휘발성 증거자료의 무결한 증거확보 절차에 관한 연구

김용호* · 이동휘* · 김귀남*

요 약

컴퓨터 시스템이 침해를 당하여 네트워크를 사용할 수 없게 된 경우, 안전하게 휘발성 데이터나 중요 데이터의 자료를 얻는 방법으로, 최초 조사관이 사건발생장소로 직접 가서 CD나 USB의 형태로 만들어진 스크립트로 휘발성 데이터를 수집하여 생성되는 해시값으로 무결성을 증명하고 또 해시값이 적혀 있는 참관인의 서명을 받고 이를 네트워크를 사용 가능한 안전한 시스템으로 가서 해시값으로 인증을 하고 분석을 하는 시스템을 제안하였다.

A Stable Evidence Collection Procedure of a Volatile Data in Research

Yong-Ho Kim* · Dong Hwi Lee* · Kuinam j. Kim*

ABSTRACT

I would like to explain a method how to get important data from a volatile data securely, when we are not available to use network in computer system by incident.

The main idea is that the first investigator who collects a volatile data by applying scripts built in USB media should be in crime scene at the time. In according to volatile data, he generates hash value, and gets witness signature. After that, he analyses the volatile data with authentication in forensics system.

Key words : Forensic

* 경기대학교 정보보호학과

1. 서 론

언제부터인가 컴퓨터나 디지털매체는 우리들에게 있어 없어서는 안 될 만큼 우리들의 일상생활이 다가와 있다.

지금 현재 디지털매체를 통한 첨단 범죄들이 나날이 증가하고 있는 추세인 지금 이러한 첨단범죄를 다룸에 있어서 지금 현재 컴퓨터 시스템에서 하드디스크 자료나 디지털 증거를 획득함에 있어 무결성을 증명하고 이를 처리하는 절차가 절실한 실정이다.

본 논문에서는 먼저 절차법이 중요시되고 있는 사례와 휘발성 증거물의 어떻게 처리하는가에 대해서 알아보고 현재 우리나라에서는 휘발성 증거물이 처리되고 있는 실정과 문제점을 분석하여 새로운 대안을 제시한다.

2. 디지털 증거물의 취급

2.1 증거의 정의

SWGDE/IOCE표준에서는 컴퓨터 범죄 사건의 증거를 <표 1>에서 분류하고 있다.

〈표 1〉 컴퓨터 범죄사건 증거의 분류

분 류	내 용
디지털 증 거	범죄사건과 관련된 정보중 디지털 형태로 저장되거나 전송된 것
데이터 객 체	범죄사건과 관련된 정보중 물리적 항목과 관련된 것
물리적 항 목	디지털 정보를 저장하고 있거나 디지털 정보를 전송한 물리적 객체

디지털증거는 원본 디지털증거와 사본 디지털증거로 분류 될 수 있다.

'문서화된' 증거를 분류하는 또 다른 방법은 예증적 증거와 서류적 증거로 분류하는 것이다.

- 예증적 증거(demonstrative evidence)는 사건 현장이나 사고자체를 재구성하는 증거다. 배심원은 그래프, 차트, 그림, 모델과 같은 여러 시각 자료를 통해 사건을 재구성할 수 있다.
- 서류적 증거(documentary evidence)는 증거를 구성하는 문서를 가리킨다. 많은 법률전문가는 디지털 증거가 서류적 증거보다는 예증적 증거에 가깝다고 판단한다[2].

왜냐하면, 컴퓨터 포렌식 분야는 기본적으로 범죄의 현장을 재구성하는 것을 목적으로 하고 있기 때문이다. 그렇지만 이러한 분류는 특정한 범죄와 관련된 디지털증거의 종류에 따라서 달라질 수 있다.

기본적으로 제출된 문서는 원본문서가 파괴되지 않았고, 특별한 예외 상황이 아닌 한 원본이어야 한다. 그렇지만 미국연방 증거규칙(Federal Rules of Evidence)에서는 컴퓨터 증거를 다른 증거와 다르다고 보고 있다. 규칙1001-3은 "데이터가 컴퓨터나 다른 유사 장치에 저장돼 있다면, 원본데이터를 그대로 반영하는 출력도 원본데이터이다."라고 주장하고 있다. 여기에서 중요한 것은 증거를 제시하는 측에서 증거에 원본 데이터가 그대로 반영됐다는 것을 보이는 것이다. 증거를 제시하는 측에서는 증거의 내용이 오류가 없고, 압류된 이후 증거에 변경이 가해지지 않았다는 것을 보여야 한다.

그렇지 않으면 법정에 제출할 수가 없다.

2.2 증거의 채택기준

법정에 채택될 수 있는 증거는 몇 가지 요구사항이 있다. 증거는 자격이 있어야(믿을 만해야)하고, 관련이 있어야(사건에 관한 사실을 입증해야)하며, 물질적이어야(사건과 관련된 주제를 실증해야 한다)한다.

덧붙여서 미국법정에서는 합법적으로 얻은 증거만을 사용할 수 있다. 즉 증거는 연방법과 각 주법에서 정한 수색과 압류 절차를 통해 수집돼야 한다. 만약 어떤 증거가 불법수색으로 인해 발견됐다면, 그 증거가 피고의 유죄를 입증한다 하더라

도 정당한 증거로 인정받지 못한다.

이것을 위법증거수집 배제의 원칙(exclusionary rule)이라고 한다.

일부 관할지역의 판례에서는 과학적으로 타당한 증거에 대한 특별한 규칙을 설정하고 있다. 연방증거규칙 402에서는 미국의 헌법, 의회법, 연방증거규칙자체를 위반하지 않는 모든 관련 증거를 법정에서 채택하도록 하고 있다(예를 들어 용의장의 법적 권리를 위반하면서 얻은 증거는 채택하지 않는다).

규칙 401은 관련 있는 증거를 '기존사실의 진위여부를 판단하는데 도움을 주는 모든 증거'로 정의하고 있다. 이 규칙을 관련성 테스트 (relevancy test)라고 한다. 과학적 증거에 적용되는 또 다른 표준에는 일반적 합격판정시험(general acceptance test) 또는 Frye 표준이라는 것이 있다. 이 표준에서는 과학적기법의 결과가 증거로 제출되기 전에 과학적 기법 자체를 증거로 받아들여야 한다고 한다[2].

3. 휘발성 데이터의 보존

시스템의 메모리에 임시로 저장된 데이터를 휘발성데이터라고 부른다. 그 이유는 메모리는 전력을 이용해 데이터를 저장하기 때문이다. 시스템의 전원이 나가면 메모리에 저장된 데이터는 사라진다.

IEEE 인터넷드래프트인 Guidelines for Evidence Collection and Archiving 이라는 글에서는 휘발성이 큰 증거를 먼저 수집하라고 제시한다. 이 말은 가장휘발성이 큰 증거가 가장 사라질 가능성이 크기 때문이다. 그 문서에서 설명하는 '휘발성 순서'는 다음과 같다[1].

① 레지스터와 캐시
② 라우팅 테이블, ARP 캐시, 프로세스 테이블, 커널 통계
③ 시스템 메모리 내용
④ 임시 파일 시스템
⑤ 디스크 데이터

휘발성 데이터를 수집하는 과정은 한가지 문제점을 불러일으킨다. 그것은 시스템의 상태를 변경하게 된다는 것이다. 일부전문가는 수사자 또는 범죄 현장 기술자들이 현재실행중인 프로세스, 네크워크 상태와 연결정보, RAM 데이터 '덤프'를 캡쳐하고 그것을 하기 위해 실행하는 작업이나 명령을 문서화 할 것을 권장한다. 이 프로그램들은 수사관이 가지고 다니는 특수 포렌식 CD에서 실행되어 용의자 컴퓨터의 하드디스크에 있는 동일한 명령을 실행하는 대신 명령을 수행하고, 컴퓨터 하드디스크에 있는 다른 프로그램이나 라이브러리를 사용해서는 안된다.

3.1 피해야 할일

부주의한 행동으로 인해 증거물을 파괴하는 경우가 많다.

① 증거수집이 끝날 때까지 시스템을 끄지 말아야 한다. 많은 양의 증거물이 파괴될 것이고 공격자가 증거물을 파괴하기 위한 시작, 종료 스크립트를 작성했을 수도 있다.
② 시스템 상에 있는 프로그램을 믿지 말라. 증거물 수집을 위해 보호된 장치(e.g., CD)에 따로 마련한 프로그램을 사용하라.
③ 모든 파일의 access time을 변경시키는 프로그램을 사용하지 말라.

3.2 Chain of Custody

증거물이 어떻게 발견되었고 어떻게 다루어졌는지를 비롯한 증거물에 관련된 모든 일들을 명확하게 기술할 수 있어야 한다[1].

아래의 내용들이 문서화되어야 한다.

① 언제, 어디서, 누가 증거물을 발견하였고 수집하였는가?
② 언제, 어디서, 누가 증거물을 다루었고 검사하였는가?

③ 누가 어느 기간에 증거물을 관리했는가, 어떻게 저장되었는가?
④ 언제 관리에 대한 변경이 일어났고, 언제 어떻게 이송되었는가?

4. 휘발성 증거수집 무결성 검증 모델

4.1 현재 증거물 취급의 문제점

현재까지의 처리기준은 하드디스크에 대한 무결성을 증명하기 위하여 bit by bit 이미지를 생성한다든지 CRC 값을 생성함은 물론 디스크이미지의 전체 해시값이나 파일 각각의 해시값을 생성하여 디스크 이미지나 파일별 원본자료에 대한 무결성을 증명한다. 또한 휘발성 데이터의 획득은 정상적인 서비스가 가능한 상태에서의 네트워크로의 휘발성자료나 원본자료의 이미지을 전달하는 방법을 사용하고 있다. 현재까지 휘발성데이터를 획득하는 과정에서의 네트워크로의 전달방법은 휘발성자료의 획득과정이나 전달과정에서 휘발성데이터가 무결한지 또 운반과정이나 기타 처리과정에서 증거 data가 변경이 되지 않았는지에 대한 검증은 미비한 상태로 증거로서 쓰여지고 있는 실정이다.

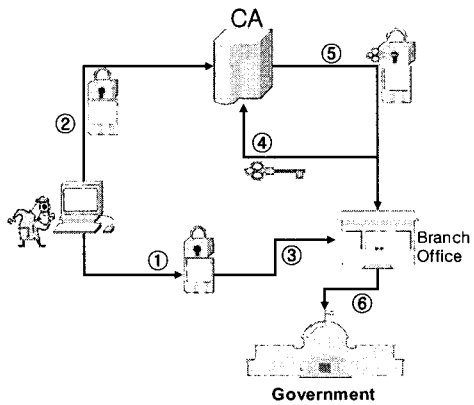
그러면 현재 실정에서 이러한 문제가 발생되었을 경우에 어떠한 결과가 벌어질지는 자명한 일이다.

미국의 연방법에서는 실제로 법정에서 증거물에 의해 "유죄가 확정될만한 단서가 나왔다 하더라도 해당증거자료에 대한 무결성이나 원본 훼손이 가해졌을 경우에는 그 자료를 무효로 한다." 라는 조항이 있을 정도로 자료에 대한 무결성 확보는 중요하다. 열심히 자료를 분석하고 복원하고도 무결성과 데이터의 정당성을 증명하지 못하면 그 자료는 무용지물이 되고 말 것이다.

그렇다면 우리들은 어떻게 시시각각 변하고 있는 네트워크 자료나 휘발성자료를 처리해야 할 것인가?

이에 대한 대안을 찾기 위해 본 논문에서 변화무쌍한 휘발성 자료를 추출하기 위한 스크립트로 되어 있는 CD나 요즘 흔히 사용하고 있는 USB메모리에 파일형태로 만들어 여기에 디스크 포렌식에서 원본자료의 무결성 수단으로 사용되고 있는 해시값을 통해 자료의 변경유무를 증명하고 또 자체 인증서버를 두어 수집 동시에 해당 해시값이 인증서버로 전달되어 휘발성자료가 파일형태로 만들어질 당시에 해시값으로 증거 자료 제출시 해시값을 증명하여 증거물이 변경되지 않았다는 것을 입증하는 방법을 제안하고자한다.

4.2 안전한 휘발성 증거수집과 무결성 검증과정



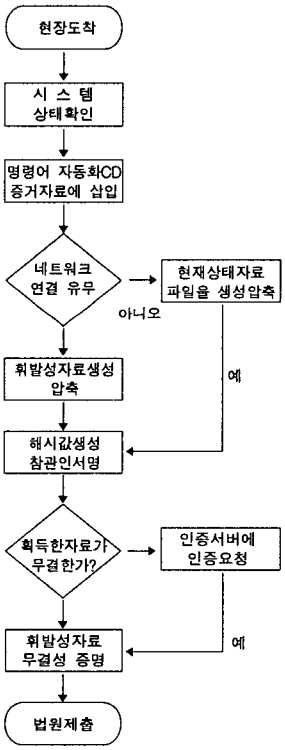
(그림 1) 휘발성 자료 획득과 검증 절차

(그림 1)의 무결한 휘발성자료 획득순서
수사관 현장 도착하여 증거물의 현재상태 확인
① 휘발성 증거자료 취득시 자동화CD디스크에 대한 명령어 취득(검색하였던 해당시간 현장 증거획득자의 성명 등 관련증거 생성과 동시에 해시값 생성)
② 휘발성자료 취득 후 네트워크 사용이 가능한 안전한 장소로 이동
③ 취득한 사람의 자료와 해쉬값을 인증서버에 보냄.
④ 최초 취득한 사람의 인증과 함께 해당 해시

값 비교하여 일치하는지 확인(관련자의 동의는 인증기관에서 발급된 인증서로 동일인임을 증명하고 다른 사람이 접근할 수 없음)

⑤ 추후 증거자료 무결성 증명시 압축파일에서 생성된 해시값과 증거자료 제출본의 해시값이 일치하면 무결성 증명

⑥ 관련기관에 제출

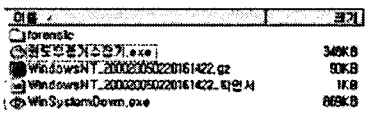


(그림 2) 휘발성자료 무결성 수집 절차 및 검증

위의 절차도 (그림 2)는 현장감식자가 현장에 도착하였을 때부터 휘발성자료를 획득하는 전 과정에 거쳐 설명하는 순서도이다. 중요한 내용은 명령어 CD를 사용한다는 점인데 명령어 자동화 CD는 증거자료의 통일성과 최초 증거확보의 미숙으로 오류를 범하는 것을 방지하기 위해 CD를 실행하기만 하면 자동으로 명령어를 수행하는 스크립트 형식으로 제작되어 무결성과 편의성을 두었다. 만일 CD의 내용이 불충분할 경우에는 전문가의 도움을 받아 CD를 다시 제작하거나 USB메모리 형태로 만들어서 상황에 맞게 대처하는 방법이 좋은 예라 할 수 있겠다. 편리하게는 만들었지만, 모든 시스템과 모든 사건을 다 처리할 수는 없기 때문이다.

CD에서 만들어진 명령어로 인해 만들어진 파일을 저장하는 공간은 플로피디스크나 USB메모리 형태로 받을 수 있지만, 요즘 USB메모리가 활성화되고 있어 USB메모리 타입을 추천한다. 플로피드라이브를 추천하지 않는 경우는 PC방과 같은 여러 사람이 공동으로 사용하는 공간이나 노트북 컴퓨터의 경우에는 플로피 드라이브가 사용하는 사람이 많지 않아서 아예 처음부터 구입을 하지 않아서 없는 경우가 많고 USB드라이브는 메인보드에 장착되어있기 때문에 없는 경우가 없기 때문이다.

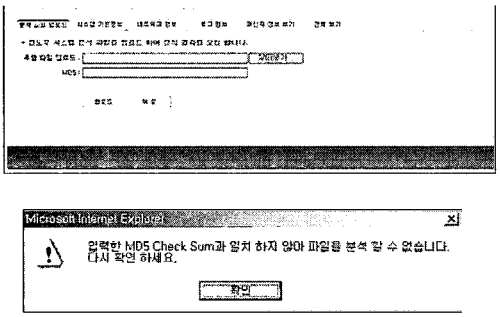
또한, 절차도에서 중요하게 살펴보아야 할 점은 시스템의 해킹이나 악성 프로그램 유포의 경우 신속히 네트워크를 단절해야 한다는 것이다. 네트워크를 단절하게 되면, 역추적을 하는데 매우 중요한 침입경로 정보와 프로세스 등의 아주 중요한 자료들이 전부 사라져 버리게 된다. 이럴 경우 최초 신고자와 조사자는 신중히 판단을 하여 피해시스템에서만 증거를 확보할 수 있는 지 아니면 다른 곳에서 증거를 확보할 수 있는 지를 고려하여 네트워크를 단절해야 할 것이다.



(그림 3) 증거수집과 확인서가 생성된 화면

CD에서 얻어진 결과 값은 (그림 3)과 같은 구성으로 되어있다. 자동으로 결과 값과 함께 해시값을 생성한다. 많은 파일의 경우 압축프로그램으로 압축된 압축파일도 존재한다. 그 압축파일을 풀어 그 안에 있는 해시값으로 휘발성 자료의 생성 당시의 날자와 시간의 문서를 작성해 참관인의 서명을 받아야 한다. 참관인의 서명은 나중에 해당 장소와

해당시간에 휘발성 자료가 CD에 의해 안전하게 획득된 것을 증명하는 중요한 자료이다. 문서의 내용에는 파일을 획득한 시간과 생성된 해시값을 포함 서명하는 곳이 있다. 반드시 서명을 받아 물리적 논리적으로 자료의 동일성 증명과 동시에 2중으로 생성 당시의 무결성을 증명할 수 있다.



(그림 4) 인증서버에서 해시값 인증과 해시값이 맞지 않았을 경우 에러화면

• 휘발성 자료 수집의 내용

RFC 3227문서 내용에서 휘발성데이터의 주용도를 정의는 하고 있지만 서건별로 정확히 휘발성 데이터를 추출하기 위해 작성될 스크립트는 상당히 다양하다. 모든 경우에 하나의 스크립트 파일로 적용할 수도 없고, 사례를 적용할 때마다 그에 맞는 스크립트를 적용할 수도 없는 실정이다. 그래서 한두 가지의 표준 스크립트를 만들어 사용하고 표준에서 벗어나는 상황에서는 그 상황에 맞는 스크립트를 그때마다 직접 제작하여 사용하도록 한다.

표준으로 제작할 스크립트는 윈도우즈용과 리눅스용으로 나누고 먼저 윈도우즈의 스크립트 내용은 다음과 같이 작성한다.

4.2.1 윈도우즈용 표준 스크립트 내용

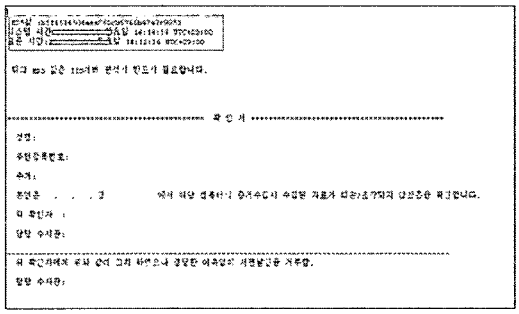
1) 비정상 네트워크 확인
   ① 비정상 네트워크 연결 확인
   ② 비정상 네트워크와 매핑된 프로세스 확인
   ③ 비정상 NetBIOS 연결 확인
2) 비정상 프로세스 확인
3) 비정상 서비스 확인
4) 레지스트리에 등록된 자동실행 프로그램 확인

4.2.2 리눅스용 표준 스크립트 내용

1) 중요 설정 파일 정보 수집
2) 파일 취약점 정보 수집
3) 시스템 로그 정보 수집
4) 시스템 메모리 정보 수집

이를 표준으로 제작하고 다른 기타 운영체제나 특이한 사안이나 이나 다른 경우에는 그에 맞는 스크립트를 제작해서 사용한다. 특별히 CD 형태의 명령어 스크립트를 사용하는 이유는 조사자의 실수로 인한 누락방지와 오류를 줄이기 위함이다.

본 논문에서 예제로 사용하는 스크립트와는 달리 각 기관에 맞게 침해사고에 대응할 수 있는 스크립트를 제작하는 것도 좋은 방법이다. 휘발성 자료는 한번 취득하면 그 자료가 변할 수 있으므로 신중을 기해야 하며 관련자의 동의도 그때마다 얻을 수 없으므로 한 번에 정확한 자료를 획득하여야 한다. 이렇게 자료가 수집되면 수집된 내용을 압축파일의 형태로 압축을 하며 압축과 동시에 생성된 시간과 해시 값을 생성하게 된다. 마지막에 한 장의 출력물을 생성하게 되는데 출력물에는



(그림 5) 휘발성자료취득과 함께 생성되는 참관인의 양식

생성된 시간, 해시값, 관련자의 동의를 얻는 문서가 생성되며, 이 문서를 소유자나 관계자가 읽고 서명날인 하는 곳이 있다. 자료를 획득한 사람은 반드시 관계자의 서명을 받아야 한다. 이 문서는 나중에 법정에서 무결한 자료의 증명을 요청할 때 중요한 자료가 될 수 있을 것이다.

아래의 (그림 5)의 내용은 참관인의 최종 확인을 위한 확인서의 내용이다.

5. 결 론

우리는 앞에서 안전한 휘발성증거에 대한 무결한 자료의 획득방법과 온/오프라인에서의 증거처리과정과 신뢰성확보에 대해 살펴보았다. 시스템이 더 이상 네트워크 서비스를 할 수 없을 경우 네트워크로의 전송과 인증은 불가능하다. 그러므로 직접 근원지로 찾아가서 휘발성자료를 획득해야 함은 물론 신뢰성확보를 위하여 조사자가 직접 입력하는 대신 정형화된 CD 형태의 스크립트를 사용하여 추후 있을 논란의 소지를 없애는 것이다.

그러므로 안전한 피해시스템의 휘발성증거자료의 획득은 조사자가 직접현장에서 취득함이 바람직할 것이며, 특히 법정과 같은 진술조서가 중요하게 작용하는 곳에서는 취득시 소유자나 관리자로부터의 확인과정도 필요하게 되는 것이다.

향후의 연구과제로는 휘발성증거자료의 무결성을 증명 프로세스와 좀 더 나은 형태의 방법의 자료 획득을 하는 데에 역점을 두어야 할 것이다. 그리고 스크립트를 제작할 경우 상황에 대처할 수 있게 능동적인 형태의 선택 가능한 스크립트를 사용하는 것도 고려할 사항이지만, 먼저 디지털 범죄 관련 법안이 하루 빨리 제정되어 수사에 혼동을 빚는 일이 없도록 해야 할 것이다.

참 고 문 헌

[1] RFC 3227 Guidelines for Evidence Collection and Archiving, 2002.

[2] scene of the cybercrime computer forensics handbook, Debra Littlejohn Shinder Ed tittel.

[3] Warren G, Kruse II, Jay G Heiser. "COMPUTER FORENSICS : Incident response Essentials", Addison Wesley, 2001.

[4] Kevin Mandia, Chris prosise, and Matt Pepe, "Incident response and computer forensics, Second Edition".

[5] 박영신, 오세민, 최용락, "컴퓨터 · 네트워크 통합 포렌식스를 위한 전자적 증거수집 모듈 설계", 한국사이버테러정보전학회, 2005.

김 용 호

2002년 광운대학교 정보통신학과 (공학석사)

2005년~현재 경기대학교 정보보호학과(박사과정)

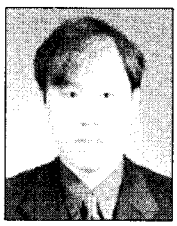
2002년 11월~현재 경찰청 사이버테러대응센터 기술지원팀 연구원

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)

2003년 경기대학교 정보보호기술공학과(공학석사)

2004~현재 경기대학교 정보보호학과(박사과정)



김 귀 남

미국 캔자스대학 수학과 (응용수학사)

미국 콜로라도주립대학 통계학과 (통계학석사)

미국 콜로라도주립대학 기계산업공학과(기계 · 산업공학박사)

현재 경기대학교 정보보호학과 주임교수