Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.491

No Disk System 환경에서의 사용자 행위 분석*

김 등 화,† 남 궁 재 웅, 박 정 흠, 이 상 진‡
고려대학교 정보보호대학원

User behavior analysis in No Disk System Configuration*

Deunghwa Kim,† Jaeung Namgung, Jungheum Park, Sangjin Lee‡
Center for Information Security Technologies(CIST), Korea University

요 약

빅 데이터 시대의 도래와 함께, SSD(HDD) 도입 비용의 증가 등에 따라 최근 국내외 PC방 및 기관에서는 NDS(No Disk System) 솔루션을 도입해 오고 있다. NDS는 일종의 클라우드 컴퓨팅 기반의 스토리지 가상화 솔루션으로서 기존의 개별 컴퓨터에 설치되어 관리하였던 운영체제와 응용 프로그램을 중앙 서버에서 관리하는 방식이다. 본 논문에서는 NDS 환경에서의 사용자 행위 분석에 대한 방법에 대하여 알아보도록 하겠다.

ABSTRACT

With the advent of big data and increased costs of SSD(HDD), domestic and foreign Internet cafes and organizations have adopted NDS(No Disk System) solution recently. NDS is a storage virtualization solution based on a kind of cloud computing. It manages Operating System and applications in the central server, which were originally managed by individual computers. This research will illustrate the way to analyze user's behaviors under NDS circumstance.

Keywords: Digital Forensics, Cloud Computing, NDS(No Disk System), Hardless System, Diskless System

I. 서 론

최근 세계적인 경제위기 속에서 국·내외의 기업들은 IT 분야의 비용 절감을 통한 위기 극복 방안을 모색하고 있으며, 이러한 상황에서 클라우드 컴퓨팅(Cloud Computing)은 위기 극복을 위한 최적의 솔루션으로 빠르게 부상하고 있다.

같은 맥락에서 최근 국내·외 수많은 PC방 및 기관에서는 클라우드 컴퓨팅의 핵심인 가상화(Virtualization) 기술과 네트워크 기술을 접목한 NDS(No Disk System)을 도입함으로써 많은 비용을 절약하고 있다. 또한 NDS 솔루션을 도입하는 경우, 각각의 클라이언트 PC에 하드디스크를 장착할 필요가 없을 뿐만 아니라, Operating System, 각종 프로그램, 게임 관련 Patch 등을 모든 클라이언트 PC에 일일이 설치할 필요가 없기 때문에 관리의 용이함과 효율성 측면에서 많은 이점을 제공하고 있다.

위와 같은 이유로 최근 NDS(No Disk System) 솔루션을 도입하는 기관 및 PC방의 수가 증가하고 있다. 문제는 지금까지 해당 시스템 환경에서의 증거수집 방법과 사용자 행위 분석 등에 대한 연구가 전혀 이루어지지 않았다는 점이다.

따라서 본 논문에서는 클라우드 컴퓨팅 서비스 중에서 IaaS(Infrastructure as a Sevice) 기반의 스토리지 가상화 기술과 네트워크 기술을 접목하여 개발된 NDS에 대한 전반적인 소개와 함께 기본적인 구

접수일(2013년 3월 4일), 수정일(1차 : 2013년 4월 18일, 2차 : 2013년 5월 6일), 게재확정일(2013년 5월 13일)
* 본 논문은 미래창조과학부 및 정보통신산업진흥원의 "지식정보보안인력양성 최고정보보안전문가과정" 사업의 연구결과로 수행되었음(과제번호: NIPA-H2102-13-1002)
† 주저자, kma14981@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr(Corresponding author)

동원리에 대하여 설명하며, 디지털 포렌식 관점에서 해당 시스템에서의 사용자 행위 분석 방법에 초점을 맞추고 연구를 진행하고자 한다.

II. NDS 소개

2.1 NDS 정의

NDS(No Disk System)는 Hardless System 또는 Diskless System으로 불리는 일종의 클라우드 컴퓨팅 기반의 스토리지 가상화 솔루션으로서 기존의 개별 컴퓨터에 설치되어 관리하였던 운영체제와 응용 프로그램을 중앙 서버에서 관리하며, 사전 부팅 실행 환경(PXE : Pre-Boot Execution Environment) 의 네트워크 인터페이스를 기반으로 서버에 미리 저장된 가상 운영체제 이미지를 이용하여 클라이언트 PC를 부팅 및 구동시키는 솔루션을 말한다[1].

2.2 NDS의 특성[2]

NDS(No Disk System)은 말 그대로 로컬 PC 내에 하드 디스크를 장착하지 않은 채 운용이 가능한 시스템으로서 기존 시스템과 비교하여 볼 때, 다음과 같은 특성이 있다.

첫째, 기존 시스템과 달리 클라이언트 PC에는 HDD를 장착하지 않고, 서버의 디스크 이미지를 시스템 드라이브로 마운트 하여 사용하는 일종의 스토리지 가상화 기술을 적용하였기 때문에 하드웨어 측면에서 볼 때 비용절감의 효과가 있다.

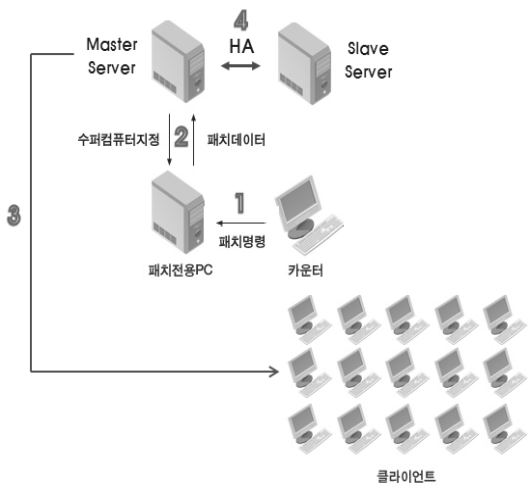
둘째, 클라이언트 PC 중에서 하나의 PC를 슈퍼컴퓨터로 지정한 이후 특정 데이터를 변경(업데이트, 새로운 프로그램 및 패치 설치 등)하면, 동일 네트워크 내의 모든 클라이언트 PC에 해당 변경사항이 일괄적으로 적용되는데, 관리 측면에서 매우 효율적이다. 즉, 모든 프로그램을 전체 클라이언트를 대상으로 일괄 설치 및 삭제할 수 있기 때문에 각각의 클라이언트 PC에 일일이 프로그램을 설치하는 시간을 1/N만큼 줄일 수 있다.

셋째, 일반적으로 클라이언트 사용자가 해당 로컬 PC를 종료한 이후, 재부팅을 하는 경우에 이전 사용자가 변경한 모든 내용은 저장되지 않으며, 항상 일정한 Desktop 환경을 제공한다는 특성을 가지고 있다. 이는 No Disk System의 장점인 동시에 단점이 될 수도 있는데, 해당 자동 복구(Recovery Mode) 기능은 사용자의 고의 및 과실에 의한 시스템 파일의 삭제, 악성 코드 및 바이러스 감염 등으로 인한 운영체제 손상, 오작동으로 인한 심각한 오류 등을 즉시 복구할 수 있다는 이점이 있으나, 동시에 일반적으로 사용자의 흔적이 자동 삭제된다는 점에서 해당 시스템을 악용할 수 있다는 취약점이 공존한다.

그 밖에도 NDS에서는 멀티부트 기능을 지원하며, 일반 시스템 대비 소비전력이 절약되어 물리적인 시스템의 수명을 연장할 수 있는 장점이 있다.

2.3 NDS의 구조

NDS는 랜선, 랜카드, 스위치허브 등 기가비트(Gigabit) 전송 방식으로 구성된 네트워크 시스템으로, 클라이언트 PC의 HDD를 제거하고 중앙서버 관리 방식으로 전체 PC가 구동이 가능하도록 설계된 클라우드 컴퓨팅 시스템의 일종이다. NDS는 [그림 1]과 같은 기본 구조를 가진다.



[그림 1] NDS 기본 구조

[그림 1]에서 보는 바와 같이, 관리자가 Master Server의 [Boot Center]를 통하여 패치전용 PC에서 데이터를 변경(업데이트, 새로운 프로그램 및 패치 설치 등)하면, 해당 업데이트 내역이 Master Server에 연동되어 저장된다. 이후 Master Server에서는 변경된 업데이트 내역을 네트워크 내의 모든 클라이언트에게 일괄적으로 적용시킨다. 끝으로, 일종의 백업 개념으로 Master Server는 변경된 모든 내역들을 Slave Server에 전송 및 저장케 한다. 기본

적으로 Master Server에서는 클라이언트 정보와 클라이언트가 사용하게 될 자원을 저장하고 있으며, Slave Server에는 HA(High Availability) 기능을 사용하여 실시간으로 Master Server의 변경된 정보 및 자원을 감지하여 이를 동기화(Synchronization)하고 백업한다.

2.4 NDS 구성품

NDS를 구성하기 위해서는 일반적인 네트워크 환경과는 다른 구성 품목들이 구비되어야 한다. NDS를 구성하기 위하여 기본적으로 필요한 구성품은 〔표 1〕과 같다.

〔표 1〕 NDS 구성품목

구 분	상세 내용
	• 하드리스 Server • Master(Main) Server • Slave(Backup) Server
	• 기가비트용 랜 케이블 • UTP CAT.5E : 적용 가능 • UTP CAT.6 : 추천 • UTP CAT.7 : 적용가능 (고가)
	• 기가비트용 스위치 허브 • 전 포트가 기가비트의 속도로 지원되는 스위치 허브 (추천)
	• 기가비트 지원 랜 카드 • 랜 카드가 기가비트 전송속도를 지원하는 여부를 확인
	• 랜 부팅이 가능한 메인보드 • 메인보드 CMOS 설정 메뉴에서 랜 부팅 메뉴 선택이 가능해야 함

III. NDS 솔루션 보급현황

3.1 국외에서 유통되는 NDS 솔루션

전 세계적으로 유통되고 있는 대표적인 NDS 솔루션에는 HDDLESS 시스템이 있다. 하드리스 시스템은 중국 상하이에 본사를 두고 있는 글로벌 IT 기업인 RICHTECH(중국, 미국, 한국 지사 보유 등)사에서 개발한 NDS 솔루션이다. 그 중에서도 중국은 최초로 NDS 솔루션을 도입한 국가로서, 통상적으로 대규모 단위의 PC방을 운용하는 중국 시장의 특성상 NDS 솔루션이 보편화 되어 있다. 실제로 2011년을 기준으로 중국에는 전체 PC방의 99%인 16만여 개의 PC방에서 NDS 솔루션을 도입하여 사용하고 있다. 그 중에서도 RICHTECH사의 HDDLESS 시스템이 중국 전체 PC방 시장의 60%(9만여개)를 점유하고 있다〔3〕. 이 밖에도 중국 PC방 시장의 경우, MZD, CCBOOT, VHD에서 배포 중에 있는 여러 가지 NDS 솔루션들을 사용하고 있는데, 기본적으로 RICHTECH사의 HDDLESS 시스템과 동일한 소스 코드를 사용하기 때문에 기능 및 성능 측면에서 큰 차이는 없다.

3.2 국내에서 유통되는 NDS 솔루션

〔표 2〕는 현재 국내 PC방 시장에서 유통되고 있는 NDS 솔루션의 종류에 대하여 정리한 내용이다.

〔표 2〕에서 보는 바와 같이, 국내에 보급 중인 NDS 솔루션은 크게 네 가지가 있으며, NDS 솔루션을 도입하고 있는 국내 PC방은 약 1000여개 가량 된다. 또한 로컬 시스템에 요구되는 HDD의 크기 증가와 SSD 도입 비용의 부담 등으로 인하여 NDS 솔루션을 도입하는 PC방의 수가 지속적으로 증가하고 있는 추세이다.

현재 국내 PC방 시장에서 유통되고 있는 NDS 솔루션 제품은 모두 중국 시장을 통해 들여온 제품들인데, 중국 시장에 비교하여 IT 강국인 국내의 NDS 솔루션 도입이 늦어진 원인은 아이러니하게도 국내 데이터 통신의 빠른 속도에 기인한다. 즉, 기가 비트 단위의 빠른 데이터 전송속도를 보장하기 위한 기술적인 보완 및 물리적인 장비 개발의 소요에 따라 국내 PC방 시장에서의 NDS 솔루션 도입은 다소 늦어졌다고 볼 수 있다.

〔표 2〕 국내 보급 중인 NDS 솔루션의 종류〔4〕

제품명	한국유통사	버전	중국 기업
NOHDD	㈜리더스소프트	윈도우, 리눅스	MZD, 신우
HDDLESS	㈜하드리스	윈도우	RICHTECH
슈퍼피방	㈜참네트워크, ㈜와이디엠	윈도우	CCBOOT
스카이넷	아이닉스피사모, ND솔루션	리눅스	VHD

한편, 최근에는 PC방뿐만 아니라 학교, 시(도)청, 항만 등의 기관에서도 NDS(No Disk System)을 도입하고 있다. 국내의 NDS 총판 업체에서는 위와 같은 특정 기관에서 해당 시스템을 사용할 수 있도록 기존의 NDS 솔루션에서 일부 기능을 추가한 솔루션을 출시하고 있다. 그 중에서도 가장 대표적인 것은 VTOP 솔루션으로 위에서 언급한 스카이넷 21 솔루션에 몇 가지 기능을 추가한 버전이다.

기본적으로 현재 국내의 PC방에서 유통되고 있는 네 가지 솔루션과 앞서 언급한 VTOP 솔루션은 모두 동일한 원리로서 구동되며, 그 형태와 구조 그리고 특성까지 큰 차이점이 존재하지는 않는다. NDS 환경에서의 사용자 행위 분석 방법에 대한 연구를 위하여 저자는 VTOP 솔루션을 실제 환경과 동일하게 구성하였으며, 이후 사용자 행위분석을 위한 테스트를 진행하였다.

IV. NDS 실험환경 구축 및 동작 원리

4.1 NDS 실험환경 구축

NDS 환경에서의 사용자 행위에 대한 분석 실험을 위하여 위에서 언급한 VTOP 솔루션을 실제 사용자 환경과 동일하게 구성하였는데, 세부 테스트 구축 환경은 〔표 3〕과 같다.

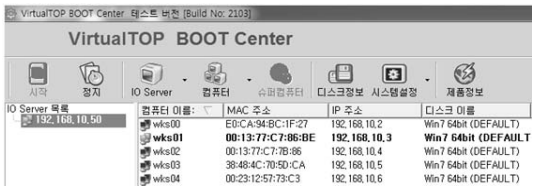
〔표 3〕에서 보는 바와 같이, VTOP 솔루션의 서버

〔표 3〕 NDS 환경의 세부 실험환경

구 분	OS	System Configuration	Install Program
Server PC	Win 7	〈CPU〉 DualCore Intel Core 2 Duo E8400, 3000 MHz 〈Main Board〉 Intel Eaglelake Q43	VTOP-Server- 2013.exe
Client PC #1	Win 7	〈CPU〉 Intel Core i5 650 〈Main Board〉 Intel Havendale IMC	VTOP-Win7 - 2369.exe (서버와의 연동을 위한 클라이언트 프로그램)
Client PC #2			
Patch 전용 PC			
유의사항	· CMOS 설정에서 LAN BOOTING을 지원해야 함 · 모든 클라이언트 PC 및 Patch 전용 PC의 시스템 사양이 동일해야 함 (For Desktop Provisioning) · IP 자동 할당을 위한 DHCP 서버 구성 필요		

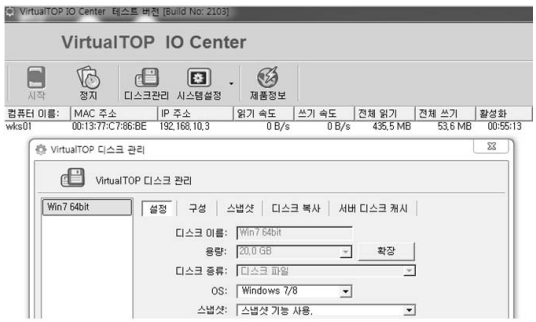
에는 VTOP-Server 프로그램을 별도로 설치해야 한다. VTOP 서버에 해당 프로그램을 설치하면 두 종류의 GUI 관리자 프로그램이 자동 생성되는데, 각각의 프로그램에서 수행하는 기능은 다음과 같다.

첫째, VirtualTOP Boot Center가 생성 되는데, 해당 프로그램은 클라이언트 PC들에 대한 전반적인 관리(MAC 주소, IP 주소, 컴퓨터 이름 등 관리) 업무를 수행한다. 또한 네트워크 정보 등 각종 시스템을 설정하고, 로컬에서 서버로의 디스크 복사 승인여부를 결정하며, 슈퍼 컴퓨터[1] 의 지정 및 해제 등의 역할을 수행한다.



〔그림 2〕 VirtualTOP BOOT Center

둘째, VirtualTOP I/O Center가 생성되는데, 해당 프로그램은 클라이언트 PC의 부팅 이미지가 되는 VM 디스크 이미지를 생성 및 관리하고, 각종 시스템 경로(DISK, USER, WKS) 등을 설정하는 역할을 수행한다.



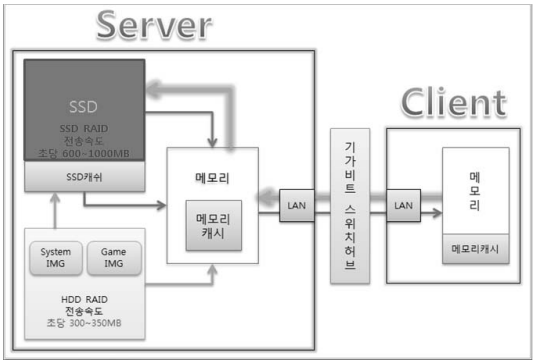
〔그림 3〕 VirtualTOP I/O Center

4.2 데이터 교환 방식

NDS 환경에서는 기본적으로 클라이언트 PC단에 하드 디스크가 존재하지 않으며, 일정량의 데이터가메모리에 저장된다. 결국 NDS에서 데이터를 읽고 쓰기

1) 클라이언트 PC의 변경사항(업데이트, 프로그램 추가 등) 관리를 위한 일종의 관리자 모드 PC

위해서는 서버와 클라이언트 간의 네트워크 통신이 이루어져야 한다. [그림 4]는 NDS 솔루션의 데이터 전송 방식을 요약한 내용이다.



[그림 4] No Disk System의 데이터 교환[5]

4.2.1 데이터 쓰기

클라이언트 PC에서 데이터를 쓰는 방식은 크게 총 두 가지로 구분할 수 있다.

첫째, 시스템을 효율적으로 운용하기 위해 클라이언트에 장착된 메모리의 일부분을 램 디스크로 활용하는 방식이다. 램 디스크는 이름 그대로 시스템 메모리의 일부를 로컬 디스크로 인식시키는 것으로, 이를 사용하면 읽기/쓰기 속도가 기존 하드디스크보다 훨씬 속도가 빠른 장점이 있다.

둘째, 램 디스크의 공간이 꽉 차면 기가비트 속도의 네트워크 망을 이용해서 서버 SSD(HDD)에 파일을 쓰는 방식이다.

4.2.2 데이터 읽기

클라이언트 PC에서 데이터를 읽는 방식은 크게 총 세 가지로 구분할 수 있다.

첫째, 클라이언트 PC에서 가장 많이 사용하는 1순위 프로그램을 서버 메모리의 일정 영역에 캐시로 자동 저장을 하는 방식이다. 해당 영역에 특정 파일이 저장되면 클라이언트는 메모리에서 직접 파일을 전송받을 수 있다. 다시 말해, 서버 메모리의 일부분을 램 디스크로 활용하여 성능을 극대화시키는 방식이다.

둘째, 서버 메모리 영역의 캐시 용량이 초과되면 일정 공간의 SSD를 캐시로 사용하는 방식이다.

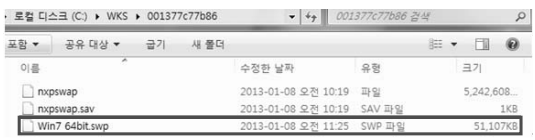
마지막으로, 서버의 SSD 캐시 영역을 모두 사용하면 SSD와 HDD에서 직접 파일을 전송 받는 방식이다. 이 경우, 효율적인 시스템 운영을 위하여 고사양 프로그램 등은 최대한 SSD에 저장하며, 저사양 프로그램 등은 HDD에 저장하는 것이 유리하다.

4.3 NDS 솔루션의 기본 구동 원리

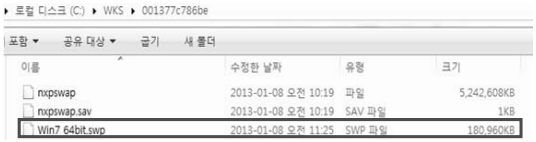
NDS 환경에서 클라이언트 PC를 구동하면, 서버 하드 디스크에 저장된 부트 이미지를 통한 PXE 부팅이 시작된다. 부트 이미지의 경로는 서버의 [C드라이브]-[\Disk]-[\부트 디스크 이름] 경로의 Disk 파일이며, 해당 경로는 [I/O Center]에서 관리자가 임의로 지정할 수 있다.

부팅 이후, 클라이언트 PC에서 사용자의 모든 행위는 [C드라이브]-[\WKS]-[\Mac Address] 경로의 (부트디스크).swp 파일에 기록되며, 부트 이미지와 동일하게 swp 파일의 해당 경로도 [I/O Center]에서 관리자가 임의로 지정할 수 있다.

활성 상태의 클라이언트 PC 상에서 특정 크기(129,136KB)의 파일을 복사한 이후, 서버 내의 (부트디스크).swp 파일의 크기 변화를 확인해 본 결과 [그림 5], [그림 6]에서 보는 바와 같이, 복사된 파일의 크기만큼 swp 파일의 크기가 증가한다.



[그림 5] 활성 상태에서 특정 파일 복사 이전



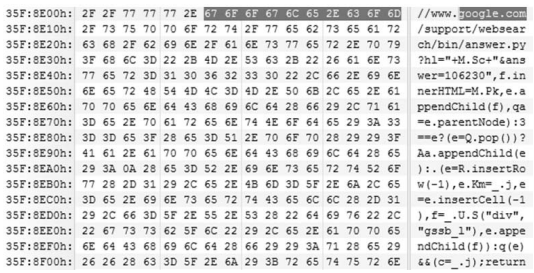
[그림 6] 활성 상태에서 특정 파일 복사 이후

V. NDS 환경에서의 사용자 행위 분석

5.1 NDS 환경에서의 사용자 행위 확인

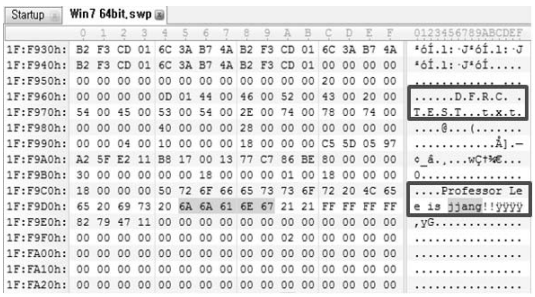
NDS 환경에서의 사용자 행위에 대한 흔적을 확인하기 위하여 몇 가지 테스트를 수행해 보았다.

첫째, 특정 사이트(www.google.com)를 방문한 이후 서버 내의 swp 파일에서 해당 URL을 검색해 본 결과, [그림 7]과 같이 정확히 식별 되었다.

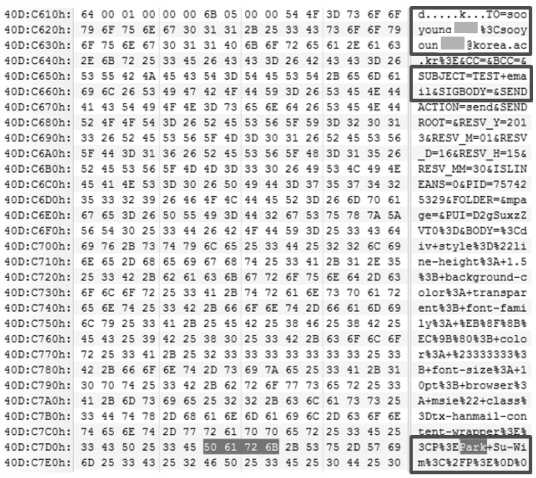


〔그림 7〕 인터넷 접속 사이트 흔적 확인

둘째, 임의의 텍스트 문서를 생성 및 저장하고 서버 내의 swp 파일에서, 해당 텍스트 문서의 제목과 내용을 String Search 방법으로 확인해 보았다. 텍스트 문서의 제목은 'DFRC Test.txt'이며, 문서의 내용은 'Professor Lee is jjang!!'이었다. 실험 결과 〔그림 8〕에서 보는 바와 같이, swp 파일에서 임의로 저장한 텍스트 문서의 제목과 내용이 제대로 검색 되었다.



〔그림 8〕 스트링 검색 결과



〔그림 9〕 사용자 E-Mail 이용 흔적 확인

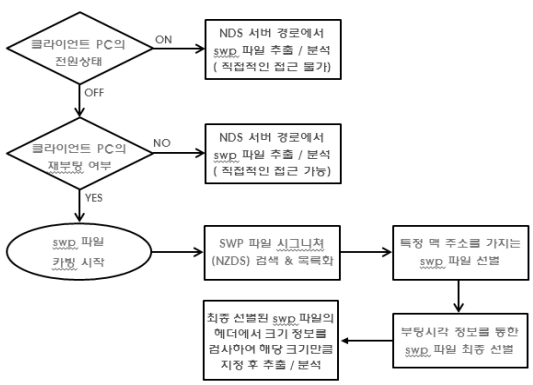
셋째, 특정 메일을 보낸 이후 서버 내의 swp 파일에서 사용자가 전송한 메일의 주소, 제목, 메일의 내용들에 대해서 검색해 보았다. 테스트에 사용된 수신자의 이메일 주소는 sooyounxxxx@korea.ac.kr이며, 제목은 'TEST email', 내용은 'Park Su-Wim'이었다. 실험 결과 〔그림 9〕에서 보는 바와 같이, 전송된 Test E-mail에 대한 모든 정보가 swp 파일에서 제대로 검출됨을 볼 수 있다.

추가적인 실험을 통해서 확인해 본 결과, swp 파일에는 각종 포털 사이트에 로그인 시 입력하는 ID 정보를 비롯하여 검색 창에 입력하는 Keyword 값 등 사용자 행위에 의해 발생되는 모든 데이터들을 포함하고 있음을 알 수 있었다.

5.2 NDS 환경에서의 swp 파일 획득 방법

NDS 솔루션의 경우, 로컬 클라이언트 PC에는 하드 디스크가 존재하지 않기 때문에 전원을 종료하고 시스템을 재부팅 할 시, 항상 표준화된 Desktop 환경을 제공하는 특성이 있다. 결과적으로 활성 상태인 클라이언트 PC에서의 사용자 행위 정보는 NDS 서버의 swp 파일을 분석함으로서 손쉽게 획득할 수 있는 반면에, 시스템이 재부팅 되는 경우에는 NDS 서버의 swp 파일이 초기화되기 때문에 시스템 사용자의 행위 정보를 일반적인 방법으로는 획득할 수 없다.

결국 NDS 환경에서 클라이언트 PC의 재부팅이 일어난 경우에는 서버 디스크의 비할당 영역에서 특정 swp 파일을 카빙하는 방법으로 데이터를 획득해야만 한다. 또한 반복적인 테스트를 진행해 본 결과, swp 파일의 초기화는 시스템이 종료되는 시점에 발생하는 것이 아니라 시스템이 재부팅되어 표준화된 Desktop



〔그림 10〕 NDS 환경에서의 swp 파일 획득 절차

을 Delivery 하는 시점에 발생됨을 확인하였다.

결과적으로, NDS 환경에서 사용자 행위를 분석하기 위해서는 swp 파일을 획득해야 하는데, swp 파일을 획득하는 방법은 아래 〔그림 10〕과 같이 다음 세 가지 상황에 따라 상이하게 적용될 것으로 보인다.

5.2.1 클라이언트 PC가 활성 상태인 경우

클라이언트 PC가 활성 상태인 경우에는 해당 시스템 사용자의 행위가 NDS 서버의 swp 파일에 고스란히 남게 된다. 따라서 NDS 서버의 swp 파일 경로에 접근하여 해당 파일을 분석하면 되는데, 시스템이 활성상태인 경우에는 해당 파일에 대한 직접적인 접근이 불가능하기 때문에 전용 도구를 활용하여 해당 드라이브를 마운트 한 이후, 특정 swp 파일을 추출하여 분석하면 된다.

5.2.2 클라이언트 PC가 비활성 상태이나 재부팅이 일어나지 않은 경우

클라이언트 PC가 비활성 상태이나 재부팅이 일어나지 않은 경우에는 NDS 서버의 swp 파일이 초기화되지 않는다. 따라서 위와 같은 경우에는 해당 swp 파일 경로에 물리적으로 접근하여 해당 파일을 추출한 이후 분석을 진행하면 된다.

5.2.3 클라이언트 PC에서 재부팅이 일어난 경우

클라이언트 PC에서 재부팅이 일어나면, 기존의 swp 파일은 삭제되고 새로운 swp 파일이 할당되기 때문에 NDS 서버 디스크의 비할당 영역에서 특정 swp 파일을 카빙해야 한다. 일반적으로 NDS 서버의 디스크에는 로컬 클라이언트들의 swp 파일들이 무수히 많이 존재한다. 따라서 포렌식 조사관이 원하는 특정 swp 파일만을 선별하여 카빙하기 위해서는 다음과 같은 정보들이 우선적으로 파악되어야 한다.

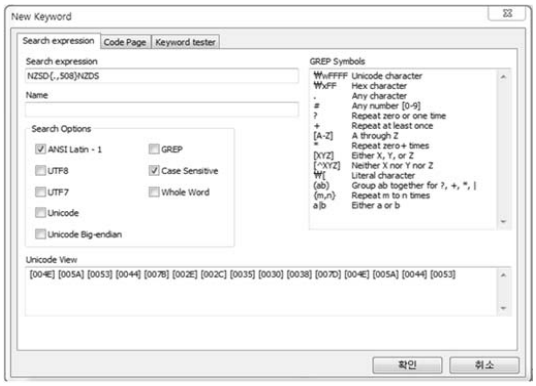
첫째, 클라이언트 PC의 MAC 주소 정보를 알아야 한다. 이는 NDS 환경에서의 수많은 클라이언트 PC들 중에서 특정 클라이언트 PC의 swp 파일들만을 수집하기 위해 필요한 정보이다.

둘째, 부팅 시간 정보(OLE Time)를 알아야 한다. 이는 클라이언트 PC에서 사용자가 이용을 시작했을 때의 시간 정보인데, 해당 정보를 알아야만 클라이언트 PC의 MAC 주소 정보를 통해 추출된 swp 파일들 중에서 특정 사용자가 해당 시간대에 사용했을 것이라 예상되는 swp 파일만을 선별할 수 있다.

셋째, swp 파일의 크기 정보를 알아야 한다. 위 두 단계를 거쳐 최종 선별된 swp 파일의 특정 offset에서 해당 swp 파일의 크기 정보를 얻을 수 있는데, 획득된 swp 파일의 크기 정보를 통하여 시작 지점에서부터 해당 swp 파일의 크기만큼 데이터를 지정하여 추출할 수 있다.

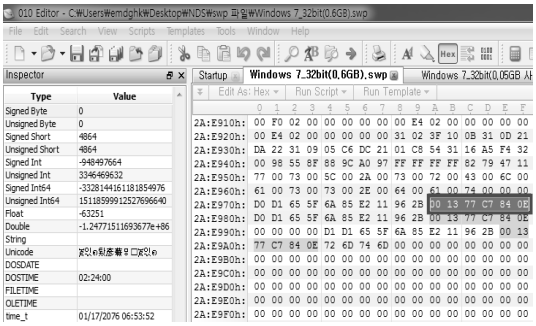
지금부터는 위에서 언급한 정보들을 활용하여 구체적인 카빙 방법에 대하여 알아보도록 하겠다.

먼저 〔그림 11〕과 같이, EnCase의 Signature (NZSD) 검색 기능을 활용하여 NDS 서버 디스크의 비할당 영역에 존재하는 swp 파일들을 추출한다.



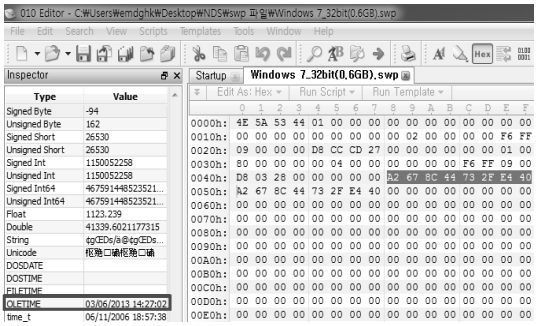
〔그림 11〕 시그니처 검색을 통한 swp 파일 추출

둘째 아래 〔그림 12〕와 같이, 추출된 수많은 swp 파일들 중에서 클라이언트 PC의 MAC 주소 정보를 이용(ASCII String 검색)하여 특정 주소를 가지는 클라이언트 PC의 swp 파일만을 선별한다.



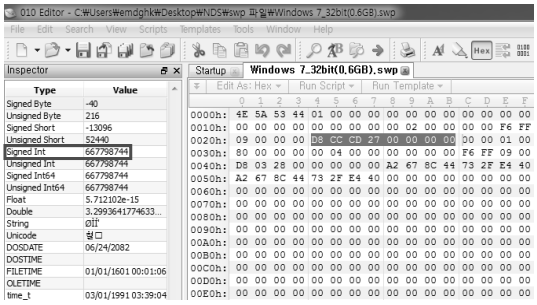
〔그림 12〕 MAC 주소 정보를 통한 swp 파일 선별

셋째, 위에서 선별된 swp 파일 중에서 시간 정보(OLE Time)를 검사하여 찾고자 하는 swp 파일을 최종 선별한다. 이 때 시간정보는 아래 〔그림 13〕에서 보는바와 같이, swp 파일 헤더의 Offset 0x48 ~ 0x4F(8byte)에서 확인할 수 있다.



〔그림 13〕 부팅 시각 정보를 통한 최종 swp 파일 선별

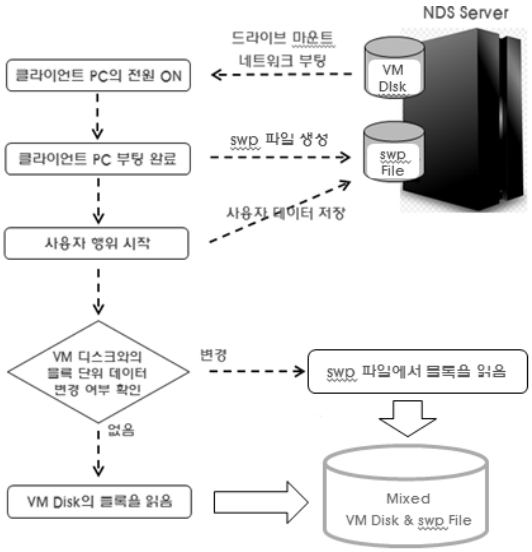
마지막으로, 최종 선별된 swp 파일에서 크기 정보를 검사하여 시작 지점에서부터 해당 swp 파일의 크기만큼 데이터를 지정하여 추출한다. 이 때 swp 파일의 크기정보는 아래 〔그림 14〕에서 보는바와 같이, swp 파일 헤더의 0x24 ~ 0x2B(8byte)에서 확인할 수 있다.



〔그림 14〕 swp 파일의 크기 정보 확인

5.3 NDS 환경에서의 사용자 행위 분석 방법

NDS 환경에서의 사용자 행위를 분석하기 위해서는 NDS 서버의 원본 VM Disk 파일과 각각의 클라이언트별로 생성되는 swp 파일이 필요하다. VM Disk 파일의 경우에는 NDS 서버에서 손쉽게 물리적으로 획득할 수 있으며, swp 파일의 경우에는 앞서 언급한 바와 같이 직접 접근 또는 카빙의 방법으로 획득이 가능하다.



〔그림 15〕 NDS 환경에서의 데이터 관리(읽기)

위 〔그림 15〕는 NDS 환경에서 실제 데이터를 관리(읽기)하는 방법을 요약한 내용이다. 위와 같이, NDS 환경에서는 내부적으로 사용자 행위로 인하여 변경되는 데이터들을 swp 파일을 통하여 관리하는데, 해당 시스템에서는 우선적으로 원본 VM 디스크를 기준으로 블록 단위별 데이터 변경 여부를 확인하게 된다. 이후, 데이터가 변경된 블록은 해당 클라이언트의 swp 파일에서 데이터를 읽어 들이고, 데이터가 변경되지 않은 블록은 원본 VM 디스크에서 데이터를 읽어 들인다.

NDS 환경에서는 위와 같은 과정을 통하여, 시스템 자체적으로 원본 VM 디스크와 swp 파일이 Mix된 일종의 가상 디스크 이미지를 생성하게 된다. 결과적으로 NDS 환경에서 사용자 행위를 분석하기 위해서는 1차적으로 원본 VM 디스크와 swp 파일이 Mix된 가상 디스크 이미지를 생성해야 한다. 이후에는 해당 디스크 이미지를 마운트 한 뒤, 일반 디지털 포렌식의 절차와 동일한 방법으로 분석을 시도하면 되겠다.

VI. 결 론

최근 세계적인 경제 위기 속에서 비용 절감을 위한 하나의 대안으로서 클라우드 컴퓨팅(Cloud Computing)은 위기 극복을 위한 최적의 솔루션으로 빠르게 부상하고 있다. 또한, 빅 데이터 시대의 도래와 함께 SSD(HDD) 도입 비용의 증가 등에 따라 최근 국내외 PC방 및 기관에서는 클라우드 컴퓨팅 기반의 스

토리지 가상화 기술을 접목시킨 NDS(No Disk System) 솔루션을 도입하고 있는 추세이다.

본 논문에서는 NDS 환경에서의 사용자 행위 분석에 대한 연구를 진행하였는데, 향후 추가적으로 보완·발전시켜야 할 사항들에 대해서 간략히 언급하고자 한다.

첫째, NDS 환경에서 로컬 클라이언트가 재부팅되는 경우, 카빙 기술을 사용하여 사용자 데이터를 복구할 수 있음을 실험을 통해서 확인하였는데, 현실적으로 삭제된 swp 파일을 카빙하기에는 많은 어려움이 있다는 점이다. 왜냐하면, 해당 서버의 디스크 크기는 매우 클 뿐만 아니라, 해당 디스크에는 수많은 swp 파일들이 존재할 것으로 예상되는데, PC방의 경우 해당 서버에서 특정 swp 파일을 선별하여 카빙하기 위해서는 많은 시간이 소요될 것으로 예상된다. 이는 결과적으로 해당 NDS 시스템의 과부하를 초래하거나 정상적인 시스템 사용에 제한을 줄 것으로 보인다. 이와 같은 측면에서 볼 때, NDS 환경에서의 사용자 행위 분석은 해당 클라이언트 PC가 재부팅이 일어나지 않거나 활성 상태인 경우에 수행하는 것이 바람직할 것으로 보인다.

둘째, 본 논문에서는 NDS 환경에서의 사용자 행위 분석을 위한 방법으로서, NDS 서버의 특정 경로에 저장된 swp 파일을 추출/분석하는 내용만을 다루었다. 하지만, 추가적으로 로컬 클라이언트의 메모리와 캐시 정보 등을 분석한다면 디지털 포렌식 관점에서 볼 때 좀 더 유용한 정보 등을 획득할 수 있을 것이라 생각한다.

셋째, NDS 환경에서의 사용자 행위 정보는 결과적으로 NDS 서버 내의 swp 파일을 통해서 획득할 수 있는 바, 향후에는 swp 파일의 구조에 대한 분석, 파일 시스템 분석과 같은 연구가 추가적으로 진행되어야 할 것으로 보인다.

참고문헌

〔1〕 http://msdn.microsoft.com/en-us/library/ms912891(v=winembedded.5).aspx

〔2〕 http://en.wikipedia.org/wiki/Diskless_node

〔3〕 HDDLESS, "하드리스 시스템 소개," http://hddlesshn.com/base/m5/menu1.php?com_board_basic=read_form&com_board_idx=11&com_board_page=&com_board_search_code=&com_board_search_value1=&com_board_search_value2=&left=1&topmenu=5, 2012년 6월.

〔4〕 http://blog.naver.com/ddparkid?Redirect=Log&logNo=20168646035

〔5〕 RICHTECH KOREA, "하드리스 시스템," http://www.richtechkorea.com/Page/Business.php?page_num=1, 2013년 2월.

〔6〕 "VTOP_운영설명서(Version : 3.0.1).pdf," http://www.virtualtop.co.kr

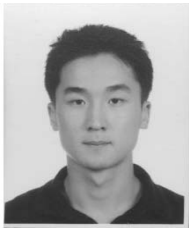
〔7〕 "VTOP_설치설명서_Windows_7_Client.pdf," http://www.virtualtop.co.kr

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

〔9〕 Dominik Birk, "Technical Challenges of Forensic Investigations in Cloud Computing Environments," Workshop on Cryptography and Security in Clouds, pp. 1-8, January 2011.

〈저자소개〉

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



남 궁 재 웅 (Jaeung Namgung) 학생회원
2010년 2월: 세종대학교 전자정보공학대학 컴퓨터전공 공학사
2011년 3월~2013년 2월: 고려대학교 정보보호대학원 석사수료
〈관심분야〉 디지털 포렌식, 데이터베이스 포렌식

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

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