RP Log Tracker

blueangel

blueangel1275@gmail.com

http://forensic-note.blogspot.kr/

Junghoon Oh

Index

1. Introduction

2. Restore Point

3. RP Log Tracker

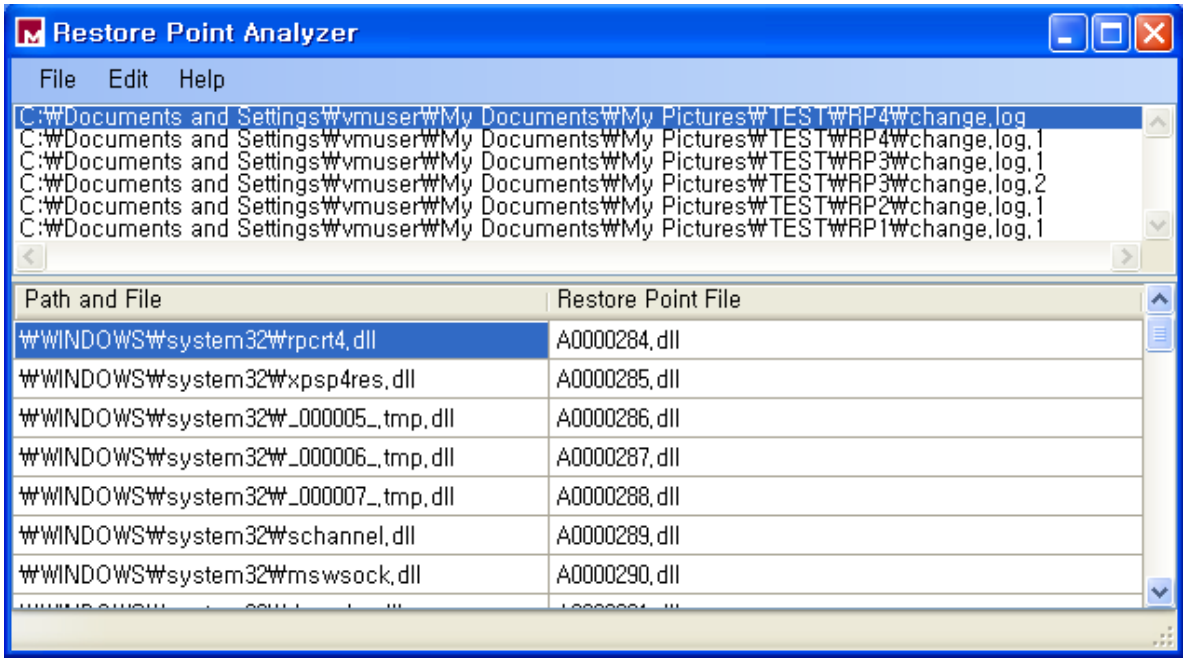
4. Conclusion

Introduction

Restore Point Forensics ?!!

- A long time ago…

- **Why?**
  - **Restore Point Analyzer(created by Mandiant)**
  - **다른 도구는??**

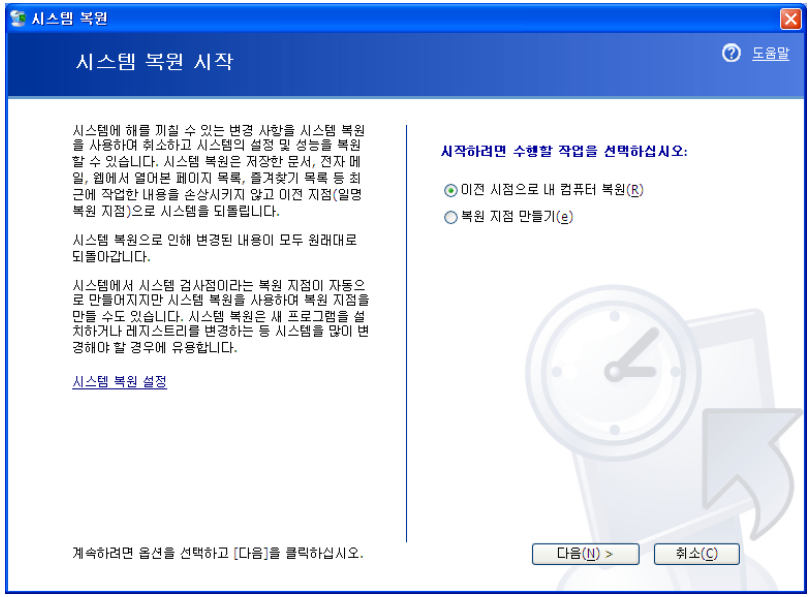


Restore Point

- **복원 지점??**
- 복원 지점 구조

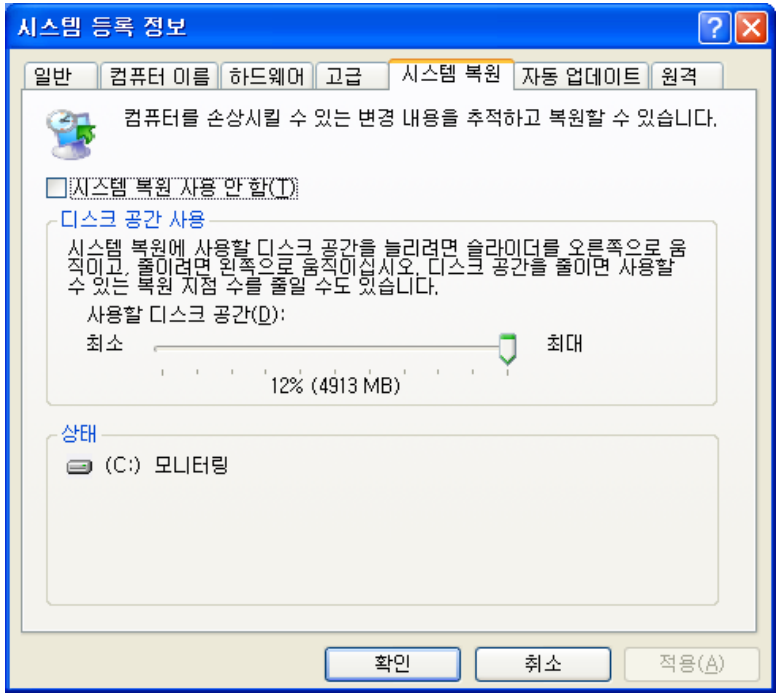
복원 지점??

- **시스템 백업 기능**
  - Windows ME ~ Windows XP
  - Server 버전에는 지원 X
  - 기본적으로 활성화되어 있음
  - 해당 기능은 Vista 로 넘어오면서 VSC(Volume Shadow Copy)가 대체
    - ✓ Vista에서는 두 기능 모두 사용



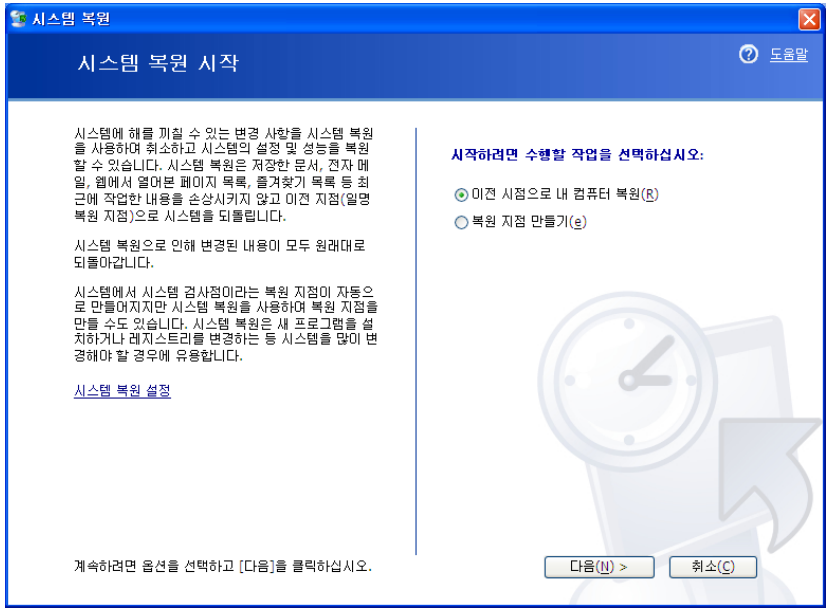
복원 지점??

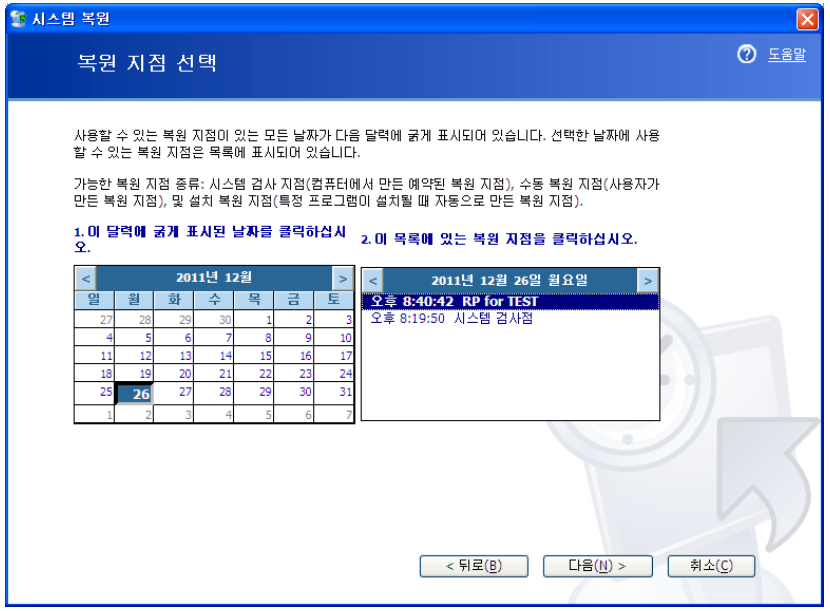
- **설정**
  - 시스템 등록 정보 ➔ 시스템 복원
  - 할당 영역 크기 제한
    - ✓ 볼륨 크기가 4G 이상일 경우 : 볼륨 크기의 12%
    - ✓ 볼륨 크기가 4G 이하일 경우 : 400MB



복원 지점??

- **시스템 복원/복원 지점 만들기**
  - 시작 ➔ 보조프로그램 ➔ 시스템도구 ➔ 시스템 복원





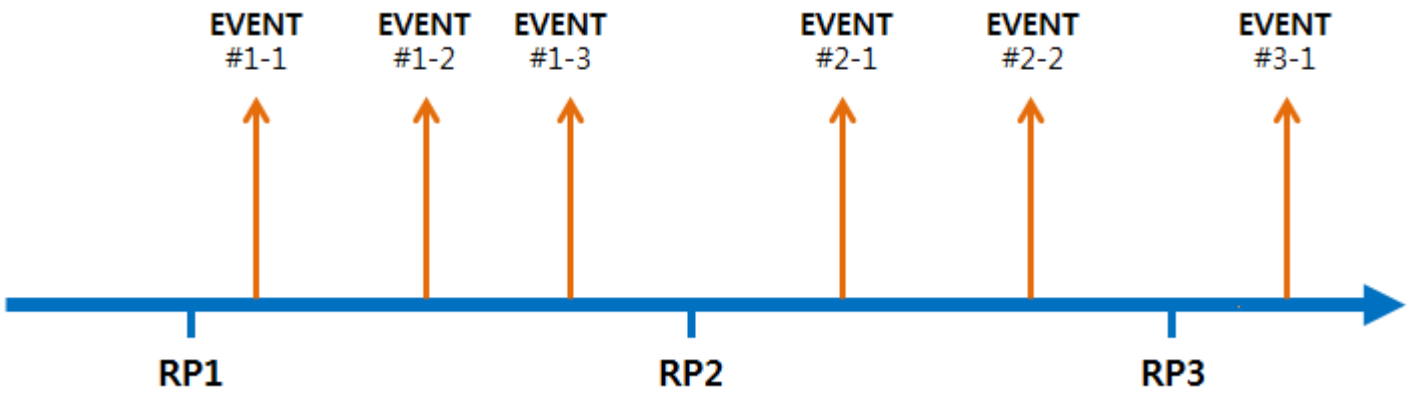
복원 지점??

- **복원 지점 생성 시점**
  - 초기 시스템 검사 시
    - ✓ 운영체제를 설치하고 처음 시작할 때, 시스템 검사와 함께 생성
  - 주기적인 생성
    - ✓ 시스템 켜져 있는 경우에는 24시간 마다 생성
    - ✓ 24시간 이상 꺼져 있는 경우에는 다음 부팅 시 생성
  - 프로그램 설치 및 제거 시
    - ✓ 윈도우 설치 관리자(Windows Installer)에 의해 프로그램을 설치/제거할 때 생성
  - 자동 업데이트 시
    - ✓ 자동 업데이트를 통해 다운받은 업데이트 파일이 설치되기 전 자동으로 생성
  - 시스템 복원 전
    - ✓ 시스템 복원 작업은 시스템을 변경시키므로 복원 작업 전에 생성
  - 서명되지 않은 장치드라이 설치 시
    - ✓ WHQL(Windows Hardware Quality Labs)에 의해 인증되지 않은 드라이버 설치 시 생성
  - 사용자가 수동으로 생성
    - ✓ 시스템 복원 마법사를 통해 사용자가 수동으로 생성

복원 지점??

- **복원 지점 폴더**
  - 복원 지점이 생성되면 아래 경로에 폴더가 생성되고 관련 파일이 저장됨
    - ✓ %HOMEDRIVE%₩System Volume Information₩_restore{GUID}₩RP# (#은 복원지점 생성 번호)

- **복원 지점 원리**
  - 복원 지점 생성 후, 다음 복원 지점이 생성될 때까지 시스템 모니터링하면서 관련 내용 추가
  - 아래의 경우, RP1 복원 지점 생성 후, 각 이벤트 발생시 관련 백업 내용이 RP1 폴더에 저장됨
  - RP2 로 복원할 경우, EVENT #1-3 까지 적용된 이후의 상태로 돌아감



복원 지점??

- **복원 지점에 저장되는 정보들**
  - 레지스트리
    - ✓ 복원 지점 생성시 스냅샷 형태(?)로 백업됨
      - %HOMEDRIVE%₩System Volume Information₩_restore{GUID}₩RP#₩snapshot 폴더 아래 저장됨
    - ✓ 백업된 파일은 레지스트리 분석 도구(ex : REGA)로 분석 가능
  - 사용자 프로파일
  - COM+ DB
  - WFP.dll 캐시
  - WMI DB
  - IIS Metabase
  - filelist.xml에 <Include>가 설정된 항목
    - ✓ filelist.xml : 모니터링 대상 리스트를 저장

Restore Point

- 복원 지점??
- **복원 지점 구조**

복원 지점 구조

- **%SYSTEMROOT%₩system32₩Restore₩**
  - filelist.xml : 모니터링할 대상 리스트 설정
  - MachineGuid.txt : 시스템의 GUID로 "_restore{GUID}" 폴더 경로의 GUID 값과 일치
  - rstrui.exe : 시스템 복원 응용프로그램
  - srdiag.exe : 시스템 복원지점과 관련된 텍스트 파일(cfg, txt, log, xml)을 CAB 형식 변환
  - srframe.mmf : 시스템 복원 응용프로그램과 관련된 설정 파일

- **%HOMEDRIVE%₩System Volume Information₩_restore{GUID}₩**
  - _driver.cfg : 드라이버와 관련된 설정 정보를 저장
  - _filelst.cfg : filelist.xml의 설정 정보를 저장
  - drivetable.txt : 각 볼륨의 마운트 포인트 위치, 볼륨 상태, 복원지점 공간 정보를 저장
  - RestorePointSize : 시스템 복원지점의 크기를 저장
  - snapshot (DIR) : 레지스트리 스냅샷이 저장된 폴더
  - A#######.(원본파일의 확장자) : 백업된 파일 복사본 (####### 번호는 백업 순서)
  - rp.log : 복원지점 생성 시 발생한 이벤트 및 생성 시간이 저장
  - change.log(change.log.#) : 모니터링 로그
  - fifo.log : 복원지점에 할당된 용량의 90%가 넘으면, 자동 삭제하여 75%까지 용량을 줄이는데 이 때 제거되는 파일들의 정보를 기록

복원 지점 구조

- **filelist.xml**
  - 모니터링할 대상 리스트 설정
  - XML 포멧
  - 주요 노드(우선순위순)
    - ✓ <FILES> : 모니터링할 파일 설정
    - ✓ <DIRECTORIES> : 모니터링할 디렉터리 설정
    - ✓ <EXTENSIONS> : 모니터링할 확장자 설정
  - 서브 노드
    - ✓ <Include> : 모니터링 목록
    - ✓ <Exclude> : 모니터링 제외 목록
  - filelist.xml에 설정된 파일들은 생성, 변경, 삭제 이벤트가 발생할 때마다 이벤트 내역, 경로, 파일의 복사본 등이 백업됨

복원 지점 구조

- **filelist.xml 의 예**

```
<PCHealthProtect>
    <VERSION>1.0</VERSION>
    <DEFTYPE>E</DEFTYPE>
    <FILES>
        <Exclude>
            <REC>%windir%₩system.ini</REC>
            <REC>%windir%₩tasks₩desktop.ini</REC>
            <REC>%windir%₩win.ini</REC>
            <REC>*:₩AUTOEXEC.BAT</REC>
            <REC>*:₩CONFIG.MSI</REC>
            <REC>*:₩CONFIG.SYS</REC>
            <REC>*:₩DUMPFILE.SYS</REC>
        </Exclude>
        <Include>
            <REC>c:₩placeholder₩ph.dll</REC>
        </Include>
    </FILES>
    <DIRECTORIES>
        <Exclude>
            <REC>%cookies%</REC>
            <REC>%favorites%</REC>
            <REC>%History%</REC>
            <REC>%internetcache%</REC>
            <REC>%nethood%</REC>
            <REC>%personaldocuments%</REC>
            <REC>%ProgramFiles%₩WindowsUpdate</REC>
            <REC>%windir%₩Downloaded Program Files</REC>
            <REC>%windir%₩SoftwareDistribution</REC>
            <REC>%windir%₩Offline Web Pages</REC>
            <REC>%windir%₩PCHealth₩HelpCtr₩Config</REC>
            <REC>%windir%₩PCHealth₩HelpCtr₩Database</REC>
            <REC>%windir%₩PCHealth₩HelpCtr₩DataColl</REC>
            <REC>%windir%₩PCHealth₩HelpCtr₩System</REC>
            <REC>%windir%₩PCHealth₩HelpCtr₩Vendors</REC>
            <REC>%windir%₩pchealth₩ErrorRep₩UserDumps</REC>
            <REC>%windir%₩prefetch</REC>
            <REC>%windir%₩temp</REC>
            <REC>*:₩~MSSETUP.T</REC>
            <REC>*:₩$WIN_NT$.~LS</REC>
            <REC>*:₩$WIN_NT$.~BT</REC>
            <REC>%windir%₩$NtServicePackUninstall$</REC>
            <REC>%windir%₩security₩Database</REC>
            <REC>*:₩System Volume Information</REC>
            <REC>*:₩SIS Common Store</REC>
            <REC>*:₩TEMP</REC>
            <REC>*:₩TMP</REC>
            <REC>*:₩₩95UNDO.INI</REC>
            <REC>*:₩₩98UNDO.INI</REC>
            <REC>*:₩₩SXUNDO.INI</REC>
            <REC>*:₩₩ININSTO.400</REC>
            <REC>*:₩₩INLFN.INI</REC>
            <REC>*:₩₩INUNDO.INI</REC>
            <REC>%SRDataStoreRoot%</REC>
            <REC>%windir%₩system32₩wbem₩repository</REC>
            <REC>%windir%₩system32₩wbem₩repository.tmp</REC>
            <REC>%windir%₩system32₩wbem₩repository.bak</REC>
            <REC>%SystemDrive%₩Documents And Settings₩All Users₩Favorites</REC>
            <REC>%SystemDrive%₩Documents And Settings₩All Users₩Documents</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩My Documents</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩NetHood</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩Favorites</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩Cookies</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩Cache</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩Local Settings₩History</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩Local Settings₩Temp</REC>
            <REC>%SystemDrive%₩Documents And Settings₩Default User₩Local Settings₩Temporary Internet Files</REC>

        </Exclude>
        <Include>
            <REC>*:₩Documents And Settings₩*₩Application Data₩Microsoft₩Internet Explorer₩Quick Launch</REC>
        </Include>
    </DIRECTORIES>
    <EXTENSIONS>
        <Include>
            <REC>~~C</REC>
            <REC>~~D</REC>
            <REC>12A</REC>
            <REC>1PA</REC>
            <REC>1ST</REC>
            <REC>386</REC>
            <REC>8BA</REC>
            <REC>8BY</REC>
            <REC>8LI</REC>
            <REC>A2A</REC>
            <REC>AAS</REC>
            <REC>AAX</REC>
            <REC>ABM</REC>
            <REC>ABR</REC>
            <REC>ACF</REC>
            <REC>ACG</REC>
            <REC>ACO</REC>
            <REC>ACS</REC>
            <REC>ADK</REC>
            <REC>ADW</REC>
            <REC>ADX</REC>
            <REC>AFM</REC>
            <REC>AID</REC>
            <REC>AIP</REC>
            <REC>ALT</REC>
            <REC>AM</REC>
            <REC>AMB</REC>
            <REC>APL</REC>
            <REC>APM</REC>
            <REC>APP</REC>
                .....

            <REC>VDB</REC>
            <REC>VER</REC>
            <REC>VFM</REC>
            <REC>VFX</REC>
            <REC>VIL</REC>
            <REC>VLX</REC>
            <REC>VM</REC>
            <REC>VOF</REC>
            <REC>VPH</REC>
            <REC>VPX</REC>
            <REC>VQA</REC>
            <REC>VQM</REC>
            <REC>VSC</REC>
            <REC>VSH</REC>
            <REC>VWP</REC>
            <REC>VXD</REC>
            <REC>W32</REC>
            <REC>W98</REC>
            <REC>WA_</REC>
            <REC>WBD</REC>
            <REC>WBM</REC>
            <REC>WCD</REC>
            <REC>WDL</REC>
            <REC>WDS</REC>
            <REC>WINSYS</REC>
            <REC>WIPEINFO</REC>
            <REC>WIPESLACK</REC>
            <REC>WMZ</REC>
            <REC>WPC</REC>
            <REC>WPX</REC>
            <REC>WRF</REC>
            <REC>WSL</REC>
            <REC>WTB</REC>
            <REC>WTR</REC>
            <REC>XLL</REC>
            <REC>XMX</REC>
            <REC>XRS</REC>
            <REC>XTU</REC>
            <REC>ZFSENDTOTARGET</REC>
            <REC>ZH</REC>
            <REC>ZH_TW</REC>
            <REC>ZHW</REC>
        </Include>
    </EXTENSIONS>
</PCHealthProtect>
```

복원 지점 구조

- **snapshot 폴더**
  - 백업된 레지스트리 파일이 저장됨
  - 복원 지점 생성시, 동시에 폴더 생성 및 백업

- **A########.(원본파일의 확장자)**
  - 백업 파일
  - 확장자는 유지됨
  - 원본 파일이 변경 및 삭제시 백업됨
  - **원본 파일의 시간 정보 유지됨~!!**
    - ✓ Create Time
    - ✓ Modify Time
    - ✓ Access Time
    - ✓ MFT Modified Time

Name	File Created	Last Written	Last Accessed	Entry Modified
A0074180.sys	2013-01-09 08:39:07	2013-04-06 21:36:20	2013-04-08 00:52:41	2013-04-06 21:36:20
A0074181.sys	2013-01-09 08:39:07	2013-04-06 21:36:20	2013-04-06 22:36:22	2013-04-06 21:36:20
A0074182.sys	2013-01-09 08:39:07	2013-04-06 21:36:20	2013-04-06 22:36:22	2013-04-06 21:36:20
A0074183.sys	2011-12-20 11:12:05	2013-04-06 21:36:20	2013-04-06 22:36:22	2013-04-06 21:36:20
A0074184.old	2013-01-09 08:39:11	2013-04-06 21:36:20	2013-04-06 22:36:22	2013-04-06 21:36:20
A0074185.out	2013-01-09 08:49:50	2013-04-06 21:36:21	2013-04-08 00:52:41	2013-04-06 22:36:22
A0074186.old	2013-01-09 08:39:14	2013-04-06 21:36:21	2013-04-06 22:36:22	2013-04-06 21:36:21
A0074187.old	2013-04-04 18:35:30	2013-04-06 21:36:21	2013-04-06 21:36:21	2013-04-06 21:36:21
A0074188.old	2013-01-09 08:39:15	2013-04-06 21:36:21	2013-04-06 22:36:23	2013-04-06 21:36:21

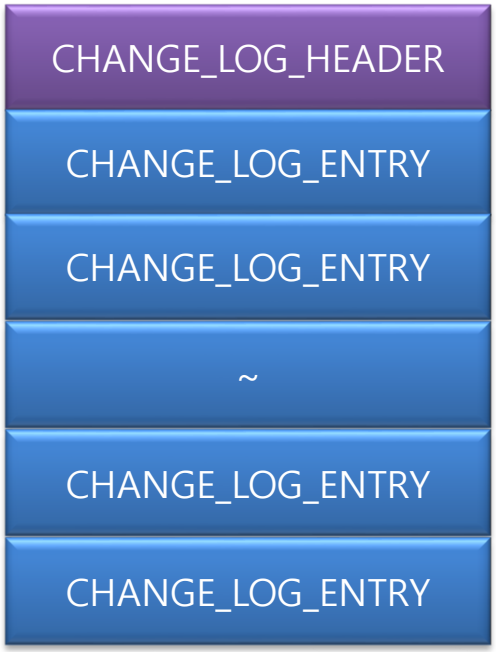
복원 지점 구조

- **rp.log**
  - 복원 지점 이름, 생성 시간, 생성원인 등의 정보가 저장됨
  - 이벤트 유형 및 복원지점 유형에 대한 자세한 정보는
    ➔ http://msdn.microsoft.com/en-us/library/windows/desktop/aa378903(v=vs.85).aspx

위치	크기	설명
0 – 3	4 bytes	이벤트 유형 0×00000064(100) : BEGIN_SYSTEM_CHANGE 0×00000065(101) : END_SYSTEM_CHANGE 0×00000066(102) : BEGIN_NESTED_SYSTEM_CHANGE 0×00000067(103) : END_NESTED_SYSTEM_CHANGE
4 – 7	4 bytes	복원지점 유형 0×00000000(0) : APPLICATION_INSTALL 0×00000001(1) : APPLICATION_UNINSTALL 0×00000002(2) : DESKTOP_SETTING 0×00000003(3) : ACCESSIBILITY_SETTING 0×00000004(4) : OE_SETTING 0×00000005(5) : APPLICATION_RUN 0×00000006(6) : RESTORE 0×00000007(7) : CHECKPOINT 0×00000008(8) : WINDOWS_SHUTDOWN 0×00000009(9) : WINDOWS_BOOT 0x0000000A(10) : DEVICE_DRIVER_INSTALL 0x0000000B(11) : FIRSTRUN 0x0000000C(12) : MODIFY_SETTINGS 0x0000000D(13) : CANCELLED_OPERATION 0x0000000E(14) : BACKUP_RECOVERY
8 – 15	8 bytes	순서번호
16 – 527	512 bytes	복원지점 이름(유니코드)
528 – 535	8 bytes	복원지점 생성시간 (Windows 64bit Time)

복원 지점 구조

- **change.log**
  - 모니터링 로그
  - 생성, 변경, 삭제, 이름변경 등의 이벤트가 기록됨
  - 파일 구조 : CHANGE_LOG_HEADER + CHANGE_LOG_ENTRY(s)



복원 지점 구조

- **change.log(계속)**
  - **CHANGE_LOG_HEADER**

위치	크기	설명
0 – 7	8 bytes	레코드 헤더 (RECORD_HEADER)
8 – 11	4 bytes	시그니처 (0xABCDEF12)
12 – 15	4 bytes	로그 버전 (항상 0×00000002)
16 – 23	8 bytes	데이터 헤더 (RECORD_HEADER)
24 -	4 bytes	로그 이름

  - **RECORD_HEADER**

위치	크기	설명
0 – 3	4 bytes	엔트리 크기
4 – 7	4 bytes	레코드 유형 0×00000000 : LogHeader 0×00000001 : LogEntry 0×00000002 : VolumePath 0×00000003 : FirstPath => Target Path 0×00000004 : SecondPath => Renamed Path 0×00000005 : TempPath => Backup Path 0×00000006 : AclInline 0×00000007 : AclFile 0×00000008 : DebugInfo 0×00000009 : ShortName

복원 지점 구조

- change.log(계속)
  - CHANGE_LOG_ENTRY

위치	크기	설명
0 – 7	8 bytes	레코드 헤더 (RECORD_HEADER)
8 – 11	4 bytes	시그니처 (0xABCDEF12)
12 – 15	4 bytes	엔트리 유형 0×00000001 : STREAMCHANGE 0×00000002 : ACLCHANGE 0×00000004 : ATTRCHANGE 0×00000008 : STREAMOVERWRITE 0×00000010 : FILEDELETE 0×00000020 : FILECREATE 0×00000040 : FILERENAME 0×00000080 : DIRCREATE 0×00000100 : DIRRENAME 0×00000200 : DIRDELETE 0×00000400 : MOUNTCREATE 0×00000800 : MOUNTDELETE 0×00001000 : VOLUMEERROR 0×00002000 : STREAMCREATE 0×00010000 : NOOPTIMIZE 0×00020000 : ISDIR 0×00040000 : ISNOTDIR 0×00080000 : SIMULATEDELETE 0×00100000 : INPRECREATE 0×00200000 : OPENBYID
16 – 19	4 bytes	엔트리 플래그 0×00000001 : TEMPPATH 0×00000002 : SECONDPATH 0×00000004 : ACLINFO 0×00000008 : DEBUGINFO 0×00000010 : SHORTNAME
20 – 23	4 bytes	파일 속성
24 – 31	8 bytes	순서번호
32 – 63	32 bytes	0×00000000
64 ~		이후 부터는 레코드 반복, 각 레코드들은 레코드 헤더 정보를 RECORD_HEADER 형식으로 가지고 있음

복원 지점 구조

- **change.log(계속)**
  - RP# 폴더 아래 change.log.# 파일들의 생성시간이 **모두 같음**;;
    1. 현재 모니터링 내용은 change.log 파일에 기록됨
    2. 로그 파일 변경시(이유모름 —,.—), change.log 파일을 change.log.# 파일로 변경함
    3. 새로운 change.log 파일을 생성하여 모니터링 내용을 기록함
    4. 새로 생성되는 change.log 파일을 "파일 시스템 터널링" 에 의해 이전 파일의 생성시간이 유지됨

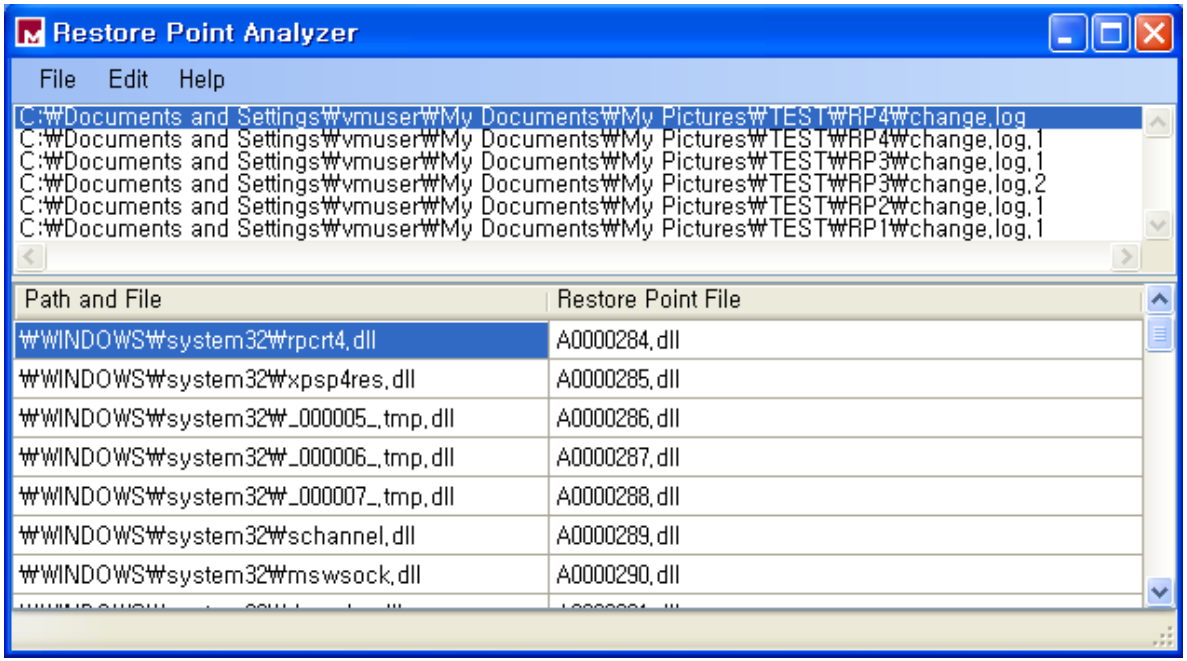
Name	File Created	Last Written	Last Accessed	Entry Modified
change.log.1	2013-02-20 00:00:32	2013-02-20 00:06:45	2013-02-20 19:00:29	2013-02-20 00:06:45
change.log.2	2013-02-20 00:00:32	2013-02-20 00:10:25	2013-02-20 19:00:30	2013-02-20 00:10:25
change.log.3	2013-02-20 00:00:32	2013-02-20 00:38:37	2013-02-20 19:00:31	2013-02-20 08:29:24
change.log.4	2013-02-20 00:00:32	2013-02-20 13:22:57	2013-02-20 19:00:31	2013-02-20 13:25:49
change.log.5	2013-02-20 00:00:32	2013-02-20 15:16:51	2013-02-20 19:00:31	2013-02-20 15:16:57

TimeStamp	USN	FileName	Full Path(from $MFT)	Event
2013-04-02 18:07:13	4583177024	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added, Data_Overwritten, File_Closed
2013-04-03 08:27:59	4583181208	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Renamed_Old
2013-04-03 08:27:59	4583181288	change.log.1	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log.1	File_Renamed_New
2013-04-03 08:27:59	4583181376	change.log.1	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log.1	File_Renamed_New, File_Closed
2013-04-03 08:27:59	4583181464	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created
2013-04-03 08:28:00	4583183608	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added
2013-04-03 08:28:51	4583385856	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added, Data_Overwritten
2013-04-03 13:27:23	4591257880	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added, Data_Overwritten, File_Closed
2013-04-04 08:32:26	4591261912	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Renamed_Old
2013-04-04 08:32:26	4591261992	change.log.2	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log.2	File_Renamed_New
2013-04-04 08:32:26	4591262080	change.log.2	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log.2	File_Renamed_New, File_Closed
2013-04-04 08:32:26	4591262168	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created
2013-04-04 08:32:26	4591264272	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added
2013-04-04 08:39:02	4591761904	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added, Data_Overwritten
2013-04-04 08:59:29	4592386576	change.log	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log	File_Created, File_Added, Data_Overwritten, File_Renamed_Old
2013-04-04 08:59:29	4592386656	change.log.3	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log.3	File_Created, File_Added, Data_Overwritten, File_Renamed_New
2013-04-04 08:59:29	4592386744	change.log.3	₩System Volume Information₩_restore{CA7A4D52-B42C-4E6D-A8C8-6DA391EDAB9A}₩RP704₩change.log.3	File_Created, File_Added, Data_Overwritten, File_Renamed_New, File_Closed

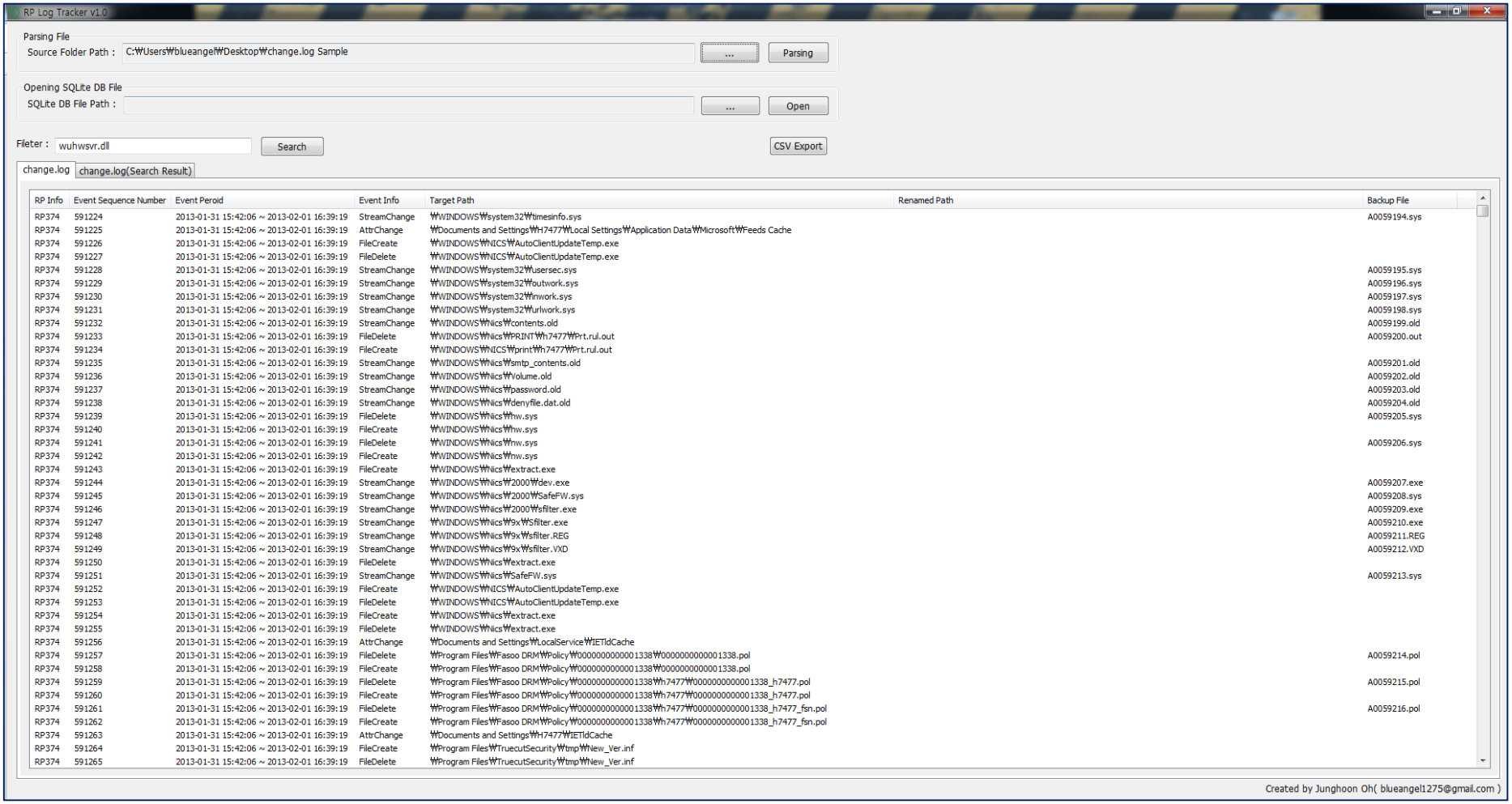
RP Log Tracker

Why?

- **Restore Point Analyzer(created by Mandiant)**
  - 백업 파일의 원본 파일 간의 관계만 알려줌;;
  - Change.log 에 있는 생성, 수정, 삭제, 이름 변경 이벤트는???

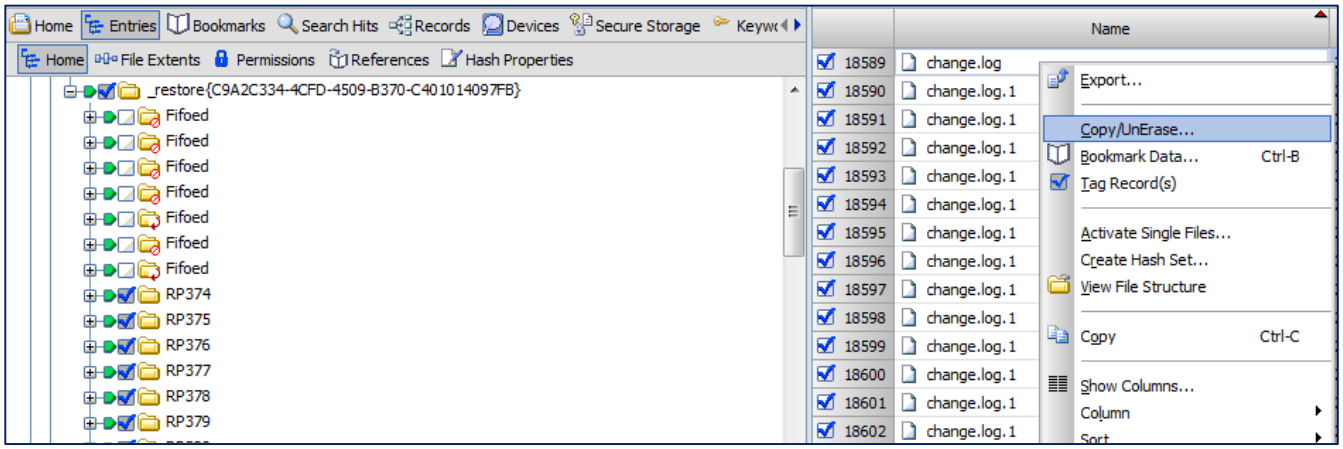


도구 개발

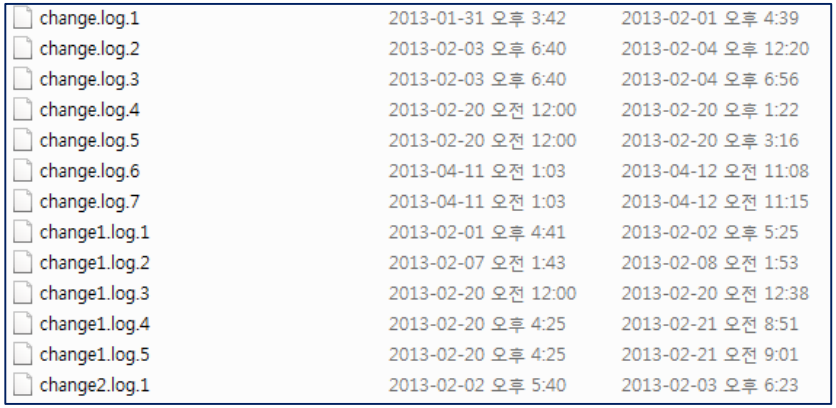

RP Log Tracker v1.0
Parsing File
Source Folder Path : C:₩Users₩blueangel₩Desktop₩change.log Sample
...
Parsing
Opening SQLite DB File
SQLite DB File Path :
...
Open
Fileter : wuhwsvr.dll
Search
CSV Export
change.log
change.log(Search Result)
RP Info | Event Sequence Number | Event Peroid | Event Info | Target Path | Renamed Path | Backup File
RP374 | 591224 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩system32₩timesinfo.sys | | A0059194.sys
RP374 | 591225 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | AttrChange | ₩Documents and Settings₩H7477₩Local Settings₩Application Data₩Microsoft₩Feeds Cache | |
RP374 | 591226 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩NICS₩AutoClientUpdateTemp.exe | |
RP374 | 591227 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩NICS₩AutoClientUpdateTemp.exe | |
RP374 | 591228 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩system32₩usersec.sys | | A0059195.sys
RP374 | 591229 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩system32₩outwork.sys | | A0059196.sys
RP374 | 591230 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩system32₩nwork.sys | | A0059197.sys
RP374 | 591231 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩system32₩urlwork.sys | | A0059198.sys
RP374 | 591232 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩contents.old | | A0059199.old
RP374 | 591233 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩nics₩PRINT₩h7477₩Prt.rul.out | | A0059200.out
RP374 | 591234 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩NICS₩print₩h7477₩Prt.rul.out | |
RP374 | 591235 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩smtp_contents.old | | A0059201.old
RP374 | 591236 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩volume.old | | A0059202.old
RP374 | 591237 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩password.old | | A0059203.old
RP374 | 591238 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩denyfile.dat.old | | A0059204.old
RP374 | 591239 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩nics₩nw.sys | | A0059205.sys
RP374 | 591240 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩nics₩nw.sys | |
RP374 | 591241 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩nics₩nw.sys | | A0059206.sys
RP374 | 591242 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩nics₩nw.sys | |
RP374 | 591243 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩nics₩extract.exe | |
RP374 | 591244 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩2000₩dev.exe | | A0059207.exe
RP374 | 591245 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩2000₩SafeFW.sys | | A0059208.sys
RP374 | 591246 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩2000₩sfilter.exe | | A0059209.exe
RP374 | 591247 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩9x₩sfilter.exe | | A0059210.exe
RP374 | 591248 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩9x₩sfilter.REG | | A0059211.REG
RP374 | 591249 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩9x₩sfilter.VXD | | A0059212.VXD
RP374 | 591250 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩nics₩extract.exe | |
RP374 | 591251 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | StreamChange | ₩WINDOWS₩nics₩SafeFW.sys | | A0059213.sys
RP374 | 591252 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩NICS₩AutoClientUpdateTemp.exe | |
RP374 | 591253 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩NICS₩AutoClientUpdateTemp.exe | |
RP374 | 591254 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩WINDOWS₩nics₩extract.exe | |
RP374 | 591255 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩WINDOWS₩nics₩extract.exe | |
RP374 | 591256 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | AttrChange | ₩Documents and Settings₩LocalService₩IETldCache | |
RP374 | 591257 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩Program Files₩Fasoo DRM₩Policy₩00000000000001338₩00000000000001338.pol | | A0059214.pol
RP374 | 591258 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩Program Files₩Fasoo DRM₩Policy₩00000000000001338₩00000000000001338.pol | |
RP374 | 591259 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩Program Files₩Fasoo DRM₩Policy₩00000000000001338₩h7477₩00000000000001338_h7477.pol | | A0059215.pol
RP374 | 591260 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩Program Files₩Fasoo DRM₩Policy₩00000000000001338₩h7477₩00000000000001338_h7477.pol | |
RP374 | 591261 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩Program Files₩Fasoo DRM₩Policy₩00000000000001338₩h7477₩00000000000001338_h7477_fsn.pol | | A0059216.pol
RP374 | 591262 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩Program Files₩Fasoo DRM₩Policy₩00000000000001338₩h7477₩00000000000001338_h7477_fsn.pol | |
RP374 | 591263 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | AttrChange | ₩Documents and Settings₩H7477₩IETldCache | |
RP374 | 591264 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileCreate | ₩Program Files₩TruecutSecurity₩tmp₩New_Ver.inf | |
RP374 | 591265 | 2013-01-31 15:42:06 ~ 2013-02-01 16:39:19 | FileDelete | ₩Program Files₩TruecutSecurity₩tmp₩New_Ver.inf | |
Created by Junghoon Oh(blueangel1275@gmail.com)

도구 사용법

- **Change.log 파일 수집**
  - Encase 와 같은 도구를 통해 change.log 파일들을 시간 정보를 유지하면서 수집

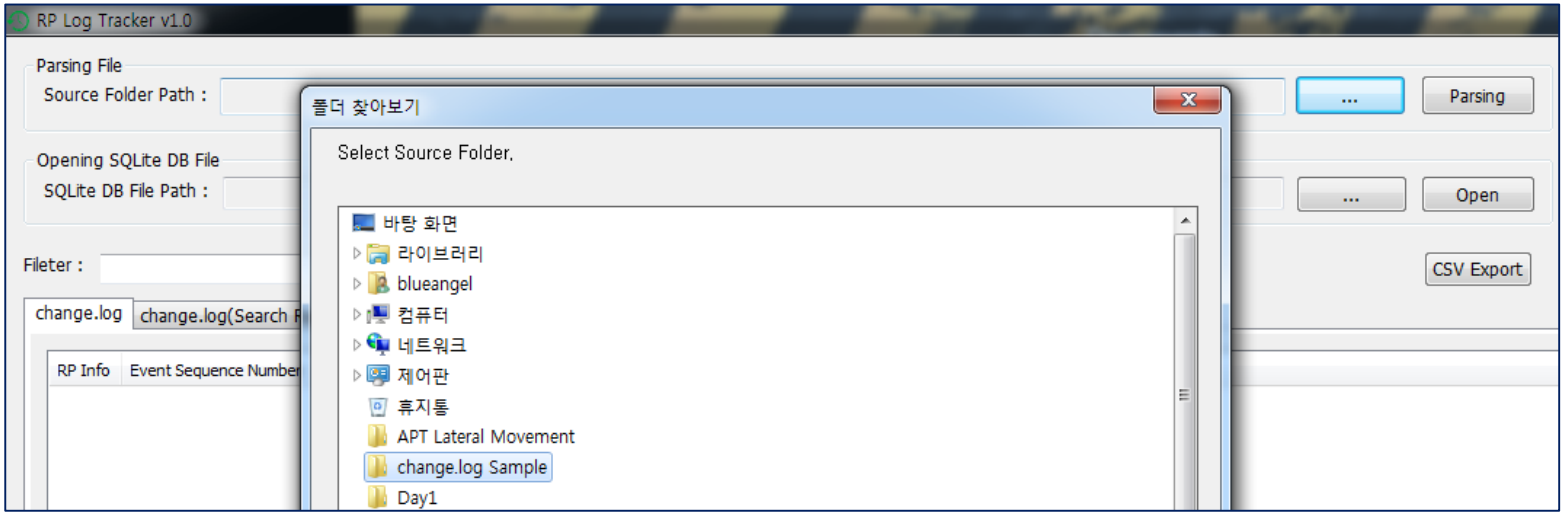


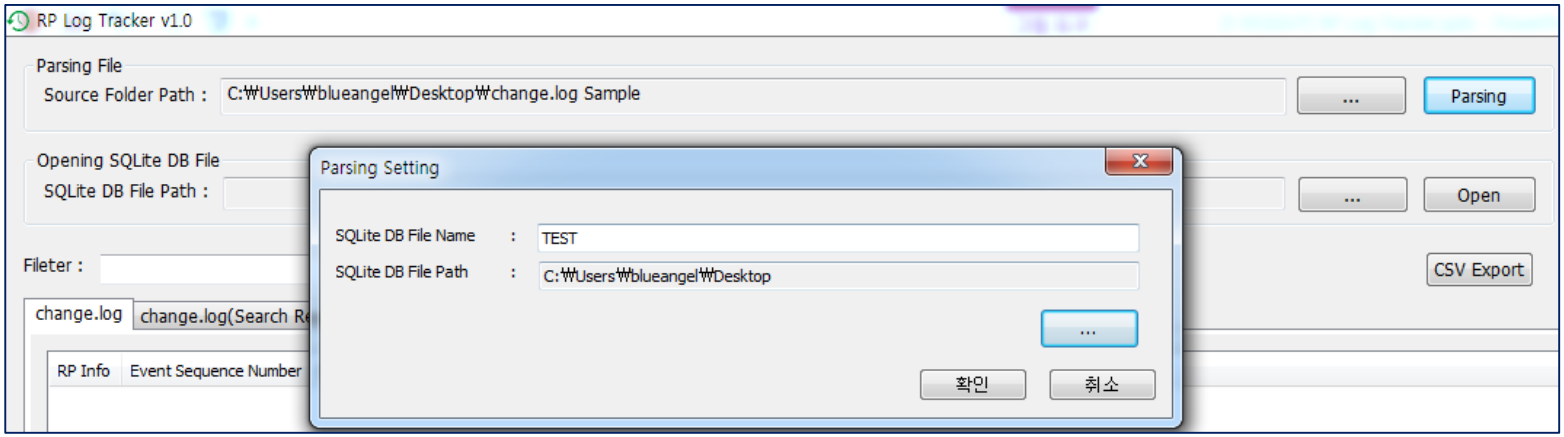
  - 수집한 파일들을 한 폴더에 저장함(시간정보 유지되어야함~!!)



도구 사용법

- 수집한 폴더를 입력으로 Parsing 시작~!!!





이벤트 발생 시간대 구하는 방법??

- **RP# 폴더 아래 change.log 파일들의 생성시간은 모두 같음;;**
  - 첫 번째 파일의 이벤트 발생 시간 구간은 "생성시간 ~ 수정시간" 으로 계산
  - 그 다음 파일 부터는 "전 파일의 수정시간 ~ 현재 파일의 수정시간 " 으로 계산

Name	File Created	Last Written	Last Accessed	Entry Modified
change.log.1	2013-02-20 00:00:32	2013-02-20 00:06:45	2013-02-20 19:00:29	2013-02-20 00:06:45
change.log.2	2013-02-20 00:00:32	2013-02-20 00:10:25	2013-02-20 19:00:30	2013-02-20 00:10:25
change.log.3	2013-02-20 00:00:32	2013-02-20 00:38:37	2013-02-20 19:00:31	2013-02-20 08:29:24
change.log.4	2013-02-20 00:00:32	2013-02-20 13:22:57	2013-02-20 19:00:31	2013-02-20 13:25:49
change.log.5	2013-02-20 00:00:32	2013-02-20 15:16:51	2013-02-20 19:00:31	2013-02-20 15:16:57

  - 계산 예
    - ✓ Change.log.1 ➔ 00:00:32 ~ 00:06:45
    - ✓ Change.log.2 ➔ 00:06:45 ~ 00:10:25
    - ✓ Change.log.3 ➔ 00:10:25 ~ 00:38:37
    - ✓ Change.log.4 ➔ 00:38:37 ~ 13:22:57
    - ✓ Change.log.5 ➔ 13:22:57 ~ 15:16:51

복원 지점 활용 방안

- **백업 파일**
  - 백업된 파일은 원본 파일과 동일
  - 활용
    - ✓ **용의자가 고의로 삭제한 파일 복구**
    - ✓ **삭제된 악성코드 탐지**
      - 백업 파일들을 대상으로 Anti-Virus 프로그램 수행
        - ➔ 마운트하고 수행하면 System Volume Information 폴더에 접근 못함...;;
        - ➔ 파일 추출 혹은 System Volume Information 폴더와 그 하위 모든 파일들의 소유자를 현재 시스템 계정으로 변경

- **rp.log**
  - 복원 지점 생성 시간, 생성 원인 저장
  - 활용
    - ✓ **설치/제거된 프로그램 흔적 추적**
    - ✓ **인증 받지 않은 드라이버 설치 흔적 추적**

복원 지점 활용 방안(계속)

- **change.log**
  - 파일 시스템의 생성, 수정, 삭제, 이름 변경 이벤트 저장
  - 활용
    - ✓ **파일 시스템 히스토리 추적**
      - $LogFile, $UsnJrnl 에 저장된 로그는 기간이 너무 짧음;; ➔ **복원 지점은 최대 90일까지 저장**
      - **악성코드 흔적 추적**

RP Info	Event Sequence Number	Event Peroid	Event Info	Target Path
RP449	714765	2013-04-11 01:03:48 ~ 2013-04-11 21:05:11	FileCreate	₩windows₩system32₩BusMgr.sys
RP449	714766	2013-04-11 01:03:48 ~ 2013-04-11 21:05:11	FileCreate	₩windows₩System32₩6to4adv.dll
RP449	714767	2013-04-11 01:03:48 ~ 2013-04-11 21:05:11	FileCreate	₩Documents and Settings₩Default User₩Application Data₩Microsoft₩ODBC.INI
RP449	714768	2013-04-11 01:03:48 ~ 2013-04-11 21:05:11	FileCreate	₩Program Files₩Common Files₩ODBC₩msjet.dll
RP449	714769	2013-04-11 01:03:48 ~ 2013-04-11 21:05:11	FileCreate	₩Program Files₩Common Files₩ODBC₩jet.dll
RP449	714770	2013-04-11 01:03:48 ~ 2013-04-11 21:05:11	StreamChange	₩WINDOWS₩system32₩spoolss.dll

      - **문서 열람 흔적 추적**

RP Info	Event Sequence Number	Event Peroid	Event Info	Target Path
RP374	591772	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Recent₩2.6 백업관리대장_20121023.xls.lnk
RP374	591773	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Recent₩13년 대기자료.lnk
RP374	591774	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileDelete	₩Documents and Settings₩H7477₩Recent₩2.6 백업관리대장_20121023.xls.lnk
RP374	591775	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Recent₩2.6 백업관리대장_20121023.xls.lnk
RP374	591776	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileDelete	₩Documents and Settings₩H7477₩Recent₩13년 대기자료.lnk
RP374	591777	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Recent₩13년 대기자료.lnk
RP374	591778	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileDelete	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩13년 대기자료.LNK
RP374	591779	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩2.6 백업관리대장_20121023.xls.LNK
RP374	591780	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩13년 대기자료.LNK
RP374	591781	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileDelete	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩2.9. 월별 정기점검 내역(표지)_20111019.xls.LNK
RP374	591782	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileDelete	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩2.6 백업관리대장_20121023.xls.LNK
RP374	591783	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileDelete	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩13년 대기자료.LNK
RP374	591784	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩2.6 백업관리대장_20121023.xls.LNK
RP374	591785	2013-01-31 15:42:06 ~ 2013-02-01 16:39:19	FileCreate	₩Documents and Settings₩H7477₩Application Data₩Microsoft₩Office₩Recent₩13년 대기자료.LNK

Conclusion

Conclusion

- **백만년 된 Restore Point Forensics…**
  - Win XP 시스템은 아직도 존재…예산 문제???

- **RP Log Tracker**
  - 기존 도구의 불편함…
  - change.log 파싱 ➔ 파일 시스템 히스토리 추적~!!(정확한 시간은 몰라요…ㅠ.ㅠ)

Question and Answer