情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

서버 가상화 환경의 가상머신 이미지에 대한 법적 증거로서의 허용성에 관한 연구*

김 동 희†, 백 승 조, 심 미 나, 임 종 인‡
고려대학교, 정보경영공학전문대학원

A Study on the Admissibility of the Virtual Machine Image File as a Digital Evidence in Server Virtualization Environment*

Dong-Hee Kim†, Seung-Jo Baek, Mina Shim, Jong-In Lim‡
Graduate School of Information Management and Security, Korea University

요 약

오늘날 많은 기업들이 비용절감을 위해 서버 가상화 기술의 이용 및 보급을 확대함에 따라 가상화 서버에서의 사이버범죄도 크게 증가할 것으로 예상된다. 서버 가상화 솔루션은 각 가상화 서버에 대한 가상머신 이미지를 생성하는 기능을 기본적으로 제공하기 때문에 서버 가상화 환경에서는 기존의 디지털 포렌식 수사과정의 디스크 이미지 수집과정을 생략하고 가상머신 이미지를 법적증거로 직접 활용함으로써 보다 신속하고 효율적인 수사가 가능하다. 하지만 가상화 서버의 구조적 특징으로 인해 나타날 수 있는 보안 취약성, 그리고 서버 가상화 솔루션의 신뢰성과 증거수집 절차상의 문제들로 인해 가상머신 이미지 자체만으로는 법적증거로서의 허용성을 인정받지 못한다. 본 논문에서는 가상머신 이미지가 법적증거로서 허용성을 인정받기 위해 서버 가상화 솔루션이 갖추어야 할 보안 요구사항, 디지털 포렌식 도구로서의 신뢰성 조건들을 도출하였으며, 가상머신 이미지가 증거로서의 연계보관성을 만족시키기 위해 갖추어야할 부가요소들을 제안한다. 또한 이러한 조건들을 통해 가상머신 이미지 증거가 미국 연방증거법의 법적 허용성 기준들을 만족시키는지 살펴보고, 이를 위한 관련 기관들의 구체적인 역할 및 세부 추진계획들을 제안한다.

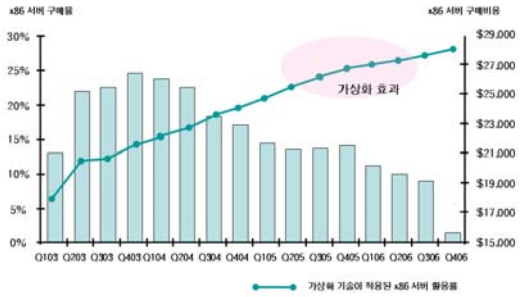
ABSTRACT

As many companies are considering to use server virtualization technology to reduce cost, the crime rates in virtual server environment are expected to be increasing rapidly. The server virtualization solution has a basic function to produce virtual machine images without using any other disk imaging tools, so that investigating virtual servers are more efficient because the investigator only has to collect the virtual machine image and submit it to the court. However, the virtual machine image has no admissibility to be the legal evidence because of security, authenticity, procedural problems in collecting virtual machine images on virtual servers. In this research, we are going to provide requirements to satisfy security, authenticity and chain of custody conditions for the admissibility of the virtual machine image in server virtualization environment. Additionally, we suggest definite roles and driving plans for related organizations to produce virtual machine image as a admissible evidence.

Keywords : Digital Forensics, Digital Evidence, Server Virtualization, Virtual Machine Image, Admissibility

Ⅰ. 서 론

가상화 서버는 기존의 물리적 서버와 달리 여러 사용자가 하나의 호스트 서버 자원을 논리적인 서버 자원으로 할당받아 사용할 수 있다는 특징을 가지고 있기 때문에 서버자원의 사용량이 상대적으로 많은 기업 또는 조직의 비용 절감, 친환경 IT정책 차원에서 서버 가상화 기술의 보급 및 이용이 확대되고 있다. 실제로 IDC는 가상화 서버의 보급률이 2009년 약 5백만 대에 이를 것으로 전망하였으며, 기존의 x86서버 제품의 구매율은 2004년 이후 현저히 낮아지는데 반해 서버 가상화 기술을 적용한 x86 서버의 활용률은 지속적으로 상승하고 있다고 조사, 발표하였다[1].



[그림 1] 가상화 효과에 따른 x86 서버 시장의 구매 패턴 변화

서버 가상화 시장이 커짐에 따라 이와 같은 환경에서 발생할 수 있는 사이버범죄에 대응하기 위한 디지털 포렌식 수사도 활발하게 이루어질 것으로 예상된다. 기존의 물리적 서버 환경에 대한 디지털 포렌식 수사는 해당 서버에 접근하여 별도의 디지털 포렌식 도구를 이용하여 원본 디스크와 완전히 동일한 디스크 이미지(image)를 수집한다. 이렇게 디스크 이미지를 수집하는 것은 원본 증거의 무결성 유지 및 증거의 연계보관성(chain of custody)을 만족시키기 위한 매우 중요한 절차에 해당된다. 이와 달리 서버 가상화 솔루션은 호스트 서버 내에 존재하는 각 가상화 서버(또는 가상머신)들에 대한 이미지 파일을 생성하는 기능을 기본적으로 갖추고 있다.

따라서 가상화 서버에 대한 수사과정에서 수집한 가상머신 이미지 파일을 분석과정을 거쳐 법적 증거로 바로 제출할 수 있으며, 기존의 디스크 이미지 파일 생성 단계를 생략하고 포렌식 수사 절차의 간소화할 수 있기 때문에 보다 신속하고 효율적인 수사가 가능하다. 하지만 서버 가상화 환경은 기존의 물리적 서버와 구조적인 차이점들을 가지고 있으며, 이로 인해 나타날 수 있는 여러 가지 보안 위협들을 통해 가상머신 이미지는 위·변조 및 훼손될 수 있다는 문제점이 있다. 또한 서버 가상화 솔루션의 가상머신 이미지 생성기능이 검증되지 않아 증거로서의 신뢰성을 인정받지 못하는 문제, 가상머신 이미지의 수집에서 법정 제출 단계까지의 연계보관성을 보장해주는 해쉬(hash), 타임스탬프(timestamp), 전자서명과 같은 기능들이 수행되지 않기 때문에 가상머신 이미지는 그 자체만으로 법적증거로서의 허용성을 인정받지 못한다.

본 연구는 이와 같은 문제점들을 구체적으로 살펴보고 미국의 법·제도를 중심으로 가상머신 이미지가 갖추어야 할 법적증거로서의 허용성 조건들을 도출하였으며, 실제로 가상머신 이미지의 법적증거로서의 허용성 조건들을 만족시키기 위한 사회 각 주체별 역할 및 세부계획을 나타내는 추진체계를 간략히 살펴본다.

본 논문의 나머지는 다음과 같은 순서로 구성된다. II장에서는 서버 가상화와 디지털 포렌식의 개념을 간단히 살펴보고, 가상화 환경을 이용한 디지털 포렌식 수사 방법에 대한 기존의 연구들을 살펴본다. III장에서는 가상머신 이미지 수집과정에서 나타나는 여러 가지 문제점들과, 이로 인해 가상머신 이미지가 법적증거로서의 허용성을 인정받지 못하는 문제가 발생함을 살펴본다. IV장에서는 가상머신 이미지가 법적증거로서의 허용성을 인정받기 위한 기준들을 제안하였으며, 이를 만족시키기 위한 관련 기관들의 역할 및 수행해야 할 세부계획들을 간략하게 살펴본다. V장에서는 본 논문의 결론을 맺는다.

II. 관련 연구

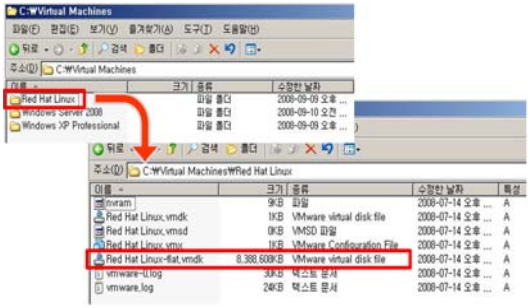
2.1 서버 가상화(Server Virtualization)

가상화(Virtualization)란, 하나의 물리적 요소를 여러 개의 논리적 요소로 나누어 관리할 수 있게 하거나, 복

접수일: 2008년 9월 12일; 채택일: 2008년 10월 8일
* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))
† 주저자, dhk0831@korea.ac.kr
‡ 교신저자, jhlim@korea.ac.kr

수 개의 물리적 요소를 하나의 논리적 요소로 통합하여 관리할 수 있게 하는 기술을 말한다. 서버 가상화는 하나의 물리적 서버 내에 여러 개의 논리적 가상머신(또는 가상화 서버)들을 두어 CPU, 메모리, 네트워크, 스토리지 자원 등을 공유하는 기술을 말한다[19].

서버 가상화 환경에서 기본적으로 생성되는 정보는 가상머신 설정 및 파라미터 정보를 담고 있는 가상머신 설정(configuration) 파일, 가상머신 로그(log), 호스트 서버의 시스템 레지스터 정보, 가상머신 이미지 등이 있다. 특히 가상머신 이미지는 각각의 가상머신이 할당받은 가상 스토리지 자원이 기존의 물리적 서버에서의 하드디스크 이미지와 같은 형태의 비트 대 비트(bit-by-bit) 방식으로 생성되어 호스트 서버에 저장되며, 해당 이미지 내에는 가상머신에 탑재되는 게스트(Guest) OS를 비롯하여 데이터베이스 자원, 기타 정보들이 모두 기록된다. 따라서 가상머신 이미지는 서버 가상화 환경에서 가장 많은 정보를 담고 있기 때문에 동 환경에 대한 수사 과정에서 가장 먼저 접근하여 수집해야하는 대상으로 매우 중요하다고 볼 수 있다.



[그림 2] VMware Server에서의 가상머신 이미지 생성

서버 가상화 기술에서의 핵심적인 역할은 하이퍼바이저(또는 가상머신 모니터)가 담당한다. 하이퍼바이저는 호스트 시스템의 CPU 인터럽트, 상태 관리(state management) 등을 통해 각 가상머신에 대한 추상화(abstraction), 격리(isolation) 기능을 제공하며 물리적 서버 자원을 효율적으로 공유하고 분배하는 물리적 하드웨어 상의 추상적인 개념의 소프트웨어 계층(layer)이다.

추상화는 각 가상머신들이 사용하고 있는 호스트 서버의 물리적 위치 주소를 숨겨주는 기능으로, 가상화 환경에서 실행되는 논리적 가상머신들이 마치 물리적으로 떨어져 있는 개별 서버들인 것과 같은 효과를 준다.

또한 격리는 가상화 서버의 프로세스, 애플리케이션 등이 동일한 물리적 서버 내의 다른 논리적 가상화 서버에 전혀 영향을 주지 않은 것을 말한다. 즉, 하나의 물리적 장치가 가상화를 통해 여러 개의 논리적 파티션으로 나누어지고 각각의 논리적 파티션 내에 존재하는 데이터와 프로세스들이 다른 파티션의 프로세스로부터 전혀 영향을 받지 않는 것을 말한다.

2.2 디지털 포렌식(Digital Forensic)과 가상화

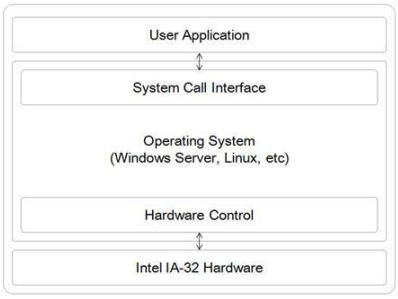
IT의 발달은 우리 사회 대부분의 정보를 디지털화하여 생성하고 처리하고 있으며, 이러한 정보들은 컴퓨터, 모바일 장치 등 각종 디지털 정보기기에 저장된다. 이에 따라 디지털 정보기기를 활용한 범죄는 사이버 공간 뿐 아니라 일상 생활공간에서도 점차 증가하고 있는 추세이며, 해당 장치는 수사를 위한 증거로서 매우 중요한 역할을 하게 되었다. 이렇게 디지털 정보기기 내에 저장된 불법행위 및 범죄의 증거를 수집하고 분석하는 보안 서비스를 디지털 포렌식이라고 한다.

디지털 포렌식과 가상화의 관계에 대한 연구는 대부분 가상화 기술을 디지털 포렌식 수사 도구로 활용하는데 초점을 맞추고 있다. Arnes(2006)[2]는 가상화 기술을 이용하여 가상 보안테스트 환경(virtual security testbed)을 조성하고, 공격자의 침입 유형 분석을 통해 각종 사이버범죄 관련 수사에 활용하는 연구를 진행하였다. Bem(2007)[3]은 두 개의 컴퓨터 하드디스크 이미지 사본을 생성하여 기존의 디지털 포렌식 수사절차에 따른 증거분석과 가상화 환경을 이용한 증거분석을 병행하는 방법을 제시하였다. 또한 Bem(2007)[4]은 USB 드라이브의 이미지를 생성하여 가상화 환경을 통해 이를 분석하는 연구도 진행하였다. 하지만 이러한 연구들은 가상화 환경이 실제 범죄 환경을 재구성함으로써 신속하고 효율적인 증거분석을 수행할 수 있게 해주는 장점이 있지만, 이미지 파일에 대한 무결성 및 신뢰성을 보장하지 못하기 때문에 법적 증거로 인정되지 않으며 기존의 증거분석 방법과 병행되어야만 한다는 문제점이 있다.

III. 서버 가상화 환경에서 가상머신 이미지 수집 시 문제점

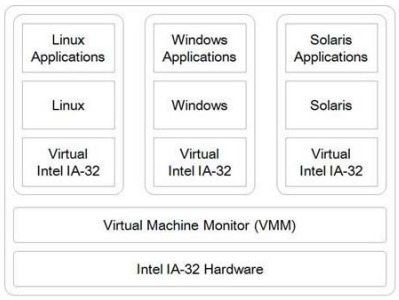
기존의 물리적 서버는 [그림 3]과 같이 하나의 단일

시스템으로 구성되어 있으며 사용자들은 특정 운영체제가 설치된 하나의 논리적인 파티션으로 접근하여 동일한 하드웨어 자원을 공유한다.



[그림 3] 기존의 물리적 서버 환경

이와 달리 서버 가상화 환경은 [그림 4][5]에서 볼 수 있듯이 하나의 하드웨어 자원이 하이퍼바이저의 논리적 파티셔닝을 통해 생성된 각각의 가상머신에 할당되며, 이들은 완전히 격리되어 있기 때문에 가상화 서버 사용자들은 마치 하나의 독립적인 서버 자원을 사용하는 것과 같은 효과를 가진다.



[그림 4] 서버 가상화 환경

서버 가상화 환경의 이러한 구조적인 특성은 디지털 포렌식 수사과정에서 가상머신 이미지의 수집에 많은 문제점들을 야기한다. 즉, 서버 가상화 기술의 보안 취약성에 따른 가상머신 이미지의 위·변조 및 훼손, 가상머신 이미지를 생성하는 서버 가상화 솔루션의 신뢰성 확보, 가상머신 이미지 수집 과정에서의 법·제도적 문제들이 나타날 수 있다. 본 장에서는 서버 가상화 환경에서 가상머신 이미지를 수집할 때 나타날 수 있는 여러 가지 문제점들을 구체적으로 알아보고, 이로 인해 가상머신 이미지가 그 자체만으로 미국 연방증거규칙(Federal Rules of Evidence, FRE)[6]의 법적 허용성 기준들을 만족시키지 못하는 이유를 구체적으로 살펴본다.

3.1 서버 가상화 환경의 보안 문제

가상머신 이미지는 서버 가상화 기술에서 나타날 수 있는 보안 취약성들로 인해 법적 증거로서의 허용성 기준들을 만족시키지 못한다. 각각의 가상머신들은 하이퍼바이저의 추상화와 격리 기능을 통해 생성된 논리적 파티션으로, 물리적으로 완전히 분리되어있는 기존의 물리적 서버 환경보다 많은 보안위협들이 나타날 수 있다.

서버 가상화 환경은 호스트, 가상머신, 하이퍼바이저에 대한 접근통제의 취약성들로 인한 보안 위협들을 가지고 있으며, 이러한 위협들이 가상머신 이미지에 부정적인 영향을 미쳐 법적 증거로서의 허용성 기준을 만족시키지 못하는 문제가 발생할 수 있다. [표 1]은 서버 가상화 환경에서의 보안 위협들이 가상머신 이미지에 어떠한 영향을 미치는지 보여준다.

3.1.1 호스트 서버의 보안 위협

서버 가상화 환경에서는 허가받지 않은 사용자가 하이퍼바이저를 거치지 않고 호스트 서버 시스템으로 접근하여 각 가상머신에 할당된 가상 CPU, 하드디스크, 네트워크 자원의 설정을 변경하거나 다른 가상머신의 서버 자원을 독점함으로써 가용성을 침해할 위험이 있다. 또한 호스트 서버로의 접근은 해당 시스템 내에 존재하는 모든 정보에 대한 접근권한을 가질 수 있게 되므로 가상머신 이미지 파일이 위·변조 및 훼손될 수 있다. 이외에도 호스트 서버의 물리적 접근통제의 취약성으로 인해 악의적인 목적을 가진 사용자가 시스템을 강제 종료시킬 수 있으며 홍수, 지진 등 각종 자연재해로 인한 호스트 서버의 물리적 손상으로 가상머신 이미지 파일의 생성 과정에 오류가 발생할 수 있다.

3.1.2 가상머신의 보안 위협

서버 가상화 환경에서 사용자 또는 애플리케이션 및 운영체제의 실행 권한이 잘못 설정될 경우, 특정 가상머신 사용자는 하이퍼바이저의 격리 기능을 우회하여 권한이 없는 메모리 영역으로의 접근이 가능하다. 이를 통

[표 1] 서버 가상화 환경에서 나타날 수 있는 보안 위협

취약성	보안 위협	내 용	가상머신 이미지에 미치는 영향
서버 가상화 환경의 각 구성요소들의 접근통제 취약성	호스트 서버의 보안 위협	① 다른 가상머신이 사용하는 서버 자원의 설정 변경 또는 부적절한 이용으로 인한 가용성 침해	가상머신 이미지 위·변조 및 훼손
		② 호스트 서버 내에 존재하는 가상머신 정보 변경 가능	가상머신 이미지 위·변조
		③ 천재지변으로 인한 호스트 서버의 비정상적인 종료	가상머신 이미지 훼손
		④ 악의적인 목적을 가진 사용자의 호스트 서버 강제 종료	가상머신 이미지 훼손
	가상머신의 보안 위협	⑤ 특정 가상머신 사용자가 격리 환경을 우회하여 다른 가상머신에 대한 데이터 접근 또는 통신이 이루어질 수 있음	가상머신 이미지 위·변조 및 훼손
	하이퍼바이저의 보안 위협	⑥ 하이퍼바이저로의 허가받지 않은 접근을 통해 가상머신에 대한 위·변조 또는 악의적인 가상머신 생성 가능	가상머신 이미지 위·변조
		⑦ 가상 루트킷 설치 가능	가상머신 이미지 위·변조

해 악의적인 목적을 가진 사용자가 다른 가상머신 메모리 영역에 악성코드 및 멀웨어 등을 심어놓고 이를 참조하는 다른 가상머신을 감염시킴으로써 가상머신 이미지에 대한 위·변조 및 훼손이 가능하다.

3.1.3 하이퍼바이저의 보안 위협

하이퍼바이저로의 접근 권한 획득 시 사용자는 악의적인 가상머신의 생성, 삭제, 위·변조, 보안설정 변경 등이 가능하다. 또한 호스트 서버를 악성코드가 삽입되어 있는 저장매체로 부팅함으로써 가상머신 루트킷(Rootkit)을 실행시킬 수 있다.

3.2 디지털 포렌식 도구로서의 신뢰성 확보 문제

현재 널리 상용화되고 있는 디지털 포렌식 도구들의 기능에 대한 과학적 검증작업은 미 국립표준 기술원(NIST)의 컴퓨터 포렌식 도구 테스트 프로그램(Computer Forensic Tool Testing Program, CFTT) [18]에서 수행하며 컴퓨터 포렌식 도구의 테스트 방법론 및 해당 도구의 특징, 테스트 절차, 성능 지표 등을 제공한다. 그리고 사법기관은 이러한 결과가 Daubert Factor [11]를 만족시키는지 판단하여 디지털 증거가 과학적이고 객관적인 포렌식 도구를 통해 수집, 분석되었다는 것을 신뢰할 수 있다.

하지만 가상머신 이미지는 그 생성 과정 및 해당 이미지 파일에 대한 과학적 검증 절차가 마련되어있지 않고 있으며 몇몇 벤더들이 서버 가상화 기술에 대한 기본적인 수준의 정보들만 제공하고 있기 때문에, 가상머신 이미지 자체만으로 법적증거로서의 허용성을 인정받지 못한다는 문제점이 있다.

3.3 서버 가상화 환경에서의 가상머신 이미지 파일 수집절차 문제

서버 가상화 환경은 기존의 물리적 서버 환경과의 구조적 차이로 인해 [표 2]와 같이 가상머신 이미지 파일 수집 과정에서 압수·수색 관련법규 및 지침의 준수, 증거의 수집과 이송·보관 과정에서의 진정성과 무결성 유지와 같은 법·제도적인 문제들이 발생할 수 있다.

3.3.1 관련법류 및 지침에 규정된 일반적인 원칙과 절차 준수

수사관은 물리적 서버에서 디스크 이미지를 수집, 분석하기 위해 필요한 경우에 '적법절차의 원칙'에 따라 압수·수색 영장에 명시된 물리적 서버 자체를 조사할 수 있다. 이에 반해 서버 가상화 환경에서 물리적 호스트 시스템 자체를 대상으로 압수·수색이 이루어지게 될 경우, 다른 가상화 서버 사용자의 호스트 서버 자원에 대한 가용성을 침해할 수 있기 때문에 '비례성 원칙', '적법절차의 원칙'에 위배될 수 있다는 문제점이 있다.

[표 2] 가상머신 이미지 수집 과정에서의 문제점

	기존 물리적 서버 환경	가상화 서버 환경
관련법규 및 지침에 규정된 일반적인 원칙과 절차 준수	'적법절차의 원칙'에 따라 압수·수색 영장에 명시된 물리적 서버 디스크 이미지 수집	다른 가상화 서버 사용자의 시스템 가용성 침해에 따른 '적법절차의 원칙' 위배
수사에 필요한 최소한의 증거만 수집	사건과 관련된 물리적 서버의 디스크 이미지만 수집	가상화 서버 수사를 위해서는 호스트 서버로의 접근이 이루어지며, 다른 가상머신 정보 수집 가능
디지털 증거는 기술적, 절차적 수단을 통해 진정성, 무결성 보존	수집한 디스크 또는 파일에 대한 단방향 암호화 알고리즘값(해쉬값) 생성 및 출력 후 입회인의 서명 날인, 원본과의 대조 후 무결성 검증	가상머신 이미지 생성과정에서 무결성, 책임추적성을 보장할 수 있는 기술 장치 부재

3.3.2 수사에 필요한 최소한의 증거만 수집

기존의 물리적 서버 환경은 단일구조를 가지기 때문에 수사관이 압수·수색 영장에 명시된 서버 외의 다른 서버에 대한 정보를 수집하는 것이 불가능하다. 서버 가상화 환경은 이와 달리 하나의 물리적 서버 내에 여러 논리적 가상화 서버들이 존재하며, 가상화 서버에 대한 수사를 위해 호스트 서버로의 접근이 요구된다. 수사관은 호스트 서버 관리자 권한을 획득함으로써 하이퍼바이저를 통해 각 가상화 서버로의 접근 및 이미지 파일의 수집이 가능하다. 이 과정에서 수사관의 서버 가상화 환경에 대한 이해부족 또는 악의적인 접근을 통해 사건과 무관한 다른 가상머신 이미지 또는 관련 정보를 수집할 수 있는 위험이 존재한다.

3.3.3 디지털 증거는 기술적, 절차적 수단을 통해 진정성, 무결성 보존

일반적으로 서버에서 디지털 포렌식 도구를 이용하여 수집한 디스크 이미지는 해쉬와 타임스탬프, 전자서명을 통해 증거의 무결성과 연계보관성을 보장받을 수 있다. 서버 가상화 솔루션은 기본적으로 가상머신 이미지를 생성하는 기능이 있기 때문에 이를 활용한 증거분석을 통해 보다 효율적인 수사가 가능하다. 하지만 서버 가상화 솔루션은 가상머신 이미지에 대한 해쉬, 타임스탬프 및 전자서명 기능이 제공되지 않기 때문에 해당 증거의 무결성 및 책임추적성 보장이 어려워 가상머신 이미지 자체만으로는 법적증거로 인정받지 못한다.

3.4 가상 머신 이미지의 법적증거로서의 허용성 문제

현재 우리나라 법 · 제도에서는 디지털 증거의 개념 및 법적 허용성 조건들이 명시되어있지 않다. 따라서 국내 각종 소송에서 디지털 증거는 출력 서면으로 전환되어 원문과 동일하다는 입증 하에 서증으로 사용된 이후, 전문법칙(hearsay rule)을 적용하여 진술자 또는 작성자의 진술에 의해 진정성이 증명되어야 법적 증거로 인정받을 수 있다. 이에 반해 미국의 경우, 디지털 증거의 정의 및 법적 허용성 조건들이 연방증거규칙(FRE)에 명확하게 명시되어있다. 본 절에서는 앞서 살펴본 서버 가상화 환경에서의 가상머신 이미지 수집 시 발생할 수 있는 문제점들을 토대로 실제 가상머신 이미지가 미국 연방증거규칙의 법적증거로서의 허용성 조건들을 만족시킬 수 있는지 알아보고자 한다.

3.4.1 디지털 증거(Digital Evidence)로서의 가상머신 이미지

기존의 디지털 증거를 법적증거로 인정하는 기준은 해당 증거가 컴퓨터가 생산한 기록(Computer Generated Record, 이하 CGR) 또는 컴퓨터에 저장된 기록(Computer Stored Record, 이하 CSR)인지의 여부로 판단하였다[17] CGR은 사람의 의견 또는 진술(statement)이 포함되지 않고 기계 자체적으로 생산하는 기록으로 대표적인 예로 로그(log)기록이 여기에 해당된다. CSR은 사람의 의견 및 진술이 개입되어 생산, 저장되는 데이터 기록으로 이메일, 텍스트 메시지, 채팅 콘텐츠, 인터넷 게시물 등이 존재한다. 이와 같이 분류된 디지털 증거는 전문성 예외법칙(hearsay exception rule)에 따라 CGR만 적법성을 인정받으며, 업무기록(business record)과 같이 전문성 예외법칙이 적용되지 않는 특정 CSR의 경우 또한 증거로서 채택 가능하다. 가상머신 이미지는 서버 가상화 환경의 여러 가지 접근통제 취약성들로 인해 위·변조 또는 훼손이 가능하기 때문에 사람의 의견 및 진술이 개입된 CSR이라고 볼 수 있다. 또한 서버 가상화 솔루션의

[표 3] 가상머신 이미지에 적용될 수 있는 Paul Grimm 판사의 법적 허용성 기준

Rule			내 용
901 신뢰성	901(b)(1)	전문가의 증언	해당 증거는 同 분야 전문가로부터 감정을 받아야 한다.
	901(b)(3)	이미 신뢰성이 인정된 어떤 사실을 시도해본 사람 또는 전문가의 증언과 비교	기존의 사례와 비교하여 해당 증거의 신뢰성을 인정받을 수 있어야 한다.
	901(b)(9)	정확한 프로세스 또는 시스템의 결과로 생산된 증거	해당 증거가 정확한 프로세스 또는 시스템의 결과로 생성된 것이라면 신뢰할 수 있다.
902 자기 신뢰성	902(7)	각종 기록 및 서명, 라벨 등을 통한 자기 신뢰성	해당 증거는 메타데이터, 헤더 등에 나타난 사용자 정보 등을 통해 신뢰성을 인정받을 수 있다.
1001		원본과의 동일성	해당 증거의 복사본, 출력 서면은 원본과 동일해야 한다.

신뢰성이 확보되지 않았기 때문에 가상머신 이미지 생성 과정이 기계 자체적으로 오류 없이 생산된 기록이라는 근거가 없으므로 CGR로 분류되기 어렵다. 따라서 가상머신 이미지 그 자체만으로는 법적증거가 될 수 없다.

3.4.2 가상머신 이미지의 법적 허용성 만족 여부

최근에 디지털 증거는 CGR, CSR의 개념이 아닌 미국의 연방증거규칙을 통해 법적증거로서의 허용성 만족 여부가 판단된다. 2007년 미국의 Paul Grimm 판사는 Lorraine v. Markel 사건[9]의 판결문을 통해 기존의 연방증거규칙 조항들을 재해석함으로써 디지털 증거의 법적 허용성을 만족시키기 위한 조건들을 제시하였다. 가상머신 이미지가 디지털 증거로서 법적증거로 인정받기 위한 연방증거규칙 조항들로는 [표 3]과 같이 901조의 '신뢰성(Authenticity)', 902조의 '자기신뢰성(Self Authenticity)', 1001조의 '원문과의 동일성'이 존재한다.

서버 가상화 솔루션은 전문가 또는 신뢰할 수 있는 기관으로부터 가상머신 이미지의 생성과정 및 이에 대한 오류율, 정확성 등은 검증되지 않고 있어 가상머신 이미지는 Rule 901의 '신뢰성'을 인정받지 못한다. 또한 가상머신 이미지는 기존의 디지털 포렌식 도구를 이용한 디스크 이미지 생성과정과 달리 타임스탬프, 해쉬, 전자서명 등과 같은 정보들을 포함하지 않기 때문에 가상머신 이미지의 위・변조, 훼손 등에 대한 책임추적성이 보장되지 않으므로 Rule 902의 '자기 신뢰성'이 인정되지 않는다. 그리고 서버 가상화 솔루션에 대한 보안 요구사항 검증이 이루어지지 않고 있어 가상머신 이미지가 위・변조 및 훼손될 수 있기 때문에 Rule 1001의 '원본과의 동일성'을 보장하기 어렵다. 이와 같이 가상머신 이미지는 그 자체로서 미국 연방증거규칙의 허용성 기준들을 만족시키지 못한다는 것을 살펴볼 수 있다.

IV. 가상머신 이미지의 법적증거로서의 허용성 만족 조건

가상머신 이미지가 법적 증거로서의 허용성 기준들을 만족하기 위해서는 앞서 살펴보았던 서버 가상화 환경에서 나타날 수 있는 여러 가지 문제점들이 해결되어야 할 것이다. 이를 위해 서버 가상화 솔루션은 안전한 가상머신 이미지 생성을 위한 보안 요구사항들을 만족해야할 것이며, 이를 생성하는 과정을 검증받음으로써 디지털 포렌식 도구로서의 신뢰성을 인정받을 수 있을 것이다. 또한 가상머신 이미지 수집 과정에서의 법・제도적인 문제점들을 해결하기 위한 증거의 연계보관성 조건들이 만족된다면 가상머신 이미지는 법적 증거로 인정받을 수 있을 것이다.

4.1. 서버 가상화 기술의 보안 요구사항 만족

가상머신 이미지는 서버 가상화 솔루션에 나타날 수 있는 보안 위협들로 인해 위・변조 및 훼손될 가능성이 존재한다. 따라서 해당 솔루션에서 제공하는 가상머신 이미지가 법적증거로서 인정받기 위해서 기본적으로 아래 [표 4]와 같은 보안 요소들이 만족되어야 할 것이다.

4.1.1 완전한 격리

완전한 격리를 통해 서버 가상화 환경 내에 논리적으로 분리된 파티션 간 허가받지 않은 방법으로 수행되는

[표 4] 서버 가상화 환경에 요구되는 보안 요소

보안 요구사항	내 용
완전한 격리 (Perfect Isolation)	하이퍼바이저는 완전한 격리 기능을 제공함으로써 서버 가상화 환경 내 각 구성요소들 간에 서로 영향을 미치지 않도록 해야 한다. (☞ 보안위협 ①, ②, ⑤, ⑥)
식별 및 인증 (Identification & Authentication)	서버 가상화 솔루션은 사용자 및 연결 장치에 대한 식별 및 인증 기능을 제공해야 한다. (☞ 보안위협 ①, ②, ④, ⑤, ⑥, ⑦)
접근통제 (Access Control)	서버 가상화 솔루션은 물리적, 논리적 접근통제 기능을 제공해야 한다. (☞ 보안위협 ①, ②, ④, ⑤, ⑥, ⑦)
감사 (Auditing)	가상화 서버의 보안 위협에 대한 적절한 모니터링 및 보안 로그 수집을 통한 보안 감사 기능이 수행되어야 한다. (☞ 보안위협 ①, ②, ④, ⑤, ⑥)
암호화 (Encryption)	서버 가상화 환경에서 저장 및 전송되는 데이터는 암호화가 이루어져야 한다. (☞ 보안위협 ②, ⑤, ⑥)
복구 및 백업 (Recover & Backup)	서버 가상화 솔루션은 복구 및 백업 기능을 갖추어야 한다. (☞ 보안위협 ③, ④)

데이터의 전송 및 공유는 불가능하며, 각 파티션 내의 애플리케이션들은 다른 파티션의 메모리나 저장 공간 영역에 접근할 수 없다. 따라서 악의적인 목적의 이용자가 다른 가상머신의 이미지에 대한 위 · 변조 또는 훼손이 불가능하기 때문에 해당 이미지 파일의 무결성이 보장된다.

4.1.2 식별 및 인증

서터에 대버 가상화 솔루션은 해당 환경 내에 존재하는 각 구성요소들에 대한 사용자 및 해당 서버에 연결된 기타 부가장치들의 식별 및 인증 기능을 제공해야 한다. 식별 및 인증은 가상머신 이미지 뿐 아니라 기타 가상화 서버 내에 존재하는 데이한 접근통제 기능을 수행하기 위해 선행되어야 한다.

4.1.3 접근통제

서버 가상화 환경은 물리적 접근통제를 통해 호스트 서버의 훼손을 방지하고, 호스트 운영체제, 가상머신 운영체제 및 애플리케이션, 하이퍼바이저에 대한 사용자 역할기반(호스트 관리자, 가상머신 관리자, 일반 이용자 등), 주요 가상화 설정 파일 및 시스템 로그 정보와 같은 감사 데이터 등을 대상으로 한 데이터별(읽기, 쓰기, 변경) 접근권한 설정이 이루어져야 한다. 이와 같은 물리적, 논리적 접근통제를 통해 허가받지 않은 이용자의 가상머신 이미지 위 · 변조 및 삭제가 불가능하다.

4.1.4 감사

서버 가상화 솔루션은 가상머신의 생성·복제·이동·제거, 주요 데이터에 대한 접근, 각 구성요소들에 대한 환경설정 변경, 로그인 등 모니터링 및 로그 기록을 생성해야 하며, 이를 사용자 접근권한에 따라 제공으로써 가상머신 이미지의 위 · 변조 및 훼손을 예방하고 탐지할 수 있다.

4.1.5 암호화

서버 가상화 솔루션은 가상머신 내에 저장되는 주요 데이터 및 다양한 접근 경로를 통해 유입되는 패킷, I/O 요청 정보 등의 기밀성, 무결성 유지를 위한 암호화를 수행할 수 있어야 한다. 가상머신 이미지가 암호화됨으로써 네트워크를 통한 전송 과정에서 제3자에 의한 도청 및 위 · 변조를 방지할 수 있다.

4.1.6 복구 및 백업

서버 가상화 솔루션은 복구 및 백업 기능을 제공함으로써 각종 재해 등 가용성 침해 시 발생할 수 있는 가상머신 이미지의 위 · 변조 및 훼손을 방지할 수 있다.

4.2. 디지털 포렌식 수사 도구로서의 신뢰성 확보

가상머신 이미지가 법적 증거로 인정받기 위해서는 CFTT와 같이 가상머신 이미지를 생성하는 서버 가상

[표 5] Daubert Factor를 만족시키는 서버 가상화 솔루션 검증작업

Daubert Factor		내 용
1	해당 이론 또는 기술이 일반적으로 검증 가능한지(또는 검증되었는지) 여부	· 가상화, 디지털 포렌식 분야 전문가 및 관련 단체의 가상머신 이미지 생성 과정에 대한 공개 의견 · 서버 가상화 솔루션의 가상머신 이미지 테스트 S/W 공개 · 웹 페이지에 테스트 보고서 공개
2	해당 이론 또는 기술이 전문가에 의해 검증 또는 출판물로 제시되었는지 여부	· 가상머신 이미지 테스트 명세서 개발 과정에 관련 분야 및 법률 전문가 참여 · 가상화, 디지털 포렌식 분야 전문가 및 관련 단체의 가상머신 이미지 생성 과정에 대한 공개 의견 · 피드백을 명세서에 반영
3	해당 과학 기술이 현저히 낮은 오류율을 가지는지 여부	· 테스트 수행 - 서버 가상화 솔루션의 가상머신 이미지 생성 작업 반복 테스트
4	해당 방법론이 관련 학계에서 널리 인정받고 있는지 여부	· 가상화, 디지털 포렌식 분야 전문가 및 관련 단체의 가상머신 이미지 생성 과정에 대한 공개 의견 · 서버 가상화 솔루션의 가상머신 이미지 테스트 S/W 공개 · 검증 위원회의 보고서 검토 · 웹 페이지에 테스트 보고서 공개 ※ 상기 항목들을 인용한 각종 판례 및 연구 보고서

화 솔루션에 대한 과학적 검증 절차가 마련되어야 하며, 디지털 포렌식 도구로서의 역할을 충실히 수행할 수 있는지 Daubert Factor를 이용하여 신뢰성을 검증할 수 있어야 한다.

CFTT의 디지털 포렌식 도구 테스트 과정과 같이 서버 가상화 솔루션에 대한 과학적 검증작업은 가상머신 이미지 생성 기능 테스트에 요구되는 사항들의 명세화, 해당 분야의 전문가 및 관련 단체의 의견 수렴과 피드백 반영을 통한 테스트 환경 구축 및 S/W를 개발하는 단계를 거쳐 실제 테스트가 수행되어야 한다. 이러한 일련의 과정들의 결과물이 법정에서 Daubert Test의 각 항목들을 만족시키는지의 여부를 통해 신뢰성을 인정받을 수 있게 된다.

4.2.1 해당 이론 또는 기술이 일반적으로 검증 가능한지 (또는 검증되었는지) 여부

서버 가상화 솔루션들에 대한 검증작업은 가상화 및 디지털 포렌식 분야의 전문가와 관련 단체의 검토의견 수렴, 가상머신 이미지 생성 테스트 S/W를 공개함으로써 일반인들이 서버 가상화 솔루션의 검증작업을 실제로 수행해볼 수 있도록 한다. 또한 해당 도구의 사용자 및 이해관계자들이 참고할 수 있도록 테스트 결과 보고서를 웹 페이지에 공개한다. 이처럼 서버 가상화 솔루션에 대한 명세서 개발 단계부터 전문가~일반인에 이르는 다양한 사용자의 참여 유도, 테스트 S/W 및 환경을 제공함으로써 모든 사람들이 검증작업에 참여할 수 있도록 한다.

4.2.2 해당 이론 또는 기술이 전문가에 의해 검증 또는 출판물로 제시되었는지 여부

서버 가상화 솔루션의 가상머신 이미지 검증을 위한 명세서 개발과정에 컴퓨터 포렌식 전문가 및 법률 전문가를 참여시킴으로써 서버 가상화 솔루션에서 생성한 가상머신 이미지가 법적 증거로 인정받기 위한 기술적 · 법적 요구사항들을 만족시키는지 검토한다. 또한 이러한 결과물에 대해 가상화, 디지털 포렌식 분야의 전문가 및 관련 단체의 검토가 이루어지고 이들의 의견이 웹 페이지를 통해 공개되며 향후 명세서에 반영된다.

4.2.3 해당 과학 기술이 현저히 낮은 오류율을 가지는지 여부

서버 가상화 솔루션의 테스트는 가상머신 이미지 생성 기능의 반복 테 해당스트 과정을 거쳐 발생할 수 있는 오류를 식별하고, 오류에 대한 대응이 어떻게 이루어지고 있는지 기록하는 일련의 과정을 거친다. 서버 가상

화 솔루션에 대한 테스트 반복 횟수 및 결과는 테스트 보고서를 통해 공개된다.

4.2.4 해당 방법론이 관련 학계에서 널리 인정받고 있는지 여부

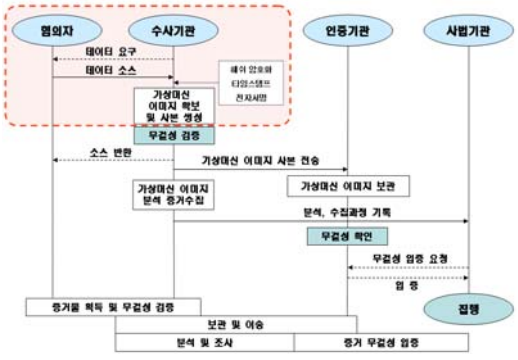
도구의 검증 방법론 개발 단계부터 실제 테스트 과정에 이르기까지 관련 커뮤니티 및 단체의 의견을 수렴하며, 최종 테스트 결과 보고서는 디지털 포렌식 및 가상화 기술 분야의 전문가들로 구성된 위원회에 의해 검토된다. 이러한 결과는 최종적으로 웹 페이지에 공개됨으로써 관련 연구 보고서 또는 판례에 인용될 수 있다.

4.3 가상머신 이미지의 연계보관성(Chain of Custody) 조건 만족

기존의 디지털 증거 수집 · 분석과정에서 별도의 디스크 이미지 생성 및 인증기관을 통해 무결성을 검증받았던 것과 달리, 서버 가상화 솔루션에서 해쉬 암호화, 타임스탬프 기능을 제공함으로써 가상머신 이미지 생성과정에서의 무결성을 보장받을 수 있다. 또한 전자서명을 통해 가상머신 이미지를 생성한 자의 책임추적성을 제공함으로써 가상머신 이미지가 법적 증거로서 신뢰성을 인정받을 수 있을 것이다.

4.4 가상머신 이미지의 법적 허용성 기준 만족을 위한 추진체계

지금까지 서버 가상화 환경에서 수집한 가상머신 이미지가 법적증거로서의 허용성을 만족시키기 위한 조건



[그림 5] 가상머신 이미지의 연계보관절차

[표 6] 가상머신 이미지의 법적 허용성 만족 여부

Rule	내 용
Rule 901(b)(1) Rule 901(b)(3) Rule 901(b)(9)	서버 가상화 솔루션은 관련 분야의 전문가 또는 검증기관들로부터 반복 테스트를 통해 가상머신 이미지 생성 과정의 현저히 낮은 오류율과 정확성을 검증받고, 보안 요구사항들을 만족시킴으로써 가상머신 이미지의 위·변조 및 훼손을 방지하여 법적 허용성을 인정받을 수 있다.
Rule 902(7)	가상머신 이미지 생성과정에서 타임스탬프, 해쉬, 전자서명과 같은 부가적인 정보를 포함시킴으로써 가상머신 이미지 파일 자체로서의 무결성 및 책임추적성을 만족시킬 수 있기 때문에 법적 증거로서 신뢰성을 인정받을 수 있다.
Rule 1001	서버 가상화 솔루션의 타임스탬프 및 해쉬 기능, 보안 요구사항들의 검증작업을 통해 가상머신 이미지의 위·변조 또는 훼손을 방지할 수 있다. 따라서 가상머신 이미지는 원본 가상머신 시스템과 동일하다고 인정받을 수 있다.

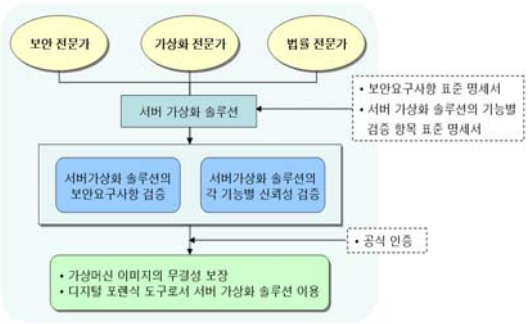
들을 살펴보았으며, [표 6]을 통해 살펴볼 수 있듯이 가상머신 이미지가 실제로 이와 같은 조건들을 만족시킬 때 미국 연방증거규칙에 의거하여 법적증거로 인정받을 수 있는 것으로 나타났다.

서버 가상화 솔루션에 요구되는 여러 가지 조건들이 갖추어지기 위해서는 여러 관련 기관들의 공동 노력이 필요하다. 정부, 수사기관, 법원, 서버 가상화 솔루션 벤더와 이를 이용하는 기업들은 다음과 같은 구체적인 역할 및 세부 계획들을 수행할 수 있어야 한다.

4.4.1 정부

정부는 서버 가상화 솔루션의 가상머신 이미지 생성과정의 신뢰성 및 보안 요구사항들을 만족시키는지 테스트하는 검증기관을 구축하고 운영해야 한다.

서버 가상화 솔루션 검증기관은 해당 솔루션에서 나타날 수 있는 보안 위협들에 의해 가상머신 이미지가 위 · 변조 또는 훼손 되는 것을 방지하기 위한 보안 요구사항들을 검증하며, 서버 가상화 솔루션이 수행하는 각각의 세부 기능들에 대한 테스트를 통해 신뢰성을 검증하는 역할을 한다. 이러한 검증기관은 가상화 기술뿐만 아니라 디지털 포렌식 기술 및 법률 지식을 갖춘 전문



[그림 6] 서버 가상화 솔루션 검증제도

가들로 구성되어 운영되어야 하며, 서버 가상화 솔루션에 대한 보안 요구사항, 디지털 포렌식 도구로서의 신뢰성 검증절차 및 항목들이 구체화된 표준 명세서를 개발하여 활용함으로써 가상머신 이미지의 무결성 및 신뢰성을 공식적으로 인증하는 제도를 갖추어야 한다.

4.4.2 수사기관

서버 가상화 환경은 기존의 물리적 서버 환경과 구조적인 차이점을 가지기 때문에 수사관이 가상머신 이미지를 수집하기 위해서는 서버 가상화 환경을 명확히 이해할 수 있어야 하며, 동 환경에 대한 정형화된 압수 · 수색 원칙 및 절차가 마련되어야 할 것이다. 또한 가상머신 이미지를 수집, 분석, 제출하는 단계까지 연계보관성을 보장하기 위한 해쉬값, 타임스탬프 생성과 비교 등 일련의 절차 및 방법론이 마련되어야 한다.

4.4.3 서버 가상화 솔루션 벤더

서버 가상화 솔루션 벤더는 가상머신 이미지의 위·변조 및 훼손을 방지하기 위해 해당 솔루션에 보안 요구사항들을 만족시키는 기술적 보안조치를 취해야 하며, 가상머신 이미지 생성 시 해쉬 암호화, 타임스탬프, 전자서명 등의 기능을 추가함으로써 가상머신 이미지의 무결성 및 책임추적성을 보장할 수 있어야 한다. 또한 각 벤더 간 가상머신 이미지 생성 프로세스 및 관련 기술을 표준화함으로써 서버 가상화 환경에서의 보다 원활한 디지털 포렌식 수사가 이루어질 수 있도록 해야 한다.

[표 7] 서버 가상화 솔루션에 대한 각 기관별 추진계획

목 표				
서버 가상화 솔루션에 대한 디지털 포렌식 수사과정에서 수집 가능한 가상머신 이미지의 법적증거로서의 허용성 만족				
각 기관별 추진 체계				
정부	수사기관	서버 가상화 솔루션 벤더	서버 가상화 솔루션 이용 기업	법원
서버 가상화 솔루션 검증기관 구축 및 운영	서버 가상화 환경에 대한 압수, 수색 및 가상머신 이미지 수집 원칙·절차 마련	서버 가상화 솔루션에 가상머신 이미지의 무결성, 책임추적성 보장 장치 추가	가상머신 이미지에 대한 접근통제 수단 마련	가상머신 이미지의 법적증거로서의 허용성 기준 마련
서버 가상화 솔루션에 대한 보안 요구사항 검증제도 도입 및 시행	가상머신 이미지의 연계보관성 보장 방안 마련	가상머신 이미지 생성 및 기타 기능에 대한 벤더 간 표준화 작업	가상머신 이미지 위·변조 및 훼손에 대비한 백업 및 복구 대책 수립	
세부 추진 계획				
· 각 검증기관은 가상화 기술, 디지털 포렌식, 보안, 법률 등 각 분야별 전문가로 구성	· 수사관들의 서버 가상화 환경에 대한 디지털 포렌식 원칙 및 절차 숙지	· 서버 가상화 솔루션의 가상머신 이미지 생성 시 해쉬 암호화, 타임스탬프, 전자서명 기능 추가	· 가상화 서버에 대한 허가받지 않은 사용자의 물리적, 논리적 접근 통제	· 디지털 증거의 명확한 개념 정의 및 디지털 증거로서 가상머신 이미지의 법적 허용성 기준 마련
· 서버 가상화 솔루션의 보안 요구사항 및 디지털 포렌식 도구로서의 신뢰성 항목 명세서 표준화	· 가상머신 이미지 수집, 분석 시점에서의 해쉬값 및 타임스탬프 비교	· 여러 서버 가상화 솔루션들의 가상머신 이미지 생성 기능 표준화	· 각종 재해 및 침입 피해로 인한 가상머신 이미지 위·변조 및 훼손에 대한 백업 및 복구정책 수립	· 서버 가상화 환경에 대한 압수·수색 영장 작성 기준 마련

4.4.4 서버 가상화 솔루션 이용 기업

서버 가상화 솔루션을 도입하여 활용하고 있는 기업 또는 조직은 가상머신 이미지가 위·변조 및 훼손되지 않도록 해당 시스템에 대한 물리적, 논리적 접근통제를 수행해야할 것이며, 각종 자연재해 및 시스템 침입·강제종료로 인한 가상머신 이미지 훼손에 대비한 백업 및 복구정책을 수립하고 운영할 수 있어야 한다.

4.4.5 법원

법원은 가상머신 이미지가 법적증거로서의 허용성을 인정받기 위한 기준을 마련하고, 해당 증거가 이를 만족시키는지의 여부를 판단할 수 있어야 한다. 또한 판사는 서버 가상화 환경을 명확하게 숙지하고 적법절차의 원칙에 근거한 압수·수색이 이루어지도록 영장을 발부할 수 있어야 한다.

4.5 비교 분석 및 평가

기존의 물리적 서버 환경과 서버 가상화 환경에서의 이미지 증거 수집과정 간의 차이점은 [표 8]과 같이 나타나며, 이를 구체적으로 살펴보면 다음과 같다.

4.5.1 수사준비

일반적으로 디지털 증거의 획득은 수집된 디스크 매체로부터 대상 데이터를 복제한 후, 이를 이용하여 검색 및 분석하는 등 일련의 표준화된 수사 절차와 원칙을 통해 이루어지며 신뢰성 있는 증거의 확보를 위해 검증된 도구의 사용이 요구된다. 이를 위해 국내 정보통신단체(TTA) 표준에 의거하여 1년에 1번씩 디지털 포렌식 도구에 대한 검증작업이 수행되고 있으며, 해당 포렌식 도구를 이용하여 수집된 디지털 증거는 법적 증거로 인정받고 있다. 하지만 서버 가상화 환경의 경우, 가상머신 이미지 위·변조 및 무결성 방지를 위한 서버 가상화 솔루션의 가상머신 이미지 생성 기능에 대한 검증 작업은 이루어지지 않고 있다.

4.5.2 증거물 수집

기존의 물리적 서버 환경에서의 증거물 수집은 범죄현장에서 수집 대상을 신속하고 효율적으로 획득하기 위해 범죄 유형 및 확보해야할 정보를 파악하고, 디지털 증거가 존재한다고 판단되는 물리적 장치를 확보하는 과정으로 이루어진다. 또한 디지털 포렌식 도구를 이용하여 디스크의 이미지를 수집한 후 이에 대한 해쉬 암호화를 통해 무결성 및 객관성을 인증 받아 법적증거로 활용할 수 있다. 서버 가상화 환경의 경우, 해당 서버 가상화 솔루션이 각 가상머신 이미지의 생성 기능을 기본적으로 제공하고 있기 때문에 별도의 디스크 이미징 작업을 생략할 수 있다는 점에서 신속하고 효율적인 수사가 가능하다. 하지만 서버 가상화 솔루션에서 가상머신 이미지의 무결성 확보를 위한 기술적 지원이 이루어

[표 8] 기존의 물리적 서버와 서버 가상화 환경에서의 증거수집 과정 비교

수사 절차	기존의 물리적 서버 환경	서버 가상화 환경	비 교
수사준비	· 포렌식 툴 검증 · 장비 확보 · 협조체계 확립	· 서버 가상화 솔루션 검증 · 장비 확보 · 협조체계 확립	· 가상머신 이미지의 위·변조 및 훼손을 방지하기 위해 서버 가상화 솔루션의 이미지 생성과정에 대한 신뢰성 및 보안 요구사항 만족 여부 검증 필요
증거물 수집	· 현장분석 · 활성 데이터 수집 · 디스크 이미징 · 이미지 증거 인증	· 현장분석 · 가상머신 이미지 수집 · 가상머신 이미지 인증	· 서버 가상화 솔루션에서 각 가상머신 이미지 생성 기능을 제공하기 때문에 기존의 포렌식 툴을 이용한 별도의 디스크 이미지 생성 과정 생략 가능 · 서버 가상화 솔루션의 가상머신 이미지 생성과정에서 해쉬, 타임스탬프 기능 제공을 통해 1차적인 무결성 검증 가능
보관 및 이송	· 이미지 복사 · 증거물 포장 및 운반	· 가상머신 이미지 복사 · 가상머신 이미지 전송	· 서버 가상화 솔루션에서 해당 가상머신 이미지에 대한 전자서명 기능을 제공함으로써 복사, 보관 및 이송 과정에서 연계보관성 보증

지고 있지 않기 때문에 해당 이미지 파일은 법적 증거로 인정받지 못한다는 문제점이 있다.

4.5.3 보관 및 이송

기존의 물리적 서버 환경에서 수집된 디스크 이미지는 쓰기 방지 장치를 이용하여 원본의 변경 없이 복제된 후 해쉬값 비교를 통해 위・변조 여부가 확인된다. 또한 해당 디스크 이미지의 이송 과정에 대한 책임자, 관리자, 일시, 장소 등의 기록이 문서화됨으로써 증거의 연계보관성이 보증된다. 하지만 서버 가상화 솔루션은 가상머신 이미지의 생성자, 보관 및 이송 과정에서의 책임추적성을 보장하는 기본적인 수단을 제공하지 않기 때문에 가상머신 이미지는 그 자체로서 법적 허용성을 인정받지 못한다.

4.5.4 평가

각 과정에서 살펴본 문제점들로 인해 가상머신 이미지는 물리적 서버 환경에서의 디스크 이미지와 달리 법적증거로서의 허용성을 인정받지 못한다는 것을 알 수 있었다. 하지만 본 논문에서 제시한 서버 가상화 솔루션에 대한 보안 요구사항 및 신뢰성의 검증, 가상머신 이미지의 복제 및 이송 시 연계보관성을 보장해주는 기술적인 장치들이 추가된다면 가상머신 이미지의 위・변조 및 훼손 방지와 같은 기본적인 무결성 및 책임추적성이 보장되어 증거로서의 객관성 및 허용성 조건들을 인정받을 수 있을 것으로 기대된다. 또한 이러한 조건들이 현실적으로 반영되기 위해서는 서버 가상화 환경에 대한 디지털 포렌식 수사와 관련된 정부, 수사기관, 서버 가상화 솔루션 벤더 및 이를 이용하는 기업, 법원과 같은 사회 각 주체들이 각각의 역할에 따른 세부 계획들을 수행할 수 있어야 함을 살펴볼 수 있다.

Ⅴ. 결 론

앞서 살펴본 것처럼 일반적으로 기존의 물리적 서버 환경에 대한 디지털 포렌식 수사는 해당 서버의 디스크 이미지 수집 ・ 분석을 통해 획득한 증거를 법정에 제출하는 방식으로 이루어졌다. 이에 반해 서버 가상화 환경에서는 서버 가상화 솔루션이 기본적으로 제공하는 가상머신 이미지를 수집 ・ 분석하여 기존의 디스크 이미지 수집 과정을 생략할 수 있기 때문에 보다 신속하고 효율적인 수사가 이루어질 수 있다. 하지만 서버 가상화 환경에서 호스트, 가상머신, 하이퍼바이저와 같은 각각의 구성요소들에 대한 보안위협들로 인해 가상머신 이미지가 위・변조 및 훼손될 위험이 있으며, 서버 가상화 솔루션의 가상머신 이미지 생성 과정에 대한 객관적 검증작업이 이루어지지 않고 있기 때문에 해당 서버 가상화 솔루션이 디지털 포렌식 도구로서 신뢰성을 인정받지 못하는 문제점이 있다. 또한 서버 가상화 환경이 가지는 기존의 물리적 서버환경과의 구조적 차이점들로 인해 가상머신 이미지의 압수・수색 과정에서 적법절차의 원칙 준수, 증거의 수집 및 보관 과정에서의 연계보관성 보장 등의 문제들이 발생할 수 있다. 따라서 이러한 문제점들로 인해 현재 서버 가상화 환경에서 수집되는 가상머신 이미지는 법적증거로서의 허용성 기준들을 만족시키지 못하기 때문에 증거로 인정받지 못한다.

본 논문에서는 가상머신 이미지가 법적증거로서의 허용성 기준들을 만족시키기 위한 조건들을 제시하였다. 먼저, 서버 가상화 솔루션이 완전한 격리, 식별 및 인증, 접근통제, 감사, 암호화, 복구 및 백업과 같은 보안 기능들을 갖춤으로써 가상머신 이미지의 위・변조 및 훼손을 방지하여 무결성을 보장받을 수 있으며, 서버 가상화 솔루션의 가상머신 이미지 생성과정에 대한 검증체계를 구축함으로써 디지털 포렌식 도구로서의 신뢰성을 인정받기 위한 Daubert Test 항목들을 만족시킬 수 있음을 살펴보았다. 또한 서버 가상화 솔루션이 가상머신 이미지의 생성 및 보관과정에서 해쉬, 타임스탬프, 전자서명 등의 기능을 제공함으로써 수사관의 가상머신 이미지 수집 시 무결성, 책임추적성을 보장받아 증거의 연계보관성 조건을 만족시킬 수 있는 것으로 나타났다.

마지막으로 서버 가상화 환경에 대한 효율적인 디지털 포렌식 수사를 위해 앞서 살펴본 조건들이 실제 환경에서 적용될 수 있도록 정부, 수사기관, 서버 가상화 솔루션 벤더, 서버 가상화 솔루션 이용 기업, 법원과 같은 관련 기관들에 요구되는 역할 및 세부추진계획안을 담고 있는 서버 가상화 환경에서의 디지털 포렌식 정책 프레임워크를 제시함으로써 가상머신 이미지가 법적증거로서 허용성을 인정받기 위해 나아가야할 보다 구체적인 정책 방향을 보여준다.

추후 연구로 본 논문에서 제시한 서버 가상화 환경의 디지털 포렌식 정책 프레임워크를 구체화할 것이며, 서버 가상화 솔루션에 요구되는 요구사항들의

명세화를 통해 가상머신 이미지가 법적증거로서의 허용성 기준 만족도를 객관적으로 측정할 수 있는 방안에 대한 연구를 진행할 예정이다.

참고문헌

[1] IDC, “irtualization and Multi-core Innovations Disrupt the Worldwide Server Market” March 2007.

[2] A. Arnes, P. Haas, G. Vigna, R. Kemmerer, “Digital Forensic Reconstruction and the Virtual Security Testbed ViSe”, Vol.4064. 2006.

[3] D.Bem, E. Huebner, “Computer Forensic Analysis in a Virtual Environment”, International Journal of Digital Evidence, 6(2), Fall 2007.

[4] D. Bem, E. Huebner, “Analysis of USB Flash Drives in a Virtual Environment”, Small Scale Digital Device Forensics Journal, 1(1), June 2007.

[5] J. Smith, R. Nair, Virtual Machines, Elsevier, 2005, p.370

[6] U.S. Federal Rules of Evidence http://www.uscourts.gov/rules/Evidence_Rules_2007.pdf

[7] NIST, “Digital Forensics at the National Institute of Standards and Technology, NISTIR 7490”, 2008.4.

[8] IDC, “Worldwide Virtual Machine Software 2008-2012 Forecas”, May 2008.

[9] Lorraine v. Markel American Insurance Co., U.S. Dist. LEXIS 33020(D. Md.), May 2007.

[10] 이규안, 박대우, 신용태, “포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구”, 한국컴퓨터정보학회 2006동계학술발표논문집 &학회지, 14(2), December 2006.

[11] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 1993.

[12] S. Garfinkel, “nti-Forensics: Techniques, Detection and Countermeasures” Proceeding of The 2nd International Conference on i-Warfare and Security, 2007.

[13] Jesse D. Kornblum, “xploiting the Rootkit Paradox with Windows Memory Analysis” International Journal of Digital Evidence, 2006.

[14] 한국정보통신기술협회(TTA), “컴퓨터 포렌식 가이드라인(정보통신단체표준 TTAS.KO-12.0058)”, 2007.

[15] 한국 IBM 시스템테크놀로지그룹, 가상화 기술의 새로운 패러다임, 한국경제신문, 2007.

[16] 오기두, “형사절차상 컴퓨터 관련증거의 수집 및 이용에 관한 연구”, 서울대학교 학위논문, 1997.

[17] United States Department of Justice, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, July 2002.

[18] NIST Computer Forensic Tool Testing Program, http://www.cftt.nist.gov

[19] 김동희, 백승조, 심미나, 임종인, “가상서버 시스템의 안전한 하이퍼바이저 설계에 요구되는 보안 요소”, 한국정보보호학회 2007동계학술대회, 17(2), pp.661~666, 2007.

<著者紹介>

김 동 희 (Dong-Hee Kim) 학생회원
2007년 2월 : 단국대학교 경영정보학과 졸업
2007년 3월~현재 : 고려대학교 정보경영공학전문대학원 석사과정
<관심분야> 개인정보보호, 정보보호 정책, 디지털 포렌식

백 승 조 (Seung-Jo Baek) 학생회원
2005년 2월 : 세종사이버대학교 정보보호학과 졸업
2007년 9월 : 고려대학교 정보경영공학전문대학원 석사 학위 취득
2007년 10월~현재 : 고려대학교 정보경영공학전문대학원 박사 과정
<관심분야> 정보법학, 개인정보보호, 지적재산권, 디지털 포렌식, 위험관리

심 미 나 (Mina Shim) 학생회원
1996년 2월 : 성신여자대학교 전산학과 졸업
2006년 2월 : 고려대학교 정보보호대학원 석사 학위 취득
2008년 2월 : 고려대학교 정보경영공학전문대학원 박사 수료
<관심분야> 개인정보보호, 정보보호영향평가제도, 의료정보보호, 정보보호법제

임 종 인 (Jong-In Lim) 종신회원
1980년 2월 : 고려대학교 수학과 졸업
1982년 2월 : 고려대학교 수학과 석사 학위 취득
1986년 2월 : 고려대학교 수학과 박사 학위 취득
1986년 3월~2001년 1월 : 고려대학교 자연과학대학 정교수
2001년 2월~현재 : 고려대학교 정보경영공학전문대학원 원장, 고려대학교 정보보호기술연구센터 센터장
<관심분야> 정보법학, 디지털 포렌식, 개인정보보호, 전자정부보안, E-Discovery