포렌식 관점에서의 시스템 복원지점 활용 방안[1)]

*윤선미 **이석희 ***이상진

고려대학교 정보보호기술연구센터

*sera314@korea.ac.kr

Usage of System Restore Point in Digital Forensics

*Yun, Sun-mi **Lee, Seokhee ***Lee, Sangjin

Center for Information Security Technologies, Korea University

요 약

디지털 증거분석 단계에서 조사관은 용의자 시스템을 통해 사건 날짜와 시간에 실행된 응용 프로그램이나 악성 프로그램의 설치 여부 등을 유추하여 관련 증거를 발견할 수 있다. 그러나 대부분의 범죄자는 혐의 부인을 위해 대상 시스템에서 특정 프로그램의 설치 및 사용 정보를 삭제하여 증거를 인멸한다. 이와 같이 디지털 포렌식 조사를 방해하는 기술이나 도구와 관련된 분야를 안티포렌식(Anti-Forensics)이라 한다. 사이버 범죄의 증가로 인해 디지털 포렌식 기술이 발전할수록 범죄의 흔적을 남기지 않기 위한 안티포렌식 기술 또한 발전하고 있다. 이러한 안티포렌식에 대응하기 위해, 본 논문에서는 프로그램 사용 또는 설치와 같은 흔적을 시스템에서 삭제한 경우 시스템 복원지점을 이용한 증거탐지 방법을 제시한다. 또한 실제 발생 가능한 상황을 예로 들어 설명하고 수사 시 유용하게 쓰일 수 있는 도구 개발에 대한 계획을 제시한다.

1. 서론

최근 발달된 IT 기술을 악용하는 사이버 범죄가 증가하고 있어 그 피해가 사회적으로 문제가 되고 있다. 이는 우리의 생활을 매우 편리하게 만들어주는 최첨단 기술의 또 다른 이면이라 할 수 있다. 이러한 사이버 범죄의 증가로 인해 디지털 포렌식 분야의 다양한 기술들이 점차 발전되고 있다. 이에 대응하여 범죄자들은 흔적을 남기지 않기 위한 기술을 개발하기 위해 노력하고 있으며, 이러한 기술들을 안티포렌식(Anti-Forensics)이라 한다. 안티포렌식이란 디지털 포렌식에 대항하는 수단 및 행동 등을 의미하며, 디지털 증거의 유효성과 유용성을 약화시키기 위한 모든 시도를 포함한다.[1] 더욱이 IT 기술의 발달에 힘입어 안티포렌식을 위한 도구의 개발자들 또한 더욱 강화된 기술을 이용하고 있으며,[2] 이러한 안티포렌식에 대응하여 컴퓨터에 남아 있는 증거나 흔적을 찾기 위한 컴퓨터 포렌식 기술도 점차 발달하고 있다.[3]

디지털 포렌식 절차는 사건이 발생한 후 디지털 증거를 수집하기 위한 절차를 기술하고 있으며, 그 절차는 다음과 같다.[4]

그림 [1] 디지털 포렌식 절차

사이버 범죄가 발생하면 디지털 포렌식 수사 절차에 따라 수사를 진행하며, 수사 과정에서 디지털 포렌식 기술을 적용하여 컴퓨터에 남아 있는 증거물을 획득하고, 분석·조사한다. 다양한 사이버 범죄 상황 중 프로그램의 설치와 관련된 증거를 찾아야 하는 경우 용의자의 범죄 행위를 유추하기 위해 설치 응용프로그램에 대한 조사를 수행한다. 이러한 경우 수사 과정 중 증거물 분석 및 조사 단계에서 시스템 복원지점을 분석한다면 유용한 정보를 획득할 수 있을 것이다.[5] 본 논문에서는 먼저 시스템 복원지점에 대해 설명하고, 수사 과정에서 마주칠 수 있는 두 가지 상황을 가정하여 디지털 포렌식 수사 절차의 5단계 중 증거물 분석 및 조사 단계에서 활용할 수 있는 시스템 복원지점의 분석 방안을 살펴본다.

2. 선행 연구

가. 시스템 복원지점

시스템 복원은 과거의 특정 시점으로 시스템의 상태를 되돌리는 기능이다. 시스템 복원 기능은 운영체제 Windows ME 버전부터 존재하였으며 기본적으로 활성화되어 있다.[6] 본 논문에서는 Windows XP 환경에서의 시스템 복원을 대상으로 한다.

시스템 복원 기능을 수행하면 프로그램 설치 등에 의해 변경된 시스템 구성을 사용자가 선택한 시점으로 복원하는데, 이와 같이 사용자가 선택할 수 있는 특정 시점을 '시스템 복원지점'이라 한다. 시스템 복원지점은 Windows 초기 부팅 시, 컴퓨터를 켜놓은 후 기본 24시간마다, 또는 프로그램 설치나 제거와 같은 이유로 시스템이 변경될 때 시스템에 의해 자동으로 생성되며, 사용자가 임의로 복원지점을 만드는 것 또한 가능하다.[7]

1) 본 연구는 과학재단 디지털 정보 획득 기반기술 연구(M10740030004-07N4003-00410)의 지원으로 수행되었습니다.

나. 모니터링 대상 지정

시스템 복원 기능이 활성화되어 있는 동안 모니터링 될 대상의 목록은 'filelist.xml'이라는 파일에 저장되어 있다. 시스템 복원 기능은 모든 파일들을 모니터링하지 않기 때문에, 특정 디렉토리, 파일, 파일 확장자에 대하여 모니터링 여부를 filelist.xml 파일에 정의하고 있다. filelist.xml은 C:\WINDOWS\system32\Restore 디렉토리에 위치하는 파일로써 숨김 속성을 가지며, 모니터링에 포함할 목록은 include, 제외할 목록은 exclude로 정의한다. 그림 [2]는 filelist.xml 파일의 일부분으로, 모니터링 대상에서 제외하거나 포함할 파일명의 목록이다. 파일의 확장자 중 include 목록에 포함되어 있는 확장자에는 exe, lnk, dll, sys, ini 등과 같이 시스템 상태에 영향을 줄 수 있는 파일의 확장자들이 있으며 doc, pdf, bmp와 같은 응용 프로그램 파일의 확장자들은 대부분 포함되지 않는다.[7] 또한 컴퓨터 사용자가 많이 사용하는 '내 문서' 디렉토리는 exclude 목록에 포함되어 있어 시스템 복원의 모니터링 대상에서 제외된다.

```
- <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>
      </Exclude>
    - <Include>
        <REC>c:\placeholder\ph.dll</REC>
      </Include>
    </FILES>
```

그림 [2] filelist.xml

다. 복원지점 폴더

복원지점이 생성되면 C:\System Volume Information_restore{GUID} 안에 RP##(#는 복원지점이 생성되는 순서대로 붙은 일련번호)라는 이름으로 복원지점 폴더가 생성된다. System Volume Information 폴더는 기본적으로 시스템 권한으로 접근이 가능하다.

RP## 폴더에는 해당 복원지점 폴더에 대한 정보를 담고 있는 rp.log 파일, filelist.xml의 모니터링 목록에 따라 파일들의 생성, 변경, 또는 삭제 시 그 경로를 기록하는 change.log 파일, 그리고 삭제된 파일들의 복사본과 레지스트리 스냅샷(snapshot)이 저장된다. 삭제된 파일의 복사본이 이 폴더에 저장될 때는 'A0011751.lnk'와 같은 형태로 저장된다. 즉 확장자는 변경되지 않지만 파일 이름은 A에 7자리 숫자를 붙인 형태로 새 이름이 지정되며, A 뒤의 숫자는 복원지점 폴더에 저장된 순서대로 지정된다. 파일 삭제 시 휴지통을 거치거나 프로그램 삭제 시 제어판의 '프로그램 추가/제거' 또는 uninstall 기능을 이용한 경우 해당 파일과 프로그램 관련 파일들이 복원지점에 저장된다. shift+del를 이용한 완전 삭제의 경우 파일은 저장되지 않지만 삭제된 기록은 change.log 파일에 남는다. 또한 filelist.xml의 include 목록에 포함되어 있는 확장자를 가지는 파일은 그 확장자를 변경하면 변경 전의 원본 파일이 복원지점에 저장된다.

라. 복원지점에 대한 정보

각 복원지점 폴더에는 해당 복원지점에 대한 정보를 담고 있는 rp.log 파일이 존재한다.[8] rp.log 파일의 포맷을 분석하여 확인된 정보로는 복원지점의 종류(type), 복원지점에 대한 설명(description), 생성 시간이 있다.

'복원지점의 종류'는 오프셋 4부터 4바이트의 값에 따라 구분할 수 있다. 해당 위치의 값이 0x00000000이면 프로그램 설치로 인한 복원지점 생성, 0x00000001이면 프로그램 제거로 인한 복원지점 생성, 0x00000006이면 시스템 복원에 의한 복원지점 생성, 0x00000007이면 시스템 검사에 의한 복원지점 생성을 의미한다.

'복원지점에 대한 설명'이란 시스템 복원을 실행하면 원하는 복원지점을 선택하는 화면에서 보여주는 설명을 의미하며, '시스템 검사점', '00 프로그램 설치됨'과 같은 것을 말한다. 이것은 rp.log 파일의 오프셋 16부터 존재한다.

'복원지점의 생성 시간'은 rp.log 파일의 가장 마지막 8바이트에 존재하며, FILETIME 형식으로 저장되어 있다.

복원지점의 종류를 나타내는 부분의 경우 다른 값도 가질 수 있을 것이라 생각한다. 따라서 다양한 실험을 통해 어떠한 값들이 더 존재하는지 연구하고 있다. 또한 오프셋 0부터 4바이트는 0x00000064 또는 0x00000066을 값으로 가졌으며, 이 부분도 복원지점에 대한 어떤 정보를 나타내는 것이라 생각한다. 따라서 이 부분이 의미하는 것과 아직 정확히 밝혀지지 않은 부분에 대해서도 계속 연구할 계획이다.

마. 시스템 변화 기록

change.log 파일에는 filelist.xml의 include 목록에 파일 확장자가 포함되어 있는 파일들의 변경사항이 모두 기록된다. 파일이 처음 생성될 때는 그 경로와 이름이 기록되고, 변경사항이 있는 경우에는 변경되기 전과 후의 경로와 이름이 기록된다. 삭제되어 휴지통으로 이동한 경우에는 이동하기 전의 경로와 이름, 휴지통의 경로와 휴지통으로 이동하면서 새로 지어진 이름이 기록되며, 복원지점에 저장되는 경우에는 저장되기 전의 경로와 이름, 복원지점에 저장되면서 새로 지어진 이름 등이 기록된다(그림 [3]). 앞서 언급한 것과 같이 삭제 시 shift+del를 이용한 경우에도 기록은 남는다.

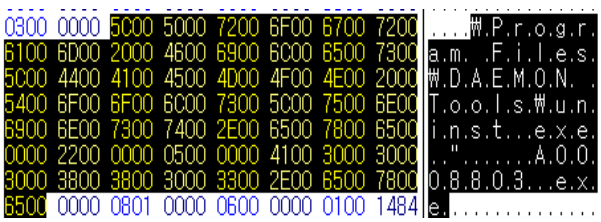

그림 [3] change.log에 기록된 원래 경로와 이름, 복원지점에서의 새 이름

확장자가 include 목록에 포함되어 있는 파일이더라도 exclude 목록에 포함되어 있는 디렉토리 안에 있다면 모니터링 대상에서 제외되어 change.log 파일에 어떤 기록도 남지 않으며 삭제해도 복원지점에 저장되지 않는다. 확장자가 include 목록에 포함되어 있는 파일은 그 파일을 포함하는 디렉토리가 include 목록에 존재하지 않더라도 모니터링 대상이 된다.

change.log 파일의 크기가 1MB 이상이 되거나[6], 복원지점이 처음 생성된 후 다음 복원지점이 생성되기 전까지 시스템이 새로 시작될

때마다 기존에 존재하던 change.log 파일에는 확장자 뒤에 번호가 붙고 동시에 새로운 change.log 파일이 생성된다. 즉, 기존 파일은 change.log.1로 이름이 변경되고 새로 change.log 파일이 생성되며, 다시 한 번 시스템을 새로 시작한다면 다시 생성되었던 change.log 파일이 change.log.2로 변경되며 새로운 change.log 파일이 생성된다. 이러한 작업은 다음 복원지점이 생성될 때까지 계속되며, change.log.2로 변경된 후에 다음 복원지점이 생긴다면 존재하는 change.log 파일이 change.log.3으로 변경된 후 더 이상 change.log 파일이 생기지 않고 해당 복원지점에서의 작업을 마치게 된다.

바. 레지스트리 스냅샷(snapshot)

스냅샷은 현재 사용하고 있는 파일 시스템에 대한 읽기만 가능한 사본이미지라 볼 수 있다. 즉, 최초 대상 파일의 풀백업을 통해서 대상 시스템의 레지스트리 파일을 유지하였다가 이후 발생하는 레지스트리 값의 변경을 유지하여, 백업 수행 시 변경된 레지스트리 정보만을 가져와 기존의 전체 레지스트리 파일에 덮어쓰고, 그 시점의 파일을 재 저장하는 방식이다.[9]

RP## 폴더 안의 snapshot 폴더는 Security, SAM과 같은 특정 레지스트리 파일들을 스냅샷하여 저장한다. 시스템에 대한 많은 정보를 저장하고 있는 레지스트리 파일들이 복원지점 폴더마다 저장되어 있기 때문에 시스템 상태에 대해 분석하고 조사하는 경우 매우 유용하게 사용될 수 있다.

사. 복원지점 삭제 기록

시스템 복원지점의 최대 크기는 기본적으로 4GB 이상의 드라이브인 경우 드라이브 크기의 12%, 4GB 이하의 드라이브인 경우 400MB로 제한되어 있다.[7] 복원지점에 할당할 최소 크기는 사용자가 설정 변경을 통해 200MB까지 줄일 수 있다. 복원지점에 할당된 크기의 90%가 채워지면 선입선출(FIFO) 방식에 의해 먼저 생긴 복원지점들을 삭제하여 할당된 크기의 75%까지 줄인다.[7] 복원지점이 삭제되면 fifo.log라는 파일이 생성되어 그림 [4]와 같이 복원지점들이 삭제된 날짜와 시간, 복원지점 폴더의 이름 등이 기록된다.

```
09/04/07-14:26:21 : Fifoed RP1 on drive C:\
09/04/07-14:26:21 : Fifoed RP2 on drive C:\
09/04/07-14:26:21 : Fifoed RP3 on drive C:\
09/04/07-14:26:21 : Fifoed RP4 on drive C:\
09/04/07-14:26:21 : Fifoed RP5 on drive C:\
09/04/07-14:26:22 : Fifoed RP6 on drive C:\
09/04/07-14:26:22 : Fifoed RP7 on drive C:\
09/04/07-14:26:22 : Fifoed RP8 on drive C:\
09/04/07-14:26:22 : Fifoed RP9 on drive C:\
09/04/07-14:26:23 : Fifoed RP10 on drive C:\
```

그림 [4] fifo.log

3. 가정 시나리오 연구

불법 스팸 메일 발송이나 키로거(Key Logger)로 인한 개인정보 유출과 같은 사건이 발생하였을 경우, 범죄자는 범행을 부인하기 위해 스팸 메일을 발송한 컴퓨터에서 스팸 메일 전송 프로그램을 삭제한다거나, 피해 시스템에서 키로거를 삭제할 것이다. 이러한 경우 범죄에 사용된 프로그램에 대한 흔적을 찾는다면 수사에 많은 도움이 될 것이다. 본 절에서는 시스템 복원지점에서 얻을 수 있는 정보를 이용하여 특정 프로그램에 대한 흔적을 찾는 방안을 논의한다.

가. 가정 1 - 삭제

먼저 용의자가 자신의 컴퓨터 또는 피해 컴퓨터에서 어떤 프로그램을 사용했던 흔적을 지우기 위해 관련 프로그램을 삭제하는 경우를 살펴본다. 용의자가 프로그램을 삭제하는 방법에는 다음과 같은 것들이 있다.

- 제어판의 프로그램 추가/제거 이용
- 해당 프로그램에서 제공하는 uninstall 기능 이용
- 해당 프로그램 관련 파일을 shift+del로 완전 삭제

프로그램 삭제 시 대부분 해당 프로그램의 uninstall 기능을 이용하거나 제어판의 프로그램 추가/제거를 이용할 것이다. 이러한 경우 실행파일(exe)이나 설치파일(msi)과 같이 확장자가 filelist.xml에 include 되어 있는 것들은 삭제와 동시에 해당 파일이 복원지점에 저장된다. 복원지점에 파일이 저장될 때는 새 이름이 지정되기 때문에 복원지점의 파일 자체만으로는 어떤 것이 우리가 원하는 파일인지 알 수 없다. 따라서 그림 [3]과 같이 원래의 경로와 이름, 새 이름이 함께 저장되어 있는 change.log 파일들을 조사하면 의심스러운 파일을 좀 더 쉽게 찾아낼 수 있을 것이다.

프로그램의 uninstall 기능이나 제어판의 프로그램 추가/제거를 이용하지 않고 shift+del을 이용하여 삭제한 경우, 파일이 복원지점에 저장되지 않더라도 그 흔적은 change.log 파일에 기록된다. 따라서 복원지점 폴더 내에서 수상한 파일을 발견하지 못한 경우에는 모든 복원지점의 change.log 파일들을 전부 조사한다면 의심스러운 기록을 발견할 수 있을 것이다.

나. 가정Ⅱ- 복원 역이용

두 번째로 프로그램을 설치하기 전으로 시스템을 복원시켜서 사용 흔적을 지우려는 경우를 살펴본다.

시스템 복원 기능을 이용하여 프로그램을 설치하기 전으로 되돌리는 경우, 해당 프로그램과 관련된 파일이 남아있는 경우가 많다. 시스템 복원 기능은 앞서 언급했던 바와 같이 filelist.xml 파일의 include 목록에 포함되어 있는 것들만 모니터링 한다. 따라서 프로그램을 설치하여 사용한 후 설치 전으로 복원시키는 경우 설치되었던 모든 것이 삭제되는 것이 아니라, 설치된 것들 중 시스템 복원 기능의 모니터링 대상에 포함되어 있는 것들만 삭제되어 복원지점에 저장되고 모니터링 대상이 아닌 것은 그대로 남아있게 되는 것이다. 따라서 시스템 복원을 역이용한 경우에도 가정 1과 같이 복원지점 폴더 내의 파일과 change.log 파일을 비교하면 그 흔적을 발견할 수 있다. 또한 수상한 파일을 발견하여 change.log 파일에서 해당 파일에 대한 기록을 발견했다면 그 파일의 원래 경로를 통해 복원 후에도 남아있는 해당 프로그램 관련 파일들의 위치도 알아낼 수 있으며, 이는 더욱 확실한 증거가 될 것이다.

프로그램이 설치되었던 디렉토리와 관련 파일들이 복원 후에도 남아있는 것을 용의자가 발견하여 삭제할 수도 있을 것이다. 하지만 이미 시스템 복원지점에 그 흔적이 남아 있으며 복원 후 남아있던 파일들을 삭제한 흔적 또한 change.log 파일에 기록될 것이다. 따라서 시스

템 복원을 역이용한 경우에도 복원지점의 분석을 통해 그 흔적을 발견할 수 있다.

4. 결론

시스템 복원지점을 분석하는 데에는 몇 가지 제약이 따른다. 복원 기능을 비활성화 시키면 복원지점 폴더가 모두 삭제되며, TTL(Time To Live)이 기본 90일로 지정되어 있어서 생성된 지 90일이 지나면 복원지점 폴더가 삭제된다. 하지만 시스템 복원기능은 기본적으로 활성화되어 있어 대부분의 사용자들이 이 기능에 대해 특별히 인식하고 있지 않으며, 디지털 포렌식 수사 관점에서 90일이라는 시간은 부족한 시간이 아니다. 따라서 시스템 복원지점의 분석은 용의자의 시스템 사용 흔적에 대한 증거를 발견하는 데에 유용한 정보를 제공할 수 있는 방법이다.

5. 향후 연구 계획

앞서 설명한 두 가지 가정 상황에 대하여, 시스템 복원지점의 정보를 더욱 효율적으로 수사관에게 보여줄 수 있는 도구가 있다면 수사에 많은 도움이 될 것이라고 생각한다. change.log 파일과 rp.log 파일은 일반적으로 읽을 수 있는 텍스트 형태가 아니기 때문에 분석하는 데에 어려움이 따르고, 가정 1의 마지막 부분에서 언급한 것처럼 모든 복원지점의 change.log 파일들을 전부 조사해야 하는 경우 많은 시간이 소모될 것이다. 컴퓨터 포렌식 도구에서도 복원지점에 대한 정보를 볼 수는 있지만 수사관이 원하는 정보가 어떤 것인지 알기 어려울 것이다.

따라서 본 논문의 저자는 복원지점의 정보를 한 눈에 보여줄 수 있는 도구를 만들어보고자 현재 설계 중이다. 우선 rp.log 파일의 포맷에 대해 더 조사한 후, 알아낸 정보를 이용하여 복원지점 폴더를 종류(시스템 검사점, 프로그램 설치, 제거 등)에 따라 구분하고 수사관에게 필요한 정보를 보여주고자 한다. 프로그램의 설치 또는 제거에 의해 생성된 복원지점의 경우 복원지점 설명 부분에서 복원지점이 생성되게 한 파일의 이름을 알 수 있기 때문에 이러한 정보를 시간 정보와 함께 보여줄 수 있다면 수사를 더욱 효율적으로 할 수 있도록 도울 수 있을 것이라 생각한다. 특히 rp.log 파일에 저장되어 있는 복원지점 생성 시간은 수사 중 시간정보 분석에 추가적인 정보를 제공할 수 있으며 특정 시간대에 시스템에 변화가 있었는지 파악해야 하는 경우에도 도움을 줄 수 있다.[5]

덧붙여 snapshot 폴더 내의 레지스트리와, 분석 중인 change.log 파일에 기록되어 있는 정보들에 대하여 기록원인(생성, 삭제, 변경)을 구분하고 각각에 맞추어 원래 경로, 이름, 바뀐 이름 등을 매칭 시켜 보여준다면 수사 시에 더욱 유용하게 쓰일 수 있을 것이다.

참 고 문 헌

[1] R. Harris, “Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem,” 2006 Proceedings of the DFRWS, August 14, 2006.

[2] A. Householder, K. Houle, C. Dougherty, “Computer attack trends challenge Internet security,” IEEE Comput. vol. 35, Issue 4, pp. 5-7, 2002.

[3] 김현상, 박상헌, 이상진, 임종인, “디지털 포렌식을 위한 최적화된 슬랙 공간 검색 기법,” 한국정보보호학회 동계정보보호학술대회 논문집, pp. 471-477, 2005년 12월.

[4] Chris Prosise, Kevin Mandia, "Incident Response & Computer Forensics, Second Edition," McGraw-Hill, 2003.

[5] Harlan Carvey, "Windows Forensic Analysis," Syngress Publishing, Inc.

[6] Mark E. Russinovich, David A. Solomon, "MICROSOFT WINDOWS INTERNALS, Fourth Edition," Microsoft, 2005.

[7] Kris Harms, "Forensic analysis of System Restore points in Microsoft Windwos XP," Digital Investigation, vol. 3, Issue 3, pp. 151-158, Sep. 2006.

[8] http://msdn2.microsoft.com/en-us/library/bb395209.aspx

[9] R. J Green, A. C. Baird, and J. C. Davies. Designing a fast, on-line Backup System for a long-structured file system. Digital Technical Journal of Digital Equipment Corporation, 8(2):32-45, October 1996