디지털 포렌식 관점에서의 Mac OS X 사용 흔적 분석

최지성*, 전상준*, 박정흠*, 이상진*
*고려대학교 정보보호연구원

e-mail:{chjs207, heros86, junghmi, sangjin}@korea.ac.kr

A Digital Forensic Analysis for Mac OS X Main Artifacts

Ji-Sung Choi*, Sang-Jun Jeon*, Jung-Heum Park*, Sang-jin Lee*
*Center for Information Security Technologies, Korea University

요 약

최근 iPhone, iPad의 높은 사용율과 더불어 Apple 의 Mac 계열 제품에 대한 관심도 높아지고 있다. 이는 Apple의 운영체제인 Mac OS X의 사용율 증가와 함께 디지털 포렌식 수사 환경에서의 Mac OS X의 중요성이 높아짐을 의미한다. 디지털 포렌식 관점에서 Mac OS X에는 사용자의 사용 정보를 남기는 주요 Artifacts들이 있다. 외부 저장 장치 연결 정보, 어플리케이션 설치 정보, 사용자 인증 정보, 어플리케이션 설정 정보 등이 대표적인 Artifacts들이며, 이러한 정보들은 특정 위치의 로그 파일에 남게 된다. 본 논문은 Mac OS X의 대표적 Artifacts 들을 대상으로 사용 흔적 정보가 남는 파일을 분석하여 디지털 포렌식 수사 시 활용할 수 있도록 한다.

1. 서론

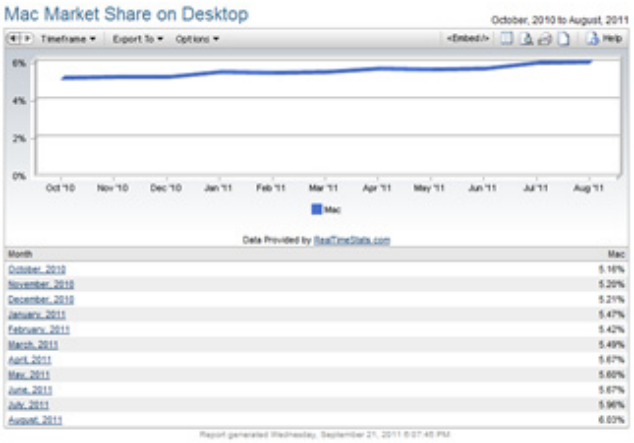
iPhone이 국내 시장에 출시된 이래로 iPhone과 iPad는 Apple社 제품에 대한 접근성의 향상을 가져왔다. 이는 운영체제에 익숙지 않다는 이유로 구매를 꺼리던 Apple社의 Mac 계열 제품에 대한 선호도를 높였고 이는 자연스레 제품에 대한 구매로 이어졌다. Apple社의 데스크탑 및 랩탑인 iMac, Mac Pro, MacBook Pro, MacBook Air, Mac mini의 사용율 증가는 국내 운영체제 시장에서 Mac 의 운영체제인 Mac OS X의 점유율이 증가하는 결과로 나타났다. 현재 Mac OS X는 윈도우즈 계열에 이은 두 번째의 높은 점유율을 가지는 운영체제이다(2011.08). 이는 디지털 포렌식 수사 환경에서 Mac OS X가 윈도우즈 계열 다음으로 마주할 가능성이 높은 운영체제로 자리하고 있음을 의미하며 수사관 및 분석가 들은 디지털 포렌식 환경에서 어떠한 운영체제를 마주할지 모르므로 Mac OS X의 데이터 수집, 분석 방법에 대한 지식을 쌓아야 한다. 이에 본 논문에서는 Mac OS X 스노우 레오파드(10.6)를 대상으로 국·내외 디지털 포렌식 연구 현황을 파악하고 이를 토대로 주요 사용 흔적에 대한 디지털 포렌식 관점의 분석을 진행하였다.

* 본 연구는 한국연구재단을 통해 교육과학기술부의 바이오연구개발사업으로부터 지원받아 수행되었습니다.(20100020634)

2. Mac OS X의 사용 및 연구 현황

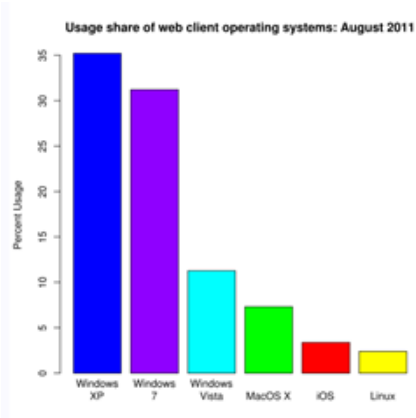
2.1 사용 현황

현재 운영체제 시장은 크게 윈도우즈 계열 운영체제, Linux 및 Unix 계열 운영체제, Mac OS X 운영체제로 나눌 수 있다. Mac OS X는 윈도우즈 계열 운영체제 다음으로 높은 시장 점유율(6.03%, 2011.08)을 가지고 있다. 이는 iPhone OS인 iOS의 시장 점유율(53.04%, 2011.08)과 함께 지속적으로 증가하고 있다.



(그림 1) Mac 운영체제 시장 점유율 변화(2011.08)

Mac OS X의 운영체제 점유율은 윈도우즈 계열 운영체제에 비하면 매우 낮은 점유율을 보이고 있다.



(그림 2) 운영체제 시장 점유율(2011.08)

하지만 6.03% 라는 수치는 Mac OS X에 대한 디지털 포렌식 수사 가능성과 연구의 필요성을 말해주고 있다.

2.2 연구 현황

현재 Mac OS X에 대한 연구의 방향은 파일 시스템과 물리 메모리, 디스크 데이터 추출 방법과 같은 데이터 수집 관점에서의 연구로 진행되고 있다. 사용자의 정보 또는 사용 기록과 같은 디지털 포렌식 수사 관점에서의 사용 흔적 들에 대한 분석은 미흡한 편이다.

2.2.1 파일 시스템

Mac OS X의 파일 시스템인 HFS+ 파일 시스템은 Apple社에서 Mac OS X를 위해 개발한 파일 시스템이다. 초기 Macitosh에서는 HFS(Hierarchical File System)을 사용하였다. HFS는 Unix 파일 시스템인 UFS를 기반으로 제작되었다. 여러 한계점들로 인해 저널링 기능을 선택적으로 포함하는 HFS+ 또는 HFSX 파일 시스템으로 발전하였다.

HFS+는 최상단 1024바이트와 최하단 512바이트를 예약 영역으로 분류하고 있다. Volume Header와 Alternate Volume Header는 두 예약 영역과 연속되어 고정된 영역으로 존재하지만 나머지 영역들은 Volume Header의 정보를 사용하여 위치를 확인한다. Catalog File은 파일의 계층 구조와 메타 정보를 담고 있다.

2.2.2 물리 메모리 분석

Mac OS X의 물리 메모리 분석을 위해서는 3가지 요소가 필요하다. 분석할 메모리의 이미지를 수집해야 하고, 심볼 정보를 가지는 커널 이미지 파일, 커널 이미지가 어떤 아키텍쳐로 이루어졌는지를 확인해야 한다.

현재 알려진 수집 방법으로는 Firewire 케이블을 이용한 직접 수집 방법, 메모리 관리 장치인 '/dev/mem'을 이용하는 방법, 하이버네이션(Hibernation)을 통해 생성되는 하이버네이션 이미지를 수집하는 방법이 있다.

2.2.3 디스크 데이터 추출 방법

Mac OS X는 다른 운영체제와 같은 데이터 수집 방법인 논리적 파일 수집 방법과 물리적 디스크 이미지 수집 방법이 존재한다. 논리적 수집 방법은 해당 시스템에서 직접 파일을 복사하는 방법과 "Target Disk Mode"를 이용하여 수집하는 방법으로 나뉜다. Apple社의 "Target Disk Mode"는 커널 패닉으로 인한 운영체제의 비정상 동작의 경우를 대비하여 사용자의 데이터를 다른 시스템에 백업할 수 있도록 지원하는 기술이다. 이를 위해 연결 대상이 되는 Mac OS X 시스템과 Firewire케이블이 필요하다. 디지털 포렌식 수사관은 부팅이 안되는 시스템에 대해서도 Firewire케이블을 통해 대상 시스템의 데이터를 손쉽게 수집할 수 있기 때문에 유용하게 사용되는 방법이다

물리적 디스크 이미지 수집 방법은 "dd 명령"을 이용하는 방법과 시스템에서 하드디스크를 추출하여 수집하는 방법으로 나뉜다. Mac OS X는 BSD나 Darwin과 같은 오픈소스 Unix 커널을 이용한 운영체제이다. 그렇기에 Unix에 존재하는 명령어 대부분은 Mac OS X에도 함께 존재한다. Unix 시스템은 디스크나 물리 메모리를 이미징하기 위해 "dd"를 많이 사용하였고 이는 Mac OS X에도 동일하게 존재한다.

3. 주요 사용 흔적 분석

Mac OS X는 사용자가 시스템을 사용하면서 발생하는 이벤트 정보들을 텍스트 형태의 로그 데이터로 저장한다. 이렇게 저장되는 이벤트 정보로는 저장 장치 연결 정보, 어플리케이션 설치 정보, 사용자 인증 정보, 어플리케이션 설정 정보가 존재한다.

3.1 저장 장치 연결 정보

저장 장치 연결 정보는 USB와 같은 외부 저장 장치의 시스템 연결 정보를 의미한다. 외부 저장 장치를 연결할 때 발생하는 이벤트 정보는 로그 형식으로 저장되고 역할에 따라 내용을 분류하여 관리한다. 외부 저장 장치 연결 정보는 '/private/var/log'내에 있는 두 파일인 'kernel.log'와 'system.log'에 상황에 따라 저장된다.

3.1.1 kernel.log

'kernel.log'에는 시스템 상태 변경 정보, 네트워크 상태 변경 정보, 파일 접근 정보, 네트워크 장치 정보 및 상태 변경 정보를 비롯한 시스템 상태 변경 정보가 기록되어 있다. 또한 하드웨어 연결 정보도 저장되어 있는데 이를 통해 USB와 같은 외부 저장 장치 연결 정보도 확인 할 수 있다.

```
Sep 22 16:13:11 jiseong-choeui-MacBook-Air kernel[0]: disk1s1: media is not present.
Sep 22 16:16:15 jiseong-choeui-MacBook-Air kernel[0]: USBMSC Identifier (non-unique):
5A10011958861 0x54c 0x243 0x100
```

(그림 3) kernel.log

USB 및 외부 저장 장치에 대한 로그 정보는 'Sep 22 16:16:15 jiseong-choeui-MacBook-Air kernel[0] : USBMSC Identifier (non-usique) : 5A10011958861 0x54c 0x243 0x100'와 같은 형식으로 기록된다. 각 항목에 대한 정보는 다음과 같다.

<표 1> kernel.log에 저장되는 정보

종류	정보
날짜 및 시간	Sep 22 16:16:15
이벤트	USB Identifier
Serial Number	5A10011958861
Vendor ID	0x54c
Product ID	0x243
Firmware Revision	0x100

3.1.2 system.log

system.log는 시스템에서 일어나는 주요 변화들을 기록한다. 서비스 시작 및 종료, 네트워크 연결 정보, 제한된 영역에 대한 접근 시도와 같은 이벤트 들과 더불어 외부 저장 장치의 연결 정보도 기록한다. system.log를 분석하면 외부 저장 장치의 마운트 된 위치를 확인할 수 있다.

```
Sep 22 16:36:02 jiseong-choeui-MacBook-Air fseventsd[40]: check_vol_last_mod_time:XXX failed to
get mount time (25; &mount_time == 0x10047f8b8)
Sep 22 16:36:02 jiseong-choeui-MacBook-Air fseventsd[40]: log dir: /Volumes/JISUNG/.fseventsd
getting new uuid: 481A0EF6-0207-4AF9-BA82-2F36B032C9B4
```

(그림 4) system.log

Mac OS X는 외부 저장 장치가 시스템에 연결될 때, 검색 속도를 위해 캐시 데이터를 생성한다. 파일 시스템의 변화가 발생했을 때, '.fsevent'를 통해 캐시 데이터의 내용을 변경한다. 그리고 이러한 변화에는 system.log 에 기록한다.

kernel.log와 system.log를 이용하면 어떠한 외부 저장 장치가 시스템에 연결되었는지 유추할 수 있다.

3.2 어플리케이션 설치 정보

Mac OS X의 어플리케이션 설치는 다음과 같은 세 가지 방식으로 진행된다. 설치 패키지를 통한 방법, 드래그 앤 드롭 방법, 설치 파일 더블 클릭 방법이 있다. 이 중 설치 패키지를 통한 방법은 '/private/var/log'폴더 내에 있는 'install.log'파일에 어플리케이션 설치 정보를 로그로 남긴다. 어플리케이션 설치 정보는 패키지 설치 로그 파일인 install.log 파일에 'Sep 22 20:16:43 jiseong-choeui-MacBook-Air installd[3910] : PackageKit : ~~ com.estsoft.mac.alzip.pkg'와 같은 형태로 저장된다. 이를 통해 어플리케이션의 설치 시간, 시스템 이름, 설치 패키지에 관한 정보를 확인 할수 있다.

```
Sep 22 20:16:43 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: ----- Begin install
-----
Sep 22 20:16:43 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: request=PKInstallRequest
<1 packages, destination=/>
Sep 22 20:16:43 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: packages=(\n
"PKLeopardPackage <file://localhost/Users/JiSung/Library/Application%20Support/AppStore/
450698556/mzm.ytjksxru.pkg#com.estsoft.mac.alzip.pkg>"\n)
Sep 22 20:16:43 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: Extracting file://
localhost/Users/JiSung/Library/Application%20Support/AppStore/450698556/
mzm.ytjksxru.pkg#com.estsoft.mac.alzip.pkg (destination=/var/folders/zz/zzzivhrRnAmviuee+++++++
++++/Cleanup At Startup/PKInstallSandbox-tmp/Root/Applications, uid=0)
Sep 22 20:16:44 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: Shoving /var/folders/zz/
zzzivhrRnAmviuee++++++++++/Cleanup At Startup/PKInstallSandbox-tmp/Root (1 items) to /
Sep 22 20:16:44 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: Registered bundle
file://localhost/Applications/ALZip.app/
Sep 22 20:16:44 jiseong-choeui-MacBook-Air installd[3910]: Installed "" ()
Sep 22 20:16:44 jiseong-choeui-MacBook-Air installd[3910]: PackageKit: ----- End install -----
```

(그림 5) install.log

3.3 사용자 인증 정보

Mac OS X에서 사용자 인증은 '/private/var/log/secure.log' 파일에 저장된다. '/private/var/log/monthly.out' 로그는 월별 통계 로그로써 시스템에 존재하는 여러 계정에 따라 월 별로 시스템 사용 빈도에 대한 정보를 저장한다.

3.3.1 secure.log

secure.log는 사용자가 맺는 세션의 시작과 종료와 같은 네트워크의 보안 관련 정보를 저장한다.

```
Sep 21 00:45:55 localhost com.apple.SecurityServer[24]: Session 0x5fbff962 created
Sep 21 00:45:55 localhost com.apple.SecurityServer[24]: Entering service
Sep 21 00:45:56 localhost com.apple.SecurityServer[24]: Succeeded authorizing right
'config.modify.com.apple.CoreRAID.admin' by client '/System/Library/PrivateFrameworks/
CoreRAID.framework/Versions/A/Resources/CoreRAIDServer' for authorization created by '/System/
Library/PrivateFrameworks/CoreRAID.framework/Versions/A/Resources/CoreRAIDServer'
```

(그림 6) secure.log

3.3.2 monthly.out

monthly.out는 월 별로 Mac OS X 가 남기는 정보를 저장한다.

```
Mon Aug  1 19:24:15 KST 2011

Rotating fax log files:

Doing login accounting:
        total     1022.85
        JiSung    1022.45
        root         0.40

-- End of monthly output --
```

(그림 7) monthly.out

monthly.out에는 시스템에 등록 되어있는 사용자 계정별로 정보를 저장하고 있으며, 시스템을 사용한 빈도수를 기록하고 있다. 이 정보를 통해 주된 사용자가 누구인지 확인할 수 있다. 또한 계정을 삭제하더라도 그 해당 월에는 계정 정보가 남아 있기 때문에 사용 계정 정보를 확인하는데에 도움을 준다.

3.4 어플리케이션 설정 정보

윈도우즈 계열 운영체제에는 사용자에 의해 변경되는 설정 들에 대한 정보를 담는 레지스트리 항목이 있다.

Mac OS X에는 레지스트리는 없지만 이와 유사한 default 명령이 존재한다. Mac OS X에서는 다양한 어플리케이션 및 시스템 환경 설정 정보를 읽을 수 있다. 이러한 정보들은 Mac OS X에서 제공하는 터미널 또는 어플리케이션의 환경 설정에서 변경할 수 있다.

3.4.1 Facetime 설정정보

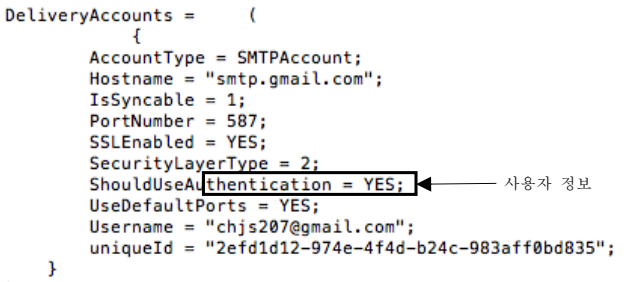
Facetime은 Apple社가 개발한 영상 통화 소프트웨어이다. iPhone, iPad 와 같은 iOS 기반의 모바일 기기와 Mac OS X 운영체제를 사용하는 제품에서 사용할 수 있다.

(그림 8) Facetime 설정 정보의 일부

'/Users/사용자/Library/Preferences/com.apple.facetime.plist'파일은 영상 통화 시간 정보도 함께 포함하고 있다. 또한 최종 사용자 정보 및 영상 통화 상대의 정보도 확인할 수 있다.

3.4.2 Mail 설정정보

Mac OS X는 사용자의 이메일 관리를 위한 Apple Mail을 제공한다. Apple Mail의 사용자 이메일 설정 정보는 defaults 명령을 통해 확인할 수 있다. 그리고 '/Users/사용자/Library/Preferences/com.apple.mail.plist'파일을 통해 사용자 계정 정보를 확인할 수 있다는 점은 디지털 포렌식 수사 시 사용자 확인에 도움을 줄 수 있다.



(그림 9) Mail 설정 정보의 일부

4. 결론 및 향후 계획

그 동안의 디지털 포렌식 분야는 윈도우즈 계열의 운영체제에 치우쳐 발전해왔다. 이는 디지털 포렌식 수사 환경에서 윈도우즈 계열의 운영체제가 아닌 시스템을 마주하였을 때 어려움을 겪을 수 있음을 의미한다.

본 논문에서는 Apple社에서 제공하는 문서와 여러 논문 정보 및 블로그 정보를 토대로 Mac OS X의 사용 현황을 통해 Mac OS X 디지털 포렌식 분석에 대한 당위성을 제시하였고, Mac OS X 관련 연구들이 주로 시스템 분야에 국한되어 있기에 디지털 포렌식 수사 관점에서의 미흡한 점이 있음을 말하였다. 이러한 상황에서 관련 연구들의 미흡한 부분을 개선하고자 사용자의 사용 정보인 외부 저장 장치 연결 정보, 어플리케이션 설치 정보, 사용자 인증 정보, 어플리케이션 설정 정보들의 저장 위치 및 형태를 분석하였다.

Mac OS X의 분석은 앞으로 더 진행될 여지가 많다. 본 논문에서 말하고 있는 외부 저장 장치 연결 정보, 어플리케이션 설치 정보, 사용자 인증 정보, 어플리케이션 설정 정보 뿐만 아니라 물리 메모리 정보 분석 및 Spotlight와 같은 Mac OS X만의 사용 흔적들 또한 연구된다면 더욱 효율적인 Mac OS X 분석이 가능할 것이다.

참고문헌

[1] Michael Becher, Maximillian Dornsief, Christian N.Klein, "Firewire: all your memory are belong to us", CansetWest2005, 2005.

[2] Philip Craiger, Paul K. Burke, "Mac Forensics: Mac OS X and the HFS+ File System", 2005.

[3] NETMARKETSHARE, http://www.netmarketshare.com, 2011.

[4] Amit Singh Accessing Kernel Memory on the x86 Version of Mac OS X, http://www.osxbook.com/book/bonus/chapter8/kma/, Mac OS X internals, 2006.

[5] AhnLab. [Case Study] HFS+의 파일 시스템과 파일 복구, 사라진 파일을 추적하라, 2011.

[6] Lee Kyeongsik, Sang-jin Lee, "Mac OS X Physical Memory Analysis", 2010.

[7] Joon-ho Choi, Sang-jin Lee, "Mac OS X Forensic Analysis", 2009.