디지털 포렌식 수사 절차 모델 제안[1)]

신재룡**, 이석희**, 이상진**
**고려대학교 정보보호대학원 / 정보보호기술연구센터

A Proposal of Digital Forensic Investigation Process Model

Jaelyong Shin**, Seokhee Lee**, Sangjin Lee**
**Center for Information of Secutity of Technologies(CIST), Korea University.

요 약

완벽한 디지털 범죄 수사를 위해서는 우수한 디지털 포렌식 기술이 우선적으로 요구되겠지만, 범죄수사의 특성상 기술이외에도 법적, 제도적 측면들이 적절하게 조합되어야만 한다. 본 논문에서는 디지털 포렌식의 제도 및 정책적인 면에서 디지털 범죄 수사의 절차가 현실적으로 적용 가능하고, 범죄 해결에 효율적이며 합법성을 유지하면서 진행될 수 있도록 새로운 형태의 디지털 포렌식 절차를 제안하고자 한다.

I. 서론

컴퓨터와 인터넷의 대중화로 인하여 디지털 장비의 사용 및 가상환경에서의 생활이 일상화 되어 가고 있고, 많은 점에서 윤택한 삶을 제공해 주고 있다. 하지만 인지하는 바와 같이 최근의 거의 모든 범죄 유형에서 컴퓨터가 사용되고 있다. 예를 들어, 전통적인 일반 범죄인 살인, 성폭행의 경우에도 범행의 동기 와 수법을 추적하기 위해 e-mail이나 피해자 PC를 조사하고 있다.

이처럼 현대사회의 수사국면 변화를 볼 때, 효율적이고 체계화된 범죄 수사를 위해서 현 수사 환경에 적용이 가능하고 발전하고 있는 범죄기술에 대응할 수 있는 디지털 포렌식 절차가 필요하게 되었다. 적합한 디지털 포렌식 절차의 제안을 위하여 기존에 발표된 여러 관련 분야의 연구 결과를 바탕으로 새로운 절차 모델을 제안하고자 한다.

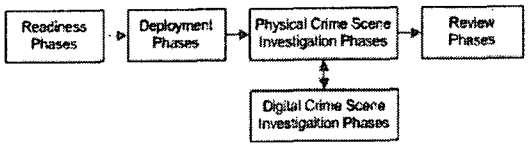
1.1 기존에 제안된 모델

기존에도 시스템 및 네트워크 침해 사고와 관련된 대응 절차를 수립한 연구결과들이 다수 존재하고 있다. 대표적인 연구 결과들을 살펴보면, 먼저 침해사고 대응의 측면에서 "Incident Response"라는 책의 "incident response methodology"가 있으며,[1] 법 집행 기관의 측면에서는 미 법무부(U.S. Department of Justice)에서 발간한 "Electronic Crime Scene Investigation Guide"가 있다.[10] 더불어 미 공군에서는 다양한 절차 모델의 특성을 모아서 일반화시키기 위한 노력으로 발간한 "Abstract Process Model"을 개발하였다.[5]

하지만 본 논문이 기초로 하여 개선, 발전시키고자 한 절차 모델은 Brian Carrier 등이 발표한 "An Integrated Digital Investigation

1) 본 연구는 정보통신부 대학 IT 연구센터 육성·지원 사업의 연구 결과로 수행되었습니다.

Process" 이다. 이 모델은 5개의 큰 단계안에 총 17개의 세부단계를 포함하고 있으며, 전통적인 일반 범죄에 대한 수사 절차 이론을 근간으로하여 발전시켰으며, 절차를 세분화하고 일반화시키고자 노력하였다.[5]



(그림 1) Integrated Digital Investigation Process

1.2 기존 절차의 개선 및 요구 사항 도출

"Integrated Digital Investigation Process(IDIP)" 모델 등에서 현실적인 적용의 문제점과 더불어 수사 절차상의 효율성 및 체계성 그리고 일반 범죄까지의 적용이 필요한 측면들에서 개선점을 발견할 수가 있었다.

· 실제 수사에 적용 가능한 모델이야 한다.

IDIP 모델에서의 "Deployment" 단계에서 수행하는 범죄에 대한 신고 및 탐지 이후에 범죄 사실 여부를 확신하고 수사를 전개하는 것은 현실적으로 어떠한 형태의 범죄 현장 조사가 수반되지 않고서는 실시될 수 없다. 하지만 독립적으로 "Deployment"단계 이후에 수사 단계를 설정함으로써 현실성이 결여되어 있다.[4]

· 범죄 현장별로 구분된 수사절차가 필요하다.

일반적으로 범죄는 그 범행 현장이 구분된다. 예를 들어 일반 범죄인 살인의 경우에도 실제 범행 현장은 '1차 범행현장'으로 이후에 사체유기 등으로 발생한 범행현장을 '2차 범행현장'으로 구분하여 정의하고 있다. 이처럼 디지털 포렌식 범죄도 1차 범행현장은 용의자측이 되고, 2차 범행현장은 피해자측으로 정의하는 것이 필요하다. 더불어 각각의 범행현장은 물리적, 디지털적인 범행현장으로 구분하여 정의할 필요가 있다. 따라서 효율적인 수사 및 대응을 위해서는 각 현장에 대한 분명한 명시와 구분되는 수사절차 및 방법론의 적용이 필요하다.

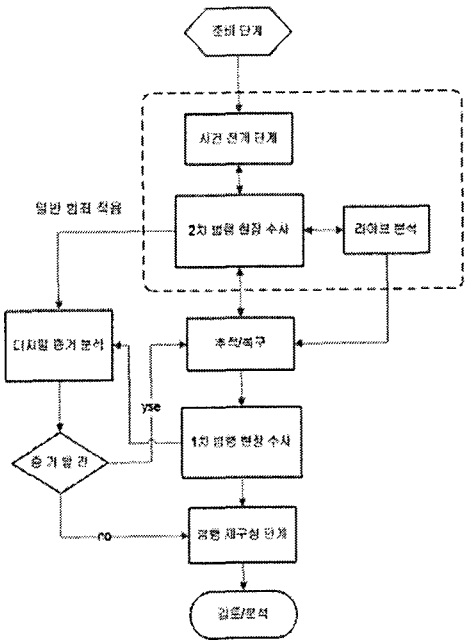
· 전통적인 일반 범죄의 디지털 증거에 대한 적용이 가능해야 한다.

해킹 등과 같은 관련 디지털 범죄 외에도 일반 범죄에서도 컴퓨터와 같은 디지털 장비에는 범죄와 관련된 증거 및 자료가 다수 존재한다. 이것은 프랑스 법과학자 로칼드가 주장한 접촉하는 두 개체는 서로의 흔적을 주고받는다는 "Locard's Exchange Principle"으로도 설명이 가능하다. 예를 들어 피해자의 컴퓨터에서 생성되는 인터넷 히스토리나 임시파일들은 범죄에 대한 직접적인 증거 또는 범죄에 접근할 수 있고 용의자의 범위를 좁힐 수 있는 참고자료로도 활용할 수 있다.[7][8]

본 논문에서 제안하는 모델은 위에서 언급한 각 개선 요구 사항들을 포함하여 체계화된 범죄 수사를 지원하게 되는 디지털 범죄 수사 모델링을 추가하여 좀더 발전된 형태의 디지털 포렌식 절차를 제안하였다.

II. 디지털 포렌식 수사 절차 제안

아래 (그림 2)에서 보는 바와 같이 제안한 모델은 일반 범죄 적용 분야를 제외하고 크게 8개의 단계로 구성되며 선형적인 절차가 아니라 현실적으로 적용이 가능한 동적인 절차 모델이다.



(그림 2) 제안한 디지털 포렌식 절차

이 모델은 법집행기관인 사법기관 및 제한된 기업체 자체의 사고 대응팀에서 모두 적용이 가능한 모델로 세부 단계별 설명은 다음과 같다.

2.1 준비단계

보통 수사를 논의할 때 수사 절차상의 기법에 대해서 많은 관심을 가지고 여러 연구가 진행되어 왔지만, 준비단계는 다소 간과되는 경향이 있었다. 그러나 디지털 포렌식의 준비과정은 다음과 같은 많은 이득을 제공할 수 있는 중요한 단계이다.

- 범죄 예방효과(범죄의지 제거)
- 증거 제공으로 효율적인 수사 지원[6]

이를 위해서는 첫째, 수사 진행 전에 현재 기술 및 동향에 맞는 장비를 구비해야 하며, 항상 사용가능하게 준비가 되어 있어야 한다. 뿐만 아니라 실제 수사에 투입되는 인력은 적절한 교육을 통하여 다양한 범죄환경에서 임무를 수행할 수 있게 준비되어야 한다. 둘째, cctv와 같은 사회 전반의 보안 인프라가 구축됨으로써 범죄에 대한 잠재적인 증거들의 수집 및 최종적인 범죄 해결이 용이해질 수 있다.[5]

2.2 사건 전개 단계

여러 형태로 사고에 대한 탐지 및 신고가 이루어지고 난 뒤 2차 범행 현장에 대한 최소한의 수사가 이루어짐으로써 해당 사고를 사건화(범죄화)시킬 것인지를 결정할 수 있다. 이 결과를 바탕으로 압수·수색 영장을 발부하는 것과 같이 법적인 수사 승인을 득하고 난 후 용의점에 수사를 집중하는 단계이다.

더불어 이단계의 수사 결과 및 획득된 증거 및 정황을 바탕으로 효율적인 수사 진행을 위해 수사 진행 계획 및 전략을 수립하는 '디지털 범죄 수사 모델링'작업이 필요하다. 이러한 모델링 작업은 다음과 같은 장점을 가지고 있다.

- 수사 진행에 대한 시각화를 제공한다.
- 수사과정에서 발생한 변동사항에 대한 유동적이고 체계적인 대응이 가능하다.
- 수사 업무의 분담이 용이해진다.
- 유사한 형태의 범죄에 대해서 잘 만들어진 모델링은 재사용이 가능하다.

이러한 모델링 방법은 UML(Unified Modeling Language)등을 사용하여 디지털 포렌식 관점의 범죄 수사 모델링을 생성할 수 있다.[3]

2.3 2차 범행 현장 수사 단계

2.3.1 물리적 범행 현장 수사

피해자측 범행 현장의 물리적인 증거 또는 환경에 대한 수사가 이루어지는 단계이다.

1. 현장 확보 : 차후 원활한 수사진행을 위해 범행 현장 및 잠재적인 증거를 확보하는 단계이다.

2. 현장 조사 및 기록 : 범행 현장을 확인하여 증거를 수집하고, 범행 현장의 범위를 한정한다. 이 때, 가용한 모든 수단(사진, 스케치, 녹화)으로 잠재적인 증거를 위해 기록을 남겨야 한다.

3. 증거 수집 및 조사 : 추가적인 증거 수집과 수집된 증거를 조사하여 용의점을 확보한다. 필요에 따라 디지털 범행 현장 수사의 시작 및 수사 연계를 조율할 수 있다.

2.3.2 디지털 범행 현장 수사

디지털 범죄 증거와 범죄가 존재하는 가상 공간에 대한 수사 단계이다.

1. 현장 확보 : 디지털 범행 현장을 복제하여 이미지화하여 잠재적인 증거들을 확보한다. 이 단계에서부터 디지털 증거에 대한 무결성을 위한 "Chain of custody"가 시작되어야 한다.

2. 증거 수집 및 조사, 기록 : 증거 수집과 범죄 수사 모델링을 기반으로 데이터의 상호 연관성을 그래프 및 맵핑, 타임라인 작업으로 증거를 세부적으로 조사한다. 이때 전문 조사 툴을 사용하며, 각 조사 과정을 기록하는 작업을 연동해야 한다.

2.4 라이브 시스템 분석 단계

2차 범행현장 수사 단계의 선택적인 단계이다. 라이브 시스템은 현재 시스템이 작동중인 상태를 말하며, 라이브 시스템 분석 단계는 매우 예민한 과정이고 라이브 상태에서만 획득이 가능한 정보들이 많이 존재하므로 간과해서는 안 된다. 이 단계에서는 실행되는 다수의 휘발성 정보인 실행 프로세스, 메모리 내용, 네트워크 활동 정보, 임시파일을 손상 없이 분석할 수 있으며, 용의자를 지속적으로 감시할 수 있는 장점이 있다.[2]

2.5 추적/복구 단계

피해자측의 2차 범행 현장 수사 결과를 바탕으로 용의자(1차 범행 현장)를 추적하고 복구하는 단계이다. 예를 들어, 획득된 Public, Private IP 주소를 통해 1차 범행 현장의 위치를 추적하는 단계이다.

이 단계에서 심도 깊은 수사진행과 민감한 정보에 대한 합법적인 접근을 위해 반드시 법적으로 충분한 권한을 재확인 및 획득해야 한다.[4]

2.6 1차 범행 현장 수사 단계

추적하여 발견된 1차 범행 현장은 2차 범행 현장에서의 수사 방법과 유사하게 물리적인 수사와 디지털 수사가 병행으로 이루어진다. 2차 범행 현장 수사와 구별되는 점은 1차 범행 현장에서 발견되는 증거는 범행사실을 결정할 수 있는 증거이어야 한다는 것이다. 예를 들어, 디지털 장비를 실제로 용의자가 사용했다는 것을 증명할 수 있어야 하며 해당 범행 시간에 맞는 타당한 증거들이어야 한다는 것이다. 세부 절차는 2.3과 동일하다.

2.7 범행 재구성 단계

본 논문에서는 이 단계를 강화하고자 한다. 이유는 수사의 진정한 목적을 달성하기 위해 좀더 많은 노력을 기울일 필요가 있기 때문이다. 수사의 진정한 목적은 범인의 체포보다도 범행이 가설이 아니라 최대한 사실화시켜 범죄의 실체를 파악하는 것이다. 따라서 여러 전 단계에서 수집된 개별적인 증거들을 모아 범행의 실체를 재구성하는 것이 필요하다.

2.7.1 디지털 프로파일링

범죄자 프로파일링은 심리학을 근간으로 발전한 분야로 범인의 독특한 행동양상이나 특성을 고려하여 용의선상의 축소나 궁극적인 범죄해결을 추구하는 분야이다. 디지털 범죄에서도 마찬가지로 각종 범죄에서 발생한 디지털 증거자료를 기반으로 범죄자 프로파일링이 가능하다. 본 논문에서는 '디지털 프로파일링'이라는 용어로 표현하겠다.[7][9]

예를 들어 피해자 측과 용의자 측에서 수집된 디지털 증거자료들 중에 컴퓨터에 저장되어 있는 이메일, 웹브라우져의 임시파일이나 히스토리파일, 채팅 및 메신져 기록, 각종 문서나 동영상 파일, 실행파일 등으로 범인의 특성이나 행동 양상, 범행 타임라인 등을 구성할 수가 있다. 물론 이러한 자료들이 결정적인 증거로써 사용될 수도 있으나, 그렇지 않더라도 범죄의 진실에 접근하는데 사용이 가능하다.

2.8 검토/분석 단계

수사의 목표를 이루고 난 후에 수사 전반에 대한 검토와 분석을 통하여 해당 범죄를 마무리하고, 차후에 보완할 점을 도출하는 단계이다. 명심할 것은 수사간에 발생한 문제점과 실수도 명확히 분석함으로써 차후에 과오를 막을 수 있으며 수사의 질을 향상시킬 수 있다.

III. 결론

본 논문에서는 디지털 포렌식 수사가 시작해서 사건을 마칠 때까지의 전반적인 절차를 제시하였다. 제안한 절차의 장점을 간략히 정리하면 다음과 같다.

첫째, 가능한 실제 일반적인 수사과정의 흐름과 절차에 맞추었으며, 둘째, 사건 전개 단계에서 '디지털 범죄 수사 모델링'의 적용으로 전체적인 수사진행에 효율성과 체계성을 제공하였다. 셋째, 한 범죄 안에 존재하는 다양한 범행 현장을 구분함으로써 명확한 수사 범위를 한정할 수 있다. 넷째, 범죄의 실체를 파악하기 위하여 결정적인 증거 이외에 앞에서 언급한 각종 관련 디지털 자료들을 '디지털 프로파일링'하여 활용할 수 있다.

요컨대 디지털 포렌식 수사 능력을 향상시키기 위해서는 기술, 절차, 제도의 각 요소가 삼위일체 되어야 한다. 이러한 측면에서 이 논문은 디지털 범죄 수사의 절차를 재정립하고 새로운 형태의 절차 모델을 제시하였다.

[참고문헌]

[1] Chris Prosise and Kevin Mandia , "Incident Response & Computer Forensics, second edition", McGraw-Hill, 2003.

[2] 이현우, 심정재, "사례로 배우는 해킹사고

분석&대응", 영진닷컴, 2004.

[3] A. Chris Bogen and David A.Dampier, "Preparing for Large-Scale Investigations with case Domain Modeling", presented at Digital Forensics Research Workshop, New Orleans, LA, 2005.

[4] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model",http://www.dfrws.org/(current 2005 January 11), 2004.

[5] Brian Carrier and Eugene H. Spafford, "Getting Physical with the Digital Investigation Process", International Journal of Digital Evience, Fall 2003, Volume 2, Issue 2.

[6] Robert Rowlingson Ph.D, "A Ten Step Process for Forensic Readiness", International Journal of Digital Evience, Winter 2004, Volume 2, Issue 3.

[7] E. Casey "Criminal Profiling, Computers, and the Internet", Journal of Behavioral Profiling, May, 2000, Volume 1, No. 2.

[8] E. Casey "Digital Evidence and Computer Crime-Forensic Science, computers and the Internet, Second Edition", ELSEVIER, 2004.

[9] 브라이언 이니스, "프로파일링", 휴먼앤북스, 2005.

[10] National Institute of Justice.(July 2001) Electronic Crime Scene Investigation a Guide for First Responders. http://www.ncjrs.org/pdffiles1/nij/187736.pdf.