정보유출 방지를 위한 디지털 포렌식 기술 비교분석 연구

박 광 민*, 홍 승 완**, 김 종 필***, 장 항 배****

요 약

IT 발전 및 급격한 정보화 사회로의 변화에 따라 컴퓨터 관련 범죄뿐만 아니라 일반 범죄에서도 중요 증거 또는 단서가 컴퓨터를 포함한 디지털 정보기기 내에 보관되는 경우가 증가하게 되었다. 최근에 발생하고 있는 산업기술 및 영업비밀 유출 사건은 컴퓨터, 스마트폰, USB 등 다양한 디지털 저장매체와 관련성을 가지는 경우가 많다. 본 논문에서는 디지털 포렌식 기술 현황 및 비교분석을 통해 포렌식 분야 발전방향을 도출하였으며, 이를 통해 정보유출을 방지할 수 있는 방안에 대해서 모색해 보고자 한다.

A Study on Comparison Analysis of Digital Forensic Technology for Preventing Information Leakage

Gwangmin Park*, Seungwan Hong**, Jongpil Kim***, Hangbae Chang****

ABSTRACT

Important evidence or clue in general crime as well as crime relevant to computer has been discovered in digital devices including computer with advance of information technology and turning into a information-oriented society. A leakage of industrial technology and confidential business information is related to digital devices such as computer, smart phone, USB, etc. This paper deal with a current state and comparison analysis of digital forensic technology for developing way of forensic field, so we seek for method of preventing information leakage.

Key words : 디지털 포렌식, 디지털 증거, 포렌식 도구, 포렌식 절차

접수일(2016년 11월 23일), 게재확정일(2016년 12월 12일)

* 중앙대학교/일반대학원 산업융합보안학과
** 중앙대학교/일반대학원 산업융합보안학과
*** 중앙대학교/경영경제대학 융합보안학과
**** 중앙대학교/경영경제대학 산업보안학과(교신저자)

1. 서 론

과학기술의 발달은 디지털 장치 특히 컴퓨터 를 이용한 범죄의 증가를 가져왔다. 또한 정보화 사회의 도래는 디지털 문화라는 새로운 문화를 탄생시켰다 세계에서 생성되고 있는 정보의 90% 이상이 디지털 형태로 생성되고 있다. 이러한 환경 속에서 범죄의 글로벌화가 가속화되고 있으며, 기업의 내부정보 및 개인정보 유출로 대형 보안사고가 자주 발생하고 있다.

이에 따라 디지털 증거를 다루는 디지털 포렌식이 전 세계 법집행기관에 중요한 화두로 대두되고 있다. 미국 등의 선진국은 이미 1990년대 초반부터 이 분야에 대한 발전을 위해 막대한 예산을 투자하여 탄탄한 기반을 구축해 나가고 있으며 국내에서도 2000년대 초반부터 법과학으로서 디지털 포렌식에 대한 인식을 새로이 하고 노력을 기울이고 있다.

IT 기술이 끊임없이 진화하면서 최근에는 스마트폰과 같은 새로운 디지털 기기의 보급 및 활용도가 높아졌으며, 디지털증거도 휴대폰과 같은 이동형 디지털 저장매체(스마트폰, 노트북, USB 등)에서 더 많이 확보하게 되었다. 다양한 디지털 저장매체의 출현으로 인해 조사 대상은 점점 다양해지고 복잡하게 변모하고 있으며, 디지털 증거를 찾기 위한 분석 시간이 지속적으로 증가하고 있다.

최근에 발생하고 있는 산업기술 및 영업비밀 유출 사건은 컴퓨터, 스마트폰, USB 등 다양한 디지털 저장매체와 관련성을 가지는 경우가 많으며, 이로 인해 디지털 포렌식 분석 도구는 디지털 저장매체별로 각각 다양하게 존재하고 있다.

본 논문에서는 디지털 포렌식 기술을 비교분석 하고, 정보유출을 방지할 수 있는 방안을 모색해보고자 한다.

2. 디지털 포렌식 개념

전통적으로 포렌식이란 개념은 지문, 모발, DNA 감식, 변사체 검시 등 법의학 분야에서 주로 사용되어 왔다. 그러나 최근 다양한 정보기기들의 활용과 정보생산 및 유통에 있어서 대부분이 디지털 형태로 이용됨에 따라 포렌식 개념은 물리적 형태의 증거뿐만이 아니라 전자적 증거(electronic evidence)를 다루는 디지털 포렌식 분야로 확대되고 있다.

포렌식은 첨단과학기법으로 각종 부정행위를 밝혀내기 때문에 과학수사라고 말하기도 한다. 개인용 컴퓨터가 개발되고 이용되기 시작한 1990년대 초부터 디지털 포렌식의 개념이 등장하게 되었고, 이후 포렌식이란 개념이 컴퓨터 보안영역 및 법학분야에서 사용되기 시작하였다.

초기에는 법집행기관에서 컴퓨터를 중심으로 압수 및 수색하는 문제와 압수된 기기로부터 잠재적인 증거를 발견하는 것에 중점을 두었으나 차츰 단순히 과학적인 컴퓨터 조사방식 및 절차뿐만 아니라 법률 제도와 각종 기술을 포함하는 분야로 자리 잡게 되었다.

IT 기술의 발전 및 급격한 정보화 사회로의 변화는 정보의 디지털화를 가속화 시키는 계기가 되었고, 이로 인하여 컴퓨터 관련 범죄뿐만 아니라 일반 범죄에서도 중요 증거가 컴퓨터를 포함한 디지털 정보기기 내에 보관되는 경우가 증가하게 되었다. 이에 따라 디지털 증거의 수집 및 분석을 위한 기술이 요구되었다. 디지털 범죄의 증가는 자연스럽게 디지털 증거를 수집 및 분석하고, 디지털 증거가 변조되거나 위조되지 않았다는 무결성 확보를 목적으로 하는 초기의 디지털 포렌식 개념을 탄생시켰다.

디지털 포렌식은 법적으로 받아들여질 수 있는 방법으로 디지털 증거를 식별(identifying), 보존(preserving), 분석(analyzing), 제출(presentation)하는 과정(process) 혹은 범죄에 관한 사건의 재구성이나 계획된 작업에 해를 가하는 인가받지 않은 행위에 대한 예측을 가능하게 하기 위한 목적으로 디지털 소스로부터 추출한 디지털 증거를 보존(preservation), 수집(collection), 검증(validation), 식별(identification), 분석(analysis), 해석(interpretation), 문서화(documentation), 제출(presentation)하는 과학적으로 도출되고 증명된 수단의 이용으로 정의할 수 있다.

3. 디지털 증거의 개념과 특성

3.1 디지털 증거(digital evidence)

IOCE(International Organization on Computer Evidence)는 디지털 증거를 2진수 형태로 저장 혹은 전

송되는 것으로서 법정에서 신뢰할 수 있는 정보로 정의하고 있으며, SWGDE(Scientific Working Group on Digital Evidence)는 디지털 형태로 저장·전송되는 증거 가치가 있는 정보로 정의하고 있다.

일반적으로 '디지털 증거'를 '전자적 증거(electronic evidence)' 와는 다른 층위의 개념으로 구별하여 사용하고 있다. 전자적 증거는 아날로그방식 또는 디지털방식으로 저장된 정보 혹은 데이터를 총체적으로 의미하는데 반해서, 디지털 증거는 이 중에서 후자의 방식으로 저장된 정보 및 데이터만을 의미한다.

3.2 디지털 증거의 특성

디지털 증거가 기본의 물리적 증거와 구별되는 특성은 크게 매체독립성, 대량성, 원본과 사본의 구별곤란성, 변조용이성, 비가시성, 전문성으로 나눌 수 있다.

디지털 정보는 저장매체나 매개체의 특성에 따른 영향을 받지 않는다. 즉 저장되는 매체의 성질에 좌우되지 않고, 항상 일정한 정보의 값을 유지한다(매체독립성). 디지털정보는 복사 또는 기타 방법을 통한 정보의 생산과 이전 등이 자유롭기 때문에 원본 및 사본의 대량생산이 가능하다(대량성). 디지털 정보는 반복된 복사과정을 거치더라도 디지털 정보의 값 혹은 가지가 동일하게 유지되지 때문에 질적인 측면에서 원본과 사본의 구별되지 않게 된다(원본과 사본의 구별 곤란성). 디지털 증거는 가변적인 증거로서 간단한 조작만으로도 위조 내지 변조가 가능하고, 일부 내용 삭제 내지 변경이 용이하다는 점에서, 증거로서의 취약성을 갖게 된다(변조용이성). 디지털 증거는 전자적 정보의 형태로 기록·저장되어지기 때문에 인간의 오감으로는 직접 정보의 내용을 인지할 수 없다(비가시성). 디지털 증거를 재판에서 증거로 활용하기 위해서는, 디지털형태로 저장된 정보를 다시 현시적인 증거로 가시화하는 변환과정이 필수적으로 요구되며, 이에 관한 전문가의 참여가 필요하다(전문성).

4. 디지털 포렌식 절차와 종류

4.1 디지털 포렌식 절차

일반적으로 범죄현장에서 수집된 증거가 포렌식 전문기관에서 분석되어 결과물인 보고서가 작성되기까지의 과정이 절차적인 모델에 기반하여 디지털 포렌식 체계가 이루어지고 있다. 디지털 포렌식 절차에 대한 절차 모델들은 이미 많은 학자와 전문가들에 의해 제시되고 있으며 예컨데 미 법무부의 가이드라인은 디지털 증거의 처리과정을 평가, 획득, 분석, 문서화와 보고의 단계로 구분하고 있다. 평가와 획득은 범죄현장에서 현장에 임장한 수사관에 의해 이루어지며, 증거가 포렌식 전문기관으로 이송된 이후에 전문적인 포렌식 조사관 혹은 분석관에 의해 이루어진다. 이러한 일반적인 절차는 전통적인 물리적 증거의 처리 절차와 매우 비슷하다.

디지털 포렌식은 크게 증거 수집, 증거 분석, 증거 제출과 같은 절차로 이루어진다. 손상되기 쉽고, 사라지기 쉬운 디지털 증거가 저장된 저장매체(컴퓨터 메모리, 하드디스크, USB 등)에서 데이터의 무결성을 보장하면서 데이터를 읽어 내야 한다. 이 때 무결성이란 원 저장매체에 대한 데이터 변조가 일어나지 않음을 의미한다. 증거 수집에서 유용한 기술로는 무결성을 보장하는 이미징(imaging) 기술 등이 있다.

증거 수집으로 얻은 데이터로부터 유용한 정보를 이끌어 내야 한다. 유용한 정보는 보통 저장 매체에 존재하는 파일 시스템의 내부나 외부에 존재할 수 있다. 예를 들면, 범죄자는 저장매체에 존재하는 NTFS와 같은 파일 시스템 내부나, NTFS에서 사용하지 않는 저장매체 구역에 중요 정보를 숨길 수 있다. 증거 분석에서 유용한 기술로는 삭제된 파일 복구 기술이나 암호화된 파일 해독 및 문자열 검색 기술 등을 들 수 있다.

입수된 디지털 증거가 법적 증거로 채택되기 위해서는 증거자료의 신뢰성이 확보되어야 한다. 이를 위해 법률적으로 디지털 포렌식에 대한 표준 절차뿐만 아니라 포렌식 툴에 대한 검증 절차 또한 이루어져야 한다.

4.2 디지털 포렌식 종류

디지털 포렌식 종류는 크게 컴퓨터 포렌식, 모바일 포렌식, 네트워크 포렌식으로 나누어 볼 수 있다.

컴퓨터 포렌식은 Windows나 Unix와 같은 운영

체제를 탑재한 범용 컴퓨터를 대상으로 하는 디지털 포렌식을 말한다.

모바일(임베디드) 포렌식은 핸드폰과 같은 모바일 기기나 태블릿, 디지털 카메라, 캠코더, PDA와 같은 다양한 디바이스에 대한 디지털 포렌식을 말한다.

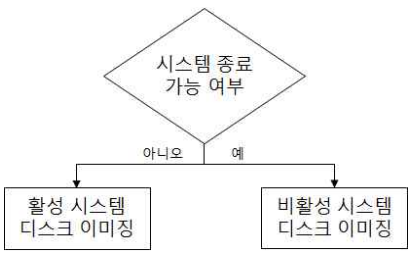
네트워크 포렌식은 컴퓨터나 핸드폰과 같은 통신 디바이스를 사용해서 통신이 이루어지는 경우에, 이런 통신 디바이스에서 네트워크 정보, 사용자 로그, 인터넷 사용 기록 등과 같은 정보를 수집 및 분석하는 포렌식을 말한다.

5. 증거수집 단계의 디지털 포렌식

5.1 비활성 시스템 포렌식

비활성 시스템 포렌식은 운영체제가 종료된 컴퓨터나 핸드폰 같은 기기에 대한 증거 수집을 말하며, 주로 하드디스크나 플래시 메모리로부터 데이터를 얻는 것으로 이루어진다.

핸드폰 기기와 같이 비휘발성 저장매체를 분리 및 접근하기가 용이하지 않은 기기는 상대적으로 컴퓨터 하드디스크와 같이 쉽게 저장매체를 분리 및 접근할 수 있는 기기보다 데이터 획득이 어렵다. 데이터를 쉽게 획득할 수 있는 컴퓨터 하드디스크에서도 원본 데이터의 이미지를 만들게 되는데, 이는 나중에 증거 분석을 할 경우에 원본데이터가 변경되는 것을 막기 위해서이다. 따라서 본 저장매체에 있는 데이터의 무결성을 보장할 수 있는 이미징 기술이 필요하다.



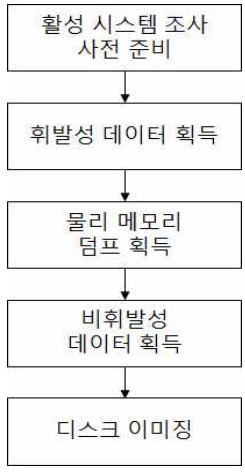
(그림 1) 디스크 이미징 단계

5.2 활성 시스템 포렌식

활성 시스템 포렌식은 운영체제가 종료되지 않은 컴퓨터나 핸드폰 같은 기기에 대한 증거 수집을 말한다. 하드디스크와 같은 비휘발성 매체뿐만 아니라 컴퓨터 메모리와 같은 휘발성 저장매체로부터 데이터를 얻는 것으로 이루어진다.

운영체제가 종료되지 않은 시스템에서의 데이터 획득 순서는 휘발성 저장매체에 있는 데이터들을 먼저 획득한 후에, 비휘발성 저장매체에 있는 데이터들을 획득하는 순서로 이루어진다. 포렌식 대상이 되는 활성 시스템에서 휘발성 저장매체나 비휘발성 저장매체에서 데이터를 획득하기 위해서는 활성 시스템 운영체제에 있는 명령어들을 사용하기 보다는 포렌식 도구를 사용해서 데이터를 획득해야 한다.

왜냐하면 대상 시스템의 운영체제 명령들이 공격자에 의해서 이미 바뀌어 있어서 그 명령을 사용할 경우 사건 증거들을 삭제할 가능성이 있고, 영체제 명령어들이 바뀌지 않았다 하더라도, 정상적인 운영체제 명령의 실행이 시스템 정보를 변경할 가능성이 있기 때문이다. 또한, 운영체제는 시스템 보호를 위해서 일부 데이터나 파일들에 대해 사용자들의 접근을 막고 있다. 즉, 운영체제에서 제공하는 명령어들에 의해서는 접근할 수 없는 데이터나 파일들이 존재한다. 따라서 운영체제의 보호 체계를 우회할 수 있는 포렌식 도구의 사용이 필요하다.



(그림 2) 활성 시스템 포렌식 단계

6. 증거분석 단계의 디지털 포렌식

6.1 덤프 메모리 분석

프로세스가 사용 중인 가상 메모리의 덤프를 획득했을 경우에 사용자 ID나 패스워드와 같은 유용한 정보가 가상 메모리에 남아 있을 수 있다. 프로세스를 위한 가상 메모리는 보통 코드 영역, 데이터 영역, 스택 영역 등으로 나누어지며, 데이터 영역이나 스택 영역이 프로세스에서 필요한 여러 정보를 저장하고 있다.

6.2 윈도우(Windows) 레지스트리 분석

Windows는 레지스트리(registry)에 프로그램이나 시스템에 관한 다양한 정보를 저장하고 있다. 레지스트리 정보는 regedit와 같은 명령으로 살펴볼 수 있다. 레지스트리 Hive 파일들 중 SAM 파일은 패스워드들의 해시 정보를 가지고 있으며, 운영체제에 의해서 암호화되어 보호되고 있다.

6.3 타임라인(Timeline) 분석

파일 시스템들은 각각의 파일들이 만들어진 시간 정보와 마지막으로 접근된 시간 정보 그리고 마지막으로 수정된 시간 정보들을 가지고 있다. 또한 NTFS 파일 시스템에서는 $LogFile과 $UsrJrnl이라는 시스템 파일이 존재하며, 파일 시스템에 대한 사용 로그를 남기고 있으므로 이로부터 좀 더 많은 정보를 얻을 수 있다.

6.4 삭제된 파일 복구

하나의 파일은 여러 클러스터들의 리스트로 이루어져 있으며, 이런 리스트 정보가 파일 시스템에 들어있다. 일반적으로 하나의 파일을 삭제할 경우에 파일 시스템은 클러스터들에 들어 있는 파일 내용을 지우는 것이 아니라 파일에 할당된 클러스터들을 인식하지 못하게 하여 파일을 지운다. 따라서 인식되지 않은 클러스터들이 다른 파일에 할당되지 않는 한 삭제된 파일을 복구할 가능성이 있다.

6.5 비정상적인 파일 찾기

사용자가 중요한 데이터를 숨길 경우에 윈도우에서 파일을 숨김 속성으로 놓거나 파일 확장자를 바꾸어서 데이터를 숨기려 할 수 있다. 보통 하나의 파일 형식은 하나의 파일 확장자를 가지며 또한 하나의 식별자(identifier)라 불리는 유일한 값을 가진다. 이 식별자는 파일 생성 시 헤더에 자동으로 저장된다. 따라서 확장자를 바꿀 경우에는 파일 확장자와 이 식별자가 맞지 않으므로 확장자가 바뀐 파일들을 찾을 수 있다.

6.6 이메일 분석

파일 시스템에서 삭제된 파일을 복구하는 것과 비슷하게 로컬 시스템에서 삭제된 이메일을 복구할 수 있다. 하나의 이메일을 삭제할 경우에 이메일 프로그램은 메일박스에 있는 이메일의 내용을 지우는 것이 아니라 이메일의 헤더 값을 바꾸어서 이메일을 삭제하게 된다. 따라서 삭제된 이메일을 복구할 가능성이 있다.

6.7 로그 분석

어떤 장치나 응용 프로그램을 사용하게 되면, 운영체제나 응용 프로그램이 로그를 남기는 경우가 있으며 이런 로그는 사건 분석에 중요한 정보가 될 수 있다.

NTFS 파일 시스템의 경우 $LogFile, $UsrJrnl에 파일 생성, 접근 등에 관한 로그가 남아 있으며, USB 포트에 연결했던 USB들의 사용로그가 레지스트리에 남아 있다. 또한, 임시파일, 쿠키, 즐겨찾기, ActiveX 등으로부터 인터넷 사용 행적을 조사할 수 있다.

6.8 슬랙 공간(slack space) 분석

파일 시스템은 하나의 큰 파일을 저장할 때 여러 클러스터들로 나누어 저장하게 된다. 이 때 가장 마지막 클러스터에는 파일의 가장 뒷부분을 저장한 다음 남게 되는 공간이 생길 수 있는데 이런 공간을 파일 슬랙 공간(slack space)이라고 한다. 하드디스크에는 할당되지 않은 공간들과 볼륨 슬랙 공간, 파티션 슬랙 공간 등이 있다. 사용자들이 이런 슬랙 공간에 데이터를 숨겨 놓을 수 있다.

6.9 가상 데스크톱 분석

클라우드 컴퓨팅은 최근 IT 시장에서 가장 큰 성장

을 보이고 있는 분야 중 하나로, 수많은 기업들이 비용 절감 및 효율 향상을 위해 사설 클라우드 컴퓨팅 서비스로 가상 데스크톱 환경을 도입하고 있다.

사용자가 가상머신에 접속하면, 이와 관련된 정보가 사용자 컴퓨터에 기록되는데, Windows 7 환경에서 VMware는 레지스트리, 로그 기록이 생성된다. Microsoft는 Windows에서 기본으로 제공하는 원격 데스크톱 관련 레지스트리에 생성되고 로그 기록은 생성되지 않는다. 하지만 Microsoft는 웹으로 가상머신에 접속 시 고유의 시그니처를 사용하므로 이를 이용하여 웹 히스토리에서 접속 흔적을 찾을 수 있다.

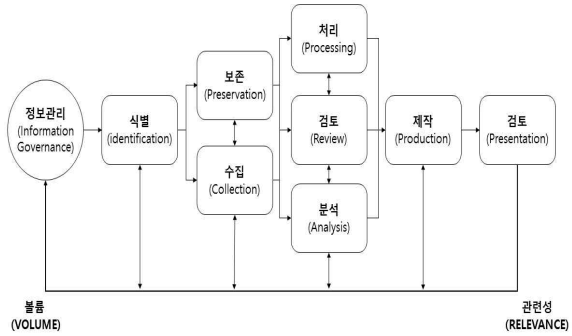
<표 1> 포렌식 기술 비교 분석

기 술	복구	검색	분석
덤프 메모리 분석			O
윈도우 레지스트리 분석		O	O
타임라인 분석			O
삭제된 파일 복구	O		
비정상적인 파일 찾기		O	
이메일 분석	O		O
로그 분석	O		O
슬랙 공간 분석			O
가상 데스크톱 분석			O

7. 전자증거개시제도(e-Discovery)

전자증거개시제도는 영미법에서 유래한 제도로 정식재판이 진행되기 전, 법원의 개입 없이 소송당사자가 서로 공소 제기된 사건과 관련한 정보를 서로의 요청에 의해 공개하는 제도이다. 서로 필요한 정보를 재판 전에 제공받기 때문에 시간낭비를 줄이고 쟁점을 명확히 할 수 있다. 공개된 정보는 법률적 지식을 갖춘 소송당사자의 변호인에게 미리 검토를 받기 때문에 재판 없이 합의를 이끌어 내는 실효적 효과도 거두고 있다.

기존 증거개시와는 다른 다양한 조건을 요구하는 전자증거개시를 위한 별도의 절차적 모델이 논의되었는데 이것이 바로 전자증거개시 참조모델(Electronic Discovery Reference Model, EDRM)이다. 전자증거개시 참조모델은 전자증거개시의 각 절차에 대한 기능을 정의하고 있으며 자세한 사항은 EDRM 공식 사이트(www.edrm.net)에서 확인할 수 있다. 기본적인 EDRM 절차는 다음 그림과 같다.



(그림 3) 기본적인 EDRM 절차

정보관리(Information Governance) 단계는 사건과 관련된 정보를 필요할 때 빠르고 정확하게 산출할 수 있도록 사전에 관리하는 과정이다. 증거개시를 요청받으면 일정 기간 내에 관련 자료를 전달해줘야 하는데 사전에 관련 데이터가 특징 별로 명확히 구분되어 있지 않다면 증거개시절차를 제대로 따를 수 없다.

식별(Identification) 단계는 소송발생 시 증거개시의 가능성이 있는 모든 자료를 확인하는 과정이다. 이 과정에서는 각 자료의 소유자 및 관리자의 물리 및 논리적 위치를 명확하게 파악한다.

보존(Preservation) 단계는 식별 단계에서 파악된 자료가 변경 혹은 삭제되지 않도록 보존하는 과정으로 소송자료보존(Litigation Hold)라는 용어로 명시하고 있다. 실수든 고의든 보존해야 할 자료가 변경되거나 삭제될 경우 많은 불이익을 받게 된다.

수집(Collection) 단계는 식별하여 보존된 자료를 원본의 무결성을 훼손하지 않고 추출하는 과정이다. 원본의 무결성을 보장하기 위해서는 검증된 도구를 사용해 원본을 복제 혹은 이미징을 하거나 별도의 논리적 증거파일로 만들어 추출한다.

처리(Processing) 단계는 수집된 자료의 정보를 취

합하는 과정이다. 자료의 정보는 자료의 내용뿐만 아니라, 파일의 메타데이터(파일명, 생성시간, 크기 등)까지 해당되며, 이 정보를 추후에 효과적으로 분석 및 검토할 수 있도록 전용 솔루션을 이용해 취합한다.

검토(Review) 단계는 처리된 자료와 사건과의 관련성을 살펴보는 과정이다. 검토는 변호사가 바로 수행하기도 하지만 사건의 규모가 크고 자료가 방대한 경우, 법률팀이나 대리인을 통해 사전처리를 거치기도 한다.

분석(Analysis) 단계는 수집된 자료에서 사건과 관련된 문맥이나 내용을 기반으로 검토가 필요한 정보를 선별하는 과정이다. 보통 특정 시간 범위 내에서 키워드로 검색하거나 포맷 별로 분류하여 선별한다.

제작(Production) 단계는 처리, 검토, 분석을 마친 자료를 당사자나 법원에서 합의된 포맷으로 변환하는 작업이다. 메타데이터가 손상되지 않은 원본데이터를 전달하기도 하지만 검토가 쉬운 TIFF나 PDF 형태의 포맷으로 변환해서 전달하는 것이 일반적이다.

제출(Presentation) 단계는 제작을 마친 자료를 서로 합의한 방법으로 당사자 혹은 법원에 공개하는 과정이다.

기존 증거개시와 다르게 전자증거개시는 디지털 형태로 저장된 전자증거(Electronically Stored Information)의 특성으로 인해 이에 대한 전문적 지식을 갖춘 외부 전문가의 도움이 절대적으로 필요하고, 쉽게 변조될 수 있기 때문에 별도의 보존의무를 지켜야 한다. 또한 원본데이터 자체는 가독성이 없으므로 일정한 형태로 변환해 제출해야 하는데 이때 메타데이터도 고려되어야 한다. 또한, 개시요청자가 당사자의 시스템에 현장 조사를 요구할 수도 있는데 이 때 면책특권이 포함된 자료나 사건과 관련 없는 개인 혹은 비밀정보가 포함될 수도 있기 때문에 범위와 대상을 명확히 할 필요가 있다.

과거에는 전자증거개시제도가 미국 내에서만 중요시 되었지만 최근 미국으로 진출한 글로벌 기업에서 미국 시장에서의 소송을 위해 전자증거개시를 준비하고 있다. 따라서, 국내에서도 글로벌 시대에 맞추어 전자증거개시와 관련된 연구가 활발하게 진행될 필요가 있다.

8. 결 론

디지털 포렌식은 정보기기에 내장된 디지털 자료를 근거로 삼아 그 정보기기를 매개체로 하여 발생한 어떤 행위의 사실 관계를 규명하고 증명하는 신규 보안 서비스 분야로써, 검찰, 경찰 등의 국가 수사기관에서 범죄 수사에 활용되며, 일반 기업체 및 금융회사 등의 민간분야에서도 디지털 포렌식 기술의 필요성이 증가하고 있다.

IT기술의 발달과 더불어 디지털 포렌식 기술 또한 다양해지고 발전하였지만 디지털 포렌식 분야는 사용자의 컴퓨터 시스템에 대한 정보 수집 및 분석에서 벗어나 다양한 모바일(임베디드) 시스템을 모두 조사 대상으로 해야 하는 시점에 이르렀다.

또한, 최근에는 안티 포렌식 기법 또한 다양해지고 안티 포렌식 도구가 늘어나고 있다. 정보유출을 방지하기 위해서는 안티 포렌식 기법에 대한 체계적이고 심도 있는 연구가 진행되어야 하며, 다양한 장치와 시스템에 맞는 개별적인 분석 방안과 수집 및 분석 연구가 진행되어야 할 것이다.

참고문헌

[1] 신용녀, 신승목, “대용량 디지털포렌식 서비스에 대한 실증적 연구”, 한국인터넷진흥원(IIS), 제1권, 제2호, pp.83-100, 2010.

[2] 정익래, 홍도원, 정교일, “디지털 포렌식 기술 및 동향”, 전자통신동향분석, 제22권, 제1호, pp.97-104, 2007.

[3] 임경수, 박종혁, 이상진, “디지털 포렌식 현황과 대응 방안”, 보안공학연구논문지, 제5권, 제6호, pp.461-474, 2008.

[4] 장상희, 김등화, 박정흠, 강철훈, 이상진, “가상 데스트톱 환경에 대한 디지털 포렌식 연구”, 정보보호학회논문지, 제23권, 제2호, pp.203-212, 2013.

[5] 김봉수, “디지털 증거(Digital evidence)와 포렌식(Forensics)”, 정보통신방송정책, 제21권, 제6호, pp. 37-54, 2009.

[6] 송유진, 이재용, “외장형 USB 저장장치의 포렌식 조사방법”, 한국산업정보학회논문지, 제15권, 제4호, pp.39-45, 2010.
[7] 이승원, 노영섭, 한창우, “윈도우 환경에서의 증거 수집 시스템 설계 및 구현에 관한 연구”, 정보보호학회논문지, 제23권, 제1호, pp.57-67, 2013.
[8] 조규상, “윈도우즈 파일시스템에서 파일명령 구별을 위한 디지털 포렌식 방법”, 보안공학연구논문지, 제12권, 제4호, pp. 379-396, 2015.
[9] 이종찬, 박상준, “포렌식에서 디지털 증거의 우선순위 스케쥴링”, 한국정보통신학회논문지, 제17권, 제9호, pp.2055-2062, 2013.
[10] 박기홍, 노시영, “클라우드 서비스에 대한 포렌식 측면의 수사 방법”, 한국산업정보학회논문지, 제17권, 제1호, pp.39-46, 2012.
[11] 탁희성, “전자증거개시제도(E-Discovery)에 관한 연구”, 연구총서, 제11권, 제13호, pp.11-145, 2011.

[著者紹介]

박 광 민 (Gwangmin Park)
2015년 선문대학교 신문방송학과 졸업
2015년 중앙대학교 산업융합보안학과 석사과정
email : pakkoamin@gmail.com

홍 승 완 (Seungwan Hong)
2015년 대진대학교 컴퓨터공학과 졸업
2015년 중앙대학교 산업융합보안학과 석사과정
email : sw25sw25@cau.ac.kr

김 종 필 (Jongpil Kim)
2015년 중앙대학교 융합보안학과 석사과정
email : jpkim@softcamp.co.kr

장 항 배 (Hangbae Chang)
2006년 연세대학교 정보시스템관리 박사
2007년 대진대학교 경영학과 조교수
2012년 상명대학교 경영학과 조교수
2014년 중앙대학교 산업보안학과 부교수
email : hbchang@cau.ac.kr