

클라우드 서비스에 대한 포렌식 측면의 수사 방법[†]

(Cloud Services for the forensic aspects of the
investigative methods)

박기홍*, 노시영**

(Gi Hong Park and Si Young No)

요약 본 논문에서는 클라우드 시스템에 대한 포렌식 측면의 수사 방법을 제시한다. 스마트폰의 성장기에 접어들면서 다양한 어플리케이션들이 개발 되었고 그중 클라우드 시스템은 개인 정보 및 정보 자산의 공유 어플리케이션으로써 사건 발생시 사건에 대한 증거 자료 수집에 중요한 요소가 되는 반면 이에 대한 체계적인 수사 방법은 미흡하여 수사 과정 중 혼동을 줄 수 있다. 따라서 본 논문은 클라우드 시스템에 대한 포렌식 측면의 수사 절차를 제안하여 사건 현장에서의 체계적인 수사 지원 및 은닉 자료에 대한 증거 수집을 지원한다.

핵심주제어 : 모바일 포렌식, 클라우드 포렌식, 클라우드 서비스

Abstract In this paper, for the cloud system by explaining how the forensic aspects of the investigation. Smartphone Growth Entering a variety of applications were developed which cloud systems of personal information and information assets sharing applications as during incidents on the case evidence collection, an important factor, whereas such systematic investigative methods, born in the course of my investigation of the can be confusing. This paper on the forensic aspects of the cloud system by proposing a crime scene investigation procedures, investigative support, and aiding in the systematic collection of data to support evidence.

Key Words : Mobile forensics, Cloud forensic, Cloud Services

1. 클라우드 시스템 개념 및 정의

21세기 IT에서 최고의 키워드는 모바일이라 할 수 있다. 이는 단순 통신 및 텍스트 전송에 그치는 모바일 한계를 벗어나 스마트폰으로 진화함으로써 다양한 기능과 어플을 통해 사용자의 편의성 증대와 정보 공

유의 한계를 초월하는 것으로 사용자는 장소에 구애 되지 않는 IT 서비스를 이용할 수 있다. 이러한 IT 서비스 중에서 대표적인 것으로는 클라우드 서비스가 있으며 가트너사는 클라우드의 정의에 대하여 “인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅의 형태”라고 하였다. 이러한 클라우드 서비스는 초기에 부족한 IT 자원으로 관심을 못 받다가 최근 풍부해진 IT 자원 및 네트워크의 발전을 통해 이슈가 되고 있

[†] 이 논문은 2011년 군산대학교 대학자제 학술공모과제 연구비 지원에 의해 연구되었음.

* 군산대학교 컴퓨터정보공학과학과, 제1저자

** 군산대학교 컴퓨터정보공학과학과, 교신저자

다.[1,2] 클라우드 서비스는 애플의 휴대 기기간 동기화 서비스인 Mobile Me, 구글의 offiex 생산성 어플리케이션인 구글 Apps for your domain, 서비스나 어플리케이션 개발을 위한 API와 웹 기반 SW모듈을 제공하는 아마존 flexible payment API 등등 많은 기업이 서비스를 시작함으로써 사용자들이 서비스를 이용할 수 있게 되었다.[3,4] 국내에서는 KT에서 제공하는 Ucloud, 네이버에서 제공하는 n드라이브, 다음에서 제공하는 다음 클라우드 등이 서비스를 하고 있다. 클라우드 서비스의 사용자가 늘어남에 따라 클라우드 서비스에 대한 보안에 대한 연구가 필요하다. 하지만 기업 측면의 정보 자산의 보호 또는 클라우드 컴퓨팅의 보안 기술에 관한 연구가 중점으로 연구가 되고 있는 반면 포렌식 측면의 수사 방법에 관한 연구는 부족한 실정이다. 본 논문은 클라우드 서비스 수사 방법론을 목적으로 다양한 클라우드 어플들 중에서 KT사의 Ucloud, NHN사의 N드라이브, 다음사의 다음클라우드에 대한 클라우드 포렌식 수사 방법에 대하여 연구한다.

2. 관련 연구

2.1 클라우드 서비스 발전 배경

클라우드 서비스는 스마트폰 시장의 거침없는 성장을 가속화 시킬 수 있는 촉매제로서 부각되고 있다.[5, 6] 첫째 킬러 어플리케이션의 확대를 위한 기반으로 스마트폰이 성장기에 접어들면서 일반 사용자들은 휴대용 단말기에서도 간단한 게임뿐만 아니라 PC 수준 또는 그 이상의 기능이 구현되기를 점차 희망하게 된다. 이에 따라 이러한 요구에 부응 할 수 있는 킬러 어플리케이션이 필요하게 될 것이다. 킬러 어플리케이션이란 등장하자마자 다른 경쟁 제품을 몰아내고 시장을 완전히 재편할 정도로 인기를 누리는 상품이나 서비스를 정의하는데 킬러 어플리케이션의 경우 방대한 데이터베이스가 필요하거나 해당 DB에 대하여 지속적인 업데이트가 필요한 어플리케이션일 경우가 많다. 이러한 경우 스마트폰 디바이스 자체에 DB를 저장하는 것은 비효율적이며 이러한 비효율을 최소화시킬 수 있는 방안으로 클라우드 서비스가 주목받고

있다. 둘째로 어플리케이션 스토어의 한계를 극복하는 것으로써 어플리케이션의 개발자들은 스마트폰의 다양한 OS에 맞게 어플리케이션을 개발하여야 한다. 하지만 클라우드 기반으로 웹을 통해 어플리케이션을 개발하거나 가상화 기반으로 모바일 클라우드가 진행된다면 어플리케이션 개발자들은 OS에 구애 받지 않고 어플리케이션을 개발할 수 있으며 사용자 측면에서도 OS 종류와 관계없이 웹을 통해 어플리케이션을 이용할 수 있다. 셋째로 모바일 기기의 편의성 증대에 기여하는 것이다. 클라우드 서비스를 사용할 경우 대용량의 스토리지에 대한 부담을 줄일 수 있으며 클라우드 기반의 SaaS는 일반 S/W 대비 저 사양의 스펙을 요구하기 때문에 전반적으로 디바이스 자체의 크기를 소형화 시킬 수 있다.

2.2 클라우드 서비스의 장단점

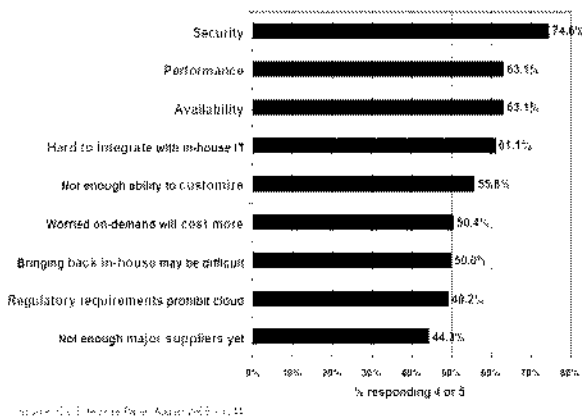
클라우드 서비스는 기업적인 측면에서 IT환경 구축 비용을 절감하는 효과를 가질 수 있는데 현재 기업에서 IT환경 구축을 하기 위해서는 서버, 소프트웨어 및 이를 관리할 담당자들을 투자해야 하며 증가하는 서비스를 예측하여 보다 많은 장비를 준비해야만 한다. 하지만 클라우드 서비스로 서비스를 대체하게 되면 기업에서는 보다 저렴한 비용으로 이러한 복잡한 문제를 해결할 수 있어 SW 개발이나 테스트 작업에 용이하게 이용할 수 있으며 시장 진입 시 비용을 절감할 수 있고 탄력적으로 시스템을 운영할 수 있는 장점이 있다.[7]

단점으로는 기업측면에서 취약한 보안을 해결해야 한다. 가상화 기반의 클라우드 서비스의 경우 기반 서비스는 모든 데이터가 서버에 집중되어 있기 때문에 더욱 큰 위험성을 내포하고 있다. 다음 그림1은 IDC에서 244명의 IT 관련 임원들에게 IT Cloud 서비스에 관하여 그들의 견해와 활용에 대하여 조사한 것으로 클라우드 서비스 도입에 보안이 얼마나 중요한 문제인가를 확인할 수 있다.

또한 클라우드 컴퓨팅 기반으로 모든 업무를 처리하는 기업의 경우 서비스 불가시 업무 마비를 일으킬 가능성이 있다. 그 예로 구글 앱스 서비스가 몇 시간 정도 장애를 일으키며 거의 사용할 수 없는 상태가

되기도 했고 아마존 또한 클라우드 서비스가 사용 불가능 상태에 빠지기도 하는 등의 사례가 있다.

Q: Rate the challenges/issues ascribed to the 'cloud/on-demand model' (ranked highest to lowest significant)



<그림 1> IT Cloud 서비스 해결 과제

개인적인 측면의 클라우드 서비스는 개인의 자료를 장소에 구분되지 않고 확인이 가능하며 동기화 기능으로 자료를 보다 편하게 작업 및 관리할 수 있어 작업 속도나 관리 측면에서 효율적인 반면 클라우드 디바이스의 분실 시 개인 자료의 유출 및 개인 계정 정보 유출로 인한 개인 정보 자산의 유출에 대한 준비가 필요하다.

2.3 클라우드 서비스의 종류

클라우드의 대표적인 서비스는 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service)가 가장 대표적인 서비스로 분류할 수 있다.[8]

SaaS는 클라우드 서비스 사업자가 인터넷을 통해 소프트웨어를 제공하고 사용자가 인터넷상에서 이에 원격 접속해 해당 소프트웨어를 활용하는 모델이다. 클라우드 컴퓨팅의 최상위 계층에 해당하는 것으로 다양한 애플리케이션을 다중 임대 방식을 통해 온디맨드 서비스 형태로 제공한다. 여기서 다중 임대 방식은 공급업체 인프라에서 구동되는 단일 소프트웨어 인스턴스를 여러 클라이언트 조직에 제공하는 것을 말한다. 즉 우리가 흔히 사용하는 이메일 관리 프로그램

이나 문서 관련 소프트웨어에서 기업의 핵심 어플리케이션인 전사적 자원 관리(ERP), 고객 관계 관리(CRM) 솔루션 등에 이르는 모든 소프트웨어를 클라우드 서비스를 통해 제공받는다. 그러나 SaaS는 클라우드 컴퓨팅이 IT 업계의 화두로 부상하기 이전에 독립적인 영역으로 이미 사용된 기술로 다른 서비스에 비해 인지도가 높다.

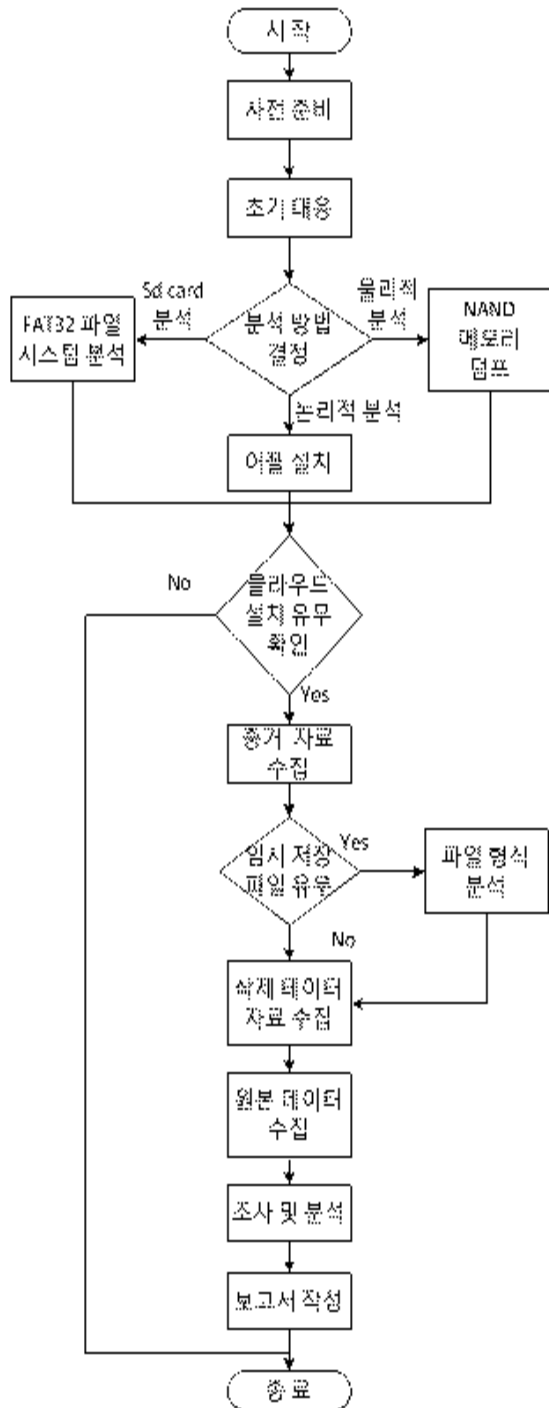
PaaS는 사용자가 소프트웨어를 개발할 수 있는 도구를 제공해 주는 서비스이다. 클라우드 서비스 사업자는 PaaS를 통해 서비스 구성 컴포넌트 및 호환성 제공 서비스를 지원한다. 컴파일 언어, 웹 프로그램, 제작 툴, 데이터베이스 인터페이스, 파이프라인, 사용자 관리 모듈 등을 포함한다. 응용 서비스 개발자들은 클라우드 서비스 사업자가 마련해 놓은 플랫폼 상에서 데이터베이스와 어플리케이션 서버, 파일 시스템과 관련한 솔루션 등 미들웨어까지 확장된 IT 자원을 활용하여 새로운 어플리케이션을 만들어 사용할 수 있다.

IaaS는 서버 인프라를 서비스로 제공하는 것으로 클라우드를 통하여 저장 장치 또는 컴퓨팅 능력을 인터넷을 통한 서비스 형태로 제공하는 서비스이다. 사용자에게 서버나 스토리지 같은 하드웨어 자체를 판매하는 것이 아니라 하드웨어가 지닌 컴퓨팅 능력만을 서비스하는 것이다. 클라우드 컴퓨팅 서비스의 대표적인 사례로 알려진 아마존 웹 서비스(AWS)의 스토리지 서비스 S3 및 EC2가 IaaS에 해당된다.

3. 클라우드 포렌식

모바일 포렌식의 수사 방식은 통화 목록 추출 및 텍스트 메시지 분석 위주의 분석을 하였지만 스마트폰 특히 클라우드 포렌식의 경우는 모바일 포렌식의 수사 방식과 다른 분석 방법이 필요하다. 클라우드 포렌식의 경우 어플리케이션의 분석이 중요하다. 각 어플리케이션은 특성에 따라 생성 또는 저장되는 데이터들의 분류가 다양하며 각 데이터의 형식에 따라 분석 방법이 다양하기 때문에 체계적이며 표준화된 분석 방법 연구가 필요한 실정이다. 클라우드 포렌식을 위한 절차는 다음 그림 2와 같다. 본 논문에서 제시하는 클라우드 포렌식 절차는 6단계로 구성하고 있으며

각 단계는 사전 준비, 초기 대응, 분석 방법 선택, 증거 자료 수집, 조사 및 분석, 보고서 작성으로 구성되어 있다.



<그림 2> 클라우드 포렌식 순서도

3.1 클라우드 포렌식의 초기 절차

클라우드 시스템은 스마트폰 또는 태블릿PC 등에 다양한 어플로 설치가 되고 각각의 어플은 저장방식 또는 구조가 다르므로 클라우드 포렌식을 수행하기 전에 디바이스를 비롯한 클라우드 시스템에 대한 이해와 교육이 필요하다. 또한 클라우드 포렌식 초기 대응은 매우 중요하다. 그 이유는 클라우드 시스템은 인터넷 저장 공간에 개인의 데이터를 저장 보관하고 스마트폰 디바이스를 통해 동기화를 이루는 시스템이다. 따라서 인터넷 저장 공간의 원본 데이터 삭제 또는 수정을 막기 위한 클라우드 시스템의 접속의 차단은 중요하다 할 수 있다.

3.2 클라우드 포렌식 분석 방법 결정

클라우드 시스템 내의 파일을 수집하기 위해서는 우선 상황에 맞는 분석 방법을 결정하여야 한다. 클라우드 포렌식은 sd card 분석, 논리적 분석, 물리적 분석, 칩 분리로 나누고 있다.[9,10]

sd card 분석 : 거의 모든 클라우드 디바이스는 외부 sd card 저장 공간을 지원한다. sd card는 FAT32 파일 시스템으로 포맷되어 있으며 표준적인 방법으로 분석하면 된다.

논리적 분석 : 안드로이드 어플리케이션을 이용한 방법으로 클라우드 디바이스 내에 포렌식 전용 어플리케이션을 설치하여 설치된 어플리케이션 리스트, 어플리케이션의 데이터 등 다양한 정보를 얻을 수 있다.

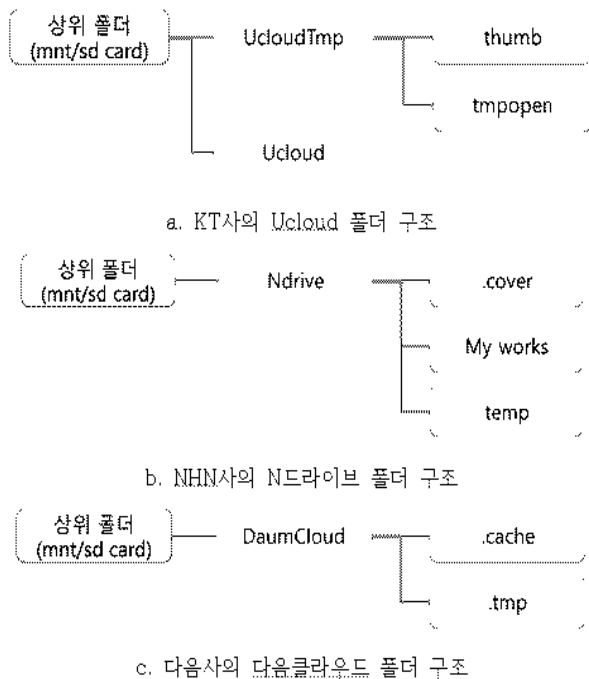
물리적 분석 : 더 자세한 분석이 필요할 경우 리눅스 dd 명령어를 통한 NAND 메모리의 덤프 이미지를 분석할 수 있으며 이 경우는 Root 권한이 필요하다. 이 방법은 다양한 사용자 데이터 파티션의 이미지를 획득할 수 있으며 이 파티션은 YAFFS2 파일 시스템을 사용한다.

칩 분리 : flash 메모리를 분리하여 flash 메모리 리더기를 통하여 정보를 얻어 분석하는 방법으로 포렌식 관점에서 가장 바람직하다고 할 수 있지만 모바일의 메모리에 종류에 따른 별도의 수집 장비를 제작해야 하며 기관에서 메모리를 분리하는 과정이 필요하므로 모바일 디바이스를 손상시킬 수 있다. 따라서

모바일 디바이스가 손상되어 정상 작동을 하지 않는 경우를 제외하고는 사용하기에 어려움이 있다.

3.3 증거 자료 수집

클라우드 디바이스에 대한 데이터 분석 방법이 결정되면 수집된 데이터를 분석하여 클라우드 어플리케이션의 설치 유무를 확인하여야 한다. 증거 자료에 대한 확장자 또는 파일 일반 정보를 안다면 디바이스 데이터 검색만으로도 증거 자료 수집이 용이하지만 클라우드 시스템의 경우 파일의 확장자 또는 파일 형식이 다양하고 또한 은닉된 파일에 대한 검색을 하기에는 어려움이 있다. 따라서 클라우드 포렌식의 경우 각 클라우드 시스템의 폴더에 대한 분석을 통하여 증거 자료를 습득하여야 한다. 클라우드 어플리케이션은 문서 또는 멀티미디어 데이터를 보관하는 보관 폴더와 미리 보기등을 통하여 임시 저장된 파일들을 보관하는 폴더를 가지고 있기 때문에 설치된 클라우드 어플리케이션의 종류에 따라 폴더에 대한 분석을 하여야 한다. 다음 그림3은 클라우드 어플리케이션의 폴더 구조를 나타내고 있다.



<그림 3> 클라우드 어플리케이션 폴더 구조

KT사의 Ucloud의 폴더의 경우 저장된 파일을 보관하는 Ucloud폴더와 임시 저장된 파일을 보관하는 UcloudTmp폴더가 존재한다. Ucloud의 데이터 저장 폴더의 경우 문서, 이미지, 음악, 동영상 파일을 디바이스에 저장 시 보관하는 폴더로써 디바이스에 문서 편집 또는 이미지 수정 어플 등을 통하여 자료의 수정이 가능함을 염두에 두고 분석을 하여야 한다. NHN사의 N드라이브는 파일을 My works 폴더에 저장하며 다음사의 다음클라우드는 DaumCloud 폴더에 저장한다. 클라우드 어플의 경우 파일을 디바이스로 저장하지 않더라도 임시 저장을 통해 웹에 있는 데이터를 확인할 수 있다. 따라서 디바이스내의 증거 자료를 찾기 위해서는 임시 저장 폴더를 확인하여야 한다. 임시 파일은 Ucloud는 은닉된 UcloudTmp폴더 내의 tmpopen 폴더에 저장되고 N드라이브는 temp폴더, 다음클라우드는 .cache 폴더에 저장되며 데이터가 삭제되더라도 임시 파일은 보존된다. 임시 저장되는 데이터 중에는 파일의 형식을 알기 어려운 데이터 또는 사용자의 고의로 은닉된 파일이 존재가능성이 있는데 이러한 경우 파일에 대한 hex 데이터를 분석하여 파일의 형식을 확인하여 증거 자료 수집 및 분석을 하면 된다. 다음 표 1(파일 hex 시그니처 값 비교 표)은 다양한 파일의 hex 시그니처를 나타내고 있다.

이미지 파일인 gif 파일의 경우 GIF87a에 대한 시그니처 47 49 46 38 37 61 또는 GIF89a에 대한 시그니처 47 49 46 38 39 61을 jpg는 JFIF에 해당하는 시그니처 FF D8 FF E0 xx xx 4A 46 49 46 00, png는 PNG에 해당하는 시그니처 89 50 4E 47 0D 0A 1A 0A, 디지털 사진 파일인 경우는 Exif에 해당하는 FF D8 FF E1 xx xx 45 78 69 66 00이 나오며 문서 파일인 PDF 파일의 경우 PDF에 해당하는 25 50 44 46, 오피스 파일의 경우 PK ZIP의 파일 시그니처인 50 4B 03 04가 나온다.

3.4 삭제된 데이터 분석 및 원본 데이터 수집

클라우드 포렌식을 수행하는데 디바이스 내의 정보 수집으로는 한계가 있다. 따라서 클라우드 디바이스 내의 정보 수집이 완료되면 웹 계정의 데이터를 수집하여야 한다. 클라우드 서비스 내의 데이터를 삭제하

이동전화 포렌식 가이드라인에서 제시한 수사 절차는 그림 4와 같으며 본 논문과의 비교는 표 2(포렌식 수사 절차 비교)와 같다.

클라우드 포렌식과 이동전화 포렌식의 절차에 대한

수 있는 절차가 될 것이다. 향후 연구 되어야 할 과제는 스마트폰 및 어플리케이션에 관한 보다 다양한 포렌식 연구로써 모바일 포렌식 분야의 매우 중요한 요소로 보다 많은 연구를 통해 사건 발생 시 체계화

<표 2> 포렌식 수사 절차 비교

단계	클라우드 포렌식 절차	모바일 포렌식 절차
1	사전 준비 - 클라우드 디바이스 이해 및 교육 - 클라우드 시스템 이해 및 교육	사전 준비 - 도구에 대한 준비 - 조사관에 대한 교육
2	초기 대응 - 클라우드 시스템의 접속 차단	초기 대응 - 사건 현장의 보존 및 기록
3	분석 방법 선택 - 물리적 분석 - 논리적 분석 - 메모리 분석	증거 수집 방법 선택 및 수집 - 물리적 분석 및 수집 - 논리적 분석 및 수집
4	증거 자료 수집 - 디바이스 내 데이터 수집 - 삭제/임시저장 된 데이터 수집 - 원본 데이터 수집	증거 수집 - 물리적 수집 - 논리적 수집
5	조사 및 분석 - 증거 자료 덤프 이미지 생성 - 무결성 확보를 위한 해쉬 값 생성	조사 및 분석 - 이동 전화 내 정보 분석 - 멀티미디어 정보 분석
6	보고서 작성 - 객관적인 보고서 작성	보고서 작성 - 객관적인 보고서 작성

비교를 통하여 클라우드 포렌식에 대한 효과를 분석하면 첫째 클라우드 환경에 맞는 증거 자료 수집 절차로 증거 수집 시 증거 자료의 무결성을 보장할 수 있고 둘째로 클라우드 시스템에 대한 수사 절차 체계화를 통하여 수사 과정에 혼선을 예비할 수 있다. 셋째로 클라우드 시스템에 맞는 증거 수집 절차로 다양한 파일과 은닉된 파일을 체계적으로 수집할 수 있다.

5. 결론

본 논문은 클라우드 포렌식의 수사 절차를 제시함으로써 클라우드 포렌식 분석 사건 발생 시 정형화된 절차가 없어 혼선을 빚었던 수사 절차에서 정형화된 수사 방법을 제공함으로써 기업의 정보 자산의 유출 시 증거 자료 확보 및 은닉 자료 검색 등 증거 수집의 향상과 분석된 증거 자료가 증거로써 가치를 가질

된 수사 방법을 제시되어야 할 것이다.

참 고 문 헌

- [1] Jin-Won Sung, Eun-Ju Back, Chang-Uk Park, Yeog Kim, and Sang-Jin Lee, "The Design and Implementation of the tool to analyze Mobile Data : Mobile Data Analyzer, Journal of Digital Forensics", Vol. 1, No. 1, pp. 63-77, Nov. 2007.
- [2] android Developer. <http://developer.android.com/guide/index.html>
- [3] 김성준, "클라우드 컴퓨팅환경에서의 기업정보보안 방안(정보보호관리체계(ISMS)를 중심으로)", 경영 컨설팅 리뷰, 제 1권, 제 2호, 2010.8 pp194-208
- [4] 나문성, 김승훈, 이재동, 클라우드 환경에서 대규모 콘텐츠를 위한 효율적인 자원처리 기법, 한국산업

- 정보학회 제 15권, 제 4호, 2010.12 pp17-27
- [5] 김학범, 전은정, 김성준, “클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구”, 경영컨설팅 리뷰, 제 2권, 제 1호, 2011.2, pp127-144
- [6] 윤용익, 김스베틀라나, “모바일 클라우드 컴퓨팅 기술 동향”, 정보통신 산업진흥원, 주간 기술동향 통권 1439호 2010.3.31.
- [7] 임철수, “클라우드 컴퓨팅 보안 기술”, 정보보호학회지 제 19권, 제 3호, 2009.6
- [8] 은성경, “클라우드 컴퓨팅 보안 기술 동향”, 정보보호학회지, 제 20권, 제 2호, 2010.4
- [9] An Introduction to Android Forensics, <http://www.dfinews.com/article/introduction-android-forensics?pid=974>
- [10] 김익수, 안영진, 이정현, 양승제, 김명호, “논리적 분석 기반의 안드로이드 스마트폰 포렌식 도구 구현” 한국 컴퓨터 정보학회 논문지, 제 16권, 제 4호, 2011.4
- [11] 이방협, “iPhone 디바이스 환경에서 효과적인 디지털 포렌식 분석”, 아주대학교 석사논문
- [12] 송유진, 이재용, 외장형 USB저장장치의 포렌식 조사방법, 한국산업정보학회, 제 4호, 2010.12 pp3

