Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1377

클라우드 아티팩트 자동 수집 및 분석 시스템*

김 민 규,† 정 두 원, 이 상 진‡
고려대학교 정보보호대학원

The Automatic Collection and Analysis System of Cloud Artifact*

Mingyu Kim,† Doowon Jeong, Sangjin Lee‡
Graduate School of Information Security, Korea University

요 약

클라우드 서비스 이용자의 증가로 클라우드 스토리지상에 개인이 생성한 중요한 파일이 다수 존재한다. 즉, 클라우드 사용 흔적은 주요 증거가 될 수 있기에 조사할 필요성이 있다. 클라우드 서비스를 조사하는 방법에는 스토리지 서버 공급자(CSP:Cloud Service Provider)를 이용하여 조사하는 방법과 클라이언트를 조사하는 방법이 있다. 이 중 본 논문에서는 클라이언트 컴퓨터를 조사할 수 있는 도구(Cloud Artifact)를 개발하였다. Cloud Artifact는 Google Drive, Dropbox, Evernote, N드라이브, Daum 클라우드, Ucloud, LG Cloud, T 클라우드, iCloud 9가지 클라우드 서비스 아티팩트를 수집 및 분석한다.

ABSTRACT

As the cloud services users' increase, there are important files created by individual in cloud storage. Thus, investigation of cloud artifact should be conducted. There are two methods of analyzing cloud service, one is that investigates cloud server provider (CSP), and another is that investigates client. In this paper, we presents an automated framework to detect the altered artifact and developes a tool that detects the cloud artifact. We also developed Cloud Artifact Tool that can investigate client computer. Cloud Artifact Tool provides feature of collection and analysis for the services such as Google Drive, Dropbox, Evernote, NDrive, DaumCloud, Ucloud, LG Cloud, T Cloud and iCloud.

Keywords : Cloud Forensics, Cloud Service, Digital Forensics, Cloud Artifact

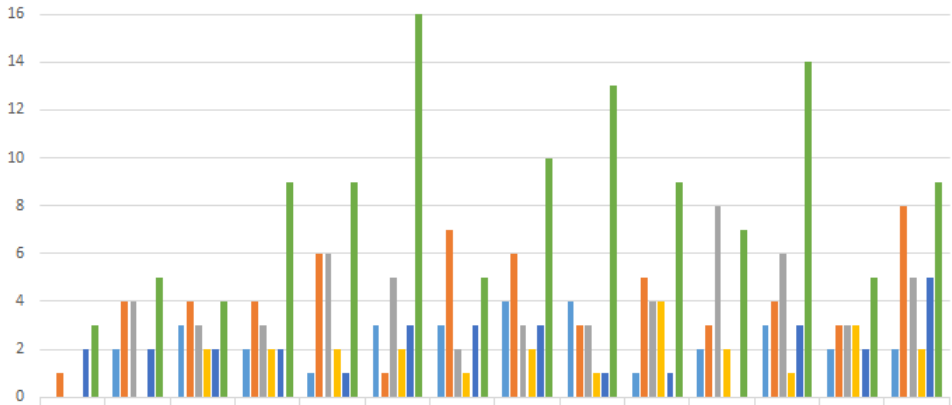
I. 서 론

클라우드 서비스가 활성화 됨에 따라 개인들이 생성한 디지털 데이터가 클라우드 스토리지에 많이 저장되고 있다. 범죄 증거 역시 클라우드 스토리지에 저장될 가능성이 크며, 동기화 서비스의 등장으로 다른 기기를 통해 원격 삭제가 가능하다[1].

따라서 범죄 조사 시에는 디지털 기기에 저장되어 있는 데이터뿐만 아니라 클라우드 서비스를 사용했는지도 신속히 파악해야 한다. 클라우드 스토리지 서비스가 다양한 스마트 기기(PC, 스마트폰, 태블릿 등)로 접근할 수 있기 때문에, 클라우드 시그니처(아티팩트)를 통해 현장에 있는 모든 기기를 조사하여 서비스를 이용했는지 확인해야 한다고 한다[2]. 하지만, 다양한 장치에 존재하는 클라우드 아티팩트를 확인하여도 업데이트가 빈번하게 발생되어 아티팩트가 바뀔 수 있다. 때문에 업데이트가 있을 때마다 아티팩트가 변경되었는지 확인해야 한다.

본 논문에서는 변경된 아티팩트를 탐지하는 업데이트 자동화 탐지 시스템을 제시하고, 클라우드 아티

Received(07. 03. 2015), Modified(09. 22. 2015), Accepted(10. 21. 2015)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단-공공복지안전사업의 지원을 받아 수행된 연구임(2012M3A2A1051106)
† 주저자, douxstar@korea.ac.kr
‡ 교신저자, sangjjn@korea.ac.kr(Corresponding author)



	2012년 1분기	2012년 2분기	2012년 3분기	2012년 4분기	2013년 1분기	2013년 2분기	2013년 3분기	2013년 4분기	2014년 1분기	2014년 2분기	2014년 3분기	2014년 4분기	2015년 1분기	2015년 2분기
GoogleDrive(Android)	0	2	3	2	1	3	3	4	4	1	2	3	2	2
Evernote(Android)	1	4	4	4	6	1	7	6	3	5	3	4	3	8
Dropbox(Android)	0	4	3	3	6	5	2	3	3	4	8	6	3	5
GoogleDrive(PC)	0	0	2	2	2	2	1	2	1	4	2	1	3	2
Evernote(PC)	2	2	2	2	1	3	3	3	1	1	0	3	2	5
Dropbox(PC)	3	5	4	9	9	16	5	10	13	9	7	14	5	9

Fig. 1. Cloud Services Update present condition

팩트를 자동으로 수집하고 분석하는 도구를 제안한다. 2장에서는 클라우드 서비스 업데이트 자동화 탐지 체계를 제시하고, 3장에서는 클라우드 아티팩트 수집 및 분석 시스템에 대해 설명한다. 마지막으로 4장에서는 결론을 기술한다. 업데이트 자동화 탐지 시스템을 통해 주기적으로 변경된 아티팩트를 확인할 수 있으며, 자동 수집 및 분석 도구를 통해서 빠르게 클라우드 서비스 사용여부를 판별할 수 있을 것이다.

II. 클라우드 서비스 업데이트 자동화 탐지 체계

2.1 클라우드 서비스 업데이트 현황

클라우드 서비스는 자주 업데이트 되거나, 새로운 서비스가 등장하기도 한다. 만약, 인지도가 하락할 경우 서비스는 종료되어 더 이상 서비스를 제공하지 않을 수도 있다. 스마트폰 앱은 iOS의 경우, 1년 동안에 평균적으로 GoogleDrive는 11번, Evernote는 17번, Dropbox는 16번 업데이트 되었다[3]. Windows 클라이언트 프로그램은 Dropbox 의 경우 1년에 약 30회 이상 업데이트가 되었다. Fig. 1은 2012년 1분기부터 2015년 2분기까지 분기별로 업데이트 횟수를 나타내는데, 조사 기간 동안 업데이트는 평균 2~3주에 한 번씩 업데이트가 발생했다. 따라서 자주 업데이트가 발생되기 때문에 포렌식 절차를 위해서는 일정 주기마다 업데이트를 확인해주는 자동화된 시스템이 필요하다[4].

2.2 업데이트 자동화 탐지 체계

클라우드 서비스의 업데이트 자동화 탐지 프레임워크는 다음 Fig. 2.과 같이 작동된다. 먼저, 클라우드 서비스의 설치프로그램을 다운받은 뒤, 해시 값을 이용하거나 설치파일의 버전을 확인하여 업데이트가 있었는지 확인한다. 업데이트 확인은 앞에 업데이트 현황에서 나온 결과처럼 2~3주에 한번씩(15일) 업데이트를 확인한다. 예를 들어 9가지 프로그램 중, Google Drive, Evernote, Dropbox, Daum 클라우드의 경우 클라이언트 프로그램을 해당 URL에 접속하여 다운받는 뒤, 다운받은 파일의 해시 값을 이전버전의 설치파일 해시 값과 비교하여 업데이트가 있는지 확인한다[5][6][7][8][9]. N드라이브의 경우, 버전 정보를 다운로드 페이지에서 확인할 수 있다[10].

만약 업데이트가 있는 경우 VM Image에 설치하고 이전 버전의 VM Image와 비교한 뒤, 만약 변경사항(데이터베이스 스키마, 데이터 경로 등)이 있다면 보고서를 생성하여 관리자에게 전송한다. 관리

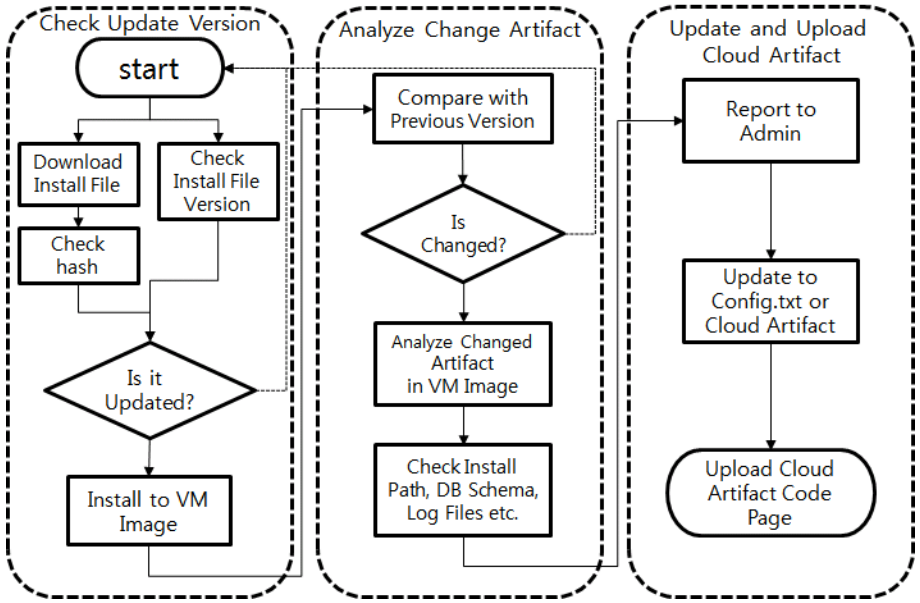


Fig. 2. Cloud Services Update Checking Procedure

자는 보고서를 보고 변경된 아티팩트에 맞게 Cloud Artifact 도구를 업데이트한다. 업데이트한 도구는 github 페이지에 업로드 한다[11].

III. 클라우드 아티팩트 수집 및 분석 시스템

이번 장에서는 클라우드 아티팩트 자동 수집 및 분석 도구에 대해서 이번 장에서 다룬다.

해당 도구는 Windows XP 뿐만 아니라 Vista 이상 환경(Windows 7, 8, 8.1)에서도 구동 가능하다. 수집 및 분석 가능한 서비스는 Google Drive, Dropbox, Evernote, N드라이브, Daum 클라우드, Ucloud, LG Cloud, T 클라우드, iCloud 총 9개다.

본 논문에서는 클라우드 아티팩트 자동 수집 및 분석 시스템을 제안한다. 해당 시스템의 특징은 소스코드 수정을 간소화하기 위해 Config.txt 파일을 이용하였다. 그리고 클라우드 아티팩트에 대한 표준 스키마를 제시하고 서비스별로 각기 다른 시간정보를 확인하였다.

3.1 클라우드 아티팩트 변화

과거 클라우드 아티팩트와 최신 클라우드 아티팩트를 비교해보았다[2]. Windows의 변경된 아티팩트 확인 결과, Appendix 1과 같이 데이터베이스 스키마나 로그파일 그리고 폴더경로가 변경된 것을 확인하였다. 이와 같이 업데이트를 통해 기존 아티팩트가 데이터의 위치가 변경된다거나 데이터가 없어지고 새로운 데이터가 다른 형태로 쌓일 수 있으므로 주기적인 확인이 필요하다.

3.2 Config.txt File

Config.txt는 소스코드 수정을 간소화하기 위한 설정파일이며, 클라우드 아티팩트에 관한 경로 및 Web History 정보를 포함하고 있다.

Config.txt파일의 내부구조는 다음과 같이 구성되어있다.

@[Service Name]
#LocalFilePath(install Path)
##xp
%UserProfile%/LocalSettings/Application Data/[Service Folder]
##etc(Vista over)
%UserProfile%/AppData/Local/[Service Folder]
#Localfiles
[Database files, log files etc.]
#URL

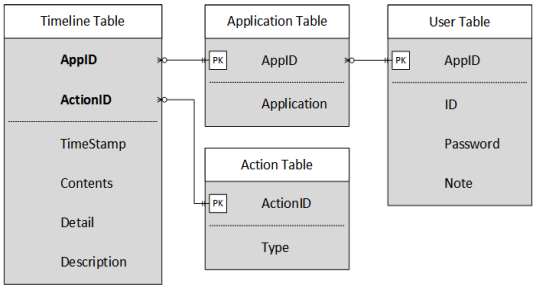


Fig. 3. Database Schema Structure

〔web histories〕, 〔action〕

'@'뒤에 서비스명을 넣고, LocalFilePath에는 해당 서비스가 설치된 경로를 xp와 vista이후 버전으로 나누어 넣는다. Localfiles에는 로그파일이나 db파일명이 있다. URL에는 해당 서비스의 인터넷 접속 기록 목록이 있다.

변경된 아티팩트에 대해 위와 같은 구조로 되어있는 파일을 업데이트함으로써, 소스코드의 수정 없이 즉각적으로 적용 가능할 수 있다.

예를 들어, 아티팩트가 변경되는 경우는 여러 가지 있다. 이 중 아티팩트가 존재하는 경로가 변경되는 경우, 해당 Config.txt파일을 이용하여 소스코드를 다시 컴파일 할 필요 없이 변경된 경로에 대해서만 바꾸어 주면 된다.

3.3 데이터베이스 스키마

클라우드 아티팩트 도구를 통해 데이터가 수집 및 분석되면, 결과가 Fig. 3.과 같이 구성된 데이터베이스 스키마에 저장된다.

데이터베이스는 Timeline, Application, User Action 테이블로 구성되어 있다. Application 테이블에는 사용자가 이용한 클라우드와 해당 서비스별로 고유 ID가 입력된다. Action 테이블은 사용자가 서비스를 이용하면서 행한 행위(예: 웹 서비스 이용, 웹 문서 보기, 로그 파일 등)별로 고유 ID가 입력된다. User 테이블에는 Applica tion 테이블에서 지정된 AppID와 해당 서비스의 사용자 계정정보가 저장된다. Timeline 테이블에는 아티팩트(서비스를 사용한 행위, 시간, URL, 내용, 상세 설명)가 시간순에 따라 저장되어 있다.

Timeline 테이블 구조는 Fig. 4.와 같다. 이를 활용하면 수사관이 분석 시, 타임라인을 통해 데이터의 사용 흐름을 빨리 파악할 수 있다. 타임라인 테이블은 로컬 컴퓨터에 설정된 UTC 시간을 기준으로 적용하였다.

3.4 각 서비스별 시간 포맷

각 클라우드 서비스마다 데이터베이스에 저장하는 시간 표현 방식은 다양하다〔12〕. 서비스별로 저장되는 시간정보는 다음 Table 1.과 같다.

Evernote의 경우, 0000년 1월 1일 00:00:00을 기준으로 1초마다 시간 값 0.000011574가 증가한다. N드라이브의 경우에는 현지 시간대가 적용된 local 시간(yyyy,mm,dd, hh:mm:ss)으로 저장한다. 이처럼 서비스별로 다양하게 저장된 시간 정보는 클라우드 아티팩트 도구를 통해 일반화하여 분석할 수 있고, 공통된 시간대(조사자의 로컬 시간대)로 데이터베이스에 저장된다.

AppID	ActionID	TimeStamp △	Contents	Detail	Description
Click here to define a filter					
4	3	2015-07-02 10:25:47	https://www.dropbox.com/release_notes		Dropbox 방문
4	3	2015-08-29 15:03:28	https://www.dropbox.com/s/nd6h6ay0z4u6u0o/pycrypto-2.6.1.win32-py2.7.exe?dl=0		Dropbox 방문
2	4	2015-08-31 09:45:52	http://cc.naver.com/cc?a=map.naverservice&r=&i=ndrive&bw=1903&px=832&py=324&sx=832&sy=324&m=1&nsc=navertop.v3&u=http://ndrive.naver.com/		ndrive 서비스이용
2	4	2015-08-31 09:45:52	http://ndrive.naver.com/#view=login		ndrive 서비스이용
2	4	2015-08-31 09:46:02	http://ndrive.naver.com/#mode=photo&type=whole&main		ndrive 서비스이용
2	4	2015-08-31 09:46:03	http://ndrive.naver.com/#photo/upload		ndrive 서비스이용
5	5	2015-09-09 18:02:20	https://docs.google.com/document/d/1M_t7eS0o0oE-q88znx4XDWULA1ZywU6_upUeYXsNMQo/edit?usp=drive_web		GoogleDrive_문서
5	5	2015-09-09 18:02:21	https://docs.google.com/document/d/1M_t7eS0o0oE-q88znx4XDWULA1ZywU6_upUeYXsNMQo/edit		GoogleDrive_문서

Fig. 4. Timeline Table

Table 1. Application's Time Expressions

Application	Time Format
Google Drive	Unix Time : Second Since 1 January,1970 00:00:00 (UTC)
Dropbox	X(Database Non-Exist)
Evernote	EvernoteTime ex) 735369.514166667 Since 1 January, 0000 00:00:00(UTC)
Daum 클라우드	yyyy-mm-dd hh:mm:ss.000 (UTC+9)
N드라이브	yyyy-mm-dd hh:mm:ss.000
Ucloud	yyyy-mm-dd hh:mm:ss.000
LG Cloud	Unix Time Since 1 January,1970 00:00:00 (UTC)
T 클라우드	X(Database Non-Exist)
iCloud	MAC: Absolute Time

3.5 도구 동작 구조

클라우드 아티팩트 탐지 도구의 시스템 구조는 Fig. 5.와 같다. 도구는 분석대상 기기에서 사용된 클라우드 서비스들을 분석할 수 있도록 아티팩트를 정규화하여 보여주는 것이 주목적이다.

먼저, 조사하고자하는 컴퓨터에서 Config.txt 파일을 통해 클라우드 서비스별 관련 파일들이 추출된다. 레지스트리 파일, 웹 브라우저 관련 파일(IE, Chrome, Safari, FireFox, Opera의 히스토리), 로그 파일 등이 추출되면, 분석 모듈이 분석할 정보를 표준화된 데이터베이스에 저장한다. 마지막으로, 통합 데이터베이스를 이용하여 조사자는 증거를 분석한다. 통합 데이터베이스에서 확인할 수 있는 내용은 클라우드 사용흔적, URL 행위 분석, 아이디, 로그 파일, 클라우드 서비스 이용 타임라인이다.

IV. 결 론

클라우드 포렌식 절차에 대한 많은 연구가 진행되었지만, 관련 도구가 없어 일선 수사관들이 이러한 연구를 활용하기에 많은 어려움이 있었다. 클라우드 서비스의 경우, 현장에서 웹 클라우드 접속기록과 설치된 클라우드 프로그램 사용 흔적을 직접 확인해야하므로 시간이 많이 소요되어 자동화된 도구가 필요하다. 본 논문에서는 이러한 문제점을 해결하기 위해 클라우드 아티팩트 자동 수집 분석 도구(Cloud Artifact)를 개발하였다[11]. 이 도구는 서비스 프로그램의 빈번한 업데이트로 인해 지속적인 관리가 필요하다. 이는 본 논문에서 제시한 클라우드 서비스 업데이트 자동화 탐지 시스템을 통해 해결할 수 있다.

향후에는 Windows 뿐만 아니라 다양한 운영체제(Mac, iOS, Android)도 클라우드 아티팩트를 분석할 수 있도록 연구하고 모듈을 업데이트 할 것이다. 또한 앞에서 제시한 클라우드 서비스 업데이트 자동화 탐지 프레임 워크도 구현할 예정이다.

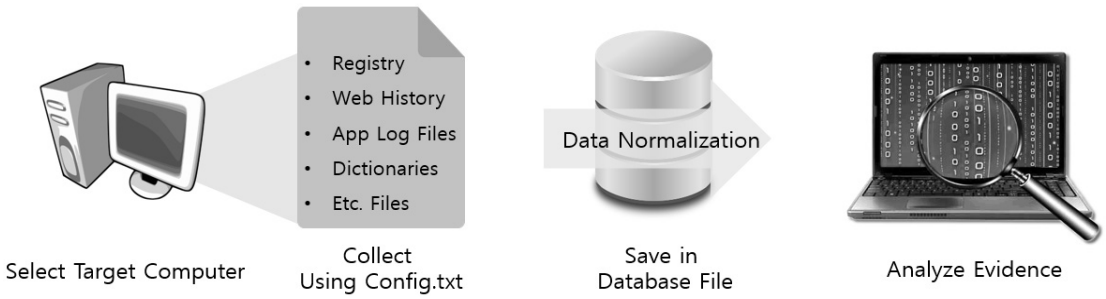


Fig. 5. Cloud Artifact System Structure.

Appendix 1. Changed Artifacts of Cloud Service(Windows)

Application	Path	File Name	Detail of Changed Artifact
Google Drive	%UserProfile%\AppData\Local\Google\Drive\user_default	sync_config.db	- Account ID
		snapshot.db	- filename - Modification Time - Create Time - File Size
		sync_log.log	- Log information
Evernote	%UserProfile%\AppData\Local\Evernote\Evernote	~\Databases\	- Changed Nothing
		~\Logs\	- Changed Nothing
Dropbox	%UserProfile%\AppData\Roaming\Dropbox\instance1	~\instance1\config.db	- Default Folder Changed - Change to dbx file(Encrypt)
		aggregation.dbx	- Recent Work list
N드라이브	%UserProfile%\AppData\Local\Naver\NaverNDrive\[UserID] %UserProfile%\AppData\Local\Naver\NaverNDrive\Temp	NDNetIOLog.db	- Upload, Download, Deleted etc. action info
		[yyyymmdd].log	- Login, Logout info
Daum 클라우드	%UserProfile%\AppData\Local\Daum\DaumCloud	daumcloud.sqlite	- Changed Nothing
		log_[version]_date.txt	- Action Log

References

〔1〕 NIST Cloud Computing Forensic Science Working Group, NIST Cloud Computing Forensic Science Challenges, http://csrc.nist.gov/publications/drafts/nistir-8006/draft nistir 8006.pdf

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

〔3〕 Application Update History Checking Site, https://www.appannie.com/

〔4〕 Hyounghwan Kim, Dohyun Kim, Jungheum Park and Sangjin Lee, "The Automatic Extraction System of Application Update Information in Android Smart Device," Journal of The Korea Institute of information Security & Cryptology, 24(2), pp. 345-352, Apr. 2014

〔5〕 Dropbox release note information, https://www.dropbox.com/release_notes

〔6〕 GoogleDrive Application Download, https://tools.google.com/dlpage/drive/thankyou.html

〔7〕 Evernote Application Download, https://evernote.com/intl/ko/download

〔8〕 Dropbox Application Download, https://www.dropbox.com/downloading?os=win

〔9〕 DaumCloud Application Download, http://get.daum.net/cloud/DaumCloudSetup.exe

〔10〕 NDrive Application Download, http://software.naver.com/software/summary.nhn?softwareI d=MFS_105031

〔11〕 CloudArtifact Tool page, https://github.com/CloudForensics/CloudArtifact

〔12〕 J. Oh, S. Lee and S. Lee, "Advanced evidence collection and analysis of web browser activity," Digital Investigation, vol. 8, pp. 62-70, Aug. 2011.

〈저자소개〉

김 민 규 (Mingyu Kim) 학생회원
2014년 2월: 한세대학교 정보통신 공학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 디지털 포렌식, 사이버 범죄 수사

정 두 원 (Doo-won Jeong) 학생회원
2011년 8월: 고려대학교 공과대학 산업경영공학과 공학사
2011년 9월~현재: 고려대학교 정보보호대학원 정보보호학과 석·박사통합과정
〈관심분야〉 디지털 포렌식, 데이터 마이닝, 이미지 포렌식

이 상 진 (Sang-jin Lee) 종신회원
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