국내 Computer Forensics의 연구동향과 발전방향

김 종 섭* · 김 귀 남**

요 약

전자정부 실현과 전자상거래의 활성화로 전자거래의 비중이 커지면서 전자거래를 둘러싼 법적 분쟁과 컴퓨터범죄도 날로 증가하고 있다. Computer Forensics는 이러한 법적 분쟁의 해결을 위하여 필수적인 디지털증거를 수집, 보전, 분석, 보고하기 위한 방법론으로 등장하였다.

본 논문에서는 Computer Forensics의 연구동향을 분석하고 이제 본격적인 연구에 들어간 국내 Computer Forensics의 발전방향을 제시하고자 한다. Computer Forensics의 과학적인 연구와 법제도의 정비, 국내 실정에 맞는 기술개발을 통하여 안전한 전자거래의 기반을 구축하는데 기여할 것으로 기대한다.

Trends and Development of Computer Forensics in Korea

Jong Seob Kim* · Kuinam J. Kim**

ABSTRACT

The legal dispute of electronic commerce and computer crimes are increasing because the electronic services like e-government and e-commerce are now widely used. Computer Forensics becomes the method for recovery, preservation, analysis and report regarding digital evidence essential to resolve the legal dispute and computer crime.

In this paper, the developmental process of Computer Forensics is discussed. It is intended to elicit constructive discussion regarding the domestic Computer Forensics. And this discussion will be of help to establish the secure e-business and e-government services in the field of the research, legal system and technical skill of domestic Computer Forensics.

* 국립과학수사연구소

** 경기대학교 정보보호기술공학과

1. 서 론

Computer Forensics는 컴퓨터 사용이 일반화되면서 법과학의 새로운 분야로 발전하기 시작하였다. 기존의 법과학(Forensic Science)이 대부분 유형의 증거물의 형상과 성질을 과학적으로 분석하거나 가시적인 범죄현장에 남겨진 범죄흔적을 연구대상으로 하는데 반하여[20], Computer Forensics는 눈으로 직접 볼 수 없는 디지털 형태로 존재하는 데이터를 연구대상으로 하며, 범죄현장 또한 눈에 보이지 않는 컴퓨터 시스템 내부이거나 인터넷과 같은 사이버공간이다. 따라서 기존의 법과학에서 연구하는 방법론을 그대로 Computer Forensics에 적용할 수 없는 특성을 가지고 있어 새로운 법과학 분야로 연구가 시작되었다.

Computer Forensics의 개념은 아직 명확하게 정립되지 않았으며 접근방법이나 관심분야에 따라 조금씩 차이가 있으며, 용어도 Computer Forensics[10, 15, 17, 18, 21, 24]을 비롯하여 Forensic Computing[12], Cyber Forensics[2], Network Forensics[11, 14] 등 다양한 용어가 사용되고 있다. 일반적으로 Computer Forensics는 '컴퓨터 등 정보처리능력을 가진 장치를 매개로 하여 이루어지는 각종 행위에 대한 사실관계를 확정하거나 증명하기 위하여 필요로 하는 정보를 수집, 분석, 보존하거나 법정에 제시하는 제반 행위'[17], '고도의 하이테크 범죄인 컴퓨터 범죄와 관련된 증거의 적법한 수집, 분석, 관리를 통한 증거자료 수집을 목적으로 하는 과학적 수사기법'[24], '정보처리 기기를 통하여 이루어지는 각종행위에 대한 사실관계를 확정하거나 증명하기 위해 행하는 각종 절차와 방법'[23], '컴퓨터에 내장된 자료의 보관, 추출, 문서화, 해독 및 분석을 하는 일련의 과정'[24]이라고 정의되고 있다. 여기서 Computer Forensics를 '행위'나 '기법' 또는 '방법'이나 '절차'로 볼 것인가 아니면 '과학'으로 볼 것인가에 대한 검토가 진지하게 논의되어야 할 것이다.

Computer Forensics에 관심을 갖는 전문가 그룹은 다양하며 응용 분야도 넓다. 최근 발생한 인터넷 마비사태와 같은 사이버테러 사건의 사고원인조사 및 긴급대응이나 전자거래의 허점을 악용하는 금융범죄 수사 등 전자정부 실현과 전자거래의 일상화에 따라 늘어나는 사이버거래에 따른 법적분쟁을 해결하기 위한 열쇠가 되는 증거수집에 광범위하게 응용된다. Computer Forensics에 관심을 갖는 전문가 그룹은 컴퓨터범죄나 사이버범죄를 대응하는 수사정보기관과 법원 등 국가기관, CERT 팀이나 정보공유분석 센터와 같은 침해사고 대응기관, 그리고 Computer Forensics 기반기술을 연구하는 연구소와 대학, 기반기술을 바탕으로 응용기술과 포렌식 도구를 개발하는 기업, 기반기술과 응용기술을 적용하여 포렌식 분석, 시험, 감정을 전담하는 감정기관 등이 있다.

본 논문에서는 지금까지 실무현장에서 '수사기법'이나 '분석 방법/절차'에 초점을 맞추어 연구되어 오던 Computer Forensics에 대한 연구방향을 바꾸어 Computer Forensics가 독립된 '과학'으로 연구되어야 할 필요성과 국내 Computer Forensics의 발전방향에 대하여 고찰하고자 한다. 본 논문의 구성은 다음과 같다. 제2장에서는 Computer Forensics의 성격과 연구현황을 살펴보고, 제3장에서는 국내 Computer Forensics의 발전방향을 제시하며, 제4장에서는 결론을 맺기로 한다.

2. Computer Forensics의 연구동향

2.1 Computer Forensics의 성격과 연구대상

2.1.1 법과학과 Computer Forensics의 성격

Computer Forensics(Computer Forensic Sci-

ence)는 법과학(Forensic Science)의 한 분과이다. 법과학은 범죄수사나 재판상의 증거물에 대한 분석과 실험에 자연과학의 이론과 기술을 응용하는 학문으로서 법정과학이라고 일컬어지기도 한다[20]. 법과학은 발생 가능한 모든 범죄현상에 대응하기 위하여 광범위한 기초과학분야를 기반으로 다양한 분야의 응용과학 이론과 기술이 활용되므로 그 분야가 매우 넓다.

법과학은 국가마다 분류가 다르지만 크게 법의학과 좁은 의미의 법과학으로 분류한다. 법의학은 사체에 대한 사인규명 등에 관한 의학적 증명을 하는 법의병리학 분야와 범죄에 관한 심리적, 정신의학적 분야를 다루는 법의정신의학 분야로 나눈다. 그리고 좁은 의미의 법과학은 범죄현장에서 수집한 증거물을 과학적으로 분석하는 분야로서 법생물학, 법화학, 법이공학, 기타 특수과학 분야로 분류하는데[20], Computer Forensics는 좁은 의미의 법과학 분야로 분류할 수 있다. Computer Forensics는 디지털증거의 법률문제를 해결하기 위한 과학과 기술을 응용하는 분야로서 과학과 법률의 통합체라고 할 수 있다[12, 9].

다만 기존의 법과학(Forensic Science)이 대부분 유형의 증거물의 형상과 성질을 과학적으로 분석하거나 가시적인 범죄현장에 남겨진 범죄 흔적을 연구대상으로 하는데 반하여, Computer Forensics는 눈으로 직접 볼 수 없는 디지털 형태로 존재하는 데이터를 연구대상으로 하며, 범죄현장 또한 눈에 보이지 않는 컴퓨터 시스템 내부이거나 인터넷과 같은 사이버공간이라는 점에서 기존의 법과학과 다른 특성이 있고, 기존의 법과학 연구 방법론을 그대로 Computer Forensics에 적용할 수 없는 특성을 가지고 있다.

Computer Forensics가 학문이냐 단순한 기술 또는 기능에 불과한 것이냐에 대한 논의는 법과학이 학문이냐 기술이냐에 관한 논의와 같은 연장선에 있는 문제이다. 대부분의 응용 과학이 출발 초기에 학문성에 대한 회의론이 많이 대두되었으나 발전을 거듭하면서 단순한 응용 기술의 차원을 넘어 학문성을 인정받는 경우가 대부분이다. Computer Forensics도 법과학과 함께 응용기술의 차원을 넘어서는 과학의 한 영역으로 자리 잡을 수 있도록 체계적인 연구가 요망되는 분야이다.

2.1.2 Computer Forensics의 응용영역과 컴퓨터범죄 수사

Computer Forensics에 대한 연구가 본격적으로 시작된 것은 컴퓨터범죄가 사회문제로 대두되면서부터이다. 미국의 경우에는 1980년대 중반부터 법집행기관과 군수사기관에서 Computer Forensics가 하이테크 수사와 정보활동에 많이 활용되어 왔으며 민간부문에서는 상대적으로 새로운 분야이다[2]. 우리나라에서도 역시 해킹사건이나 바이러스 유포사건을 수사하는 컴퓨터범죄 수사기관에서 제일 먼저 Computer Forensics에 대한 연구가 시작되었고 인터넷을 이용한 전자상거래의 규모가 커지면서 점차 민간 기업과 연구소에서 Computer Forensics에 대한 연구를 시작하였다.

Computer Forensics가 컴퓨터범죄 수사 분야에서 가장 많이 이용되고 있고 민간 기업에서 이루어진 Computer Forensics 연구가 국가 수사기관에서 필요로 하는 수사용 도구를 개발하는 수준에서 진행되어 온 것은 사실이나, Computer Forensics의 적용분야가 이에 한정되지 않는다.

Computer Forensics에 관심을 갖는 전문가 그룹은 다양하며 이를 응용하는 분야도 넓다. 먼저 Computer Forensics 관련 전문가 그룹은 컴퓨터범죄나 사이버범죄를 대응하는 수사정보기관과 법원 등 국가기관, CERT 팀이나 정보공유분석 센터와 같은 침해사고 대응기관, 그리고 Com-

puter Forensics 기반기술을 연구하는 연구소와 대학, 기반기술을 바탕으로 응용 기술과 포렌식 도구를 개발하는 기업, 기반기술과 응용 기술을 적용하여 포렌식 분석, 시험, 감정을 전담하는 감정기관 등으로 분류할 수 있다.

Computer Forensics 응용 분야는 컴퓨터범죄 수사와 사이버테러 대응을 위한 증거수집과 분석 등 범죄감식/감정업무, 침해사고의 분석과 정보공유 및 복구 등 침해사고 대응 업무와 같은 직접적인 응용 분야는 물론이고, 기업의 전자거래에 수반한 전자세금계산서 발급시스템이나 전자정부에서 발급하는 각종 민원접수와 증명서 발급을 위한 전자증명 발급 시스템 등도 응용이 가능한 분야이다. 또한 정부기록물의 관리나 회계장부의 보관 등에도 Computer Forensics 관련 기술들이 응용될 수 있을 것이다. 이와 같은 신분증명이나 증빙서류의 전자적 처리나 보존을 포함하여 전자거래에서 발생할 수 있는 법적 분쟁에 대응하기 위하여 구축되는 '디지털증거 관리시스템(DEMS : Digital Evidence Management System)은 Computer Forensics 관련 기술을 포괄적으로 응용 하여야 구축될 수 있을 것이다[17].

2.1.3 Computer Forensics의 연구대상과 디지털증거

컴퓨터 관련 증거는 컴퓨터와 그 주변장치, 운영 매뉴얼과 같은 책자나 서류, 각종 출력물과 모니터의 영상 출력, 자기테이프와 천공카드 등과 같은 다양한 형태로 존재한다. 그러나 Computer Forensics에서 가장 중요한 연구대상이 되는 것은 무엇보다도 디지털증거이다. 디지털증거(Digital Evidence)는 범죄와 관련하여 만들어지거나 범죄사실과 범죄피해자 또는 범죄사실과 범죄용의자를 연결시키는데 사용될 수 있는 모든 디지털 데이터를 말한다[5].

디지털 데이터는 0과 1의 조합으로 다양한 처리방식과 많은 종류의 매체에 존재한다. 컴퓨터 시스템과 네트워크 장비 그리고 저장매체, 각종 정보통신기기, 디지털 영상장치와 디지털 음성장치, 인터넷을 통하여 작동되는 각종 가전제품 등에 이르기까지 디지털 데이터를 사용하는 기기는 다양하며, 데이터 처리방식도 전자적 방식과 자기적 방식 또는 광방식이나 바이오 방식 등 기술발달에 따라 새로운 데이터 처리방식들이 속속 등장하고 있다. 그러나 이러한 다양한 존재방식에도 불구하고 디지털 데이터는 일정한 속성을 갖고 있어 이를 증거로 사용하기 위해서는 특별한 연구와 관리를 필요로 한다.

Computer Forensics의 연구대상을 이러한 디지털증거로 한정할 것인가 또는 가시적인 컴퓨터나 매체 자체도 포함할 것인가는 필요와 입장에 따라 달라질 것이다. 그러나 Computer Forensics의 연구대상을 디지털증거에 한정한다는 것이 디지털증거를 담고 있는 매체의 형상이나 존재 자체가 증거물로서 의미가 없다거나 디지털증거의 확보와 함께 매체를 증거로 사용해야 할 필요를 부정하는 것은 아니다. 다만 Computer Forensics의 연구 초점을 디지털증거에 집중시켜 지금까지 경험하지 못한 새로운 형태인 디지털증거에 대한 과학적 이론을 충분히 제공함으로써 급속하게 디지털 형태로 변화되고 있는 정보통신 환경에 부응하자는 것이다.

최근 대부분의 컴퓨터시스템이 네트워크를 통해 서로 연결되어 있고 e-banking이나 e-trading과 같은 전자거래가 늘면서 컴퓨터 시스템이나 저장매체 자체의 압수는 서비스 중단으로 인한 큰 손실을 발생시킬 가능성이 있어, 수사로 얻게 되는 이익과 비교해야할 필요성이 높아지고 있다. 따라서 디지털증거의 내용이 증거로서 가치가 있고 매체 자체는 증거로서 큰 의미가 없는 경우와 디지털정보가 매체에 결합된 상태가 동시에 증거로서의 가치가 있는 경우로 나누어 연구할 필요가 있다.

여기서 디지털증거의 내용이란 분석대상 데이터의 0과 1의 조합이 '어떤 순서와 크기로 존재하고 있었는가'와 이러한 존재 순서와 크기가 '언제 어떻게 바뀌었는가[혹은 바뀌지 않은 사실]' 그리고 만일 내용이 바뀌었다면 '언제 어떤 이유로 어떻게 바뀌었는가'에 대한 정보를 말한다. Computer Forensics의 연구대상이 다른 법과학 분야와 가장 큰 차이점을 나타내는 것은 바로 이러한 디지털증거의 속성에 기인한다.

디지털증거는 매체 의존적인 속성과 매체 독립적인 속성을 동시에 갖고 있다. 디지털증거는 매체 없이 스스로 존재하지 못한다는 점에서 매체 의존적 속성을 갖고 있다. 반면에 디지털증거는 어떤 매체에 옮겨 담아도 동일한 의미 내용을 갖는다는 점에서 매체 독립적 속성을 갖는다. 이는 마치 물이 어떤 용기에 담기느냐에 관계없이 동일한 양과 특성을 갖는 것과 같은 원리이다.

디지털증거의 매체 독립적 속성으로 말미암아 증거법의 일반원칙에서 요구하는 증거의 원본성에 관한 문제가 제기된다. 디지털증거는 복사를 하여도 원본과 복사본의 질적이 차이가 없다. 따라서 디지털증거의 원본성을 어떻게 정의할 것인가, 증거법의 요구사항은 어떻게 충족할 수 있을 것인가 하는 문제가 Computer Forensics의 중요한 연구 과제로 등장하게 된다. 물론 현실 문제로 돌아오면 디지털증거의 원본성에 대한 궁극적인 해법은 결국 사회 공동체의 타협의 산물인 법률의 규정이나 관행적 합리성에서 찾을 수밖에 없을 것이다. 이러한 현실적인 측면을 너무 크게 보면 Computer Forensics를 순수 과학으로서 접근하기가 어려워지고 기능적 방법론으로 접근하게 되어 Computer Forensics의 과학적 연구에 한계점으로 작용하게 된다.

2.2 Computer Forensics의 연구현황

Computer Forensics는 영미법계 국가를 중심으로 '컴퓨터에 내장된 자료의 보관, 추출, 문서화, 해독 및 분석을 하는 일련의 과정'이나 '고도의 하이테크 범죄인 컴퓨터 범죄와 관련된 증거의 적법한 수집, 분석, 관리를 통한 증거자료 수집을 목적으로 하는 과학적 수사기법'라는 개념을 가지고 비교적 최근에 연구하기 시작한 분야이다[24].

국내에서도 수사기관과 일부 정보보호업체에서 비슷한 개념으로 연구가 진행되고 있으며, 대학에서는 '컴퓨터범죄 수사기법'이라는 명칭의 강좌나(경기대학교), 'Computer Forensic(컴퓨터 범죄 분석학)'이라는 명칭의 강좌(한국정보통신대학원대학교)가 열리고 있다. 경기대학교의 경우에는 일반대학원 정보보호기술공학과의 정식 교과목으로 편성되어 있고, 한국정보통신대학원대학교에서는 뉴질랜드 Otago 대학의 Henry B. Wolfe 교수를 초청하여 단기 강좌(10시간)를 개설한 바 있다. Henry B. Wolfe 교수의 강좌 내용은 다음과 같다[6].

- Lecture 1 : Introduction to Computer Forensic, Forensic Evidence in Computing.
- Lecture 2 : Legal Precedents for Electronic Evidence Gathering Methods, Understanding Hard Disk Geometry, Acquisition, Incident Response.
- Lecture 3 : Preservation of Evidence, Understanding Backup Options.
- Lecture 4 : Specialized Online-Offline Storage, PDA's, Photocopiers, Fax, Cell-phones, Pagers.
- Lecture 5 : Physical Storage of Evidentiary Copies, System Acquisition - Seizure, Working with the Original Evidence.
- Lecture 6 : Investigating What's on the PC, Surveillance Techniques.
- Lecture 7 : Encountering Encryption/Stega-

nography, Analysis and Reporting, Findings Tips for the Expert Witness.

- Lecture 8 : Network Forensics, Conventional Forensics, Tools for Forensic Science.
- Lecture 9 : Issue of Forensic Credentials, Summary.

'컴퓨터나 다른 정보저장장치로부터 증거를 잡아내기 위한 새로운 조사기법'에 관한 내용을 다루고 있는데[6], 영미법계 국가인 뉴질랜드나 미국, 영국 등지에서 통용되는 Computer Forensics 원리가 대륙법계 국가인 우리나라에 그대로 적용할 수 없다는 문제점을 제외하면 Computer Forensics의 개념을 파악하는 데는 도움이 될 것이다.

이미 설명한 바와 같이 Computer Forensics 연구가 본격적으로 시작된 것은 컴퓨터범죄가 사회문제로 대두되면서부터이다. 자연스럽게 Computer Forensics에 관한 연구는 주로 '컴퓨터범죄수사기법' 또는 '컴퓨터범죄분석절차'라는 개념으로 컴퓨터범죄 증거의 수집과 분석 및 보전에 관련된 기술적 방법론으로 흘러가고 있다. 그리하여 지금까지 발표된 Computer Forensics의 연구내용은 'Computer Forensics 유형과 절차', 'Computer Forensics 기술과 도구'에 대한 개념적 내용에 그치고 있다[24].

2.2.1 Computer Forensics의 유형

Computer Forensics 유형은 디스크 포렌식스(Disk Forensics), 네트워크 포렌식스(Network Forensics), 인터넷 포렌식스(Internet or WWW Forensics), 전자우편 포렌식스(E-mail Forensics), 원시코드 포렌식스(Source Code Forensics), 휴대 정보기기 포렌식스(Mobile Device Forensics), 멀티미디어 포렌식스(Multimedia Forensics) 등으로 분류하고 있다[18, 19, 21, 23].

디스크 포렌식스(Disk Forensics)는 정보기기의 기억장치에 저장되어 있는 데이터에서 어떤 사실을 입증하기 위하여 필요한 증거를 추출하고, 분석하여, 보고하는 일련의 과정을 연구 대상으로 하는 것을 말한다[21]. 디스크 포렌식스의 연구 초점은 저장매체의 속성과 저장방식, 디지털 데이터의 무결성의 확보문제, 그리고 매체의 보관과정에 대한 보증문제(Chain of Custody)가 될 것이다. 매체를 확보[압수]하지 않고 매체 내에 있는 디지털 정보만을 추출하여 증거로 사용할 수 있는지, 이런 경우에 어떤 절차와 방법을 채택해야 할 것인지에 대한 연구는 컴퓨터 사용 환경이 서버-클라이언트 환경으로 급속히 변화되어 가는 최근 경향을 볼 때 매우 유용한 연구과제가 된다.

네트워크 포렌식스(Network Forensics)는 네트워크 정보(Network Traffic Flows)와 전송 데이터(Contents)를 수집하여 필요한 증거를 추출하고 분석하여 보고하는 과정을 연구 대상으로 한다. 네트워크 포렌식스에서는 필수적으로 네트워크 정보를 수집하는 도구(Network Forensics Analysis Tool[NFAT])를 사용하게 되는데 이들이 사용자들의 통신비밀을 침해하는 결과를 초래하게 되므로 주의를 요한다[11, 14]. 따라서 네트워크 포렌식스의 연구 초점은 전송되고 있는 데이터에 대한 실시간 정보수집과 분석이 이루어지므로 네트워크 사용자들의 프라이버시의 침해를 최소화 하면서 목적을 달성할 것인가의 문제와 네트워크 포렌식스에서 얻어지는 증거가 독립해서 증거가치를 갖기 위해서는 어떤 절차와 방법을 거쳐야 할 것인가 하는 문제가 중심이 된다.

인터넷 포렌식스(Internet or WWW Forensics)와 전자우편 포렌식스(E-mail Forensics)는 네트워크 포렌식스의 영역에서 크게 벗어나지 않는다. 경우에 따라서는 디스크 포렌식스의 영역에 해당하는 문제와 중복되는 경우가 있을 것이다. 다만 인터넷이나 웹 포렌식스의 경우에는

다소 개방적인 시스템을 대상으로 하는 반면, 전자우편 포렌식스는 우편물에 대한 프라이버시 보호가 특별히 요구되므로 주의를 요한다.

원시코드 포렌식스(Source Code Forensics)는 컴퓨터 프로그램의 원시코드를 분석하여 저작자를 확인하는 과정을 연구 대상으로 하며, 휴대정보기기 포렌식스(Mobile Device Forensics)는 휴대전화나 전자수첩과 PDA와 같은 휴대용 정보기기와 관련된 디지털 데이터를 수집, 분석하는 과정을 연구 대상으로 하며, 멀티미디어 포렌식스(Multimedia Forensics)는 디지털 형태의 사진, 비디오, 오디오 등을 증거자료로 수집, 분석하는 과정을 연구 대상으로 한다[21].

지금까지 논의된 Computer Forensics 유형들은 주로 매체를 중심으로 분류한 것이다. 그러나 매체 못지않게 중요한 요소가 운영체제의 차이이다. 일반적으로 개인용 PC에서 가장 많이 사용되는 Windows 계열의 운영체제와 주로 서버용으로 사용되는 UNIX 계열의 운영체계는 파일구조나 저장방식, 다중사용 여부 등에 차이가 많으므로 이러한 운영체제를 중심으로 Computer Forensics 유형을 분류하는 것도 의미가 있을 것이다. 그리고 Computer Forensics에서 분석 대상 시스템이 가동 중에 있느냐 또는 정지 중에 있느냐에 따라 분석 유형을 Live Analysis와 Offline Analysis로 분류하기도 한다[8]. 네트워크 포렌식스는 대부분 Live Analysis에 해당되는데, Offline Analysis에 비하여 증명력 확보에 어려움이 많다는 사실을 유념해야 한다.

2.2.2 Computer Forensics의 절차

(1) 준비단계

Computer Forensics의 절차는 크게 준비단계, 획득단계, 분석단계, 보고단계로 나눌 수 있다[21, 18]. 이러한 절차는 증거의 생명주기(Life Cycle of Digital Evidence)와 관련을 갖고 있다. 예를 들면 어떤 사건이 발생하여 수사관이 수사에 착수하면 범행의 내용과 범죄자를 확정하기 위하여 증거수집에 들어가게 된다. 증거수집을 위해서는 범죄현장의 상황은 어떠한지, 피해시스템의 상태는 어떠한지, Online인지 Offline인지, 휴대할 포렌식스 도구는 어떤 것이며 장비는 무엇인지, 획득한 증거는 어떻게 운반하고 어떻게 보관할 것인지 등에 대한 사전준비가 반드시 필요하다.

(2) 수집 및 보존 단계

수집단계에서는 먼저 대상 시스템의 현존 상태를 유지(Freezing the Scene, the System, and the Data)하고, 왜곡이나 손상 없이 시스템의 상태를 정확히 기술(Snapshot)하는 것이 무엇보다 중요하다.[4] 이러한 과정을 중요시 하는 이유는 여기서 얻어진 자료가 사건이 종결될 때까지 증거보전의 연속성(Chain of Custody)을 평가하는 기준점이 되고 디지털증거의 무결성의 기준점이 되기 때문이다. 만일 사건현장이나 피해시스템에 최초로 접근하는 사람이 이와 같은 처리를 소홀히 하게 되면 수집된 디지털증거의 무결성이나 Chain of Custody를 아무리 잘 관리하였다 해도 증거가치는 현저히 떨어지게 된다.

현장과 시스템에 대한 Snapshot이 완성되면, 시스템을 Online으로 유지할 것인지 Offline으로 바꿀 것인지를 결정하여야 한다. Online 상태에서 증거수집을 한다면 반드시 네트워크 상태와 시스템 접속자에 대한 감시를 하면서 작업을 수행하여 만일에 있을 공격자의 파괴행위에 대비해야 한다. Offline 상태에서도 범인이 숨겨 놓았을지도 모르는 Virus나 Trap에 당하지 않도록 주의해야 한다.

증거수집은 휘발성이 가장 강한 자료로부터 자료수집에 들어간다. 수집된 자료는 필요에 따라 디스크 복사를 하거나 파일단위로 해쉬값을 생성하고, 복사본이나 해쉬값에 대하여 관련자의 확인을 얻어야 차후 무결성에 대한 다툼을 최소

화할 수 있다. 현장에서 이루어진 모든 절차와 행동을 기록하여 보존하는 것은 수집단계에서부터 보고단계에 이르기까지 증거의 생명주기(Life Cycle of Digital Evidence) 전과정에서 이루어져야 한다. 참고로 UNIX에서는 script 명령어를 사용하면 시스템의 작업과정이 모두 기록되므로 쉽게 사용할 수 있다.

수집단계에서 반드시 체크해야 할 사항은 시스템의 순결성의 점검이다. 수사관이나 포렌식 전문가가 현장에 최초로 임장한 시점을 기준으로 증거수집 이후에는 무결성이 요구되지만, 증거수집 이전에는 컴퓨터 시스템의 순결성이 요구된다. 수집된 증거가 아무리 무결한 자료라고 해도 그 자료가 수집되기 이전에 이미 신뢰할 수 없을 정도로 시스템이 침해를 당하였거나, 그 시스템에서 얻어진 로그 자료나 기타 범행을 입증할만한 자료가 심각하게 변경되었다는 사실이 확인되면 그 자료의 증거가치는 현저히 떨어지게 된다[19]. 최악의 경우에는 시스템을 정지시키고 신뢰할만한 시스템으로 부팅한 후 피해시스템을 마운트해서 점검을 해야 한다[4].

수집된 증거물의 이동과 보관은 증거보전의 연속성(Chain of Custody)과 증거자료의 무결성(Integrity) 보장에 중점을 둔다. 증거보전의 연속성(Chain of Custody)을 확보하기 위해서는 수집된 증거물의 초기상태를 정확히 기술하여야 하고, 라벨을 부착하고 반출입사항을 기재하여야 한다. 기록항목은 증거수집 주체와 참여자, 증거수집 시간과 장소 및 방법, 대상증거물의 소유/점유/관리 권원, 증거물 인수인계자와 사유 등이 기록될 수 있도록 하여야 한다[24]. 디지털 증거의 무결성 확보를 위해서는 해쉬값을 확보하여 검증하는 방법이 가장 선호되고 있다[21, 24].

(3) 분석단계

분석단계는 수집된 증거를 대상으로 시스템이나 응용 서비스의 접근/사용 기록의 분석, 파일의 생성/접근/변경 시간(MAC Time) 분석, 숨겨진 자료의 검색, 삭제된 파일의 복구, 암호 우회 및 분석 등을 통하여 사건의 실체를 파악하고 사건에 이용된 시스템의 인터넷주소, 라우팅 경로, 시스템관리자 정보, 사용자 정보 등을 추출하고 증명하는 절차를 말한다[21, 23, 24].

증거분석은 어떤 형태로든 증거물에 변경을 가하게 된다. 분석과정에서 발생할 수 있는 증거의 변경을 최소화할 수 있는 방책들이 마련되어야 하며, 작업과정에 대한 명확한 기록(Document)이 필요하다. 미디어를 증거물로 확보한 경우에는 동일 제품의 미디어에 복사본(Imaging Copy)을 만들어 분석하도록 권장하고 있다. 미디어 없이 디지털 데이터만을 증거로 확보한 경우에도 수집된 최초 데이터는 안전한 증거보존시스템에 보관하고 반드시 백업본(Backup)을 만들어 분석하는 습관을 들여야 한다.

증거분석에 사용되는 시스템은 사전에 준비해야 한다. 시스템의 하드웨어 사양과 운영체제, 분석에 사용되는 응용 프로그램, 분석에 제공되는 서비스 등에 대한 명세를 기록하고, 시스템의 주요 파일이나 프로그램에 대한 해쉬값 등을 준비하여 시작과 종료 또는 중요한 작업 전환 시에는 초기값의 변화가 있었는지 확인하고, 만일 변화가 있으면 그 원인을 분석하여 기록에 남겨야 한다. Unix용 증거분석 시스템을 구성할 때에 운영체제는 Linux의 사용이 권장되는데[22], 이는 소스가 공개되어 있어 분석 시스템에 대한 투명한 관리가 가능하고, 대부분의 파일 시스템을 지원하는 장점이 있다[22].

시스템이 단순히 범행의 도구로 이용된 경우에는 증거수집 이후에 증거가 변경되지 않았다는 사실을 증명하기 위하여 무결성 체크가 중요시 되지만, 분석 대상 시스템이 범죄의 대상이 되어 피해를 입은 경우에는 증거수집 이전에 시스템의 순결성을 체크하여야 한다. 예컨대 해킹

피해 시스템의 경우에는 공격자가 시스템의 커널을 변조하였다든지 분석용 도구로 사용하는 프로그램, 예를 들면 ls, ps, netstat, login, ifcinfig, dd, who, last 등 프로그램 차체가 변조되었을 경우에는 이러한 도구를 사용하여 나온 분석 결과가 신뢰할 수 없는 증거이므로 수집 이후에 아무리 무결성을 잘 유지하였다고 해도 증거로서의 가치는 현저히 떨어지는 것이다. 따라서 시스템 프로그램의 변조 여부를 확인하여야 하며, 가능하면 외부에서 순결성을 점검한 프로그램을 이용하여 분석을 하여야 한다[22].

개념적으로 분석단계는 수집단계를 거친 후 이루어지는 절차이지만 Online System에서 이루어지는 Live Analysis의 경우에는 수집단계와 분석단계가 동시에 진행되는 경우도 있다. 일반적으로 다중 이용 시스템 분석은 최고 관리자 권한(Root Permission)을 가지고 수행하게 되는데, 서비스를 계속하고 있는 시스템에서의 실시간 분석은 범죄와 관련 없는 이용자의 통신비밀을 침해하는 경우가 발생할 가능성이 있다. 따라서 현장에서 작업하는 수사관이나 침해사고 처리 담당자에게 정당한 법적 권한이 주어져 있는지 확인할 필요가 있다. 특히 형사사법절차에서는 강제권의 발동에 대한 법적 규제가 심하고 불법절차에 의하여 수집된 증거는 증거능력, 즉 증거로서의 자격이 박탈되는 결과를 초래할 수도 있으므로 증거법의 요구사항뿐만 아니라 헌법규정과 통신비밀 관련 법률의 규제사항에 대한 숙지가 필요하다[13].

분석단계에서 준수되어야 할 기본원칙이 있다. 첫째, 증거는 변경되지 않아야 하고, 둘째, 분석결과가 도출되는 모든 과정이 기록되어 검증될 수 있고 분석결과는 정확해야 하며, 셋째, 반복하거나 제3자가 분석해도 똑같은 결과가 나와야 한다. 이러한 기본 원리는 1995년경 미국 연방수사국(FBI)의 특별수사관(Spacial Agent)이었던 Mark Pollitt가 제시했던 것인데, 1999년 영국의 ACPO(Association of Chief Police Officers)에서 발표한 '컴퓨터 관련 증거 실무 가이드(Good Practice Guide for Computer Based Evidence)'에 반영되었고, 오늘날 디지털증거 분석과정도 준수되어야 할 기본원칙이며, 법원에서 증거조사를 할때 신뢰성 판단의 기준으로 삼을 수 있을 것이다[1, 12].

(4) 보고단계

보고단계에서는 수집된 증거를 분석하여 도출된 결과를 제공하는 단계이다. 보고는 분석결과를 통보하는 단순한 절차가 아니고 분석결과를 사용하는 주체의 요구사항에 맞추는 작업을 필요로 한다. 물론 이러한 작업은 분석결과에 영향을 주어서는 아니 되며 더욱이 증거를 변경하거나 왜곡되는 일이 없이 수집된 증거와 분석된 결과를 이해관계자가 이해하고 납득할 수 있는 형태로 표현하는 작업이어야 한다. 보고단계에서는 분석결과에 대한 평가가 자연스럽게 이루어지게 되는데, 증거 사용자의 요구사항을 분석결과에 반영하는 과정에서 분석이 부족한 부분이나 두개 이상의 분석절차에서 서로 상충되는 결과가 도출된 경우에는 추가 분석이나 재분석에 들어가야 한다.

법정에 증거로서 제시되는 경우에는 소송법규의 요구사항을 충족하여야 하는데, 일반적으로 소송법상의 감정서나 검증서(Statement of an Expert Opinion)에 준해서 보고하면 된다. 컴퓨터 시스템을 물리적으로 파괴한 범죄에서와 같이 컴퓨터 시스템이나 저장 매체 자체가 증거물로서 가치가 있는 경우에는 물리적 존재 차체를 증거물로 제시하여야 할 것이다. 그리고 컴퓨터 운영체계나 전자기록을 손괴/변경/은닉하여 업무를 방해한 경우에는 컴퓨터 시스템과 저장 매체보다는 지워지거나 변경/은닉된 디지털 데이터에 대한 변형된 사실과 정상적인 작동이 불가능한 사실을 나타내 주는 정보가 증거로서 더 큰

비중을 갖는다. 따라서 이러한 정보를 소송법규의 요구사항에 맞추어 보고하여야 한다.

보고방법은 법정에서 이해관계자들이 그 내용을 인식할 수 있는 화면이나 출력물에 의하여 제시될 수 있다. 여기서 디지털증거를 법정에 화면이나 출력물에 의하여 제출하였을 경우 원본성에 대한 문제가 제기될 수 있다. 미국의 경우에는 연방증거규칙(Federal Rules of Evidence)에서 서면, 녹음, 사진의 내용을 증명하기 위해서는 다른 법률의 규정이 있는 경우를 제외하고는 원본을 제출하도록 하는 소위 '최적증거법칙(The Best Evidence Rule)'을 규정하고 있다(Fed. R. Evid. 1002)[7]. 그러나 컴퓨터 기록물과 같이 원본 제시가 어려운 경우에는 '원본의 진정성이 의심되지 않고, 원본 대신 사본을 사용하는 것이 부당하지 않다'는 조건아래서 복사물의 사용을 허용하고 있다(Fed. R. Evid. 1003)[7]. 또한 기록물의 양이 방대하여 원본 제시가 어려운 경우에는 차트나 요약 또는 수식표 형식으로 제출할 수 있다(Fed. R. Evid. 1006)[7]. 우리나라에서도 범죄현장에서 수집한 디지털증거의 출력물을 수사기록에 첨부하여 제출하는 방식으로 디지털증거를 제시하는 것이 일반적인 실무관행이다.

증거는 최종적으로 법원의 판결에 의하여 그 가치를 평가 받게 된다. 법원에서 증거를 평가할 때에는 두 가지 관점에서 검토하는데, 하나는 증거능력에 관한 것이고 다른 하나는 증명력에 관한 것이다. 증거능력은 증거가 법원에서 증거로서 받아들일 수 있는 자격이 있는가에 대한 허용성의 문제이고, 증명력은 법원이 사실 판단에 채택된 증거가 얼마나 가치가 있는가에 대한 신용성의 문제이다. 증거능력이 없는 증거를 법정에 제시하여 증거조사를 하게 되면 잘못된 예단을 형성할 수 있으므로 이를 방지하기 위하여 증거 가치를 조사하기 전에 배제되어야 한다.

컴퓨터 기록(Computer Record)과 같은 디지털증거에 대해서는 현행 형사소송법에서는 아무런 규정을 갖고 있지 않지만, 일반적으로 서면과 같이 취급하고 있으며, 미국에서도 대체적으로 비슷한 입장이다[13, 16, 18, 21]. 따라서 디지털증거가 사람의 진술을 내용으로 하는 것일 때에는 전문법칙이 적용되어 증거로서 사용할 수 없다(형사소송법 제 310조의 2). 그러나 전문법칙에는 넓은 예외가 인정되므로 이러한 예외에 해당하는 여부가 디지털증거의 증거능력을 가늠하는 척도가 된다. 예를 들면 공무원의 직무상 증명할 수 있는 사항에 관하여 작성한 문서, 업무상 필요로 작성한 통상문서, 기타 특히 신용할만한 정황에 의하여 작성된 문서 등의 경우에는 당연히 증거능력이 있는 것으로 형사소송법이 규정하고 있어(형사소송법 제 315조), 디지털증거가 이러한 요건을 충족하면 증거능력이 인정될 것이다.

전문법칙과 관련하여 주의할 사항은 디지털증거가 사람의 손에 의해서 작성된 것이 아니고 컴퓨터 프로그램에 의하여 자동으로 작성되었거나 사람이 작성한 경우에도 디지털증거 존재 자체가 증거로 되는 경우(이적표현 문건의 소지, 명예훼손 문건의 게시 등)에는 전문법칙의 예외에 해당하는 것이 아니고 전문법칙 자체가 적용되지 않는 경우이기 때문에 증거능력의 문제가 아닌 증명력의 문제로 귀속된다[16].

2.2.3 Computer Forensics의 기술과 도구

Computer Forensics의 주요 연구대상이 되는 디지털증거 확보와 보전에 관련된 기술은 법과학에서 사용하는 일반적인 증거분석과 시험방법에 관한 감정기술과 IT 기술 전반을 바탕으로 한 정보보호기술이 주로 응용된다. 따라서 Computer Forensics를 법과학의 분과로 분류하는 동시에 정보보호학의 분과로도 분류할 수 있다.

Computer Forensics에서 응용되는 기술은 디지털증거를 수집하기 위하여 관련 데이터의 존

재와 위치를 검색하는 기술, 검색된 데이터를 원본과 동일성을 유지하면서 복사하는 기술, 원본 또는 복사본에 대한 무결성 확보기술, 확보된 디지털증거의 이동과 보관 과정에 대한 신뢰성 유지기술 등이 포렌식스 절차의 수집 및 보전단계에서 응용되는 기술들이다. 분석단계에서 응용되는 기술로서는 자료구조/감사자료/프로세스 분석기술, 시계열 분석기술, 삭제자료 복구기술, 암호제거 및 분석기술, 은닉자료 분석기술 등이 사용되며, 보고단계에서는 보고서 작성과 열람을 위한 기술이 사용된다.

Computer Forensics에서 사용되는 도구는 디지털증거를 수집, 보전, 분석, 보고하는 과정에서 작업의 효율과 신뢰성을 확보하기 위하여 이용된다. 포렌식 도구의 사용은 때로는 작업의 효율성을 높여주는 대신 신뢰성이 떨어지거나 원본에 치명적인 손상을 가하는 경우가 있다는 사실을 명심해야 한다. 반대로 시험/분석을 행하는 입장에서는 이미 확인된 사실이지만 관계자의 이해와 신뢰를 높이기 위하여 포렌식 도구를 사용해야 하는 경우도 있다. 이와 같이 포렌식 도구의 사용은 상황과 환경에 따라 신중하게 결정해야 한다.

포렌식 도구는 처음부터 포렌식 용도로 제작된 경우도 있지만 일반 정보보호나 시스템/네트워크 관리를 위하여 제작된 것을 포렌식 도구로 활용하는 경우도 많다. 또한 포렌식 도구는 상용 제품과 함께 무료로 공개되는 프로그램에 이르기까지 매우 다양한 도구들이 사용되고 있다. 무료로 공개되는 도구들을 적절히 잘 조합해서 사용하면 비용이 절감될 뿐만 아니라 다양한 환경에 쉽게 응용할 수 있어서 포렌식 기술 향상에 많은 도움이 될 수 있다.

포렌식 도구를 이용할 때 반드시 점검해야 할 사항은 포렌식 도구 자체가 신뢰할 수 있는 프로그램인지를 체크해야 한다. 사용 전에 충분한 테스트를 거쳐서 시험결과가 항상 동일하게 나오는지, 또한 프로그램에 치명적인 결함은 없는지 여부를 확인해야 한다. 가능하면 정체불명의 프로그램은 사용하지 않는 것이 안전하며, 상용 제품의 경우도 반드시 정품에 대한 생산자의 보증을 확인하고 사용하는 것이 안전하다.

또한 소스가 공개되어 있는지 여부도 포렌식 도구의 신뢰성 확인에 중요한 요소이다. 대부분의 상용 제품이 우수한 성능을 가지고 있지만 포렌식 전문가들이 사용할 때 주저하는 것은 분석과정에서 발생할 수 있는 에러에 대한 처리를 프로그램 소스를 기반으로 설명할 수 없다는 점이다. 그리고 일반적으로 알려진 바와 같이 소스 공개 정책은 많은 참여자들의 다양한 의사가 반영되어 보다 신뢰할 수 있는 도구로 발전 가능성을 열고 있다는 점도 강점에 속한다.

3. 국내 Computer Forensics의 발전방향

3.1 Computer Forensics의 과학적 연구

국내에서 Computer Forensics를 과학으로서의 학문성을 인정할 수 있겠는가에 대한 논의는 법과학 특히 협의의 법과학 자체가 독립된 과학으로서 학문성을 인정할 수 있을 것인가에 대한 논의가 전제되어야 할 것이다. Computer Forensics가 학문이냐 단순한 기술 또는 기능에 불과한 것이냐에 대한 논의는 법과학이 학문이냐 기술이냐에 관한 논의의 연장선에 있는 문제가 될 것이기 때문이다.

국내에서 Computer Forensics에 대한 학문적 연구로 접근한 기록은 아직 발견되지 않고 있다. 다른 법과학 분야도 법의학을 제외하면 대학에서 법과학을 독립 학문으로 연구하는 곳은 없는 것으로 파악되고 있다. 다만 국립과학수사연구소에서 법의학, 법생물학, 법화학, 법물리학 등 다양한 분야에 대한 응용 기술을 실무적 필요

에 따라 연구하고 있으며, 그 결과가 국내외 법과학 관련 세미나 등에서 발표되고 있다.

외국에서도 아직 Computer Forensics를 독립된 학문으로서 인정하는 추세는 아니며, 다만 영국과 미국 등지에서 대학원 과정에 강좌를 개설하여 운영하는 곳이 있는 것으로 파악되고 있다[3, 21]. 그러나 이러한 강좌들도 대부분 현장에서 필요로 하는 기술 습득이나 조사기법 등을 다루고 있으며 학문으로서의 과학적 접근방법을 연구하는 것은 아닌 것으로 알려지고 있다[3].

국내에서 Computer Forensics에 대한 연구는 주로 수사기관의 사이버범죄 수사나 침해사고 대응을 위한 현장 중심의 수사기법이나 침해사고 대응기법에 한정된 연구였고, 연구소나 보안업체도 주로 수사기관의 수사과정에서 필요로 하는 수사용 도구를 개발하는 차원에서의 연구개발이 이루어져 왔다[21]. 그리고 수사기관의 성격상 수사기법이 노출되어 범죄자가 악용하는 것을 우려하여 관련 기술이나 도구에 대한 정보를 일반에 제공하지 못하고 있는 실정이어서 과학적인 논의가 어려운 실정이다.

또한 국내에서의 Computer Forensics에 대한 인식도 수사기관에서는 컴퓨터범죄 수사기법 정도로 이해하고 있으며, 연구소나 보안업체에서는 침해사고 대응기법이나 복구기술에 한정된 시각을 갖고 접근하고 있다. 더구나 경찰과 검찰, 국가정보원과 국군기무사령부 등 Computer Forensics를 필요로 하는 기관들이 같은 도구와 기법들을 중복적으로 연구개발하고 있어 연구인력과 예산의 낭비가 우려되고 있다.

이미 설명한 바와 같이 Computer Forensics가 독립된 학문으로서 연구 가치가 있는가에 대한 논의는 법과학 전반의 학문성과 수반하여 진행되어야 할 것이다. Computer Forensics도 법과학과 함께 응용 기술의 차원을 넘어서는 과학의 한 영역으로 자리 잡을 수 있도록 체계적인 연구가 요망되는 분야이다. 정부에서는 이러한 새로운 분야의 학문적 연구에 적극적인 지원이 있어야 할 것이다.

최근 고무적인 것은 국내에서도 Computer Forensics에 대한 관심이 고조되고 있다는 점이다. Computer Forensics를 전자정부 실현과 전자상거래의 활성화를 위한 기반기술로 인식하며 지금까지 주로 수사기관과 정보기관에서 수사기법이나 정보취득을 위한 방편으로 접근하던 관점에서 한 차원 높은 접근을 시도하고 있다. 연구에 참여하는 층도 대학, 연구소, 기업 등으로 두터워지고 있으며, 그동안 각 기관에 따라 산발적으로 이루어지던 연구개발도 각 기관의 Computer Forensics 담당자들을 중심으로 Computer Forensics 연구모임이 운영되면서 좀더 개방적이며 체계적인 접근이 시도되고 있다[21, 24].

3.2 Computer Forensics 관련 법체계의 정비

전자정부의 실현과 전자상거래의 활성화에 따라 정보통신망 이용촉진과 정보보호 분야에 대한 법체계와 제도가 새롭게 많이 정비되어 가고 있다. 그러나 이러한 법체계나 제도가 그 목적을 달성하기 위해서는 이들의 법제에 기초하여 이루어진 거래사실의 신뢰성(Reliability)과 책임성(Accountability)이 보장되지 않는다면 사상누각에 불과할 것이다. 또한 이러한 사실관계의 확정과 책임성의 확보는 개인 프라이버시의 보호와 균형을 이루지 않으면 또다른 불행이 시작된다. 따라서 Computer Forensics에 대한 과학적 접근과 함께 법제도의 명확한 정비는 지식정보사회의 기반이라 할 수 있다.

1995년 형법의 일부 개정을 통하여 '컴퓨터 등 정보처리장치'와 '전자기록 등 특수매체기록'에 관련된 범죄를 규제하는 법제의 정비가 이루어졌으나 형사절차에 관한 법률의 정비는 이루지지 않고 있다. 디지털증거의 속성과 이를 둘러

싸고 발생할 수 있는 소송법상의 여러 문제들에 대한 부담을 명백한 원칙에 의해 안배하지 못하고 있는 실정이다. 물론 수사기관과 법관, 변호사 등 소송관계자들이 기존의 오프라인 법제도를 유추하고 외국의 법제를 참고하여 실무관행을 쌓아가고 있기는 하지만 법제도의 공백은 결국 그것을 운용하는 사람의 자의적 판단이 개입할 위험이 내재해 있는 것이다.

그리고 디지털증거는 원본을 복사해도 디지털증거의 본질적 내용인 0과 1의 조합 배열이 달라지는 것이 아니라는 면에서 증거법에서 요구하는 원본성을 충족할 수 있을 것 같이 보이나, 결국 이러한 원본을 법정에서 증거로 제시하기 위해서는 어떤 형태로든 또 다른 처리과정을 거쳐야 하며, 이러한 처리과정의 결과로 도출되는 증거는 최초에 제시하려던 디지털증거의 모습을 설명하는 자료일 뿐 그 자체의 원시적인 모습은 아닌 것이다. 결국 디지털증거는 오프라인에서 실물이 존재하는 증거물과 같은 원본을 제시할 수 있는 방법은 원천적으로 불가능한 것이다. 결국 디지털증거에 관한 원본성 요구는 입법적 타협을 전제할 수밖에 없다는 결론에 다다른다.

소송법 체계를 정비하여 디지털증거에 대한 개념을 명확히 도입하고, 이에 대한 압수/수색/검증의 절차와 방법, 증거 조사방법, 원본성 인정문제, 복사물과 출력물의 생성과 조사방법 등을 명문화하여 기존의 학설과 실무관행에 의존하고 있는 중요한 논점을 입법적으로 해결하여야 할 것이다[24].

3.3 Computer Forensics 관련 운용체계의 정립

디지털증거에 관한 법제가 완비된다고 해도 이를 운용하는 시스템이 제대로 확립되지 않으면 실효를 거두기 어려울 것이다. 소송에서 사실의 인정은 증거에 의하여 이루어지기 때문에 모든 증거의 관리에는 많은 주의와 노력을 필요로 한다. 디지털증거는 눈에 보이지 않고, 변경이 쉽게 일어나는 반면 그 변화를 포착하기 어렵고, 원본과 복제본과의 구별이 어려운 특성으로 인하여 다른 어느 증거보다 그 관리에 특별한 주의와 노력을 투입해야 한다.

또한 디지털증거가 IT 기술을 기반으로 관리되고 있기 때문에 IT 기술에 대한 신뢰 여부가 곧바로 증거의 가치판단에 직접적인 영향을 미치게 된다. 즉 IT 기술을 무조건 신뢰하는 사람은 디지털증거가 컴퓨터에 의해서 작성되었다는 이유만으로 신뢰할 수 있는 증거라는 예단을 갖게 되고, 반대로 IT 기술을 전혀 신뢰하지 않는 사람은 똑같은 이유로 신뢰할 수 없는 증거라는 편견을 갖게 된다는 것이다. 증거가 사실인정의 자료로서 역할을 제대로 하게 하려면 이러한 예단과 편견을 최소화할 수 있는 방안들을 마련해야 할 것이다.

수사기관에서는 디지털증거의 특성을 감안해서 증거의 수집과 보존, 법정제출과 관련된 업무절차를 표준화하여야 한다. 그리고 특별히 보안이 요구되는 사건을 제외하고 기소 후에 포렌식 절차를 공개하여 법집행의 투명성을 높이고 보다 합리적인 실무관행을 형성하는데 기여하도록 해야 할 것이다. 법원은 디지털증거 조사의 절차와 방법을 구체적으로 제시해야 하며, 디지털증거를 조사할 수 있는 검증된 컴퓨터 시스템과 증거 현출장치를 설치하여 소송관계자들에게 디지털증거를 자유롭게 제출할 수 있는 기회를 제공해야 한다. 감정기관은 보다 객관적이고 투명한 시험과 분석방법을 개발하여 적용해 나가야 할 것이다.

그리고 급변하는 Computer Forensics 관련 환경과 기술의 변화를 반영하기 위하여 수사기관, 정보기관, 법원 등 법집행기관의 실무책임자들과 대학과 연구소, 법무법인과 보안업체 등의

포렌식스 전문가들이 모여 Computer Forensics 관련 현안 문제들을 함께 검토하고 합리적인 대안들을 제시하며, 포렌식 절차와 도구에 대한 기본 모델들을 제안하고, 수사기관과 법원 등 현업 종사자들에 대한 직무교육 기회로 제공하며, 필요에 따라 Computer Forensics 전문가 자격 인정 제도를 도입하는 등 전문가 육성 프로그램을 운영하는 개방된 커뮤니티를 구성/운영하는 것도 Computer Forensics 발전에 큰 도움이 될 것이다.

3.4 Computer Forensics의 기술개발

Computer Forensics 분야는 법제도와 운영체계를 정비함과 동시에 끊임없이 관련기술과 도구를 개발해 나가야 한다. IT 기술의 발전에 따라 컴퓨터의 성능과 용량도 계속해서 향상되고 각종 응용 프로그램과 서비스들이 매일 새롭게 등장하고 있다. 이러한 변화에 수반해서 새로운 기기와 기술을 악용한 범죄를 속속 등장하고 있으며 범행기법도 다양해져 가고 있다. 따라서 이들 범죄에 대응하기 위해서는 디지털증거의 수집과 분석 및 보전 기술을 계속 발전시켜 나가야 할 것이다.

국내 Computer Forensics와 관련한 기술과 도구는 주로 수사단서를 확보하는데 필요한 기술에 치중되어 있다[21]. 물론 범죄사실을 확정하기 위해서는 증거수집이 가장 중요한 요소임에는 틀림이 없다. 그러나 디지털증거는 수집기술과 함께 수집된 증거에 대한 보전기술과 분석기술, 그리고 법정에 제시하기 위한 보고기술도 증거로서의 가치를 유지하기 위해서는 매우 중요한 요소기술들이다. 이러한 요소기술을 고르게 발전시켜 나가야 할 것이다.

국내 Computer Forensics 기술개발의 기본방향은 분업과 협력의 적절한 조화에서 찾아야 할 것이다. 분업의 원리는 문자 그대로 Computer Forensics 기술을 필요로 하는 기관의 성격에 따라 개발해야 할 영역을 나누어 집중 투자하자는 것이다. 예를 들면 수사기관은 주로 수사단서를 찾기 위한 수집기술과 추적기술에 중점을 두어 연구하고, 정보기관은 은닉기법과 암호화에 대한 분석과 우회기술을 집중 연구하며, 감정기관은 디지털증거의 신뢰성 확보기술에 중점을 두어 연구개발을 하면 중복을 피할 수 있을 것이다.

대학과 국책연구소에서는 이미 보유하고 있는 정보보호기술, 즉 암호기술, 전자서명기술, 타임스템프 서비스기술, DRM, 디지털 워터마크 기술, 데이터베이스 관리기술과 Data Mining기술, 침입탐지/차단/역추적 기술 등을 Computer Forensics 분야에 적용시키기 위한 연구를 담당하고, 연구결과를 기업에 이전하여 포렌식 도구 개발에 활용할 수 있도록 지원해야 할 것이다.

또한 법집행기관, 대학, 연구소, 기업 등 모든 주체가 연구 개발한 결과를 서로 공유하며 협력할 수 있는 방안을 강구해 나가야 할 것이다. 이미 설명한 바와 같이 Computer Forensics는 응용되는 기술 분야가 워낙 광범위하고 기술발전 속도도 빨라서 어느 한 주체가 모든 기술을 다 보유하면서 변화하는 기술을 흡수하여 발전시켜 나간다는 것은 사실상 불가능한 일이며 국가 전체의 입장에서 보면 낭비 요인이 된다. 분업과 협력의 원리 아래서 모든 주체에 도움을 주는 WIN-WIN 전략을 찾아야 할 것이다.

4. 결 론

본 논문은 전자정부 실현과 전자상거래의 활성화로 전자거래의 비중이 커지고 있으며, 이에 수반하여 급속히 증가하고 있는 컴퓨터범죄를 포함한 법적분쟁을 해결하는데 디지털증거의 중요성이 날로 증가하면서 이에 대한 과학적이고 체계적인 연구의 필요성에 따라 Computer Forensics의 독립 과학으로서의 연구 가능성과 국

내 Computer Forensics의 발전방향을 고찰하였다.

Computer Forensics는 법과학(Forensic Science)의 한 분과로서 학문적 체계를 갖추고 연구되어야 한다. Computer Forensics의 핵심 연구대상인 디지털증거를 증거법에서는 어떻게 다룰 것인가에 대한 법률적 연구 관점도 현행법의 규정을 충실하게 검토하되 전향적인 연구자세를 가지고 입법론적인 연구가 심도 있게 수행될 수 있게 해야 한다. 이를 위해서는 법관, 검사, 변호사 등 법조인은 물론이고, 실무에 밝은 수사관들과 입법부의 입법조사관 등의 폭넓은 의견을 반영할 수 있도록 연구의 폭을 확대해 나가야 한다.

또한 Computer Forensics의 연구가 실무 현장에서 실효성 있게 이용될 수 있게 하기 위해서는 디지털증거를 취득하고 분석하고 관리하는 기술과 기법에 관한 연구가 특정한 기관에서만 이루어져서는 소기의 목적을 달성하기 어려울 것이며, 수사기관과 침해사고 대응기관의 실무 책임자들과 대학과 연구소, 기업 등 Computer Forensics에 관심을 갖고 있는 모든 사람들이 함께 참여하고 연구결과를 공유할 수 있는 열린 커뮤니티를 만들어 운영하는 것도 좋은 발전전략이 될 것이다.

Computer Forensics의 핵심 연구대상은 디지털증거이다. 디지털증거의 생명주기(Life Cycle of Digital Evidence), 증거수집/보전/분석/보고의 전 과정에서 과학적이며 합리적인 업무절차에 대한 가이드가 수립되어야 하며, 이들 업무절차가 객관적으로 입증될 수 있게 기록으로 남겨져야 한다. 이러한 가이드 수립의 일환으로 제안된 '디지털증거 획득모델'[21]과 '디지털증거 분석모델'[21], 그리고 '디지털증거 관리시스템'[17]과 '디지털증거 작업감사 시스템(Work-flow Logging System)'[19] 등이 향후 연구과제로 더욱 깊이 있는 연구가 요망된다.

참 고 문 헌

[1] ACPO, Good Practice Guide for Computer Based Evidence V2.00, The Association of Chief Police Officers(ACPO) Computer Crime Group, June 1999.

[2] Albert J. Marcella and Robert S. Greenfield, Cyber Forensics : A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Auerbach, 2002

[3] Alfred C., 해킹과 포렌식 입문, 도서출판 그린, 2002.

[4] Dan Farmer and Wietse Venema, "The Big Chill : Freezing Data for Analysis", Computer Forensics Analysis Class Handouts, August 6th, 1999, (http://www.fish.com/forensics/freezing.pdf).

[5] Eoghan Casey, Digital Evidence and Computer Crime, Academic Press, 2000.

[6] http://cyber.icu.ac.kr/main/mainframe.asp.

[7] http://www.law.cornell.edu/rules/fre/overview.html.

[8] Kevin Mandia and Chris Prosise, Incident Respone : Investigating Computer Crime, Foundstone, 2001.

[9] Mark M. Pollitt, "Computer Forensics : An Approach to Evidence in Cyberspace", Federal Bureau of Investigation, Baltimore, MD. Undated ([12]에서 인용된 것을 재인용).

[10] Michael A. Caloyannides, Computer Forensics and Privacy, Artech House, 2001.

[11] Simson Garfinkel, Network Forensics : Tapping the Internet, O'Reilly & Associates, Inc. 2002.

[12] Tony Sammes and Brian Jenkinson, Forensic Computing : A Practitioner's Guide,

Springer, 2001.

[13] United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002, (http://www.cybercrime.gov/s&smanual2002.htm).

[14] Vicka Corey, Charles Peterman, Sybil Shearin, Michael S. Greenberg, and James Van Bokkelen, "Network Forensics Analysis", IEEE Internet Computing, 2002.

[15] Warren G. Kruse II and Jay G. Heiser, Computer Forensics : Incident Response Essentials, Addison-Wesley, 2002.

[16] 구태언, "디지털 증거와 법률문제", 제 6차 컴퓨터포렌식스연구회 발표자료, 2002. 12.

[17] 김종섭, "Computer Forensics와 전자공증을 응용한 '전자증거 관리 시스템' 설계 및 운영 방향", 동국대학교 국제정보대학원(정보보호학과) 석사학위논문, 1999.

[18] 김종섭, "Computer Forensics : 현황과 전망", 제 3차 컴퓨터포렌식스연구회 발표자료, 2002. 7.

[19] 김종섭, "컴퓨터 증거 확보와 법률문제", 제 6차 해킹방지컨퍼런스 발표자료, 한국정보보호진흥원, 2002. 11.

[20] 유영찬, 법과학과 수사, 현암사, 2002.

[21] 이성진 외 8인, 해킹피해 시스템 증거물 확보 및 복원에 관한 연구 : A study on Computer Forensics, 한국정보보호진흥원, 2002.

[22] 이현우 외2인, UNIX 피해시스템 분석(v1. 1) : Scene of The Crime, 2002. 6 (http://www.securitymap.net/).

[23] 이형우 외2인, "Computer Forensics 기술", 정보보호학회지(제12권 제5호), 2002. 10.

[24] 최득신, Computer Forensics에 관한 연구, 서울대학교 행정대학원, 2002.

김 종 섭

1978년 중앙대학교 법학과 (법학사)

2000년 동국대학교 국제정보대학원(정보보호학석사)

2003년 경기대학교 대학원 정보보호기술공학과 (박사과정)

1996년～1999년 한국정보보호진흥원(협력관)

1981년～2002년 경찰청(사이버테러대응센터)

2002년～현재 국립과학수사연구소

김 귀 남

미국 캔자스대학 수학과(응용수학사)

미국 콜로라도주립대학 통계학과(통계학석사)

미국 콜로라도주립대학 기계·산업공학과(기계·산업공학박사)

현재 경기대학교 정보보호기술공학과 주임교수