情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

사설 클라우드 환경에서 수집된 VM 데이터의 무결성 입증과 관련 포렌식 도구의 신뢰성 검증*

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

Integrity verification of VM data collected in private cloud environment and reliability verification of related forensic tools*

Deunghwa Kim,[1†] Sanghee Jang,[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

최근 들어, 수많은 기업들은 IT 분야에서의 비용절감을 위하여 클라우드 솔루션을 채택해 오고 있다. 한편 디지털 흔적이 추후 법정에서 온전한 디지털 증거로 인정받기 위해서는 증거능력이 있어야 하는데, 그 중에서도 무결성은 증거능력을 갖추기 위한 여러 요건 중 하나이다. 이와 같은 맥락에서, 본 논문에서는 대표적인 사설 클라우드 솔루션(Citrix, VMware, MS Hyper-V)으로부터 수집된 VM 데이터를 대상으로 무결성 검증실험을 수행 하였으며, 그 결과로서 사설 클라우드 컴퓨팅 환경에서 수집된 VM 데이터에 대한 무결성 검증방법을 제안하고자 한다. 또한, 전 세계적으로 널리 사용되는 Guidance사의 EnCase 도구가 대표적인 가상 디스크 파일인 VHD (Virtual Hard Disk) 파일을 제대로 마운트 하지 못하는 오류가 있음을 확인하였다.

ABSTRACT

Recently, a large number of corporations are adopting cloud solution in order to reduce IT-related costs. By the way, Digital Trace should have admissibility to be accepted as digital evidence in court, and integrity is one of the factors for admissibility. In this context, this research implemented integrity verification test to VM Data which was collected by well-known private cloud solutions such as Citrix, VMware, and MS Hyper-V. This paper suggests the effective way to verify integrity of VM data collected in private cloud computing environment based on the experiment and introduces the error that EnCase fails to mount VHD (Virtual Hard Disk) files properly.

Keywords: Digital Forensics, Cloud Forensics, Citrix, VM Ware, Hyper-V, Data Export

접수일(2012년 11월 22일), 수정일(1차: 2013년 1월 24일, 2차: 2013년 3월 11일), 게재확정일(2013년 3월 19일)
* 본 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
* This research was supported by the Public welfare&Safety research program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2012M3A2A1051106)
† 주저자, kma14981@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

I. 서 론

클라우드 컴퓨팅은 최근 IT 시장에서 가장 큰 성장을 보이고 있는 분야로서 앞으로도 지속적으로 성장할 것으로 예측되고 있다. 이처럼 급속히 커져가는 클라우드 시장만큼이나 클라우드 서비스를 이용한 범죄의 발생 역시 늘어날 것으로 예상되는데, 결국 클라우드 포렌식에 대한 수요도 급증할 것으로 보인다.

본 논문에서는 클라우드 포렌식 중에서도 사설 클라우드[1] 환경에서의 VM 데이터 수집과 그에 따라 수집된 VM 데이터의 무결성 검증 방법에 대한 연구를 진행하였다. 이때, 실험대상이 되는 사설 클라우드 제품으로 Citrix, VMware, MS Hyper-V 솔루션이 사용되었다.

또한, 수집된 VM 데이터의 무결성 검증을 위하여 전 세계적으로 널리 사용되고 있는 포렌식 도구인 Guidance사의 EnCase 도구를 사용하였는데, VM 스토리지가 동적(dynamic)으로 할당된 경우 EnCase 도구는 해당 VHD 포맷의 파일을 제대로 마운트하지 못하는 오류를 가지고 있음을 확인하였다.

II. 사설 데스크톱 가상화 환경에서의 수집 데이터 무결성 검증

디지털 흔적이 추후 법정에서 온전한 디지털 증거로 인정받기 위해서는 증거능력을 갖추어야 하는데, 그 중에서도 무결성은 증거능력을 갖추기 위한 여러 가지 필수 요건 중 하나이다.

클라우드 분야에 대한 디지털 포렌식 수사에서도 수집된 VM 데이터들이 훗날 법정에서 피고인의 범죄 혐의를 입증할 수 있는 증거자료로 활용될 수 있도록 수집된 VM 데이터에 대한 무결성을 입증할 필요가 있을 것이다. 위와 같은 관점에서 본 논문에서는 Citrix, MS Hyper-V, VMware VDI 환경에서의 원본(Original) VM 디스크 이미지와 추출된(Exported) VM 디스크 이미지에 대한 해쉬값(MD5)을 계산 및 비교함으로써 사설 클라우드 환경에서 수집한 VM 데이터들에 대한 무결성 검증 테스트를 수행해 보았다.

2.1 Citrix

먼저, Citrix Xendesktop 가상화 환경에서 수집된 VM 데이터의 무결성 검증을 위한 실험환경에 대해서 알아보도록 하자.

가상 디스크 스토리지를 생성하기 위하여 Citrix의 관리도구인 XenCenter를 통하여 NFS(Network File System) Storage 서버를 구축하였으며, NFS Storage 서버 구축이 완료된 이후에는 추출 실험을 위한 대상 가상머신으로 Windows7을 NFS virtual disk storage 위에 설치하였다.

데스크톱 가상화 환경에서는 VM을 생성할 시 virtual disk storage를 고정(static)으로 할 것인지 또는 동적(dynamic)으로 할 것인지 VM 스토리지의 할당 형태(Allocation type of storage) 를 지정해 주어야 하는데, 이때 VM 스토리지의 형태를 동적(dynamic)으로 지정한 경우에는 Thin Provisioning[2] 기술이 적용되어 원본 VM을 추출 시 가상 디스크 파일(.vhd)은 최초 설정된 크기로 추출되지 않고 쓰여진 영역의 크기만큼 추출된다. Citrix VDI 환경에서 수집된 VM 데이터의 무결성 검증을 위한 세부 실험환경은 〔표 1〕과 같다.

〔표 1〕 데이터 무결성 검증을 위한 세부 실험환경

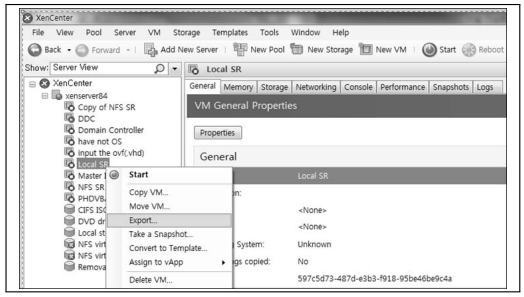
Index	Content
Type of Virtual Disk Storage	NFS disk Storage
Experiment VM OS	Windows 7(32bit)
Allocation of VM storage	Dynamic
Size of Default VM Storage	24GB
Calculation Hash-value (MD5)	EnCase v7.03.01

위와 같은 실험환경에서 스토리지의 할당 형태(Allocation type of storage)는 동적으로 설정한 이후 〔그림 1〕과 같이 Citrix VDI 솔루션의 전용 관리도구인 XenCenter의 Export 기능을 활용 하여 VM 디스크 이미지를 로컬 PC로 추출하였다.[3]

1) 일반적으로 클라우드 컴퓨팅은 이용 목적과 사용자 접근 제한에 따라서 크게 공공(Public) 클라우드, 사설(Private) 클라우드로 구분된다. 사설 클라우드는 공공 클라우드와는 달리 제한적이거나 폐쇄된 환경에서 인가된 사용자들만 사용 가능하도록 구축된 클라우드 컴퓨팅 환경을 의미하며, 대표적인 사설 클라우드에는 Citrix, VMware, MS Hyper-V 등이 있다.

2) 미리 저장된 볼륨 상에 물리적인 디스크 용량을 할당하는 것이 아니라, 실제 용량 공간은 데이터 쓰기가 발생할 때 사용되는 원리

3) Citrix XenDesktop VDI 환경에서 VM 데이터를 로컬 경로로 추출하는 그 밖의 방법에는 CLI를 통한 추출



〔그림 1〕 Exported VM(.vhd) Image File

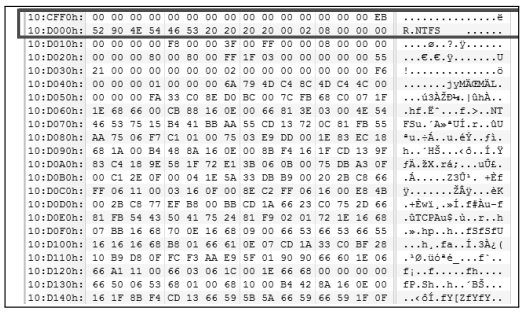
이후 무결성 검증 실험을 위하여 NFS Virtual disk Storage의 실제 경로에서 확인할 수 있는 원본 VM과 XenCenter의 Export 기능을 통하여 로컬 PC로 추출된 VM에서의 파일 크기, 해쉬값 등을 비교해 보았는데 그 결과는 〔표 2〕와 같다.

〔표 2〕 원본과 추출된 VM 이미지 파일의 무결성 검증

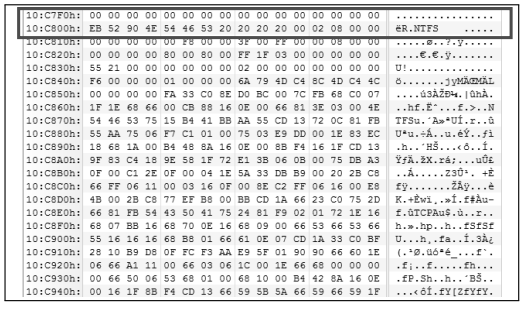
Index	원본(Original) VM	추출된(Exported) VM
UUID	010fb7c9-xxx.vhd	38fa16b2-xxx.vhd
MD5	CEDB64BD9510566BD3A7A516CADF6444	06D6A00AD0A51EFE1E31B04B0D473BE2
Disk Size	5,309,903,360 Bytes	5,200,160,256 Bytes
비 고	• VM 생성 시 Default Disk Size : 24GB • Allocation of VM Storage : dynamic	

〔표 2〕에서 보는 바와 같이 실험 대상이 되는 VM을 생성할 당시에 디스크의 Default Size는 24GB이었으나, VM Storage를 동적(dynamic)으로 할당하였기 때문에 추출된 VM의 디스크 크기는 해당 볼륨(Volume)상에 쓰여진 영역의 크기 만큼인 4.84GB (5,200,160,256 Bytes)가 되었다. 한편, Citrix Xendesktop 환경에서 VM의 스토리지를 동적으로 할당하고 추출하는 경우, 위 〔표 2〕의 〔Disk Size Column〕에서 보는 바와 같이 특이하게도 원본 VM과 추출된 VM의 디스크 크기가 달라지는 특성을 보였으며 결과적으로 서로 상이한 해쉬값(MD5)을 갖게 된다.

반복적인 실험을 통해서 확인해 본 결과, 추출된 VM의 디스크 크기는 원본 VM과 비교해 볼 때, 약 0.1GB정도 작아진다는 것을 확인할 수 있었다. 이는 Citrix VDI 환경에서 XenCenter를 통하여 원본 VM을 추출 또는 복제할 시, 가상 디스크 파일을 있는 그대로 추출 또는 복제하지 아니하고 새로운 형태의 VHD 포맷으로 재배열하기 때문이다. 〔그림 2〕와 〔그림 3〕에서 보는 바와 같이 원본과 추출된 VM 이미지 파일을 Hex Bytes로 확인한 결과, 동일한 값을 가지는 offset이 확연히 달라짐을 볼 수 있다.



〔그림 2〕 Origin VM(.vhd) Image File



〔그림 3〕 Exported VM(.vhd) Image File

실험을 통해서 확인해 본 결과 Citrix VDI 환경에서는 VM(.vhd)을 추출 시, 원본 VM의 데이터를 일정 크기의 블락 단위로 쪼개어 전송 하는 특징을 보인다. 이후 수신 노드에서는 전송 받은 데이터를 조합하여 다시 VM(.vhd) 이미지 형태로 변환하는 과정을 거치는데, 이때 새로운 형태의 VHD 포맷으로 재배열하는 것으로 확인되었다.

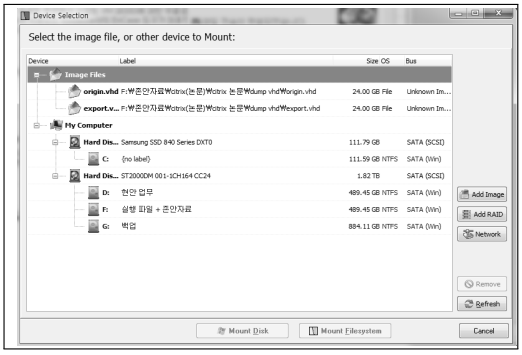
즉, VM의 추출 과정에서 VHD 포맷의 구조 자체가 달라졌기 때문에 Citrix VDI에서의 무결성 검증

과 상용 Backup 도구를 통한 추출방법이 있다. CLI를 통해서 VM을 추출하기 위한 명령어는 "xe vm-export vm=〔vm name〕 filename =〔path〕 /〔storage UUID〕/〔exported name〕" 이며, 상용 Backp 도구에는 PHD Virtual Backup 등이 있다.

은 원본 및 추출된 가상 디스크 파일들의 물리적인 해쉬값 비교를 통해서는 확인 할 수 없다.

결국, Citrix VDI 환경에서의 무결성 검증은 뒤에서 언급할 VMware, MS Hyper-V 환경 에서와 달리 원본과 추출된 가상 디스크 파일 (.vhd)의 드라이브(C\, D\) 영역에서의 해쉬값 비교를 통하여 수행되어져야 한다.

위 실험을 수행하기 위하여 아래 〔그림 4〕에서 보는 바와 같이, NFS Virtual disk Storage에 저장되어 있는 Citrix XenDeskop의 원본 VM 이미지 파일과 추출된 VM 이미지 파일을 'Mount Image Pro'라는 도구를 사용하여 각각 마운트 하였다.



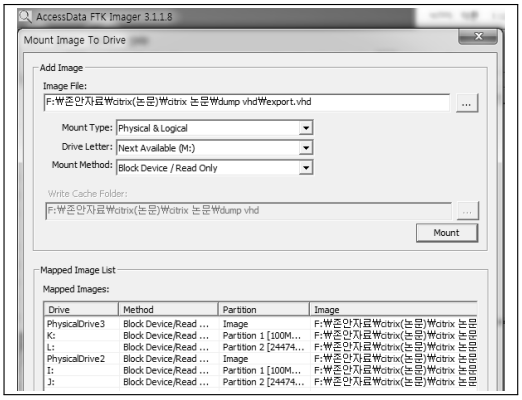
〔그림 4〕 Mount the VHD File using the Mount Image Pro

이후, EnCase 도구를 활용하여 원본과 추출된 VM에 대한 드라이브 영역에서(C\, D\)의 해쉬값을 계산한 결과 〔표 3〕에서 보는 바와 같이, 그 결과 값이 일치함을 확인할 수 있었다.

〔표 3〕 드라이브 영역에서의 무결성 검증 결과

Index	원본(Original) VM	추출된(Exported) VM
Boot Area	092D9487556456C6881F16BEA9FABCDA	092D9487556456C6881F16BEA9FABCDA
Data Area	27A83C3709DEE6F042AA064C56B7DE29	27A83C3709DEE6F042AA064C56B7DE29
비고	• Mount the Exported VM Disk : Mount Image pro • Hash Calculation : EnCase v7.03.01	

위 실험의 신뢰성을 높이기 위하여, 〔그림 5〕에서와 같이, 'FTK Imager'라는 또 다른 마운트 전용도구를 통하여 동일한 방법으로 테스트를 진행해 보았다.



〔그림 5〕 Mount the VHD File using the FTK Imager

이후, EnCase 도구를 활용하여 원본과 추출된 VM에 대한 드라이브 영역에서(C\, D\)의 해쉬값을 계산한 결과 〔표 4〕에서 보는 바와 같이, 그 결과 값이 일치함을 확인할 수 있었다.

〔표 4〕 드라이브 영역에서의 무결성 검증 결과

Index	원본(Original) VM	추출된(Exported) VM
Boot Area	092D9487556456C6881F16BEA9FABCDA	092D9487556456C6881F16BEA9FABCDA
Data Area	27A83C3709DEE6F042AA064C56B7DE29	27A83C3709DEE6F042AA064C56B7DE29
비고	• Mount the Exported VM Disk : FTK Imager • Hash Calculation : EnCase v7.03.01	

결국 Citrix VDI 환경에서의 수집된 VM 데이터에 대한 무결성 검증은 드라이브(C\, D\) 영역에서의 해쉬값 비교를 통해서 수행해야만 한다. 또한 드라이브 영역 단위의 해쉬값을 계산하기 위해서는 먼저 Mount Image Pro, FTK Imager와 같은 마운트 도구를 통하여 VHD 파일을 마운트 한 이후에 해쉬값을 계산해야 하겠다.

2.2 VMware, MS Hyper-V

VMware, MS Hyper-V VDI 환경에서 수집한 VM 데이터에 대한 무결성 검증을 수행한 결과, 가상머신 스토리지 할당 형태(static, dynamic)에 관계없이 추출된(exported) VM은 원본(original) VM

과 항상 일치하는 해쉬값을 가지고 있음을 실험을 통해 확인하였다.

결국 VMware, MS Hyper-V VDI 환경에서 수집한 VM은 드라이브 영역에서의 해쉬값 비교가 아닌, 추출된 VM(vmdk, vhd) 이미지에 대한 물리적인 해쉬값 비교를 통하여 그 무결성을 확인할 수 있다.

III. 가상 하드디스크(Virtual Hard Disk)에 대한 포렌식 도구의 신뢰성 검증

VHD(Virtual Hard Disk)는 Citrix, VMware, MS Hyper-V 가상화 솔루션에서 모두 사용될 수 있는 가상화 환경에서의 대표적인 표준 가상 디스크 포맷이다.

이전 장에서 사설 데스크톱 가상화 환경에서 수집된 데이터에 대한 무결성을 검증하기 위하여 여러 가지 포렌식 도구들을 사용하였는데, 테스트를 진행하면서 우연히 전 세계적으로 널리 사용되고 있는 Guidance 사의 EnCase Tool이 동적으로 할당된 VHD 디스크 파일을 제대로 마운트 하지 못하는 오류를 가지고 있음을 알게 되었다.

결국 우리는 연구의 범위를 넓혀서 현재 학계에서 널리 사용되고 있는 포렌식 관련 도구들이 가상 하드디스크를 제대로 마운트 하는지에 대한 신뢰성 검증 테스트를 진행하였는데, 해당 테스트를 위한 실험 환경은 〔표 5〕와 같다.

〔표 5〕 EnCase Tool의 mount error 확인을 위한 실험 환경

구 분	내 용
Solution Name	Citirx Xendesktop
Experiment VM OS	Windows 7(.vhd)
Test Tools	EnCase v6.19.6 & v7.03.01 FTK v4.1.0.165 X-ways Forensics
Mount Tool	Mount Image Pro v4 FTK Imager 3.1.1.8

3.1 VM 동적 할당(Dynamic allocation)

위 환경에서 포렌식 도구의 신뢰성 검증 실험을 위하여 스토리지가 동적으로 할당된 Windows 7 OS의 가상머신 디스크 이미지(.vhd)를 로컬 경로로 추출하였다. 이후, NFS Virtual Storage의 실제 경로에서 확인할 수 있는 원본(Original) 디스크 이미지와 로컬 경로로 추출된(Exported) 디스크 이미지를 대상으로 위에서 언급한 세 가지 Test Tool에 각각 마운트를 한 이후 해쉬값(MD5)을 계산해 보았는데, 그 결과는 〔표 6〕과 같다.

〔표 6〕 VHD 가상 디스크 이미지 해쉬값(MD5) 계산

Index	EnCase	FTK	X-way Forensics
Origin VHD	C69289228 xxxxxxxxx	C5F64F49C xxxxxxxxx	C5F64F49C xxxxxxxxx
Export VHD	64C4D1298 xxxxxxxxx	C5F64F49C xxxxxxxxx	C5F64F49C xxxxxxxxx

〔표 6〕의 실험 결과에서 알 수 있는 것처럼 EnCase 도구를 사용한 결과, 원본과 추출된 VHD 디스크 이미지의 해쉬값이 불일치하였는데, 이는 EnCase 도구가 VHD 파일 포맷을 제대로 마운트하지 못하기 때문이다. EnCase 도구의 마운트 에러 원인을 찾기 위하여 원본과 추출된 VHD 디스크 이미지를 다시 EnCase로 마운트 한 이후, 드라이브 영역내의 모든 엔트리를 대상으로 각각의 엔트리별 해쉬값을

File Name	MD5
$TxfLogContainer00000000000000000001	f3faf1ba0a4ce954dced1a884e963612
$TxfLogContainer00000000000000000001	39bbf66a82a1a00f4c037180e7c6b52e
$TxfLogContainer00000000000000000002	13ee8b61e764e132294ec96fb33b4726
$TxfLogContainer00000000000000000002	de7ca2e7a61e259cf4e9cbb9e59f6fdc
DataStore.edb	d1ef2f277315ca67e18e50a4a899ee3a
pagefile.sys	1c89f4647c7f0e86e6367d3dcaf43cd1
qmgr0.dat	37c72a3f3319b1444ee963262ea5315a
qmgr1.dat	37c72a3f3319b1444ee963262ea5315a
tmp.edb	f46d488b07f56b74d2560385c5964720
Windows.edb	16220eaec2e9a139ca45e52778ec8972
{6cced300-6e01-11de-8bed-001e0bcd1824}.TxR.0.regtrans-ms	8b36838f22c0aae32c1314a23b030bf5
{6cced300-6e01-11de-8bed-001e0bcd1824}.TxR.1.regtrans-ms	01ab52af1237d9c22ee4eb0e8bba012d
{6cced300-6e01-11de-8bed-001e0bcd1824}.TxR.2.regtrans-ms	6042552a8675884daf661a4a78026b41

〔그림 6〕 EnCase7 Mount - Original VHD

File Name	MD5
$TxfLogContainer00000000000000000001	f5f586879488dfc95359eff78ca04905
$TxfLogContainer00000000000000000001	2ab99a1757fc21c4c2515b623f916b29
$TxfLogContainer00000000000000000002	d1dd210d6b1312cb342b56d02bd5e651
$TxfLogContainer00000000000000000002	f1c9645dbc14efddc7d8a322685f26eb
DataStore.edb	e3102aa36f87630dd089d8a4a5243bfe
pagefile.sys	81b9504ec32a5c2bae1df51392bfd135
qmgr0.dat	613cbe64727cc52fd4b6b5dab55b6f06
qmgr1.dat	613cbe64727cc52fd4b6b5dab55b6f06
tmp.edb	c76e84f71e4764a3d0308150b82d1398
Windows.edb	c2d79f282079ac70f948e9c75319e55c
{6cced300-6e01-11de-8bed-001e0bcd1824}.TxR.0.regtrans-ms	23d9d810740ee44c5a3f04c3293ae578
{6cced300-6e01-11de-8bed-001e0bcd1824}.TxR.1.regtrans-ms	5f363e0e58a95f06cbe9bbc662c5dfb6
{6cced300-6e01-11de-8bed-001e0bcd1824}.TxR.2.regtrans-ms	5f363e0e58a95f06cbe9bbc662c5dfb6

〔그림 7〕 EnCase7 Mount - Export VHD

별도로 계산한 뒤, 그 일치성 여부를 확인해 보았다. 원본과 추출된 VHD 가상 디스크 이미지 각각의 모든 엔트리에 대한 해쉬값을 계산한 결과 총 59,127개의 엔트리 중에서 [그림 6]과 [그림 7]에서 보는바와 같이, 13개의 파일에서 해쉬값이 달라짐을 확인할 수 있었다.

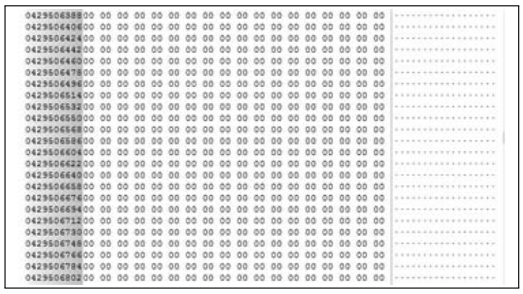
세부적인 확인을 위하여, 위 두 가지 실험군에서 식별된 13개의 파일들을 EnCase의 Export 기능을 사용하여 로컬 PC로 각각 추출하였다. 추출된 13개의 파일 중에서 Pagefile.sys 파일을 대상으로 [그림 8]과 [그림 9]에서 보는 바와 같이 Hex Bytes로 비교 작업을 수행하였는데, 동일한 Offset에서 서로 다른 값들을 가지고 있음을 확인하였다.

[그림 8] Pagefile.sys of Original VHD (EnCase7 Mount)

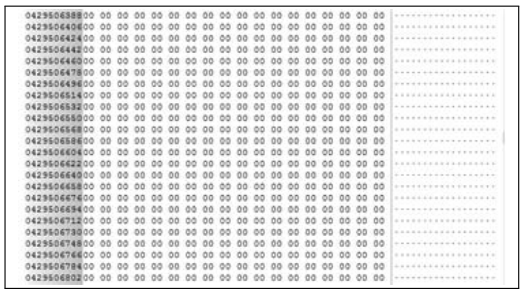
[그림 9] Pagefile.sys of Exported VHD (EnCase7 Mount)

위 그림에서 보는바와 같이, EnCase 도구는 스토리지가 동적으로 할당된 VHD 포맷의 디스크 이미지를 제대로 마운트하지 못함을 재확인할 수 있었다.

결국 EnCase 도구를 활용하여 VHD 포맷의 무결성을 검증하기 위해서는 마운트 도구를 사용하여 우선적으로 디스크 이미지를 마운트 한 이후, 분석을 시행해야 할 것이다. 아래 [그림 10]과 [그림 11]은 마운트 전용 도구인 'Mount Image Pro'라는 도구를 사용하여 원본과 추출된 VHD 포맷의 디스크 이미지를 각각 마운트 한 이후, EnCase 도구를 통하여 Pagefile.sys를 Hex Bytes로 확인한 결과이다.



[그림 10] Pagefile.sys of Original VHD (Mount Image Pro v4)



[그림 11] Pagefile.sys of Exported VHD (Mount Image Pro v4)

위 그림에서 보는바와 같이, 마운트 도구를 사용하여 VHD 포맷의 디스크 이미지를 마운트 한 이후, EnCase 도구를 사용하여 Pagefile.sys의 동일한 Offset을 봤을 때, 모든 값들이 0x00으로 되어있음을 볼 수 있다. 앞에서 추출한 13개의 파일들(해쉬값이 상이)을 대상으로 반복적인 실험을 통하여 확인한 결과, EnCase 도구의 경우 스토리지가 동적으로 할당된 VHD 포맷의 파일을 마운트 하는 과정에서, 일부 엔트리(파일)의 특정 오프셋에서 알 수 없는 값들을 반복적으로 쓰고 있음을 확인할 수 있었다.

이 밖에도 실험의 신뢰성을 높이기 위하여 Citrix, MS Hyper-V 솔루션에서 각각 Windows 7, Windows XP 운영체제의 VM을 대상으로 EnCase 도구의 마운트 오류와 관련된 실험을 수행하였는데, 그 결과는 [표 7]과 같다.

〔표 7〕 EnCase mount error 탐지 실험결과

구 분	Mount Error가 발생한 총 Entry 수	
	Windows 7	Windows XP
Citrix	13개 파일 (pagefile.sys 등)	8개 파일 (pagefile sys 등)
MS Hyper -V	2개 파일 (pagefile.sys, hiberfile.sys)	2개 파일 (pagefile.sys, hiberfile.sys)
비 고	Allocation Type of Storage : dynamic	

결론적으로, EnCase 도구는 식별되지 않은 내부 오류 등에 의해서 스토리지가 동적으로 할당된 VHD 포맷의 파일을 제대로 마운트하지 못한다. 따라서 스토리지가 동적(dynamic)으로 할당된 VHD 포맷의 데이터를 분석하거나 무결성 검증을 수행하기 위해서는 먼저 EnCase 도구 이외의 신뢰성 높은 전용 마운트 도구 등을 사용하여 VHD 포맷 데이터를 마운트한 이후에 분석을 시도해야 할 것이다.

3.2 VM 정적 할당(Static allocation)

스토리지가 정적으로 할당된 VM은 추출 시, 최초 설정한 디스크의 크기 그대로 추출되기 때문에 EnCase 도구의 경우 마운트 오류가 발생하지 않음을 실험을 통해 확인할 수 있었다.

따라서 스토리지가 정적(static)으로 할당된 VHD 포맷의 데이터를 분석하거나 무결성 검증을 수행할 시에는 별도의 마운트 전용도구가 필요하지 않으며, EnCase, FTK, Xway-Forensics 도구 등으로 무결성 검증 수행이 가능하다.

IV. 결 론

최근 국내외 수많은 기업들은 IT 분야에서의 비용절감을 이유로 기업 내 사설 클라우드 서비스를 구축하고 있다. 기업의 입장에 있어서 클라우드 컴퓨팅 환경의 도입은 비용절감의 효과뿐만 아니라, 기업내 직원들이 클라우드 서비스를 통하여 시·공간적인 제약없이 웹에 접속하여 업무를 수행할 수 있다는 측면에서 볼 때 업무의 효율성도 높이는 장점이 있다.

하지만, 아이러니하게도 기업 내 클라우드 컴퓨팅 환경이 도입됨에 따라 산업기밀유출과 같은 기업범죄에 클라우드 서비스가 범죄발생의 플랫폼으로 사용될 수 있다는 우려도 존재한다. 결국 클라우드 서비스를 이용한 범죄가 발생하는 경우, 결과적으로 용의자가 사용했을 것이라 판단되는 VM 데이터에 접근하거나 추출하는 방법을 통하여 해당 VM 데이터를 분석해야 할 것이다.

위와 같은 맥락에서, 본 논문에서는 대표적인 사설 클라우드 가상화 서비스인 Citrix, VMware, MS Hyper-V를 대상으로 VM 데이터의 수집과 추출된 해당 데이터에 대한 무결성 검증실험을 수행하였다. 본론에서 언급한 바와 같이 Citrix VDI 환경에서는 특이하게도 관리도구(XenCenter)를 통한 VM(.vhd) 데이터의 추출 및 복사 시 가상 디스크 파일을 있는 그대로 추출 또는 복제하지 아니하고 새로운 형태의 VHD 포맷으로 재배열하는 특징이 있다. 결론적으로 Citrix VDI 환경에서의 무결성 검증은 원본과 추출된 가상 디스크 파일(.vhd)의 드라이브 영역에서의 해쉬값 비교를 통하여 수행되어야 한다.

또한, 전 세계적으로 널리 사용되고 있는 Guidance 사의 EnCase 도구의 경우 스토리지가 동적으로 할당된 VHD 포맷을 제대로 마운트 하지 못하는 오류가 있기에 사용 시 주의가 요망된다.

참고문헌

〔1〕 Citrix, http://citrix.com

〔2〕 정일훈, 오정훈, 박정흠, 이상진, "IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구," 정보보호학회논문지, 21(6), pp. 55-65, 2011년 12월.

〔3〕 강성림, 박정흠, 이상진, "클라이언트 관점의 SaaS 사용 흔적 분석," 정보처리학회논문지, 19(1), pp. 1-8, 2012년 2월.

〔4〕 Mark Taylor, John Haggerty, David Gresty, and David Lamb, "Forensic Investigation of Cloud Computing Systems," Network Security, March 2011.

〔5〕 Junghoon Oh, Seungbong Lee, and Sangjin Lee, "Advanced evidence collection and analysis of web browser activity," DFRWS, pp. 62-70, August 2011.

〔6〕 Dominik Birk, "Technical Challenges of Forensic Investigations in Cloud Computing Environments," Workshop on Cryptography and Security in Clouds,

January 2011.
〔7〕 Faith Shimba, "Cloud Computing : Strategies for Cloud Computing Adoption," Dublin Institute of Technology, pp. 1-117, September 2010.
〔8〕 Cyril Onwubiko, "Security Issues to Cloud Computing," Computer Communications and Networks, pp. 271-288, July 2009.

〈著者紹介〉

김 등 화 (Deung - Hwa Kim) 학생회원
2006년 3월: 육군사관학교 운영분석학과, 이학사
2011년 8월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 클라우드

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

박 정 흠 (Jungheum Park) 학생회원
2007년 2월: 한양대학교 정보통신대학 컴퓨터전공 공학사
2007년 3월~2009년 2월: 고려대학교 정보경영공학전문대학원 공학석사
2009년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 디지털 포렌식, 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
1989년 2월~1999년 2월: 한국전자통신연구원 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 대칭키 암호, 정보은닉이론, 컴퓨터 포렌식