ISSN : 1976-5304
https://kdfs.jams.or.kr

파일 시간정보 분석을 통한 클라우드 스토리지 사용행위 추적

이 민 병, 최 지 성, 박 정 흠, 이 상 진
고려대학교 정보보호연구원 디지털포렌식연구센터

Tracking on Usage of Cloud Storage with File Timestamp Analysis

Minbyoung Lee, Jisung Choi, Jungheum Park, Sangjin Lee
Dept. of Information Security, Korea University

요 약

파일의 시간정보는 파일시스템과 응용 프로그램, 사용자의 사용행위에 따라 다양하게 나타날 수 있기 때문에, 시간정보를 분석하면 사용자의 행위를 추적할 수 있는 단서가 될 수 있다. 특히 압수수색 과정에서 클라우드 스토리지 서비스와 동기화된 디지털 증거를 발견하였을 경우, 클라우드 서비스가 제공하는 동기화 기능으로 인해 디지털 포렌식 조사자는 사용자의 행위가 해당 기기에서 발생하였는지, 또는 외부기기에서 발생하여 동기화된 것인지 고려해야 한다.

본 논문에서는 대표적인 동기화 클라우드 서비스인 Google Drive, iCloud Drive, One Drive, Dropbox, Naver Cloud에 대한 디지털 포렌식 조사 시 로컬에서 발견된 클라우드 스토리지 파일의 시간정보를 분석하여 사용자의 클라우드 스토리지 사용행위를 추적한다.

주제어 : 클라우드 스토리지, 동기화, 시간정보

ABSTRACT

Since the timestamp of a file can be displayed variously according to a file system, application, and user behavior, analyzing timestamp is a clue to track the user behavior. Especially in case of found digital evidence synchronized with cloud storage service during the search and seizure, the digital forensic investigators should consider whether the user occurred the event on the device or synchronized with the external devices due to the synchronization provided by the cloud service.

In this paper, we analyze the timestamp of a file found in local cloud storage when processing digital forensic investigation about representative synchronized cloud service, which are Google Drive, iCloud Drive, One Drive, Dropbox, and Naver Cloud to track the cloud storage user behavior.

Key Words : Cloud Storage, Synchronization, Timestamp

Ⅰ. 서 론

최근 스마트 기기와 네트워크 기술의 발전으로 다양한 클라우드 스토리지 서비스가 등장했고 이러한 서비스들은 인터넷만 연결되어 있으면 어디에서든지 접근할 수 있는 뛰어난 접근성을 사용자에게 제공한다. 그리고 클라우드 스토리지에서 일반적으로 제공하는 실시간 동기화 기능은 사용자가 기기 간에 데이터를 이동하지 않아도 자동으로 동기화하여 동일한 데이터를 저장하는 편의성을 제공한다. 이처럼 뛰어난 접근성, 편의성으로 인해 클라우드 스토리지 서비스의 이용이 증가하고 있다.[1)]

계정으로 연결된 모든 기기에 클라우드 스토리지의 데이터를 동일하게 유지하는 동기화 기능은 사용자에게 편의를 제공하지만, 디지털 포렌식 조사자가 조사과정에서 클라우드 스토리지와 동기화된 파일을 발견한다면, 그 파일이 해당 기기에서 생성된 것인지 또는 외부기기로부터 동기화된 것인지에 대해서 명확히 해야 하는 어려움을 준다. 동일한 클라우드 스토리지의 계정을 복수의 사용자가 공유하여 사용했다면, 압수수색 대상자가 로컬 기기에서 발견된 파일을 본인과 무관하다고 주장

▪ Received 22 July 2019, Revised 25 August 2019, Accepted 4 September 2019
▪ 제 1저자(First Author) : Minbyoung Lee (Email : adam1986@korea.ac.kr)
▪ 교신저자(Corresponding Author) : SangJin Lee (Email : sangjin@korea.ac.kr)

할 수 있기 때문이다. 그리고 클라우드 스토리지의 디지털 증거가 로컬에서 작성되었는지 외부기기로부터 동기화된 것인지 간과한다면 분석가의 신뢰성이 공격받을 수도 있다[6].

클라우드 스토리지의 사용 행위정보를 획득하는 방법은 서비스 제공자로부터 획득하거나, 계정정보를 이용하여 스토리지에 접근하거나, 로컬 기기에 남겨진 정보를 통해 획득할 수 있다. 하지만 서비스 제공자로부터의 획득과 계정정보를 이용하는 것은 법적 관할권 등 절차적 문제와 적시 획득의 제한, 그리고 서비스 제공자의 거부와 비밀번호 이외 추가적인 인증수단의 사용으로 인해 수집이 불가능할 수도 있다. 그렇기 때문에 클라우드 스토리지의 사용 행위정보를 로컬 기기에 남겨진 정보만으로 판단해야 하는 경우가 발생할 수 있다.

클라우드 스토리지의 데이터 동기화는 원격지의 서버에 저장되어 있는 데이터가 네트워크를 통해 전송되는 과정을 거치며 새로운 파일이 생기거나 수정되기 때문에 시간정보가 변동될 수 있다. 파일의 시간정보는 다양하며 이는 사용자의 행위에 따라 특징적으로 변경되기 때문에 로컬 기기에서 클라우드 스토리지와 동기화된 데이터를 발견한다면 남겨진 시간정보를 통해 사용자의 행위를 특정할 수 있는 단서가 될 수 있다.

본 논문은 대표적인 클라우드 스토리지 서비스인 Google Drive, iCloud Drive, One Drive, Dropbox, Naver Cloud [2]에 대해 Windows 환경에서 로컬 PC 내에 클라우드 스토리지와 동기화된 파일의 시간정보를 분석하여 사용자의 클라우드 스토리지 사용행위를 추적한다.

Ⅱ. 기존연구

기존 클라우드 스토리지 서비스에 대한 조사 논문[1]에서는 Windows, mac OS, iOS, Android 운영체제에서의 클라우드 스토리지 서비스의 사용 흔적 수집 및 조사, 분석 방법에 대해서 연구했다. 실시간 동기화 서비스에 대한 포렌식 조사 절차 논문[2]에서는 운영체제별 클라우드 기반 실시간 동기화 서비스의 사용 흔적 분석과 수집절차에 대하여 연구했고 동기화 서비스를 이용한 데이터 원격삭제를 방지하는 조사 절차를 제안했다. 그리고 클라우드 컴퓨팅 서비스에 대한 절차적 조사방안과 구체적 분석방법을 제시하였다[3].

클라우드 스토리지 데이터를 수집할 때, 데이터나 메타데이터가 변경되는지 확인한 논문[4]에서는 Windows 7 환경에서 Dropbox, Google Drive, Sky Drive에 대해서 데이터의 해시값을 비교하고, 시간정보의 변경여부를 확인했다. 로컬 PC를 활용하여 클라우드 스토리지에 접근하여 획득한 데이터는 클라우드 스토리지에 업로드, 저장 및 다운로드하는 과정에서 데이터의 내용은 변경되지 않았고, 시간정보는 많은 변경사항이 있으나, 파일의 마지막으로 작성된 (수정된)시간은 동일하게 유지한다고 하였다.

기존 연구는 클라우드 스토리지 서비스와 실시간 동기화 서비스에 대해 운영체제에 기록되는 계정정보, 사용 흔적에 대한 연구와 포렌식 조사 절차에 대해서 진행되었다. 그리고 계정정보를 합법적으로 획득한 상황에서 클라우드 스토리지의 데이터를 안전하게 보존하는 방법에 관한 연구로, 클라우드 스토리지의 데이터를 네트워크를 통해 동기화하거나 다운로드하여 획득하였을 때 데이터의 변조와 시간정보의 변화를 비교하였지만, 클라우드 스토리지와 동기화된 로컬에 존재하는 파일에 대한 사용자의 행위에 따른 시간정보의 변화에 대한 연구는 이루어지지 않았다.

파일 조작에 따른 파일 시간 변화 분석 논문[5]에서는 사용자의 행위에 따른 파일이나 폴더의 시간변화를 분석하여 이를 바탕으로 사용자의 행위를 유추하였다. 시간정보는 사용자의 행위에 따라 특징적으로 변경되고, 사건 발생 순서를 재구성하는 과정에서 유용하게 쓰일 수 있기 때문에 시간정보의 변동여부를 반드시 확인해야 한다고 주장했다.

압수수색 대상 PC에서 클라우드 스토리지와 동기화된 데이터가 발견되었을 때 그 데이터가 로컬 PC에서 생성된 것인지, 아니면 다른 곳에서 생성되어 동기화된 파일인지 분석할 수 있는 Framework가 제안되었지만[6], 사용자의 행위에 따라 특징적으로 남는 파일의 시간정보 비교분석을 통한 사용자의 클라우드 스토리지 사용행위는 조사되지 않았다.

본 논문에서는 Windows 시스템에서 클라우드 스토리지 서비스별 시간정보의 변화를 비교하여, 중요 증거파일에 대한 사용행위를 특정할 수 있는 정보에 대해서 추적한다.

Ⅲ. 클라우드 스토리지 사용 행위정보 획득

3.1. 클라우드 서비스 제공자로부터 획득

클라우드 스토리지의 사용 행위정보를 획득하는 방법은 서비스 제공자로부터 데이터를 확보하는 것이 가장 확실하고 정확한 정보를 얻는다고 할 수 있지만, 법적 관할권을 벗어나는 해외 업체의 스토리지를 사용하는 경우가 많고, 해외의 스토리지 제공자로부터 데이터를 획득하기 위해서는 해당 국가의 법 집행기관과의 협력 등을 통해 제공받아야 하므로 적시에 증

1) 한국인터넷진흥원의 2018년 인터넷이용실태조사 최종보고서에 따르면 2018년 만 12세 이상 인터넷이용자의 클라우드 서비스 이용률은 30.2%이고 이용목적으로는 '자료 및 정보 관리'가 업무용 53.2%, 개인용 69.0%로 가장 높게 나타났다.

2) 한국미디어패널통계(통계청 국가승인통계 제 405001호)에 따르면 2018년 만 20세~60세 미만 인터넷이용자의 주로 이용하는 클라우드 서비스(1~3 순위 응답기준) Naver Cloud가 1위(41.6%), Google Drive(14.9%)가 2위로 나타났다,

거 확보가 불가능할 수 있다. 그리고 각 서비스 제공자들은 법 집행기관의 요청을 자체적으로 검토하여 데이터의 제공여부를 결정한다.

각 서비스 제공자들은 해당 서비스의 사용자에 대한 법 집행기관의 정보요청에 대한 데이터를 투명성 보고서를 통해 공개하고 있다. 투명성 보고서는 기업이 정부의 이용자 정보 제공요청, 콘텐츠 삭제요청 등에 따른 통계를 정기적으로 공개하는 기업 보고서의 한 형식으로 각 기업이 자율적으로 공개하는 보고서로서 정형화된 형식은 없으며, 자유롭게 공개하고 있다. 각 서비스 제공자 별로 사용자 정보요청에 대한 데이터 제공 비율을 정리하면 〔표 1〕과 같다.

〔표 1〕에서 볼 수 있듯이 사용자 정보요청에 대한 대한민국 관할권 이외 지역 서비스 제공자의 데이터 제공 비율은 평균 39.5%로 법 집행기관이 요구하는 모든 정보를 제공하지는 않고 있다. 그러므로 디지털 포렌식 조사관들은 대부분 압수수색 대상 기기로부터 사용 행위정보를 획득하여야 한다. 클라우드 서비스 제공자가 디지털 증거를 법 집행기관에 모두 제공한다면 클라우드 스토리지에 대한 포렌식 조사는 고려할 필요가 없을 것이다〔7〕.

표 1. 사용자 정보요청에 대한 각 서비스 제공자의 데이터 제공 비율(2013. 1월 ~ 2018. 6월)
Table 1. Data Providing rate for Government request(Jan 2013 ~ Jun 2018)

구분	본사	대상	요청	데이터 제공	제공비율
Google Drive	미국 캘리포니아	대한민국	4,337	-	39%
iCloud Drive	미국 캘리포니아	대한민국	121	58	49%
One Drive	미국 워싱턴	대한민국	1,096	786	69%
Dropbox	미국 샌프란시스코	미국 이외	266	3	1%
Naver Cloud	대한민국 경기도 성남시	대한민국	83,780	69,784	83%

* Naver Cloud의 투명성 보고서 중 통신제한조치(감청) 미포함

3.2. 계정접속을 통한 획득

사용자는 클라우드 스토리지 서비스에 계정정보를 통하여 접속하고 서비스 제공자로부터 스토리지 서비스를 제공받는다. 따라서 사용자의 계정정보를 획득할 수 있다면, 스토리지에 접근하여 저장된 데이터와 사용 행위정보를 획득할 수 있다. 이전에는 계정접속을 통해 획득한 증거의 증거능력에 대해서 논란이 있었지만, 대법원에서는 적법한 절차를 통해 획득한 외국계 서버 저장 이메일에 대한 증거능력을 인정하였는 바(대법원 2017도9747 판결), 이는 클라우드 서비스에도 동일하게 적용될 것이므로, 적법한 절차를 거쳐 획득한 클라우드 스토리지의 데이터도 증거로 인정받을 수 있을 것이다.

하지만, 각 클라우드 스토리지 서비스는 보안강화를 위해 2단계 인증이라는 추가적인 인증 서비스를 제공하고 있다. 만약 이 서비스를 활성화했다면, 아이디와 비밀번호를 적법하게 획득했더라도 계정에 접근하지 못할 수도 있다.[3] 그리고 계정에 접속했다고 하더라도 어떤 기기를 사용했는지 확인하지 못할 수도 있다.

3.3. 클라우드 시그니쳐

3.3.1. 웹 브라우저 아티팩트

클라우드 스토리지 서비스의 경우, 보통 웹 페이지 기반의 호스팅 서비스이기 때문에 웹 브라우저의 쿠키나 히스토리, 그리고 로그파일을 획득하고 조사하는 것이 중요하다〔8〕〔9〕. 웹 접속을 통해 클라우드 스토리지에 접근하는 것은 웹 브라우저를 통해 수행하므로, 웹 브라우저의 쿠키, 캐쉬, 히스토리 등 아티팩트를 분석하면, 클라우드 스토리지 서비스의 사용흔적을 확인할 수 있고, 브라우저에 저장된 사용자 정보를 획득할 수도 있다. 하지만, 웹 브라우저를 통한 클라우드 스토리지 서비스의 접속 정보가 남아있다고 하더라도, 다운로드 기록은 확인할 수 있지만, 파일의 업로드와 수정여부 등 사용 행위정보 전체를 웹 브라우저 아티팩트만으로 파악하기 어렵다.

3.3.2. 클라우드 클라이언트 로그파일

각 클라우드 스토리지 서비스는 동기화를 위한 클라이언트 프로그램이 존재하며, 사용자의 행위에 따라 각종 로그 기록을 생성한다. 클라이언트 프로그램을 이용하면 웹 브라우저 접속없이 클라우드 스토리지의 이용이 가능하므로 클라우드 클라이언트 로그파일을 확인해야 한다. 클라우드 클라이언트 로그파일은 스토리지 상의 업로드, 수정, 동기화 등의 행위정보와 그 행위가 발생함에 따라 변경되는 시간정보를 기록한다.

본 소절에서는 대표적인 클라우드 클라이언트 프로그램 로그파일의 동기화 기록에 대한 조사결과를 요약한다.

3) 대법원 2017도 9747 국가보안법위반(찬양, 고무 등)등 사건에서 국가정보원 수사관 등은 2015. 11. 26.에 압수수색을 통해 획득한 이메일 주소 및 비밀번호를 입력하여 로그인을 시도하였으나 추가 인증항목이 발생하지 않은 이메일 계정에 대해서만 수색이 가능하였다.

3.3.2.1. Google Drive

Google Drive를 사용하면 〔표 2〕와 같이 클라이언트 로그파일이 생성된다. Google Drive는 SQLite DB와 텍스트 형식을 사용하여 기록을 저장한다. Snapshot.db파일에는 Cloud entry와 Local entry로 구분하여 파일의 목록을 저장하고 있으며, 〔그림 1〕과 같이 파일의 시간정보가 4Byte 단위로 기록된다. Sync_log파일에는 업로드, 삭제, 동기화 등의 행위가 기록된다. 외부기기의 행위가 로컬 기기에 동기화 될 경우 'Direction.DOWNLOAD' 이후 행위가 기록되고, 로컬 기기의 행위가 스토리지에 동기화 될 경우 'Direction.UPLOAD' 이후 행위가 기록된다〔그림 2〕. 기록되는 행위는 생성(CREATE), 삭제(DELETE), 수정(MODIFY), 이동(MOVE), 이름변경(RENAME)의 행위가 기록된다.

표 2. Google Drive 클라이언트 로그파일
Table 2. Client Log Files of Google Drive

구분	파일시스템 경로	획득 가능한 정보
Google	%UserProfile%\AppData\Local\GoogleDrive\Drive\user_default\snapshot.db	파일 목록, 수정시간
	%UserProfile%\AppData\Local\GoogleDrive\Drive\user_default\sync_log.log	동기화 로그 기록

RecNo	doc_id	filename	modified	created	acl_role	doc_type	removed	size
Click here to define a filter								
1	root	root	<null>	<null>	<null>	0	<null>	<null>
2	1n9iQsiwlyEtlVfAx3P-ZfpDbdCWEL8mZ	copy_A.xlsx	1554726267	<null>	0	1	0	9606
3	1eB7BbKfCZ1I8waKXQk3WsRHPQOlgumOF	copy_A.docx	1554726292	<null>	0	1	0	12159

그림 1. Google Drive - Snapshot.db의 시간기록
Figure 1. Recorded time in Google Drive - Snapshot.db

```
2019-04-09 14:54:31,532 +0900 INFO pid=44880 48028:CloudWatcher     cloud_watcher.py:1183
CloudWatcher generated FSChange(Direction.DOWNLOAD, Action.MODIFY, local_id=LocalID(inode=1
2019-04-09 14:10:39,404 +0900 INFO pid=17256 9316:DifferThread     aggregator.py:56 -------->
Received change FSChange(Direction.UPLOAD, Action.MODIFY, local_id=LocalID(inode=1125899906849242L,
```

그림 2. Google Drive - Sync_log의 예
Figure 2. Example of Google Drive - Sync_log

3.3.2.2. iCloud Drive

iCloud Drive는 〔표 3〕의 경로에 클라이언트 로그파일이 생성된다. client.db와 sever.db 파일에서 동기화된 파일의 생성시간과 수정시간을 기록한다〔그림 3〕. 동기화의 기록은 asl.〔시간〕_〔날짜〕.log로 남고, 클라이언트 프로그램이 작동한 시간은 알 수 있지만, 사용자의 행위가 어떤 파일에 대해 일어났는지 로그 기록을 통해서는 확인할 수 없다.

표 3. iCloud Drive 클라우드 클라이언트 로그파일
Table 3. Client Log Files of iCloud Drive

구분	파일시스템 경로	획득 가능한 정보
iCloud	%UserProfile%\AppData\Local\Apple Inc\iCloudDrive\client.db	파일 목록
	%UserProfile%\AppData\Local\Apple Inc\iCloudDrive\server.db	생성시간, 수정시간
	%UserProfile%\AppData\Roaming\Apple Computer\Logs\asl.〔시간〕_〔날짜〕.log	동기화 기록

owner_id	item_birthtime	item_filename	version_mtime	version_size	version_name	item_finder_info
Click here to define a filter						
defaultOwner	1554726615	copy_A.docx	1554726615	12159	copy_A.docx	(null)
defaultOwner	1554726615	copy_A.pptx	1554726615	33872	copy_A.pptx	(null)

그림 3. iCloud Drive - Server.db의 시간기록
Figure 3. Recorded time in iCloud Drive - Server.db

3.3.2.3. One Drive

One Drive는 〔표 4〕와 같은 경로에 로그 파일이 생성된다. SyncDiagnostic 파일은 동기화가 시작되거나 중지될 때 갱신이 된다. 이 파일에는 동기화 상태, 클라이언트 버전 정보, device ID 등의 정보를 포함하고 있다. 로컬 기기에서 One Drive에 대한 사용자의 행위는 SyncEngine-〔날짜〕〔시간〕〔고유번호〕〔순번〕으로 기록이 생성되며, 기기가 재부팅되

면 고유번호가 변경되어 순번이 1부터 다시 시작하고, 동기화가 중지되었다가 재개되면 그 전 순번에 이어서 기록한다. 만약, SyncEngine 동기화 기록이 SyncDiagnostic 이후에 생성되었다면, 로컬에서의 행위가 있었다고 추측할 수 있다.

표 4. One Drive 클라우드 클라이언트 로그파일
Table 4. Client Log Files of One Drive

구분	파일시스템 경로	획득 가능한 정보
One Drive	%UserProfile%\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncDiagnostics.log	동기화 진단보고
	%UserProfile%\AppData\Local\Microsoft\OneDrive\logs\Personal\ SyncEngine-[날짜][시간][고유번호][순번]	행위기록
	%UserProfile%\AppData\Local\Microsoft\OneDrive\logs\Personal\ ObfuscationStringMap.txt	암호화 매칭정보

ObfuscationStringMap파일은 사용자 이름, 용어, 파일이름 등을 암호화한 단어와 매칭하는 정보를 저장하고[그림 5], 동기화 기록에는 암호화된 파일명으로 기록하며, 로컬에서 행위가 발생하면 'FILE_ACTION' 이후에 업로드(ADDED), 수정(MODIFIED), 이름변경(RENAMED), 삭제(REMOVED)의 행위를 기록한다[그림 6].

그림 5. One Drive - ObfuscationStringMap의 매칭 정보
Figure 5. Matching informatino in One Drive - ObfuscationStringMap

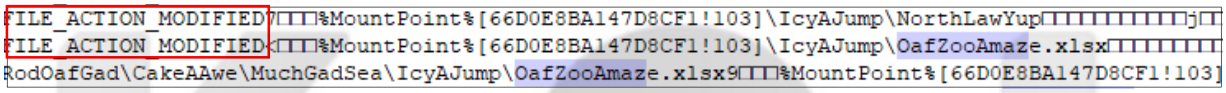

그림 6. One Drive - SyncEngine-[날짜][시간][고유번호][순번]의 예
Figure 6. Example of One Drive - SyncEngine.[date][time][unique number][sequence number].log

3.3.2.4. Dropbox

이전 연구에서 Dropbox 클라이언트(Ver.1.1.35)에서는 config.db와 filecache.db 파일에서 동기화 로그 기록을 확인할 수 있었으나, Dropbox 클라이언트(Ver.1.2.52) 이후에는 확인할 수 없었다[4]. 이를 확인할 수 있는 도구가 2017년 5월 decwindbx[10]라는 이름으로 오픈소스로 공개되어, 이번 연구에서 사용하였다.

로그파일의 경로는 [표 5]와 같고, Config.dbx에는 사용자의 정보가 포함되어 있고, filecache.dbx에는 파일의 목록과 생성, 수정시간 등을 포함하고 있다[그림 7].

표 5. Dropbox 클라우드 클라이언트 로그파일
Table 5. Client Log Files of Dropbox

구분	파일시스템 경로	획득 가능한 정보
Drop box	%UserProfile %\AppData \Local\Dropbox\config.dbx	사용자 정보
	%UserProfile %\AppData \Local\Dropbox\filecache.dbx	파일목록, 생성/수정시간

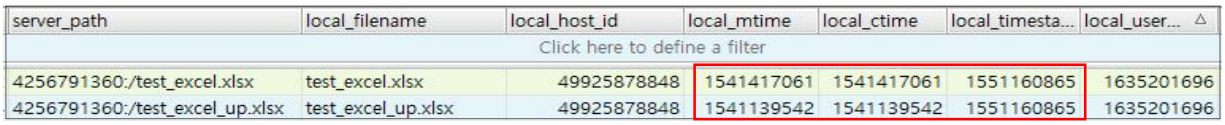

그림 7. Dropbox - filecache.dbx의 시간기록
Figure 7. Recorded time in Dropbox - fillecache.dbx

3.3.2.5. Naver Cloud

Naver Cloud의 로그 파일은 [표 6]과 같이 생성된다. 파일의 수정시간을 ODSyncLog.db에 파일타임 형식으로 기록하고[그림 8], N Drive\Temp 폴더에 날짜별로 저장되는 동기화 로그 파일에는 로컬에서 발생한 업로드(add), 이름변경(rename), 삭제(delete) 로그기록을 저장하고, 외부에서의 행위에 따라 동기화가 실행되면 'RunSync'와 동기화 실행시각, 소요된 시간을 기록한다[그림 9]. 동기화가 발생한 파일의 목록은 확인할 수 없다.

표 6. Naver Cloud 클라우드 클라이언트 로그파일
Table 6. Client Log Files of Naver Cloud

구분	파일시스템 경로	획득 가능한 정보
Naver Cloud	%UserProfile%\AppData\Local\NAVER\NaverNDrive\Temp	동기화 로그 기록
	%UserProfile%\AppData\Local\NAVER\NaverNDrive\'userID'\SyncLog\ODSyncLog.db	파일목록, 수정시간

file_name	dir_flag	sync_state	file_time	file_size	relative_path
					Click here to define a filter
q:₩users₩lmb0t₩navercloud₩내 문서₩copy_a.xlsx	0	0	1915384315:30731857	9606	₩내 문서₩copy_a.xlsx
q:₩users₩lmb0t₩navercloud₩내 문서₩copy_a.pptx	0	0	1646268047:30731857	33872	₩내 문서₩copy_a.pptx

그림 8. Naver Cloud - ODSyncLog.db에서의 시간정보 기록
Figure 8. Recorded time in Naver Cloud - ODSyncLog.db

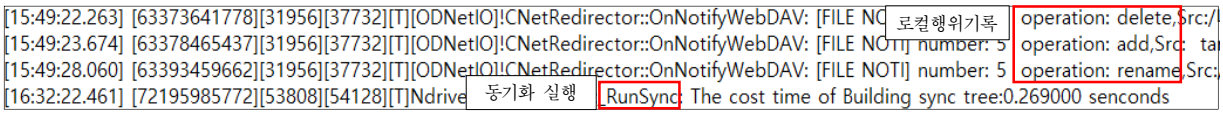

그림 9. Naver Cloud - 동기화 기록
Figure 9. Synchronization Log of Naver Cloud

3.3.3 획득 가능한 사용행위 정보

웹 브라우저 아티팩트와 클라우드 클라이언트 로그 파일을 통해 획득할 수 있는 정보에는 접속기록과 다운로드 기록, 계정정보, 동기화폴더 경로, 접속 기록, 동기화되는 파일의 목록과 그 파일의 생성시간과 수정시간, 동기화 로그 기록을 확인할 수 있다. 특히 동기화 로그 기록에는 사용자의 행위를 추적할 수 있는 정보가 기록된다. 하지만 서비스에 따라서 모든 행위를 기록하는 경우도 있으나, 기록을 찾을 수 없는 경우도 있다. 그리고 모든 행위를 기록한다고 하더라도 로그 기록을 분석하는 것은 일일이 문자열 검색을 통해 찾아내야 하므로 어렵고 시간이 오래 걸린다. 클라이언트 로그파일을 통해 획득 가능한 정보는 〔표 7〕과 같다.

표 7. 클라이언트 로그파일을 통해 획득 가능한 정보
Table 7. Information that can be acquired through Client Log

구분	계정정보	동기화 폴더 경로	저장된 파일목록	시간정보	행위정보	
					로컬	동기화
Google Drive	○	○	○	수정시간	○	○
iCloud Drive	○	○	○	생성시간, 수정시간	×	×
One Drive	○	○	×	생성시간, 수정시간	○	×
Dropbox	○	○	○	생성시간, 수정시간	×	×
Naver Cloud	○	○	○	수정시간	○	×

3.4. 파일의 시간정보

NTFS(New Technology File System) 파일시스템상에서 모든 파일은 1,024Byte 크기의 'MFT 엔트리'를 이용해 파일의 메타정보를 표현한다. MFT 엔트리는 파일의 위치, 시간정보, 크기 등의 속성 정보를 기록하며 NTFS상의 모든 파일의 MFT 엔트리는 NTFS 볼륨에 $MFT로 저장된다〔11〕. NTFS는 $Standard_Information(이하 $SI)과 $File_Name (이하 $FN)속성에 각각 생성시간(Created Time), 수정시간(Modified Time), MFT 변경시간(MFT Modified Time), 접근시간(Accessed Time)과 같이 4개 시간정보가 기록된 총 8개의 시간정보가 기록된다. NTFS의 시간값은 1601년 01월 01시(UTC)를 기준으로 100나노초(10^{-7})씩 증가하도록 만든 시간값으로 각 시간정보는 8바이트로 기록된다.

클라우드 스토리지의 동기화 폴더 역시 파일시스템상에 존재하기 때문에 파일의 타임스탬프 분석을 통해 파일에 대한 사용자의 행위를 추적할 수 있다. 클라이언트 로그파일을 통해 확인한 결과, 동기화되는 파일의 시간정보는 생성, 수정시간을 포함하고 있고, 초 단위의 정확도로 시간정보를 동기화하였다. Windows의 NTFS 파일시스템의 경우, 100나노초까지 시간값을 갖지만 클라이언트 프로그램은 초 단위의 시간정보를 가지고 동기화하기 때문에 클라이언트 프로그램을 통해 동기화가 이루어졌다면 해당 시간정보의 초 이하 부분이 0으로 표현이 될 것이다. NTFS 파일시스템 상에서 파일의 시간정보가 초 이하의 부분이 0이 될 확률은 10^{-7}이므로, 초 이하의 부분이 0이 되는 시간정보를 확인하면 파일에 대한 사용자의 행위를 추적할 수 있는 단서가 될 수 있다.

Ⅳ. 클라우드 서비스별 시간정보 변화

본 절에서는 Windows 시스템에서 클라우드 스토리지와 동기화된 파일의 시간정보를 분석하여 비교한다. 동일한 계정으로 연결된 두 개의 기기에서, 다음과 같이 사용행위를 구분하여 시간정보 변화를 분석하였다.

- 생성 : 클라우드 스토리지 동기화 폴더에 파일 직접 생성
- 복사 : 로컬 PC의 저장소에 저장된 파일을 클라우드 스토리지 동기화 폴더에 복사(Ctrl C+V)
- 수정 : 클라우드 스토리지 동기화 폴더의 파일 내용을 수정
- 이름변경 : 클라우드 스토리지 동기화 폴더의 파일 이름을 변경
- 동기화(생성) : 외부기기에서 파일 생성 후 로컬 PC에 동기화
- 동기화(수정) : 외부기기에서 파일 수정 후 로컬 PC에 동기화
- 동기화(이름변경) : 외부기기에서 파일 이름변경 후 로컬 PC에 동기화

이 실험의 목적은 파일의 시간정보를 분석하여, 해당파일에 대한 사용자의 행위가 로컬에서 수행되었는지, 외부기기에서 수행되어 동기화된 것인지 구분하는 것이다.

4.1. 실험방법

클라우드 서비스별 시간정보 변화를 시험하기 위해서, VMware Workstation 12로 Windows 7/8/8.1/10 가상머신을 각 버전별 2개(A와 B) 생성하였다. A PC에서 직접 동기화 폴더 내의 파일에 생성, 수정, 이름변경의 행위를 하여 시간정보의 변화를 분석하고, B PC에서의 사용행위가 A PC에 동기화되면 파일의 시간정보가 어떻게 변화하는지 분석하여 비교하였다. 실험대상 서비스는 Google Drive, iCloud Drive, One Drive, Dropbox, Naver Cloud이며, 실험방법을 그림으로 표현하면 〔그림 10〕과 같다. 접근시간의 갱신은 모두 비활성화한 상태로 실험하였다.

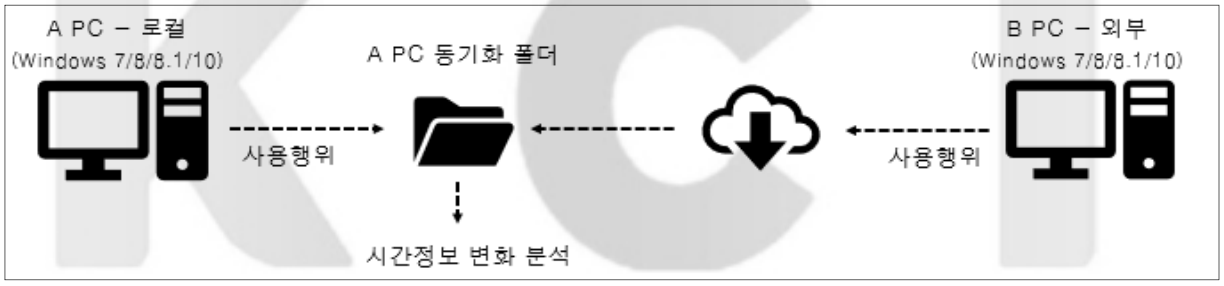

그림 10. 실험방법
Figure 10. Experiment Method

실험절차는 다음과 같고, FTK imager 4.1.1.1,로 $MFT를 추출하고, FS_Tool[4]로 시간정보를 획득하였다.

① Windows 7/8/8.1/10 버전별 각 2개(A/B)의 VM 생성
② Windows 테스트 계정생성 후 계정 폴더(%Userprofile%)를 실험용 파티션(Q:)으로 복사
③ 사용자 프로필 경로 변경을 위해 레지스트리 값 수정
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\
    * iCloud Drive는 동기화 폴더 경로 변경이 불가능하기 때문에 사용자 프로필 경로를 변경하여 실험
④ 각 클라우드 클라이언트 프로그램 설치
⑤ A PC에서 파일 생성, 복사, 수정, 이름변경 후 $MFT 추출 및 시간정보 획득
⑥ B PC에서 파일 생성, 복사, 수정, 이름변경 후 변경내용을 A PC에 동기화
⑦ A PC의 $MFT 추출 및 시간정보 획득
⑧ 각 클라우드 서비스별 시간변화 분석

4.2. 클라우드 서비스별 시간변화 분석결과

실험결과, 클라우드 스토리지 서비스별로 사용자의 행위에 따라 시간정보가 변화되는 특징이 달랐다. 특히 파일이 동기화 과정을 거치면 초 단위 이하(이하 10^{-7}초)가 0으로 설정이 되는 시간정보가 존재했다. 10^{-7}초가 0이 된다는 것은 해당 파일의 시간정보가 NTFS 파일시스템으로 인해 적용된 시간정보가 아니라는 의미를 갖는다. 즉, 10^{-7}초가 0으로 설정되는 시간

4) 고려대학교 디지털포렌식 연구센터 개발도구

정보의 비교를 통해서 파일에 대한 행위가 해당 기기에서 발생했는지, 또는 다른 기기로부터 발생되어 동기화가 되었는지 판단할 수 있다. Windows 버전에 따라 로컬에서 파일 수정시 시간정보의 변화가 달랐다. Windows 10에서 로컬 수정시 $SI의 접근시간이 수정시간으로 변경되지만, WIndows 8.1 버전 이하에서는 변경되지 않았다.

4.2.1. Google Drive

로컬에서 발생한 행위는 모든 시간정보의 시간값이 10^{-7}초 단위까지 있으며, 외부에서 파일이 수정되면 $SI 수정시간과 접근시간은 10^{-7}초가 0이 된다.

$SI 수정시간과 접근시간, $FN 수정시간과 접근시간의 10^{-7}초가 0인 파일은 동기화된 파일이거나 동기화된 파일을 로컬에서 이름변경 하였을 경우, 동기화된 파일이 외부에서 수정되거나, 외부에서 이름이 변경된 파일이다. 이 파일의 구분은 $SI 수정시간, MFT 변경시간과 $FN 수정시간, 생성시간, MFT 변경시간과의 비교를 통해 파악가능하다.

외부에서 동기화된 파일을 로컬에서 수정하는 경우, $SI 수정시간의 시간값은 10^{-7}초 단위까지 있지만, Windows 버전에 따라 10^{-7}초가 0이 되는 시간정보가 달랐다[표 8].

표 8. Google Drive에서 10^{-7}초가 0이 되는 사용행위
Table 8. Usage that makes 10^{-7}second to 0 on Google Drive

$Standard Information				$FileName				사용행위
M	A	C	E	M	A	C	E	
								로컬에서 작성한 파일을 외부에서 수정
$SI M = $FN M		C = E				C = E		외부에서 동기화
$SI M > $FN M		C < E				C = E		외부에서 동기화된 파일이 외부에서 수정
$SI M = $FN M		C < E				C = E		외부에서 동기화된 파일을 로컬에서 이름변경
		C < E				C < E		외부에서 이름이 변경
								외부에서 동기화된 파일을 로컬에서 수정(Win 10)
								외부에서 동기화된 파일을 로컬에서 수정(Win 7/8/8.1)
								로컬에서 수정 후 이름변경한 파일(Win 7/8/8.1)

* 음영 표시 부분은 10^{-7}초가 0이 되는 시간정보

4.2.2. iCloud Drive

iCloud Drive는 Google Drive와 다르게 로컬에서의 행위만으로도 10^{-7}초가 0으로 설정될 수 있다. 로컬파일을 동기화 폴더에 복사하면 $SI 생성시간과 수정시간, 접근시간의 10^{-7}초가 0이 된다. 동기화가 중지된 상태(네트워크 차단)에서 복사된 파일은 시간값이 동일하게 0이 되고 동기화 오류가 로그에 오류가 기록되지만, 생성된 파일은 모든 시간값이 10^{-7}초 단위까지 있고 동기화 오류가 로그에 기록이 되지 않는 것으로 보아, 복사된 파일은 iCloud 프로그램에 의해 시간값이 0으로 설정되는 것으로 추정된다.

$SI 생성/수정/접근시간과 $FN 생성/수정/접근시간의 10^{-7}초가 0인 파일의 구분은 각 시간정보의 비교를 통해서 가능하나, 이름변경이 로컬에서 발생했는지, 외부에서 발생했는지 구분할 수 없다.

로컬파일을 동기화 폴더에 복사하거나, 외부에서 동기화된 파일을 로컬에서 수정하는 경우 $SI 수정시간의 시간값은 10^{-7}초 단위까지 있지만, Windows 버전에 따라 10^{-7}초가 0이 되는 시간정보가 달랐다[표 9].

표 9. iCloud Drive에서 10^{-7}초가 0이 되는 사용행위
Table 9. Usage that makes 10^{-7}second to 0 on iCloud Drive

$Standard Information				$FileName				사용행위
M	A	C	E	M	A	C	E	
								로컬의 파일을 동기화폴더에 복사
M = A > C			$SI E = $FN E	M = A > C				동기화되거나, 외부수정
M = A = C			$SI E > $FN E	M = A = C				동기화폴더에 복사한 파일을 이름변경
M = A > C			$SI E > $FN E	M = A > C				동기화되거나, 외부수정한 파일을 이름변경
								동기화폴더에 복사한 파일을 로컬에서 수정(Win 10)
								동기화된 파일을 로컬에서 수정(Win 10)
								로컬에서 수정 후 이름변경(Win 10)
								동기화폴더에 복사한 파일을 로컬에서 수정(Win 7/8/8.1)
								동기화된 파일을 로컬에서 수정(Win 7/8/8.1)
								로컬에서 수정 후 이름변경(Win 7/8/8.1)

* 음영 표시 부분은 10^{-7}초가 0이 되는 시간정보

4.2.3. One Drive

모든 시간정보가 10^{-7}초 단위의 시간값을 갖는다면 로컬 PC에서 생성되거나 복사된 파일이지만, MicroSoft계정으로 연결된 Office 365 프로그램으로 생성하거나 수정한다면, $SI 수정시간과 접근시간의 10^{-7}초가 0이 된다. 외부에서 동기화되거나 수정된 파일의 $SI 수정시간과 접근시간의 10^{-7}초도 0으로 설정되는데, 이 파일의 구분은 $SI 생성시간과 수정시간의 비교를 통해서 구분이 가능하다.

$SI 수정시간과 접근시간의 10^{-7}초가 0이고, $FN 수정시간과 접근시간의 10^{-7}초가 0이면 로컬에서 생성한 파일을 이름변경하거나, 외부수정된 파일을 이름변경한 파일이다. 이 파일의 구분은 각 수정시간과 접근시간의 비교를 통해 가능하지만 이름변경이 로컬에서 발생했는지 외부에서 발생했는지는 구분할 수 없다.

외부에서 동기화된 파일을 로컬에서 수정하였을 경우, $SI 수정시간의 시간값은 10^{-7}초 단위까지 있지만, Windows 버전에 따라 10^{-7}초가 0이 되는 시간정보가 달랐다[표 10].

표 10. One Drive에서 10^{-7}초가 0이 되는 사용행위
Table 10. Usage that makes 10^{-7}second to 0 on One Drive

$Standard Information				$FileName				사용행위
M	A	C	E	M	A	C	E	
M < C								외부에서 동기화되거나, 외부에서 수정
M = C								로컬에서 생성되거나 수정된 파일(Office 365)
M < C								외부에서 동기화된 파일을 이름변경
M = C								로컬에서 생성되거나 수정된 파일을 이름변경(Office 365)
								이름변경 후 로컬 수정(Win 10)
								이름변경 후 로컬 수정(Win 7/8/8.1)
								동기화된 파일을 로컬에서 수정(Win 7/8/8.1)
								동기화된 파일을 로컬에서 수정 후 이름변경(Win 7/8/8.1)

* 음영 표시 부분은 10^{-7}초가 0이 되는 시간정보

4.2.4. Dropbox

로컬에서 발생한 행위는 모든 시간정보를 10^{-7}초 단위의 시간값을 갖게 하고, 외부에서 발생한 행위가 동기화되면 $SI 수정시간의 10^{-7}초가 0으로 설정된다. $FN 수정시간이 10^{-7}초가 0인 파일은 외부에서(또는 외부의 행위가) 동기화된 파일을 로컬에서 이름변경한 파일이다[표 11].

표 11. Dropbox에서 10^{-7}초가 0이 되는 사용행위
Table 11. Usage that makes 10^{-7}second to 0 on Dropbox

$Standard Information				$FileName				사용행위
M	A	C	E	M	A	C	E	
		C = E		M = A = C = E				외부에서 동기화되거나, 외부에서 이름변경
		C < E		C < M = A = E				외부에서 수정
		C < E			C = A = E			동기화된 파일을 로컬에서 이름변경
		C < E			C < A = E			외부수정된 파일을 로컬에서 이름변경

* 음영 표시 부분은 10^{-7}초가 0이 되는 시간정보

4.2.5. Naver Cloud

네이버 클라우드는 동기화 폴더의 경로가 두 가지로 설정된다. 첫 번째 경로는 사용자가 지정한 PC의 폴더경로(기본 경로는 %UserProfile%\NaverCloud)이고 두 번째 경로는 드라이브 형식으로 생성되는 Naver Cloud(N:)이다. 사용자가 지정한 동기화 폴더에 파일을 생성하면 $SI 수정시간은 10^{-7}초 단위의 시간값을 갖고, N:\에 생성하면 $SI 수정시간의 10^{-7}초는 0이 된다.

로컬에서 파일을 수정하거나 복사한 파일을 로컬에서 이름변경할 경우, 모든 시간정보는 10^{-7}초 단위의 시간값을 갖는다. 외부에서 발생한 행위가 동기화되면 $SI 수정시간의 10^{-7}초가 0으로 설정된다. $FN 수정시간의 10^{-7}초가 0값을 갖는 파일이면 로컬에서 이름변경한 파일이다. Naver Cloud의 클라이언트 프로그램은 두 가지 버전이 제공되는데 Windows 7에서는 네이버 클라우드 탐색기 Beta(v 1.5.)를 사용했고, Windows 8/8.1/10에서는 v2.0.을 사용했다. 탐색기 버전에 따라서 외부에서의 수정이 동기화될 때 시간변화의 차이가 발생했다[표 12].

표 12. Naver Cloud에서 10^{-7}초가 0이 되는 사용행위
Table 12. Usage that makes 10^{-7}second to 0 on Naver Cloud

버전	$Standard Information				$FileName				사용행위
	M	A	C	E	M	A	C	E	
공통	M = C								로컬에서 N:\에 생성
									로컬에서 이름변경
									로컬에서 이름변경 후 수정
v2.0	M > C								외부에서 수정된 파일
	M < C								외부에서 동기화되거나, 외부에서 이름변경
Beta(v1.5)	M < C								외부에서 동기화(생성, 수정, 이름변경)

* 음영 표시 부분은 10^{-7}초가 0이 되는 시간정보

Ⅴ. 결론 및 한계점

클라우드 스토리지의 사용 행위정보는 클라우드 스토리지 서비스 제공자로부터 획득하거나, 계정에 접속하여 획득할 수 있다. 하지만, 서비스 제공자가 정보를 제공하지 않을 수도 있고, 계정정보를 확보하지 못하거나 2차 인증 등의 문제로 접속하지 못할 수 있으므로 로컬 기기에서 획득한 정보만으로 판단해야 하는 경우가 있다.

로컬에 남아있는 정보에는 웹 아티팩트나 클라이언트 프로그램의 로그파일을 통해서도 확인할 수 있지만, 웹 아티팩트는 접속기록과 다운로드 등의 행위만 파악할 수 있고 클라이언트 프로그램의 로그파일은 분석하기 어렵고 확인할 수 있는 정보가 제한되는 경우도 있으므로, 사용자의 행위와 응용프로그램에 따라 특징적으로 변화하는 파일의 시간정보값의 비교를 통해 사용자의 행위를 추정해 보았다.

각 클라우드 스토리지 서비스의 시간정보 변화를 분석한 결과, 모든 클라우드 서비스가 사용행위에 따라 시간정보가 특징적으로 변화되고 그 특징은 클라우드 서비스 별로 다른 양상으로 변화하였다. 특히 NTFS 파일시스템상에서 10^{-7}확률로 발생하는 10^{-7}초가 0으로 설정되는 시간정보를 확인하면, 그 파일에 대한 사용자의 행위가 해당 기기에서 발생하였는지, 또는 외부기기에서 발생하여 동기화된 파일인지 추정할 수 있었다. 클라우드 스토리지 서비스의 경우, 압수수색 현장에서 웹 브라우저 접속기록과 클라이언트 로그 파일을 직접 확인하는 데에는 시간이 많이 소요되므로[12], 로컬 기기에서 획득한 파일의 시간정보 분석을 통해서 클라우드 스토리지의 사용 행위정보와 시각을 특정할 수 있다면 이후 사건을 재구성하는 단초를 얻고 조사범위를 한정할 수 있을 것이다.

특히, 압수수색 현장에서 발견한 클라우드 스토리지와 동기화된 증거파일에 대해서 로컬에서의 행위를 부정하고 악의적인 사용자가 외부에서 계정을 도용하여 발생한 행위가 동기화되었다고 주장할 경우, 로컬에서의 행위인지 외부기기에서 발생한 행위인지 사용자의 연관 여부를 시간정보로 확인할 수 있을 것이다.

다만 이 연구에서 파일 시간정보 분석은 가장 많이 사용되는 Windows 운영체제의 NTFS 파일시스템에서만 시행되었고, 다른 유형의 파일시스템에서는 분석하지 않았다. 대표적인 클라우드 스토리지 서비스 5가지에 대해서 시간정보 변경을 분석하였고 이외의 클라우드 시스템은 본 연구에서 비교하지 않았다. 그리고 시간정보를 변조 프로그램으로 변조하는 경우와 FAT 파일시스템의 파티션에서 파일을 복사하는 경우는 실험범위에 포함하지 않았고, iCloud Drive와 One Drive에서는 파일의 이름을 변경하는 경우, 시간정보의 비교만으로는 로컬에서의 행위인지 외부의 행위가 동기화된 것인지 추적할 수 없었다. 시간정보의 변화는 클라우드 클라이언트 프로그램 버전에 따라서 달라질 수 있다.

참 고 문 헌 (References)

〔1〕 H. J. Chung, J. H. Park and S. J. Lee, "Digital Forensic Investigation of Devices using Cloud Storage Service," Journal of Digital Forensics, Vol.8, pp.1-25, 2011.

〔2〕 J. H. Lee, H. J. Jung and S. J. Lee, "Forensic investigation procedure for real-time synchronization service," Journal of the Korea Institute of Information Security & Cryptology Vol.22, No.6, pp.1363-1374, 2012.

〔3〕 I. H. Jeong, J. H. Oh, J. H. Park and S. J. Lee, "Digital Forensic Methodology of IaaS Cloud Computing Service," Journal of the Korea Institute of Information Security & Cryptology, Vol.21, No.6, pp.55-65, 2011.

〔4〕 D. Quick and K. K. R. Choo, "Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?," Digital Investigation Vol.10, No.3, pp.266-277, 2013.

〔5〕 J. W. Bang, B. Y. Yoo and S. J. Lee, "Timestamp Analysis of Windows File Systems by File Manipulation Operations," Journal of the Korea Institute of Information Security & Cryptology, Vol.20, No.3, pp.79-91, 2010.

〔6〕 J. Boucher and N. A. Le-Khac, "Forensic framework to identify local vs synced artefacts," Digital Investigation, Vol.24, pp.S68-S75, 2018.

〔7〕 J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," Digital Investigation, Vol.9, pp.S90-S98, 2012.

〔8〕 S. Easwaramoorthy, S. Thamburasa, G. Samy, S. Bhushan and K. Aravind, "Digital Forensic Evidence Collection of Cloud Storage Data for Investigation," 2016 International Conference on Recent Trends in Information Technology (ICRTIT), 2016.

〔9〕 H. J. Chung, J. H. Park, S. J. Lee and C. H. Kang, "Digital forensic investigation of cloud storage services," Digital Investigation, Vol.9, No.2, pp.81-95, 2012.

〔10〕 A sort of a toolkit to decrypt Dropbox Windows BDX files, https://github.com/dfirfpi/decwindbx

〔11〕 S. M. Ho, D. Kao and W. Y. Wu, "Following the breadcrumbs: Timestamp pattern identification for cloud forensics," Digital Investigation, Vol.24, pp.79-94, 2018.

〔12〕 M. G. Kim, D. W. Jeong and S. J. Lee, "The Automatic Collection and Analysis System of Cloud Artifact," Journal of the Korea Institute of Information Security & Cryptology, Vol.25, No.6, pp.1377-1383, 2015.

저 자 소 개

이 민 병 (Minbyoung Lee)
준회원
2008년 3월 : 공군사관학교 졸업
2018년 3월 ~ 현재 : 고려대학교 정보보호학과 석사과정
관심분야 : 디지털 포렌식

최 지 성 (Jisung Choi)
정회원
2011년 2월 : 고려대학교 졸업
2015년 6월 ~ 2016년 12월 : ㈜마크애니 기술연구소 대리
2011년 3월 ~ 현재 : 고려대학교 정보보호학과 석박사통합과정
관심분야 : 디지털 포렌식, 운영체제 포렌식, 스마트폰 포렌식

박 정 흠 (Jungheum Park)
정회원
2009년 2월 : 고려대학교 정보경영공학전문대학원 공학석사
2014년 2월 : 고려대학교 정보보호대학원 공학박사
2014년 3월 ~ 2014년 12월 : 고려대학교 정보보호대학원 연구교수
2015년 1월 ~ 2018년 12월 : National Institute of Standards and Technology(NIST), Guest Researcher
2019년 1월 ~ 현재 : 고려대학교 정보보호대학원 연구교수
관심분야 : 디지털 포렌식, 사이버 보안, 사이버 물리 시스템

이 상 진 (Sangjin Lee)
정회원
1989년 10월 ~ 1999년 2월 : ETRI 선임연구원
1999년 3월 ~ 2001년 8월 : 고려대학교 자연과학대학 조교수
2001년 9월 ~ 현재 : 고려대학교 정보보호대학원 교수
2008년 3월 ~ 현재 : 고려대학교 디지털포렌식연구센터 센터장
2017년 3월 ~ 현재: 고려대학교 정보보호대학원 원장
관심분야 : 디지털 포렌식, 심층암호, 해쉬함수