MRU – Open Saved	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU Windows 에서 가장 최근에 복사되거나 저장된 파일 이름과 경로들의 목록 저장
WMP XP-Recent Files	HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList
WMP XP-Recent URLs	HKCU\Software\Microsoft\MediaPlayer\Player\RecentURLList
Outlook Express – 최근 첨부 파일	HKCU\Software\Microsoft\Office\version\Common\Open Find\Microsoft Office Outlook\Settings\Save As\File Name MRU
MS 파워포인트 - 최근 문서	HKCU\Software\Microsoft\Office\version\PowerPoint\Recent File List HKCU\Software\Microsoft\Office\version\Common\Open Find\Microsoft PowerPoint\Settings\Open\File Name MRU HKCU\Software\Microsoft\Office\version\Common\Open Find\Microsoft PowerPoint\Settings\Save As\File Name MRU
Access - Filename MRU	HKCU\Software\Microsoft\Office\version\Common\Open Find\Microsoft Access\Settings\File New Database\File Name MRU
Publisher – 최근 문서	HKCU\Software\Microsoft\Office\version\Common\Open Find\Microsoft Office Publisher\Settings\Save As\File Name MRU

<b>FrontPage - Recent lists</b>	HKCU\Software\Microsoft\FrontPage\Explorer\FrontPage Explorer\Recent File List
<b>MS Excel - 최근 문서</b>	HKCU\Software\Microsoft\Office\version\Common\Open Find\Microsoft Office Excel\Settings\Save As\File Name MRU
<b>MS Word - 최근 문서</b>	HKCU\Software\Microsoft\Office\version\Word\Data
<b>MS Word - 사용자정보</b>	HKCU\Software\Microsoft\Office\version\Common\UserInfo Microsoft Office 를 설치할 때 입력한 사용자 정보 확인
<b>한글 - 최근 문서</b>	HKCU\Software\HNC\HWP\Recent File List HKCU\Software\HNC\Hwp\File Dialog\Recent Folder List
<b>Adobe Reader - Recent Files</b>	/HKCU/Software/Adobe/Acrobat Reader/version/avgeneral/crecentfiles c1, c2, c3 등으로 되어 있음
<b>구글 검색 히스토리</b>	HKCU\Software\Google\NavClient\1.1\History 인터넷 익스플로러 task bar 에 구글이 포함되어 있다면, 날짜와 시각 정보와 함께 검색 용어 목록이 저장된다.
<b>윈도우 미디어 플레이어 - 재생목록</b>	HKCU\Software\Microsoft\MediaPlayer\Player\RecentFileList
<b>WinZip - Extracted files</b>	HKCU\Software\Nico Mak Computing\FileMenu WinZip 으로 압축을 푼 파일들의 목록을 저장한다.
<b>파일 확장자 정보</b>	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\EXT type 실행된 적 있는 확장자 정보 목록(해당 파일을 열어본 실행 프로그램 정보 등)
<b>ShellBags</b>	HKCU\Software\Microsoft\Windows\Shell\BagMRU 링크 히스토리나 파일/폴더의 정보 등을 저장한다. size 변경으로 저장개수 설정가능.

### 3-2.2. 최근 삭제한 목록

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall 의 서브키에는 컴퓨터에서 설치된 프로그램이 모두 표시된다. 대부분 제어판의 프로그램 추가/삭제의 리스트와 일치하나, 장치 드라이버나 Windows 패치와 같은 프로그램의 경우에는 이 서브키에서만 확인 가능하다. 각각의 서브키는 대개 Display Name (프로그램명)과 UninstallString(어플리케이션 Uninstall 파일 경로) 두 레지스트리 값을 지닌다. 이 밖에도 설치 날짜나 설치 소스, 어플리케이션 버전과 같은 정보를 포함한 레지스트리 값들이 존재할 수 있다. (Wong, Lih Wern, 2007)

### 3-2.3. 특정 파일, 어플리케이션의 사용자 접근

UserAssist 키는 HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist 에 위치하며, GUIDs(globallyunique identifiers)로 보이는 긴 16 진수 이름을 가진 2 개의 서브키를 가진다. (IE 7 설치시 한 개의 subkey 가 추

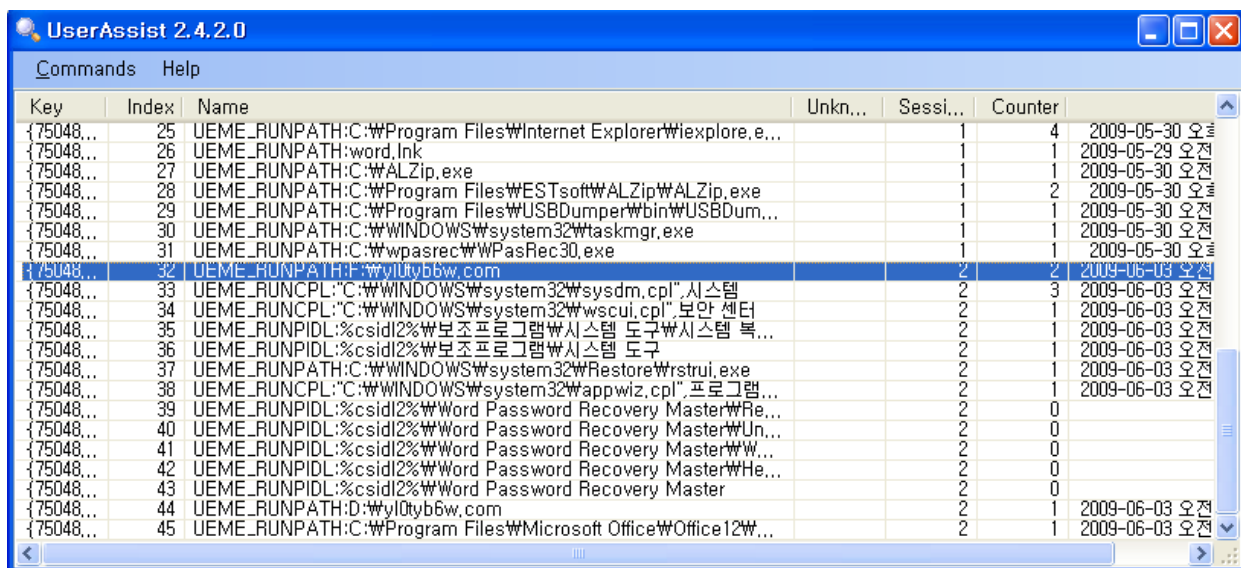
가 생성된다.) 각각의 서브키는 사용자가 그 시스템에서 허용된 특정 Object 에 딸린 값을 기록한다. 예를 들면, 제어판이나 바로가기 파일, 프로그램과 같은 것들이다. 이러한 값들은 ROT-13 (Caesar cipher) 방식으로 인코딩되어 있다.

특정 파일이나 어플리케이션에 사용자의 접근이 있었는지 유무를 알 수 있으며, 악의적인 프로그램을 설치 & 실행 후 삭제해도 레지스트리에 남은 실행 흔적을 발견할 수 있다. 범죄자가 특정파일을 제거하고 조각모음을 실행해도 레지스트리에는 해당파일을 읽었던 기록이 남게 되므로 중요한 증거가 될 수 있다.

다음은 ROT-13 으로 인코딩되어 있는 서브키를 디코딩한 결과이다.

- i. 5E6AB780-7743-11CF-A12B-00AA004AE837  
➔ Internet Toolbar (%SystemRoot%\System32\Browseui.dll)
- ii. 75048700-EF1F-11D0-9888-006097DEACF9  
➔ ActiveDesktop (%SystemRoot%\System32\SHELL32.dll)
- iii. 0D6D4F41-2994-4BA0-8FEF-620E43CD2812  
➔ 추가생성된 subkey (Support for the IE7 UserAssist GUID key)  
IE Microsoft Internet Toolbar (%SystemRoot%\system32\wiefame.dll)

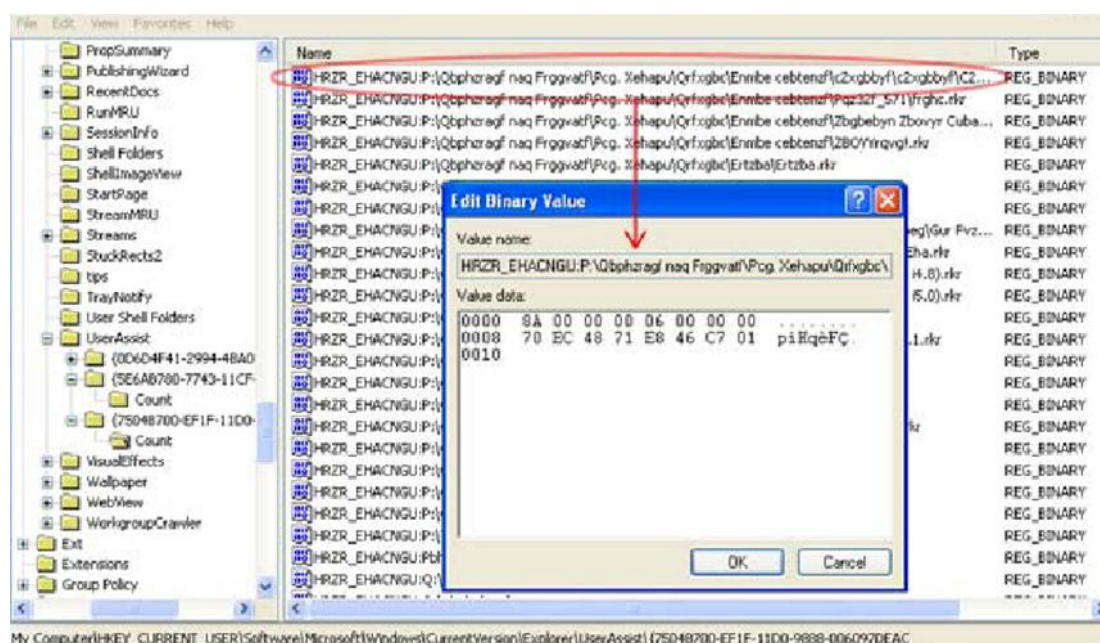
UserAssist 라는 별도의 툴을 이용하여 ROT13 으로 인코딩 된 정보를 디코딩 하여 목록을 볼 수 있다. 이 때, Counter 가 한 두번에 그치는 것들 중 악성코드 Dropper 가 있을 수 있으므로 의심해 볼 수 있으며, LastWrite time 을 통해 해당 어플리케이션이나 특정 파일의 마지막 접근 시각을 추정할 수 있다.



Key	Index	Name	Unkn...	Sessi...	Counter	
{75048...}	25	UEME_RUNPATH:C:\Program Files\Internet Explorer\explore.e...		1	4	2009-05-30 오전
{75048...}	26	UEME_RUNPATH:word.lnk		1	1	2009-05-29 오전
{75048...}	27	UEME_RUNPATH:C:\ALZip.exe		1	1	2009-05-30 오전
{75048...}	28	UEME_RUNPATH:C:\Program Files\ESTsoft\ALZip\ALZip.exe		1	2	2009-05-30 오전
{75048...}	29	UEME_RUNPATH:C:\Program Files\USB Dumper\bin\USB Dum...		1	1	2009-05-30 오전
{75048...}	30	UEME_RUNPATH:C:\WINDOWS\system32\taskmgr.exe		1	1	2009-05-30 오전
{75048...}	31	UEME_RUNPATH:C:\wpasrec\WPasRec30.exe		1	1	2009-05-30 오전
{75048...}	32	UEME_RUNPATH:F:\wyl0tyb6w.com		2	2	2009-06-03 오전
{75048...}	33	UEME_RUNCPPL:"C:\WINDOWS\system32\sysdm.cpl", 시스템		2	3	2009-06-03 오전
{75048...}	34	UEME_RUNCPPL:"C:\WINDOWS\system32\wscui.cpl", 보안 센터		2	1	2009-06-03 오전
{75048...}	35	UEME_RUNPIDL:%csidl2%\보조프로그램\시스템 도구\시스템 특...		2	1	2009-06-03 오전
{75048...}	36	UEME_RUNPIDL:%csidl2%\보조프로그램\시스템 도구		2	1	2009-06-03 오전
{75048...}	37	UEME_RUNPATH:C:\WINDOWS\system32\Restore\wstrui.exe		2	1	2009-06-03 오전
{75048...}	38	UEME_RUNCPPL:"C:\WINDOWS\system32\appwiz.cpl", 프로그램...		2	1	2009-06-03 오전
{75048...}	39	UEME_RUNPIDL:%csidl2%\Word Password Recovery Master\Re...		2	0	
{75048...}	40	UEME_RUNPIDL:%csidl2%\Word Password Recovery Master\Un...		2	0	
{75048...}	41	UEME_RUNPIDL:%csidl2%\Word Password Recovery Master\W...		2	0	
{75048...}	42	UEME_RUNPIDL:%csidl2%\Word Password Recovery Master\He...		2	0	
{75048...}	43	UEME_RUNPIDL:%csidl2%\Word Password Recovery Master		2	0	
{75048...}	44	UEME_RUNPATH:D:\wyl0tyb6w.com		2	1	2009-06-03 오전
{75048...}	45	UEME_RUNPATH:C:\Program Files\Microsoft Office\Office12\W...		2	1	2009-06-03 오전

그림 9. UserAssist Program 실행 모습

이러한 엔트리들이 구체적인 날짜와 시각 정보와는 연계되어 있지 않아 결정적이지 않더라도, 사용자의 특정 행동들을 추론하게 해주기 때문에 훌륭한 증거가 될 수 있다. 그림 10과 10-a의 디코딩한 값에서 잠재된 정보를 찾아보자. 먼저, exe 파일이 실행된 사용자 폴더를 통해 사용자의 프로필 중 이름을 알 수 있다. 또한 실행된 파일을 찾아봄을 통해 어떤 작업을 하려던 것이었는지 유추가 가능하며 이는 보다 심층적인 분석을 가능하게 해준다. 또한 같은 폴더에 다른 작업 결과들이 남아있지 않은지 확인 가능하다. (Derrick J. Farmer, 2008)



### 그림 10. UsrerAssist Key

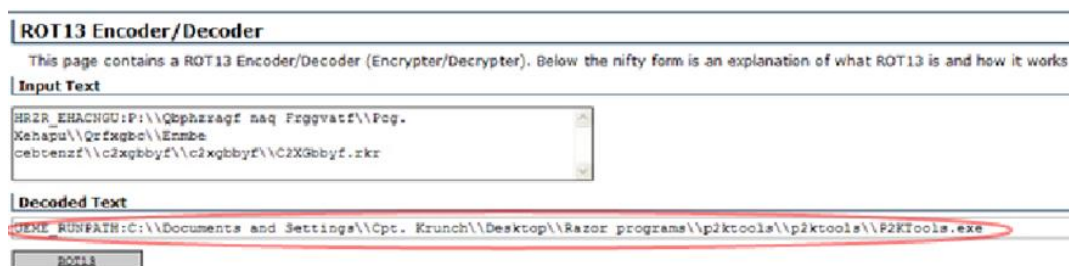


그림 10-a. ROT-13 디코딩한 결과

### 3-3. 시스템 정보

#### 3-3.1. USB 장치 (USB Memory, PDA, 핸드폰 등)

어떤 장치든 USB(Universal Serial Bus)에 연결하면, 드라이버를 비롯한 장치 정보가 레지스트리(eg. thumb drives)에 저장된다.

HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR에는 해당 시스템에 연결된 적이 있는 모든 USB 장치의 생산자와 ID 값 등이 기록되어 있다. 그림 11을 보면, ipod과 두 개의 외장 하드 드라이브, 디지털 비디오 캠코더, 그리고 여러 다른 종류의 thumb 드라이브 목록을 볼 수 있다.

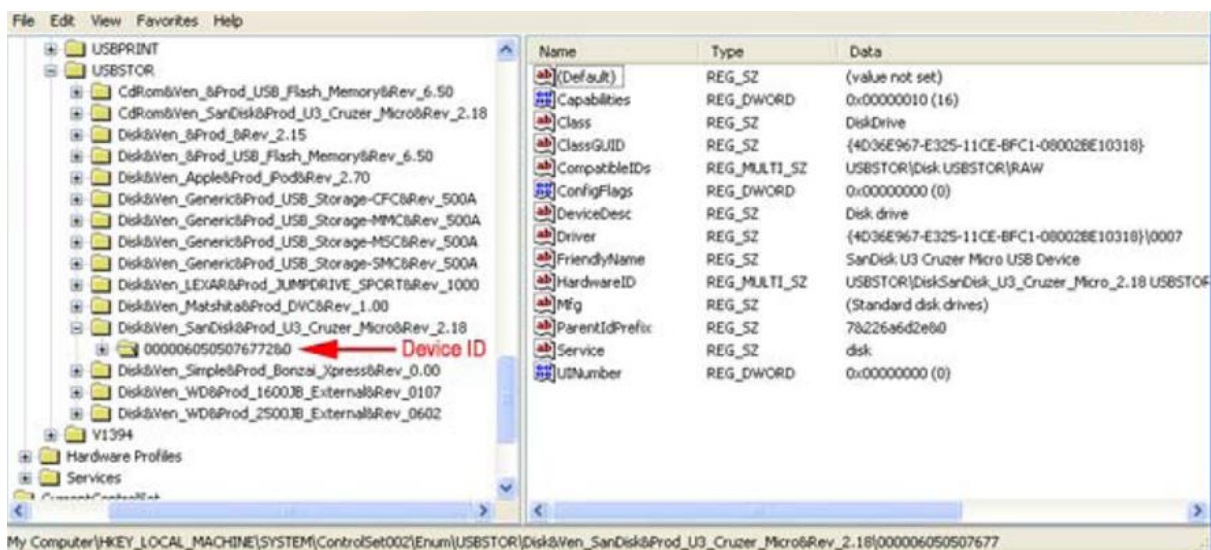


그림 11. USBSTOR Key

서브키는 보통, Disk & Vendor\_XXX & Product\_XXX & Revision\_XXX으로 구성되고, XXX 부분은 PNP Manager가 Device Descriptor에서 가져온다. 하위 키를 보면 많은 숫자와 기호를 볼 수 있는데, 이는 네트워크 인터페이스 카드의 MAC 주소와 같이 생산자에 의해 특정된 값이다. UsbDrive 제조사 유니크한 Serial 번호를 플래시롬에 설정하여 생산하면, MS로부터 Windows Logo(인증)을 부여받는다. 따라서 이 Serial 번호를 통해, 특정 USB 장치를 타 Windows 시스템에 연결한 적이 있는지 그 여부를 확인가능하다. 그러나 모든 thumb drive가 device ID를 갖지는 않는다. 예를 들어 저가형 중국산 벌크 제품의 경우는 정식 device ID를 가지고 있지 않아, PnP Manager에서 임시로 시리얼번호를 자동 부여한다. 이를 Instance ID라고 하는데, 2번째 위치에 & 기호가 있는 것이 특징이다. (eg. 6&26c97b61&d)

유니크한 시리얼 번호가 있을 경우 해당 드라이브는 100% 연결된 것이 확실하다고 볼 수 있으며, Instance ID (&) 로 생성된 Drive 는 연결되긴 했으나 정확히



누구의 것인지는 알 수 없고, 해당 USB 의 MAC 타임을 조사하여 사고조사에 유용하게 사용할 수 있다.

USB 장치의 사용 시각은 Instance ID와 ParentIdPrefix 값에 등록된 USB Key의 Lastwrite time을 통해 추정가능하다. 시각은 HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses에 정의되어 있다. 로그를 확인하여, 이 2개의 서브키에 등록된 USB 키의 LastWrite time(마지막 쓴 시간)을 통하여 USB 저장 장치가 장착된 시각을 확인할 수 있다.

InstanceID : 53f56307-b6bf-11d0-94f2-00a0c91efb8b

ParentIdPrefix : 53f5630d-b6bf-11d0-94f2-00a0c91efb8b

키 이름:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
DeviceClasses\{53F56307-b6bf-11d0-94f2-
00a0c91efb8b}\##?
#USBSTOR#Disk&Ven_BMKT&Prod_MemoRive&Rev_1.00#20080
040000000000000360&0#{53F56307-b6bf-11d0-94f2-
00a0c91efb8b}\##
```

클래스 이름: <클래스 없음>

마지막 쓴 시간: 2009-06-10 - 오후 10:27

그림 12. setupapi.log 에서 해당 USB LastWrite time 확인

USB 장치 관련 로그는 (Windows XP) %systemroot%\WINDOWS\setupapi.log, (Windows Vista) %systemroot%\WINDOWS\setupapi.dev.log 에 저장된다. setupapi.log파일은 Windows XP 로부터 만들어진 파일로, 이 파일 안에는 사용자가 윈도우 설치 후, 설치하고 삭제한 장치들에 관하여 상세하게 기록되어 있다. 지금까지의 USB를 확인하려면, 찾기 옵션을 사용하여 '대용량 저장소'나 'USB\UID\_'와 같이 검색하면 된다. 또한, 특정한 하나의 USB 저장 장치를 특정하기 위해서는, ParentIdPrefix를 이용하여 검색하는 것이 도움이 된다.

### 3-3.2. 마운트한 장치들

시스템과 연결한 적이 있는 모든 드라이브를 볼 수 있는 레지스트리 키가 있다. HKLM\SYSTEM\MountedDevices 이며, NTFS 파일 시스템에 의해 사용된 적이 있는 마운트된 볼륨들의 데이터베이스를 저장하고 있다. 각각의 \DosDevices\X: 값들은 해당 볼륨을 인식하기 위한 정보들을 이진 데이터 형태로 저장한다. 그림 13을 보면, STORAGE Removable Media 라고 적힌 정보를 볼 수 있다. 이 정보는 디지털 포렌식 조사관에게 시스템에 연결했던 하드웨어 장치를 보여주므로 유용한 단서가 될 수 있다. 만약 MountedDevices 목록에는 존재하나 현재 시스템에 연결되어 있지 않은 하드웨어 장치가 있다면, 사용자가 증거를 은닉하기 위해 감춘 것으로 추측해볼 수 있을 것이다. 이러한 경우, 조사관은 추가적인 증거를 찾으려는 노력을 해볼 수 있겠다. (Lih WernWong, 2007)

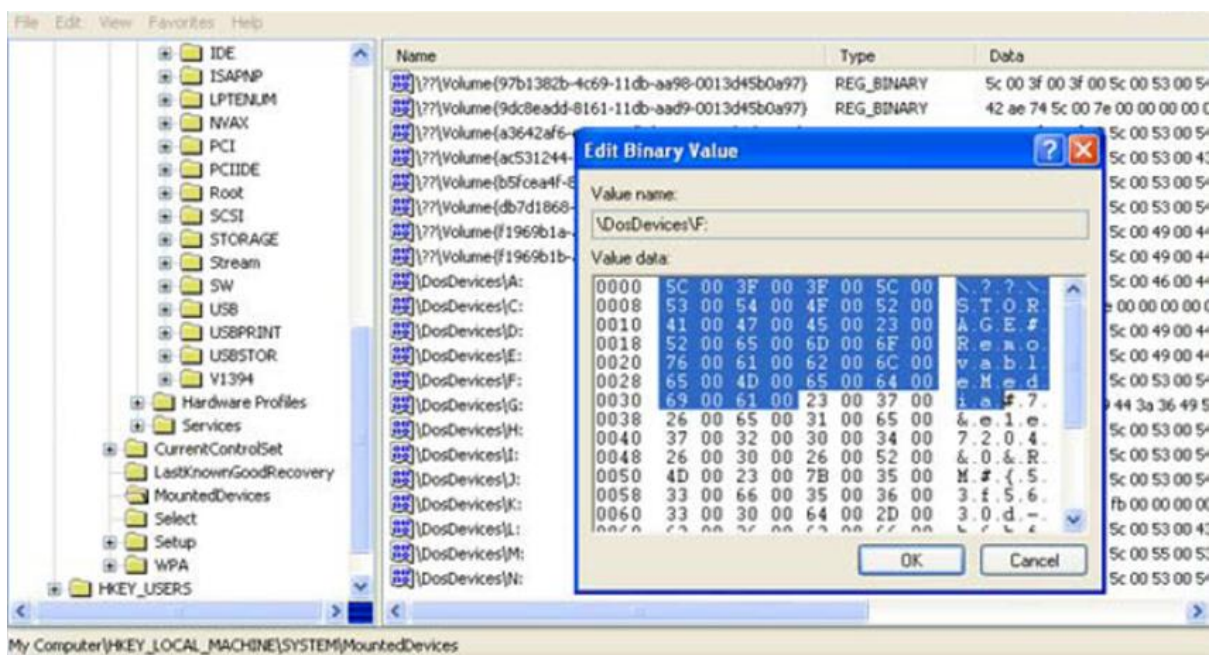


그림 13. \DosDevices\F: 볼륨 정보

### 3-3.3. 기타 포렌식 관점으로 주시할 사항

시스템 속성에 정의된 컴퓨터 이름 목록

HKLM\System\CurrentControlSet\Control\ComputerName

최근 시스템에 마운트한 동적 디스크 정보

HKLM\System\ControlsetXXX\Services\DMIO\Boot Info\Primary Disk Group

운영체제가 설치된 날짜, 버전, Product ID, 등록된 사용자 등 정보

HKLM\Software\Microsoft\Windows NT\CurrentVersion

시스템 종료 시각

HKLM\System\ControlSetXXX\Control\Windows

Time Zone (설치 후 수정 가능)

HKLM\System\ControlSet001(002)\Control\TimeZoneInformation\StandardName

시스템에 마지막 로그인한 사용자 정보 (도메인, 사용자 계정)

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

마지막 로그인, 계정 비밀번호 수정, 계정 만료, 로그인 실패 시각

HKLM\SAM\Domains\Account\Users\F key

사용자 이름과 SID

HKLM\SAM\Domains\Account\Users\V key

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList



### 3-4. 네트워크

#### 3-4.1. 무선 네트워크

무선 네트워크의 사용은 날로 증가하고 있는 추세이다. 무선 이더넷 카드는 해당 범위 내에서 SSID(service set identifier)로 인증이 허용된 지점(Access Point)을 찾아 접속한다. 이렇게 네트워크에 접속할 때, SSID는 Windows XP에 레지스트리 키 값으로 로그가 남게 된다. HKLM\Software\Microsoft\WZCSVC\Parameters\Interfaces key 에 위치한다.

이 레지스트리 키 안에는, GUIDs를 가지는 UserAssist 처럼 보이는 서브키들이 있으며 각각 Active Settings나 Static#0000과 같은 값(Value)들을 저장하고 있다. 이 중 Static\$ value들은 해당 시스템이 접속한 바 있는 모든 무선 네트워크의 Access point의 SSIDs를 저장한다. 오른쪽 버튼을 클릭하여 이 값들을 보거나 수정 가능하다. (Derrick J. Farmer, 2008)

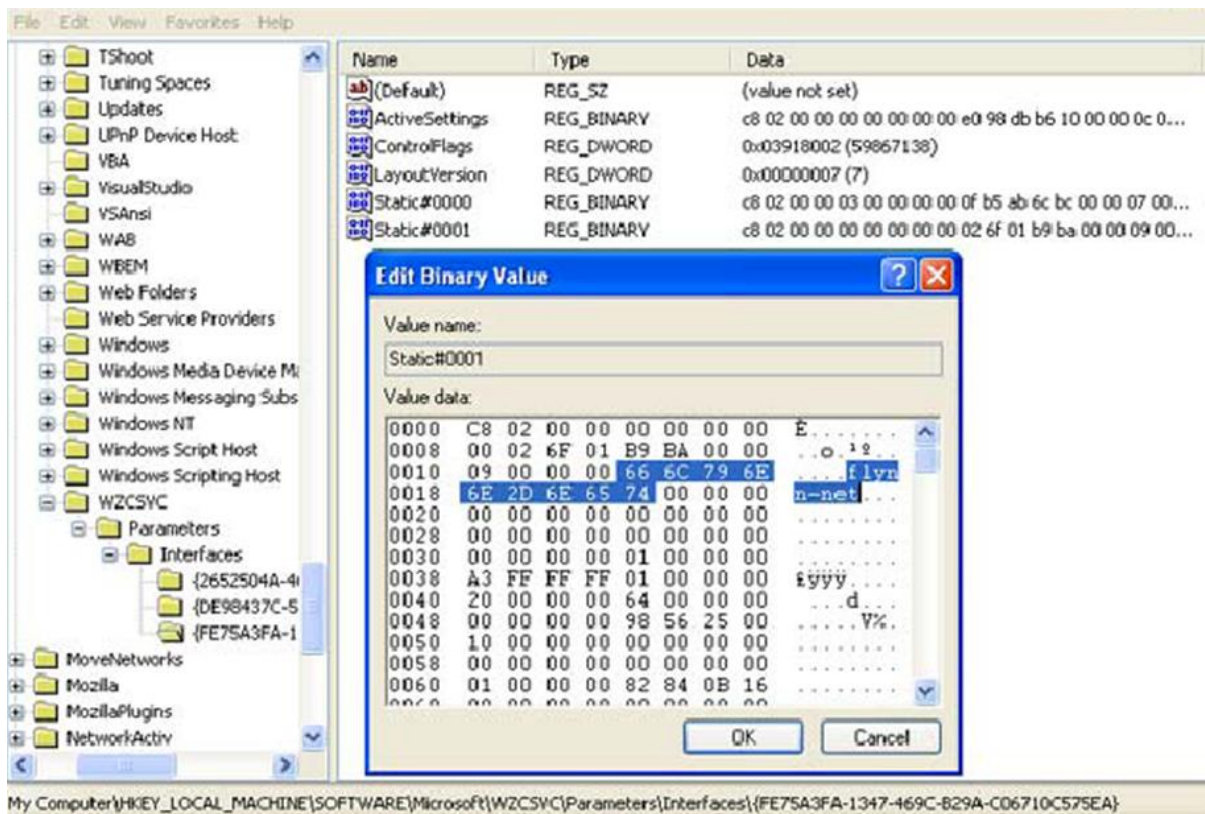


그림 14. SSID flynn-net

SSID 이름을 저장하고 있는 외에도, Windows는 특정 연결에 대한 네트워크 설정 정보(IP 주소, DHCP 도메인, 서브넷 마스크 등)도 기록한다. HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\에 위치한다.

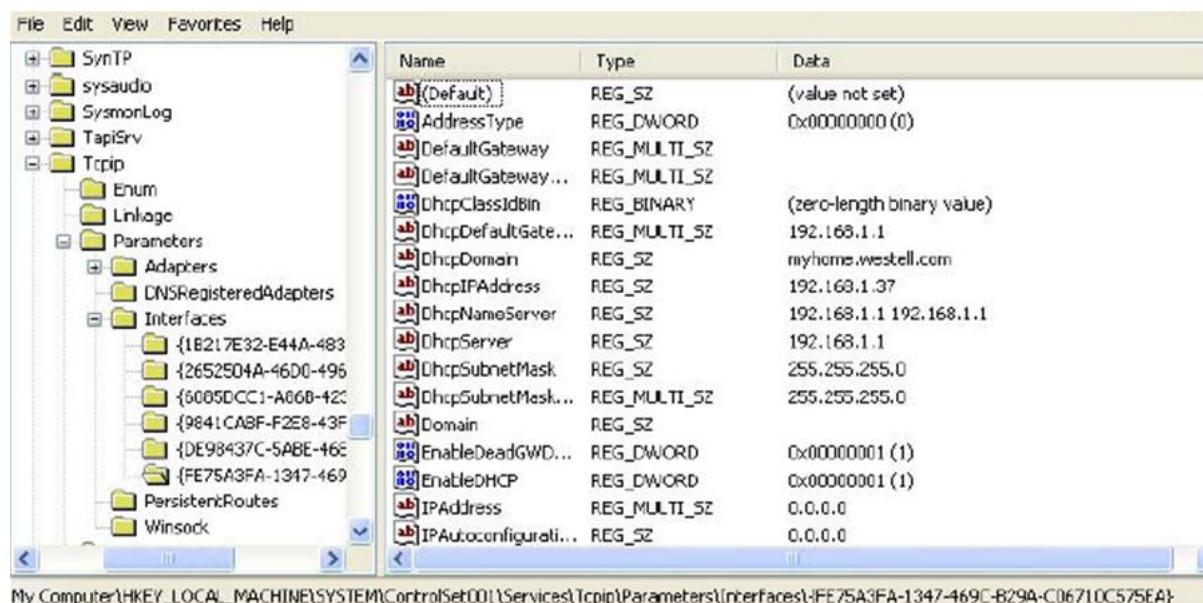


그림 14-a. SSID "flynn-net"의 네트워크 설정

무선 네트워크 정보에 기반하여, 포렌식 조사관은 사용자가 특정 무선 Access Point에 접근한적이 있는지, DHCP 서버에 의해 사용자의 IP가 인증받은 바 있는지 등을 알아낼 수 있게 된다. 이는 War-driving으로 여러 네트워크에 연결하며 불법적으로 인터넷을 사용한 용의자를 검거하기 위한 유용한 수단이 될 수 있다. 용의자 컴퓨터에서 어떤 네트워크에 연결하였는지를 알 수 있고, 이후 ISP에 대한 영장을 발부받아 사용한 바 있는 IP 주소를 확인 가능하다.

### 3-4.2. 로컬 네트워크

Windows XP는 내 네트워크 환경이라고 하는 네트워크 매핑 툴을 제공한다. 이를 통해 Local Area Network에 있는 다른 사용자를 쉽게 확인할 수 있다. 이 역시 레지스트리에 저장되기 때문에, 사용자가 LAN에 얼마 접속하지 않았더라도 그 장치들(데스크톱 컴퓨터, 노트북, 프린터 등)의 목록은 남아있게 된다. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions 에 위치한다. ComputerDescription 키는 특정 LAN 또는 특정 컴퓨터에 접속한 적이 있는지 그 여부를 조사하는데 매우 유용할 수 있다.

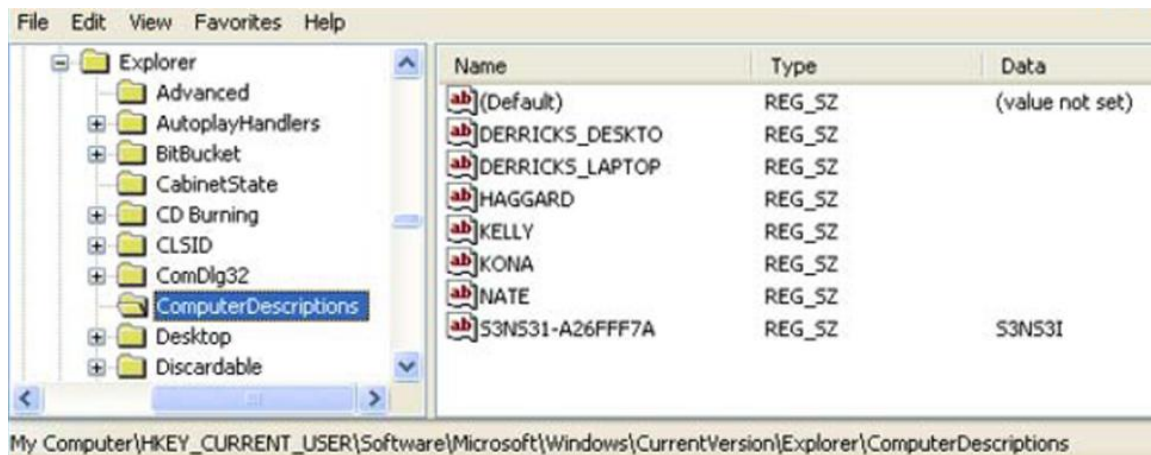


그림 15. ComputerDescription key : LAN 내 컴퓨터 목록

### 3-4.3. Intelliforms(자동완성기능)

HKCU\Software\Microsoft\Protected Storage System Provider 키에 저장된다. Protected Storage는 Microsoft 프로그램들이 Autocomplete(자동완성) 기능을 위하여 개인 정보를 저장하는 공간을 제공하는데 사용되는 서비스이다. (Carvey, 2004) Protected Storage에 저장되는 정보는 MSN Messenger, Internet Explorer 등의 자동 로그인을 위한 계정 및 비밀번호이다. 포렌식 조사관에게 중요한 정보가 될 수 있는, 신용카드 번호 등의 정보도 저장된다.

이 키들을 보호하기 위하여 Microsoft는 레지스트리 엔트리들을 인코딩하여, 레지스트리 편집기는 관리자를 포함하여 사용자들이 이 레지스트리 키를 볼 수 없도록 하고 있다. Default 설정으로 시스템 계정만의 접근은 허용하고 있다. 그러나 PassView (NirSoft, 2004) 나 PSoreView (PSoreView, 2005) 와 같은 툴을 이용하면, Live system 에서 이를 디코딩하여 볼 수 있다. 또한 AccessData Registry Viewer (AccessData, 2005)는 오프라인 방식으로 서브키를 디코딩하고 접근할 수 있다. Windows Secret Explorer 는 Live system과 레지스트리 파일 모두에서 디코딩 기능을 제공한다.

### 3-4.4. 기타 포렌식 관점으로 주시할 사항

로컬 계정의 security ID 목록

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network

Drive MRU

최근 매핑한 네트워크 드라이브 목록

HKLM\Software\ControlSet\Control\Print\Printers

현재 시스템에 설정한 모든 프린터 목록과 정보

HKLM\Software\ControlSet\Control\Print\Environments\WindowsNTx86\

Drivers\Version...

현재 시스템의 도메인과 호스트네임 데이터 목록

HKLM\Software\ControlSet\Services\Tcpip\Parameters

현재 IP 주소와 게이트웨이 정보

HKLM\Software\ControlSet\Services\Tcpip\Parameters\

### 3-5. 웹 브라우저

#### 3-5.1. 인터넷 익스플로러

Internet Explorer 는 Windows 운영체제의 기본 웹 브라우저로서, 다른 어플리케이션처럼 레지스트리의 정보를 많이 이용한다. 정보는 HKCU\Software\Microsoft\Internet Explorer 키에 위치한다. 포렌식 관점에서 보기에 중요한 세가지 서브키가 존재하는데, 첫 번째는 HKCU\Software\Microsoft\Internet Explorer\Main이다. 이 키는 사용자의 인터넷 익스플로러 설정정보를 저장한다. 예를 들어, 검색 바, 시작 페이지, 브라우저 서식 설정 같은 것들이다. 두 번째로는 HKCU\Software\Microsoft\Internet Explorer\TypedURLs 키이다. 그림 16을 보자. 이 데이터로부터, 조사관은 사용자가 gmail과 hotmail 이메일 주소를 가지고 있고, tdbanknorth라는 온라인 बैं킹을 이용하며, 디지털 포렌식 웹사이트에 관심이 있고, 아마도 Champlain에 있는 대학을 다니고, 그 지역 아파트에 대해 알아보고 있다는 추측이 가능하다. (Derrick J. Farmer, 2008)

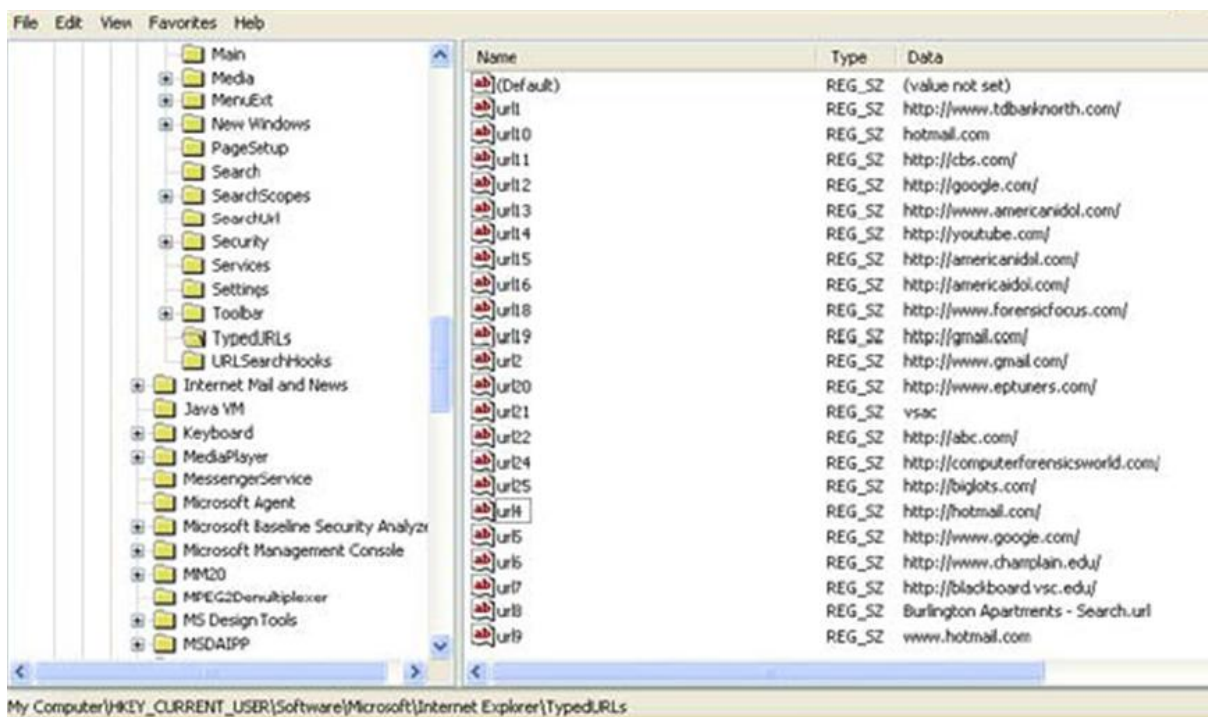


그림 16. TypedURLs Key

세번째 서브키는 HKCU\Software\Microsoft\Internet Explorer\Download Directory 이다. 이 키는 인터넷 익스플로러로부터 다운로드 받은 파일을 마지막으로 저장한 폴더를 보여준다. 조사관에게 사용자가 파일들을 어디에 저장하는지 알려주는 것이다.



이 밖에도 로그로 활용하기 위한 정보가 담겨있는 레지스트리 키에는  
 ₩Software₩Microsoft₩Protected Storage System Provider₩SID₩Internet Explorer₩Internet Explorer - URL:StringData 이 있다. Internet Explorer 자동 로그인 아이디와 비밀번호가 날짜, 시각 정보와 함께 저장되어 있다.  
 ₩Software₩Microsoft₩Protected Storage System Provider₩SID₩Internet Explorer₩Internet Explorer - q:StringIndex 에는 Internet Explorer 검색어가 날짜, 시각 정보와 함께 저장된다. ₩Software₩Microsoft₩Internet Explorer₩IntelliForms 에는 자동 완성 비밀번호 웹 페이지가 인코딩되어 저장된다.

### 3-5.2. Opera

Internet Explorer는 웹 히스토리를 Windows 레지스트리 데이터베이스를 참조하는 Index.dat라고 하는 파일로 저장한다. 따라서 우리는 TypedURLs 키에서 히스토리 내용을 볼 수 있었던 것이다. Opera는 이와 달리, opera.dir 이라는 파일로 히스토리를 저장한다. 파일의 디폴트 위치는 C:₩Documents and Settings ₩UserProfile₩Application Data₩Opera₩Opera₩profile₩ 이다. 이 브라우저를 설치하고 사용하자마자, 레지스트리에 남는 것은 install path 뿐이다. Opera의 Feature를 살펴보면(<http://operawiki.info/WhyOpera>) 이 브라우저를 선택하는 두 가지 큰 이유를 알 수 있다. 이 브라우저는 데이터를 저장하는데 레지스트리를 사용하지 않으며, 그 사이즈가 매우 작다는 것이다. 실행파일은 1.8 mb 정도이며, 제어판의 프로그램 추가삭제를 통해 살펴보면 총 용량이 5.33 mb에 그친다.

### 3-5.3. Netscape, FireFox

Opera처럼 Netscape와 Firefox도 레지스트리에 매우 적은 흔적만을 남긴다. 이들은 모두 웹 히스토리를 아스키 포맷으로 이루어져 바로 식별이 가능한 history.dat 파일에 저장한다. Firefox의 히스토리 파일의 위치는 C:₩Documents and Settings ₩User Profile₩Application Data₩Mozilla₩Firefox₩Profiles₩x.default 이며, Netscape는 C:₩Documents and Settings ₩derrick.farmer₩ Application Data ₩Netscape₩NSB₩Profiles₩x.default 이다. (Derrick J. Farmer, 2008)

### 3-6. P2P 클라이언트

P2P(Peer-to-Peer) 네트워크는 사용자들끼리 불법 프로그램이나 음란물 등을 공유하는 용도로 주로 사용되고 있다. P2P를 사용한 자가 누구인지, 무엇을 다운로드받고 업로드하였는지, 다운로드받은 파일은 어디에 저장되는지, 어떤 검색어를 사용하였는지 등을 확인할 수 있을 것이다. Limewire, Kazaa, Morpheus, ShareBox, FileZilla 등 유명한 P2P 클라이언트 및 웹하드 프로그램이 레지스트리에 남기는 정보에 대하여 알아보기로 한다.

#### 3-6.1. Limewire

사용자 작업에 대한 매우 적은 흔적만을 남기는데, 검색 로그나 다운로드한 파일에 대한 정보는 찾을 수 없다. 유용하다고 할 만한 레지스트리 정보는 install path 이다. 이 정보는 조사해야할 파일시스템이 어떤 것인지 정도를 알려줄 수 있겠다. Limewire의 기본 설치 주소는 C:\Program Files\Limewire 이며, 공유 폴더는 C:\Documents and Settings\User Profile\Shared 이다. (Derrick J. Farmer, 2008)

#### 3-6.2. Kazaa

Kazaa에서는 두 가지 의미있는 레지스트리 키를 발견할 수 있다. 첫 번째는 HKCU\Software\Kazaa 이다. 이는 검색을 용이하게 해주는 사용자 환경설정 정보를 담고 있다. 예를 들면, 성인정보 필터링과 같은 검색 결과 필터링 기능이 있다. 기본적으로 성인 정보 필터링이 설정되어 있으므로, 이 설정이 off 되어 있다면, 사용자가 Kazaa 옵션을 통해 바꾸었다는 것을 의미한다. 다른 서브키는 HKLM\Software\Kazaa 인데 연결정보와 다운로드한 파일의 저장 폴더 등을 기록한다. 기본 다운로드 폴더는 C:\Program Files\Kazaa\My Shared Folder 이다.

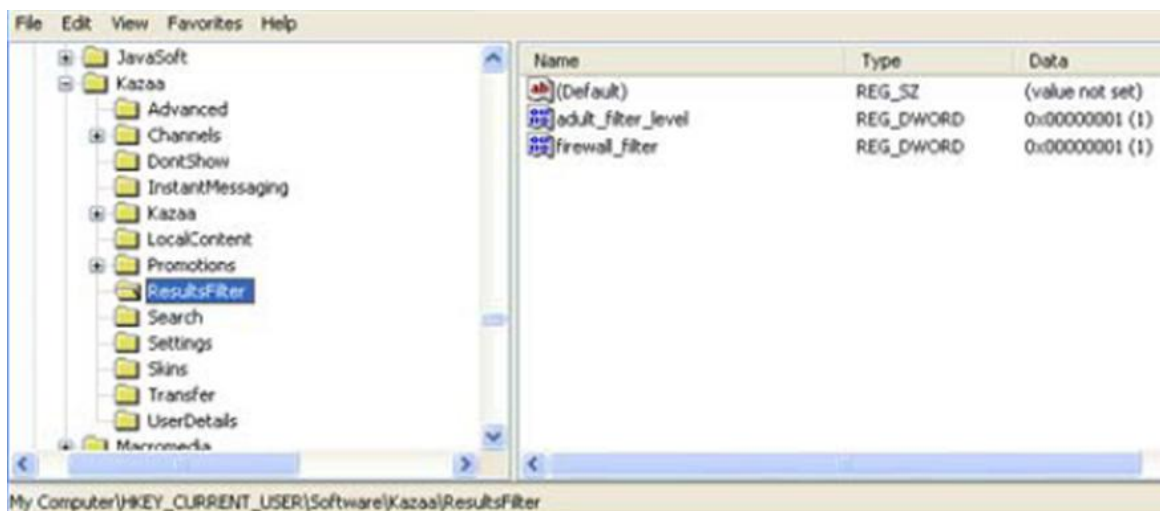


그림 17. Kazaa key

### 3-6.3. Morpheus

Morpheus는 레지스트리에 최근 검색 키워드 등을 기록한다. Morpheus를 통해 불법 콘텐츠를 다운로드했다고 의심되는 사용자를 심문할 때 유용한 정보가 될 수 있다. HKCU\Software\Morpheus\GUI\SearchRecent 키에 위치한다. (Derrick J. Farmer, 2008)

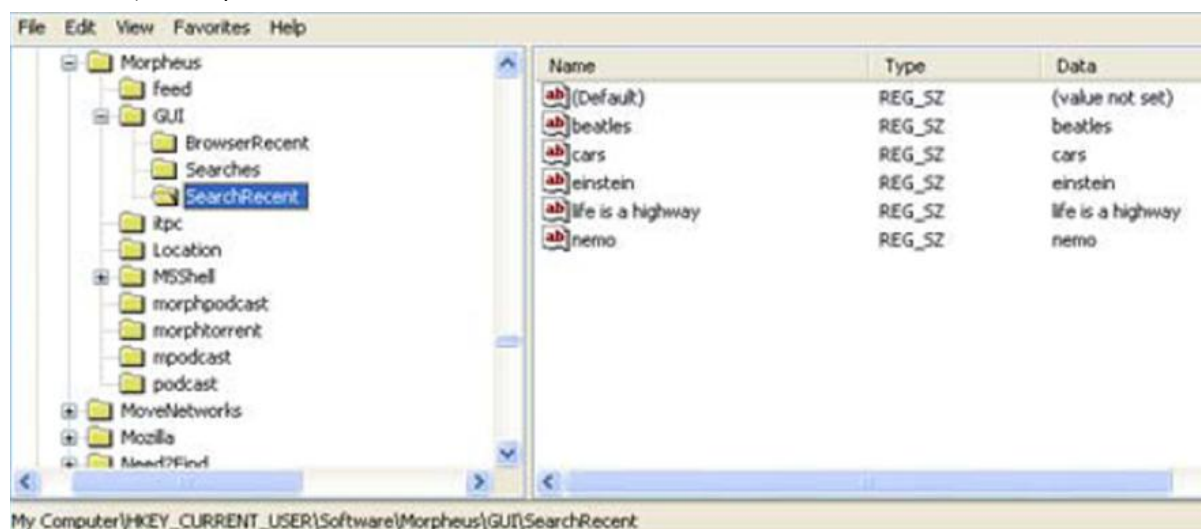


그림 18. Morpheus 최근 검색 목록

### 3-6.4. 기타 국내 P2P 및 웹 하드

#### a. Donkey7

국내에서 제작된 P2P 프로그램 이물(eMule) 클론 버전으로 추정되는 당나귀7 프로그램은 사용자 계정 정보가 SID (eg. S-1-5-21-1659004503-1767777339-682003330-1004) 형태로 들어있다. 아래에는 설치시 입력한 사용자 정보 및 다운로드 폴더의 위치 등이 저장된다.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData

#### b. HiDisk

다운로드 폴더 및 ActiveX 설치파일 관련 정보가 저장된다. 프로그램 설치 폴더는 C:\Program Files\HiDisk이며, HKLM\Software\Microsoft\Windows\CurrentVersion\SharedDlls 에서 그 값으로 "C:\Windows\Downloaded Program Files\Hidisk.ocx"를 확인할 수 있고, HKLM\Software\Classes\TypeLib\{D13EF3E7-4615-4526-8B1D-F546883E64F7}\1.0\0\win32 (Default=C:\WINDOWS\Downloaded Program Files\HiDisk.ocx)을 통해 기본 다운로드 폴더를 확인할 수 있다.



c. ShareBox

HKCR \software\ShareBoxPoint 와 HKCR \software\ShareBoxSearchBar 에는 INST\_DATE 라고 하는 인스톨 시각이 기록된다. HKLM\software\Classes\AppID\ShareBoxCtrl.DLL 에는 어플리케이션 ID가 저장된다. 이 CLASS ID값을 이용하여 HKLM\software\Classes\clsid\{180C8380-22BA-4A62-A0E8-79F8DCE56B19}을 살펴보면 프로그램 버전, 다운로드 폴더 위치 등을 알 수 있다.

d. FileZilla

HKCU\SOFTWARE\FileZilla Server 와 HKLM\SOFTWARE\FileZilla Server 에 설치 경로와 언어, 안전모드 작동여부 등이 저장된다.

e. 토토 브라우저

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{xc865\xc865\wf? \xb7ed} 에 설치 경로, 버전 정보 등이 수록 된다.

### 3-6.5. 공통 레지스트리 키

위 P2P 클라이언트들과 공통적으로 관련된 레지스트리 키가 있다.

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List 이다. 이는 서비스팩 2 이후부터 생긴 Windows 방화벽에 의해 외부 접근을 허용하는 어플리케이션 목록이다. P2P 프로그램이 이 목록에 포함되어 있지 않다면, P2P 클라이언트의 서버로 접근하는 TCP 나 UDP 포트를 허용하지 않아 연결이 막힐 것이다. 따라서 파일 공유를 목적으로 하는 모든 프로그램은 이 목록에 있어야만 한다. 조사하는 시스템에 다른 파일 공유 어플리케이션이 존재하는지 확인할 때 유용하다.

### 3-7. Messenger

#### 3-7.1. MSN Messenger

하이프 파일은 NTUSER.DAT다. HKCU\Software\Microsoft\MessengerService\ListCache\NET MessengerService\\* 에 위치한다. IM groups, contacts, 파일 전송 정보 등이 담겨있다. (PCIN.net, 2007)

파일 공유 : 파일 공유 설정이 켜져있는지 확인가능하다.

HKCU\Software\Microsoft\MSN Messenger\FileShairing-Autoshare

파일 전송 : Received Files 폴더의 위치를 보여준다.

HKCU\Software\Microsoft\MSN Messenger\FTReceiveFolder

메시지 기록 : 1이면 메시지 기록 설정이 되어 있는 것이다.

HKCU\Software\Microsoft\MSN Messenger\PerPass  
portSettings\#####\-MessageLoggingEnabled

메시지 히스토리 파일의 위치

HKCU\Software\Microsoft\MSN Messenger\PerPass  
portSettings\#####\-MessageLog Path

주소록 : CTT, Contact List) 파일의 위치

HKCU\Software\Microsoft\Messenger Service - ContactListPath

#### 3-7.2. Nateon

HKEY\_LOCAL\_MACHINE\SOFTWARE\SK Communications 에 위치한다. 서브 키 중 Configuration은 auto\_upgrade 설정 여부(디폴트는 1이나, 0으로 설정시 자동 업데이트를 막을 수 있다.), Description URL, Download Path('네이트온 받은 파일' 폴더의 위치), error\_notice\_url, Force Serial, Nateon Path(네이트온 프로그램 설치 위치), Script URL, Version 등의 정보를 저장하고 있으며, Network 는 P2Plisten Port, ProxyPort(1080), Proxy 사용여부 등을 기록한다.

Settings 는 로그인 보안 단계, 비밀번호 저장 여부(자동으로 들어가기 설정으로 비밀번호 저장시, 이진형태의 User Key 값 생성됨), User ID(로그아웃하여도 마지막으로 로그인한 ID 기록되어 있음, 레지스트리 편집기에서 지워주거나 C:\Program Files\NATEON\BIN 폴더 안의 숫자와 영어로 된 폴더 내 '아이디@nate.com' 폴더 삭제 가능) 등을 기록한다.

### 3-7.3. Yahoo

방문하거나 만든 적이 있는 채팅방 정보(Chat), 파일전송 설정정보(FileTransfer), 사용자들의 ID(All Identities), 대화명과 ID(screen name), 메시지 설정 정보(Archive), 최근 연락한 주소(IMVironments\Recent) 등  
 HKCU\Software\Yahoo\Pager\profiles\screen name  
 야후 메신저를 이용하여 파일 전송을 한 총횟수  
 HKCU\Software\Yahoo\Pager\File Transfer (global value)  
 마지막 로그인한 사용자(Yahoo! User ID), 저장된 비밀번호(Saved Password)  
 HKCU\Software\Yahoo\Pager

### 3-7.4. AOL Instant Messenger (AIM) (Aim Recovery)

파일전송 및 공유설정(Xfer), 보낸 메시지(IamGoneList), 사용자 프로필(DirEntry),  
 HKCU\Software\America Online\AOL Instant Messenger(TM)\CurrentVersion  
 \Users\screen name\  
 마지막으로 로그인한 사용자의 대화명  
 HKCU\Software\America Online\AOL Instant Messenger(TM)\CurrentVersion  
 \Login - Screen Name  
 최근 연락한 친구목록(recent IM ScreenNames), 친구저장 폴더(configTransport)  
 HKCU\Software\America Online\AOL Instant Messenger\CurrentVersion\Users  
 \username

### 3-7.5. Windows Messenger

주소록 등 저장. IdentityName으로 마지막 로그인한 사용자를 확인 가능.  
 HKCU\Software\Microsoft\MessengerService>ListCache\NET Messenger  
 Service  
 전송되는 파일을 받은 폴더 위치  
 HKCU\Software\Microsoft\MessengerService-FtReceiveFolder\Received Files

## 3-8. Outlook and Outlook Express

계정 비밀번호 저장  
 HKCU\Software\Microsoft\Protected Storage SystemProvider\SID\Identification  
 \INETCOMM Server Passwords  
 Outlook 열었던 첨부파일의 저장 경로  
 HKCU\Software\Microsoft\Office\version\Outlook\Security

## 4. 레지스트리에서 공격자의 흔적 찾기

### 4-1. 루트킷 탐지

#### 4-1.1. 도입

Windows 루트킷은 시스템에서 그 존재를 감추기 위해 많은 기법을 사용하는 데, 이 때 대부분 공통적으로 시스템 부팅시 로드되는 메커니즘을 사용하고 이는 레지스트리 사용을 포함하게 된다. 시작프로그램 엔트리를 확인하여 루트킷 존재를 감지하는 Sysinternals의 Autoruns와 같은 툴을 우회하기 위하여, 정상 API들로 해당 레지스트리 키들을 숨기곤 한다. 이를 탐지하는 가장 보편적인 방법은 cross-view 탐지이다. 레지스트리 편집기 툴과 같은 Windows API를 이용하여 레지스트리를 보는 하이레벨 관점과 로우 레벨로서 디스크에 있는 데이터 구조를 직접 보는 관점, 이 두가지를 서로 비교하여 숨겨진 엔트리를 찾아내는 것이다. 물론 하이레벨과 로우레벨 스캔 상 시간 차이로 인해 발생하는 실제 불일치인 경우도 있으나, 대부분 숨겨진 엔트리는 루트킷을 위한 경우가 많다. (Mihir Nanavati)

#### 4-1.2. 레지스트리 Hives (SYSTEM, SOFTWARE)

루트킷과 루트킷 탐지 툴 모두 SYSTEM, SOFTWARE 하이브에 집중되어 있다. SYSTEM 하이브는 해당 시스템의 서비스와 드라이브 목록을 포함한다. 커널 레벨 루트킷(eg. Hacker Defender or BadRkDemo)은 SYSTEM 하이브에서 탐지되며, Vanquish[6]와 같은 DLL Injection 은 SOFTWARE 키에서 발견된다. (Dolan-Gavitt, 2007; Walters, 2006)

#### 4-1.3. 로우 레벨 Data 획득

레지스트리의 로우 레벨 데이터는 여러 방법으로 획득 가능하다. Offline System을 스캔하는 경우에는 파일을 찾아 복사하고 파싱하면 된다. Live System을 스캔하는 경우에는 레지스트리 하이브를 디스크로 덤프(dump)하기 위하여 RegSaveKeyEx()와 같은 API 함수를 이용한다. (B. Cogswell and M. Russinovich. RootkitRevealer <http://www.sysinternals.com/>) 다른 방법은 레지스트리 하이브가 로우 레벨 카피 루틴을 통해 저장되는 드라이브의 물리적 위치를 알기 위해, 파일 시스템 전부를 파싱하는 것이다.

#### 4-1.4. Helios 툴을 이용한 Cross-View 탐지

Helios는 시스템의 레지스트리를 Live로 스캔한다.(온라인 스캔이라고도 한다.) NTFS 구조가 파싱된 후 하드드라이브의 섹터를 직접 읽어들이어 로우레벨 데이터를 획득한다. 즉, Windows API를 사용하지 않고 레지스트리 하이브 파일을 얻고자 할 때 로우레벨 수행을 한다. 이후 데이터는 파싱되고, 그 안에 있던 모든 키와 값, 데이터는 저장된다. 하이레벨 관점은 레지스트리 편집기(regedit)가 레지스트리를 보여주는데 사용하는 RegEnumKeyEx()와 RegEnumValueEx() API 함수를 이용하여 얻도록 한다. 하이레벨에서는 숨겨진 레지스트리 키와 값이 보이지 않는다. Helios는 이러한 불일치를 찾아 체크한다. 이 기법은 레지스트리에에서 자신을 은닉하려는 대부분의 루트킷을 탐지 가능하다. Helios는 Hacker Defender, Vanquish, BadRkDemo를 모두 탐지하며, 숨겨진 키를 표시해준다.

#### 4-1.5. 한계

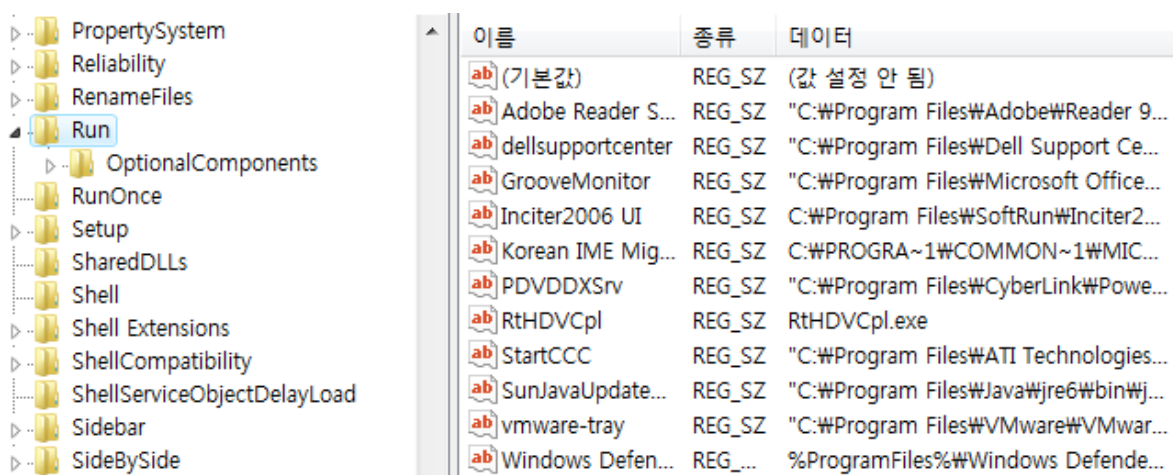
Live 스캔의 가장 어려움은 바로 정보의 믿을만한 소스를 구하는 것이다. 시스템이 정확하게 상태를 기록한다고 믿을수 없기 때문이다. 편리하다고 Live System에서 스캔하는 경우 리스크가 따른다. 서버와 같이 재부팅될 일이 없는 시스템을 공격하는 경우에는 비영속적인 루트킷을 사용하는데, 이는 디스크나 레지스트리에 흔적을 남기지 않기 때문에, cross-view 탐지 기법으로는 찾을 수 없다. 또한 레지스트리는, RootkitRevealer와 같이 RegSaveKeyEx()를 이용하는 경우 공격자가 레지스트리 함수를 후킹하고 파일을 덤프하기 전에 관련 데이터를 필터링하면 얼마든지 우회할 수 있다. Helios는 레지스트리 파일을 얻기 위해 디스크를 읽지만 이 또한 read 함수를 후킹하여 ntfs.sys나 disk.sys를 필터링하여 우회가능하다.

## 4-2. 자동실행(Autoruns), 시작 프로그램(Startup) 관련

Autorun locations는 부팅 과정에서 프로그램이나 어플리케이션들을 실행하는 레지스트리 키이다. 일반적으로 조사 시에 이 키들을 많이 살피게 된다. 시스템 침입 피해 의심이 있을 경우 대개 autorun locations가 관찰된다. 사용자가 이러한 변화를 눈치채지 못할 경우, 그 시스템은 감염되고 공격의 시발점이 된다. 이때 autorun locations는 trojan 백도어가 설치되어 공격자가 재량껏 활동할 수 있도록 시스템이 취약해졌음을 증명해준다고 볼 수 있다. Autoruns, startup program 설정 관련 레지스트리도 함께 살펴보도록 한다.

### 4-2.1. 일반적인 autuorun locations 목록

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run  
 HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx  
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices  
 HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce  
 HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run  
 HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
 HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce  
 HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices  
 HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce  
 (ProfilePath)\Start Menu\Programs\Startup



이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
Adobe Reader S...	REG_SZ	"C:\Program Files\Adobe\Reader 9...
dellsupportcenter	REG_SZ	"C:\Program Files\Dell Support Ce...
GrooveMonitor	REG_SZ	"C:\Program Files\Microsoft Office...
Inciter2006 UI	REG_SZ	C:\Program Files\SoftRun\Inciter2...
Korean IME Mig...	REG_SZ	C:\PROGRA~1\COMMON~1\MIC...
PDVDDXSrv	REG_SZ	"C:\Program Files\CyberLink\Power...
RtHDVCpl	REG_SZ	RtHDVCpl.exe
StartCCC	REG_SZ	"C:\Program Files\ATI Technologies...
SunJavaUpdate...	REG_SZ	"C:\Program Files\Java\jre6\bin\j...
vmware-tray	REG_SZ	"C:\Program Files\VMware\VMwar...
Windows Defen...	REG_...	%ProgramFiles%\Windows Defende...

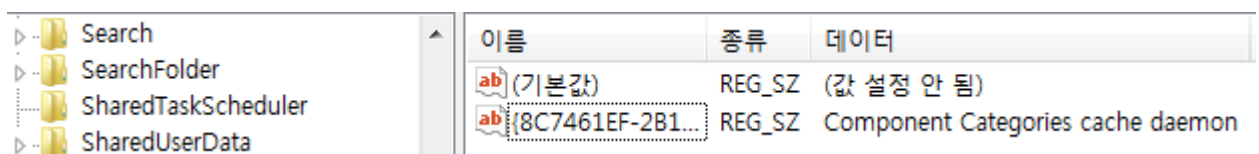
그림 19. CurrentVersion\Run Key

#### 4-2.2. SharedTaskScheduler

윈도우에서 레지스트리를 이용해서 자신의 프로그램을 자동으로 시작 시킬 수 있는 레지스트리는 여러 개 있다. 이러한 키들을 빠르게 스캔하고 싶다면, Sysinternals Autoruns 프로그램을 활용하면 편리하다. SharedTaskScheduler 는 시작 프로그램으로 등록되는 그러한 레지스트리 키들 중 하나이며, 문제의 소지가 많다. 대부분의 유저(99.9%)가 사용하지 않는 기능이므로, 사용되고 있다면 의심해볼 만 하다. Windows 의 Shell 프로그램인 Explorer.exe 프로세스가 로드되자마자 특정 레지스트리 항목에 지정된 dll 들을 참조하여 불러오는 형태이다. CLSID 형태로 지정된다. (Kim Tae-il, 2008)

적용되는 시스템 : Windows Vista, XP, 2000, NT

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTask Scheduler



이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안 됨)
{8C7461EF-2B1...}	REG_SZ	Component Categories cache daemon

그림 20. SharedTaskScheduler Key

#### 4-2.3. Shell\Open\Command

HKCR\exefile\shell\open\command\

이 키는 어떤 exe 확장자 파일을 가리킨다. default value는 "%.1. %\*" 만을 가진다. (ShaolinTiger, 2003).그러나 이 값이 "어떤 파일명 "%1" %\*" 과 같이 수정된 경우, 조사관은 용의자가 어떤 프로그램을 숨겨 자동실행하고자 함을 알 수 있다. 이러한 방식은 다음 키들에도 적용 가능하다. (Carvey, 2004)

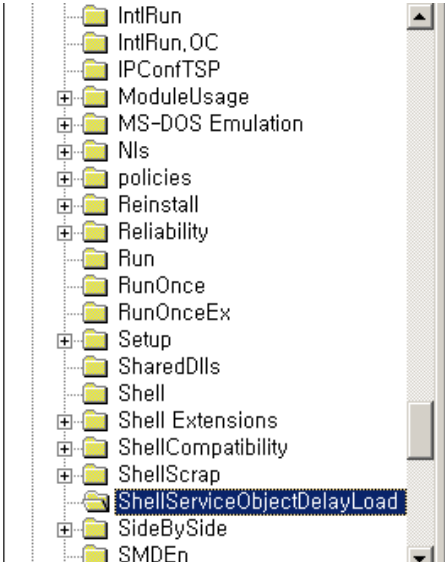
HKEY\_CLASSES\_ROOT\batfile\shell\open\command

HKEY\_CLASSES\_ROOT\comfile\shell\open\command

#### 4-2.4. ShellServiceObjectDelayLoad(SSODL)

Undocumented 된 Windows 자동 실행방법 중 하나이다. 보통 몇몇 Windows system 구성요소에 의해 사용된다. 그 목록은 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad 에 위치하며, Windows 의 Shell 프로그램인 Explorer.exe 프로세스가 시작되면, 레지스트리 항목에 지정된 dll 들을 참조하여 불러온다.

일반적인 SSODL item 목록을 사용하여 Hijack 하곤 하므로, 알려지지 않은 악성 레지스트리인지 확인이 필요하다. (Kim Tae-il, 2008)



이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안됨)
ab]CDBurn	REG_SZ	{fbeb8a05-beee-4442-804e-409d6c4515e9}
ab]PostBootReminder	REG_SZ	{7849596a-48ea-486e-8937-a2a3009f31a9}
ab]rdshost	REG_SZ	{097A9EC6-7C08-4ED4-BBA2-E9F326A75383}
ab]SysTray	REG_SZ	{35CEC8A3-2BE6-11D2-8773-92E220524153}
ab]WebCheck	REG_SZ	{E6FB5E20-DE35-11CF-9C87-00AA005127ED}

그림 21. ShellServiceObjectDelayLoad(SSODL) Key

c.f) explorer.exe 을 target 으로 injection 하는 악성코드라면, 아래와 같은 곳에 launchpoint 를 잡아서 부팅시 로드될수 있게 한다.

- i. SSODL(ShellServiceObjectDelayLoad)
- ii. SharedTaskScheduler 에 launch 한다.

#### 4-2.5. SYTEM.INI / WIN.INI File

Windows 부팅 시 참조되거나 로딩되는 환경설정 및 드라이버 관련 내용들을 담고 있는 파일들이다. 두 파일의 내용은 NT 계열로부터 레지스트리 항목으로 대신 참조된다. 악성코드는 해당 항목들을 조작하여 Windows 부팅시 악성코드가 자동 시작되도록 만든다. (Symantec, 2004)

SYSTEM.INI 파일 : 악성코드는 Shell 혹은 Userinit 값의 데이터를 조작하여 부팅 시 자동실행되도록 한다. 예를 들어, Shell value는 디폴트로 Explorer.exe가 세팅되어 있으므로, Shell=Explorer.exe %system%\System32.exe 와 같이 수정하여 시스템 재부팅 후 로그인시에 자동 실행되도록 한다. (Symantec, 2003)

HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon



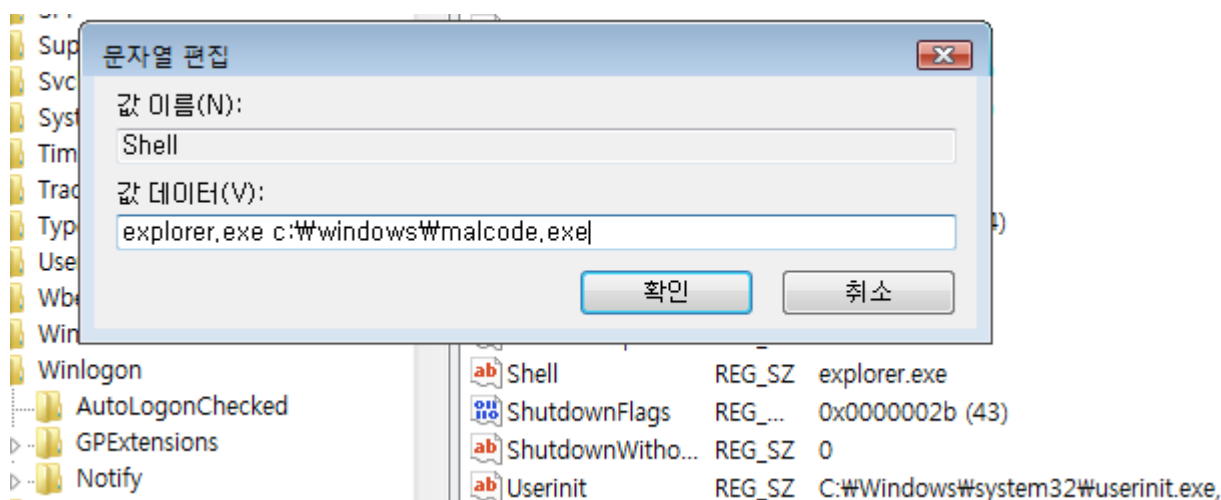


그림 22. SYSTEM.INI

WIN.INI 파일 : 악성코드는 Load 혹은 Run 값의 데이터를 조작하여 부팅 시 자동실행되도록 한다.

HKCU\Software\Microsoft\Windows NT\Current Version\Windows

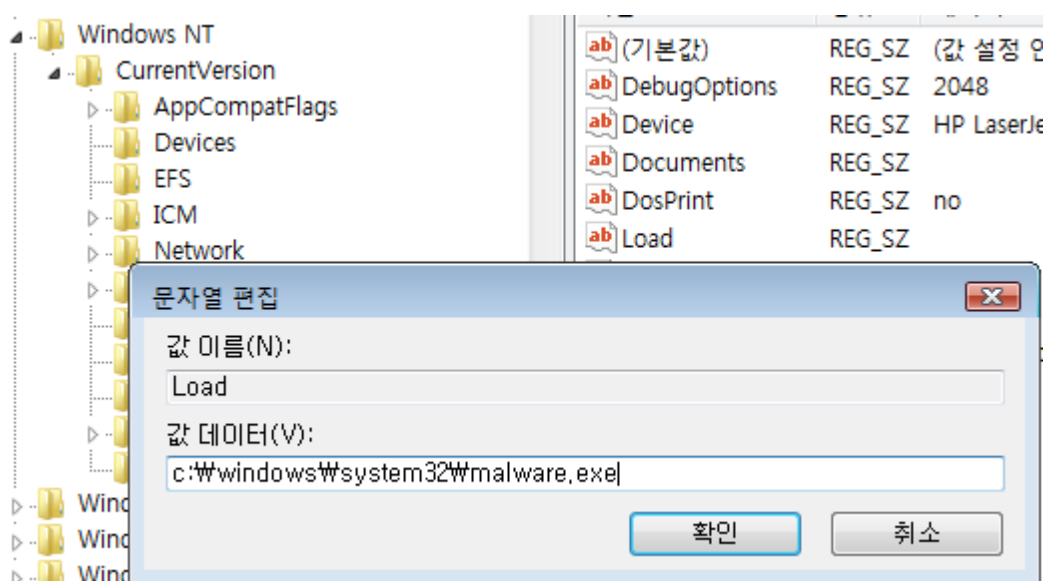


그림 23. WIN.INI 확인

#### 4-2.6. ShellExecute Hook

Windows Explorer(ShellExecute)을 이용하여 프로그램을 실행하는 경우 ShellExecuteHooks 에 등록된 모듈이 먼저 실행된다.

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks

#### 4-2.7. AppInit\_DLL 레지스트리 값 자동 실행

현재 로그인 한 세션에서 각 어플리케이션에 의해서 로드가 되는 DLL 항목이 지정된다.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows

#### 4-2.8. AppInit\_DLLs

AppInit\_DLLs 라는 이름은 Application Initialize DLLs 을 줄인 것으로 보인다. 따라서 이 값은 응용 프로그램이 초기화할 DLL 목록을 기억하고 있는 값으로 추정된다. 레지스트리 값을 자동실행하며, 현재 로그인 한 세션에서 각 어플리케이션에 의해서 로드가 되는 dll 항목이 지정된다. AppInit DLLs 는 User32.dll 의 DLL\_PROCESS\_ATTACH 중 LoadLibrary()에 의해 로드된다.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows

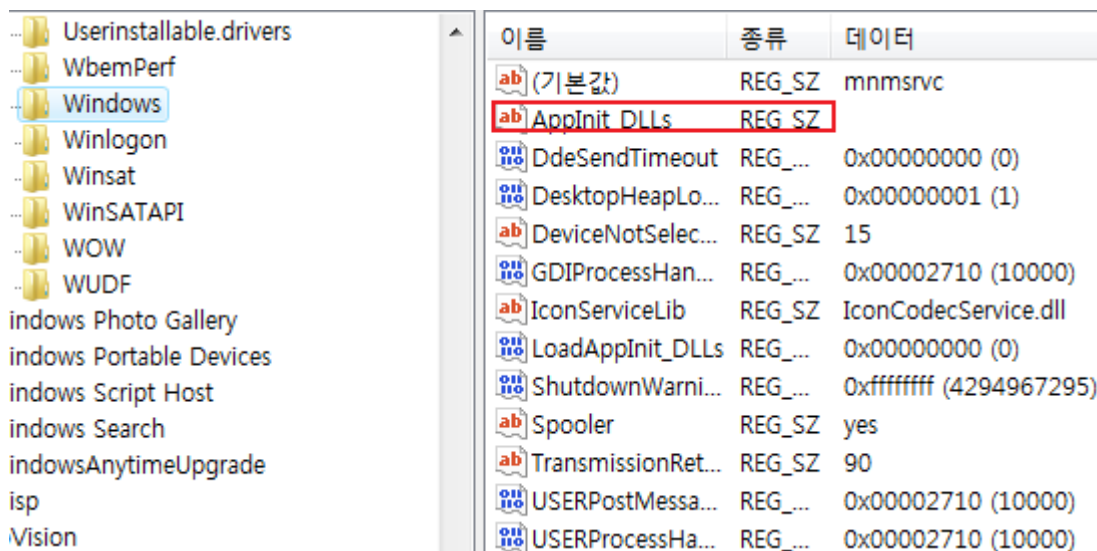


그림 24. AppInit\_DLLs

#### 4-2.9. Winlogon Notification Package

Winlogon 이벤트 핸들러를 익스포트하고 있는 dll

Winlogon 은 특정이벤트(eg. 사용자의 시스템 로그인) 발생 시 notification package 에서 해당 이벤트의 정보를 제공하는 익스포트한 핸들러를 수행한다.

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify

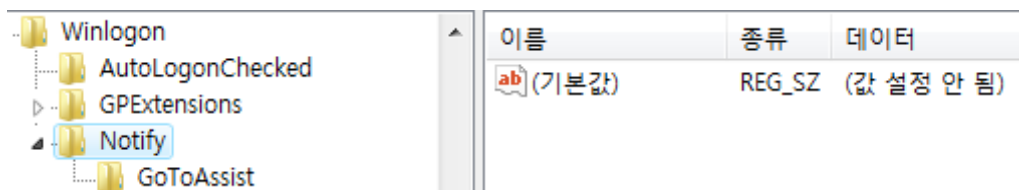


그림 25. Winlogon Notification Package

#### 4-2.10. UserInit Key

사용자가 시스템에 로그인 한 후 실행되어야 하는 프로그램을 지정한다.

디폴트는 Userinit.exe 로 이 프로그램은 사용자의 실행환경을 설정하고 바로 종료된다. 따라서 Userinit.exe 가 부팅 이후 상당한 시간이 지났는데도 실행중일 경우 의심해 보아야 한다.

Userinit.exe 외에 추가적으로 실행할 프로그램을 등록할 수 있다.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit



REG\_SZ C:\Windows\system32\userinit.exe,

그림 26. Userinit key Default

## 4-3. Internet Explorer 관련

### 4-3.1. Browser Helper Object (BHO)

eg. Adobe Acrobat Plug-in, IE Developer Toolbar

#### i. BHO 란?

BHO 는 Browser helper Object 의 줄임말로 Internet Explorer Browser 에서 지원하지 못하는 기능을 추가적으로 지원하기 위해서 Plug-in 형태로 Internet Explorer 에 추가되는 DLL 모듈을 뜻한다. DLL 형태로 지원이 된다.

#### ii. DLL(Dynamic Link Library)을 사용하는 이유

DLL 은 특정 프로그램을 고치지 않더라도 DLL 파일만 수정하여 배포하면 프로그램의 업그레이드가 가능하기 때문에 많이 쓰인다. 그리고 DLL 을 로드하기 때문에 별다른 프로그램의 제작이 필요하지 않고, 필요한 DLL 파일을 로드만 하면 되기 때문이다.

#### iii. CLSID(Class ID)

Class ID 는 특정 컴포넌트나 서버에 의해 만들어진 ActiveX 또는 OLE2.0 객체와 관련된 식별자로서, Class ID 값은 서버가 만들 수 있는 각 객체의 형식에 따라 Register 내에서 고유한 값을 가져야 한다.

[Browser Helper Object 위치]

\\HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Browser helper Object

위에서 matching 이 되는 Registry Key 는 따로 등록에 되어 있는데 위치는 다음과 같으며 제조 회사, 로드 되는 DLL, DLL 의 위치 등이 등록되어 있다.

\\HKCR\\CLSID

\\HKCR\\BHO

#### iv. BHO 체크 방법

위에서 말한 register 에서 직접 확인해서 체크 하는 방법과 BHOChecker 라는 공개 tool 을 이용하여 체크 하는 방법이 있다.

#### v. Internet Explorer 에서 BHO 기능 사용여부 설정

인터넷 익스플로러 설정에도 BHO 기능을 사용할 것 인지를 결정할 수 있는 설정이 포함되어 있다. 영문 Explorer 에서 한글 버전으로 번역을 하며, 일반 사용자는 이해하기 어려운 표현으로 되어 있다.

인터넷 익스플로러 도구 -> 인터넷옵션 -> 고급

☐ 타사 브라우저 확장명 사용(다시 시작해야 함)

## vi. 결론

BHO 는 DLL 로 제공되기 때문에 일반 사용자들이 쉽게 눈으로 확인 할 수가 없다. BHO 를 악용하여 시스템의 주요정보를 탈취하거나 다른 악성코드를 자유롭게 다운로드하는 형태로 이용될 수 있으므로, 포렌식 조사관은 피해 시스템을 조사시 확인해볼 필요가 있다.

#### 4-3.2. IE Start page / search page / search bar / search assistant URL

이 곳에 심겨있는 unknown 키의 경우, 심각한 악성코드라기 보다는 Adware 정도에 그치는 경우가 많다. IE 의 시작페이지와 검색도우미(search assistant)에 관련된 항목이다. 라인 마지막 부분의 웹주소가 사용자가 설정하지 않았거나 의심스러운 것이면 확인해볼 필요가 있다.

```
HKCU\Software\Microsoft\Internet Explorer\Main
HKCU\Software\Microsoft\Internet Explorer\Search
HKCU\Software\Microsoft\Internet Explorer\SearchURL
HKCU\Software\Microsoft\Internet Explorer\Toolbar
HKLM\SOFTWARE\Microsoft\Internet Explorer\Search
HKLM\SOFTWARE\Microsoft\Internet Explorer\SearchURL
```

#### 4-3.3. Default URL Searchhook

URL Search Hook 에 관련된 항목이다. URL Search Hook 은 사용자가 웹 브라우저의 주소 창에 정확한 프로토콜(http://, ftp:// 등)을 표시하지 않고 웹주소만 입력한 경우에 사용된다. 웹브라우저가 정확한 프로토콜을 찾아내는데 실패하면 URL Search Hook 객체를 호출한다.

기본값은 {CFBFAE00-17A6-11D0-99CB-00C04FD64497}라는 CLSID(클래스 아이디)가 기본값(Default Value)으로 설정되어 있다. 대다수의 IE Hijacker 는 사용자가 프로토콜을 입력하지 않은 상태로 url 을 입력할 경우 공격자의 사이트로 리다이렉트 시키는 방법을 통해 악성코드를 다운받게 한다.

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\URLSearchHooks
```

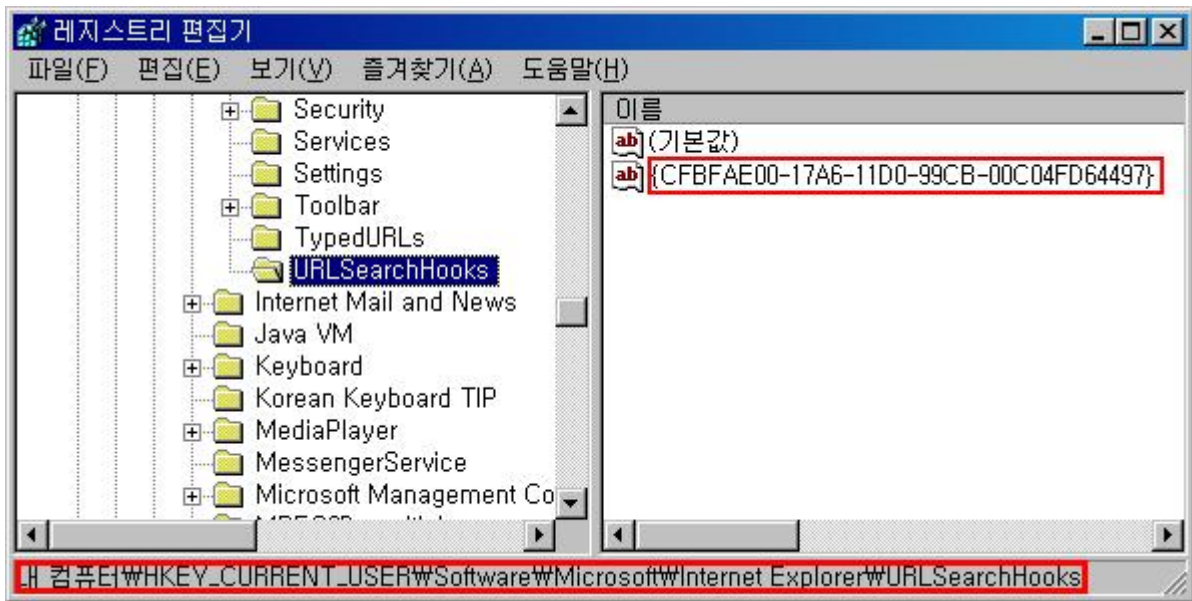


그림 27. URLSearchHooks key Default

#### 4-3.4. IE Options access restricted by administrator

악성코드에 감염되었을 때 사용자의 IE Options 항목에 대한 접근을 제한한다. 레지스트리 값은 모두 DWORD 형식이다. 값을 사용하려면 1로 설정하고 사용하지 않으려면 0으로 설정하면 된다.

컴퓨터 관리자가 적절한 레지스트리 값을 구현하여 메뉴 명령을 제한하면 사용자가 메뉴 명령을 사용하려고 할 때 다음과 유사한 오류 메시지가 나타날 수 있다. (참조 : <http://support.microsoft.com/kb/823057/ko/>)

이 작업은 시스템 제한 때문에 취소되었습니다. 시스템 관리자에게 문의하십시오.

HKLM\Software\Policies\Microsoft\Internet Explorer\Restrictions

HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions

#### 4-3.5. Extra Items in IE right-click menu

IE에서 마우스 우클릭했을 때 보여지는 확장항목 관련 레지스트리이다. 각각의 서브키들은 메뉴 아이템들을 나타낸다. 원하지 않는 것들은 지울 수 있다. 악성코드는 사용자가 해당항목을 클릭하도록 하여 악의적인 스크립트가 있는 페이지를 실행하도록 할 수 있다. (참조 : <http://support.microsoft.com/kb/177241/ko/>)

HKCU\Software\Microsoft\Internet Explorer\MenuExt

## 4-4. 기타 포렌식 관점으로 주시할 사항

### 4-4.1. Windows Services

윈도우 서비스 관련 레지스트리.

윈도우의 서비스와 커널 드라이버에 대한 구성 요소가 저장되어 있다. 윈도우의 서비스를 추가하면, 보통 새로 추가한 서비스가 사용하는 키가 이곳에 추가된다. services.msc 는 레지스트리에 등록된 정보들을 보여준다. 하지만 서비스 항목도 rootkit으로 감출 수 있다. BackOrifice2K와 같은 악성프로그램은 스스로를 서비스로 설치하여 이 키에 흔적을 남기기도 한다. (Carvey, 2001).

HKLM\SYSTEM\CurrentControlSet\Services

- \* 중점적으로 살필 사항 :
1. 현재 실행되고 있는 서비스
  2. 자동실행이 설정되어 있는 서비스
  3. Service Name
  4. Display Name
  4. Description
  5. 해당 dll 찾아서 MAC Time 조사
  - . 최근에 상태가 변경되거나 최근 등록된 서비스 목록을 뽑아 살피는 것이 효과적이다.

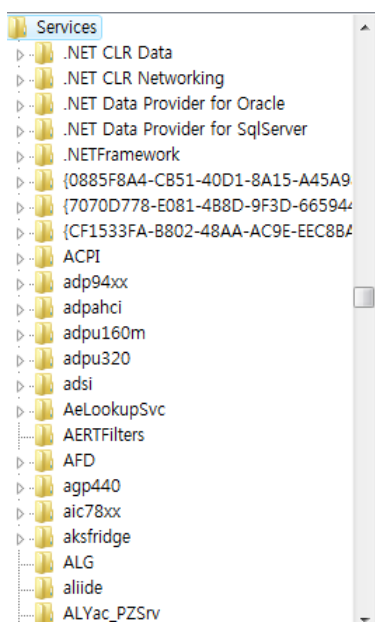


그림 28. Windows Services

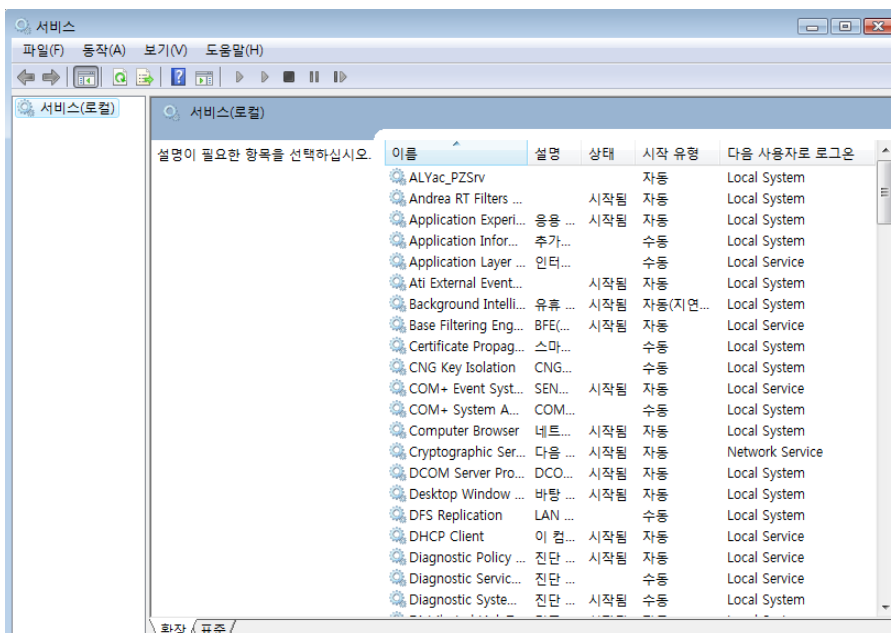


그림 29. services.msc 로 살펴본 레지스트리 등록 정보

#### 4-4.2. Hidden Resource configuration

Hidden 기능과 관련된 레지스트리 값에 따라 숨겨진 자원을 볼 수 있는지의 여부가 결정된다. 악성코드는 사용자가 Windows Explorer의 "Show all hidden files or folders(숨김 파일 및 폴더 모두 보기)" 옵션을 변경하지 못하도록 레지스트리 값을 변경한다. 이러한 수정을 체크하기 위해서는 Windows Explorer를 열고, 도구 메뉴 - 폴더 옵션에 들어가 보기 탭에서 확인해보면 된다. 감염이 되었다면 "Show all hidden files or folders" 옵션이 사용불가능하다. 악성코드는 해당 항목의 'CheckedValue' 값을 조작하여 자신의 위치가 노출되지 않도록 하는 것이다.

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL

다음은 악성코드에 의해 수정된 레지스트리 엔트리이다.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL : "Type" 이 빈칸으로 세팅됨 (원래 값은 "radio" 이다.)

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced :  
"ShowSuperHidden" 이 0 으로 세팅됨

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\HideFileExt : "UncheckedValue" 가 1 로 세팅됨

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL : "CheckedValue" 가 0 으로 세팅됨

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden : "UncheckedValue" 가 1 로 세팅됨



#### 4-4.3. Hosts 파일 (Domain Hijack)

Domain Name Resolving 과 관련된 hosts 파일을 이용하여 인터넷 사이트의 Redirection 을 행할 수 있다.

hosts 파일은 DNS 서버가 해야하는 일을 네트워크를 거치지 않고 내 컴퓨터 안에서 수행하게 할 수 있는 파일이다. 인터넷 초창기 시절 이름과 ip 를 1:1 로 맞추어 쓰던 때에는 이 파일을 참고하여 인터넷을 했지만 인터넷 규모가 커져서 이전 시스템과의 호환성을 위해 호스트 파일을 먼저 찾은 뒤 DNS Server 를 쿼리하는 방식으로 바뀌게 되었다.

Hosts 파일은 웹사이트 이름을 아이피주소로 변환해 주는 기능이 있다. 실제로 컴퓨터가 이를 이용하지는 않고 있지만 hosts 파일의 내용을 텍스트로 쉽게 기록할 수 있는 특성 때문에 시스템관리자나 스파이웨어가 이용 할 수 있다.

아래와 같은 형식으로 생성하면 된다. 그러면 웹 브라우저는 kisa.or.kr 도메인의 아이피주소를 DNS 서버를 이용하지 않고 hosts 파일에 있는 아이피주소를 보고 웹서핑을 하게 된다.

(아이피주소)	(웹사이트주소)
211.252.150.11	kisa.or.kr

이 아이피주소를 스파이웨어나 악성코드를 배포하는 사이트의 아이피주소로 몰래 변경하게 되면 사용자가 kisa 사이트를 웹브라우저주소창에 입력한 후 연결을 시도하면 kisa 사이트 대신 악성사이트로 연결되게 된다.

또한 윈도우, 백신 등의 주요 update server ip 를 가짜로 hosts 파일에 기록해 놓는 경우에도 각종 업데이트를 막아버릴 수 있다. Hosts 파일 내에 이상한 목록이 있다면, hosts 파일의 수정시각을 탐지해보도록 한다.

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath

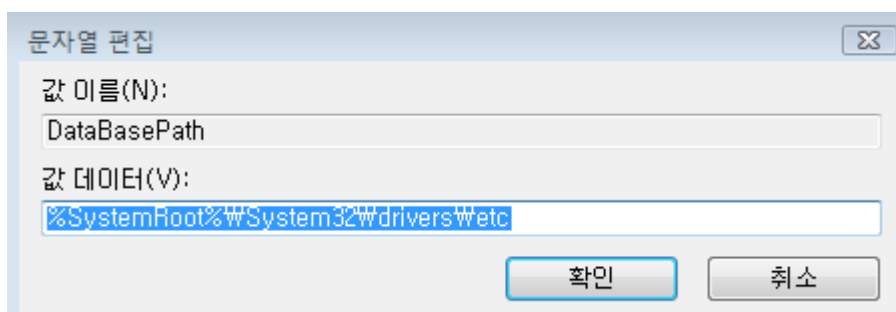


그림 30. hosts 파일 기본 값 확인

#### 4-4.4. Regedit access restricted by administrator

레지스트리 편집기(regedit.exe)에 대한 실행가능 여부를 결정할 수 있는 레지스트리 항목이다. 악성코드는 해당 항목 'DisableRegistryTools' 값의 데이터가 0x00000001 일 경우 'regedit.exe' 프로그램을 실행되지 않도록 할 수 있다.

HKLM\Software\Microsoft\Windows\Currentversion\Policies\System

#### 4-4.5. Event Log Restrictions

이벤트 로그를 읽을 수 있는 권한을 규제할 수 있다. 값이 1 인 경우 접근을 막고, 0 이면 guest 도 접근 가능하다. 로그를 읽기 전, 시스템 사용자 혹은 범죄 용의자가 이 설정으로 로그를 읽는 것을 막아놓았는지 확인하여야 한다.

(PCIN.net, 2007)

HKLM\System\ControlSet\###\Services\EventLog\Application

#### 4-4.6. URL Default Prefix Hijack

Internet Protocol Setting 과 관련된다. IE 에서 URL 을 입력할 때 Prefix 를 제외하고 입력하면 자동으로 Prefix 에 해당하는 내용을 추가한다. 악성코드는 관련 레지스트리 항목을 수정하여 악의적인 사이트로 접근하도록 유도한다.

Value : type	Description
ftp : REG_SZ	"ftp://"
home : REG_SZ	"http://"
www : REG_SZ	"http://"

HKLM\Software\Microsoft\Windows\Current Version\URL\DefaultPrefix

HKLM\Software\Microsoft\Windows\Current Version\URL\Prefix

#### 4-4.7. WinSock LSP (Layered Service Provider)

LSP 는 Layered Service Provider 의 약자로 Winsock 기능을 확장하기 위하여 Microsoft 에서 제공하는 방법이다. WinSock Catalog 의 Base Provider 또는 다른 Layered Provider 사이에 설치되며, Winsock API 를 가로챌 수 있다. 요약하면 LSP 인터페이스에 맞게 제작된 DLL 을 통하여 Winsock API 를 가로챌 수 있는 것이다.

(Name Server 의 응답 조작 등 패킷 조작 모듈을 제작하여 Winsock LSP 를 hijack 할 수 있다.)

정상적인 프로그램에서는 LSP 를 잘 사용하지 않으므로, LSP 지정목록을 확인하는 것이 필요하다. 깨끗한 시스템과 비교하거나 MAC Time 확인으로 조작 여부를 알아본다. (더 나아가 분석하려면 리버싱을 하면 된다.)

이 때 조작된 것으로 여겨져 무작정 삭제를 해서는 절대 안 된다. LSP 의 Chain 이 깨져 부팅이 안될 수 있기 때문이다. 전문 tool 을 활용하도록 한다.

HKLM\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\

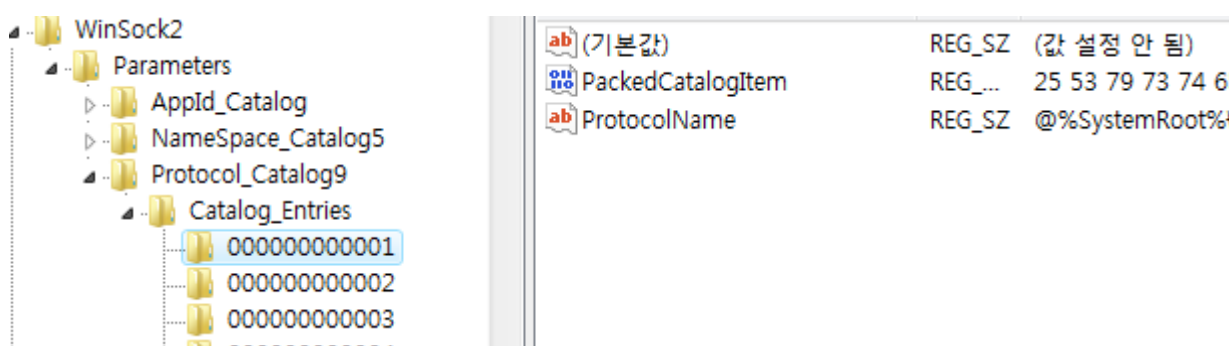


그림 31. WinSock LSP Parameter

이 레지스트리 키는 구성이 다소 복잡하기 때문에 HijackThis 나 AhnReport 같은 전용 툴을 이용하는 것이 좋다. LSP 로 등록된 파일만 삭제하고 LSP 체인 (관련 레지스트리)을 복구하지 않으면 인터넷을 사용할 수 없다. (LSP 체인이 끊긴다는 표현을 하기도 한다.) SZ 는 LSP 로 등록된 파일을 진단하는 경우 LSP 체인을 복구하는 치료 기능을 엔진에 탑재하고 있다. 다른 LSP 체인 복구 도구로는 LSPFix 가 유명하며, HijackThis 로도 복구가 가능하다.

Winsock API Hijack 이 가능하기 때문에 보안 프로그램, 유해사이트 차단 프로그램에 사용하기도 하지만, 충돌이 자주 일어나고 불안정하기 때문에 MS 에서도 권장하지 않는 방법이다. Winsock 통신을 감시하고 변조하거나, 광고를 위하여 LSP 를 사용하는 경우도 있으며 LSP 를 이용하는 대표적인 스파이웨어에는 Win-Adware/NewDotNet, Win-Adware/Roogoo, Win-Spyware/CWS, Win-Adware/CommonName, Win-Adware/MarketScore, Win-Adware/Cnnic 등이 있다.

모든 LSP 가 유해하다고 할 수는 없지만 Winsock 통신을 감시, 변조하기 위하여 사용되는 경우 범죄의 증거가 될 수 있다.

#### 4-4.8. 가상메모리 파일 자동삭제

Windows XP/2000 Default 설정으로는 시스템이 종료될 때 가상 메모리 파일을 삭제하지 않는다. HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management 키는 Windows 가상 메모리 (페이징 파일) 설정 정보를 가진다. 대개 C:\pagefile.sys 와 같은 페이징 파일은 중요한 증거 자료가 될 수 있기 때문에 용의자가 컴퓨터를 종료하며 삭제하려 할 수 있다.

ClearPagefileAtShutdown은 이러한 자동 삭제 여부를 저장하는데, 그 값을 1로 변경하는 경우 시스템의 종료시 자동으로 페이징 파일을 지우게 된다. (Microsoft, 2003) 포렌식 조사관은 증거수집 과정에서 용의자 컴퓨터를 종료하기 전에 이 값의 체크 여부를 확인하여야 한다.

#### 4-4.9. 실행 파일을 다른 프로그램으로 연결

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ 키는 관리자 권한으로 실행 파일명과 타 프로그램을 매치시킬 수 있게 한다. 용의자는 이 기능을 이용하여, 전혀 다른 실행 프로그램 (악성프로그램)을 시작 프로그램으로 작동하게 할 수 있다. (Epp, 2005)

notepad.exe나 taskmgr.exe 와 같이 실행 가능한 파일로 보이는 이름의 서브키를 만들고, 그 안에 실제로 실행할 프로그램(eg. Backdoor)을 가리키도록 한다. 이를 통해 history에 남은 결과를 분석하는 포렌식 조사관을 속일 수 있다. (Symantec, 2005).

#### 4-4.10. 임시 폴더 및 공유 폴더

HKCU\Environment\Tmp&Temp 키는 Windows 임시 파일이 저장되는 Temp 폴더의 위치를 저장하는 환경 변수이다.

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\\* 에서는 다양한 서브키 조작을 통하여, 내문서, 최근 문서, 시작 프로그램과 같은 특정 폴더의 위치를 바꿀 수 있다. 이러한 폴더의 위치 변화는 특정 폴더로 연결하는 모든 링크를 바꾼다. 따라서 포렌식 조사관은 어디와 연관되어 있는지 확인하는 것 외에도 그 내용을 확인할 필요가 있다. 예를 들면, 시작 프로그램 폴더가 리다이렉트되어, 새로운 위치로부터 시작프로그램이 실행될 수 있기 때문이다.

HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\\* 에는 모든 사용자에게 의해 사용되는 폴더와 연관된 링크 정보를 가진다. 이를 이용하여, 악의적인 이유로 다른 파일 시스템 위치에 리다이렉트시킬 수 있다.

## 5. 레지스트리 복구

### 5-1. Registry Key Recovery

#### 5-1.1. 레지스트리 키 복구 원리

범죄자가 자신의 흔적을 지우기 위해 Registry Key 를 삭제하는 경우 이를 복구할 수 있다. Key 를 삭제하는 경우에도 Key 의 데이터는 Hive File 에 남아있기 때문이다. Registry Key 삭제 메커니즘을 파악한다면 해당 키의 복구가 가능하다. 그러나 삭제된 키를 모두 복구 할 수 있는 것은 아니며, RegistryHive File 에 존재하는 삭제된 Key 만을 복구할 수 있다. 삭제된 Registry Key 는 실제로 지워지는 것이 아니라 Offset 정보가 변경되고, 사이즈 정보는 음수에서 양수로 바뀌는 것이기 때문이다. Registry Key 가 삭제된 Hive File 의 정보를 삭제하기 전의 정보로 변경할 경우 Key 를 복구할 수 있는 것이다. (Kim Tae-il, 2009)

#### 5-1.2. 레지스트리 키 삭제 매커니즘

Registry 에 key 가 삭제되어도 key 의 Data 는 그대로 남아있다. Registry Key 가 삭제되면 Size 정보가 변경된다. Windows Registry 는 Key 의 사이즈 정보를 Negative 로 표현하는데, Key 가 삭제되는 경우 해당 Key 의 사이즈 정보는 Positive 로 변한다. Key Cell 의 Size 정보와 Value Cell 의 Size 정보가 변경된다. Parent Key 와 연결을 끊기 위해서 Subkey 개수를 감소시키며, Key(NK) Cell 과 SubkeyList 에서 개수가 감소된다.

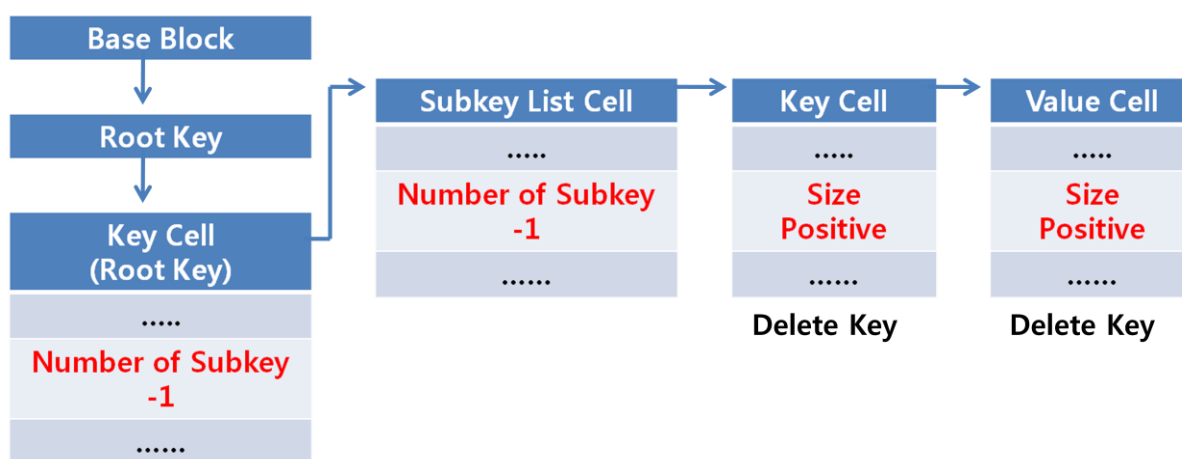


그림 32. 서브키 개수 감소, Size 정보 변경

### 5-1.3. Reglookup-recover 을 이용한 삭제된 키 복구

Reglookup-recover 는 Key 가 삭제된 Hive 파일을 분석하여 삭제된 Key 를 찾아준다. Signature NK 를 갖는 key 들 중에 사이즈 정보가 양수로 되어 있는 것을 검색하고, 삭제된 키의 상위 keyoffset 정보를 분석하여 상위 key 를 검색한다. 아래 그림 33 의 표시된 "nk"는 시그니처이고, "A0 00 00 00"은 Size 정보가 양수로 되어 있음을 말해주며, "20 00 00 00"은 삭제된 키의 부모 키 offset 정보를 이용하여 상위키 정보를 획득하여 검색할 수 있음을 보여준다.

07 E5 3B 2B 01 02 00 00	A0 00 00 00	6E 6B 20 00	.â;+.... .nk .
D0 A2 B4 33 D2 C5 C9 01	00 00 00 00	20 00 00 00	Đç'30ĂÉ.....
00 00 00 00 00 00 00 00	FF FF FF FF	FF FF FF FF	.....yyyyyyyy
00 00 00 00 FF FF FF FF	FF FF FF FF	FF FF FF FF	...yyyyyyyyyyyy
00 00 00 00 00 00 00 00	00 00 00 00	00 00 00 00	.....

그림 33. 삭제 메커니즘에 의해 변경된 정보

이렇게 찾은 삭제된 Key 에 대하여, 삭제 메커니즘을 역으로 수행하여 변경된 값들을 삭제 전으로 복구할 수 있다. 아래의 변경된 사항을 이전으로 돌려놓으면 된다.

상위 key 의 Subkey 개수

SubkeyList 의 삭제된 key 의 offset 정보

삭제된 Key 의 Size 정보

삭제된 Key 의 Value 또는 Value List offset

삭제된 Key 의 Value Cell 의 Size 정보

## 5-2. Restore Point (RP)

### 5-2.1. 개요

Restore Point 는 시스템의 안정성을 위해 Windows XP 등에서 제공하는 기능으로 시스템에 문제가 발생하는 경우 생성된 Restore Point 를 이용하여 최근의 상태로 시스템을 복구할 수 있다. 기본 설정은 On 되어있다. 따라서 이를 이용하여 범죄자가 자신의 흔적을 조작하기 전의 Registry 상태와 일부 백업된 파일들을 복구하고 확인할 수 있다.

Restore Point 생성 시기 : Schedule Base, Manually, 시스템에 중요한 변경이 가해진 경우 (Unsign 된 드라이버의 설치 등)

### 5-2.2. 설정 상태 확인

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore 에서 확인할 수 있으며, DisableSR, RPGlobalInterval 등의 value 가 있다. 디폴트는 On 상태이며 매 24 시간마다 Restore Point 가 생성되어, 최근 90 일 정도의 기록이 유지된다.

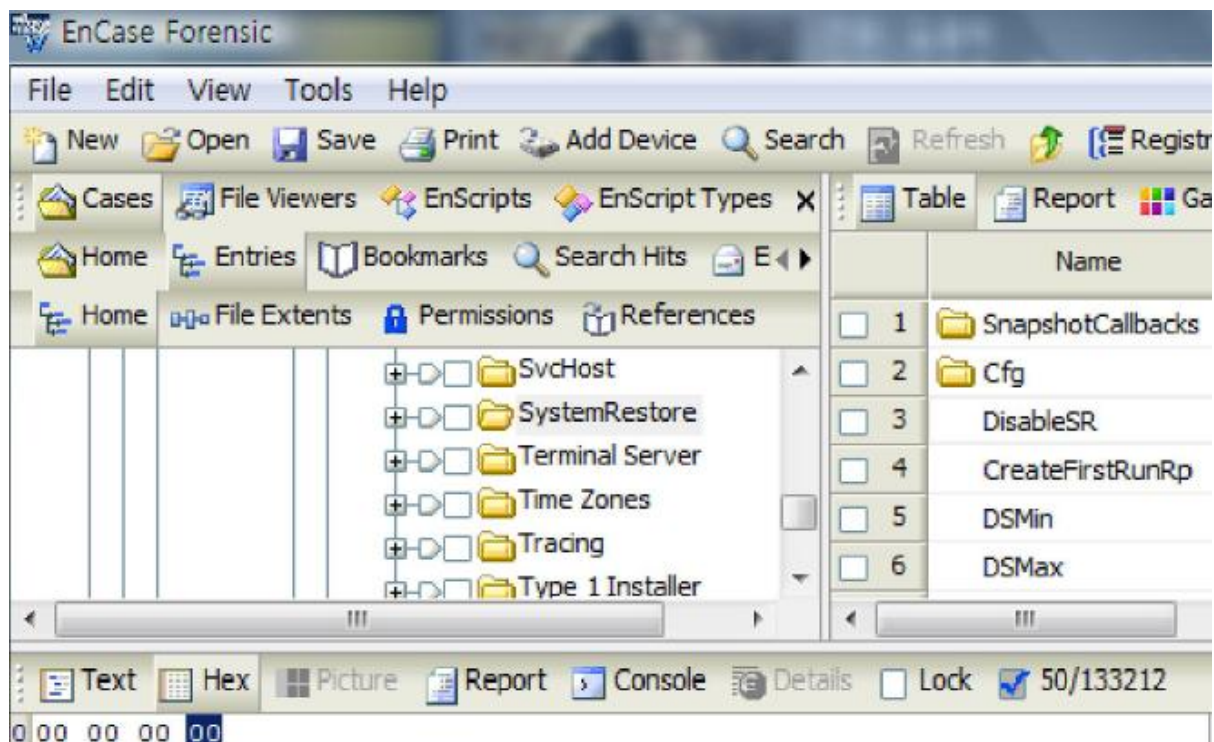


그림 34. Restore Point 설정 상태 확인



### 5-2.3. Restore Point 위치

₩System Volume Information₩\_restore{GUID}₩RP## 에서 ## 는 Sequential 한 일련번호이다.

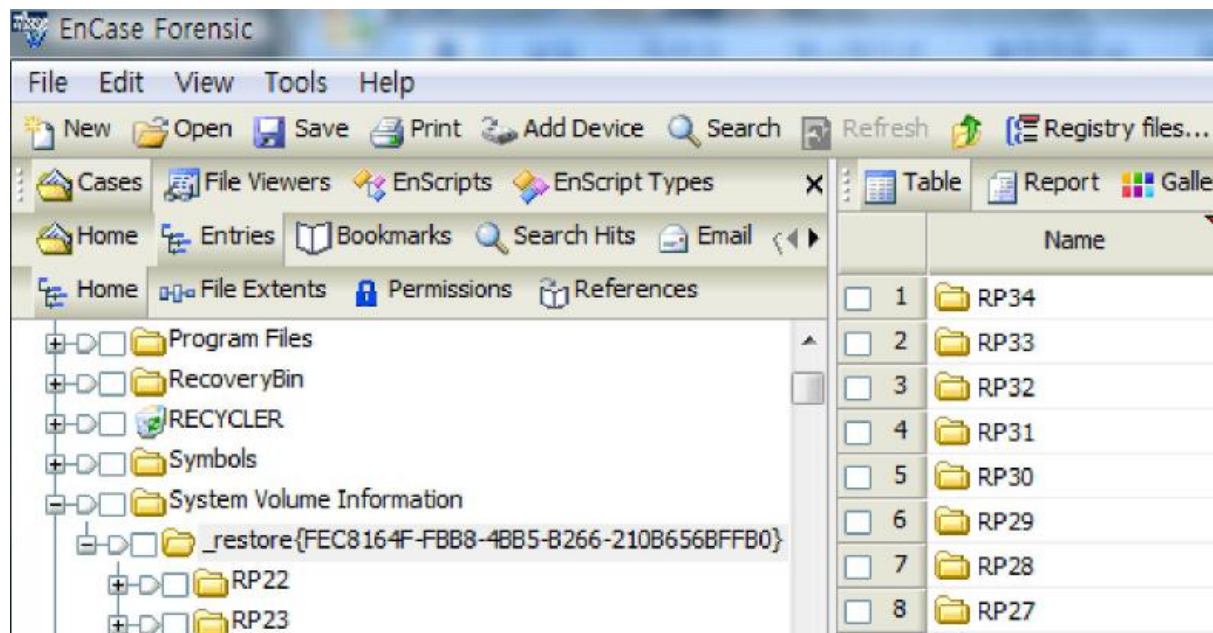


그림 35. Restore Point 위치

### 5-2.4. 조사가 필요한 Restore Point 선택

RP## 폴더의 LastWriteTime 이 대략의 생성 시각과 일치하므로 범죄 행위 또는 그 흔적을 지운 시점 등을 파악하여 해당 Restore Point 를 선택한다.

### 5-2.5. 백업 파일 조사

백업된 파일은 RP## 에 존재하나 이름이 A#####.ext 형태로 변경된다.  
(#####은 임의 숫자이며, ext 는 원래의 파일 확장자를 말한다.) 변경되기 전의 이름은 change.log 에서 확인 가능하다.

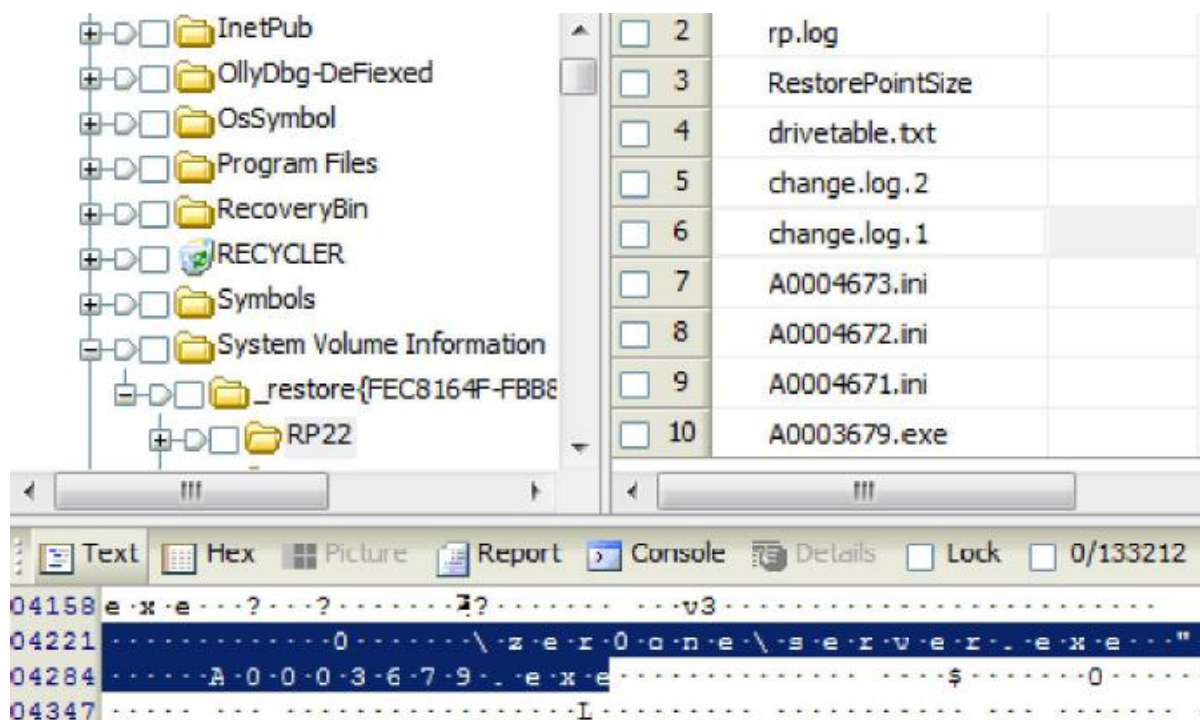


그림 36. 백업 파일 조사

### 5-2.6. 백업 레지스트리 조사

백업된 레지스트리(하이프 파일) 는 RP##\snapshot 폴더에 존재한다.

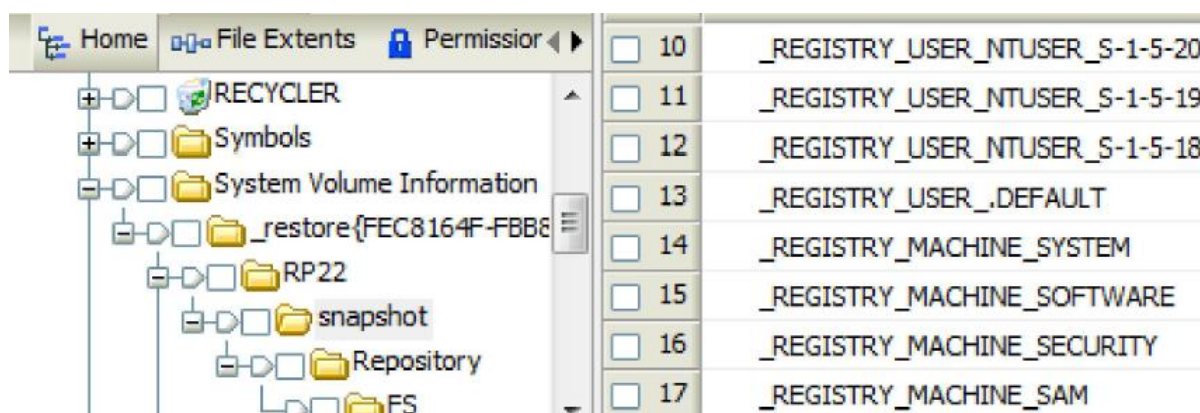


그림 37. 백업 레지스트리 조사

## 6. Registry Forensic 관련 툴 소개

### 6-1. Hijackthis

시스템을 전반적으로 스캔하여 윈도우 내의 전반적인 상황을 한 눈에 볼 수 있게 해주며, 악성코드의 레지스트리 변경 등을 점검하고 복구할 수 있게 해 주는 툴이다. hijack 이란 용어는 '사용자 동의 없는 시스템 브라우저 설정 변경'의 뜻으로 사용된다.

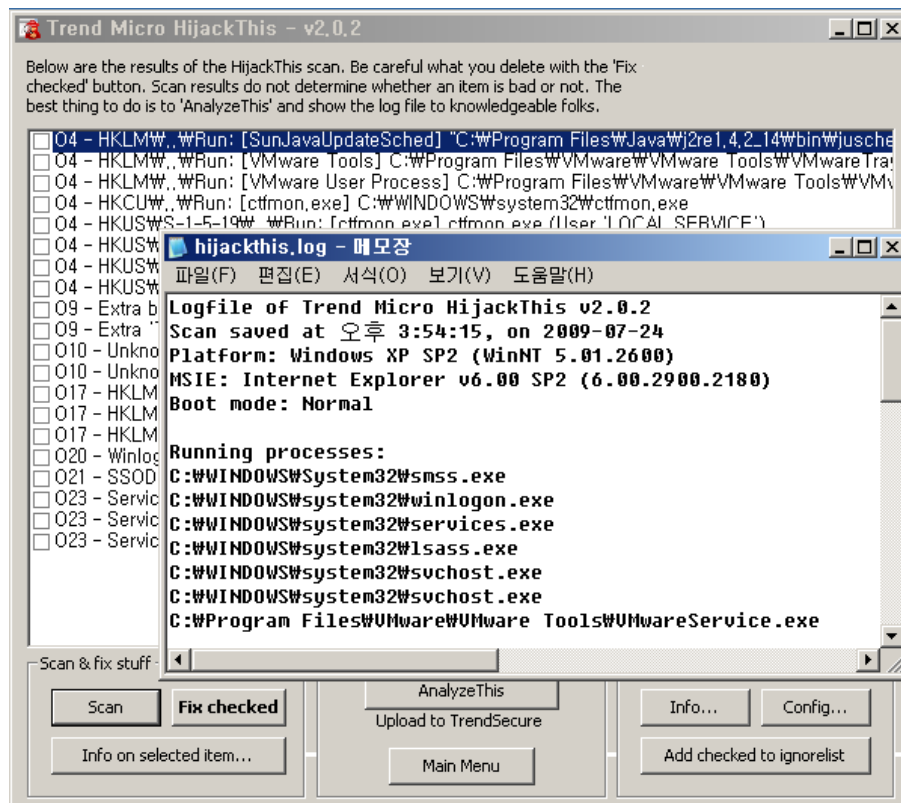


그림 38. Hijackthis

### 6-2. Registry Viewer

레지스트리 편집기(regedit)와 유사한 사용자 인터페이스를 지닌다. 레지스트리 분석을 위한 정보들을 아래쪽에 배치해 놓음으로 인해 보기 편한 인터페이스를 제공한다.

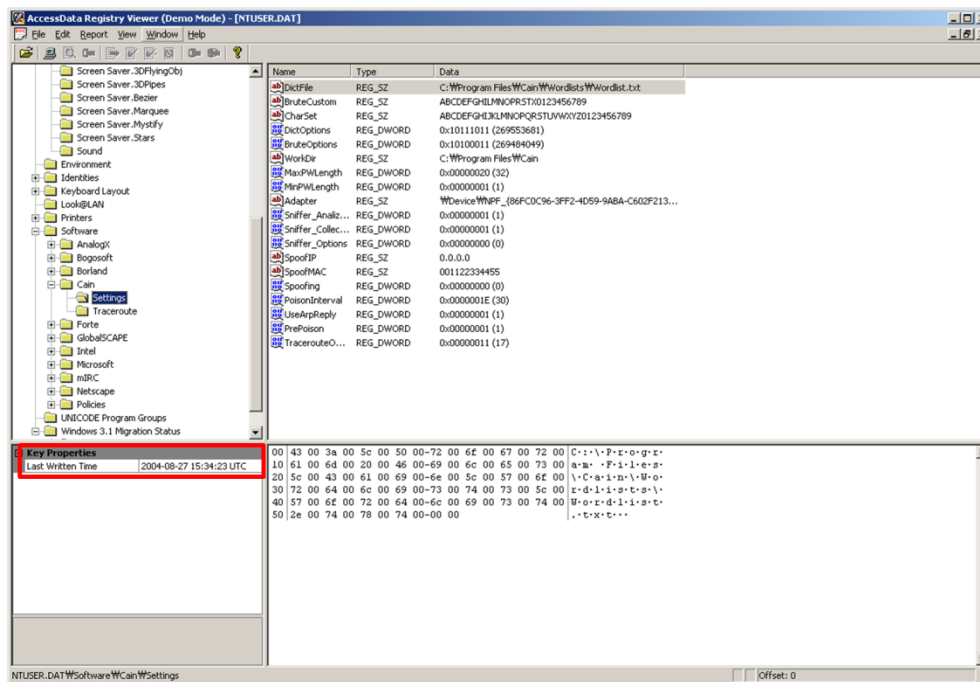


그림 39. Registry Viewer

### 6-3. SysinternalsSuits 중 Autoruns

시작 프로그램 관리 툴중 가장 세세한 사항들까지 제공하는 것으로, msconfig 나 또는 각종 시작 프로그램 관리 프로그램이 포함된 도구에서는 보여주지 못하는 많은 Startup, Autoruns의 관리가 가능하다. 시작 프로그램의 레지스트리 정보를 레지스트리 편집기를 실행시켜 보여주기도 한다.

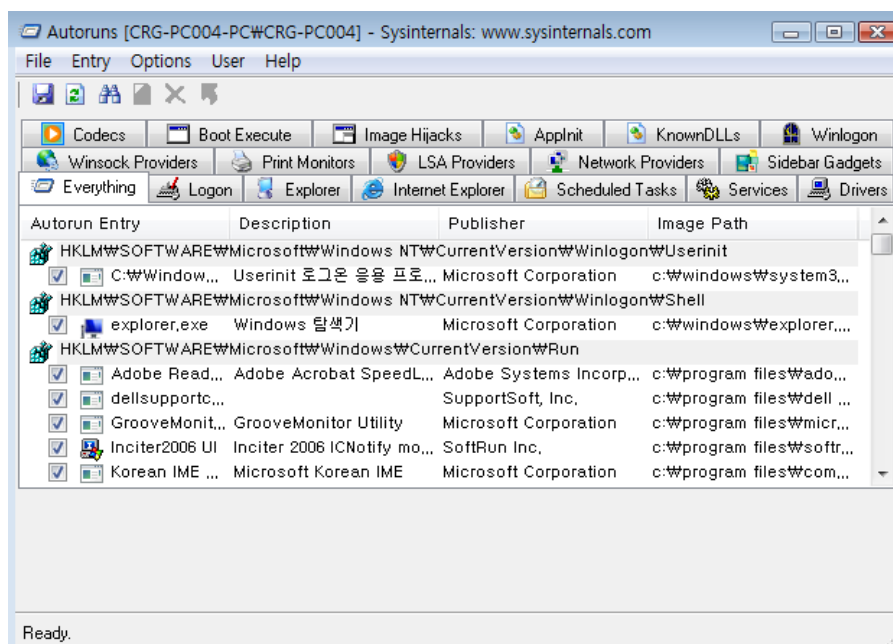


그림 40. SysinternalsSuits - Autoruns

## 6-4. Paraben Registry Analyzer

시스템의 레지스트리를 읽어오기도 하며, 이미 등록된 레지스트리 키에 대해서 빠르게 분석이 가능하도록 도와준다.

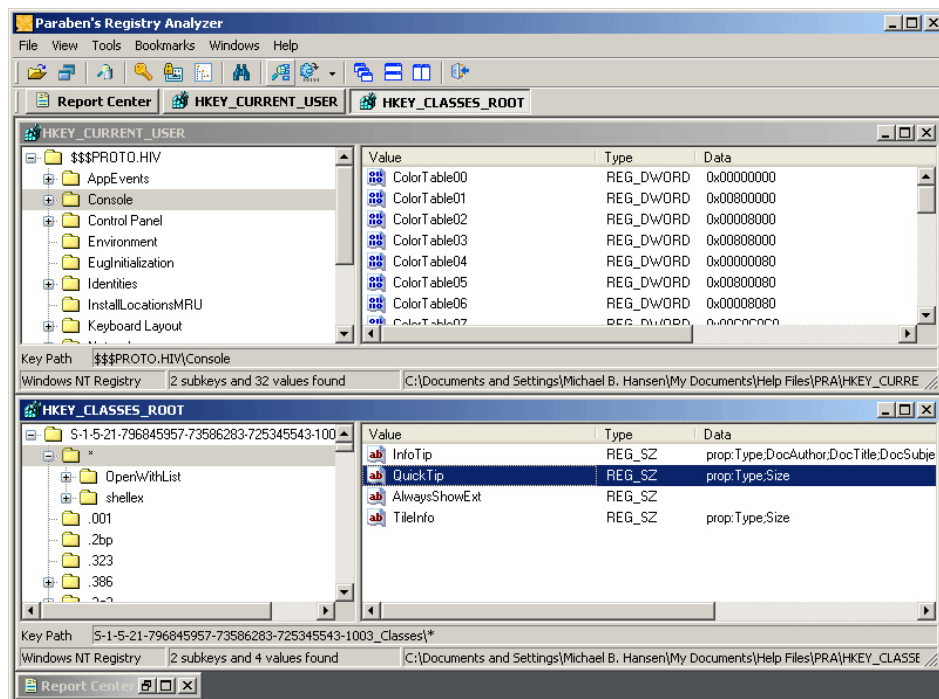


그림 41. Paraben Registry Analyzer

## 6-5. Regripper

Registry 파일을 읽은 후 하위 폴더인 plugins을 검색하여 옵션으로 넘겨준 플러그인들을 실행하여 줌. 각 플러그인들을 묶어서 모듈로 실행할 수도 있다.

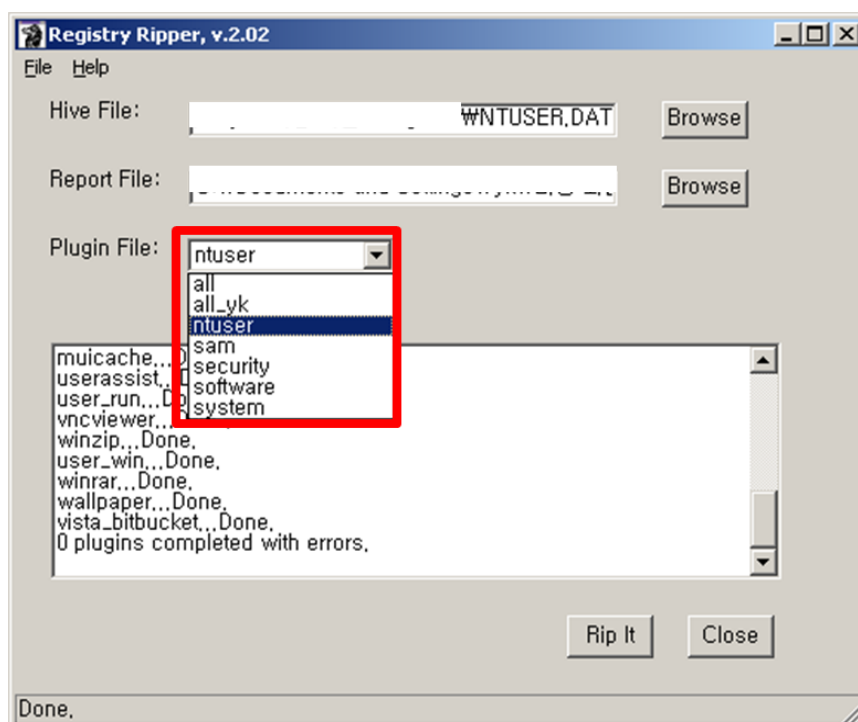


그림 42. Registry Ripper



## 6-6. Regshot

레지스트리의 변경 전과 변경 후의 스냅샷을 각각 찍어, 레지스트리의 수정 변경되는 부분을 쉽게 알 수 있게 도와준다.

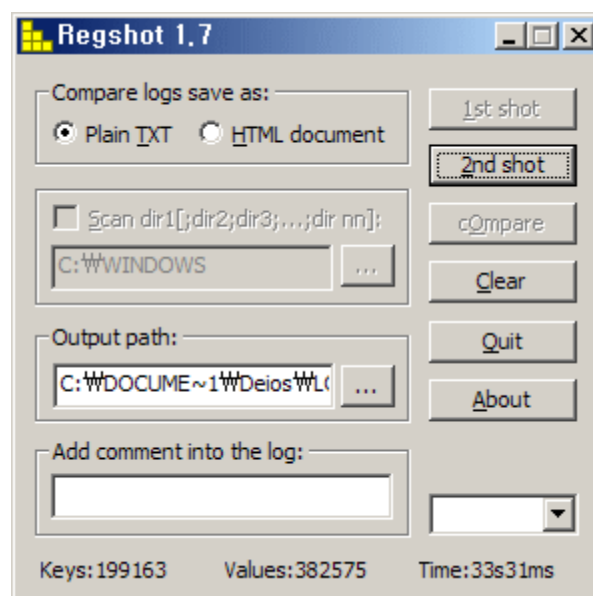


그림 43. Regshot

## 6-7. Regmon

Registry monitor의 준말로, Sysinternals에서 제공하는 실시간으로 동작하는 레지스트리 정보를 로그 방식으로 기록하여 분석에 활용할 수 있는 툴이다.

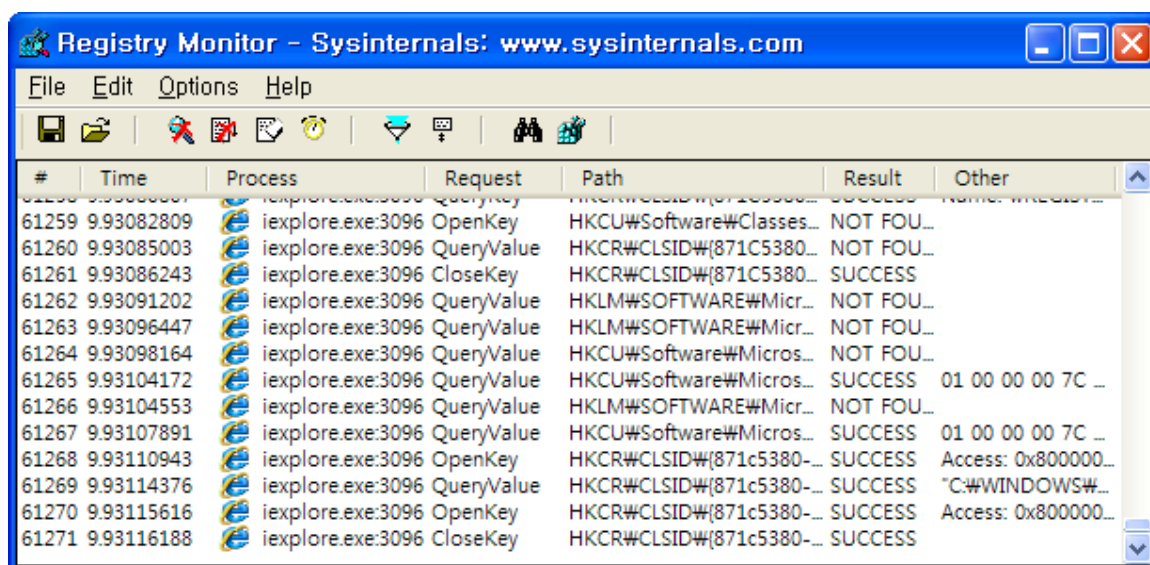


그림 44. Registry Monitor

## 7. 결론

집과 사무실 등 거의 모든 곳에서 Windows 운영체제를 사용함에 따라, 컴퓨터 포렌식 전문가가 Windows 레지스트리의 복잡성을 이해해야할 필요성이 대두되었다. 레지스트리에 남아있는 정보와 잠재적 증거들은 중요한 포렌식 자원이 될 수 있다. 포렌식 관점에서 레지스트리의 원리를 이해하는 것은, 조사관이 해당 시스템에서 어떠한 작업이 이루어졌는지 보다 정확하게 설명하는데 도움이 된다. 이 논문은 레지스트리 조사에 대한 모든 것을 담지 못했다. 어떤 종류의 데이터가 찾아질 수 있고 이를 어떻게 찾으며, 이는 포렌식 관점에서 어떤 방식으로 설명될 수 있는지 몇몇 예시를 들었을 뿐이다. 시스템을 깊게 아는 공격자가 메모리 레지스트리에 그 흔적을 남기지 않고 중요한 계정을 수정할 수도 있다. 이러한 경우에는, RAM과 하드 디스크 모두에서 레지스트리 데이터를 수집하고 이 둘을 비교하여 완전한 Windows 레지스트리를 얻어 조사를 하면 된다. 이 논문에 제시된 바와 같이 공격자의 흔적을 직접 찾기 어려운 조사관은 Chapter 5에서 추천한 관련 툴을 활용하면 좋을 것이다. 운영체제가 환경설정 데이터베이스로서 레지스트리를 사용하고, 어플리케이션들이 이 데이터베이스를 계속해서 사용하는 한, 수사에 필요한 중요한 증거로서 살펴보아야 할 레지스트리는 항상 존재할 수 밖에 없을 것이다.

## 8. 참고문헌

### 도서

- Chad Steel. Windows Forensics. The Field Guide for Conducting Corporate Computer Investigations. Wiley Publishing, Inc, 2006
- Honeycutt, Jerry. Microsoft Windows Registry Guide. 2nd. Redmond, WA: Microsoft Press, 2005.
- Kruse, Warren G., and Jay G. Heiser. Computer Forensics: Incident Response Essentials. New York: Addison-Wesley, 2004.
- Nelson, Bill, Amelia Phillips, Frank Enfinger, and Christopher Steuart. Guide to Computer Forensics and Investigations. 2nd. Canada: Course Technology, 2006.
- Russinovich ME, Solomon DA. Microsoft Windows internals, Fourth edition: Microsoft Windows Server(TM) 2003, Windows XP, and Windows 2000 (pro-developer). Redmond, WA, USA: Microsoft Press, ISBN 0735619174; 2004.

### 논문

- Carvey, Harlan. "The Windows Registry as a forensic resource." Digital Investigation: The International Journal of Digital Forensics & Incident Response 2(2005): 201-05.
- Carvey, Harlan, and Cory Altheide. "Tracking USB storage: Analysis of windows artifacts generated by USB storage devices." Digital Investigation: The International Journal of Digital Forensics & Incident Response 2(2005): 94-100.
- F. Apap, A. Honig, S. Hershkop, E. Eskin, and S. Stolfo. Detecting malicious software by monitoring anomalous windows registry accesses. Proceedings of the Fifth, International Symposium on Recent Advances in Intrusion Detection (RAID 2002)
- Salvatore J. Stolfo, Frank Apap, Eleazar Eskin, Katherine Heller, Shlomo, Hershkop, Andrew Honig, and Krysta Svore, "A Comparative Evaluation of Two Algorithms for Windows Registry Anomaly Detection", Department of Computer Science, Columbia University, New York NY 10027, USA
- Walters A." FATKit: detecting malicious library injection and upping the 'anti'" Technical report. 4TFResearch Laboratories; July 2006.



## 온라인

Aim Recovery. <<http://www.dark-e.com/des/software/aim/index.html>>

Anand G. Internal structures of the Windows registry. 2008.

<<http://blogs.technet.com/ganand/archive/2008/01/05/internalstructures-of-the-windows-registry.aspx>>

Carvey, Harlan. "Windows Incident Response." [Weblog Mounted Devices] 21 Dec 2004. 8 Apr 2007 <[http://windowsir.blogspot.com/2004\\_12\\_01\\_archive.html](http://windowsir.blogspot.com/2004_12_01_archive.html)>.

Davies, Peter. "Forensic Analysis of the Windows Registry." Peter Davies. 2006. 3 Feb 2007 <[http://www.pkdavies.co.uk/documents/computer\\_forensics/registry\\_examination.pdf](http://www.pkdavies.co.uk/documents/computer_forensics/registry_examination.pdf)>.

Derrick J. Farmer. "A FORENSIC ANALYSIS OF THE WINDOWS REGISTRY", 2008 <<http://www.eptuners.com/forensics/Index.htm>>

DFRWS. The DFRWS 2005 forensic challenge.

<<http://www.dfrws.org/2005/challenge/index.html>>

Dolan-Gavitt B. "The VAD tree: a process-eye view of physical memory." Digital Investigation, September 2007;4:62-4

<<http://dfrws.org/2007/proceedings/p62-dolan-gavitt.pdf>>.

Dolan-Gavitt B. Cell index translation, 2008

<<http://moyix.blogspot.com/2008/02/cell-index-translation.html>>

Dolan-Gavitt B. Enumerating registry hives, 2008

<<http://moyix.blogspot.com/2008/02/enumerating-registry-hives.html>>.

Dolan-Gavitt B. Reading open keys. 2008

<<http://moyix.blogspot.com/2008/02/reading-open-keys.html>>

Dolan-Gavitt B. SysKey and the SAM, 2008

<<http://moyix.blogspot.com/2008/02/syskey-and-sam.html>>

Jones, Kieth J., and Rohyt Belani. "Web Browser Forensics, Part 1." Security Focus. 30 Mar 2005. 13 Apr 2007 <<http://www.securityfocus.com/infocus/1827>>.

Kim Tae-il, 2008, "Web Hacking Defense & Response Education",

<[www.nahs.or.kr/upload/bbs/UPFILE1\\_1245915402.pdf](http://www.nahs.or.kr/upload/bbs/UPFILE1_1245915402.pdf)>

Kim Tae-il, 2009, "Windows Forensics", <<http://www.aegisone.pe.kr/>>

Microsoft, "Description of the Microsoft Windows Registry." Help and Support. 27

Jan 2007. Microsoft Corp. 8 Apr 2007 <<http://support.microsoft.com/kb/256986/>>.  
Microsoft, "INFO: Working with the FILETIME Structure." Help and Support. 23 Jan 2007. Microsoft Corp. 8 Apr 2007 <<http://support.microsoft.com/kb/188768>>.  
Microsoft, "Windows registry information for advanced users." 2008.  
<<http://support.microsoft.com/kb/256986>>  
Mihir Nanavati, Bhavesh Kothari, MIEL Labs, MIEL e-Security Pvt. Ltd., Mumbai, "Detection of Rootkits in the Windows Registry", <[helios.miel-labs.com/downloads/registry.pdf](http://helios.miel-labs.com/downloads/registry.pdf)>  
NirSoft (2004). Protected Storage PassView v1.62 . Recover Protected Storage Passwords. Retrieved October 9, 2005 <<http://www.nirsoft.net/utlis/pspv.html>>  
Opera, "Why Choose the Opera Internet Suite?." Operawiki. 2007. 13 Apr 2007 <<http://operawiki.info/WhyOpera>>.  
PCIN.net, "Windows Registry Tips and Tweaks", 2007, <<http://pcin.net/>>  
PStoreView (2004). Retrieved October 9, 2005  
<<http://www.ntsecurity.nu/toolbox/pstoreview>>  
"Registry Recovery in Windows 2K/XP",  
<<http://forums.pcpur.com/showthread.php?t=384102>>  
"Registry Quick Find Chart." AccessData. 2005. AccessData Corp. 1 Apr 2007  
<[http://www.accessdata.com/media/en\\_US/print/papers/wp.Registry\\_Quick\\_Find\\_Chart.en\\_us.pdf](http://www.accessdata.com/media/en_US/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf)>.  
"ROT 13 Encoder/Decoder." Consulting, Development, Research, and Support. 2007. Edoceo, inc.. 14 Apr 2007 <<http://www.edoceo.com/utilis/rot13.php>>.  
Rusinovich, M. (1999, May). Inside The Registry. Retrieved September 27, 2005  
<<http://www.windowsitpro.com/Articles/Print.cfm?ArticleID=5195>>  
Rusinovich, M. (1997, April). Inside the Windows NT Registry. Retrieved September 27, 2005  
<<http://www.windowsitpro.com/Articles/Print.cfm?ArticleID=122>>  
Shannon, M. (2004, March 26). Accessing and Analyzing the Windows Registry. Retrieved September 25, 2005 <<http://www.agilerm.net/linux2.html>>  
Srinivasan, Ramesh. "Registry MRU Locations." Ramesh's Site: Troubleshooting Windows. 2006. 14 Apr 2007 <<http://windowsxp.mvps.org/RegistryMRU.htm>>.  
Symantec (2004, October 19). Symantec Security Response - Trojan.Watson.A. Retrieved September 30, 2005

<<http://securityresponse.symantec.com/avcenter/venc/data/trojan.watson.a.html>>

Symantec (2005, February 27). Symantec Security Response - W32.Zellome@m. Retrieved September 30, 2005

<<http://securityresponse.symantec.com/avcenter/venc/data/w32.zellome@m.html>>

Tan, J. (2001, July 17). Forensic Readiness. Retrieved September 26, 2005

<[http://www.atstake.com/research/reports/acrobat/atstake\\_forensic\\_readiness.pdf](http://www.atstake.com/research/reports/acrobat/atstake_forensic_readiness.pdf)>

UVCView (2005, June 17). UVCView . Diagnostic Tool for USB Video Class Hardware. Retrieved October 1, 2005,

<<http://www.microsoft.com/whdc/device/stream/vidcap/UVCView.msp>>

Walters A. The Volatility framework: volatile memory artifact extraction utility framework. 2008. <<https://www.volatilesystems.com/default/volatility>>

Websense, "Emerging Threats: Peer-to-Peer File Sharing." Advanced Systems Group. Websense, Inc. 13 Apr 2007

<[http://www.virtual.com/whitepapers/Websense\\_Emerging\\_Threats\\_Peer-to-Peer\\_wp.pdf](http://www.virtual.com/whitepapers/Websense_Emerging_Threats_Peer-to-Peer_wp.pdf)>.

Wong, Lih Wern. "Forensic Analysis of the Windows Registry." Forensic Focus. 1

Feb 2007 <<http://www.forensicfocus.com/index.php?name=Content&pid=73&page=1>>