DOI: 10.3745/KIPSTC.2010.17C.4.335

Mac OS X 운영체제상의 사용자 흔적정보 수집방안 연구

최 준 호[†] · 이 상 진[††]

요 약

Mac OS X는 애플에서 제작한 컴퓨터 운영체제이다. 1984년도부터 MAC OS의 마지막 버전인 9를 계승하여 지금의 Mac OS X 10.6(Snow Leopard)에 이르고 있다. 전 세계 운영체제 점유율에서 애플의 Mac OS X운영체제는 10% 정도를 차지하고 있으나, 현재 디지털 포렌식 조사에 활용되고 있는 포렌식 도구들은 Mac OS X에 대한 포렌식 분석을 제대로 수행할 수 없다. Mac OS X에 대한 포렌식 조사를 하는데 있어서, 운영체제 상에서 사용자의 행위와 흔적과 관련된 정보는 중요한 디지털 증거가 될 수 있다. 본 논문에서는 Mac OS X 운영체제 상의 사용자 흔적 정보 수집에 관한 방안을 제시한다.

키워드 : 디지털 포렌식, 애플 매킨토시 운영체제, 사용자 흔적 정보

The Acquisition Methodology Study of User Trace Data in Mac OS X

Joonho Choi[†] · Sangjin Lee[††]

ABSTRACT

Mac OS X is the Computer Operating System that develop in Apple Inc. Mac OS X is the successor to Mac OS 9 Version which had been Apple's primary operating system since 1984. Recently, Mac OS X 10.6 (Snow Leopard) has been manufactured and is distributed to user. Apple's Mac OS X Operating System is occupying about 10% in the world Operating System market share. But, Forensic tools that is utilized on digital forensic investigation can not forensic analysis about Mac OS X properly. To do forensic investigation about Mac OS X, information connected with user's action and trace can become important digital evidence in Operating System. This paper presents way about user trace data acquisition methodology in Mac OS X.

Keywords : Digital Forensic, Apple Mac OS X, User Trace Data

1. 서 론

Mac OS X는 10.0버전의 Cheetah를 시작으로 하여, 최근에는 Snow Leopard(1.6)가 개발되어 사용자에게 배포되고 있다. Mac OS 시스템은 Darwin 커널 위에 OpenGL 기반의 그래픽 계층이 존재하며 상위에 Cocoa, Carbon과 같은 기술을 활용한 애플리케이션 계층과 Aqua GUI 환경을 제공한다.[2]

전통적으로 Mac 운영체제는 전자출판, 디자인, 멀티미디어 부문 등에서 높은 시장 점유율을 차지하고 있었다. 현재의 Mac 운영체제는 랩톱 컴퓨터 Mac Book, 데스크톱 컴퓨터 iMac을 비롯한 iPod, iPhone, iPad와 같은 휴대용 모바일 기기에 이르기까지 광범위하게 탑재되어 전 세계적으로 많은 사람들에 의해서 이용되고 있다. 기존의 전자출판, 디자인과 같은 미디어를 포함한 Mac OS에 대한 활용성이 일반 개인 사용자에게도 사용률이 점차 증가하고 있다.

Mac OS X를 사용하는 일반 컴퓨터 사용자가 증가함에 따라 Mac OS X를 조사할 가능성이 높아지고 있다. 실제로, "The New York State Computer Crime Unit"의 자료에 의하면 전체 컴퓨터 범죄 수사 중에 만나게 되는 대상 시스템 중에 약 5~10%가 Mac OS X임을 확인할 수 있다.[1] 그러나 최근까지 운영체제에 대한 포렌식 분석기법연구 등은 MS Windows 또는 Linux 계열의 OS 위주로 이루어져 왔다.

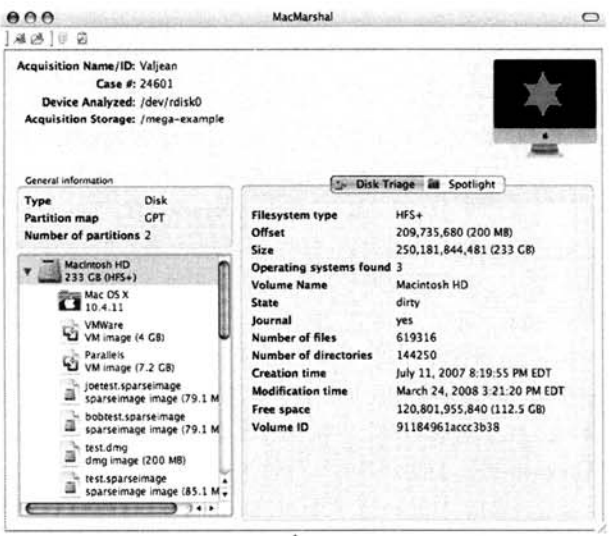
기존의 MS 계열 운영체제 위주로 연구가 진행되어 오던 디지털 포렌식 분석 기법으로는 MS의 운영체제와는 전혀 다른 원리와 구조를 가진 Mac OS X를 조사하는 것은 어렵다. 본 논문에서는 Apple Mac OS X Leopard(10.5)와 최근에 출시된 Snow Leopard(10.6) 운영체제에서 중요 증거가 될 수 있는 사용자 흔적 정보 수집에 관한 방안을 제시한다.

† 준 회 원 : 고려대학교 디지털 포렌식 연구센터 연구원
†† 종신회원 : 고려대학교 정보경영공학전문대학원 교수
논문접수 : 2010년 4월 15일
수 정 일 : 1차 2010년 6월 1일
심사완료 : 2010년 6월 15일

2. 관련 연구

Mac 운영체제에 대한 디지털 포렌식 분석 기법 분석의 필요성이 요구되면서 기초적으로 Mac OS X를 분석하는데 있어서 사전에 준비해야 할 항목과 시스템에 대한 포렌식 절차와 기법에 관한 기초적인 사항에 대해서 Phlip Craiger가 서술했다.[8, 12] Phlip Craiger가 제시한 기본적인 Mac OS X 분석을 위해 필요한 준비사항과 절차를 바탕으로 Mac OS X 시스템에 대한 디지털 포렌식 분석에 있어 필요한 점검 사항과 분석대상으로 삼아야 할 시스템상의 중요 항목에 대해서 Robert A. Joyce[1], Nick Peelman[13]이 언급했다. 이와 같은 Mac OS X 포렌식 연구에서 Mac 운영체제의 디지털 포렌식 분석을 위해서 필요한 검사항목과 조사해야 할 사항에 대해서 제시가 되었다.

기존의 연구를 바탕으로 좀 더 효율적인 Mac OS X 디지털 포렌식 분석을 위한 MacMarshal과 같은 Mac 운영체제 디지털 포렌식 분석 도구가 개발, 판매되고 있다.(그림 1) 그러나 앞서 제시된 Mac OS X 디지털 포렌식 분석 방법과 도구에서는 Mac OS X 시스템 상에서 분석해야 할 대상 선정에 있어 운영체제의 기초적인 사항만을 논하고 있어, 포렌식 분석 과정에서 필요한 사용자 행동을 파악하기 위해 필요한 중요 정보를 획득하는데 어려움이 있다. 또한 언급한 운영체제상의 중요 항목을 분석하기 위한 좀 더 구체적이고 자세한 기법연구가 부족하기 때문에 사용자 흔적 정보 수집에 대한 효과적인 방안을 세울 수가 없다. 이에 본 논문에서는 Mac OS X 시스템 상의 사용자 행위를 유추 또는 역추적 할 수 있는 중요 사용자 행위 및 흔적 정보를 효과적으로 수집할 수 있는 방안을 제시하고자 한다.



(그림 1) Mac Marshal

3. Mac OS X 포렌식 분석을 위한 준비 단계

기존의 Windows / Linux 계열 디지털 포렌식 조사시 활성 데이터 수집 및 여러 다양한 디지털 포렌식 분석에 앞서 지켜야할 사항과 준비과정에 관한 작업을 Mac 환경에서 수행할 경우 신속한 라이브 데이터 수집 및 기타 여러 분석에 방해를 줄 수 있으며, 중요한 디지털 증거의 무결성을 손상시킬 수 있다. Mac OS X 시스템의 원활한 데이터 수집과 디지털 증거의 무결성을 지키기 위해서는 Mac 운영체제의 포렌식 작업을 수행하는 분석가는 Windows/Linux 계열과는 다른 Mac 운영체제만의 특성을 파악하고 이해하고 있어야 한다.

3.1 장치 중재 데몬 시스템 (Disk Arbitration)

Mac OS X에서는 사용자 컴퓨터상에 새롭게 마운트, 언마운트가 이루어지는 저장장치나 미디어 관련 또는 파일 시스템 상에서 변화되는 상황에 대해서 실시간으로 감시/제어하고 이에 대한 사항을 운영체제에 통보하기 위한 장치 중재 데몬이 있다. Mac OS X에서는 사용자가 일일이 직접 새로운 하드웨어나 저장장치를 추가하기 위해 마운트, 언 마운트를 실행해야 할 필요가 없이, 장치 중재 데몬에 의한 장치 관리가 자동으로 이루어진다.[2] 포렌식 분석을 수행하기 위해 USB, CD와 같은 매체를 대상 컴퓨터에 장착시켰을 경우 장치 중재 데몬 시스템에 의해 지정된 파티션 지점에 장치가 마운트 된다. 이러한 장치의 변경 사항은 현재 운영체제에서 동작중인 모든 프로세스에 통보가 되고, 최종적으로 조사가 진행 중인 도중에 대상 하드 디스크 드라이브에 변화를 일으켜 버린다.[8] 이러한 사항은 디지털 포렌식 분석에 있어서 최고 우선시 되고 있으며, 가장 중요한 사항인 증거의 무결성을 해칠 수 있는 요소가 된다. Mac OS X에 대한 활성시스템 조사 및 하드 디스크 드라이브 이미지 복사를 수행하기 위해서는 조사대상 컴퓨터의 '/usr/ sbin/diskarbitrationd' 서비스를 중지시켜야 한다.

3.2 Property List

Apple 계열의 운영체제는 시스템 운영에 필요한 설정, 관련 옵션, 프로그램/서비스 로그, 파일 속성 정보와 같은 다양한 데이터를 Property List 파일에 저장한다. Property List 파일은 다양한 형태의 정보를 객체화 시켜 저장하고 있는 직렬화 파일로서 확장자명을 .plist를 사용한다. .plist 파일은 Apple에서 자체적으로 정의한 DTD(Document Type Declaration)를 사용하는 XML (Extensible Markup Language) 포맷을 기반으로 하고 있다.[3] Mac OS X에서 동작하는 어플리케이션은 .plist 파일에 XML형태의 Foundation class/Core Foundation Type[1]을 활용하여, 새롭게 데이터를 추가하거나 수정/삭제한다. 각 class, type에서 지정한 XML 태그와 저장되어 있는 데이터의 형태는 <표 1>과 같다.

1) Foundation Class는 배열, 스트링, 날짜 데이터 등에 관련된 클래스를 제공하는 기본적인 프레임워크 구성이다. Core Foundation Type은 프레임워크에서 사용하는 다양한 형태의 콜렉션 객체를 정의하고 있다.

〈표 1〉 Property List Format

Foundation class	CoreFoundation type	XML 태그	데이터 포맷
NSString	CFString	<string>	UTF-8 문자열
NSNumber	CFNumber	<real>, <integer>	십진수 숫자
NSNumber	CFBoolean	<true />, <false />	태그만 존재함
NSDate	CFDate	<date>	ISO 8601 문자열
NSData	CFData	<data>	Base64로 인코딩된 데이터
NSArray	CFArray	<array>	배열로 데이터를 저장
NSDictionary	CFDictionary	<dict>	<key> 태그, 속성 태그

3.3 기본 디렉터리 구조

초기 Mac 운영체제는 Unix 기반으로 하였기 때문에, 동일한 디렉터리 구조와 파일명을 그대로 사용하는 경우도 있으나, 최근 배포되고 있는 Mac OS X의 경우에는 Unix 운영체제와 다른 디렉터리 구조를 가지고 있다. 시스템을 운영하기 위해 필요한 설정파일과 시스템이 기본적으로 기록하는 로그파일은 /Library 폴더에 기록이 된다. 각 어플리케이션이 사용하는 각종 설정과 옵션이 기록된 파일과 로그는 /Users/[User ID]/Library 폴더에 저장되어 있다.

시스템은 별다른 옵션을 주지 않는 이상 새롭게 추가되는 각 사용자가 이용하게 될 디렉터리를 /Users의 하위 폴더에 생성한다. 운영체제에 등록된 사용자와 그룹에게 할당되어 있는 디렉터리와 쉘, 유저 아이콘에 대한 정보는 /private/var/db/dslocal/nodes/Default 폴더(<표 2>)에 기록된다.

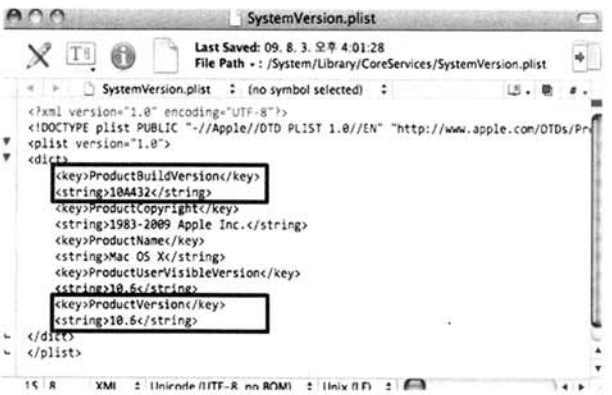
〈표 2〉 사용자 계정 및 그룹 정보

/private/var/db/dslocal/nodes/Default/users/*.plist
/private/var/db/dslocal/nodes/Default/groups/*.plist

3.4 운영 체제 버전

Mac OS X 시리즈의 운영체제는 각 버전마다 가지고 있는 OS의 특성에 따라 파일과 위치가 서로 제각각 이다. 이러한 운영체제 버전 상의 차이점에도 독립적인 포렌식 작업을 수행하기 위해서는 현재 iMac 데스크 탑 컴퓨터에 설치되어 있는 Mac 운영체제의 버전을 알아낸 후, 그에 해당하는 Mac OS X의 버전에 알맞은 적합한 포렌식 분석 기법을 선정해야 한다.

'/System/Library/CoreServices' 폴더에 속해 있는 'SystemVersion.plist' 파일(그림 2)은 현재 사용자 컴퓨터에 인스톨되어 있는 Mac OS X의 메이저 버전과 좀 더 자세한 운영체제의 빌드 버전에 관한 정보를 담고 있다.



(그림 2) SystemVersion.plist

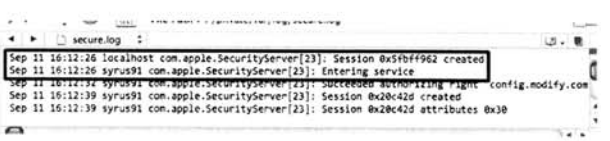
4. Mac OS X 운영체제의 사용자 흔적 정보 수집 방안

4.1 컴퓨터 부팅/종료 및 사용자 로그인 시각

컴퓨터의 부팅/종료 시각은 실질적으로 사용자가 보유한 iMac 데스크톱이 사용되었던 시간대를 알려주는 중요 데이터다. iMac 데스크톱이 시작해서 종료된 시간정보를 바탕으로 특정 시각에 컴퓨터의 구동 여부에 대해서 판단할 수 있다. Mac 운영체제가 설치되어 있는 컴퓨터의 부팅/종료/사용자 로그인 시각은 '/private/var/log/' 폴더의 secure.log에 기록되어 있다.

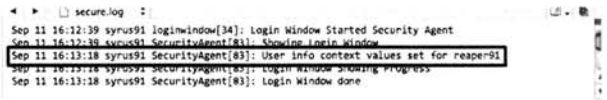
secure.log 파일에 운영체제가 부팅되면서 제일 먼저 시작하는 com.apple.SecurityServer 서비스가 구동된 시간정보로부터 컴퓨터의 전원이 켜진 시각(그림 3)을 확인할 수 있으며, 특정 사용자에 의해 컴퓨터가 종료된 시간정보(그림 4)는 secure.log에 기록되어 있는 shutdown 작업이 시작된 시각으로 부터 얻을 수 있다.

사용자가 컴퓨터에 접근한 로그인 시각은 2가지 형태로 나뉘어 기록된다. 로컬에서 로그인하여 거치는 인증방식은 SecurityAgent에 의해 이루어지며, 원격 사용자에 의한 접

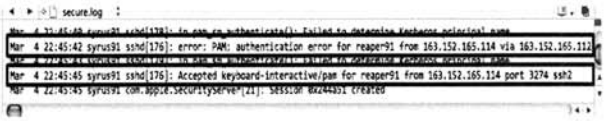


(그림 3) 컴퓨터 부팅 시각 (secure.log)

(그림 4) 컴퓨터 종료 시각 (secure.log)



(그림 5) 로컬 컴퓨터 사용자 로그인 시각 (secure.log)



(그림 6) 원격 컴퓨터 사용자 로그인 시각 (secure.log)

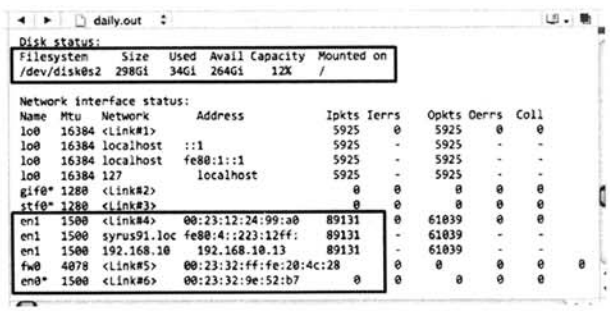
근은 telnet, ssh 등의 프로토콜에 의해 처리된다. 해당 서비스의 사용자 인증 기록을 secure.log에서 확인함으로써 로그인 시각을 알 수 있다.

4.2 하드 디스크 드라이브 / 네트워크 상태 정보

iMac 데스크톱은 기본적으로 하나의 단일 하드 디스크 드라이브와 유무선 네트워크 장비 그리고 블루투스와 FireWire와 같은 통신 장비를 탑재하고 있다. 사용자는 데스크톱에 새롭게 하드 디스크 드라이브를 추가/ 교체하고 자신만의 파티션으로 나누어 사용할 수 있으며, iMac의 네트워크 장비에 의해 인터넷 사용을 비롯한 각종 네트워크 통신 작업을 수행할 수 있다.

컴퓨터에 부착되어 있는 하드 디스크 드라이브와 네트워크 장비에 대한 사용기록은 '/private/var/log/' 폴더의 daily.out/weekly.out 각 파일에 하루/일주일 단위로 나뉘어 저장된다. 'daily.out/weekly.out' 파일에서 사용자가 지정한 파티션으로 마운트 했던 하드 디스크 드라이브와 네트워크 장비의 활성화 상태, 할당한 MAC/IP 주소에 대한 변경 내역을 확인할 수 있다.

이러한 정보를 기반으로 하드 디스크 드라이브의 파티션을 변경하거나 새롭게 추가했었던 사항과 전체크기, 사용량 변화, 네트워크 장비를 교체한 행위, 할당된 MAC/IP 주소의 변화를 추적할 수 있다.



(그림 7) daily.out

4.3 자동 실행 프로그램

운영체제가 사용하는 프로세스를 제외하고 Mac OS 시스템의 사용자는 자신만의 프로세스 또는 어플리케이션을 별도로 시작 프로세스와 데몬으로 추가할 수 있다. 시스템에

〈표 3〉 시작 프로세스/데몬의 정보를 담고 있는 파일과 디렉터리

/System/Library/StartupItems/
/Library/StartupItems/
/User/[User ID]/Library/Preferences/loginwindow.plist
/System/Library/LaunchAgents/
/System/Library/LaunchDemons/
/User/[User ID]/Library/LaunchAgents/

등록된 사용자가 추가시킨 프로세스에는 특정 시스템으로의 자동 연결 기능 또는 악의적인 의도로 제작된 어플리케이션이나 스크립트 등이 있는데, Mac OS X 운영체제가 부팅해서 가동되기 시작하면서 부터 실행되는 프로세스와 데몬에 관한 정보는 <표 3>과 같이 총 6곳의 파일과 디렉터리에 포함되어 있다. 시스템의 시작 프로그램에 관한 정보를 얻을 수 있다.

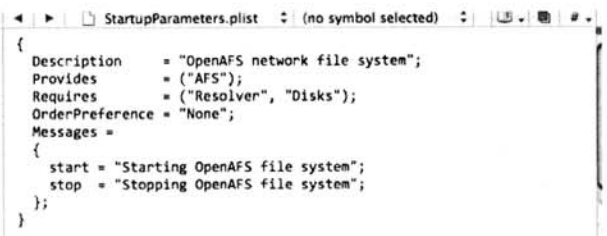
'/System/Library/StartupItems/', '/Library/StartupItems/' 디렉터리에는 Mac OS X의 부팅이 이루어지고 사용자 로그인이 완료된 후에 실행이 되는 파일이 포함되어 있다.

각 폴더는 실행되어야 할 프로그램의 실제 실행 파일과 'StartupPrameters.plist'라는 이름을 가진 파일을 포함하고 있다. 각 실행 프로그램명의 폴더에 속한 'StartupPrameters.plist' 파일에는 시작 프로그램의 초기 설정 또는 옵션을 지정하는 여러 가지 인자 값이 담겨있다.

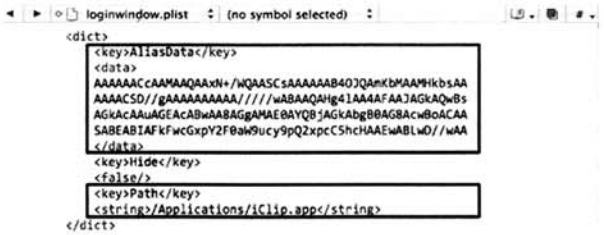
'/User/[User ID]/Library/Preferences/loginwindow.plist' 파일은 Mac OS X에 등록된 사용자가 운영체제의 데스크톱 환경에 로그인 한 후 실행되는 프로그램 목록과 각 항목의 전체경로를 저장하고 있다. 프로그램 목록의 'AliasData' 태그에는 Base64로 인코딩 되어 있다.

'/System/Library/LaunchAgents/', '/System/Library/LaunchDemons/' 디렉터리에는 Mac OS X가 부팅되면서 실행되는 각종 시스템 운영을 위해 필요한 서비스가 포함되어 있다. 운영체제에서 제공하는 기본 서비스 이외의 서비스를 '/User/[User ID]/Library/LaunchAgents/' 디렉터리에 추가적으로 등록할 수 있다.

각 'LaunchAgents', 'LaunchDemons' 디렉터리는 시작 프로그램과 관련된 정보를 담고 있는 .plist 파일(그림 10)을 저장하고 있다. 각 .plist 파일의 'Label' 태그는 현재 시스템에 등록되어 있는 시작 서비스 프로그램의 파일명이며, 'ProgramArguments' 태그는 실행파일이 가진 전체 디렉터리 경로를 가리키고 있다.



(그림 8) StartupPrameters.plist



(그림 9) loginwindow.plist

(그림 10) com.apple.airportd.plist

4.4 프로그램 사용 기록

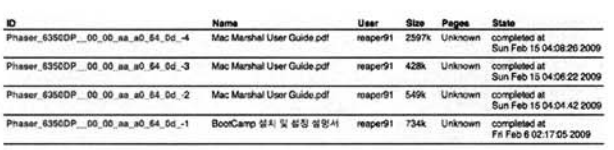
Mac에서 구동되는 프로그램은 자신이 동작하는 동안에 발생한 여러 상황과 오류에 대해서 기록을 남긴다. 운영체제에서 실행되었던 프로그램의 구동 기록은 '/private/var/log' 폴더의 system.log에 각 상황이 발생한 시간 정보와 프로그램 동작 중 발생한 사항이 저장된다.

system.log 파일에서 특정 프로그램의 실행 여부와 동작한 시간, 동작 과정에 발생한 여러 다양한 상황에 관한 정보를 획득할 수 있다.

4.5 프린터 출력 정보

Mac 운영체제에서 제공하는 프린터 인쇄 기능(Common Unix Printing System)을 활용하여 자신이 원하고자 하는 문서 또는 이미지와 같은 파일을 출력할 수 있다. 기록되어

(그림 11) system.log



(그림 12) 프린터 사용 기록

(그림 13) 프린터 장치

(그림 14) 프린터를 출력한 사용자의 ID, 출력한 문서의 파일명

있는 프린터 인쇄 기록에서 사용자가 특정 문서를 언제 어떤 프린터 장치를 이용해서 무슨 파일명의 문서를 출력했는지를 알아낼 수 있다.

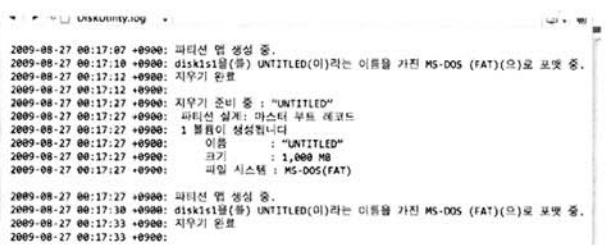
파일 출력에 관한 기록(그림 12)은 '/private/var/spool/cups' 디렉터리에 출력했던 문서별로 저장 되어있다. '/private/var/spool/cups' 폴더에 저장되어 있는 프린터 출력 기록을 토대로 프린터 장치를 사용해 문서를 출력한 사용자의 ID, 출력한 파일의 이름, 인쇄 시각을 알아낼 수 있다.(그림 13) (그림 14)

4.6 외부 저장매체 사용내역

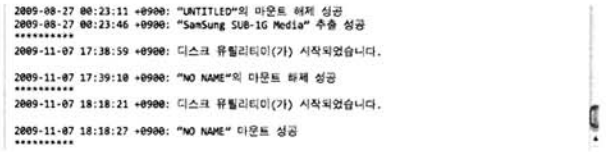
Mac 운영체제의 사용자는 자신의 iMac 데스크톱에 기본으로 장착되어 있는 하드 디스크 드라이브와는 별도로 외부 저장매체를 활용할 수 있다. Mac OS X는 사용자가 추가한 외부 저장매체에 대한 포맷, 마운트, 언 마운트, CD/DVD 데이터 복사 등의 여러 기능을 제공하고 있다.

현재 iMac 데스크톱에 어떠한 형태의 저장매체가 부착되었는가와 해당 매체에 대해서 마운트/언 마운트 행위부터 포맷, 파티션 생성에 관한 작업 기록을 파악해야 한다. 이러한 정보를 바탕으로 사용자의 iMac 데스크톱에 부착되어 있는 하드 디스크 드라이브 이외에 사건과 관련된 중요한 디지털 증거가 저장되어 있을 수 있는 외부 저장매체가 무엇인지 알아낼 수 있다.

사용자에 의해 외부 저장 드라이브, USB 그 밖의 미디어 매체에 수행한 마운트, 언 마운트, 포맷 그리고 CD/DVD 데



(그림 15) 외부 저장 매체 사용 기록 1



(그림 16) 외부 저장 매체 사용 기록 2

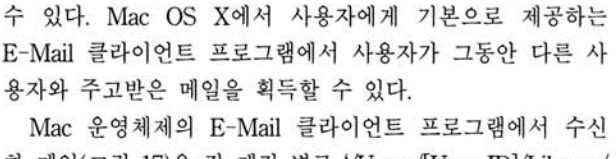
이터 복사 등과 관련된 작업을 '/Users/reaper91/Library/Logs/' 폴더의 'DiskUtility.log', 'DiscRecording.log' 파일에 기록한다.[9]

'DiskUtility.log', 'DiscRecording.log' 기록되어 있는 로그 목록에서 운영체제에 등록된 사용자가 최근에 저장매체에 수행한 다양한 작업에 관한 것을 알아 낼 수 있다. 로그 파일에 저장되어 있는 데이터를 바탕으로 외부 저장장치의 장착 여부를 알 수 있다. 또한 CD 생성 작업 역시 알 수 있다.

4.7 E-Mail

E-Mail 메시지는 사용자가 용의자로 의심할 수 있는 다른 사람과 교환한 범죄 관련 중요 데이터를 포함 함고 있을 수 있다. Mac OS X에서 사용자에게 기본으로 제공하는 E-Mail 클라이언트 프로그램에서 사용자가 그동안 다른 사용자와 주고받은 메일을 획득할 수 있다.

Mac 운영체제의 E-Mail 클라이언트 프로그램에서 수신한 메일(그림 17)은 각 계정 별로 '/Users/[User ID]/Library/Mail/[계정명]/INBOX.mbox/Messages/' 폴더에 수신된 메일별로 저장되며, 메일 데이터는 emlx 포맷 구조로 이루어져 있다.[11] emlx 포맷 구조의 이메일은 보낸 시간에 관한 정보가 저장되어 있으며, From 항목에서 이메일을 보낸 대상 서버와 사용자 계정에 관한 정보를 알아낼 수 있다. To 항목에서 메일을 받아본 사람이 누구인지 확인할 수 있으며, 실제 메일 내용은 Base64로 인코딩 되어 있다.



(그림 17) E-Mail을 보낸 사람의 서버 주소와 계정 정보 (.emlx)

(그림 18) E-Mail을 주고받은 사람과 Base64로 인코딩된 메일 본문 (.emlx)

4.8 웹 브라우저 사용 내역

Safari는 처음 Mac 운영체제를 설치하면 기본으로 제공되는 웹 브라우저 프로그램이다. 사용자는 웹 브라우저를 활용하여 다양한 웹 사이트에서 정보를 알아낼 수 있으며, 임의의 데이터를 받아볼 수 있다. Mac 운영체제 상에서 Safari를 활용하여 임의의 여러 웹 사이트를 방문한 사용자의 최근 웹 사이트 방문내역, 다운로드 받은 파일과, 즐겨찾기 목록을 확인해야 한다. 접속한 웹 페이지에서 볼 수 있는 정보와 평소 자주 방문하는 사이트에 대한 즐겨찾기 목록에서 사용자가 사이트에 자주 접속하여 알아보고자 했던 중요 데이터를 획득할 수 있다.

운영체제에 등록된 각 사용자의 사파리 웹 브라우저 사용 내역은 '/Users/[User ID]/Library/Safari/' 디렉터리에 저장되어 있는 .plist 파일(<표 4>)에서 확인할 수 있다. 각 .plist 파일에서 최근에 방문한 사이트 목록, 사용자의 즐겨찾기 목록과 최근 다운로드 받은 파일목록에 관한 정보를 얻을 수 있다.

사파리 웹 브라우저는 사용자가 자주 방문하는 웹 페이지를 즐겨찾기 이외에 별도로 Top Sites에 등록할 수 있다. Top Sites는 웹 브라우저의 새 윈도우 생성/새 탭을 생성 하게 될 경우 나타나게 되는 기본 페이지로서, 사용자는 Top Sites에 등록되어 있는 사이트를 접속할 수 있다.

사용자의 현재 Top Sites 페이지의 구성 정보는 'TopSites.plist' 파일(그림 19)에서 확인할 수 있다. 각 'TopSiteTitle'/'TopSiteURLString' 태그에서 Top Sites에 등록되어 있는 웹 페이지의 타이틀과 전체 주소를 얻을 수 있다. Top Sites의 구성 정보는 즐겨찾기에 등록되어 있는 웹 페이지 중에서도 사용자가 빈번히 방문하는 웹 사이트는 무엇인지 알 수 있게 한다.

평소 자주 즐겨 방문하는 웹 페이지에 대해서 사파리를 이용하는 사용자는 웹 브라우저에서 제공하는 북마크 기능을 활용하여 사이트를 등록할 수 있다. 사파리에 등록되어 있는 즐겨찾기 목록은 'Bookmarks.plist'파일에 기록되어 있다. 'Bookmarks.plist'에 저장되어 있는 즐겨 찾기 목록에 기반하여, 평소 사용자가 자주 방문하는 사이트와 관심 사항

〈표 4〉 웹 브라우저 사용내역

TopSites.plist	웹 브라우저의 첫 화면 구성
Historty.plist	사이트 방문 내역
Bookmarks.plist	사용자가 저장한 즐겨찾기 목록
Download.plist	사용자가 다운로드 받은 파일 목록

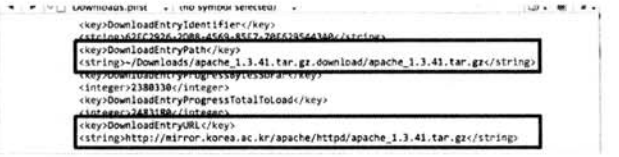
(그림 19) TopSites.plist

이 무엇인지 알아 낼 수 있다. 'Bookmarks.plist'의 'title' 태그에는 사용자가 즐겨 찾는 사이트의 타이틀이 저장되어 있고, 'URLString' 태그에는 사이트의 전체 URL 주소를 가리키고 있다.

'Downloads.plist' 파일에는 사용자가 웹 서핑을 하면서 인터넷 사이트에서 다운 받은 파일 목록이 기록되어 있다. 'Downloads.plist' 파일의 각 'DownloadEntryURL' 태그에서 사용자가 다운로드 받은 파일의 전체 URL 경로이며, 'DownloadEntryPath' 태는 저장되어 있는 정보는 다운받은 파일이 최종적으로 저장된 폴더가 어느 곳인지 가리키고 있다.

'History.plist'파일은 사용자가 방문한 웹 사이트 목록을 저장하고 있다. 'History.plist' 파일의 'displayTitle'/' LastVisitedDate' 태그는 사용자가 방문한 웹 사이트의 타이틀과 마지막으로 방문한 시간에 관한 정보, 웹 페이지의 전체 URL가 기록되어 있다.

(그림 20) Bookmarks.plist



(그림 21) Download.plist

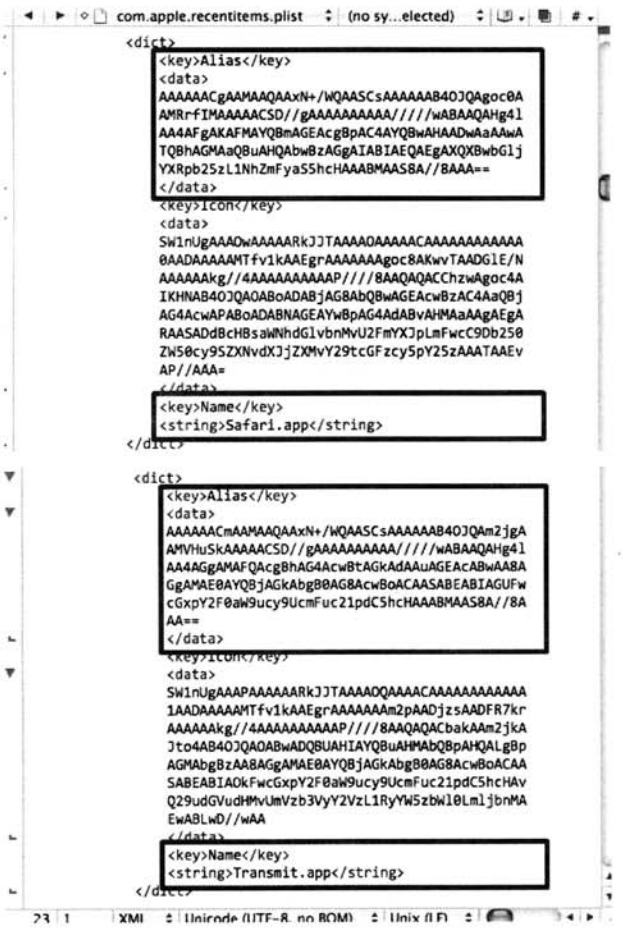
(그림 22) History.plist

웹 페이지에 사용자가 마지막으로 방문한 시간 정보를 담고 있는 'LastVisitedDate' 태그에 저장되어 데이터는 Apple에서 정의한 double 형태의 'NSTimeInterval' 변수를 사용하고 있다. 'NSTimeInterval' 변수는 10,000년의 시간차 범위를 포함하는 sub-millisecond를 사용한다. 즉, 'LastVisitedDate' 태그에 저장되어 있는 값은 sub-millisecond 표현된 0년도부터 현재 연도까지의 시간차를 뜻한다.[5] 마지막으로 방문한 시간 정보, Apple에서 제공하는 시간 관련 클래스 'NSCalendarDate'를 통해서 '연/월/일/시/분/초' 시간 표현 형태로 변환할 수 있다.

4.9 최근 원격 접속 서버와 사용 항목 및 폴더

사용자가 접속했던 외부 원격서버와 공유 디렉터리, 최근에 열람해 보았던 문서, 실행했던 프로그램에 정보는 최근 사용 항목/폴더 행태로 기록한다. 또한 Mac 운영체제의 기본 미디어 플레이어 프로그램인 퀵 타임 플레이어에서 재생된 파일, 문서 작성 도구인 Text Edit가 작성하던 파일 목록을 저장하고 있다. 최근 사용 항목/폴더 목록을 점검하여, 사용자가 가장 최근에 열람한 파일, 실행시켰던 항목, 외부 원격 서버에 대한 정보와 더불어 사용자가 재생시킨 파일, 작성하고 있었던 파일이 무엇이었는지를 확인할 수 있다.

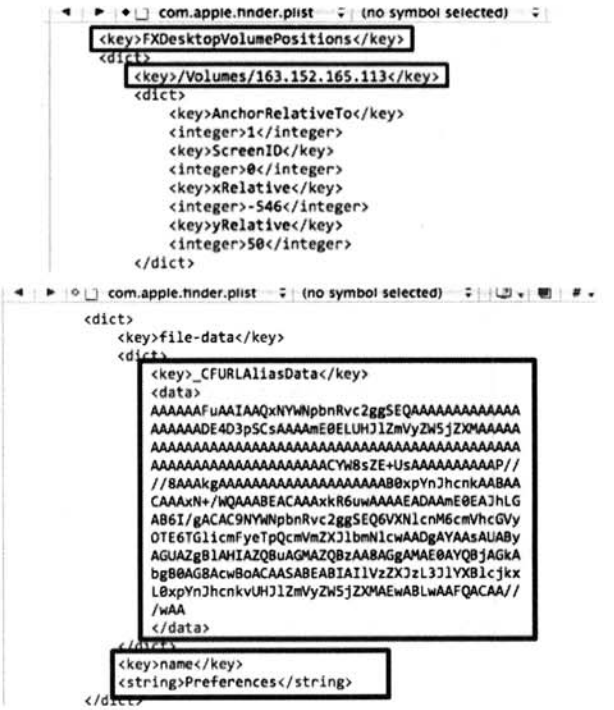
최근 사용 항목은 크게 2가지 카테고리로 분류된다. 하나는 각종 실행 파일을 포함하는 응용프로그램 카테고리이며,



(그림 23) com.apple.recentitems.plist

또 하나는 일반 문서에서부터 이미지 동영상 등 다양한 포맷 형태의 파일을 포함하는 도큐먼트 카테고리 이다. 사용자가 최근에 실행시키거나 열람해본 응용프로그램/도큐먼트 카테고리(그림 23)의 다양한 파일 항목에 관한 정보는 'com.apple.recentitems.plist' 파일에서 얻을 수 있다.

'com.apple.recentitems.plist'의 'Name' 태그에는 최근 열어본 각 파일 항목의 파일명이 저장되어 있으며, 'Alias' 태그는 파일 항목의 전체 경로를 가리키고 있는 문자열 값을



(그림 24) com.apple.finder.plist

Base64로 인코딩 하여 저장하고 있다.[4]

최근 사용 폴더는 기본적으로 사용자가 최근에 열람해 본 폴더를 기록하고 있으며, 추가적으로 컴퓨터에 연결한 외부 저장장치의 폴더 정보와 사용자가 등록한 NetBIOS/FTP와 같은 원격 공유 폴더(그림 24)의 경로를 포함하고 있다. 이런 식으로, 사용자가 최근에 열어본 폴더 또는 컴퓨터에 연결한 CD 드라이브/USB를 장치를 비롯한 외부 원격 공유 폴더에 관한 정보는 'com.apple.finder.plist' 파일에서 얻을 수 있다.

'com.apple.finder.plist'의 'Name' 태그에는 최근 사용자가 열람한 운영체제의 폴더를 비롯한 원격공유폴더/외부저장장치 디렉터리 폴더명이 기록되어 있으며, '_CFURLAliasData' 태그는 사용자가 열어본 디렉터리의 전체 경로를 가리키고 있는 문자열 값을 Base64로 인코딩 하여 저장하고 있다.

(그림 25) com.apple.quicktimeplayer.plist

(그림 26) com.apple.TextEdit.LSSharedFileList.plist

'com.apple.quicktimeplayer.plist'에서 퀵타임 플레이어를 통해 재생시킨 각종 미디어 파일의 목록을 얻을 수 있다. 'dataRef' 태그는 최근 사용자가 시청한 음악파일과 동영상 파일의 전체 경로가 Base64 형태로 기록되어 있으며, 'name' 태그는 직접적으로 사용자가 재생시킨 파일명이 저장되어 있다.

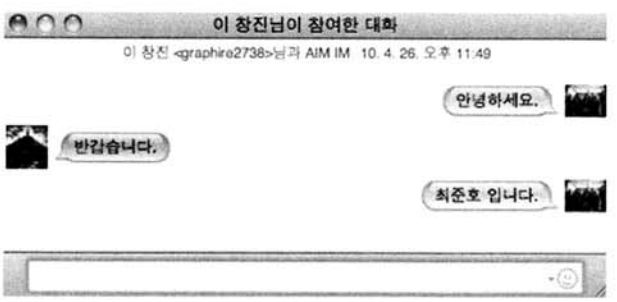
'com.apple.TextEdit.LSSharedFileList.plist'에는 사용자가 Text Edit 프로그램을 사용하여 문석 작업을 했던 문서 파일 목록을 기록되어 있다. 'Bookmark' 태그에는 최근 사용자가 새로 작성했거나 기존에 존재하던 문서 파일에 대한 전체 경로를 Base64 형태로 저장하고 있으며, 'Name' 태그에는 문서 파일의 실질적인 파일명이 적혀 있다.

4.10 인터넷 메신저 정보

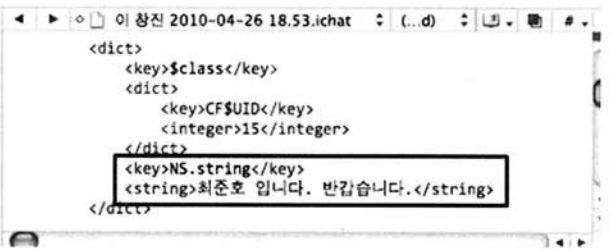
4.10.1 iChat Messenger

다른 사람과 인터넷 메시지를 주고받을 수 있는 클라이언트 프로그램으로서 Mac OS 는 기본적으로 사용자에게 iChat 메신저 프로그램을 제공하고 있다. User는 iChat 프로그램을 활용하여 AIM, Jabber의 메신저 클라이언트로서 사용할 수 있다.(그림 27)

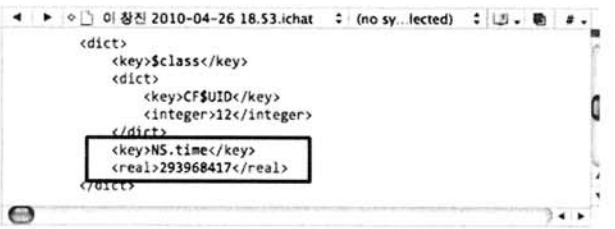
iChat을 통해 다른 사람과 대화를 나눈 사용자가 자신이 상대방과 주고받은 메시지를 저장 했을 경우, 대화내역은 '/User/[User ID]/Documents/' 폴더의 '.ichat' 파일에 저장된



(그림 27) iChat



(그림 28) 메시지 (.ichat)



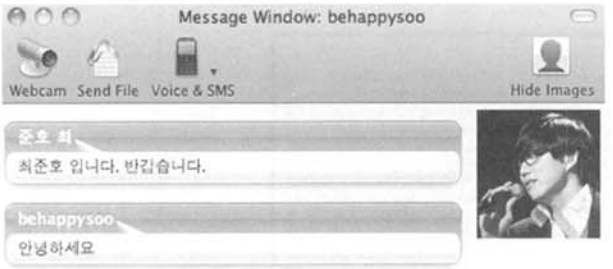
(그림 29) 메시지 보낸 시각 (.ichat)

다. .ichat 파일의 'NS.string' 태그에 저장되어 있는 값으로 부터 상대방과 주고받은 메시지를 확인할 수 있다.(그림 28) 상대방과 메시지를 주고받은 시간에 관한 정보는 NSTimeInterval 값으로 'NS.time' 태그에 저장되어 있다.(그림 29)

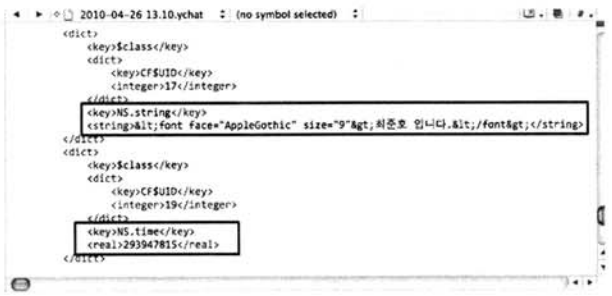
4.10.2 Yahoo Messenger

야후 메신저는 인터넷 포털 사이트 Yahoo에서 개발하여 사용자에게 제공하고 있는 인터넷 메신저 프로그램이다. 야후 메신저는 MS Windows, Mac OS X 환경에서 구동될 수 있도록 제작되었으며, 사용자는 야후 메신저를 통해 다른 사람과 인터넷 메시지를 주고받을 수 있다.(그림 30)

야후 메신저를 활용해 다른 사람과 대화를 나눈 사용자는 자신의 대화 내역을 저장할 수 있다. '/User/[User ID]/Library/Application Support/Yahoo! Messenger/Logs/[User ID]' 디렉터리의 .ychat 파일에서 메신저 사용자가 저장시킨 상대방과의 대화내역을 얻을 수 있다. .ychat 파일의 'NS.string' 태그에



(그림 30) Yahoo 메신저



(그림 31) .ychat

상대방과 주고받은 대화기록이 저장되어 있으며, 대화상대와 메시지를 주고받은 시간에 관한 정보는 'NSTimeInterval'값으로 'NS.time' 태그에 저장되어 있다.(그림 31)

4.11 캐시 데이터

Mac OS X에서 구동되는 데몬과 프로그램은 '/System/Library/Caches' 디렉터리의 하위 폴더에 자신만의 캐시 데이터 공간을 할당 받는다. 캐시 디렉터리에는 다양한 프로그램이 남긴 캐시 데이터들이 저장되어 있으며, 이러한 정보들은 중요한 디지털 증거로서 활용될 수 있다. 기본적으로 Mac OS X에서 지정한 SQLite 포맷으로 프로그램 자신의 다양한 캐시 정보를 기록하고 있으며, 각 프로그램마다 추가적으로 사용하는 특정 데이터 포맷으로 캐시 정보가 저장되어 있다.

기본 SQLite 데이터베이스 포맷으로 저장되어 있는 캐시 데이터 가운데에서 위젯 캐시 파일은 현재 위젯에 등록되어 있는 프로그램이 접속했던 아이피 주소, 위젯 프로그램이 그동안 받아보고 있던 정보가 저장되어 있다. 사파리 웹 브라우저 캐시 파일에는 그동안 사용자가 방문했던 사이트에 대한 기록이 있다.(그림 32)

4.12 Virtual Memory (가상 메모리)

보다 효율적인 운영체제의 메모리 관리를 위해 Mac OS X는 가상 메모리 기법과 캐시 메모리 방식을 사용하고 있다. 가상 메모리 방식은 컴퓨터의 물리적인 RAM 영역의 공간이 부족한 상황이 발생할 경우, 운영체제 상에서 하드 디스크의 일부분을 실제 메모리 영역과 같이 Page In/Page Out 하여 활용하는 기법을 말한다. 운영체제에서 할당한 가상 메모리 영역은 '/var/vm/' 폴더의 'swapfile0'이름을 가진 파일 형태로, 하드 디스크 상의 일부분에 할당되어 있다.[8]

가상 메모리 영역으로 사용되고 있는 '/var/vm/swapfile0' 파일에 보내진 RAM 메모리 데이터는 운영체제가 재부팅이 수행되는 과정에서도 사라지지 않고 남아있게 된다.[9] 'swapfile0' 파일에서 운영체제를 사용했던 사용자가 본 문서의 문자열과 키보드를 타이핑 했던 정보, 이미지 파일과 사용자 ID/Password 정보와 같은 포렌식 분석에 있어 중요한 데이터를 추출할 수 있다.[10]

4.13 삭제된 데이터 복원

컴퓨터의 사용자는 자신의 PC 사용기록이 저장되어 있는 여러 다양한 응용프로그램과 관련된 파일의 정보를 수정/삭제하여 중요 디지털 포렌식 분석에 있어서 중요 정보를 훼손시키는 시도를 할 수 있다. 이에 대비하기 위해 사용자에 의한 데이터 훼손으로 조작되거나 삭제된 정보를 복원 시켜 중요 증거가 될 수 있는 데이터를 획득할 필요성이 있다. 하드 디스크 드라이브 상에서 삭제된 데이터를 복원하기 위

	entry_ID	response_object	request_object	receiver_data	proto_props	user_info
1	1	<?xml version="1	<?xml version="1	4.92	<?xml version="1	
2	2	<?xml version="1	<?xml version="1	163.152.146.107	<?xml version="1	
3	3	<?xml version="1	<?xml version="1	163.152.146.107	<?xml version="1	
4	4	<?xml version="1	<?xml version="1	...	<?xml version="1	
5	5	<?xml version="1	<?xml version="1	<?xml version="1.0" encoding="UTF-8" ?>...	<?xml version="1	
6	6	<?xml version="1	<?xml version="1	<html> ...	<?xml version="1	
7	7	<?xml version="1	<?xml version="1	<html> ...	<?xml version="1	

	entry_ID	version	hash_value	storage_policy	request_key	time_stamp
179	179	0	-361799692	0	http://adcreative.naver.com/ad3/js/da.js?0903	2010-04-04 19:39:
180	180	0	2082497610	0	http://adcreative.naver.com/ad3/system/adca	2010-04-04 19:39:
181	181	0	-36050631	0	http://static.naver.com/common/login/vr_d6.g	2010-04-04 19:39:
182	182	0	-496385041	0	http://static.naver.com/green/v2/img/btn_on_2	2010-04-04 19:39:
183	183	0	-163916925	0	http://static.naver.com/common/login/bg_logi	2010-04-04 19:39:
184	184	0	1470077015	0	http://adcreative.naver.com/ad3/system/adca	2010-04-04 19:39:
185	185	0	-581521815	0	http://static.naver.com/common/login/bg_logi	2010-04-04 19:39:

(그림 32) 위젯 캐시 데이터, Safari 웹 브라우저 캐시 데이터

〈표 5〉 데이터 복원 키워드

자동 실행 프로그램	AliasData, Path, ProgramArguments
프린터 출력 목록	job-printer-uri job-originating-user-name
이메일 송/수신 메시지	Subject, Date, MIME, Content-Type, X-Mailer
웹 브라우저	TopSiteTitle, TopSiteURLString title, URLString DownloadEntryURL, DownloadEntryPath displayTitle, LastVisitedDate
최근 사용 항목	Alias, Name FXDesktopVolumePositions, _CFURLAliasData dataRef, name Bookmark, Name
메신저 사용 기록	ChatRoom, StartTime, YMIdentity, YMUser, NS.string, NS.time

해서는 각 응용프로그램 사용하고 있는 특정 키워드를 활용하여 데이터 카빙을 시도해야 한다.

각 응용프로그램과 관련된 파일에서 사용하고 있는 특정 XML 태그, 키워드를 검색어로서 활용하여 대상 하드 디스크 드라이브에 Foremost[14], Scalpel[15] 같은 데이터 카빙 도구를 적용시켜 사용자의 컴퓨터 사용기록과 관련된 중요 데이터를 복원할 수 있다.

5. 결 론

Mac OS X는 전통적으로 일반 사용자 보다는 전자출판, 디자인, 멀티미디어 부문 관련 작업을 하는 전문가가 주로 사용하는 운영체제였다. 최근에는 iPod을 비롯한 iPod Touch, iPhone, iMac, Mac Book 등과 같은 전자기기와 새롭게 발매된 Snow Leopard의 영향으로 일반 사용자도 Mac 계열 운영체제를 사용하는 비율이 증가하고 있다. 전 세계적으로 꾸준히 증가하고 있는 Mac OS X의 시장 점유율과 일반 사용자의 Mac 운영체제에 대한 활용성이 높아짐에 따라서, 디지털 포렌식 조사를 해야할 가능성도 커지고 있다.

이에 본 논문에서는 Mac OS X에 대한 디지털 포렌식 관점에서 중요한 사용자 행위 및 흔적에 관한 데이터를 선정하여, Mac OS X Leopard(10,5)와 최근에 출시된 Snow Leopard(10.6) 운영체제에서 증거자료로 활용될 수 있는 사용자 흔적 정보 수집할 수 있는 관한 방안을 제시했다. 논문에서 제시한 Mac OS X의 포렌식 기법을 활용하면 Mac 운영체제 상에서의 범죄 증거와 밀접하게 관련되어 있을 수 있는 개인 사용자가 수행한 작업과 기록을 알아낼 수 있다.

참 고 문 헌

[1] Robert A. Joyce, Judson Powers, Frank Adelstein, "MEGA : A tool for Mac OS X operaing system and application forensics," *Digital Investigation 2008.*

[2] Amit Singh, "Mac OS X Internals : A Systems Approach," *Addison Wesley.*

[3] Apple, "Introduction to Property Lists," *http://developer.apple.com/*

[4] Edward R. Marczak, "Mac OS X Advanced System Administration v10.5," *Apple.*

[5] Apple, "NSTimeInterval, NSCalendarDate," *http://developer.apple.com/*

[6] Robert A. Joyce, Judson Powers, Frank Adelstein, "Mac MarshalTM: A Tool for Mac OS X OperatingSystem and Application Forensics," *DFRWS 2008.*

[7] Ryan R. Kubasiak, "Macintosh Forensics," *New York State Police.*

[8] Philip Craiger, Paul K. Burke, "Mac Forensics : Mac OS X and the HFS+ File System," *Department of Engineering Technology University of Central Florida.*

[9] Seokhee Lee, Antonio Savoldi, Sangjin Lee, Jongin Lim, "Windows Pagefile Collection and Analysis for a Live Forensics Context", *F2GC 2007.*

[10] Seokhee Lee, Antonio Savoldi, Sangjin Lee, Jongin Lim, "Password Recovery Using an Evidence Collecting Tool and Countermeasures," *IIH-MSP 2007.*

[11] David H. Crocker, "ARPA Internet Text Messages," *http://tools.ietf.org/html/rfc822*

[12] Philip Craiger, Paul Burke, "Mac OS X Forensics," *IFIP 2006*

[13] Nick Peelman, "Basic Mac Forensics," *Purdue University*

[14] Air Force Office of Special Investigations, The Center for Information Systems Security Studies and Research, "Foremost," http://foremost.sourceforge.net/

[15] Golden G. Richard III, "Scalpel : A Frugal, High Performance File Carver," http://www.digitalforensicssolutions.com/Scalpel/

최 준 호

e-mail : investigator@mail.com

2006년 대전대학교 전산정보보호학과(이학사)

2006년~현 재 고려대학교 디지털 포렌식 연구센터 연구원

관심분야 : 디지털 포렌식, Mac OS X, 분산처리시스템

이 상 진

e-mail : sangjin@korea.ac.kr

1987년 고려대학교 수학과(학사)
1989년 고려대학교 수학과(이학석사)
1994년 고려대학교 수학과(이학박사)
1989년~1999년 ETRI 연구원 역임
1992년 국가안전기획부장 표창
1999년~현 재 고려대학교 정보경영공학전문대학원 교수
관심분야 : 디지털 포렌식, 모바일 포렌식, 심층 암호, 해쉬 함수