情報保護學會論文誌
第 22 卷 第 6 號, 2012. 12

실시간 동기화 서비스에 대한 포렌식 조사 절차에 관한 연구*

이 지 희,† 정 현 지, 이 상 진‡
고려대학교 정보보호대학원

Forensic Investigation Procedure for Real-time Synchronization Service*

Jeehee Lee,† Hyunji Jung, Sangjin Lee‡
Graduate School of Information Security, Korea University

요 약

인터넷 연결 기기와 원격지 데이터 서비스의 증가로 실시간으로 데이터를 동기화 시켜주는 서비스가 증가하고 있으며 대표적인 서비스의 형태로는 실시간으로 데이터를 동기화하는 메일, 캘린더, 저장소 서비스 등이 있다. 이러한 실시간 동기화 서비스는 사용자에게 편의성을 제공하지만 실시간으로 동기화되는 특성 때문에 기기 압수 후 데이터가 변경될 수 있으므로 수사에 어려움이 발생한다. 본 논문은 수사 시 이런 어려움이 없도록 하기 위해서 각 기기에 남는 흔적들을 조사하고 실시간 동기화 데이터 보존 방법에 대해 제안한다. 이를 기반으로 실시간 동기화 데이터의 수집 절차를 제안한다.

ABSTRACT

The number and use of Internet connected devices has dramatically increased in the last several years. Therefore many services synchronizing data in real-time is increasing such as mail, calendar and storage service. This service provides convenience to users. However, after devices are seized, the data could be changed because of characteristic about real-time synchronization. Therefore digital investigation could be difficult by this service. This work investigates the traces on each local device and proposes a method for the preservation of real-time synchronized data. Based on these, we propose the procedures of real-time synchronization data.

Keywords: Digital Forensic, Real-time Synchronization Service, iCloud, Google, Storage Service

I. 서 론

최근 SNS나 클라우드 서비스 같은 원격지에 저장된 데이터를 이용하는 서비스의 사용이 증가함에 따라 이 서비스의 조사방법이 이슈화되고 있다. 실시간 동기화 서비스는 원격지에 저장되는 데이터를 이용하는 서비스로서 파일이나 데이터를 등록된 기기에 실시간으로 동기화하는 서비스이며 실시간으로 데이터를 동기화하는 메일, 캘린더, 저장소 서비스 등으로 분류할 수 있다. 실시간 동기화 서비스는 동일 계정으로 동일 데이터에 여러 단말기기를 이용하여 접근할 수 있으며 한 개의 단말기기에서 데이터를 수정한다면 계정에 등록된 다른 단말기기들의 데이터도 변경된다. 이처럼

접수일(2012년 11월 8일), 수정일(2012년 12월 5일), 게재확정일(2012년 12월 5일)
* 본 논문은 지식경제부 산업융합원천기술개발사업으로 지원된 연구결과입니다. [10035157, 실시간 분석을 위한 디지털 포렌식 기술 개발]
† 주저자, jhleeit@korea.ac.kr
‡ 교신저자, sangjin@korea.ac.kr

동기화되는 데이터는 사용자가 할당받은 저장소에 존재하며 다양한 단말기기를 이용해서 접근할 수 있으므로 기기가 네트워크에 연결되어 있다면 실시간 동기화 서비스 때문에 기기 안의 동기화 데이터가 쉽게 변경될 가능성이 있다. 그러므로 용의자가 실시간 동기화 서비스를 사용한다면 동기화된 데이터가 삭제 또는 위조되지 않도록 빠르게 수집하여 보존하는 것이 중요하다. 실시간 동기화 서비스는 Windows 시스템, Mac 시스템, Android OS와 iOS를 탑재한 스마트 폰이나 태블릿 PC에서 사용될 수 있다. 국내에서 사용되는 대표적인 서비스로는 Apple에서 제공하는 iCloud, Google에서 제공하는 메일(Mail), 캘린더(Calendar), 드라이브(Drive)가 있고 포탈이나 통신사 등의 회사에서 제공하는 N Drive, Daum Cloud, U Cloud, U+ Box 등이 있다.

디지털 기기를 이용하는 환경이 개인 컴퓨팅 환경에서 클라우드 컴퓨팅 환경으로 변화하면서 일반적인 포렌식 절차를 적용하기 어려워졌다. 그러므로 클라우드 컴퓨팅 환경을 고려한 포렌식 조사 절차가 제안되어야 한다. 포렌식 조사관은 사건이 발생하면 사건과 관련된 데이터를 담고 있는 기기를 압수하기 위한 영장을 법원에 요청하고 압수한 기기에서 데이터를 수집하고 분석한다. 이 과정 중 기기가 압수된 이후부터는 기기 또는 데이터의 변경이 없어야 한다. 그러나 압수된 기기나 데이터가 실시간 동기화 서비스를 사용하고 있다면 용의자는 다른 기기를 이용하여 데이터를 변경할 수 있다. 만약 실시간 동기화 서비스의 저장소에 사건과 관련된 데이터가 있다면 용의자는 손쉽게 이 데이터를 변경하거나 삭제할 수 있다. 이것은 증거를 얻을 수 없도록 하기 때문에 용의자가 자신의 저장소에 접근해서 증거 인멸을 시도하지 못하도록 차단하는 새로운 절차가 필요하다.

실시간 동기화 서비스를 사용하면 데이터가 쉽게 변경될 수 있기 때문에 신속하게 데이터를 수집하고 저장소에 대한 접근을 차폐하는 절차의 정립이 필요하다. 왜냐하면 동기화 서비스의 저장소에는 사건과 관련된 중요한 자료가 있을 수 있기 때문이다. 만약 용의자가 사건과 관련된 파일을 삭제한다면 로그에 삭제된 파일에 대한 기록이 남아도 정황증거가 되지만 파일을 삭제할 수 없다면 직접증거가 되기 때문에 이 절차가 유용하다. 동기화 서비스의 데이터 수집 절차가 정립되고 흔적이 남는 위치를 알 수 있다면 포렌식 조사관은 쉽고 빠르고 정확하게 데이터를 수집하고 저장소를 차폐할 수 있다. 본 논문은 실시간 동기화 데이터를 수집하는 방안과 절차를 제시하고 동기화 데이터를 보존하는 방법과 수사에 유용한 정보를 얻는 방법에 대해 제안한다.

2절에서는 관련연구를 소개하고 3절에서는 실시간 동기화 서비스의 데이터를 어떻게 수집할 것인지에 대한 절차를 제안한다. 논문이 제안하는 절차는 포렌식 조사관이 실시간 동기화 서비스를 사용하는 사용자의 기기를 조사할 때 도움이 된다. 4절에서는 실시간 동기화 데이터의 보존 방법에 대해 제안하고 5절에서는 앞서 기술한 서비스에 대해 실시간 동기화 데이터의 흔적을 조사한 결과에 대해 설명한다. 흔적을 조사한 이유는 실시간 동기화 서비스의 사용유무를 파악하여 3절에서 제안한 절차를 적용하고 유용한 정보의 수집을 가능하도록 하기 위함이다. 6절에서는 본 논문의 결과와 향후 연구 방향에 대해 설명한다.

II. 관련연구

기존의 네트워크의 연결을 고려한 디지털 수사 절차를 제안한 논문[1]에서는 수집된 컴퓨터의 디지털 증거가 다른 컴퓨터를 이용해서 원격으로 수정될 수 있기 때문에 네트워크와 분리해야한다고 제안했다. 이 논문은 네트워크를 이용하여 원격으로 데이터 변경이 일어날 가능성을 제시했지만 원격의 저장소에 저장된 데이터의 변경으로 수집된 기기의 데이터가 변경될 수 있는 경우는 고려하지 않았다. 이 문제의 발생을 막기 위해서 원격의 저장소를 차폐할 수 있는 방법이 제안되어야 한다.

실시간 동기화 서비스 중 대표적인 서비스인 클라우드 서비스의 데이터를 조사할 경우 사용자가 저장소에 한 행동을 알아내는 것은 어렵다[2]. 이에 대한 정보는 클라우드 서버의 로그를 이용해서 확인할 수 있지만 서버의 제공자는 사용자의 개인정보까지 공개하지 않을 것이다. 하지만 동기화 서비스의 특징을 고려해 기기에 남는 흔적을 조사한다면 행동에 대한 정보를 얻을 수 있다. 또한 압수한 개인 컴퓨터에서 클라우드 서비스의 사용 흔적을 찾아서 사용자의 저장소에 접근한 후, 파일과 접속 기록의 정보를 수집함으로써 클라우드 서비스의 데이터는 조사가 가능하다[3]. 하지만 이 논문은 단일 기기만을 고려했으며 용의자가 다른 기기로 저장소에 접근해서 데이터를 변경하는 경우는 고려하지 않았다. 실시간 동기화 서비스는 저장소에 저장된 데이터에 여러 개의 기기가 접근할 수 있으므로 단일 기기만을 고려한 절차를 사용한다면 문제

점이 발생할 수 있다.다른 기기로 저장소에 접근한다면 데이터의 원격 삭제가 가능하기 때문에 이것을 막을 수 있는 방법이 필요하다. 기존의 클라우드 서비스의 포렌식 조사 절차에 관련된 연구는 사전 준비, 초기대응, 분석방법선택, 증거자료 수집, 조사 및 분석, 보고서 작성의 순으로 이루어진다[4]. 이 논문은 모바일 기기에서의 클라우드 어플리케이션에 관한 절차를 제안하고 초기 절차에서 클라우드 시스템의 접속 차단이 중요하다고 언급했다. 하지만 접속을 차단할 수 있는 방법에 대해서는 구체적으로 연구하지 않았다.

실시간 동기화 서비스의 사용이 증가함에 따라 관련된 연구도 지속되고 있다. 하지만 아직까지 실시간 동기화 서비스의 특징을 고려한 포렌식 조사 절차는 제안되지 않았다. 그러므로 이 특성을 고려한 새로운 절차가 제안되어야 한다.

III. 실시간 동기화 데이터 수집 절차

실시간 동기화 서비스를 사용하는 기기에서 데이터가 변경되지 않고 수집되기 위해서는 각 기기와 데이터에 맞는 특징을 고려한 절차가 필요하다. 이 절차에는 기기안의 데이터가 변경되지 않도록 모바일 장치와 컴퓨터 시스템의 네트워크를 차단하고 계정정보를 이용해서 실시간 동기화 데이터 저장소에 대한 접근을 차단하는 과정이 포함된다. 이 차단 방법은 용의자가 원격에 있는 저장소의 데이터를 변경할 시간이 없도록 신속하게 진행되어야 한다. 실시간 동기화 서비스는 스마트 폰과 태블릿 PC같은 모바일 장치(Mobile Device)와 컴퓨터 시스템(Computer System)에서 사용이 가능하므로 데이터 수집을 [그림 1]과 같이 2가지로 나누어서 진행한다.

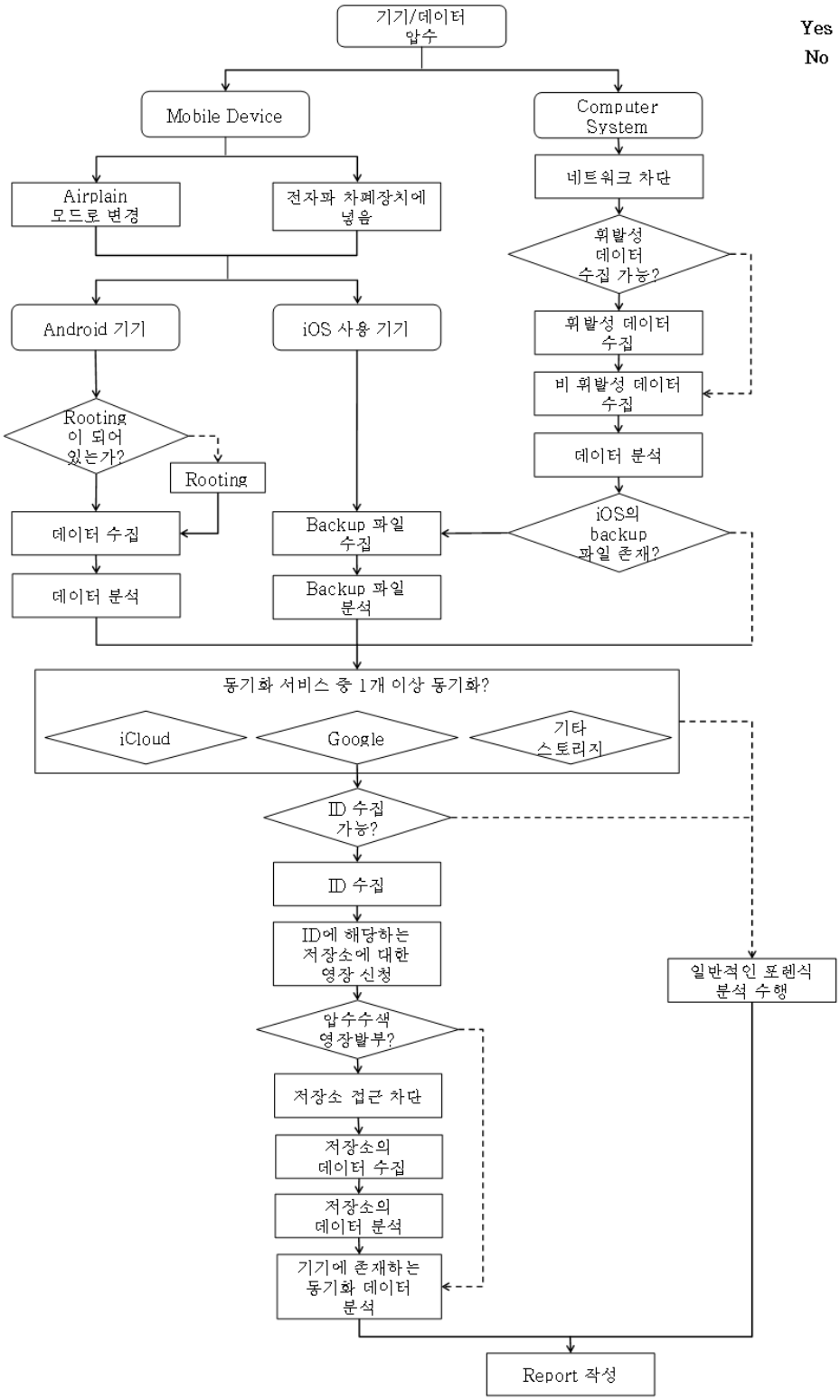
모바일 장치가 압수되면 기기에서 제공하는 비행기 모드(Airplain mode)로 변경하거나 전자파 차폐장치에 넣는다. 이것은 압수된 기기를 네트워크에 연결되지 못하도록 함으로써 장치 안의 실시간 동기화 데이터가 변경될 위험이 없도록 한다. 동기화 데이터의 변경 위험이 없기 때문에 수사관이 압수할 당시의 상태 그대로 데이터를 수집할 수 있다. 이후 압수한 모바일 장치의 운영체제가 Android인지 iOS인지 판별한다.

Android를 사용하는 기기의 데이터를 수집하기 위해서는 루팅(Rooting)이 필요하다. 따라서 루팅이 되어있지 않다면 루팅을 하고 데이터를 수집한 뒤에 분석을 한다. iOS를 사용하는 기기는 iPhone, iPod, iPad 등이 있다. iOS 기기는 Android 기기와는 다르게 탈옥(Jailbreak)을 하지 않고도 데이터를 수집할 수 있다. 이 기기의 데이터를 수집하는 방법은 Backup 파일을 얻는 것이다. Backup 파일은 쉽게 얻을 수 있으며 이 파일을 수집하고 분석하면 된다. 만약 압수된 iOS 기기가 탈옥되어 있다면 탈옥된 상태로 데이터를 수집해서 분석하면 된다.

대표적인 컴퓨터 시스템은 Windows 시스템과 Mac 시스템이 있다. 컴퓨터 시스템이 압수되면 동기화된 데이터가 변경되지 않도록 먼저 네트워크의 연결을 차단해야 한다. 왜냐하면 컴퓨터 시스템에 네트워크가 연결되면 데이터가 실시간으로 동기화되도록 설정되어있을 수도 있기 때문이다. 이 후, 이 시스템에서 휘발성 데이터가 수집 가능한지 확인한다. 만약 휘발성 데이터를 수집할 수 있다면 데이터를 수집하고, 비 휘발성 데이터를 수집한다. 이렇게 얻어진 데이터를 분석하고 이 데이터 중에 iOS의 Backup 파일이 존재한다면 파일을 따로 수집하고 이 파일은 iOS 기기의 흔적에 따라 분석한다.

분석된 모바일 장치와 컴퓨터 시스템이 실시간 동기화 서비스 중 1개 이상과 동기화 되어 있는지 확인하는 방법은 2가지가 있다. 루팅이나 탈옥되지 않은 상태에서 해당 어플리케이션의 설치 유무로 실시간 동기화 서비스의 사용 여부를 확인할 수 있으며 루팅이나 탈옥 후에는 각 서비스 별로 5절에 제안된 위치의 파일이 존재하는지의 여부로 확인할 수 있다. 기기가 동기화 되어 있다면 계정 정보와 유용한 정보 등이 수집 가능한지 확인한다. 만약 계정 정보의 수집이 가능하다면 계정 정보를 수집하고 이 계정에 할당된 저장소에 대한 영장을 신속하게 신청한다. 왜냐하면 용의자가 압수된 기기가 아닌 다른 기기를 이용해서 스토리지에 접근할 수 있기 때문이다. 용의자가 스토리지에 접근해서 압수된 기기의 데이터가 아니더라도 스토리지의 데이터를 변경할 가능성이 존재하기 때문에 계정정보를 수집하면 신속하게 영장을 신청해야 한다.

실시간 동기화 서비스와 동기화 되어 있지 않거나 동기화 되어 있지만 계정 정보를 수집할 수 없으면 일반적인 포렌식 분석을 수행한다. 5절에 제안된 위치에 수사에 유용한 데이터가 존재할 수 있으므로 이 위치도 분석한다. 압수수색 영장이 발부되면 계정 정보에 할당된 저장소에 대한 접근을 차단하고 데이터를 수집한 뒤 분석한다. 압수수색 영장이 발부되어 계정과 비밀번호를 획득한다면 비밀번호를 변경하여 용의자의 저장소 접근을 차단할 수도 있다. 기기 안에 존재하는



〔그림 1〕 실시간 동기화 데이터의 수집 절차

데이터와 저장소의 데이터가 불일치할 수 있으므로 기기안의 실시간 동기화 서비스의 데이터도 분석한다. 만약 영장이 발부되지 않는다면 기기에 존재하는 실시간 동기화 서비스의 데이터만 분석한다. 이렇게 분석된 데이터를 기반으로 보고서를 작성하면 포렌식 조사관은 압수된 기기의 실시간 동기화 데이터를 변경 없이 수집하고 조사할 수 있다.

이 절차는 서버 안의 실시간 동기화 데이터의 변경 가능성을 줄이기 위해 신속하게 진행되어야 한다.

IV. 실시간 동기화 데이터의 보존 방법

본 논문은 실시간 동기화 서비스의 특징을 고려한 동기화된 데이터를 보존하는 대표적인 방법으로 네트워크를 차단하는 방법, 저장소에 대한 접근을 차단하는 방법을 제안한다. 지금까지 실시간 동기화 데이터의 보존 방법에 대해서는 고려되거나 제안된 적이 없으므로 본 논문에서 제안된 보존 방법을 이용하면 실시간 동기화 서비스의 수사에 도움이 될 것이다.

네트워크를 차단하는 방법은 네트워크와의 직접적인 연결을 끊는 방법, 비행기 모드로 변경하는 방법, 전자파 차폐장치에 넣는 방법으로 나눌 수 있다. 네트워크와의 직접적인 연결을 끊는 방법은 연결된 기기에서 랜(LAN)선이나 무선랜 카드를 제거하거나 접속을 해제하는 방법을 사용한다. 이 방법을 사용하면 네트워크가 차단되기 때문에 실시간 동기화 데이터가 변경되지 않고 기기 안에 남는다. 비행기 모드는 통신망 또는 네트워크를 기기에서 차단하는 모드로서 항공기 운항 및 기타 전자장비의 잠재적인 방해를 줄이기 위해 무선 기능을 비활성화 한다. 이 모드를 사용하면 전화, 라디오, Wi-Fi, Bluetooth의 신호가 방출되지 않으며 GPS 수신이 꺼지는 등 다양한 기능이 비활성화 되고 기기의 데이터는 변경 없이 남게 된다. 〔그림 2〕는 비행기 모드 변경 이전과 이후, 동기화된 iCloud 데이터의 상태에 대해 실험한 것으로서 비행기 모드로 변경해도 데이터가 기기 안에 남는다는 것을 확인했다. 그러므로 이 모드를 사용하면 데이터의 변경 없이 압수상태 그대로 기기를 분석할 수 있다. 전자파 차폐장치는 외부의 전파로부터 기기를 보호하고 기기로부터 발생한 전자파가 외부로 유출되는 것을 방지하기 위한 장치이다. 이 장치는 전자 기기에서 발생하는 노이즈를 밖으로 내보내지 않고 또 외부에서 침입하는 노이즈를 차단하는 역할을 한다. 그러므로 이 장치 안에 기기를 넣으면 네트워크의 차단으로 동기화가 되지 않기 때문에 데이터가 변경되지 않게 된다.

또한 실시간 동기화 데이터는 저장소에 대한 접근을 차단함으로서 데이터를 보존할 수 있다. 일반적으로 디스크가 압수되면 쓰기방지장치(Write Blocker Device)를 사용하는 것처럼 실시간 동기화 서비스는 저장소에 대한 접근을 차단하여 데이터의 변경을 할 수 없도록 한다. 실시간 동기화 서비스의 저장소는 물리적으로 압수된 기기와 다른 위치에 존재하기 때문이다. 저장소의 위치를 알기 위해서는 저장소를 할당받은 계정 정보를 알아야 하고 서버를 소유한 회사에 알아낸 계정의 저장소에 대한 접근을 차단해달라고 요청해야 한다. 저장소에 대한 접근을 차단하면 압수 시의 데이터를 변경의 위험 없이 그대로 분석할 수 있다. 따라서 실시간 동기화 서비스를 사용하고 있는 기기가

〔그림 2〕 비행기 모드 변경 전/후의 iCloud 데이터 상태 비교

압수되면 용의자가 다른 기기에서 동일 계정을 이용해서 접근하지 못하도록 서비스의 계정정보를 알아내서 신속하게 접근 차단을 요청한다.

V. 실시간 동기화 데이터 흔적 조사

실시간 동기화 데이터를 수집하기 위해서는 실시간 동기화 서비스를 사용할 때 어떤 흔적이 남으며 이 중 유용한 정보는 어떤 것인지 알아야 한다. 본 절에서는 대표적인 실시간 동기화 서비스인 iCloud, Google, 기타 저장소 서비스에 대해서 각 기기별로 남는 흔적을 정리한다. 본 절에서 흔적을 조사한 실시간 동기화 서비스의 종류와 서비스 버전에 대한 정보와 사용 가능한 시스템에 대한 정보는 〔표 1〕에 있으며 지원하지 않는 서비스에 대해서는 'X'로 표시했다.

iCloud는 Apple에서 제공하는 실시간 동기화 서비스이다. 이 서비스는 Windows 시스템, Mac 시스템, iOS 사용 기기에서 실시간으로 데이터가 동기화 되도록 한다. 하지만 Android OS를 사용하는 기기에서는 iCloud를 사용할 수 없다. iCloud를 이용해서 동기화할 수 있는 데이터는 메일, 연락처, 캘린더, 책갈피, 노트, 사진 등이 있다.

Google에서 제공하는 대표적인 실시간 동기화 서비스는 메일, 캘린더, 드라이브가 있다. 서비스를 사용하기 위해서는 Google 계정이 필요하며 본 논문에서 다루는 4가지 시스템 상에서 모두 사용 가능하다.

대표적인 실시간 동기화 서비스 중 기타 저장소 서비스로는 N Drive, Daum Cloud, U Cloud, U+ Box 등이 있다. 본 논문에서는 이 4개의 서비스를 사용함으로써 디지털 기기에 남는 흔적을 조사했다. 이 중 3개의 서비스는 4가지 시스템을 모두 지원하지만 U+ Box 서비스는 Mac 시스템을 지원하지 않는다.

각 기기별로 남는 실시간 동기화 데이터의 흔적의 경로는 〔표 2〕에 정리되어 있으며 사용 흔적은 다음과 같다.

5.1 Windows System

Windows 시스템에서는 iCloud, Google 동기화 서비스인 메일, 캘린더, 드라이브, 기타 4가지 동기화 서비스 모두 사용이 가능하다. 조사에 사용된 Windows 시스템은 Windows 7이다.

윈도우 시스템에서 iCloud를 사용하려면 iCloud 제어판을 설치해야 한다. 이 서비스를 이용해서 실시간 동기화 할 수 있는 데이터의 종류로는 메일, 연락처, 캘린더, 책갈피, 사진 스트림이 있다. 메일, 연락처, 캘린더는 Outlook을 이용해서 데이터가 동기화 되고 책갈피는 인터넷 브라우저의 즐겨찾기와 동기화 된다. 사진 스트림은 업로드와 다운로드할 각 폴더의 경로를 지정하면 이 경로들의 데이터가 동기화 된다.

iCloud 제어판을 설치하면 MobileMeAccounts.plist 파일이 생성된다. 이 파일에는 〔그림 3〕과 같이 사용자의 ID 정보, 사용자의 이름, 각 서비스에 관련된 정보가 저장되어 있다.

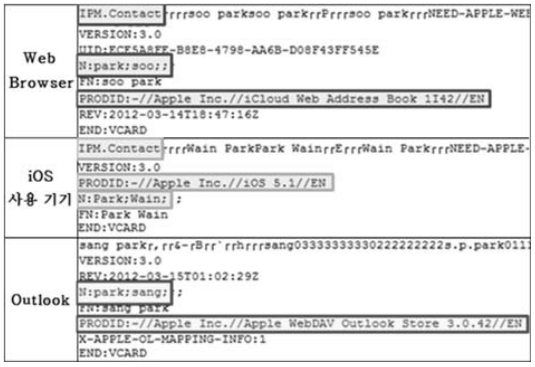
〔표 1〕 실시간 동기화 서비스 정보와 서비스 가능 시스템의 예

실시간 동기화 서비스		Windows	Mac	Android	iOS
iCloud	E-mail	1.0.1	OS X 10.8	X	iOS 5.1.1
	Contact				
	Calendar				
	Bookmark				
	Note				
	Photo				
Google	E-mail	Microsoft Outlook 14.0.6112.5000	OS X 10.8	2.3.5.2	iOS 5.1.1
	Calendar			2.3.6 GingerBread	
	Drive	1.4.3365.1552	1.3.3243.6774	1.1.1.6	1.0.2
기타 저장소 서비스	N Drive	1.2.0.8	1.1.5.111	2.0.5	2.0.5
	Daum Cloud	1.1.0.6	1.1.0.28	1.5.0	1.5.0
	U Cloud	1.0.4.73132.20110420	1.0.5.87211.20120304	2.1.9	1.3.0
	U+ Box	1.0.7.65	X	2.0.3	1.18.05

〔표 2〕 실시간 동기화 서비스의 흔적 경로

실시간 동기화 서비스		파일시스템 또는 레지스트리 경로
Windows		
iCloud	Mail, Memo	%UserProfile%\AppData\Local\Microsoft\Outlook\"Account Name".pst
	Contacts, Calendar	%UserProfile%\AppData\Local\7D4B79FA-F92D-49B5-990A-92FB793E38AB.aplzod\main.db
	Bookmarks	%UserProfile%\Favorites
Google	Mail, Calendar	%UserProfile%\AppData\Local\Microsoft\Outlook\"Account Name".pst
	Drive	%UserProfile%AppData\Local\Google\Drive
기타 저장소 서비스	N Drive	%UserProfile%\AppData\Local\Naver\NaverNDrive\'userID'
	Daum Cloud	%UserProfile%\AppData\Local\Daum\DaumCloud\daumcloud.sqlite %UserProfile%\AppData\Local\Daum\DaumCloud\log_'version'_'date'.txt
	U Cloud	%UserProfile%\AppData\Local\ucloud\lvol.db\index_fs_dn_parent.db %UserProfile%\AppData\Local\ucloud\sc1.log
	U+ Box	HKCU\Software\UPlusBox Drive
MAC		
iCloud	Mail	AosIMAP-forensic.study\INBOX.mbox
	Memo	AosIMAP-forensic.study\Notes.mbox
	Contacts	86FDF76A-C649-445C-9A50-7B3FAAB3B30C\Configuration.plist
	Calendar	81C9F971-5590-4A97-AF45-5174C1D6AD4B.caldav\"Calendar Name"
Google	Drive	Keychain
기타 저장소 서비스	N Drive	Keychain
	Daum Cloud	%User%Library/ApplicationSupport/Daum/DaumCloud/daumcloud.sqlite
	U Cloud	%User%Library/ApplicationSupport/UCloud/lvol.db/default_db.bdb
Android		
Google	Mail	/dbdata/databases/com/google/android.gm
	Calendar	/data/data/com.android.calendar/shared_prefs/com.android.calendar_preference.xml
	Drive	/data/data/com.google.android.apps.docs/shared_prefs/accountFlags'ID'.xml
기타 저장소 서비스	N Drive	/data/data/com.nhn.android.ndrive/shared_prefs/ndrive.settings.xml
	Daum Cloud	/data/data/net.daum.android.cloud/shared_prefs/net.daum.android.cloud_preferences.xml
	U Cloud	/data/data/com.kth.widgets.uucloud/databases/webview.db /data/data/com.kth.widgets.uucloud/shared_prefs/uCloudVariable.xml
	U+ Box	/data/data/lg.uplusbox/databases/lg_imory.db
iOS		
iCloud	Account	Library/Preferences/com.apple.accountsettings.plist
	Mail	Library/Mail/AutoFetchEnable
	Contacts	Library/AddressBook/AddressBook.splitedb
	Calendar	Library/Calendar/Calendar.sqlitedb
	Bookmarks	Library/Safari/Bookmarks.db
	Memo	Library/Notes/notes.sqlite
Google	Calendar	Library/Calendar/Calendar.sqlite
	Drive	com.google.Drive/Documents/items_snapshot_'ID'.db com.google.Drive/Documents/feed_snapshot_'ID'.db com.google.Drive/Library/Preferences/com.google.Drive.plist
기타 저장소 서비스	N Drive	Library/Preferences/com.nhncorp.NaverNDrive.plist
	Daum Cloud	Documents/DaumDisk.sqlite
	U Cloud	Library/Preferences/com.kth.ucloud.plist
	U+ Box	Library/Preferences/kr.co.uplusbox.uplusbox.plist

〔그림 3〕 MobileMeAccounts.plist 파일 내용



〔그림 4〕 PRODID에 남는 기기의 특성정보

사용자가 메일을 사용하면 계정명.pst 파일이 생성된다. 이 파일은 pst형식의 파일을 확인할 수 있는 Encase 같은 도구로 보면 데이터를 손쉽게 확인할 수 있다. 연락처 데이터 동기화와 캘린더 데이터 동기화를 사용하면 main.db 파일에 데이터가 저장된다. 이 파일에는 동기화된 데이터가 존재했던 기기의 특징이 남기 때문에 어떤 기기에서 동기화 되었는지 알 수 있다. 〔그림 4〕는 연락처 데이터 동기화시 생성되는 파일의 PRODID 항목에 기기의 특징이 남는 것을 보여준다. Web을 이용해서 동기화된 데이터는 'iCloud Web Address Book', iOS를 사용하는 기기에서 동기화된 데이터는 'iOS 버전명', Outlook에서 동기화된 데이터는 'Apple WebDAV Outlook Store'가 PRODID에 저장된다. 책갈피 데이터를 동기화하면 '즐겨찾기'에 동기화가 된다. 이 후, 'BookmarksMenu' 폴더가 생성되고 이 폴더 안에는 MAC 시스템과 iOS 기기의 '책갈피메뉴'의 URL이 저장된다. 이를 제외한 다른 내용은 변경 없이 같은 이름으로 동기화된다. 또한 '즐겨찾기'에 위치한 모든 하위 폴더에는 Apple.plist 파일이 생성되고 이 파일에는 어떤 계정의 iCloud에서 동기화된 것인지 알 수 있는 serverID 항목이 존재한다.

Google의 실시간 동기화 서비스 중, 메일과 캘린더를 Windows 시스템에서 사용하려면 Outlook을 이용하면 된다. Outlook에서 메일과 캘린더 동기화를 설정하면 자동으로 데이터가 동기화 된다. 이 서비스를 사용하면 iCloud와 같이 계정명.pst 파일이 생성되고 이 파일을 확인할 수 있는 도구로 확인하면 된다. 구글 드라이브를 사용하기 위해서는 설치 파일을 받아서 실행한다. 설치가 완료되면 'Google 드라이브' 폴더가 생성된다. 구글 드라이브에 있던 파일이나 폴더는 이 폴더에 다운로드 되고 이 폴더에 파일을 넣으면 자동으로 업로드 된다. 그렇기 때문에 이 폴더에서 자동으로 데이터 동기화가 일어난다. 드라이브는 SQLite형식의 sync_config.db 파일에 사용자 메일 주소, 최상위(root) 경로 등의 정보를 저장한다.

Windows 시스템에서는 N Drive, Daum Cloud, U Cloud, U+ Box 서비스를 사용할 수 있다. N Drive 서비스를 설치하면 사용자의 계정명으로 폴더가 생성되고 자동 로그인을 설정하면 레지스트리에 2개의 키가 생성된다. 이를 이용하여 용의자의 시스템이 N Drive에 자동 로그인 된다는 것을 알 수 있고 동기화 데이터를 획득할 수 있다. Daum Cloud를 사용하면 daumcloud.sqlite 파일이 생성되고 이 파일에 ID, 업로드 된 파일 이름, 파일 경로가 존재한다. 또한 log_버전_날짜.txt 파일이 생성되며 이 파일에는 접속한 시간, 동기화 시작과 종료시간, 업로드한 파일 이름, 삭제한 파일 이름이 저장된다. U Cloud 서비스는 ID를 찾을 수는 없지만 index_fs_dn_parent.db에 존재하는 파일들의 경로가 저장되어 있다. 또한 sc1.log 파일을 이용해서 로그인 성공과 실패 여부, 동기화한 파일의 경로와 파일 이름 등의 시간 순서를 알 수 있다. U+ Box 서비스를 설치하면 레지스트리에 사용자의 계정 정보가 남는다.

5.2 Mac System

Mac 시스템에서는 iCloud, Google 동기화 서비스인 메일, 캘린더, 드라이브, U+ Box를 제외한 기타 3가지 동기화 서비스의 이용이 가능하다. 조사에 사용된 Mac 시스템은 OS X 10.8 이다.

iCloud는 Mac 시스템에서 기본으로 제공하며 이 서비스를 사용하여 메일, 연락처, 캘린더, 책갈피를 동기화 할 수 있다. iCloud 동기화를 사용하면 Windows 시스템과 같이 MobileMeAccounts.plist 파일이 생성되고 이 파일에는 사용자의 ID 정보, 사용자의 이름, iCloud를 이용해 동기화한 각 서비스에 관련된 정보가 저장되어 있다. 사용자가 메일과 메모를 동기화하면 INBOX.mbox와 Notes.mbox 등 서비스와 관련된 폴더가 생성되고 각 서비스의 데이터가 emlx 형태의 파일로 저장된다. 연락처를 동기화하면 Configuration.plist 파일이 생성된다. 이 생성 파일의 name 키를 이용해서 iCloud의 사용 여부를 알 수 있고, me-card나 url 관련 키를 이용해서 계정명을 알 수 있다. 캘린더는 각 데이터의 PRODID 키에 iCal의 버전이 남으므로 이것을 이용해서 설치된 버전과 다른 버전정보는 타 기기에서 작성되었음을 유추할 수 있다.

Mac 시스템에서 Google의 실시간 동기화 서비스를 사용하기 위해서는 설정과 파일의 설치가 필요하다. 하지만 메일과 캘린더의 경우는 계정명 등 수사에 유용한 흔적이 남지 않았다. Google 드라이브를 설치하면 〔그림 5〕와 같이 Mac 시스템의 Keychain에 ID와 암호화된 비밀번호가 남는다.

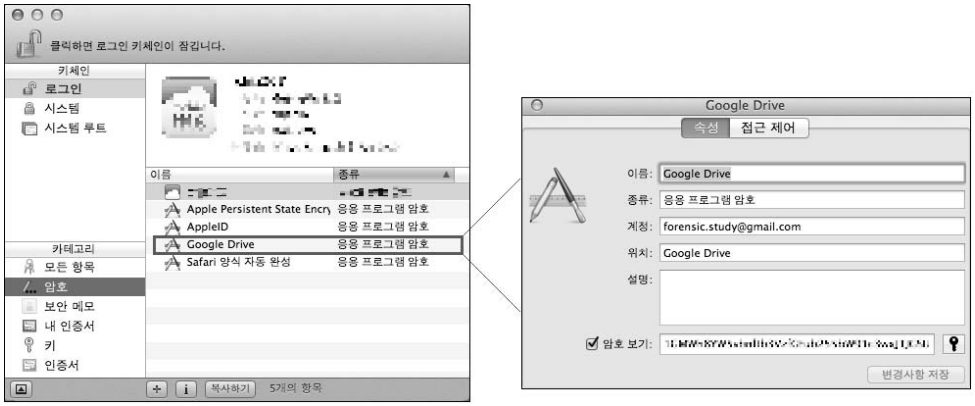
기타 저장소 서비스 중 Mac 시스템에서는 N Drive, Daum Cloud, U Cloud 서비스를 사용할 수 있다. 3가지 서비스들은 인터넷에서 다운받은 후 설치할 수 있다. N Drive를 설치하면 사용자의 계정명으로 폴더가 생성되기 때문에 사용자의 계정정보를 얻을 수 있으며 Keychain에도 계정정보가 남는다. Daum Cloud와 U Cloud는 daumcloud.sqlite 파일의 DISKUSER테이블의 DAUMID 키 값과 default_db.bdb 파일의 displayName 키 값에 각각 계정정보가 남는다.

5.3 Android 사용 기기

Android 사용 기기에서는 iCloud를 사용할 수 없다. 하지만 구글 동기화 서비스와 기타 4가지 동기화 서비스를 사용할 수 있다. 사용된 Android의 OS의 버전은 2.3.6 이다.

Android 기기에서 Google의 메일과 캘린더 실시간 동기화 서비스를 사용하기 위해서는 별도의 다운로드 없이 설정 후 손쉽게 이용가능하다. 메일을 동기화하면 mailstore.'accountID'.db파일이 생성되고 이 파일의 이름을 이용해서 계정정보를 얻을 수 있으며 이 계정에 동기화된 메일 데이터도 추출할 수 있다. 또한 gmail.db파일을 이용해서 conversation테이블의 user_name의 키 값으로도 계정정보를 얻을 수 있다. 캘린더는 업로드를 1회 이상하면 com.android.calendar_preferences.xml 파일의 default_sync_account키에 계정명이 남으며 데이터를 삭제해도 지워지지 않는다. Google 드라이브는 Market에서 다운받아서 설치한 후 사용한다. 설치 후 로그인하고 동기화하면 accountFlag+'ID'.xml 파일이 생성되므로 사용자의 계정명을 알 수 있다. 또한 DocList.db파일에 동기화된 데이터와 그 때 사용된 계정명이 표시되므로 이 파일을 이용해서 유용한 데이터를 얻을 수 있다.

이 기기에서는 N Drive, Daum Cloud, U Cloud, U+ Box 서비스를 Market에서 다운받아 사용할 수 있다. N Drive를 사용하면 ndrive.settings.



〔그림 5〕 Mac 시스템의 Key Chain에 남는 Google 드라이브의 흔적

xml 파일이 생성되고 이 파일에 사용자의 계정 정보가 존재한다. Daum Cloud 서비스를 설치하면 daum.android.cloud_preferences.xml이 생성되고 사용자의 계정 정보와 비밀번호 정보가 저장된다. 통신사에서 제공하는 U Cloud는 webview.db 파일과 uCloudVariable.xml 파일이 생성된다. 이 파일들에는 사용자의 계정명과 이름이 존재한다. 마지막으로 U+ Box 서비스는 lg_imory.db 파일이 생성되며 이 파일에는 사용자의 계정명과 비밀번호가 저장된다.

5.4 iOS 사용 기기

iOS를 사용하는 기기는 iCloud, Google 동기화 서비스, 기타 4가지 동기화 서비스 모두 사용이 가능하다. iOS 기기를 조사할 때에는 iOS 5.1.1 버전이 사용되었다.

iCloud 서비스는 iOS를 사용하는 기기에서는 기본으로 제공한다. 이 서비스에서는 메일, 연락처, 캘린더, 미리알림, 책갈피, 메모, 사진 등의 데이터를 동기화 할 수 있다. iOS 사용 기기에서는 컴퓨터 시스템 기기에서 존재하는 MobileMeAccounts.plist 파일은 존재하지 않지만 com.apple.accountsettings.plist 파일이 존재하고, 이 파일에는 사용자의 계정명이 남는다. 메일을 동기화하면 AutoFetchEnable 파일의 값이 〈false/〉에서 〈true/〉로 변경된다. 연락처, 캘린더, 북마크의 데이터를 동기화하면 AddressBook.sqlitedb, Calendar.sqlitedb, Bookmarks.db에 동기화된 데이터가 저장된다. 이 데이터에는 'ID'-contacts.icloud.com, 'ID'-caldav.icloud.com, 'ID'-bookmarks.icloud.com이 각각 남으므로 계정정보를 알 수 있다. 사진 데이터를 동기화하면 iOS 사용 기기는 이 데이터를 PhotoStreamData로 관리한다. 동기화를 시키면 동기화된 파일의 이름을 가진 여러 개의 파일이 생성되고 관련 파일은 바로 추출이 가능하다. 메모 데이터를 동기화 하면 notes.sqlite에 데이터가 저장된다. 이 파일의 데이터가 본 기기에서 생성된 데이터라면 계정정보가 남지 않지만 iCloud의 동기화로서 타 기기에서 생성된 데이터라면 계정 정보가 남는다.

이 기기에서는 Google의 서비스인 메일, 캘린더, 드라이브의 서비스를 사용할 수 있다. 메일을 동기화하면 유용한 데이터의 흔적이 남지 않는다. 캘린더의 경우는 Calendar.sqlite파일의 DefaultCalendarName 키에 계정명이 남으며 이 파일에서는 캘린더의 데이터 확인도 가능하다. Google 드라이브 서비스는 App store에서 다운로드 받아서 설치 후 사용할 수 있다. 이 서비스를 설치하면 '경로+ID.plist' 파일이 생성되며 이 파일의 이름을 이용해서 사용자의 계정명을 알 수 있다.

iOS 사용 기기는 N Drive, Daum Cloud, U Cloud, U+ Box 서비스를 사용할 수 있다. 이 서비스들을 App Store에서 다운로드 받은 후 설치하면 데이터 동기화를 실시간으로 제공한다. N Drive 서비스를 사용하면 NaverNDrive.plist 파일이 생성되고 사용자의 계정과 비밀번호의 길이가 저장된다. Daum Cloud 서비스는 DaumDisk.sqlite가 생성되며, 이 파일은 사용자의 계정정보와 이름을 포함하고 있다. U Cloud 서비스는 ucloud.plist 파일을 만든다. 이 파일에는 사용자의 계정, 비밀번호, 이름 정보를 포함하고 있으므로 U Cloud 서비스를 파악하는데 중요한 역할을 할 수 있다. 마지막으로 U+ Box 서비스는 uplusbox.plist 파일이 생성되고 사용자의 계정과 비밀번호 정보가 저장된다.

VI. 결 론

압수되는 기기나 데이터가 변경되지 않고 수집되는 것은 디지털 포렌식 조사에서 중요하다. 하지만 인터넷과 스마트 폰 보급의 증가로 사용이 늘어나고 있는 실시간 동기화 서비스는 데이터가 손쉽게 변경될 수 있다. 이 서비스는 파일이나 데이터를 업로드하고 등록된 기기에 실시간으로 동기화하기 때문이다. 그러므로 데이터의 변경이 일어나지 않도록 실시간 동기화 서비스의 특성을 고려한 데이터 수집 절차가 필요하고, 이 절차는 데이터의 변경 가능성을 줄이기 위해 신속하게 진행되어야 한다.

본 논문에서는 대표적인 실시간 동기화 서비스인 iCloud, Google 동기화 서비스, 기타 포털 또는 통신사의 동기화 서비스에 대해 4가지 시스템에서의 흔적을 조사했고, 네트워크 접속 차단과 저장소 접근 차단 같은 실시간 동기화 데이터 보존에 대한 방법을 연구했다. 또한 연구된 보존 방법과 조사된 흔적을 기반으로 데이터를 변경 없이 수집하고 분석할 수 있는 절차를 제안했다. 이 절차는 신속하게 진행되어야 하므로 국내와 국외의 영장 적용에 대한 협력이 가능해야 한다. 논문에서 제시한 절차를 사용하면 기기 또는 데이터가 압수된 후 용의자가 데이터를 변경하더라도 압수된 데이터가 변경되지 않을 것이다. 또한 분석된 흔적

을 이용해서 사용자의 계정정보나 다른 기기에 대한 정보 등의 데이터를 얻을 수 있고 이렇게 얻어진 데이터는 추가적인 수사와 방향에 큰 도움이 될 것이다.

모바일 장치가 발달함에 따라 컴퓨터 시스템과 모바일 장치의 차이가 줄어들고 있다. 그러므로 두 형태의 장치를 수사할 경우에 특성을 고려하는 경우가 줄어들 것이다. 또한 사용자의 요구에 따라 실시간 동기화 서비스의 종류와 형태가 다양하게 진화하고 있으므로 이 서비스에 대한 지속적인 조사와 분석이 필요하다.

참 고 문 헌

〔1〕 B. Carrier and E.H. Spafford, "Getting physical with the digital investigation process," International Journal of Digital Evidence, vol. 2, no. 2, Fall 2003.

〔2〕 M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," Network Security, vol. 2011, no. 3, pp. 4-10, Mar. 2011.

〔3〕 H. Chung, J. Park, and S. Lee, "Digital forensic investigation of cloud storage services," Digital Investigation, vol. 9, no. 2, pp. 81-95, Nov. 2012.

〔4〕 박기홍, 노시영, "클라우드 서비스에 대한 포렌식 측면의 수사 방법," 한국산업정보학회논문지, 17(1), pp. 39-46, 2012년 3월.

〔5〕 M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, "Digital evidence in cloud computing systems," Computer Law & Security Review, vol. 26, no. 3, pp. 304-308, May 2010.

〔6〕 J. Mishra, S.K. Dash, and S. Dash, "Mobile-cloud: A framework of cloud computing for mobile application," Advances in Computer Science and Information Technology. Computer Science and Information Technology, vol. 86, pp. 347-356, 2012.

〔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, Supplement, pp. S90-S98, Aug. 2012.

〔8〕 D. Barrett and G. Kipper, "Virtualization and forensics: A digital forensic investigator's guide to virtual environments," Syngress, 225 Wyman Street Waltham 02451 United States, pp. 197-209, 2010.

〔9〕 최지성, 전상준, 박정흠, 이상진, "디지털 포렌식 관점에서의 Mac OS X 사용흔적 분석," 한국정보처리학회 추계학술발표대회, 18(2), pp. 846-849, 2011년 6월.

〈著者紹介〉

이 지 희 (Jeehee Lee) 학생회원
2011년 2월: 연세대학교 컴퓨터공학과 학사
2011년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식, 클라우드 포렌식, 모바일 포렌식,

정 현 지 (Hyunji Chung) 정회원
2010년 2월: 고려대학교 컴퓨터정보공학, 산업시스템공학 공학사
2010년 3월~2012년 2월: 고려대학교 정보보호대학원 공학석사
2012년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 소셜 네트워크 포렌식, 클라우드 포렌식

이 상 진 (Sangjin Lee) 정회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수