제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

국내 환경을 고려한 디지털 포렌식 조사 모델 정립 방안

임경수*, 이창훈**
*한국전자통신연구원 지식정보보안연구부
**한신대학교 컴퓨터공학부
e-mail: lukelim@etri.re..kr*; chlee@hs.ac.kr**

A Study on Digital Forensic Investigation Model for Korea

Kyung-Soo Lim*, Changhoon Lee**
*Knowledge-based Information Security & Safety Research Department, ETRI
**School of Computer Engineering, Hanshin University

요 약

국내에 디지털 포렌식 연구가 시작된 2000년 초반에는 디지털 증거의 취약성에 주의하여 디지털 증거의 보존을 중심으로 조사·분석을 어떻게 할 것인가에 초점을 맞추었다. 이를 통해 수집한 데이터와 분석한 결과를 법적인 증거 자료로 어떻게 인정받을 것인지가 주요 이슈였다. 하지만 최근에는 디지털 포렌식 조사가 일반 민사·형사 사건에 모두 활용되면서 디지털 증거 처리만이 아닌 사건 발생부터 법정 증언까지 고려한 전체 조사 과정을 아우르는 모델로 발전하고 있다. 따라서 이러한 변화에 따르고 국내 환경에 적합한 디지털 포렌식 조사 모델이 필요하다. 본 논문은 국내외 디지털 포렌식 조사 모델에 대한 연구를 살펴보고, 이를 국내 환경에 적합하도록 정립하기 위한 방안을 기술한다.

1. 서론

디지털 포렌식에서 가장 기본이 되는 분야 중의 하나가 디지털 포렌식 조사를 위한 수행 절차 즉 조사 모델이다. 디지털 포렌식 진행 과정을 살펴보면, 사건 발생을 인지한 순간부터 증거 수집, 조사 과정을 거친 후, 그 결과를 법정에 제출하는 형태로 진행된다. 기존에 널리 알려진 디지털 포렌식 조사 모델은 각각 중요시하는 초점에 따라 제안한 절차가 달라, 조사관에게 혼란을 가중하였다. 예를 들어 과학적 체계, 기술적인 방법, 조사 절차, 법적 절차 등 다양한 초점에 맞춘 조사 모델이 존재한다. 국내 수사기관의 경우는 초창기의 미국 수사기관에 제안한 수사 가이드라인을 그대로 적용하였고, 향후 대검찰청 디지털 증거 압수수색 모델과 같은 형태로 발전하였다.

국내에 디지털 포렌식 연구가 시작된 2000년 초반에는 디지털 증거의 취약성에 주의하여 디지털 증거의 보존을 중심으로 조사·분석을 어떻게 할 것인가에 초점을 맞추었다. 이를 통해 수집한 데이터와 분석한 결과를 법적인 증거 자료로 어떻게 인정받을 것인지가 주요 이슈였다. 하지만 최근에는 디지털 포렌식 조사가 일반 민사·형사 사건에 모두 활용되면서 디지털 증거 처리만이 아닌 사건 발생부터 법정 증언까지 고려한 전체 조사 과정을 아우르는 모델로 발전하고 있다.

한편 이러한 연구는 조사 프로세스의 적용 범위나 과학적으로 정립하기 위한 연구는 많이 발표되었지만, 급변하는 IT 환경 변화에 대응하기에는 방안에 대해선 미흡한 부분이 존재하며, 국내 환경에 적합한 조사 모델에 대한 연구는 수행되지 않고 있다. 본 논문은 최근의 포렌식 동향을 반영하여 국내 환경에 적합한 디지털 포렌식 조사 모델을 정립하기 위한 방안에 대해 기술한다.

2. 국외 포렌식 조사 모델

먼저 Kruse와 Heiser[7]가 제안한 디지털 포렌식 수사 모델은 단순히 증거 처리에만 중점을 두었으며, 증거 수집, 증거 조사, 증거 분석 단계로 간단히 구분하였다. Lee[8]가 제안한 현장 수사 모델은 전체 수사 절차에 중심을 둔 것이 아니라, 범죄 현장에서 어떻게 대응할 것인지를 제시하였으며, 일반적인 물리 증거 조사까지 포괄하는 모델이다. 이 모델은 인지(recognition), 식별(identification), 특정(individualization), 재현(reconstruction)으로 나뉜다. 즉 어떤 대상을 잠재적인 증거 자료로 삼을 것인지를 파악하여 “무엇을(What)”, “어디서(Where)” 찾을 것인지를 결정하고, 이를 기록·수집·보존하는 인지 단계, 물리적·생물학적·화학적 및 그 이외의 증거들을 분류하여 기존 실험 결과와 비교하는 식별 단계, 이러한 가능성 있는 증거들로부터 개인이나 사건(event)을 실험과 해석을 통해 유일한 대상을 선정하는 특정 단계, 이전 단계까지 도출된 결과를 종합하여 사건을 재현하고 이를 보고·현출하는 재현 단계로 나뉜다. 이처럼 체계적이고 방법론적인 모델을 제시하였지만, 조사 준비, 데이터 수집, 법정 제출에 대하여는 자세히 언급하지

않고 있으며, 디지털 데이터의 처리에 대해서는 구체적인 언급이 없다.

2001년에 디지털 포렌식 분야의 국제 학술 대회인 DFRWS (Digital Forensic Research Workshop)에서는 디지털 포렌식을 중심으로 한 새로운 조사 모델이 발표되었다[5]. DFRWS의 조사 모델은 인지, 보존, 수집, 조사, 분석, 현출, 결정의 단계로 나뉜다. 이 모델의 초점은 법적 효력이 있는 디지털 증거를 다루기 위해 각 단계별로 필요한 기술들을 소개하고, 앞으로 어떠한 연구를 수행해야 할 것인가를 제시한 것이다. 하지만 [표 5-1]과 같이 각 단계에 대하여 필요한 기술이나 방법론을 나열하는 수준에 그치고 있다. 예를 들어 분석 과정은 기본적으로 증거 자료의 보존성을 기반으로 수행하며, 분석 과정에 대한 추적 가능성, 파일 유형이나 데이터에 대한 통계 분석, 데이터 마이닝 기술을 활용한 분석 기술, 타임라인 분석을 통한 시간 정보 별 이벤트 분석, 여러 데이터들의 연관 관계를 판별하여 특이점을 도출하는 상관 분석 등을 나열하였다.

<표 1> DFRWS에서 제시한 디지털 포렌식 조사 과정

사건 확인	보존	수집	조사	분석	제출
사건 인지	사건 관리	보존	보존	보존	기록
조사 결정	이미징 기술	증명된 방법	추적성	추적성	전문가 증언
프로파일링	연계 보관	증명된 하드웨어	유효성 기술	통계 분석	설명
비정상 탐지	시간 정보 확인	증명된 소프트웨어	필터링 기술	프로토콜 분석	요점 중심 진술
고소		법적 권한	패턴 매칭	데이터 마이닝	대응책
시스템 모니터링		비손실 압축	은닉 데이터 조사	타임라인 분석	통계 해석
감정 분석		샘플링	은닉 데이터 추출	상관 분석	
기타		데이터 축소			
		복구 기술			

Casey가 제안한 사이버 수사 절차[4]는 사건 발생, 가치 평가, 현장 대응, 확인・압수, 보존, 복구, 조사, 분류, 재구성 및 검색, 분석, 보고, 진술 및 증언의 단계로 나뉘며, 전체 수사 절차를 다루고 있는 것이 특징이다. 사건 발생 단계는 범죄가 신고 되거나 위법 행위가 감지되어 수사를 시작하는 단계이며, 가치 평가 단계는 사전 준비의 일환으로 전반적인 수사 과정에서 어떤 대상이 우선적으로 조사할 가치가 있는지를 평가하여 순위를 선정하는 단계이다. 현장 대응은 수사를 진행하는 기관의 입장에서 자체적으로 수립한 규칙・절차에 따라 조사를 진행하는 것을 말한다. 확인・압수 단계는 이전 단계에서 수립한 가치 평가와 현장 대응 절차를 바탕으로, 수사 대상을 확인하고 이를 압수, 포장하는 과정까지를 포함한다. 보존 단계는 무결성을 유지하기 위해 사본을 생성하고 압수한 원본을 적절한 보관시설에 보존하는 단계이며, 복구 단계는 삭제되거나 은닉된 데이터를 복구하여 가능한 모든 데이터를 추출하는 과정이다. 수집 단계는 복구된 데이터를 비롯하여 사건 해결에 필요한 데이터를 수집하는 과정을 가리키며, 분류 단계는 이러한 데이터를 특정 기준으로 분류하여 분석 과정에 필요 없는 데이터를 삭제하여 조사 대상을 줄이는 과정이다. 재구성 및 검색은 사건과 관련된 정보를 이용하여 수집한 데이터를 재구성하여 필요한 정보를 검색하는 과정이며, 분석 단계는 이전 단계의 결과를 바탕으로 평가, 실험, 종합, 상관 분석, 유효성 판단 과정을 거쳐 법정에 제출할 증거 자료를 생성하는 과정이다. 보고 단계는 생성한 증거 자료가 법정에서 받아들여질 수 있도록 상세히 기록하고 그 과정들을 문서화하는 과정이며, 진술 단계는 이러한 증거 자료, 기록, 관련 조서들을 법정에서 활용할 수 있도록 알기 쉽게 해석하고 이를 진술・증언하는 과정이다. 이처럼 최근에 발표되는 모델은 사건 조사의 전체 과정을 다루는 모델로 발전되고 있다.

<표 2> 디지털 포렌식 조사 모델 비교

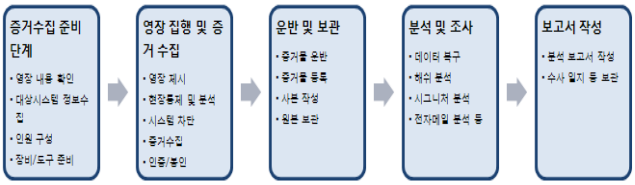
구분	Séamus 확장 모델[3]	Kruzer 모델[7]	LEE 모델[8]	DFRWS 모델[5]	Reith 모델[4]	Casey 모델[6]
조사 준비	인지 (Awareness)				확인	사건 발생
	허가 (Authorization)					
	계획 (Planning)				준비	가치 평가
	고지 (Notification)					
현장 대응	탐색/식별 (Search/Identification)		인지, 확인	확인		현장 대응
	수집 (Collection)	수집	수집, 보존	수집, 보존	수집, 보존	확인, 압수, 보존
이송 및 보	이송 (Transport)					
	보관					

관	(Storage)					
분석	조사 (Examination)	조사	구별	조사	조사	복구,조사,분류, 구성 및 검색
	재구성 (Hypothesis)	분석	재구성	분석	분석	분석
법적 대응	제출 (Presentation)		보고 및 제출	보고	보고	보고
	증명/변호 (Proof/Defense)			결정		진술 및 증언

2. 국외 포렌식 조사 모델

국내 관련 연구로 대검찰청 디지털 증거 압수 수색 모델과 경찰청 디지털 증거 처리 가이드라인을 소개한다. 먼저 대검찰청 디지털 증거 압수 수색 모델은 수사 기관에서 수행하는 절차이므로 영장 집행 위주로 구성된 것이 특징이며, 증거수집 준비단계, 영장 집행 및 증거 수집, 운반 및 보관, 분석 및 조사, 보고서 작성 단계로 나누어진다.

"증거수집 준비단계"는 현장 출동 전에 수사를 준비하는 단계이다. 수사를 시작하기에 앞서 사건 정보와 영장 내용을 확인하고, 필요 인원과 장비·도구 등을 준비하는 단계이다. 먼저 사건 관련 확인 사항을 숙지하여 사건 유



(그림 2) 대검찰청 디지털 증거 압수수색 모델 개관

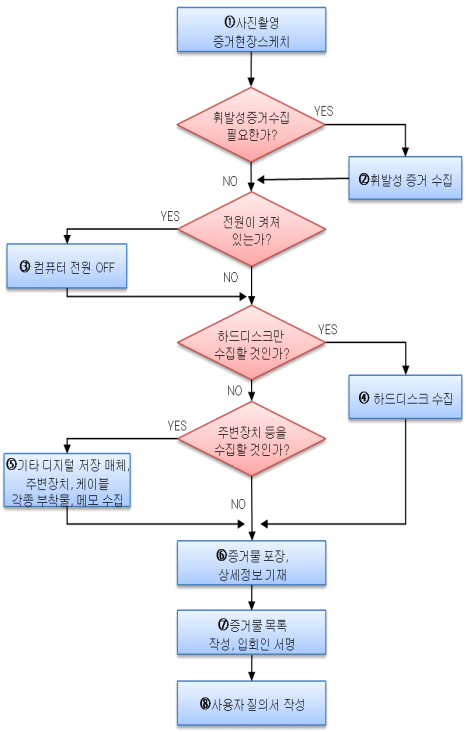
형, 영장의 내용과 범위, 수사 대상 시스템 파악, 증거 수집 장비와 도구를 준비한다.

"증거 수집 단계"는 현장에서 증거 자료의 수집에 어려움이 없도록 준비 사항을 면밀히 검토하고, 수사 진행을 위한 전체 과정을 확인한다. "영장 집행 및 증거 수집 단계"는 사건 현장에서 조사를 수행하는 과정으로, 현장에서의 대응 요령, 증거 수집, 증거 포장 및 인증 절차로 진행된다. 먼저 영장을 대상 기관에 제시하여 수사 협조를 구한 뒤, 현장을 통제하여 증거 인멸 시도를 차단한다. 나아가 현장 시스템의 접근을 차단하고, 주요 조사 시스템을 선별하여 필요한 증거 시스템을 확보하거나 필요한 증거 데이터를 수집한다. 확보한 시스템이나 수집한 증거 자료는 제3자의 공증이나 피수사 담당자의 확인 과정을 거쳐 봉인한다.

"운반 및 보관" 단계는 봉인된 증거 자료를 해제하고 증거물의 법적 효력을 위해 기록·등록한다. 원본 증거 자료는 사본을 생성하여 향후 분석할 수 있도록 하며, 원본은 전자기장 및 충격으로 부터 보호할 수 있는 공간에 별도로 보관한다.

"분석 및 조사" 단계는 생성한 사본을 바탕으로, 삭제 데이터 복구, 해쉬값 분석, 파일 시그니쳐 분석, 응용 프로그램 사용 흔적 분석(전자메일을 비롯한 인터넷 메시징 서비스 등)을 수행한다. 분석된 결과는 분석 보고서를 작성하여 보관하며, 향후 법정에서 증거 자료로 제시할 수 있도록 문서화한다.

경찰청 디지털증거 처리 표준 가이드라인은 전반적인 수사 전체에 대한 모델을 제시하기 보다는 전반적인 증거 처리 원칙부터 증거 수집, 분석, 결과보고서 작성 등에 대해 상세히 다루고 있는 것이 특징이다. 가이드라인에서 제시한 수사 모델은 증거수집, 증거분석 의뢰, 증거분석, 결과보고서로 나뉜다. [그림 5-3] 은 가이드라인에서 제시한 디지털 증거 수집 절차도를 나타내며, 이처럼 가이드라인은 세부적인 수사 절차와 주의 사항을 설명하는 것에 중점을 둔다. 증거분석 과정은 유형별로 증거분석 표준절차를 나눈 것이 특징으로, 디스크 분석, 네트워크 분석, 웹 사용 분석, 전자우편, 악성코드, 데이터베이스, CCTV, 휴대폰, 암호화 파일 등으로 나뉜다.



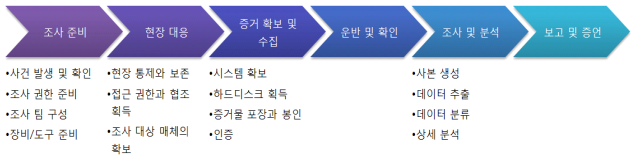
(그림3) 경찰청 디지털 증거 수집 절차도

3. 국내 환경을 고려한 디지털 포렌식 조사 모델

앞서 살펴 보았듯이 디지털 포렌식 조사 모델은 단순히 증거 조사만을 다루다가 점차 사건 인지부터 법정 증언까지 증거 처리의 전과정을 아우르는 형태로 발전하고 있으며, 제안하는 기관의 특성에 맞게 세분되고 있다.

이러한 연구들을 비교하여 최상위 관점에서 정의한 디지털 포렌식 조사 모델은 “조사 준비”, “현장 대응”, “증거물 확보 및 수집”, “운반 및 확인”, “조사 및 분석”, “”, “법정 증언”까지 6 단계로 나뉜다.

디지털 포렌식 조사 모델의 첫 번째 단계는 전반적인 조사 진행을 위한 조사 준비 단계이다. 일반 범죄 수사와 동일하게 피해자의 신고나 자체 조사를 통해 위법 행위가 발견되면 본격적인 수사가 시작된다. 본격적인 수사에 앞서 내부적으로 준비 과정을 거치게 된다. 이러한 조사 준비 과정은 사건 발생 및 확인, 조사 권한 획득, 인원 구성, 장비・도구 준비 단계로 나누어진다.



(그림 4) 디지털 포렌식 조사 모델 정의

사건 준비과정이 완료되면 해당 기관은 현장에 출동하여 조사에 필요한 조치를 취하게 된다. 즉 사전 준비 단계에서 면밀히 준비한 사항들을 현장에 적용하여 현장 통제 및 조사 권한 획득, 관계자 면담, 현장 통제 및 보존, 조사 대상 시스템의 확보 과정을 수행한다. 이 단계의 목표는 본격적인 증거 수집을 시작하기 이전에 현장을 통제하고 이를 보존하여 향후의 증거 수집 과정을 준비하는 것이다.

현장 조사의 기본적인 조치를 수행하였으면, 조사 대상자의 증거물을 확보(압수)하고 어떤 데이터를 어떠한 방법으로 수집할 것인지를 결정한다. 수사 기관은 영장의 기재 내용에 의거하여 압수 수색을 진행하여 필요한 증거물을 압수하는 과정이다. 조사 기관은 의뢰인의 협조를 얻어 현장에서 데이터를 수집 및 분석할 것인지, 시스템이나 중요 자료에 대해 사본을 생성하여 이를 확보할 것인지 협의한다.

증거 운반 및 확인 과정에서 가장 핵심적인 것은 획득한 증거물의 무결성 유지와 훼손방지이다. 또한 증거물의 누락 및 도난이 없도록 견고한 절차를 거치는 일 또한 중요하다. 디지털 증거 획득 절차가 완료되면 획득한 증거물 및 기록한 증거물 목록이 완성된다. 증거물을 인수인계할 때 반드시 이 목록을 함께 전달하여 증거물들을 비교 한 후, 누락된 증거물은 없는지 확인해야 한다.

조사 및 분석은 분석하여야 할 데이터가 많고, 사건에 따라 조사하여야 할 데이터가 서로 다르므로 많은 시간이 소요될 수 있다. 따라서 어떠한 방법으로 분석을 수행할 것인지에 대한 전략을 수립하고 분석할 전체 데이터를 유형에 따라 분류한 후, 상세 분석을 통해 신속하고 효율적인 분석 과정이 될 수 있도록 한다.

결과 보고서는 조사・분석자의 모든 행동과 관찰 내역, 분석 과정 등의 정확히 기록되어야 하고 각 단계의 결과와 완벽히 일치해야 그 결과를 증거로 인정받을 수 있게 된다. 보고서의 내용은 쉽게 이해할 수 있는 용어를 사용하여 정확하고 간결하며 논리 정연하게 작성한다. 작성자는 결과 보고서에 서명하고 작성 내용에 대해 책임을 진다.

3. 결론 및 향후 연구

본 논문은 국내외 디지털 포렌식 조사 모델을 비교항여 국내 환경을 고려한 표준화 형태의 조사 모델을 정의하였다. 국내 수사기관에서 사용하고 있는 조사모델은 포렌식 연구가 시작된 초창기의 모델을 그대로 적용하였기 때문에 최신 연구 내용이 반영되어 있지 못하기 때문에 표준화된 형태의 조사모델이 필요하다. 향후 연구로는 정립한 조사 모델에 대한 자세한 수행 절차와 방법을 연구한다. 또한 최근의 IT 환경, 즉 클라우드 컴퓨팅, 스마트폰, 태블릿 PC 와 같이 조사 대상의 다변화에 적용할 수 있도록 연구할 계획이다.

Acknowledgement

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(No. 2011-0005648)

참고문헌

[1] Sundresan Perumal, Digital Forensic Model Based On Malaysian Investigation Process, International Journal of Computer Science and Network

[2] Ricci S.C. Ieong, FORZA – Digital forensics investigation framework that incorporate legal issues, Digital Investigation, Volume 3, Supplement 1, The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06), 2006

[3] Séeamus Ó Ciardhuáain, An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Volume 3, Issue 1, 2004

[4] Mark Reith, Clint Carr, Gregg Gunsch, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Volume 1, Issue 3, 2002

[5] DFRWS, DFRWS TECHNICAL REPORT-A Road Map for Digital Forensic Research, 2001

[6] Eoghan Cesay, Digital Evidence And Computer Crime-Forensic Science Computers And The Internet 2nd edtion, Elsevier, 2004

[7] Warren G Kruse, Jay Heiser, Computer Forensics: Incident Response Essentials, Addison-Wesley Professional, 2001

[8] Timothy Palmbach, Marilyn Miller, Henry Lee, Henry Lee's Crime Scene Handbook. San Diego, Academic Press, 2001