윈도우 활성 시스템상의 디지털 증거 수집 도구 설계 및 구현*

백은주** · 성진원** · 임경수** · 이상진***

요 약

포렌식 수사에 있어서 많은 포렌식 도구들이 수사에 사용되고 있지만 기존의 포렌식 도구는 일반 수사관이 사용하기에 불편하다는 단점이 있다. 정보 유출과 관련하여 긴급히 증거를 수집해야 할 상황에서 데이터를 수집해 증거로 활용할 수 있게 만들 때까지는 시간이 걸린다. 따라서 일반 수사관이 간단한 클릭만으로도 증거를 수집하고 또한 심층 수사로 갈 것인지를 판별할 수 있는 사전 조사격의 포렌식 도구가 필요하다. 따라서 본 고에서는 활성 시스템에서 수집할 수 있는 증거에 대해 알아보고 사전 조사에 사용할 수 있고 일반 수사관이 다루기 쉬운 포렌식 툴을 설계 및 구현하고자 한다.

Design and Implementation of Forensic Tool on Window Live System

Eun ju Baek** · Jin won Sung** · Kyoung su Lim** · Sang jin Lee***

ABSTRACT

Nowadays, there exist many forensic tools in forensic investigation. For common investigator it may cause some difficulty in handling the existing forensic tools. In case of urgent condition, if it takes long time to get the useful evidence from data, thenit makes the investigation process difficult. Thus, the common investigator can collect the evidence easily by simple clicking the mouse. The only thing he needs is a tool for examination before investigating in details. Therefore, in this paper we refer to useful information in the forensic investigation, discuss the design and the implementation of tool.

Key words : Live System, Digital Evidences, Volatile Evidences, Computer Forensics, XML(eXtensible Markup Language)

---

* 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음(2007-S019-01, 정보투명성 보장형 디지털 포렌식 시스템 개발).

** 고려대학교 정보경영공학전문대학원

*** 고려대학교 정보경영공학전문대학원 교수

1. 서 론

포렌식 수사의 발전과 함께 점점 더 많은 포렌식 도구들이 수사에 사용되고 있다. 이러한 포렌식 도구들은 서로 별개의 프로그램으로 하나의 스크립트에 의해 증거를 수집한다[1]. 그러나 이렇게 모아진 증거들은 수사관들이 일일이 분석/조사한 후에 비로소 증거로서의 가치가 있는지 없는지를 알 수 있게 된다. 수집 데이터가 유용한 증거가 되기까지는 '증거 수집→조사→분석→보고서 작성'이라는 다단계에 걸친 작업이 필요하다. 증거가 되기 전의 데이터는 일반 수사관이 의미를 파악하기가 어렵고 종전의 포렌식 도구는 일반 수사관이 사용하기에는 너무나 전문적이기 때문에(예를 들어, EnCase) 이러한 형태의 포렌식 도구는 전문적인 컴퓨터 포렌식 수사관이 아닌 일반 수사관이 사용하는데 어려움이 있다.

증거를 수집함에 있어서 그 시스템의 상태에 따라 수집해야 할 증거들은 분명히 다르다. 활성 상태에서 수집해야 하는 데이터가 있고 비활성 상태에서 얻어낼 수 있는 데이터가 존재한다. 활성 상태에서 수집해야 하는 데이터는 휘발성 데이터와 아이디/패스워드 같은 정보이다. 휘발성 데이터는 장치의 전원이 나가면 사라져 버리는 증거로 현재 네트워크 상태, 실행 중인 프로세스, 열려진 파일 등을 포함한다[2]. 이러한 데이터를 수집하여 분석해야만 현재 시스템이 침해를 당하고 있는지 침해를 가하고 있는지를 파악할 수 있다. 또한 압수 후에 수집할 수 없는 데이터를 수집해 사건에 대해 좀 더 유용한 정보들을 생성하도록 돕는다. 사고 발생 현장에서 수집된 데이터를 통해 심층 수사를 할 것인지를 판단할 수도 있고 수사의 초기 대응 단계의 작업을 하게 된다. 휘발성 데이터 및 ID/Password 정보뿐만 아니라, 시스템의 구성을 신속히 파악하기 위하여 레지스트리 정보를 수집할 필요성이 있다. 물론 레지스트리 정보는 비활성 상태에서도 수집할 수 있지만 레지스트리의 일부 키는 시스템이 시작할 때마다 그 값을 다시 생성하므로[3] 활성 상태에서 시스템의 상태가 변하기 전에 수집하는 것이 증거로서 더 가치가 있고 심층 수사를 하기전 사전 조사에 도움을 준다.

본 고에서는 수사의 초기 대응 단계에 해당하는 데이터를 수집할 수 있는 포렌식 도구를 설계하고 구현하여 비전문 수사관이 현장에서 데이터를 수집할 수 있는 방법을 제시하고자 한다.

2. 기존의 연구

현재 증거를 수집함에 있어서 활성 시스템에 대한 여러 연구가 존재하며 이와 관련된 도구가 존재한다. 포렌식 수사에 있어 수집해야 할 정보들에는 레지스트리 정보, 파일 및 폴더 정보 등이 있으며 증거를 수집하는 도구로는 스크립트를 이용한 방법, 라이브 CD를 이용한 수집이 존재한다. 본 장에서는 기존의 연구에 대해 알아보도록 한다.

2.1 레지스트리 정보 수집

윈도우즈 레지스트리는 시스템의 설정 정보들을 저장하고 있는 데이터베이스로 모든 Windows NT 계열의 OS에서 사용하고 있다[4]. 윈도우즈 레지스트리 분석은 임의의 응용프로그램들과 사용자의 행동들이 남기는 흔적을 발견하는 방법이다[5]. 레지스트리 정보를 수집할 때 수사관은 "autostart", "user activity", "MRU lists", "UserAssist", "USB removable storage", "Wireless SSIDs"에 대한 정보를 수집해야 한다[5]. 기존의 레지스트리 편집기는 시스템의 전체 레지스트리 정보를 트리 형식으로 나열하는 정도의 수준에 지나지 않기 때문에 수사에 필요한 레지스트리 정보만을 수집하고 보기 쉽게 나열하여 사전 조사에 대한 정보를 제공해야 한다.

2.2 파일 및 폴더 정보 수집

윈도우즈는 개인용 컴퓨터에 설치되면서 다양한

폴더와 특별한 파일들을 생성한다[6]. 또한 어떤 폴더, 어느 파일에 “키 파일”이 존재하는가를 이해하는 것은 파일 시스템을 이해하고 포렌식 수사에 있어서 분석을 위한 기초를 제공한다[6]. “키 파일”이란 윈도우즈가 생성하는 여러 가지 파일 중 폴더의 요약 정보를 담고 있는 “Thumbs.db”, DNS를 찾기 전에 윈도우즈에서 가장 처음으로 접근하는 “Hosts”, 시스템의 설정 정보들과 관련된 “SAM”, “Security”와 같은 레지스트리 하이브 파일, 최근 인터넷 사용이력들을 저장하고 있는 “Index.dat”와 같은 핵심 파일을 말한다[6]. 이러한 파일들은 로그인 정보나 인터넷 사용에 대한 정보와 같이 시스템 사용자와 관련된 정보를 얻을 수 있으므로 포렌식 분석에 도움을 줄 수 있는 정보들을 담고 있다. 수사관이 따로 폴더나 파일에 대한 정보를 일일이 수집하는 것보다는 일련의 작업을 통해 여러 폴더 및 파일들을 손쉽게 수집할 수 있는 도구가 필요하다.

2.3 스크립트를 이용한 수집

포렌식 수사에 있어서 활성 시스템에 대한 증거 수집은 스크립트를 사용하는 것이 보통이다. 현재 윈도우즈 기반 시스템에서 증거 수집은 윈도우즈의 여러 커맨드 라인 옵션을 사용하여 수행되고 있다.

Foundstone社의 “fport”[7], Everett Murdock이 만든 “DOSKEY”, Sysinternals社[8]의 “Psinfo”, “PsGetSID”, “psloggedon”, “pslist”, Microsoft Windows에서 제공하는 “arp”, “ipconfig”, “netstat”, “nbtstat”, “net share”, “at”과 같은 도구로 사용자가 직접 입력하거나 배치파일을 사용해 활성 시스템에서 증거를 수집한다. <표 1>은 일반적인 포렌식 도구가 사용하는 명령어 목록이다. 이러한 포렌식 도구들은 단지 증거를 수집하는 것이 목적이다. 따라서 스크립트를 이용해 수집한 데이터를 분류/분석 작업이 필요하다. 스크립트를 이용해 데이터를 수집한 것과 같은 효과를 내고 그에 더해 수집한 데이터를 분류/분석하는 보다 자동화된 포렌식 도구가 필요하다.

2.4 라이브 CD

포렌식 라이브 CD란 증거 수집을 위한 포렌식 도구로 대상 하드 드라이브에 있는 데이터는 전혀 사용하지 않고 CD 자체만으로 부팅을 하여 CD에서 제공하는 포렌식 소프트웨어로 증거를 수집하는 것을 말한다[9]. 외국의 경우 Hellix[10], Penguin Sleuth Bootable CD[11], FIRE[12]와 같은 라이브 CD가 있다. 이러한 CD는 시스템을 재부팅해야만 하기 때문에 휘발성 데이터를 수집하는데 문제가 있다. 따라서 현장에서 타겟 시스템를 압수하기 전에 휘발성 데이터를 손쉽게 수집할 수

〈표 1〉 수사에 사용되는 포렌식 도구

활성 데이터	포렌식 도구
활성화 상태의 윈도우 프로세스 리스트	pslist
현재 로그온 한 윈도우 사용자의 세션 정보	pslog
로컬 또는 원격 윈도우 시스템 정보	psinfo
사용자 계정 데이터베이스 업데이트/계정의 암호와 로그온에 필요한 사항	Net Accounts
서버에 열려있는 모든 공유 파일 이름	Net File
로컬 IP 라우팅 테이블 항목	Route Print
로컬 컴퓨터의 모든 세션 정보	Net Session
현재 실행 중인 서비스 목록	Net Start
사용자 계정 추가/수정 및 사용자 계정 정보	Net User
컴퓨터 공유 리소스 연결/해제 및 컴퓨터 연결 정보 표시	Net Use

있는 포렌식 도구가 필요하다.

3. 휘발성 데이터 수집 도구 설계

수사는 크게 “초기 대응 – 분석/조사 – 보고서 작성”으로 이루어진다[13]. 이 중에서 초기 대응 단계는 심층 수사를 위한 초석이 되며 사건 현장을 보존하는 중요한 단계이다. 사건의 초기 대응을 하는 수사관이 모두 포렌식 전문가일 수는 없다. 따라서 초기 대응 단계에서 누구나 쉽게 데이터를 수집하고 가독성 있는 결과를 산출할 수 있다면 인력 부족에 시달리는 포렌식 수사에 있어 큰 도움이 될 것이라고 생각한다. 활성 시스템에서 수집할 수 있는 데이터는 휘발성 데이터와 비휘발성 데이터로 구분을 할 수 있다[14]. 본 고에서는 포렌식 관점에서 의미있는 데이터들에 대해 알아본다. 또한 위에서 언급한 두 가지 타입의 데이터 일부를 수집해 가독성 있는 형태로 파싱하여 제공하고 인터넷 사용 정보, 이메일 사용 정보, 메신저 사용 정보, 하드웨어 사용 정보 등 정보 유출에 대한 사전 조사 정보를 제공하는 데이터를 수집하는 포렌식 도구를 설계 및 구현하고자 한다.

또한 최근 디지털 포렌식 학계의 화두는 자동화이다[15]. 즉, 포렌식 수사에 있어 증거의 수집에서부터 조사/분석에 이르기까지가 복잡한 작업 없이 이루어져야 함을 말한다. 범죄가 증가하면 할수록 처리해야 할 데이터들은 많아지고 수사관들은 많은 양의 데이터들을 처리함에 있어서 실수를 범할 확률이 높아진다[16]. 또한 기술의 발전으로 인해 저장 공간(예를 들어, 하드 디스크)이 커지고 있어 수사관이 확인해야 하는 단위가 점점 커지고 있다. 많고도 많은 데이터 속에서 어떤 데이터가 잠재적으로 증거가 될 수 있는지를 쉽게 파악할 수 있어야 한다. 수사의 초기 대응 단계에서 일반 수사관들도 보다 손쉽게 포렌식 수사에 임할 수 있는 도구, 심층 조사를 해야 하는 상황인지에 대한 사전 조사용으로 사용할 수 있는 도구 그리고 간단한 클릭만으로 포렌식 수사에 있어서 의미있는 데이터들을 추출하는 통합형 증거 수집 포렌식 도구가 필요하다.

3.1 휘발성 데이터

정보화 시대에는 개인용 컴퓨터 한 대만이 홀로 작동하기 보다는 인터넷에 연결하여 다른 사용자와 정보를 공유하는 용도로 더 많이 쓰이고 있다. 또한 휘발성 데이터 정보는 대상 컴퓨터가 반드시 활성 상태일 때 수집해야 하는 증거이다. 왜냐하면 전원이 나갔다 다시 들어온 후에는 그 이전 상태에 변화가 있기 때문이다. 휘발성 데이터 정보에서 제공하는 데이터는 용의자가 연결한 원격 컴퓨터의 IP나 용의자의 컴퓨터에 연결된 IP, 현재 열린 포트, 현재 실행 중인 프로세스 등에 대한 정보를 제공하므로 현장에서 즉시 범죄를 적발할 수 있는 정보라고 할 수 있다. 본 고의 포렌식 툴에서 수집하는 휘발성 데이터 정보는 “IP정보”, “Process 정보”로 나뉘며 먼저 “IP 정보”는 원격 컴퓨터 정보, 열려있는 포트 정보, 원격 컴퓨터의 IP/MAC 정보, 예약된 작업 등에 대한 정보를 수집한다[17]. “IP 정보”로 획득한 데이터로는 대상 시스템에 연결된 네트워킹 정보들을 얻을 수 있으므로 대상 시스템이 피해를 당하였는지 혹은 침해를 주고 있는지를 확인할 수 있다. “Process 정보”에서 획득할 수 있는 데이터는 현재 활성화 중인 Process의 목록, 로컬 시스템(대상 시스템)의 정보, 윈도우 업데이트 정보(설치된 Hotfix), 설치된 소프트웨어의 목록에 대한 정보를 획득할 수 있다[18]. 따라서 “Process 정보”는 대상 시스템에서 실행 중인 프로세스의 정보를 얻어올 수 있으므로 그 결과 현장의 상태를 가장 잘 알 수 있는 정보들을 얻어올 수 있다.

3.2 인터넷 사용정보 수집

분석 시스템의 인터넷 사용 기록을 분석하는 것

은 시스템 사용자가 사용한 인터넷 뱅킹 서비스, 온라인 구매 서비스, 검색어 등 인터넷으로 작업한 일들이 기록으로 남아 수사관이 그 기록을 분석함으로써 사용자의 행동을 추적, 재구성할 수 있기 때문에 수사에 도움이 되는 정보이다[19].

인터넷 사용정보는 대상 시스템에서 사용되는 웹 브라우저에 대한 정보와 쿠키 파일, 임시 인터넷 파일, 접속한 URL등의 정보 등을 수집할 수 있다. 웹 브라우저를 사용하면서 자동으로 생성되는 쿠키 파일, 캐시 파일, 히스토리 파일 등은 분석을 통하여 사용자의 행동을 추적할 수 있는 유용한 정보로 이를 통해 용의자의 개인 성향과 관심사까지도 파악할 수 있게 된다. 쿠키 파일은 서버에서 사용자 식별을 위해 자동으로 저장하는 파일로 웹브라우저 사용자가 들어간 사이트와 횟수, 계정 정보를 제공한다. 캐시 파일은 빠른 접속을 위하여 웹 브라우저가 저장하고 있는 이미지나 텍스트 파일이다. 목적은 빠른 접속이지만 이외에도 사용자가 접속한 사이트(블로그, 개인 홈페이지 등)의 사진이나 텍스트들을 획득할 수 있어 사용자와 관련된 정보를 얻을 수 있다. 그리고 히스토리 파일은 사용자가 방문했던 사이트를 날짜, 시간, 요일 별로 저장하고 그 파일이 마지막으로 수정된 시간을 저장하고 있어 사용자의 행동을 시간별로 추적할 수 있는 정보를 제공한다. 인터넷 사용 정보에서 데이터 수집의 대상이 되는 응용 프로그램은 Microsoft社의 인터넷 익스플로러[20], Netscape communicator社의 넷스케이프 커뮤니케이터[21], AOL-타임워너의 모질라 프로젝트의 결과인 파이어폭스[22]이다.

3.3 이메일 정보 수집

이메일 사용 정보는 사용자의 메일 송/수신 정보를 확인할 수 있는 정보이다. 이메일은 응용 프로그램에서 동작하는 것과 웹 메일로 나뉘는데 본고의 포렌식 도구에서는 응용 프로그램을 다룬다. 이메일 응용 프로그램에서는 사용자가 송/수신한 메일이나 파일 등의 기록을 보관하고 있기 때문에 용의자가 범행을 공모하고 그에 대한 정보나 파일을 공모자와 이메일 응용 프로그램을 사용하여 주고받았다면 이와 관련된 정보를 수집할 수 있는 중요한 정보이기 때문에 수사에 도움을 줄 수 있는 중요한 정보이다. 이메일 사용정보에서 데이터 수집의 대상이 되는 응용 프로그램은 Microsoft社의 아웃룩, 아웃룩 익스프레스[23]이다.

3.4 메신저 정보 수집

메신저는 네트워크 상에서 다른 사람과 의사소통을 위해 개발되었다. 메신저는 이메일이 제공하는 의사소통 기능에 실시간 통신이라는 장점을 부과하여 상대방과의 실시간 대화와 파일 송/수신을 지원한다. 메신저의 편리성 때문에 메신저는 현재 많은 사람들에게 사용되고 있다. 메신저 사용정보에서 수집해야 하는 증거는 사용자의 ID와 대화 내용 저장 폴더, 파일 다운로드 폴더, 쿠키 파일 등이다. 메신저 사용정보는 현재 사용자가 사용하고 있는 메신저를 파악하고 메신저를 통해 주고받은 파일을 확인할 수 있게 한다. 또한 대화 내용을 저장하도록 설정하였다면 상대방과의 대화 기록을 통해 대화 내용을 확인하고 불건전한 정보의 공유 사실이나 범행의 공모, 비밀/기술자료 유출에 대한 사실을 확인할 수 있다. 메신저 사용정보에서 데이터 수집의 대상이 되는 응용 프로그램은 다음 커뮤니케이션의 DAUM 메신저[24], SK Telecom의 NATEON[25], 버디버디주식회사의 BuddyBuddy[26], Microsoft社의 MSN 메신저[27]이다.

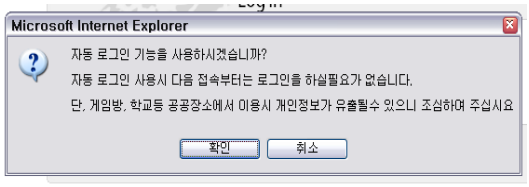
3.5 하드웨어 사용 정보 수집

하드웨어 사용 정보에서 획득할 수 있는 데이터는 대상 시스템에 부착된 하드웨어에 대한 정보들로 디바이스의 종류, Unique ID(고유 값), 디바이스 이름, ClassGUID 등에 대한 정보를 제공하고

있다. 하드웨어 사용 이력을 분석하면 이동식 저장 장치의 Unique ID를 통해 비인가 저장 매체를 파악할 수 있으며 용의자로부터 압수한 이동식 저장 장치의 메모리 디스크가 해당 시스템에 사용되었는가를 확인할 수 있으므로 인증되지 않은 접근을 파악할 수 있는 중요한 정보이다. 또한 네트워크 카드에 대한 정보를 이용하여 허가되지 않은 네트워크 카드의 사용 여부에 대한 데이터를 획득하게 한다.

3.6 ID/Password 정보

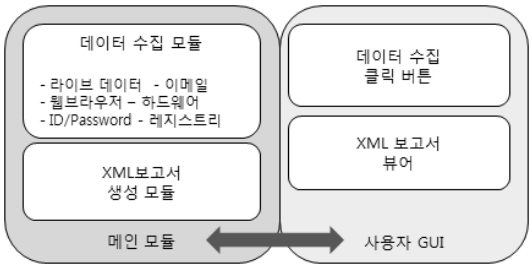
ID/Password 정보는 대상 시스템에 저장되어 있는 사용자의 계정 정보와 비밀번호를 획득할 수 있다. 용의자가 범행 사실을 은폐하기 위하여 계정 정보와 비밀번호를 언급하지 않을 경우 사용될 유용한 정보이다. 용의자가 사용하는 개인용 컴퓨터 혹은 공용 컴퓨터에서 (그림 1)과 같이 자동 완성기능을 사용한다면 자주 방문하는 웹 사이트의 계정과 비밀번호까지도 알 수 있다. 또한 용의자가 비밀번호를 기억시키지 않았다고 하더라도 웹 사이트에서 사용한 계정이나 메신저의 비밀번호 정보를 수집할 수 있다. 일반적으로 사람은 계정과 비밀번호를 여러 사이트들에서도 똑같이 사용하고 있거나 계정이 다르다고 하더라도 비밀번호는 같은 것을 사용하는 경우가 많다. 따라서 하나의 계정과 비밀번호를 알아내게 된다면 여러 다른 곳에서 사용하는 비밀번호를 유추할 가능성이 크기 때문에 ID/Password는 수사에 있어서 아주 중요한 정보가 된다.



(그림 1) 자동 로그인 기능

3.7 도구 구조

(그림 2)는 본 고에서 소개하는 포렌식 도구를 도식화 한 것이다. 위에서 언급한 포렌식 수사에 있어서 증거로서의 의미가 있는 데이터 수집을 위해 여러 가지 수집 모듈을 만들고 이를 통합적으로 수집/분석하여 GUI를 통해 보여주는 기능이 포함된다.



(그림 2) 포렌식 도구의 설계 도식

포렌식 도구에서 획득할 수 있는 데이터는 크게 6가지로 분류한다. 메인 모듈은 데이터 수집 모듈과 보고서 파일 접근 모듈을 제어하여 데이터를 수집하고 XML 보고서 파일을 작성하도록 하는 중간 매니저 역할을 하게 된다. 데이터 접근 모듈은 각각 필요한 데이터들을 수집하는 작업을 하며 사용자 인터페이스는 하위 레벨에서 진행되는 복잡한 모듈간 통신을 숨겨 수사관이 간단한 클릭만으로도 프로그램을 제어할 수 있도록 하게 한다.

4. XML을 이용한 수집 데이터 관리

본 고에서 소개한 포렌식 툴은 수집한 데이터를 이용하여 보고서를 만드는 기능을 제공한다. 보고서 기능은 데이터를 획득한 후 XML 형태로 보고서를 만들게 된다. 컴퓨터 시스템에 대한 전문적인 지식이 없는 수사관이라 하더라도 증거를 수집하고 보고서를 만드는 것을 도와준다. XML은 암

호화와 전자서명이 제공되기 때문에 어떤 다른 방법을 적용하지 않아도 된다[28, 29].

4.1 XML을 이용한 기존 연구

XML은 1996년 W3C에서 정의한 마크업 언어로 SGML에서 파생하여 확장이 쉬운 텍스트 포맷이다[30]. XML을 사용하면 데이터 처리 및 교환이 용이하고 태그의 이름이 곧 그 태그가 의미하는 것을 알 수 있는, 사용자가 읽기 쉽고 이해하기 쉬운 마크업 언어이다[30].

XML을 이용해 포렌식 수사에 적용하는 기법은 이미 활발히 연구되고 있다. W. Alink는 XIRAF 프레임워크를 만들어 XML DB를 구축해 수사의 결과물을 만들고 손쉬운 쿼리와 인덱싱 작업을 지원한다[31]. 또한 Tye Stallard와 Karl Levitt의 연구에서는 XML 형태의 중간 결과물로 결정 트리를 생성한 후 JESS에 넣어 시간 조작을 분석하는 툴을 개발하였다[32].

ProtectStorage Password			
ResourceName	ResourceType	UserNameValue	Password
http://sugang.korea.ac.kr:7080	AutoComplete Passwords	2006[redacted]	
http://sugang.korea.ac.kr:7080/	AutoComplete Passwords	2006[redacted]	
http://sugang.korea.ac.kr:7080/	AutoComplete Passwords	ej[redacted]	

Mail Password				
Application	Email	Type	User	Password

Network Password			
ItemName	Type	User	Password
	Autologon Password		10[redacted]
WindowsLive:name=[redacted]@hotmail.com	Generic	[redacted]@hotmail.com	

(그림 3) 개인용 컴퓨터에서 수집한 아이디/패스워드

XML을 적용하여 포렌식 도구를 구현하고 이러한 기법 연구가 활발히 진행되고 있기 때문에 이러한 경향에 맞추어 증거 분석 결과를 XML 포맷으로 산출하고자 하였다.

4.2 XML과 수집 데이터의 결합

수집된 데이터를 보다 효과적으로 수집, 배포하기 위해 보고서 포맷을 구조화하고 이를 XML 스키마로 정의한다. 위에서 언급했듯이 XML의 태그는 사용자가 지정하기 나름이기 때문에 이러한 장점으로 인해 다른 포렌식 도구가 수집한 텍스트 결과보다 XML로 파싱된 보고서는 이해하기가 쉽다. 이렇게 구조화된 XML 문서는 원하는 데이터를 추출/병합이 쉽기 때문에 문서에 대한 확장 및 수정이 용이하다. 증거를 저장하기 위해 데이터 구조를 XML로 정의하는 것은 단순히 텍스트로 표현된 것보다 구조화된 XML 문서가 이해하기 쉽고 데이터 처리 면에서도 편리하기 때문이다. 또한 우리나라에서 증거에 대한 보고서 표준 양식이 정립되지 않았기 때문에 XML로 보고서를 표준화한다면 상호 데이터 교환이나 이동 및 가공이 편리해진다. 그리고 데이터 추출 및 수정이 용이한 XML의 장점을 사용하여 수사관은 수집된 증거에서 필요한 부분만을 추출하여 또 다른 보고서를 만들기 쉽다.

증거에 대한 보고서를 XML로 구조화하면 쉽게 데이터들의 계층 구조를 알 수 있고 전문적인 지식이 없는 수사관도 그 계층 구조를 쉽게 알아볼 수 있는 가독성을 제공한다. 그리고 포렌식 도구에 어떤 기능이 추가되더라도 추가된 증거의 데이터 구조만을 정의하면 되기 때문에 쉽게 업그레이드가 가능한 장점을 지닌다.

5. 구현 및 성능 평가

5.1 구현 환경

본 고에서 구현한 포렌식 도구의 구현 컴파일러는 Microsoft Visual Studio 6.0을 사용하였는데 이것은 차후 버전인 7.0, 7.1, 8.0에 비해 오랫동안 사용되어 안정적이며 여러 시스템의 환경에 구애

받지 않고(e.g. .NET Framework 1.1을 설치하지 않은 시스템) 배포가 가능하기 때문에 이를 선택하였다.

5.2 성능 평가

본 고에서 소개하는 포렌식 도구로 개인용 컴퓨터에서 테스트를 하였다. (그림 3)은 아이디/패스워드 정보 보고서 중 일부이다. 실제 필자가 사용하고 있는 사이트의 아이디와 메신저 로그인 정보를 볼 수 있다. 일반적으로 개인용 컴퓨터에는 공용 컴퓨터보다 특정 개인에 대해 더 많은 정보를 남기게 되기 때문에 용의자가 사용하는 개인용 컴퓨터에서는 용의자와 관련된 정보를 쉽게 수집할 수 있다. 본 고의 포렌식 도구를 사용해 활성 상태에서 시스템의 휘발성 데이터들과 여러 데이터들을 수집하여 그 자리에서 바로 결과물을 볼 수 있다. 또한 사용자의 로그인 계정 정보, 검색어를 통해 알 수 있는 개인의 관심사, 메신저 계정 정보 등을 간단한 조작을 통해 시스템에서 수집할 수 있다. 간단한 클릭 몇 번으로 데이터를 수집하고 가독성 있는 XML 보고서 형태로 결과를 도출할 수 있다.

본 고에서 제안한 포렌식 도구의 수행 시간을 각 시스템의 사양별로 아래 <표 2>에 정리하였다. 결과에 따르면 수집해야 하는 데이터의 양이 많고 시스템의 성능이 낮을수록 데이터를 수집하는 시간이 늘어나는 경향이 있음을 알 수 있다. 그러나 수집과 XML 파싱을 하는데 까지 걸리는 시간은 다른 포렌식 도구에 비해서 짧은 편이며 사건현장에서 사용하기에 긴 시간이 아님을 알 수 있다.

6. 향후 과제 및 결론

현재까지 데이터 획득 도구는 “휘발성 데이터(실행 프로세스, 열린 포트, 예약된 실행, 로그온 사용자 정보, 설치 소프트웨어 및 윈도우 업데이트 정보, 설치된 장치, ARP 테이블)”, “인터넷 사용정보”, “이메일 사용정보”, “메신저 사용정보”, “하드웨어 사용정보”, “아이디/패스워드 정보”, “레지스트리 하이브 파일”을 수집할 수 있으나 향후에는 좀 더 활성 시스템에서의 증거 획득을 강화하여 구체적인 의미에서의 휘발성 데이터인 메모리(RAM) 덤프와 그의 조사/분석이 이루어져야 한다. 또한 운영체제에 있어서 XP뿐만이 아니라 Windows NT, Windows 2003 그리고 더 나아가서는 Windows Vista까지도 확대되어야 할 것이다. 그리고 최근에는 지적 재산권과 관련하여 P2P에 대한 분석과 그에 대한 데이터를 수집하는 모듈이 추가되어야 한다.

지금까지 살펴본 통합형 포렌식 증거 도구는 다음과 같은 장점을 제공한다.

① 포렌식 지식이 없는 수사관이 증거를 수집함에 있어서 어려움이 없다.
② 하나의 시스템에서 증거를 수집함에 있어서 단 한 번의 작업만으로 증거를 수집한다.
③ 심층 조사 전 사전 조사용으로 사용한다.
④ XML을 이용한 보고서를 통해 증거에 대한 가독성 및 확장성을 제공한다.

앞으로 한국형 통합 포렌식 도구는 전문 포렌식 수사관이 부족한 우리나라의 현실 속에서 포렌식

〈표 2〉 시스템 사양 별 포렌식 도구 수집 시간

PC	휘발성데이터	ID/Password	웹 브라우저	이메일	메신저	하드웨어	레지스트리	전체
1*	3분 12초	11초	5분 18초	44초	3분 5초	16초	25초	13분 11초
2**	2분 14초	2초	3분 10초	1초	51초	1초	5초	6분 23초
3***	54초	1초	6분 5초	1초	4분 45초	1초	3초	10분 54초

주) * 인텔 펜티엄 4, Windows Home Edition, 256M RAM, CPU 724 MHz, HDD 23.8G.
** 인텔 펜티엄 4, Windows Professional, 1G RAM, CPU 3.4 GHz, HDD 200G.
*** 인텔 펜티엄 4, Windows Professional, 0.99G RAM, CPU 2.13 GHz, HDD 68.3G.

지식이 없는 수사관도 증거들을 손쉽게 수집하고 포렌식 수사 지식이 없어도 직관적으로 이해할 수 있는 가독성 높은 증거를 제시할 수 있도록 끊임없이 개발되어야 할 것이다.

참 고 문 헌

[1] 이하영, 이상진, 임종인, “포렌식 툴의 무결성 확보를 위한 LiveCD 제작”, 한국정보보호학회, 한국정보보호학회 동계학술대회 논문집, Vol. 14, No. 1, pp. 478-482, Dec. 2005.

[2] Keith J. Jones, Richard Bejtlich and Curtis W. Rose, “Real Digital Forensics - Computer Security and Incident Response”, Addison Wesley, p. 3, 2006.

[3] Mark E. Russinovich and David A. Solomon, “Microsoft Windows Internals Microsoft Windows Server 2003, Windows XP, Windows 2000 Forth Edition”, Microsoft Press, pp. 183-211, 2004.

[4] Registry, Microsoft MSDN, http://msdn2.microsoft.com/en-us/library/ms724871.aspx.

[5] Harlen Carvey, “The Windows Registry as a forensic resource”, Science Direct, Digital investigation, pp. 201-205, 2005.

[6] Chad Steel, “Windows Forensics - The field guide for conducting corporate computer investigations”, Wiley publishing, Inc., pp. 97-114, 2006.

[7] 파운드스톤, fport, http://www.foundstone.com.

[8] 시스인터널즈, Windows Sysinternals, http://www.microsoft.com/technet/sysinternals/default.mspx.

[9] 이하영, 이상진, 임종인, “포렌식 툴의 무결성 확보를 위한 LiveCD 제작”, 한국정보보호학회, 한국정보보호학회 동계학술대회논문집, Vol. 14, No. 1, pp. 478-482, Dec. 2005.

[10] Helix, http://www.e-fense/com/helix.

[11] Penguin Sleuth Bootable CD, http://penguinsleuth.org/index.php?option=com_wrapper&Itemid = 39.

[12] FIRE, http://fire.dmzs.com.

[13] Wayne Jansen and Rick Ayers, “Guidel ines on Cell Phone Forensics”, NIST, 2006.

[14] Keith J. Jones, Richard Bejtlich and Curtis W. Rose, “Real Digital Forensics - Computer Security and Incident Response”, Addison Wesley, p. 3, 2006.

[15] Brian D. Carrier and Eugene H. Spafford, “Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence”, Digital Forensic Research Workshop(DFRWS), 2005.

[16] Simson L. Garfinkel, “Forensic feature extraction and cross-drive analysis”, Digital Investigation 3S, pp. S71-S81, 2006.

[17] Chad Steel, “Windows Forensics - The field guide for conducting corporate computer investigations”, Wiley publishing, Inc., pp. 157-165, 2006.

[18] Chad Steel, “Windows Forensics - The field guide for conducting corporate computer investigations”, Wiley publishing, Inc., pp. 178-180, p. 186, 2006.

[19] Keith J. Jones, Richard Bejtlich and Curtis W. Rose, “Real Digital Forensics - Computer Security and Incident Response”, Addison Wesley, p. 247, 2006.

[20] Internet Explorer, http://www.microsoft.com/korea/windows/products/winfamily/ie/default.mspx.

[21] Netscape Browser, http://browser.netscape.com/ns8/.

[22] Firefox, http://mozilla.com/en-US/firefox.
[23] Outlook/Outlook Express, http://office.microsoft.com/ko-kr/outlook/FX100487751042.aspx.
[24] DAUM Messenger touch, http://messenger.daum.net/section/main/index.jsp.
[25] NATEON, http://nateonweb.nate.com/.
[26] Buddybuddy Messenger, http://messenger.buddybuddy.co.kr/.
[27] MSN Messenger, http://im.msn.co.kr/new/function/function_01.asp.
[28] W3C Recommendation, "XML Encryptio n Syntax and Processing", http://www.w3.org/TR/xmlenc-core/, Oct. 2003.
[29] W3C Recommendation, "XML-Signature Syntax and Processing", http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, Feb. 2002.
[30] 백은주, 이석희, 이상진, 임종인, "XML 서명을 이용한 디지털 증거의 무결성 보장 및 인증에 관한 연구", 한국정보보호학회, 한국정보보호학회 동계정보보호학술대회논문집, Vol. 16, No. 2, pp. 375-378, Dec. 2006.
[31] W. Alink, R. A. F. Bhoedjang, P. A. Boncz and A. P. de Vries, "XIRAF-XML-based indexing and querying for digital forensics", Digital investigation 3S, pp. s50-s58, 2006.
[32] The Stallard and Karl Levitt, "Automated Analysis for Digital Forensic Science : Semantic Integrity Checking", 19th Annual Computer Security Applications Conference, Dec. 2003.

백 은 주

2006년 강원대학교 멀티미디어전공(공학사)
2006년~현재 고려대학교 정보경영공학전문대학원 (공학석사)

성 진 원

2006년 세종사이버대학교 정보보호전공(공학사)
2006년~현재 고려대학교 정보경영공학전문대학원 (공학석사)

임 경 수

2006년 부경대학교 컴퓨터멀티미디어 전공(공학사)
2006년~현재 고려대학교 정보경영공학전문대학원 (공학석사)

이 상 진

1994년 고려대학교 수학과 박사
1989년~1999년 한국전자통신연구원 선임연구원
1999년~2001년 고려대학교 자연과학대학 조교수
2001년~2006년 고려대학교 정보보호대학원 부교수
2006년~현재 고려대학교 정보경영공학전문대학원 정교수