정 보 보 호 학 회 지
제 29 권 제6호, 2019. 12

Windows 10 환경의 Box 클라우드 아티팩트 분석

윤 혜 민*, 김 재 욱*, 황 은 비*, 김 해 니*, 권 태 경**

요 약

클라우드 서비스는 사용자에게 데이터 저장, 공유, 다운로드 등을 용이하게 해주는 성질과 시, 공간적 특성과 관계없이 사용할 수 있는 특성으로 최근 IT 산업에서 많이 사용되고 있다. 그러나 서버가 공격당할 경우 데이터와 사용자 개인 정보를 포함한 민감 정보가 유출되는 등 다양한 범죄에 노출되어 있다. 이러한 이유로 클라우드의 포렌식 분석 필요성이 증가하였으며, 현재 많이 상용화되어 있는 응용 프로그램에 대해서는 많은 연구가 진행되었다. 본 논문에서는 Box 클라우드에 대해 포렌식 분석을 진행하고 수집한 아티팩트에 관해 설명한다.

Ⅰ. 서 론

클라우드 서비스는 현재 IT에서 가장 많이 사용되고 있는 서비스로, 인터넷으로 연결된 초대형 고성능 컴퓨터(데이터 센터)에 사용자의 소프트웨어와 콘텐츠를 저장해 두고 사용자가 필요할 때마다 액세스할 수 있다. 단순한 자료 저장 기능뿐만 아니라 웹에서 제공하는 응용 프로그램의 기능을 사용하여 사용자가 원하는 작업을 수행할 수 있고 여러 사람이 동시에 파일을 공유하면서 작업할 수 있다.

클라우드 컴퓨팅은 클라우드 서비스를 제공하는 클라우드 서버들이 모여 있는 환경을 통틀어 지칭하는 것으로, 사용자가 인터넷을 통해 컴퓨터 하드웨어와 소프트웨어를 원격으로 접속하여 사용할 수 있는 방법이다[3]. 또한, 인터넷에 연결된 컴퓨터나 다른 디바이스들이 자원 및 데이터 등을 요청할 경우 이를 제공한다. 이때, 컴퓨터 네트워크나 어플리케이션과 같은 컴퓨팅 자원에 대한 환경이 달라지더라도 클라우드에 접근 가능하게 한다. 이러한 클라우드 컴퓨팅의 주요 특징은 웹상 서버를 통한 데이터 저장, 콘텐츠 사용 등 IT관련 서비스를 사용자가 필요한 만큼 제공받아 소유자와 관리자를 분리하는 것이다.

하지만 클라우드 컴퓨팅은 클라우드 서버가 공격당할 시 개인정보가 유출될 수 있다는 취약점을 가지고 있으며 사용자가 원하는 어플리케이션을 설치하려고 할 경우 제한되거나 지원하지 않는 경우가 있다[1]. 또한, 클라우드 서비스는 인터넷 연결이 가능한 장치에서 액세스되기 때문에 인터넷 통신 환경이 열악하면 서비스를 지원받기 어렵고 물리적인 개별 정보의 위치를 파악할 수 없다. 위 문제점들로 인해 보안 위협이 증가하였고 많은 침해 사고가 발생하였으며, 이에 따라 클라우드의 디지털 포렌식 측면에서 분석의 필요성이 대두되었다. 클라우드 서비스 이용 시 사용자 행위에 대한 데이터가 로컬 시스템에 대부분 남지 않으며, 원격 서버 시스템에 데이터가 저장되기도 한다. 이러한 이유로 클라우드 서비스를 사용하는 용의자의 서버시스템을 조사할 때 기존 디지털 포렌식 수사를 적용 하는 것은 한계가 있으며 클라우드 컴퓨팅 환경에 적합한 포렌식 기술을 연구해야 한다[4]. 하지만 현 기술은 학문적 측면에서 체계화 수준이 미비하여 실제 수사 환경을 고려한 연구가 필요하다.

Ⅱ. 연구 배경

클라우드 서비스 모델은 3가지로 구분되며 IaaS, PaaS, SaaS이다[1]. 특히 SaaS (Software as a Service)는 on-demand 소프트웨어 혹은 소프트웨어 플러스 서비스라고도 불린다[2]. 즉, SaaS는 오피스 소프

본 논문은 2019년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00513, 기계학습을 활용한 UNIX 기반 커널 취약점 탐지 자동화 연구)
* 연세대학교 정보대학원 석사과정(hyemin3307@naver.com, freak91uk@naver.com, gosl4576@naver.com, ebhwange95@naver.com)
** 연세대학교 정보대학원 교수(taekyoung@yonsei.ac.kr)

트웨어, 메시징 소프트웨어, 급여 처리 소프트웨어, DBMS 소프트웨어, 관리 소프트웨어, CAD 소프트웨어, 개발소프트웨어, 게임, 가상화, 회계, 협업, CRM (Customer Relationship Mana gement), HRM (인적자원관리), 인재취득, 학습관리시스템, CM (콘텐츠 관리), GIS (지리정보시스템) 및 서비스 데스크 관리 등 많은 비즈니스 어플리케이션 전달 모델이다[2]. 이는 서버-클라이언트 구조로써 웹을 통해 접속하는 구조이기 때문에 클라이언트에 사용자가 저장한 데이터가 남지 않는다. 그러나 웹브라우저 사용 증거인 히스토리 파일, 쿠키 파일, 인터넷 임시 파일 등과 같은 활성 데이터를 저장하는 물리 메모리 분석을 통해 사용자 데이터 수집이 가능해진다[1,2]. SaaS 서비스 모델 중 한 분야로 스토리지 클라우드 서비스가 있다.

스토리지 클라우드 서비스는 사용 측면에서의 편리성과 활용 범위가 넓다는 점에서 이용자가 급증하였고, Google Drive, Dropbox, OneDrive, Box 클라우드 등 다양한 서비스가 개발되고 있다. 클라우드 서비스는 PC, 모바일 등 디바이스 유형과 시간에 관계없이 주요 파일들을 공유 및 액세스 할 수 있다는 장점으로 관련 컴퓨팅 환경이 보편화되고 여러 분야에서 사용되고 있다. 그러나 기업처럼 보안성이 높은 환경에서 중요 데이터를 액세스하기 위한 악의적인 공격에도 동일 사유를 적용할 수 있는 점 등을 근거로 많은 사건, 사고들이 발생하기 때문에 이를 추적 및 증명할 수 있어야 한다.

특히 Box 클라우드는 무료로 제공되는 서비스로 다양한 옵션 제공을 강점으로 하는 솔루션이다. 온라인으로 모든 형식의 파일을 저장하고 컴퓨터, 휴대폰, 태블릿 등에서 쉽게 액세스할 수 있다. Box 클라우드를 사용하여 짧은 링크로 대용량 파일을 빠르게 공유할 수 있고, 온라인과 오프라인에 상관없이 모든 종류의 파일을 보고, 공유하고, 편집할 수 있다. 폴더를 공유 온라인 작업 공간으로 지정하여 디바이스 간 문서 작업을 공유할 수 있으며, Box에 파일을 안전하게 보관하기 때문에 하드 드라이브가 고장이 나도 중요 문서를 분실할 위험이 적다[5].

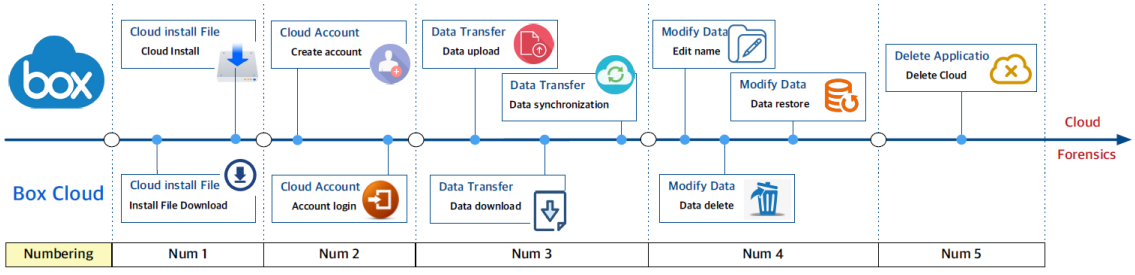
Ⅲ. Box 클라우드 서비스 포렌식 분석

Box 클라우드는 기본적으로 pc와 클라우드 서버의 파일을 동기화하여 인터넷 접속이 가능한 곳에 사용자의 파일을 접근 가능하게 해주는 서비스를 제공한다. 이러한 동기화의 과정을 확인하기 위해서 동기화 폴더인 test를 생성하였으며, 이 폴더에는 일반적으로 많이 사용되는 한글문서, 오피스 문서 등 사용자가 쉽게 접근하여 작성할 수 있는 파일을 실험용 도구로 채택하여 구성하였다. 생성한 파일은 test 1부터 test 10까지 총 10개의 파일을 저장하였고 각 파일은 .hwp, .docx, .ppt, .xlsx 등 다양한 확장자로 구성하였다.

클라우드 분석을 수행하기 위해 VM Ware에 Windows 10 x64를 설치하여 진행하였으며, 설치, 계정 생성, 로그인, 업로드, 다운로드, 동기화, 삭제 및 복원, 프로그램 삭제 등의 행위를 수행하여 아티팩트를 수집하였다[그림 1]. 행위 수행 시 VM Ware snap shot 기능으로 상태를 저장하고, .vmdk 파일을 .vhd 파일로 변환하여 Autopsy를 활용해 수집한 아티팩트를 분석하였다. .vmdk 파일이란 Virtual Machine Disk의 줄임말로 가상 시스템에서 사용할

가상 하드 드라이브의 컨테이너를 설명하는 파일 형식이고, .vhd 파일은 Virtual Hard Disk의 줄임말로 마이크로소프트 윈도우 가상 PC가 사용하는 하드 디스크 파일이다.

수행한 실험을 분석하기 전에, 주로 나타나는 아티팩트에 대해 먼저 설명하고자 한다. WebCacheV01 .dat



(그림 1) Cloud Scenario of planning

는 Internet Explorer와 Microsoft Edge에서 클라우드 서비스를 이용하였을 때 Cache, Cookie, History, Download list 등의 정보가 존재하는 파일로, 경로는 %USERPROFILE%AppData\Local\Microsoft\Windows\WebCache\이다. LNK 파일은 Windows 운영체제에서만 존재하는 기능으로 Windows 기본 폴더인 내 PC, 바탕화면, 문서 등의 폴더에는 기본적으로 만들어지고, 어플리케이션 설치 시 바로가기 아이콘을 생성 옵션을 선택할 경우, 사용자가 직접 생성하는 경우 등을 통해 해당 파일을 만들 수 있다. 레지스트리에서는 총 5가지를 찾을 수 있고, HKCR(HKEY_ CLASSES\ ROOT)는 파일 확장자 연결 정보, 파일과 프로그램 간 연결 정보가 들어 있고, HKCU(HKEY_CURR ENT_USER)는 현재 로그인된 사용자의 설정 정보를 담고 있다. HKLM(HKEY_LOCAL_MACH INE)은 컴퓨터 하드웨어 및 소프트웨어의 모든 정보를 저장하고 있으며 HKU(HKEY_USERS) 는 다중 사용자 지원 시스템에서 각 사용자에 대한 키 항목이 생성되어 환경 정보를 저장하고 있다. 마지막 HKCC(HKEY_ CURRENT_CONFIG)에는 현재 사용 중인 윈도우 디스플레이, 폰트, 프린트 등의 설정 정보가 저장되어 있다.

해당 섹션에서는 Windows 10 기반 PC에서 사용할 수 있는 클라우드 서비스를 이용해 분석을 수행하며, 해당 운영 체제에서 설치한 Box 클라우드에서 수행한 행위 목록은 아래와 같다.

- 설치파일 다운로드 및 실행
- 계정 생성 / 로그인
- 데이터 업로드 / 동기화 / 삭제 / 복원
- 데이터 이름 변경
- 프로그램 삭제

본 논문에서는 프로그램 설치, 파일 업로드/동기화/삭제, 프로그램 삭제 행위와 관련된 아티팩트에 관하여 설명하고 Box 클라우드와 관련된 사건 시나리오를 분석한다.

3.1. 설치파일 다운로드 및 실행

설치파일을 다운로드하고 난 후 파일 시스템에서 생긴 아티팩트로는 WebCacheV01.dat와 .msi 설치 파일이 있다. WebCacheV01.dat에서 먼저 Content 데이터베이스를 살펴보면 URL과 File name을 볼 수 있고, 동기화 시간, 생성 / 수정 시간 만료 시간, 접근 시간, ResponseHeader 등을 추가적으로 확인할 수 있다. https://cdn03. boxcdn .net/ 는 Box 클라우드 메인 홈페이지를 의미하며 .js 파일과 .css 파일에 따라 포함된 내용이 다르다. https://cdn03.boxcdn.net/sites/default/files/styles/1440x495/public/2018-03/herofinder0.png?itok=TeB8j4E 는 설치파일 다운로드 페이지를 들어갔을 때 Box 사용 시 폴더 사용 예시로 나와 있는 화면이고, https://cdn03.boxcdn.net/sites/default/files/styles/1440x900/public/2017-10/drivebg.jpg?itok=Kn-0G3W7 은 다운로드 홈페이지의 배경화면 이다. 이와 관련된 내용은 아래 History 데이터베이스에서도 확인할 수 있다.

History 데이터베이스[표 1]에서는 방문한 URL과 해당 URL의 Page Title을 확인할 수 있고, 그 외로 Urlhash 값, 동기화 시간, 생성 및 수정 시간, 만료 시간, 접근 시간 등을 확인할 수 있다. 설치 파일을 다운로드할 경우 Box 클라우드에 접속하여 다운로드 메뉴에 들어간 후의 URL과 다운로드 받은 파일 이름을 확인할 수 있다. 여기서 favicon이란 웹 페이지에 접속했을 시 상단 탭에 보이는 아이콘을 의미하며, 대부분 아이콘 파일(.ico)의 형태를 띠고 있고 사이트의 로고 개념과 비슷하다.

iedownload 데이터베이스에서도 마찬가지로 URL, File name, 동기화 시간, 생성 및 수정 시간, 만료 시간,

〔표 1〕 History Database-설치파일 다운로드

URL	Page Title
https://www.box.com/resources/downloads/drive	https://www.box.com/themes/custom/box/favicons/favicon-32x32.png?v=eEagRR2lRz
https://e3.boxcdn.net/boxinstallers/desktop/releases/win/Box-x64.msi	-

(그림 2) iedownload Database-설치파일 다운로드

접근 시간 등을 확인할 수 있고 추가적으로 iedownload라는 탭에서 파일을 다운로드 받은 URL, 다운로드 받은 파일 형식, Cache 데이터 위치, 다운로드 위치 등을 확인할 수 있다[그림 2].

.msi 파일로는 총 3가지를 발견하였고, 관련된 리스트는 다음과 같다.

- %USERPROFILE%AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!001\MicrosoftEdge\Cache\87IX58EI\Box-64[1].msi
- %USERPROFILE%Downloads\Box-x64.msi
- \Windows\Installer\c8b21.msi

Box-64[1].msi은 Microsoft Edge 브라우저를 사용하여 다운로드 받은 Box 클라우드 설치 파일의 Cache 데이터를 의미하고, 두 번째는 실제로 Box-x64.msi를 다운로드 받아 저장한 위치를 뜻하며, 마지막 \Windows\Installer는 Windows용 응용 프로그램 설치와 패치 작업을 위한 영역으로 해당 폴더에도 저장된다.

다음으로 레지스트리 기록을 살펴보면 HKCR에는 Windows 64 bit 환경에서 32 bit 프로그램을 실행하기 위해 호환성을 제공하는 Windows on Windows(WOW) 폴더가 공통적으로 존재하였으며, 하위 폴더로 AppID, protocols, typelib가 생성되었다. AppID 는 COM 객체의 guid 값이고 protocols는 하위에 classID나 Default로 html텍스트를 필터링 하여 보여주며, 인터페이스가 레지스트리에 등록 되고 해당 인터페이스에 정의된 레지스트리를 들어가면 typelib가 연결되어 나타난다. HKU 에서는 muicache와 관련된 내용을 확인할 수 있었다. muicache는 프로그램이 실행할 때 마다 윈도우가 실행 파일의 리소스에서 프로그램의 이름을 추출하여 추후 사용을 위해 저장하는 것을 말하며 다중 언어 지원을 위한 프로그램 이름을 캐시하는 역할을 한다. 특히 muicache\41\71f2 3c34 은 프로그램에서 사용하는 언어 관련 정보를 저장하며 한국어를 사용할 경우 ko-KR 값을 가지게 된다. HKLM에서는 hivelist 파일을 볼 수 있고, 해당 파일에는 응용 프로그램 정보, 사용자 계정 정보, 권한 정보 등이 존재한다.

설치파일을 실행하면 %USERPROFILE%AppData\Local\경로 하에 Box 폴더가 생성되고 Box 클라우드 사용 인증서, sync.db, Log, Cache 등 텍스트 파일이 저장된다. ~\Box\Box\Logs\에 저장되어 있는 BoxAU-' 클라우드 실행 날짜'.log 파일에는 권한 확인 기록, 타임 스탬프, 모니터링 기록, 세션/ 디바이스/어플리케이션 ID, 어플리케이션 버전, 데이터 위치 경로, Box 클라우드 버전 및 설치 파일이 포함된 다운로드 URL 등이 존재한다. ~\Box\Box\Metrics에 저장되어 있는 au_met rics.db 파일의 metrics 테이블에서는 해시 값과 우선순위, 가장 최근에 업데이트된 시간 등, data 테이블에서는 ID 값과 해시 집합, 어플리케이션 이름, 카테고리, 데이터 소스, 디바이스 ID, 이벤트 타입, 타임 스탬프, Metric 이름 및 타입, 세션 ID 등을 확인할 수 있고, tags 테이블에서는 ID, 태그, 태그 값 등을 확인할 수 있다.

설치파일 실행 시 레지스트리 기록 중 HKCR 에서는 HKEY_CLASSES_ROOT\boxdesktop.boxnote\shell\open\command에서 Box.exe을 실행한 기록, HKEY_CLASSES_ ROOT\boxdesktop.boxnote\shell은 데스크 톱에 설치된 box note를 실행하였음을 의미한다. HKEY_CLASSES_ROOT\installer\products*는 설치 파일 을 다운로드 받고 난 후 제품 이름, 패키지 코드, 언어, 버전, 아이콘 위치, 클라이언트와 관련된 정보가 저장되며 HKEY_CLASSES_ROOT\installer\products*\sourcelist는 설치 파일인 .msi의 정보와 이 파일이 저장된 위치를 보여준다. HKU에서는 HKEY_USERS\desktop-name\userID\software\microsoft\windows\currentversion\explorer\desktop\namespace 경로에서 Box 클라우드 실행 파일 위치, 시작메뉴에서 접속할 수 있는 폴더 경로 등을 확인할 수 있고 HKEY_USERS\desktop-name\userID\software\box\box\에서 사용한 Box의 마지막 버전을 알 수 있다. 해당 경로의 하위 폴더인 preferences 폴더에 Box가 업데이트되면서 AppData에서 현재 사용자 환경 설정 및 스마트 액세스 정책, 이상 탐지 등을 포함하게 되었고 이는 해당 폴더의 레지스트리 키를 편집할 수 있도록 수정되었다. 마지막으로 HKLM에서는 HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\installer\userdata\ntauthority\system\components*에서 설치한 소프트웨어 이름 및 사용자의 NT 권한, 오프라인에서 Box 클라우드를 사용할 수 있는 지 여부, 동기화 기능을 확인할 수

있고 HKEY_LOCAL_MA CHINE\software\box\box에서 설치 경로, 자동 업데이트 충돌 여부, rollout ID, 최신 다운로드 버전 등을 확인할 수 있다.

3.2. 데이터 업로드

데이터 업로드 시 ~\Box\Box\logs 폴더에 Shell_Ext_explorer_000.log가 생긴다. Explorer .exe는 Windows 쉘 기능을 담당하는 프로세스로 내 PC나 탐색기 등에서 실행한 프로그램을 자식 프로세스 형태로 관리한다. 즉, Box.exe를 실행하여 파일을 업로드 하였으므로 부모 프로세스인 Explorer.exe 아래 자식 프로세스로 Box.exe가 저장되는 것이다. 이 때 Shell Extension이 로딩 되는 시점은 Explorer.exe가 실행되는 시점으로, Explorer.exe가 실행될 때 레지스트리에 설정된 정보를 이용하여 해당 Extension이 존재하는 지 확인하여 로딩 여부를 결정한다. sync.db-wal 파일 역시 생성되는데, .db-wal은 데이터베이스에서 트랜잭션 실패 시 SQLite가 롤백할 수 있도록 만들어 놓은 파일을 의미한다. 해당 파일 형식은 SQLite format 3로 start up_completed_cleanly, copying_outgoing_metrics_databases, user_is_currently_logged_in, user_id, login_name, enterprise_id, display_ user_name, enterprise_name 등이 있다. 여기서 login_name, display_user_name에는 사용자의 아이디가 저장되어 있어 계정 정보를 확인할 수 있고 user_is_currently_logged_in 에서 사용자의 최근 접속 기록 등을 찾아볼 수 있다. 또한 Box 폴더에 링크 파일이 생성되며 링크 생성 시간, 접속 시간, 쓰기 시간, 드라이브 타입, 해당 폴더의 경로 등을 확인할 수 있다.

3.3. 데이터 동기화

데이터 동기화 시 파일이 저장되는 기본 폴더는 C:\ 이고 관련된 아티팩트는 txt 파일, log 파일 등이 있다. txt 파일로는 %USERPROFILE%AppData\Local\BoxSync\sync_root_folder.txt가 있으며 이는 동기화에 사용되는 프로그램인 Box Sync의 경로가 저장되어 있다. Box Sync의 기본 경로는 %USERPROFILE%Box Sync로 설정되어 있다. log 파일은 첫 번째로 %USERPROFILE%AppData\Local\BoxSync\Logs\OverlayService - yyyy-mm-dd.log 가 있다. 해당 파일에는 Sync IconOverlay Service.dll와 관련된 내용이 존재하는데, 이는 Box sync에서 설치한 소프트웨어 파일로 프로세스의 컨텍스트에서 동작하는 동적 링크 라이브러리로 로드 되며 .NET run-time 프레임워크를 설치해야 사용할 수 있다. 이 때 publisher는 Box, Inc.이고 Product 이름은 SyncIconOverlay Service 이다. 두 번째로 %USERPROFILE%AppData\Local\BoxSync\Logs\BoxSync.exe.log에는 프로그램을 사용하는 시스템, 윈도우, 보안성, xml, 서비스 모델, 엔터프라이즈 서비스, 웹 버전, 공개키 토큰 등과 관련된 내용이 존재한다. 레지스트리로는 HKU 기록[표 2]가 남았고, 해당 파일에는 BoxSync 실행 파일 위치, .ico 파일 위치, Box Sync 폴더 위치 등이 존재한다.

〔표 2〕 HKU-데이터 동기화

URL	Page Title
HKU\\software\microsoft\windows\currentversion\explorer\featureusage\appswitched	Box\Box Sync\Box Sync.exe
HKEY_USERS\s-1-5-21-3100165863-747826731-4202479803-1001_classes\clsid\{4a8fcd9f-623c-4283-96f0-10f41846a98a}\defaulticon	C:\Program Files\ Box\Box Sync\Win dowsFolder.ico
HKEY_USERS\desktop-name\userID\software\microsoft\windows\currentversion\explorer\desktop\namespace\{4a8fcd9f-623c-4283-96f0-10f41846a98a}	Box Sync

3.4. 데이터 삭제

데이터 삭제와 관련된 아티팩트는 log 파일이 있다. 첫 번째 로그파일은 %UserProfile%AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Box.exe.log로 파일은 Box.exe를 사용하였을 때 남는 로그로 시스템, 시스템 버전, 윈도우 폼, 코어 시스템, .NET 버전, 웹 어플리케이션 서비스, 런타임 캐시 등에 대해 버전, culture, 공개키 토큰 등을 설명하고 있다. 두 번째 로그파일은 %UserProfile%AppData\Local\Box Sync\Logs\Icon Overlay-yyyy- mm-dd.log로 해당 버전이 Icon Overlay Client.dll 파일로 구성되어 있음과 Box

Overlay Service가 실행되고 있는 내용이 저장되어 있다.

3.5. 프로그램 삭제

PC에서 Box 클라우드를 완전하게 삭제하기 위해 제어판에서 프로그램 추가 및 삭제에 들어가 제거하는 방법을 사용하였다. Box 클라우드 제거 후 남은 아티팩트는 로그 파일들이 있다.

첫 번째로 %USERPROFILE%AppData\Loc al\Box Sync\Logs\Context Menu-yyyy-mm- dd - yyyy-mm-dd.log의 내용은 [그림 3]과 같다.

ContextMenuClient.dll.config에서 Context menu는 그래픽 사용자 인터페이스 안에서 항목 클릭 시 뜨는 팝업 메뉴로 바로가기 메뉴라고도 부르며 이 config 파일은 Context menu와 관련된 설정에 대한 텍스트 파일이다.

두 번째로 BoxSync-클라우드 버전.log의 경로는 %USERPROFILE%AppData\Local\Microsoft\CLR_v4.0\UsageLogs 이다. CLR은 Common Language Runtime의 약어이며 Microsoft .NET 프레임 워크로 프로그램 언어로 작성된 프로그램의 실행을 관리한다. 하위 폴더인 UsageLogs에는 세션 중에 사용된 소프트웨어 등과 관련된 사용 로그 등 개인 정보가 저장되어 있다.

레지스트리에는 HKLM에서 관련 흔적을 찾을 수 있는데, 직접적으로 연관되어 있는 아티팩트로 총 12개를 확인하였다. 해당 파일에는 롤백 스크립트를 가리키는 \scripts라는 값과 Box 클라우드 및 Box Sync, Box notes 등 실행 파일 및 ico 파일, 업데이트 충돌 여부, 프로그램 삭제 플래그 값 등이 존재한다. 이와 관련된 내용은 [표 3]과 같다.

```
context menu-2019-08-08-2019-08-08.log 2019-08-08 16:34:27,158
[1] INFO  - version 1.0.8.0 configured with: C:₩Program Files₩Box
₩Box Sync₩ ContextMenuClient.dll.config
```

(그림 3) Context Menu.log-프로그램 삭제

〔표 3〕 HKLM-프로그램 삭제

File name	Viewer List
Box Sync-version.log	- Box sync 설치 여부 - Preference key - File manager - Main thread - Sync App thread
sync.db	- Program status - Last update time - Source file system - Time stamp - 소유자 - Path
metrics.db	
item_status.db	
streemfs.db	- fsnodes table - Contains name - Unix timestamp - iNode identifier
cacert.pem	- Publisher - Client - Label - Serial number - Hash value - Certification contents
INSTALL_GUID.txt	- Box sync setup execution file information (version, image size, binary type 등)
HKEY_LOCAL_MACHINE\..\reparsepoints	- DosDevices setting
HKEY_USERS\..\preferences	- Login log - Login name - Login ID - Enterprise ID - Box homepage - Sync folder path
HKEY_USERS\..\namespace\{*}	- Folder name
Other	- Migration version information

Ⅳ. 사건 시나리오 분석

클라우드 서비스의 빠른 발전으로 인해 다양한 곳에서 클라우드 서비스를 이용하고 있다. 또한 이러한 기술은 실제 범죄에 사용한 증거물이 클라우드 서비스에서 발견되는 사례가 많아지고 있다. 이에 따라, 해당 섹션에서는 현실에서 발생 가능하고 클라우드 서비스를 이용한 실제 범죄사례를 참고하여 총 2개의 시나리오를 제시한다. 또한 제시한 각 시나리오에 대한 클라우드 포렌식 분석 방법을 제시한다.

4.1. Scenario A

4.1.1. 사건 개요

PC(Windows 10)를 압수수색 하였으나 모든 문서와 사진이 삭제가 되어있는 상황에서 바탕화면 등에서 Box 스토리지 클라우드 서비스 이용한 흔적이 발생되어 아티팩트 분석을 통해 추가 영장을 발부 받고자 한다.

4.1.2. 사건 분석

본 시나리오에서는 문서와 사진이 존재하지 않기 때문에 PC(Windows 10)에서 Box 스토리지 클라우드 서비스를 실행했던 흔적, 문서와 사진 파일이 동기화 혹은 업로드 된 흔적을 확인하여 추가 증거를 확보하고자 한다.

Windows 10에서는 설치된 프로그램을 실행하고 파일을 동기화하는 행위에 대한 흔적을 여러 아티팩트에서 찾을 수 있다. 프로그램 실행 및 파일 동기화와 관련된 흔적을 찾기 위해 Log File, Database File, Registry, Certificate File, Text File, 기타 파일을 분석한다. 해당 파일에 대한 경로 및 뷰어리스트는 [표 4, 5]를 통해 확인할 수 있다.

〔표 4〕 Synchronize Box cloud of Artifacts

File name	Viewer List
Box Sync-version.log	- Box sync 설치 여부 - Preference key - File manager - Main thread - Sync App thread
sync.db	- Program status - Last update time - Source file system - Time stamp - 소유자 - Path
metrics.db	
item_status.db	
streemfs.db	- fsnodes table - Contains name - Unix timestamp - iNode identifier
cacert.pem	- Publisher - Client - Label - Serial number - Hash value
	- Certification contents
INSTALL_GUID.txt	- Box sync setup execution file information (version, image size, binary type 등)
HKEY_LOCAL_MACHINE\..\reparsepoints	- DosDevices setting
HKEY_USERS\..\preferences	- Login log - Login name - Login ID - Enterprise ID - Box homepage - Sync folder path
HKEY_USERS\..\namespace\{*}	- Folder name
Other	- Migration version information

〔표 5〕 Execute Box cloud of Artifacts

File name	Viewer List
OverlayService-yyyy-mm-dd.log	- config file - icon overlay service
BoxSync.exe.log	-
BoxUI-yyyy-mm-dd.log	-
HKEY_LOCAL_MACHINE\..\namespace	- Box .exe path
HKEY_LOCAL_MACHINE\..\delegatefolders	
HKEY_USERS\desktop-name\username\software\google\drive	- file manager version - context menu disabled
HKEY_USERS\..\recentdocs	- MRUListEx

4.2. Scenario B

4.2.1. 사건 개요

몰카 사건과 관련하여 압수하여 분석한 폰에서 2년간 사용한 흔적을 발견하였으나, 실제 사진 폴더에는 범행 현장에서 찍은 2장 이외에 아무 사진도 없는 것을 확인하고, 범인이 가지고 있던 스마트폰이 범인이 사용하는 PC(Windows 10)에 연결된 흔적이 있었고, Box 클라우드가 설치되어 있음을 확인하였다. 이때 휴대폰에 있던 사진 파일이 PC 클라우드에 업로드 되었는지 확인하여 추가범행에 대한 사진 증거를 확보하려고 한다.

4.2.2. 사건 분석

본 사건에서는 범인이 휴대폰에 있던 사진 파일들을 PC에 복사한 후 PC 설치되어 있던 Box 클라우드에 업로드 하였는지 여부를 확인해야 하므로 파일을 복사한 후 PC에서 Box 클라우드에 업로드가 된 기록을 확인한다. 본 시나리오에서는 사용자가 바탕화면으로 파일을 복사하였음을 가정하고 분석을 수행한다. 다만 스마트폰의 연결 흔적을 찾는 분석은 본과제의 범위와 맞지 않으므로, 그에 대한 분석은 별도로 진행하지 아니하였다.

Box 클라우드에 파일을 업로드 하는 행위는 Box 클라우드 폴더에 해당 파일을 업로드 하여 Box sync로 동기화 하는 것이다. 이는 LNK 파일, Database File, Log File, Registry를 분석을 통해 확인할 수 있다. 해당 파일에 대한 경로 및 뷰어리스트는 [표 6]에서 확인할 수 있다.

〔표 6〕 Synchronize Box cloud of Artifacts

File name	Viewer List
Box Sync.lnk	- Create time - Modify time - Access time - Drive type
newsroom_metrics.db	- Timestamp
Shell_Ext_explorer_000.log	- Type - Adoption date - Context menu handler - Attribute handler - Drag and Drop handler
BoxSync.exe.log	- System version - Public key token - Culture - Path(Box sync log)
HKEY_USERS\..\appswitched	- GUID - Box sync .exe path
HKEY_USERS\..\defaulticon	- Box sync display - Folder icon
HKEY_USERS\..\initpropertybag	- Attributes - Target folder pattern(Box sync)
HKEY_USERS\..\{4a8fcd9f-623c-4283-96f0-10f41846a 98a}	- Name space(Box sync)

Ⅴ. 결 론

클라우드 컴퓨팅 환경에서는 사용자 정보가 클라우드 서버에 위치하고 서로 다른 사용자 간에 자원을 독립적으로 사용하지만 결과적으로 물리적인 자원은 공유하고 여러 디바이스를 통해 접속할 수 있다는 특징이 있다. 이는 많은 보안 위협을 발생시키고, 특히 클라우드 계정 해킹 공격으로 인한 개인정보 탈취 등 문제들이 나날이 증가하고 있다.

기존 연구들을 찾아본 결과 Google Drive, One Drive 등 상용화되어 있는 클라우드에 대한 분석은 활발히 진행 중이나 본 연구에서 선정한 Box 클라우드 포렌식 분석은 미흡한 상태이다. 또한 동기화 프로그램인 Box Sync 등 여러 하위 프로그램들을 포함하고 있어 다른 클라우드와 차이점을 보인다. 이에 따라 본 논문에서는 Box 클라우드 서비스를 선정하여 포렌식 분석을 수행하였다.

이를 바탕으로 추후에 다른 스토리지 클라우드 서비스인 iCloud, Google Drive, Dropbox 등에 대해서도 아티팩트 분석을 수행하여 각 클라우드 별 아티팩트 차이점을 비교할 것이다.

참 고 문 헌

[1] 이원상, 이성식, 이정환, 탁한용, 김일수. “클라우드 컴퓨팅 환경에서의 사이버범죄와 대응방안 연구”. 한국형사정책연구원 연구총서. (2012)

[2] 강성림, 박정흠, 이상진. “클라이언트관점의 SaaS 사용 흔적 분석.” 정보처리학회논문지 C 19.1 (2012): 1-8.

[3] Zhang, Qi, Lu Cheng, and Raouf Boutaba. “Cloud computing: state-of-the-art and research challenges.” Journal of internet services and applications 1.1 (2010): 7-18.

[4] 정일훈, 오정훈, 박정흠, 이상진. “IaaS 유형의 클라우드 컴퓨팅 서비스에 대한 디지털 포렌식 연구”. 정보보호학회논문지, (2011): 21(6), 55-65.

[5] Box developer, [URL: https://developer. box.com/].

〈저 자 소 개〉

윤 혜 민 (Hyemin Yun)

2019년 2월 : 서울여자대학교 정보보호학과 졸업
2019년 3월~현재 : 연세대학교 정보대학원 석사과정
<관심분야> 정보보호, 디지털 포렌식, 암호 등

김 재 욱 (Jaeuk Kim)

2018년 2월 : 세명대학교 정보통신학부 졸업
2018년 3월~현재 : 연세대학교 정보대학원 석사과정
<관심분야> 정보보호, 디지털 포렌식, AML 등

황 은 비 (Eunbi Hwang)

2019년 2월 : 성신여자대학교 통계학과 졸업
2019년 2월~현재 : 연세대학교 정보대학원 석사과정
<관심분야> 정보보호, 디지털 포렌식, 취약점 분석 등

김 해 니 (Haeni Kim)

2018년 2월 : 경일대학교 사이버보안학과 졸업
2018년 3월~현재 : 연세대학교 정보대학원 석사과정
<관심분야> 정보보호, 디지털 포렌식 등

권 태 경 (Taekyoung Kwon)

1992년 2월 : 연세대학교 컴퓨터과학과 학사
1995년 2월 : 연세대학교 컴퓨터과학과 석사
1995년 8월 : 연세대학교 컴퓨터과학과 박사
1999년~2000년 : U.C Berkely Post-Doc 2001년~2013년 8월 : 세종대학교 컴퓨터공학과교수
2007년~2008년 : Univ. Maryland at College Park 교환교수
2013년 9월~현재 : 연세대학교 정보대학원 교수
<관심분야> 암호프로토콜, Usable Security, 소프트웨어/시스템 보안, 기계학습과보안 등