디지털 범죄 수사 절차 모델링 기법에 관한 연구 *

이석희**, 신재룡**, 임경수**, 이상진**

**고려대학교 정보보호대학원 / 정보보호기술연구센터

A Study of Digital Investigation Modeling Method

Seokhee Lee**, Jaelyong Shin**, KyoungSoo Lim**, Sangjin Lee**

**Center for Information of Security of Technologies(CIST), Korea University.

요 약

디지털 범죄 수사 능력은 디지털 포렌식 기술 개발 뿐만 아니라 정책적인 수사체계가 얼마나 잘되어 있느냐에 따라 달라진다. 점차 다양화 되고 지능화 되어가는 디지털 범죄를 수사하기 위해서는 디지털 범죄 수사 체계 모델링이 필요하다. 따라서 본고에서는 디지털 범죄의 종류와 그에 적합한 수사 절차를 언급하고, UML(Unified Modeling Language)을 이용하여 디지털 범죄 수사 절차를 체계화하고 모델링 하는 방법을 제시하고자 한다.

I. 서론

유비쿼터스 사회가 도래하게 되면서 컴퓨터 관련 범죄뿐만 아니라, 일반 범죄에서도 결정적인 증거 또는 단서가 컴퓨터에 보관되어 있는 경우가 증가하고 있다. 또한 디지털 장비들의 종류가 다양해지고 있으며, 그 수도 증가하고 있어 이에 대한 수사 기법과 적절한 수사 절차가 필요한 실정이다[10].

디지털 포렌식 연구는 기술적인 측면과 절차적인 측면으로 크게 2부분으로 구분할 수 있다. 근래에 국내 사법기관을 중심으로 디지털 포렌식에 대한 관심이 높아지면서 디지털 포렌식 기술에 대한 연구가 진행되고 있다. 그러나 디지털 범죄 수사 절차 구성을 위한 연구는 다소 미흡하다. 디지털 범죄 수사 능력은 디지털 포렌식 기술과 이를 적법절차를 준수하면서 활용할 수 있는 수사 절차가 확립되어 있는지에 따라 크게 달라진다.

따라서 디지털 포렌식 기술을 수사과학 관점에서 체계적으로 적용하기 위하여, 디지털 범죄 수사 절차를 확립해야할 필요성이 있다[10][11]. 디지털 포렌식 과정은 사고 대응 준비, 증거 수집, 증거 분석, 보고서 작성으로 크게 4가지로 구분할 수 있다[8][12].

하지만 디지털 범죄의 유형이 점점 다양해지고 지능화 되고 있기 때문에 이러한 포렌식 수사절차 또한 복잡해지고 있으며, 디지털 포렌식 기술이 범죄 유형에 따라 필요로 하는 것이 달라진다. 관련된 증거와 사건이 많아질수록 점점 더 복잡해지게 된다. 보통 이러한 경우에 한 사람의 디지털 포렌식 전문가의 경험과 판단을 바탕으로 수사가 진행되게 되는데, 이는 수사관에게 전적으로 의존하게 되어 디지털 포렌식 수사 위험성이 높아지게 된다. 따라서 포렌식 수사 절차에 대한 추상화, 정형화에 대한 연구가 필요하다.

UML(Unified Modeling Language)은 컴퓨터 포렌식 수사 절차를 개발하고, 추상화, 정형화, 모델링하려는 연구에 적합하다[1]. 따라서 UML을 이용하여 포렌식 수사절차를 모델링하는 방법을 제안하고, 모델링이 필요한 이유를

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

제시하고자 한다.

II. 사건 도메인 모델링

디지털 범죄 수사를 모델링하기 위해서는 다음과 같은 사항을 고려하면서 모델링을 하여야 한다.

- 생성할 다이어그램 선택 : 선택 다이어그램에 따라 문제를 공략하는 방법과 해결책을 실현하는 방법에 영향이 있음
- 모델을 다양한 수준으로 세밀하게 표현
- 현실을 반영한 모델 작성
- 상호 독립적인 모델들 몇 가지를 선택하여 모델링에 착수

사건 도메인은 구조 모델 중 클래스 다이어그램을 사용하도록 한다. 클래스 다이어그램은 객체들 사이의 관계 및 포함 관계를 표현하는데 적절하기 때문에 사건 도메인을 모델링하는데 적합하다[4]. 도메인이란 디지털 범죄 수사 과정 중 수사관이 조사나 분석을 해야 하는 클래스들의 집합으로 정의한다. 다시 말해 조사 범위 내에 있는 항목들을 나타낸다. 도메인을 모델링하는 방법은 다음과 같다.

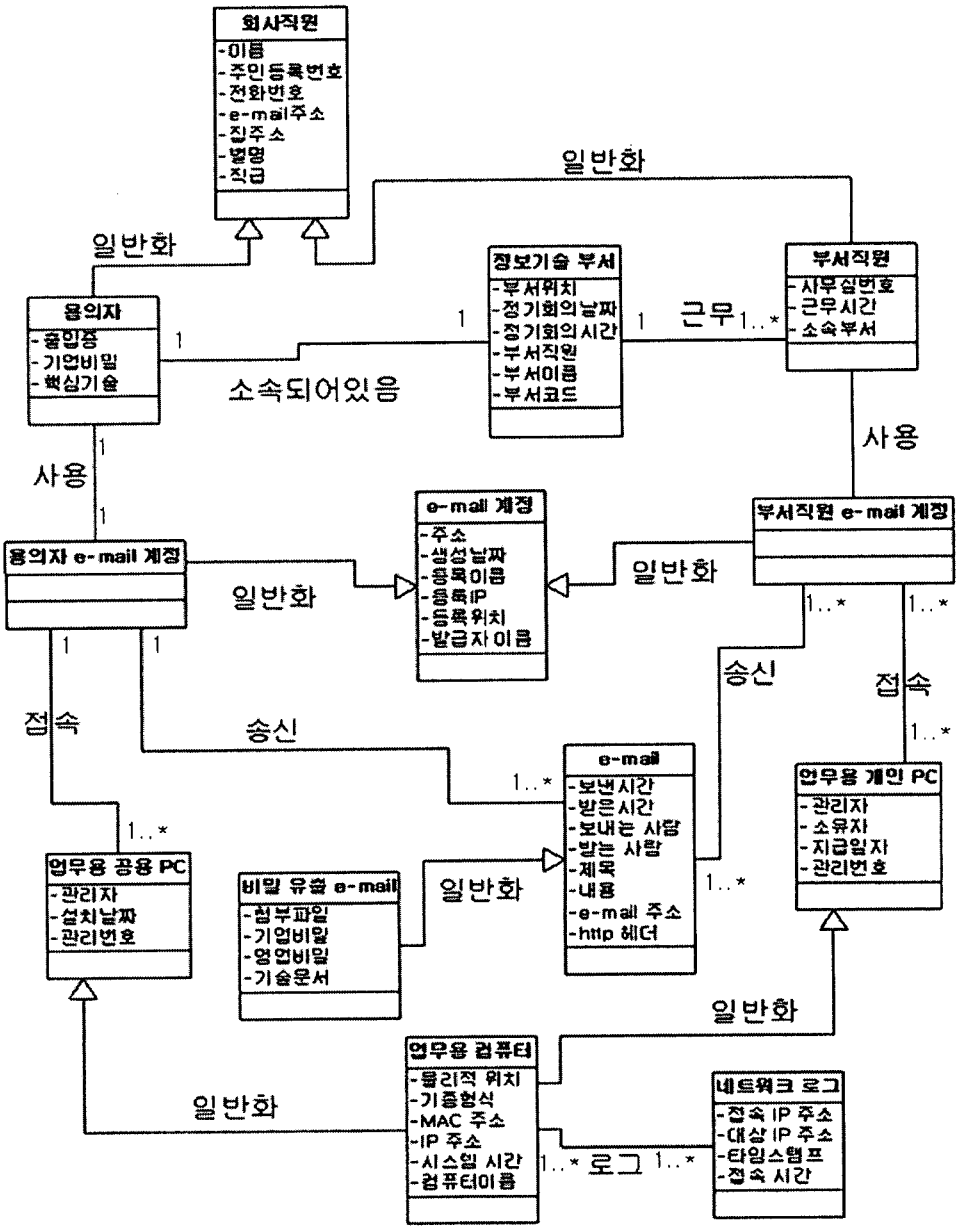
- 사건의 클래스 정립
- 사건내 항목들과 클래스들을 확인
- 사건내 클래스들 사이의 관계 확립
- 모델링 작업

클래스들은 사건의 주변 환경, 컴퓨터 시스템, 용의자, 영장, 체포 보고서, 침해사고 보고서등 사건 조사 범위 내에 있는 사항들을 나타낸다. <표 1>은 클래스를 항목별로 나타낸 것이다. 클래스 정립 완료 후 각 클래스가 가지고 있는 내용들과 관계를 확인한다. <표 2>는 클래스들 사이에 있을 수 있는 관계들의 종류를 나타낸 것이다[7].

어떤 기업의 한 정보기술 부서의 연구원이 기업 내의 인터넷 검색이나 자료 검색용으로 사용하는 공용 PC를 이용하여 기업비밀이나 기술문서를 E-mail에 첨부하여 보낸 사건을 가정한다면 부서원들과 공용 PC 그리고 e-mail 계정, 부서명 등의 클래스를 생각할 수 있다. 이러한 클래스들과 그 항목을 고려하여 사건 도메인 모델링을 <그림 1>과 같이 표현하였다[3].

클래스	예시
물리적인 장치나 물건	모바일 폰, 하드 디스크, CD-ROM
세부사항을 기술한 보고서	시장 보고서, 사고 보고서
거래, 처리내용	지불, 판매, 보증금, e-mail 전송
조사 대상이 되는 사람	용의자, 목격자
내용을 담고 있는 것	데이터베이스, 하드 디스크
담겨져 있는 내용	파일, 거래처리 내용
컴퓨터나 전자 시스템	인터넷 상점, 신용카드 인증 시스템
추상적인 단어	동기, 알리바이, 정신이상, 빈곤
조직	조직폭력단, 협조부서, 정부조직
이벤트	강도, 만남, 전화 수신 기록, 파일 접근
정책과 규칙	법률, 절차
재정보고서, 계약서, 법률적인 문제	고용계약서, 차용 계약, 영수증, 소환장
서비스	인터넷 서비스 제공자, 전화 서비스, 이동전화 서비스
매뉴얼, 책	비행 매뉴얼, 폭발물 제조 매뉴얼
장소	집, 거리

<표 1> 클래스의 종류



<그림 1> 기업기밀 e-mail 유출 사건 도메인 모델링

항 목	예 시
A는 B의 물리적인 부분	DVD Drive - Workstation
A는 B의 논리적인 부분	네트워크 지도 - 네트워크 침입
A는 B가 물리적으로 보관하고 있는 것	사용된 CDROM - CD 케이스
A는 B의 명세서	Readme 파일 - 실행 프로그램
A가 B를 소유	용의자 - 차량
A는 B의 구성원	용의자 - 조직폭력집단
A는 B의 하부 조직	정보기술 부서 - 회사
A는 B를 사용하거나 관리	시스템 관리자 - 회사 네트워크
A는 일반적인 B가 특별화 된 것	시스템 관리자 - 회사 직원
A가 B와 통신하거나 접촉	용의자 - 관련자
A는 B에 알려지거나 보고되고, 기록된 것	Email 등록 - 네트워크 로그

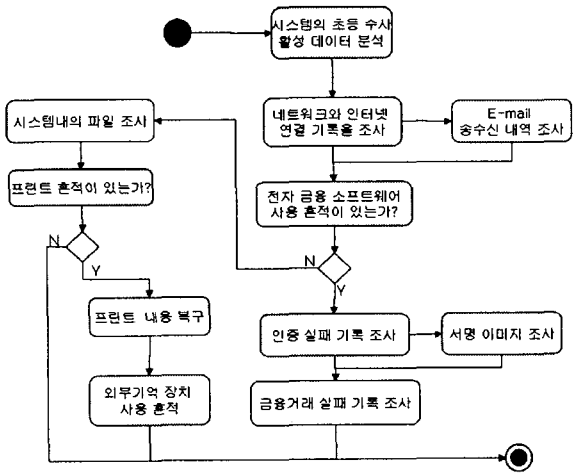
<표 2> 관계의 종류

UML의 클래스 다이어그램을 이용하여 클래스를 표현하고 그 내부 속성 값과 클래스들의 관계를 화살표와 실선으로 표기하였다[7].

III.디지털 범죄 수사 절차 모델링

앞에서 사건 도메인을 모델링하는 방법에 대해서 논의해 보았다. 사건 도메인 모델링만으로는 디지털 범죄 수사를 논리적이고 체계적으로 진행하기에는 다소 부족하다. 사건 모델은 수사해야 하는 범위만을 나타내기 때문에 실제 수사를 진행해야 하는 방법론에 대해서도 모델링 과정이 필요하다. 수사 절차 모델링은 조사해야 할 사항과 순서를 구조화하는 작업이며, 모델링된 수사 절차 모델은 사건 도메인에서 하나의 클래스 혹은 클래스 사이의 수사 진행에 적용될 수 있다.

디지털 범죄를 수사하기에 앞서 조사해야 할 내용을 범죄의 유형별로 분류하고, 그 유형에 따라서 반드시 정밀 수사를 해야 하는 사항들을 체크리스트로 만들어서 그 순서와 내용에 따라서 수사를 진행해야 한다. 이러한 내용은 Electronic Crime Scene Investigation: A Guide for Law Enforcement의 체크리스트에서 언급하고 있다[6]. 이러한 수사 절차를 활동 다이어그램 혹은 순차 다이어그램, 협력 다이어그램으로 나타낼 수 있다[5]. 협력 다이어그램은 공동 수사 또는 외부 전문가의 협조를 통한 수사가 필요할 때 협력관계를 표현하기에 적합한 다이어그램이다. 활동 다이어그램은 수사관이 단계별로 수행해야 할 수사 절차를 모델링하는 데 적합하며, 순차 다이어그램은 시간 순서에 따른 절차 모델링이나 수사 과정 중 발견된 증거와 이벤트들을 시간 순서에 따라 시나리오를 재구성하는데 적합하다.

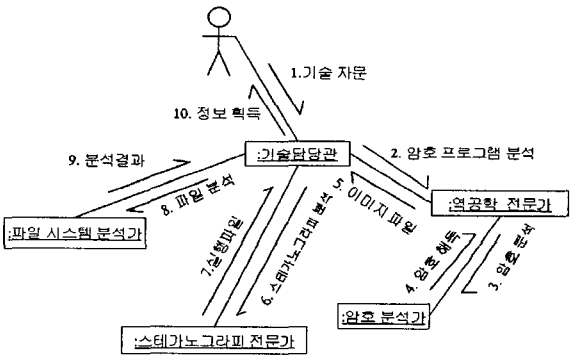


<그림 2> 금융사기 사건 수사 절차 모델링

다음 <그림 2>은 활동 다이어그램을 사용하여 금융사기 사건에 대한 수사 절차를 모델링한 것이다. 각 항목들은 Electronic Crime Scene Investigation: A Guide for Law Enforcement에서 권고하는 금융사기 사건을 수사하는 과정 중 정

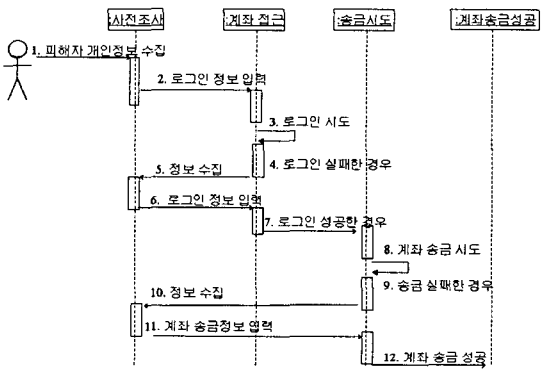
밀 분석과 세심한 조사가 필요한 사항들이다[6].

- 서명 이미지
- e-mail
- 인터넷 사용 기록
- 프린트 기록
- 금융 관련 문서
- 전자금융 조회 소프트웨어
- 전자금융 인증 실패 기록
- 금융거래 실패 기록



<그림 3> 협력 수사 절차 모델링

위의 <그림 3>는 스테가노그라피 기술 혹은 암호 프로그램을 사용하여 용의자가 자신에게 불리한 증거를 은닉하였을 때, 수사관이 암호 전문가, 역공학 전문가 등 외부의 기술 전문가와 협력수사를 진행하는 절차를 모델링한 것이다.



<그림 4> 금융사기 사건 시나리오

위의 <그림 4>는 금융사기 사건 조사와 관련하여 획득된 정보를 바탕으로 시간의 흐름 순으로 시나리오를 재구성하는 방법으로 시퀀스 다이어그램을 사용하였다.

본 장에서는 간단한 수사절차를 모델링해 보았다. 하지만 실제 현장의 디지털 범죄는 이보다 훨씬 더 복잡할 것이다. 그리고 디지털 범죄를 수사하기 위해서는 종합적인 디지털 포렌식 기술이 필요하며 상당한 전문지식을 요구한다. 현실적으로 이러한 조건을 만족하는 수사관은 그리 많지 않다. 따라서 각 분야마다 전문가가 필요한 실정이다. 이와 같이 복잡하고 전문 기술이 필요한 디지털 범죄 수사의 특성 때문에, 디지털 범죄 수사 절차를 모델링하는 것은 반드시 필요하다고 생각된다.

IV. 결론

본고에서 UML을 이용하여 디지털 포렌식 수사를 사건 도메인과 수사절차로 분류하여 모델링해 보았다. 이와 같은 모델링이 중요한 이유는 다음과 같다.

첫째, 대규모 사건 발생 시 수사관 한 사람이 사건의 모든 측면을 이해하고 파악하기는 매우 힘들다 따라서 디지털 범죄 수사를 모델링하여 범죄수사 체계를 추상화하고 구조적으로 만들어 한눈에 파악할 수 있도록 해야 한다.

둘째, 수사 진행 계획을 변경해야 할 경우, 즉 디지털 범죄 수사 과정 중 새로운 증거나 정보 등을 발견하였을 때 재빨리 조사 진행 방향을 수정하거나 조정해야 할 필요가 있다. 이러한 경우 현재 조사 상황을 세밀히 이해해야 하는데, 시각적으로 모델링된 디지털 범죄 수사 체계는 반드시 필요하다.

셋째, 비록 단순한 디지털 범죄 사건이라 할지라도, 사건에 대한 시각적 모델은 수사 절차를 논의하고 진행하는데 필요한 '핵심내용'을 제공한다.

결론적으로 중요한 점은 디지털 범죄 수사 능력을 확보하기 위해서는 디지털 포렌식 기술

개발과 더불어 디지털 포렌식 정책과 디지털 범죄 수사 절차에 대한 연구도 함께 병행해야 한다는 것이다. 그러한 연구 방법의 일환으로 본고에서 제시한 디지털 범죄 사건 모델링 방법이 있으며, 디지털 범죄 수사 체계를 확립하기 위해서는 반드시 필요하다고 생각된다.

[참고문헌]

[1] Graddy Booch and James Rumbaugh and Ivar Jacobson, *"The Unified Modeling Language User Guide"*, Addison Wesley, 1999.

[2] UML, http://www.terms.co.kr/UML.htm

[3] A. Chris Bogen and David A. Dampier, *"Unifying Computer Forensics Modeling Approaches: A Software Engineering Perspective"*, SADFE2005, Taipei, Taiwan, November, 2005, pp. 1.

[4] 전병선, *"J2EE Enterprise System 객체지향 개발 방법론"*, Youngjin.com, 2004, pp. 30-42

[5] Graddy Booch and James Rumbaugh and Ivar Jacobson, *"The Unified Modeling language Reference Manual"*, Addison Wesley, 1999

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

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

[8] G. Palmer, *"A Road Map for Digital Forensic Research,"* Utica, New York, technical report DTR-T001-0, 2001.

[9] Robert A. Maksimchuk and Eric J. Naiburg, *"UML for Mere Mortals"*, Addison Wesley, 2005

[10] 강동식, *"사이버테러 대응 공동 심포지움"*, 디지털 타임스, 2005년 10월 13일,

[11] 성연광, *"'디지털 증거물' 실효위한 법제화 '시급'"*, 머니투데이(경제신문), 2005년 10월 12일

[12] 황현욱, 김민수, 노봉남, 임재명, *"컴퓨터 포렌식스: 시스템 포렌식스 동향과 기술"*, 정보보호학회지, 2003년 8월