情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

가상 데스크톱 환경에 대한 디지털 포렌식 연구*

장 상 희,[1†] 김 등 화,[1] 박 정 흠,[1] 강 철 훈,[2] 이 상 진[1‡]
[1]고려대학교 정보보호대학원, [2]대검찰청 디지털수사담당관실

Digital Forensic Investigation of Virtual Desktop Infrastructure*

Sanghee Jang,[1†] Deunghwa Kim,[1] Jungheum Park,[1] Cheulhoon Kang,[2] Sangjin Lee[1‡]
[1]Center for Information Security Technologies(CIST), Korea University,
[2]Digital Forensic Center, Supreme Prosecutors' Office

요 약

클라우드 컴퓨팅은 최근 IT 시장에서 가장 큰 성장을 보이고 있는 분야 중 하나로, 앞으로도 지속적으로 성장할 것으로 기대되고 있다. 특히, 최근에는 수많은 기업들이 비용 절감 및 효율 향상을 위해 사설 클라우드 컴퓨팅 서비스로 가상 데스크톱 환경을 도입하고 있다. 하지만 현재 이 분야에 대한 디지털 포렌식 조사 절차 및 방법은 학문적, 기술적으로 체계화되어 있지 않다. 이를 위해서는 클라우드 컴퓨팅 서비스 형태에 따라 법적 효력을 가질 수 있는 디지털 증거 수집 체계를 확립해야 한다. 본 논문에서는 사설 클라우드 서비스로 제공되는 가상 데스크톱 환경 및 전 세계적으로 가장 많이 사용되고 있는 데스크톱 가상화 솔루션(Citrix, VMware, Microsoft)에 대해 소개하고, 각 솔루션에 대한 디지털 포렌식 조사 절차 및 방법을 제안한다.

ABSTRACT

Recently, cloud computing is one of the parts showing the biggest growth in the IT market and is expected to continue to grow into. Especially, many companies are adopting virtual desktop infrastructure as private cloud computing to achieve in saving the cost and enhancing the efficiency of the servers. However, current digital forensic investigation methodology of cloud computing is not systematized scientifically and technically. To do this, depending on the type of each cloud computing services, digital evidence collection system for the legal enforcement should be established. In this paper, we focus on virtual desktop infrastructure as private cloud computing and introduce the most widely used around the world desktop virtualization solutions of VMware, Citrix, and Microsoft. And We propose digital forensic investigation methodology for private cloud computing that is constructed by these solutions.

Keywords: cloud computing forensics, desktop virtualization forensics, citrix, vmware, hyper-v

I. 서 론

클라우드 컴퓨팅은 데이터와 응용 프로그램을 유지 및 관리하기 위해 인터넷과 원격 서버를 사용하는 기술로써, NIST에서는 "네트워크, 서버, 스토리지, 응용프로그램 등과 같은 컴퓨팅 자원들이 공유된 풀에 언제든지 편리하게 네트워크로 접근 가능한 방식의 모델이라고 정의하고 있다[1].

접수일(2012년 10월 22일), 수정일(2013년 1월 9일), 게재확정일(2013년 1월 28일)
* 본 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, lt-jsh@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

클라우드 컴퓨팅은 최근 IT 시장에서 가장 큰 성장을 보이고 있는 분야 중 하나로, 수많은 기업들이 비용 절감 및 효율 향상을 위해 사설 클라우드 컴퓨팅 서비스로 가상 데스크톱 환경을 도입하고 있다. 주로 기업 내부용으로 사용되는 사설 클라우드 컴퓨팅은 기업 내부에 가상화 기술을 이용한 클라우드 서버를 구축하여, 물리적 자원을 내부 사용자들에 한하여 공유 및 사용하는 것이다[2]. Gartner에서 분석가로 활동중인 Bittman은 2012년에 사설 클라우드 컴퓨팅 도입이 전년 대비 10배 증가하였다고 발표하였다[3]. 클라우드 서비스의 도입으로 기업은 내부 운영비를 절감하고, 사용자들은 "Any Device, Any Where, Any Time"이라는 장점을 활용하여 효율적인 업무 수행이 가능해졌다.

이처럼 클라우드 컴퓨팅 서비스 도입 및 사용이 지속적으로 증가하고 있지만, 현재 이 분야에 대한 디지털 포렌식 조사 절차 및 방법은 미흡한 실정이다. 클라우드 컴퓨팅 환경에서는 기존 데스크톱 컴퓨터 환경과 달리 사용자의 행위 및 데이터가 로컬 시스템에 거의 남지 않으며, 대부분 하이퍼바이저에 연결된 스토리지에 저장된다. 따라서 클라우드 컴퓨팅 서비스를 이용하는 사용자의 컴퓨터를 조사할 때 기존 디지털 포렌식 조사 절차 및 방법으로는 한계가 있으며, 클라우드 컴퓨팅 환경에 적용 가능한 새로운 절차 및 방법이 필요하다.

본 논문에서는 사설 클라우드 서비스로 제공되는 가상 데스크톱 환경 및 전 세계적으로 가장 많이 사용되고 있는 데스크톱 가상화 솔루션[16](Citrix, VMware, Microsoft)에 대해 소개하고, 솔루션들의 구조적 특징 및 기능을 이용하여 사용자 흔적 탐색, 사용자와 가상머신의 연결정보 확인 및 데이터 수집에 대한 디지털 포렌식 조사 절차 및 방법에 대해 제안한다.

II. 가상 데스크톱 환경

2.1 데스크톱 가상화 솔루션

일반적으로 가상화는 서버 가상화와 데스크톱 가상화로 나누어지며, 사설 클라우드 컴퓨팅에서 사용자에게 제공되는 것은 가상 데스크톱 환경(이하 VDI, Virtual Desktop Infrastructure)이다. 최근 가상화 전문 관리 업체인 Veeam에서 시장 조사 기관인 Vanson Bourne에 의뢰하여 조사한 결과, VMware가 전체 가상화 시장의 58%, Citrix가 20.2%, Microsoft가 18.6%의 시장 점유율을 가지고 있는 것으로 조사 되었으며, Citrix와 Microsoft의 시장 점유율이 매년 확대되고 있는 것으로 분석 되었다[4]. 이 솔루션들은 다양한 기능을 가진 여러 개의 프로그램으로 구성되어 있으며, VDI 환경을 구성하기 위해서는 기본적으로 다수의 가상머신이 호스트 서버의 자원을 공유하여 동시에 구동시킬 수 있는 하이퍼바이저가 필요하다. 각 솔루션별로 사용되는 하이퍼바이저는 Citrix XenServer, VMware ESX/ESXi Server, Microsoft Hyper-V이다. VDI 환경은 하이퍼바이저를 기반으로 하여 가상머신을 사용자에게 할당, 연결 및 관리하는 역할로 Citrix XenDesktop, VMware View, Microsoft Hyper-V가 사용된다.

하이퍼바이저와 데스크톱 가상화 솔루션은 VDI 환경을 구성하는 기본 솔루션이며, 실제로는 관리 및 사용의 효율성과 편의성을 위해 이 외의 다양한 프로그램들을 사용하고 있다. [표 1]은 본 논문에서 사용한 각 솔루션의 버전이다.

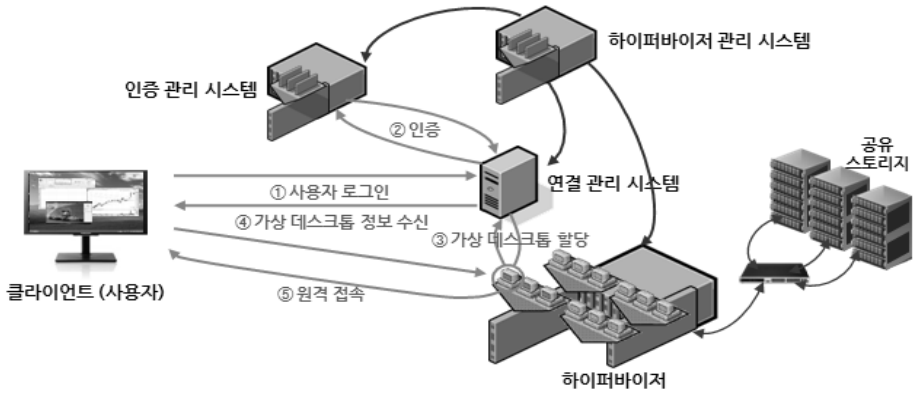
2.2 가상 데스크톱 환경 구성

VDI 환경을 구성하는 하이퍼바이저와 데스크톱 가상화 솔루션은 제조사별로 서로 다르지만, 구성 방식은 거의 동일하다. 간단하게 구성을 살펴보면, 기본적으로 가상머신을 생성하고 이를 관리할 수 있는 하이퍼바이저 및 하이퍼바이저 관리 시스템이 필요하다. 가상머신 및 사용자 데이터가 저장되는 스토리지는 하이퍼바이저의 로컬 디스크를 사용할 수도 있지만, 일반적으로는

별도의 대용량 공유 스토리지를 사용한다. 그리고

[표 1] 하이퍼바이저 및 데스크톱 가상화 솔루션 버전

구 분	Citrix	VMware	Microsoft
하이퍼바이저	XenServer 6.0	ESXi Server 5.0	Hyper-V (Windows Server 2008 R2)
데스크톱 가상화 솔루션	XenDesktop 5.6	View 5.0	Hyper-V (Windows Server 2008 R2)



〔그림 1〕 일반적인 VDI 환경 구성

사용자의 가상머신 접속 요청 시, 사용자 인증, 가상머신 할당 및 연결을 위해 인증 관리 시스템과 연결 관리 시스템이 필요하다.

위의 구성 요소들을 이용한 VDI 환경 구성이 완료면 사용자는 솔루션별 전용 프로그램 또는 웹을 통해 가상머신에 접속할 수 있다. 사용자가 가상머신에 접속하는 과정은 다음과 같다. ①사용자가 가상머신에 접속하기 위해 연결 관리 시스템에 접속 요청(로그인)을 보내면, ②연결 관리 시스템은 사용자 정보를 인증 관리시스템에 보내 사용자 인증을 한다. ③사용자 인증이 정상적으로 처리되면 연결 관리 시스템에서 사용자의 가상머신이 있는 하이퍼바이저에 가상머신 사용을 요청 및 할당 받아, ④사용자에게 전달한다. 마지막으로 사용자는 전달 받은 가상머신을 일반적인 데스크톱과 동일하게 사용하면 된다.

〔그림 1〕은 일반적인 VDI 환경 구성을 나타낸 것이며, 〔표 2〕는 솔루션별 VDI 환경을 구성하는 각 요소를 정리한 것이다.

III. 가상 데스크톱 환경에 대한 디지털 포렌식 조사 절차

VDI 환경에서 사용자 흔적은 가상머신에 접속하여 가상머신을 전달받는데 사용되는 모든 시스템에 기록된다. 따라서 VDI 환경에 대한 디지털 포렌식 조사는 사용자의 가상머신 접속 과정에 기반하여 수행되어야 한다. 〔그림 2〕는 VDI 환경을 고려한 디지털 포렌식 조사 절차를 나타낸 것이다.

VDI 환경에 대한 디지털 포렌식 조사 시 가장 먼저 해야 할 일은 용의자로 의심되는 사용자의 컴퓨터

〔표 2〕 솔루션별 VDI 환경 구성 요소

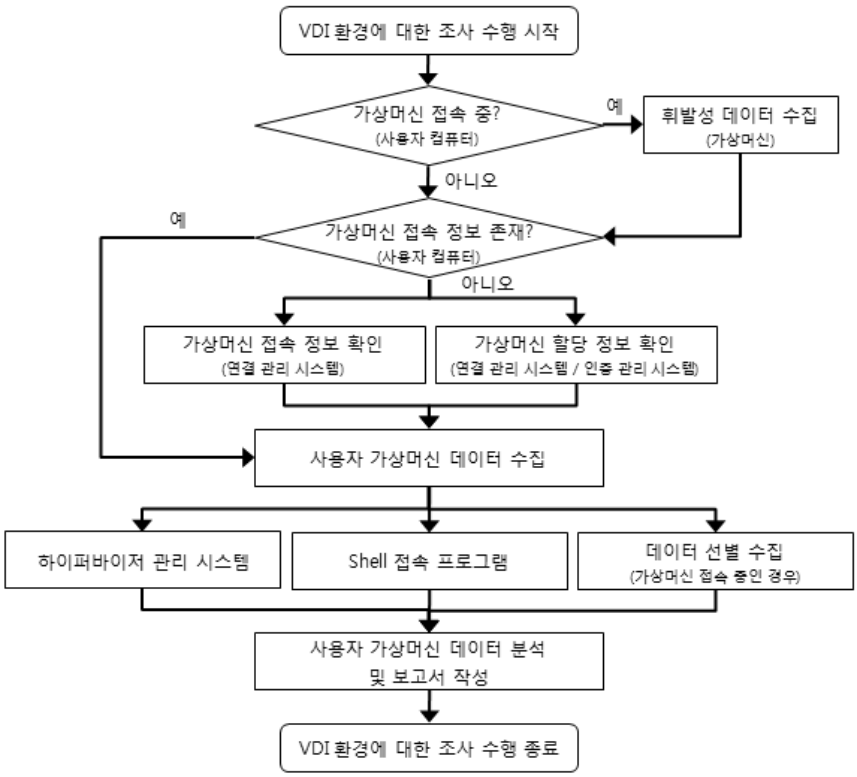
구 분	Citrix	VMware	Microsoft	설 명
하이퍼바이저	XenServer	ESX/ESXi Server	Hyper-V	가상머신 생성 및 관리
하이퍼바이저 관리 시스템	XenCenter	vCenter Server	SCVMM (System Center Virtual Machine Manager)	하이퍼바이저 통합 관리
연결 관리 시스템	DDC (Desktop Delivery Controller)	View Manager	RDCM (Remote Desktop Connection Manager)	가상머신 할당 및 연결
인증 관리 시스템	Active Directory	Active Directory	Active Directory	사용자 등록, 삭제 및 인증
가상머신 접속 프로그램	웹 접속 (Citrix Receiver 설치 필요)	View Client 또는 웹 접속	웹 접속	가상머신에 접속

에서 가상머신 접속 여부를 확인하는 것이다. 이 때, VDI 환경은 기업 내부에서 제한된 사용자에게 제공되는 사설 클라우드 서비스로 용의자로 의심되는 사용자를 구별할 수 있다고 가정한다. 만약 사용자가 가상머신에 접속 중이라면 휘발성 데이터 수집을 통해 더 많은 정보를 획득할 수 있다. 가상머신에 접속 중이 아니라면 먼저 사용자의 컴퓨터에서 가상머신에 접속한 흔적을 확인하여야 한다. 사용자가 가상머신에 접속했다면, 사용자의 컴퓨터에 레지스트리, 웹 히스토리 및 로그 기록이 남겨져 있을 것이다. 하지만, 이러한 정보들이 삭제된 경우에는 사용자의 컴퓨터에서 가상머신 접속 정보를 획득하기 어렵다. 만약, 가상머신 접속 정보를 획득할 수 없는 경우에는 연결 관리 시스템 및 인증 관리 시스템에서 사용자와 가상머신 간의 할당 및 접속 정보를 확인하여야 한다. 이를 위해서는 각 시스템에 접속하기 위한 관리자 권한(ID, Password)이 필요하다.

위의 조사를 통해 사용자가 사건 발생 추정 시간에 가상머신을 사용한 흔적을 확인한 후에는 가상머신의 데이터를 수집하여야 한다. 조사관은 솔루션별로 제공되는 Shell 접속 프로그램을 통해 가상머신 데이터를 수집할 수 있다. 이를 위해서는 하이퍼바이저 또는 하이퍼바이저 관리 시스템에 접속하기 위한 관리자 권한이 필요하다. 만약, 사용자가 가상머신에 접속 중이었다면 바로 데이터를 선별 수집하거나 전체 가상 디스크를 덤프할 수 있다. 이렇게 수집된 가상머신 데이터는 기존의 디지털 포렌식 조사 방법 및 도구를 사용하여 분석할 수 있다.

IV. 데스크톱 가상화 솔루션별 디지털 포렌식 조사 방법

앞에서 살펴본 바와 같이, Citrix, VMware, Microsoft의 일반적인 VDI 환경 구성은 거의 동일하다. 따라서 디지털 포렌식 조사도 같은 방법으로 수행된다. 사용자의 가상머신 사용 흔적 및 연결 정보는 사용자 컴퓨터, 연결 관리 시스템, 인증 관리 시스템에 남게 된다. 본 논문에서는 Citrix, VMware, Microsoft의 일반적인 VDI 환경을 구성하고, Windows 7, Ubuntu 12.04, Mac OS 10.8.2가



〔그림 2〕 VDI 환경을 고려한 디지털 포렌식 조사 절차

설치된 사용자 컴퓨터를 이용하여 연구하였다.

4.1 사용자의 가상머신 접속 정보 확인

4.1.1 사용자 컴퓨터

사용자가 가상머신에 접속하면, 이와 관련된 정보가 사용자 컴퓨터에 기록된다. Windows 7 사용자의 경우, VMware는 레지스트리, 로그 기록이 생성되고 Citrix는 레지스트리, 로그 기록, 웹 접속 기록이 생성된다. Microsoft는 Windows에서 기본으로 제공하는 Remote Desktop 관련 레지스트리에 생성되고 로그 기록은 생성되지 않는다. 하지만 Microsoft는 웹으로 가상머신에 접속 시 고유의 시그니처

〔표 3〕 Windows 사용자 컴퓨터에 남겨지는 가상머신 접속 정보

구 분	레지스트리	로그 기록 / 웹 접속 기록
Citrix	- KEY_CURRENT_USER\Software\Citrix\Xen Desktop\DesktopViewer\〔가상머신 이름〕 ⇒ 가상머신 이름, 연결 관리 시스템(DDC) IP	- %UserProfile%\AppData\Roaming\ICAClient ⇒ 가상머신 이름, 접속/접속해제 시간 - 웹 캐시/히스토리에서 'DesktopWeb'을 시그니처로 검색 ⇒ 접속 시간, 연결 관리 시스템(DDC) IP 또는 이름
VMware	- HKEY_CURRENT_USER\Software\VMware,Inc.\VMware VDM\Client ⇒ 가상머신 이름, 연결 관리 시스템(View Mana ger) URL 및 IP, 도메인 및 사용자 컴퓨터 이름	- %UserProfile%\AppData\Local\VMware\VDM\logs ⇒ 연결 관리 시스템(View Manager) URL 및 접속/접속해제 시간, 도메인 및 사용자 컴퓨터 이름 ※ 일자별 생성 (log-〔yyyy〕-〔mm〕-〔dd〕.txt)
Microsoft	- HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default ⇒ 가상머신 이름 또는 IP ※ Windows Remote Desktop 관련 레지스트리 사용으로 VDI를 이용한 접속인지 일반적인 Remote Desktop 접속인지 구분되지 않음	- 웹 캐시/히스토리에서 'RDWeb'을 시그니처로 검색 ⇒ 접속 시간, Hyper-V 서버 및 도메인 이름 ※ 웹으로 접속 시, 'https://〔Hyper-V 서버 이름〕/RDWeb'을 사용

〔표 4〕 Ubuntu 및 Mac OS 사용자 컴퓨터에 남겨지는 가상머신 접속 정보

구 분	Ubuntu 12.04	Mac OS 10.8.2(Mountain Linon)
Citrix	- 캐시 : \home\〔user name〕\.mozilla\firefox\6lhwv183.default\Cache_CACHE_〔numbers〕_ - 히스토리 : \home\〔user name〕\.mozilla\firefox\6lhwv183.default\places.sqlite - 쿠키 : \home\〔user name〕\.mozilla\firefox\6lhwv183.default\cookies.sqlite - 세션 : \home\〔user name〕\.mozilla\firefox\6lhwv183.default\sessionstore.js ⇒ 연결 관리 시스템(DDC) URL 및 IP	- 캐시 : \Users\〔user name〕\Library\Caches\com.apple.Safari\Cache.db - 히스토리 : \Users\〔user name〕\Library\Safari\History.plist - 쿠키 : \Users\〔user name〕\Library\Safari\Cookies.plist - 세션 : \Users\〔user name〕\Library\Safari\LastSession.plist ⇒ 연결 관리 시스템(DDC) URL 및 IP
VMware	- \tmp\vmware-〔user name〕\vmware-view-〔numbers〕.logs ⇒ 연결 관리 시스템(View Manager) URL 및 IP, 접속/접속해제 시간, 사용자 ID, 가상머신 및 도메인 이름	- \Users\〔user name〕\Library\Logs\VMware View Client\vmware-view.logs ⇒ 연결 관리 시스템(View Manager) URL 및 IP, 접속/접속해제 시간, 가상머신 IP, 도메인 이름
Microsoft	- \home\〔user name〕\.bash_history ⇒ 가상머신 이름 또는 IP, 사용자 ID(옵션), 사용자 Password(옵션), 도메인 이름(옵션) ※ .bash_history 파일 : terminal에서 실행한 명령어 목록을 기록한 것으로, 사용자가 가상머신에 연결하기 위해 rdesktop 명령어 사용 시 입력되는 정보 확인 가능	- \Users\〔user name〕\Documents\RDC Connections\Default.rdp ⇒ 가상머신 이름, 사용자 ID, 도메인 이름 ※ 연결 정보 저장 옵션 선택 시 저장됨

〔표 5〕 연결 관리 시스템에 남겨지는 가상머신 접속 정보

구 분	로그 기록
Citrix (DDC)	- %SystemDrive%\inetpub\logs\LogFiles\〔지정 폴더〕 ⇒ 접속/접속해제 시간, 연결 관리 시스템(DDC) 및 사용자 IP ※ 일자별 생성 (〔yymmdd〕.log)
VMware (View Manager)	- %SystemDrive%\ProgramData\VMware\V DM\logs ⇒ 가상머신 이름 및 IP, 접속/접속해제/재접속/로그오프 시간, 도메인 및 사용자 컴퓨터 이름 ※ 일자별 생성 (log-〔yyyy〕-〔mm〕-〔dd〕.txt)
Microsoft (RDCM)	- %SystemDrive%\inetpub\logs\LogFiles ⇒ 접속/접속해제 시간, 사용자 ID ※ 일자별 생성 (〔yymmdd〕.log)

(RDWeb)를 사용하므로 이를 이용하여 웹 히스토리에서 접속 흔적을 찾을 수 있다. 〔표 3〕은 Windows 사용자 컴퓨터에 기록되는 가상머신 접속 정보이다.

Ubuntu 12.04와 Mac OS 10.8.2 사용자의 경우, VMware는 Windows와 같이 생성되는 로그 기록에서 접속 흔적을 확인할 수 있지만, Citrix는 이와 달리 로그 기록이 생성되지 않기 때문에 웹 브라우저 접속 시 남겨지는 정보를 확인해야 한다. 본 논문에서는 Ubuntu의 기본 웹 브라우저인 Firefox와 Mac OS의 기본 웹 브라우저인 Safari를 대상으로 하였다. 그리고 Microsoft는 Windows와 달리 Ubuntu와 Mac OS에서 웹 브라우저를 이용한 RDWeb 접속이 불가하기 때문에 웹 히스토리 분석을 통한 접속 흔적을 찾을 수 없다. 하지만 Microsoft 가상머신에 원격 데스크톱 연결을 할 경우 남겨지는 기록에서 접속 흔적을 확인할 수 있다. 〔표 4〕는 Ubuntu 및 Mac OS 사용자 컴퓨터에 기록되는 가상머신 접속 정보이다.

4.1.2 연결 관리 시스템

연결 관리 시스템은 사용자에게 가상머신을 할당 및 관리하고 사용자 요청에 따라 연결 및 연결 해제하는 역할로, 사용자의 가상머신 접속에 관련된 모든 정보가 관리되고 기록된다. 조사관은 이 기록을 이용하여 사용자의 정확한 가상머신 접속/접속해제 시간을 확인할 수 있다. 〔표 5〕는 연결 관리 시스템에 기록되는 사용자의 가상머신 접속 정보에 대한 것이다.

4.2 가상머신 할당 정보 확인

사용자가 가상머신에 접속하기 위해서는 연결 관리 시스템을 통해 가상머신을 할당받아야 한다. 특정 사용자에게 할당된 가상머신에는 다른 사용자가 접속할 수 없으며, 특정 사용자 전용으로 사용된다. 이러한 사용자와 가상머신 사이의 연결 정보는 연결 관리 시스템 또는 인증 관리 시스템에 저장되며, 사건 용의자와 사용된 가상머신 간의 관계를 확인하는데 유용하다.

〔표 6〕 연결 관리 시스템을 이용한 연결 정보 확인

구 분	내 용
Citrix	- 사용자와 가상머신의 연결 정보를 연결 관리 시스템(DDC)에서 관리 ① DDC에 설치된 Citrix Desktop Studio 실행 ② Desktop Studio - Assignments : 등록된 가상머신 및 그룹 확인 ③ 가상머신 또는 그룹 선택 : Desktop Studio - Search로 전환되면서 해당 가상머신 또는 그룹의 연결 정보 확인
VMware	- 사용자와 가상머신의 연결 정보를 연결 관리 시스템(View Manager)에서 관리 ① View Manager에 설치된 View Administrator Console 실행 ② Inventory - Desktops : 등록된 가상머신의 연결정보 확인
Microsoft	- 사용자와 가상머신의 연결 정보를 인증 관리 시스템(Active Directory)에서 관리 ① Active Directory 사용자 및 컴퓨터 실행 ② 사용자 - 속성 - 개인용 가상 데스크톱 탭 : 사용자에게 할당된 가상머신 확인

〔표 7〕 연결 관리 시스템 및 인증 관리 시스템 DB를 이용한 연결 정보 확인

구 분	내 용
Citrix	- DDC에 XenDesktop DB가 생성됨 ① MS SQL Server Management Studio를 이용하여 DB 접속 ② 〔DDC PC 이름〕 - 〔Databases〕 - 〔CitrixXenDesktopDB〕 - 〔Tables〕 - 〔chb_State.AccountNames〕 : 사용자 이름 및 Uid 확인 ③ 〔DDC PC 이름〕 - 〔Databases〕 - 〔CitrixXenDesktopDB〕 - 〔Tables〕 - 〔chb_State.WorkerDiags〕 : 사용자(Uid)에게 할당된 가상머신 확인
VMware	- View Manger에 ADAM DB가 생성됨 ① Active Directory Explorer를 이용하여 DB 접속 (View Manager IP, 관리자 ID, PW 입력) ② 〔DC=vdi,DC=vmware,DC=int〕 - 〔OU=Servers〕 : 등록된 가상머신의 고유 CN(Com mon Name) 값 및 정보 확인 ⓐ description : 가상머신 이름 ⓑ member : 가상머신을 할당 받은 사용자의 CN ③ 〔DC=vdi,DC=vmware,DC=int〕 - 〔CN=ForeignSecurityPrinciple〕 : 등록된 사용자의 고유 CN 값 및 정보 확인 ⓐ description : 사용자 및 도메인 이름
Microsoft	- Active Directory에 ADAM DB가 생성됨 ① Active Directory Explorer를 이용하여 DB 접속 (Active Directory IP, 관리자 ID, PW 입력) ② 〔DC=도메인 이름〕 - 〔OU=Hyper-V〕 : 등록된 사용자 이름 및 정보 확인 ⓐ msTSPrimaryDesktop : 할당 받은 가상머신 이름

사용자와 가상머신 사이의 연결 정보를 확인하는 방법으로는, 연결 관리 시스템을 이용하여 확인하는 것과 연결 관리 시스템 또는 인증 관리 시스템에 저장되는 DB를 확인하는 것이 있다. 〔표 6〕과 〔표 7〕은 사용자와 가상머신의 연결 정보를 확인하는 방법에 대해 정리한 것이다.

4.3 가상머신 데이터 수집

가상머신 데이터는 각 솔루션별 하이퍼바이저 관리 시스템 및 전용 Shell 접속 프로그램을 이용하여 수집할 수 있다. 또한 사용자가 가상머신에 접속 중이었다면 바로 데이터를 선별 수집하거나 전체 가상 디스크를 덤프할 수 있다.

4.3.1 하이퍼바이저 관리 시스템

각 솔루션에서 제공하는 하이퍼바이저 관리 시스템을 이용하면 가상머신을 Export, 복제 또는 가상머신 구성 파일을 다운로드 할 수 있다. 수집하는 방법별로 가상머신 데이터를 압축하거나 원본 그대로 수집하게 되는데, 압축하여 수집된 데이터는 다시 원본과 동일한 새로운 가상머신을 생성해야만 분석이 가능하다. 또한 가상머신 복제도 원본과 동일한 새로운 가상머신을 생성한다는 측면에서 이와 동일하다. 그리고 원본 그대로 데이터가 수집되는 경우에는 분석 도구를 이용하여 바로 분석 가능하다. 〔표 8〕은 하이퍼바이저 관리 시스템을 이용한 가상머신 데이터 수집 방법을 정리한 것이다.

4.3.2 Shell 접속 프로그램

각 솔루션은 다양한 기능이 포함된 Shell 접속 프로그램을 제공하고 있다. 이들 기능 중, 가상머신의 가상 디스크를 수집할 수 있는 기능도 있다. 단, VMware와 Microsoft는 원본 디스크와 동일한 데이터를 수집하지만 Citrix는 압축된 파일로 수집되기 때문에 XenCenter를 이용하여 복원하여 분석하여야 한다. 〔표 9〕는 Shell 접속 프로그램을 이용한 가상머신 데이터 수집 방법을 정리한 것이다.

4.3.3 수집된 데이터의 무결성 검증

수집된 데이터의 무결성 검증은 그것이 증거로써 가지는 가치를 판단할 수 있는 가장 좋은 방법이다. 본 논문에서의 수집 데이터 무결성 검증은 각 솔루션별 스토리지에 저장된 원본 가상 디스크의 해쉬 값과 수집된 가상 디스크의 해쉬 값과 비교하였다. 사용된 해쉬는 MD5와 SHA1 이며, 원본 가상 디스크의 해쉬 값은 하이퍼바이저 또는 하이퍼바이저 관리 시스템

〔표 8〕 하이퍼바이저 관리 시스템을 이용한 가상머신 데이터 수집

구 분	가상머신 Export	가상머신 복제	가상머신 구성파일 다운로드
Citrix (XenCenter)	- 가상머신 선택 - 메뉴 - VM - Export - 지정 경로에 .xva 또는 .ovf 파일 Export ⇒ 복원 시 원본과 동일한 가상머신 생성	- 가상머신 선택 - Copy VM - Full copy ⇒ 원본과 동일한 가상머신 생성	
VMware (vCenter)	- 가상머신 선택 - 메뉴 - 파일 - 내보내기 - OVF 템플릿 내보내기 - 지정 경로에 .ovf 파일 Export ⇒ 복원 시 원본과 동일한 가상머신 생성	- 가상머신 선택 - 복제 ⇒ 원본과 동일한 가상머신 생성	- 하이퍼바이저 호스트 또는 가상머신 선택 - 요약 - 리소스 - 스토리지 - 데이터스토어 선택 - 데이터스토어 찾아보기 ⇒ 데이터스토어에 저장된 모든 가상머신 및 데이터를 트리 구조로 확인 및 다운로드 가능
Microsoft (Hyper-V 관리자 및 SCVMM)	- Hyper 관리자 - 가상머신 선택 - 내보내기 - 지정 경로에 .vhd 파일 Export ⇒ 원본 가상 디스크와 동일	- SCVMM - 가상머신 선택 - 복제 - 가상 컴퓨터를 호스트에 배치 ⇒ 원본과 동일한 가상머신 생성	

에 Shell 접속 후 생성하였다. 특히, 데이터 수집 시 압축되어 수집된 데이터(Citrix의 가상머신 Export, Shell 접속 프로그램 및 VMware의 가상머신 Export)는 복원 후 생성된 가상머신의 가상 디스크를 이용하였다.

해쉬 값 비교 결과, VMware와 Microsoft는 모두 해쉬 값이 일치하지만 Citrix는 일치하지 않았다. Citrix에서 해쉬 값이 일치하지 않는 이유는 원본 가상 디스크가 XenCenter를 통해 Export, 복제 또는 복사될 때 원본과 다른 새로운 형태의 VHD 포맷으로 재배열하기 때문이다. 이는 원본과 수집된 데이터의 내부 Offset 값을 비교함으로써 알 수 있다. 하지만 이는 Offset의 재배열에 따른 것으로 내부적인 파일 시스템 영역이나 전체 파일의 해쉬 값을 비교한 결과는 원본과 수집된 데이터가 일치한 것을 확인할 수 있었다. 따라서 포렌식적으로 수사를 진행하는데 있어 증거로써의 가치는 분명히 있다.

현재 Citrix의 데이터 추출 시 발생되는 VHD 포맷 재배열과 관련된 문제는 다양한 실험을 통한 추가 연구를 진행 중에 있다.

〔표 9〕 Shell 접속 프로그램을 이용한 가상머신 데이터 수집

구 분	Shell 접속 프로그램
Citrix (XenCenter)	- 하이퍼바이저에 Shell 접속 또는 XenCenter에서 "Console" 탭 선택 - 디스크 수집 명령어 : xe vm-export vm=〔가상머신 이름〕 filename=〔파일이름〕.xva
VMware (vSphere PowerCLI)	- vSphere PowerCLI를 이용하여 Shell 접속 - 디스크 수집 명령어 : copy-datastoreitem 〔데이터스토어 드라이브〕:\〔원본 경로〕 〔지정 경로〕 ※ vSphere PowerCLI 설치 필요 - VMware에서 제공하는 것으로, 하이퍼바이저 또는 하이퍼바이저 관리 시스템에 Shell 접속하여 하이퍼바이저를 컨트롤 할 수 있는 라이브러리로 구성되어 있음
Microsoft (Windows PowerShell)	- Windows PowerShell을 이용하여 Shell 접속 - 디스크 수집 명령어 : export-vm -vm "〔가상머신 이름〕" -server 〔Hyper-V 서버 이름〕 -path 〔지정 경로〕 ※ PowerShell Management Library for Hyper-V 설치 필요 - CodePlex(http://pshyperv.codeplex.com)에서 제공하는 것으로, Windows PowerShell을 이용하여 Hyper-V 서버를 컨트롤 할 수 있는 라이브러리로 구성되어 있음

Ⅴ. Ⅴ. 결론

가상 데스크톱 환경의 도입은 기업 또는 조직의 입장에서는 비용절감의 효과를 누릴 수 있으며, 개인 사용자 입장에서는 웹 서비스를 더욱 편리하게 사용할 수 있다는 측면에서 큰 축복이 될 수 있다. 하지만 최근 빠른 속도로 발전하고 성장하는 클라우드 시장에 비하여 클라우드 컴퓨팅 환경에 대한 디지털 포렌식 조사 기법은 아직 걸음마 단계인 것이 현실이다. 본 논문에서는 사설 클라우드 서비스로 제공되는 가상 데스크톱 환경 및 전 세계적으로 가장 많이 사용되고 있는 데스크톱 가상화 솔루션(Citrix, VMware, Microsoft)에 대해 소개하고, 각 솔루션들에 대한 디지털 포렌식 조사 절차 및 방법에 대해 연구하였다. 이를 통해 디지털 포렌식 조사관은 가상 데스크톱 환경에 대한 디지털 포렌식 조사 시 사용자의 로컬 컴퓨터, 연결 관리 시스템, 인증 관리 시스템에서 사용자의 가상머신 사용 흔적을 확인하고, 이 후 본 논문에서 제시한 다양한 방법을 통해 사용자의 가상머신 데이터를 수집할 수 있다. 이렇게 수집된 데이터는 기존 디지털 포렌식 조사 방법을 이용하여 분석할 수 있기 때문에 현장의 조사관들에게 매우 유용하게 사용될 것이다. 또한 빠른 속도로 증가하고 있는 다양한 클라우드 컴퓨팅 환경에 대응하기 위한 디지털 포렌식 조사 절차 및 방법에 대한 연구가 본 논문을 계기로 더욱 활성화되기를 기대해 본다.

참고문헌

〔1〕 Peter Mell and Tinothy Grance, "The NIST Definition of Cloud Computing," NIST, http://csrc.nist.gov/publications/ nistpubs/800-145/SP800-145.pdf/, Sep. 2011.

〔2〕 US-CERT, Alexa Huth and James Cebula, "The Basics of Cloud Computing," US-CERT, http://www.us-cert.gov/sites/ default/files/publications/CloudComputingHuthCebula.pdf/, 2011.

〔3〕 Thomas J. Bittman, "Top Five Private Cloud Computing Trends, 2012," Gartner, http://blogs.gartner.com/thomas_bittman/2012/03/22/top-five-private-cloud-computing-trends-2012/, March 22, 2012.

〔4〕 윤경, "가상화 솔루션 선두 'VM웨어' 맹추격하는 'MS 하이퍼-V'," Betanews, http://www.betanews.net/article/545054, 2011년 7월 18일.

〔5〕 Gartner, "Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010," http://www.gartner.com/newsroom/id/1389313/, Jun. 2010.

〔6〕 Mark Taylor, John Haggerty, David Gresty and David Lamb, "Forensic investigation of cloud computing systems," Network Security, Vol. 2011, no. 3, pp. 2-20, Mar. 2011.

〔7〕 M. Taylor, J. Haggerty, D. Gresty and R. Hegarty, "Digital evidence in cloud computing systems," Computer Law & Security Review, Vol. 26, no. 3, pp. 304-308, May, 2010.

〔8〕 Ben Martini and Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, Vol. 9, no. 2, pp. 71-80, Nov. 2012.

〔9〕 Robert L. Grossman, "The Case for Cloud Computing," IEEE, Vol. 11, no. 2, pp. 23-27, Mar.-Apr. 2009.

〔10〕 F. John Krautheim, "Private Virtual Infrastructure for Cloud Computing," HotCloud '09 Conference, Jun. 2009.

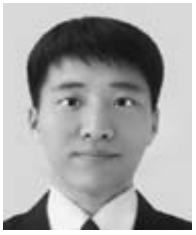
〔11〕 Stephen Biggs and Stilianos Vidalis, "Cloud Computing: The Impact on Digital Forensic Investigations," International Conference for Internet Technology and Secured Transactions, 2009, Nov. 2009.

〔12〕 Hyunji Chung, Jungheum Park, Sangjin Lee and Cheulhoon Kang, "Digital forensic investigation of cloud storage services," Digital Investigation, Vol. 9, no. 2, pp. 81-95, Nov. 2011.

〔13〕 D Barrentt and G Kipper, Virtualization and Forensics: A Digital forensic Investigator's Guide to Virtual Environments, Syngress, Burlington, MA 01803, USA, 272p, 2010.

〔14〕 정일훈, 오정훈, 박정흠, 이상진, "IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구," *정보보호학회논문지*, 21(6), pp. 55-65, 2011년 12월.
〔15〕 강성림, 박정흠, 이상진, "클라이언트 관점의 SaaS 사용 흔적 분석," *정보처리학회논문지*, 19(1), pp. 1-8, 2012년 2월.
〔16〕 Thomas J. Bittman, George J. Weiss, Mark A. Margevicius and Philip Dawson, "Magic Quadrant for x86 Server Virtualization Infrastructure," Gartner, Jun. 2012.

〈著者紹介〉



장 상 희 (Sanghee Jang) 정회원
2011년 8월~현재 : 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 정보보호

김 등 화 (Deunghwa Kim) 학생회원
2011년 8월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 사이버 범죄 수사

박 정 흠 (Jungheum Park) 학생회원
2007년 2월: 한양대학교 정보통신대학 컴퓨터전공 공학사
2009년 2월: 고려대학교 정보경영공학전문대학원 공학석사
2009년 2월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 디지털 포렌식, 안티-안티 포렌식

강 철 훈 (Cheulhoon Kang) 정회원
대전대학교 컴퓨터공학과 학사
연세대학교 공학대학원 컴퓨터공학과 석사
현 대검찰청 디지털수사담당관실 데이터베이스 포렌식팀 팀장
〈관심분야〉 데이터베이스 포렌식, 회계 포렌식

이 상 진 (Sangjin Lee) 종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월 ~ 2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
2010년: 대한민국 사이버치안대상 대통령 표창
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수