디지털 컴퓨팅 환경의 디지털 증거화를 위한 침해 데이터 보증 메커니즘

An Assurance Mechanism of Intrusion Data for Making Digital Evidence in Digital Computing Environment

장 은 겸*
Eun-Gyeom Jang

요 약

디지털 컴퓨팅 환경에서 가질 수 있는 기기의 오류에 의해 오작동과 악의적인 침해가 발생할 수 있다. 이러한 침해행위는 개인의 사생활을 위협하는 치명적인 요소로 작용한다. 이러한 침해행위에 대한 법적 대응을 위해 침해증거 확보 기술과 관리 기술을 세계적으로 연구하고 있다. 침해행위에 대한 증거확보기술은 사건발생 시점을 기준으로 증거 대상시스템을 압수하여 법정에서 증거자료로 활용한다. 그러나 수집된 증거물은 증거물 수집, 증거물 분석, 법정의 영역에서 변조 및 손상에 위험성을 가질 수 있다. 즉, 증거물의 무결성과 대상시스템에서 수집된 증거물이 맞는지에 대한 신뢰성에 문제점을 갖는다.

본 논문에서는 디지털 컴퓨팅 환경에서 시스템의 오작동 및 침해증거를 보호하여 컴퓨터 포렌식스를 지원할 수 있도록, 디지털 증거물의 무결성 및 신뢰성 보증을 위한 기법을 제안한다. 제안한 기법으로는 피해시스템, 증거수집, 증거 관리, 법정(제3의 신뢰기관)의 각 개체간에 상호 인증을 통해 증거물을 관리하고 증거물이 법정에서 법적 효력을 발휘할 수 있도록 접근통제 보안 모델을 제안하여 안전한 증거물 관리 정책을 수립한다.

ABSTRACT

In digital computing environment, for the mal functions in appliances and system errors, the unaccepted intrusion should be occurred. The evidence collecting technology uses the system which was damaged by intruders and that system is used as evidence materials in the court of justice. However the collected evidences are easily modified and damaged in the gathering evidence process, the evidence analysis process and in the court. That's why we have to prove the evidence's integrity to be valuably used in the court. In this paper, we propose a mechanism for securing the reliability and the integrity of digital evidence that can properly support the Computer Forensics. The proposed mechanism shares and manages the digital evidence through mutual authenticating the damaged system, evidence collecting system, evidence managing system and the court(TTP: Trusted Third Party) and provides a secure access control model to establish the secure evidence management policy which assures that the collected evidence has the corresponded legal effect.

☞ KeyWords : Computer Forensics, integrity, Authentication, Security Model, 컴퓨터 포렌식스, 무결성, 인증, 보안 모델

1. 서 론

정보보호 사고에 의한 법적 판단은 정보유출을 비롯한 정보보안 사고 발생시의 상황을 그대로 재현할 수 있는 보안사고 원인 분석 기능을 갖추어, 모든 트래픽과 다른 시스템간의 연관성을 저장한 후 감식 기술로 분석하여 당시 상황을 그대로 재현할 수 있는 시나리오를 도출할 수 있는 기법을 필요로 한다[1,2].

현재 컴퓨터 포렌식스 도구는 EnCase와 TCT가 대표적이다. 대다수의 포렌식스 도구들[3,4]은 삭제된 파일을 복구할 수 있는 복구기능, 다양한 방식으로 문자열이나 파일을 검색할 수 있는 검색기능, NIST(National Institute of Standard and

* 정 회 원 : 대전대학교 컴퓨터공학과 겸임교수
(주)엠투엠코리아 연구소장
jangegu@nate.com
[2010/01/018 투고-2010/01/21 심사(2010/04/12 2차)-2010/06/11 심사완료]

Technology)와 NDIC(National Drug Intelligence Center)에서 배포한 NSRL(National Software Reference Library)과 HashKeeper Library를 이용한 파일 추출 기능, 파일의 Magic Number를 이용하여 속성이 변경된 파일을 검색하는 시그니쳐 분석기능, 효과적으로 보고서를 작성할 수 있도록 하는 레포팅 기능을 제공한다.

이러한 포렌식스 도구들을 활용하여 사이버 범죄에 이용된 시스템을 압수 수색하여 법적 대응 증거를 추출한다. 그러나 법정 증거 자료로 활용된 자료가 수사 대상시스템에서 수집된 증거인지에 대한 무결성 및 신뢰성에 문제점을 잠재적으로 가진다. 즉, 사이버 범죄 수사가 착수된 시점에서의 증거가 법정에서 제시한 증거가 같다는 것이 입증되어야 효력을 발휘할 수 있다. 이러한 증거물의 신뢰성을 보증하기 위한 기술이 필요하므로 본 논문에서는 디지털 컴퓨팅 환경에서 발생할 수 있는 범죄 행위에 대해, 오작동 및 침해행위의 근거자료를 법정에서 시스템 침해의 증거로 효력을 발휘할 수 있도록 증거자료의 신뢰성 문제를 보증하기 위한 메커니즘을 제안한다.

2. 컴퓨터 포렌식스 기술

2.1 컴퓨터 포렌식스 동향

컴퓨터 포렌식스를 위한 관련 연구기관은 대표적으로 미국 법무부, CFTT(Computer Forensics Tool Testing), HTCN(High-Tech Crime Network), CERIAS, ASCLD, IACIS를 들 수 있다.

미국 법무부는 전자 증거물에 대한 압수 수색 절차를 안내하는 가이드라인을 발행하고 CCIPS (Computer Crime and Property Section)를 개설하였다. 컴퓨터 범죄에 관련된 문서들을 비롯해 주요 인프라 보호 요령, 지적재산권 보호, 전자상거래의 법적 문제에 관한 세션들을 담고 있다. CFTT는 포렌식스 도구가 필수적으로 갖추어야할 기능에 대한 요구사항을 목록화하고 포렌식스 소프트웨어 도구를 평가할 수 있는 방법론을 제시하고 있다. HTCN는 컴퓨터 포렌식스에 관련된 교육 및 테스팅 기관 정보, 컨퍼런스, 세미나 등 교육정보, 컴퓨터 포렌식스 관련 도구 및 기술 자료들에 정보를 제공하고 있다. CERIAS는 기술적인 내용에 대한 연구뿐만 아니라, 교육, 법 분야, 언어 분야, 경제 분야 문제들에 대한 관계와 그 의존성에 대한 연구를 병행하고 있다. 그 외에 ASCLD는 연구시설이나 기관들이 컴퓨터 포렌식스를 수행함에 있어서 따라야 할 기준을 제정하고 Proficiency Testing 및 지속적인 교육과 트레이닝 활동을 규정해 놓고 있다. 그리고 IACIS에서는 컴퓨터 범죄 처리 절차를 만들어 컴퓨터를 압수하고 컴퓨터에서 전자적 증거물을 획득하는 방법을 확립했으며 교육과정을 설립해 포렌식스 전문가를 위한 지속적인 훈련을 진행하고 있다[5].

2.2 컴퓨터 포렌식스 도구 분석

2.2.1 EnCase

EnCase[6]는 많은 양의 컴퓨터 증거 관리를 GUI 기능을 제공하고, 미 연방 법원에서 EnCase를 통해 얻은 결과물을 법적인 증거로 채택한 판례로 더욱 성능을 인정받고 있는 도구이다.

EnCase의 주요 기능은 증거 자료의 다양한 파일 시스템 지원, 증거 자료의 무결성 보장, 유연한 이미지 추출 방법 제공, 파일의 정확한 Timeline 추적, 삭제된 파일과 폴더 및 비 할당 클러스터 영역 검색 및 복구, 레포팅이다.

- 다양한 파일 시스템 지원- 윈도우(NTFS, FAT 16/32), 리눅스(ext2), 유닉스(UFS), MacOS 파일 시스템 분석 가능
- 증거자료의 무결성 보장(Digital finger printing)- 증거 자료로서의 무결성을 보장하기 위해서 피해 시스템의 하드 디스크를 MD5 hash algorithm을 사용하여 digital finger printing(다양한 해쉬 알고리즘 지원)
- 유연한 이미지 추출 방법 제공- Fast Bloc을

이용한 bit 단위의 drive-to-drive 이미지 생성, Parallel Port를 이용한 이미지 전송, 활성화된 NIC을 통한 네트워크 전송 지원
- 사용자 정의 스크립트 작성을 통한 자동화 작업 가능

EScript를 이용하여 숨겨진 E-Mail, NT Security event log, Internet History 등을 검색하고, 일반 텍스트와 HTML 형식을 지원하는 레포팅 기능과 삭제된 파일과 비할당 클러스터 영역 검색 및 복구 기능을 제공한다.

2.2.2 TCT

TCT[7,8]은 침해 사고 발생 당시의 이벤트 수집 및 분석을 보다 정확하고 수월하게 수행하기 위한 기능을 제공한다. 피해 시스템의 상태 정보에 대한 snapshot을 생성하며, 백업된 디스크 이미지 분석 및 파일 복구에 유용하게 사용할 수 있다. TCT 구성 프로그램의 주요 기능은 다음과 같다.

- grave-robber: 피해 시스템의 휘발성 정보를 캡쳐한다. 네트워크 상태 정보, 주요 설정 파일, 일반 시스템 정보 등을 수집
- pcat: 메모리에 로그된 프로세스를 수집
- ils: 파일시스템의 inode 정보를 수집, 기본적으로 지워진 파일에 대한 inode 정보를 제공
- file: 복구된 파일의 file type를 출력
- unrm, iazarus: 파일시스템에서 할당되지 않은 디스크의 블록들을 분석하고 복구
- mactime: 파일의 접근, 수정시간을 조사하고 파일시스템에 대한 timeline 생성

그 외의 도구로 TCTUtil, Sleuth Kit, Autospy forensics Browser은 TCT 프로그램과 유사한 기능을 갖추고 있다. Sleuth Kit는 NTFS, FAT, FFS, EXT2FS, EXT3FS를 지원해 다양한 파일시스템을 분석할 수 있다. 또한 Autospy는 피해 시스템 분석을 진행하는데 있어서 작업을 용이하게 하기 위해 개발된 웹 브라우저 기반의 GUI 프로그램이다[3,4].

2.3 기존 컴퓨터 포렌식스 분석

일반적인 네트워크 환경에서 발생하는 공격 형태는 공격이 발생한 시점을 기준으로 피해 시스템, 가해 시스템, 경유 시스템으로 분류할 수 있으며, 법 과학 측면에서 컴퓨터 포렌식스 방법론은 수사착수, 증거식별, 증거수집, 증거보존, 전송 및 저장, 수사종결의 절차를 따른다. 기존 기술의 문제 및 요구사항은 다음과 같다.

- 디지털 증거의 수집·보관에 대한 신뢰성: 디지털 증거가 사고 발생시에 수집한 증거자료와 법정에 제출한 증거자료가 같다는 사실을 입증해야만 법적 효력을 받는다.
- 기존의 컴퓨터 포렌식스 분야의 기술은 법집행기관의 법 과학 실험실을 중심으로 수행: 전통적인 법과학적 컴퓨터 포렌식스는 대상 시스템을 압수하여 증거를 분석한다. 법 과학 실험실로 옮겨 온다는 것은 시스템 운영상 매우 어려운 실정이다.
- 포렌식스 절차의 표준화 중심의 연구: 지금까지 발표된 컴퓨터 포렌식 분야의 연구 결과는 주로 절차의 표준화와 세부적인 증거수집 방법론이 제시되어 왔을 뿐이고 디지털 증거의 본질적인 속성에 초점을 맞춘 과학적인 접근 방법에는 상대적으로 소홀히 하고 있다.

본 논문에서는 디지털 증거의 매체 독립적 속성과 법과학적 문제점을 컴퓨터 포렌식스 관련에서 분석하고 디지털 증거의 매체 독립적인 접근 방법에 적합한 법과학적 디지털 증거 보증 메커니즘을 제시하여 사이버범죄 수사절차와 침해 사고 대응과정에서 획득하는 디지털 증거에 대한 신뢰성을 향상시키고자 한다.

이러한 문제점을 해결하기 위해 신뢰된 DEC (Digital Evidence Collecting) 모델을 이용하여 디

지털 증거를 관리하여 디지털 증거의 수집·보관에 대한 신뢰성을 보장하고 증거를 확보했다는 전제를 기반으로 제안시스템은 운영된다. DEC의 전제하에 DEC와 TTP(Trusted Third Party), DEM (Digital Evidence Management)간의 인증 정책을 제안하여 증거물 수집 및 원본의 무결성을 보증하여 법 과학 실험실로 대상시스템을 압수 수색하는 어려움을 해결한다.

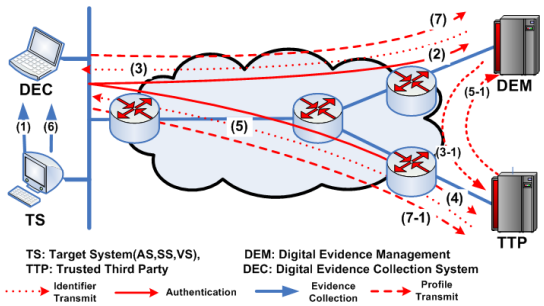
3. 디지털 증거물 보증 메커니즘

3.1 시스템 환경 및 구성

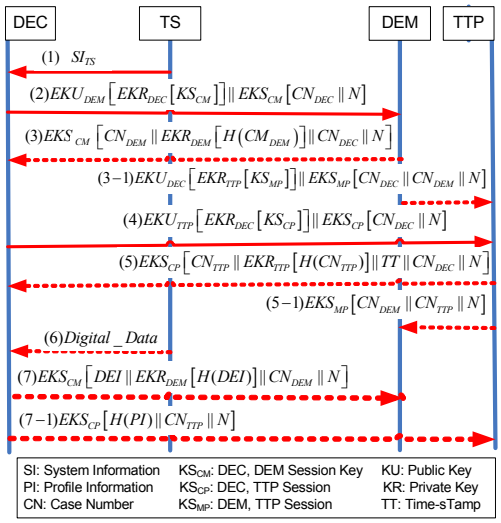
본 논문의 제안 메커니즘을 일반 네트워크 환경에 적용하기 위해서 DEM, DEC 및 TTP으로 구성한다.

DEM은 네트워크상에서 발생하는 보안 침해 사고의 감시 및 접수 기능을 수행하고, 보안 침해 사고가 발생되면 대상시스템(TS)에 DEC를 설치한다. TS에 설치된 DEC는 TS에 내포된 디지털 데이터를 분석하여 디지털 증거를 생성한다. 이때 생성되는 디지털 증거는 DEM 및 TTP에 식별자를 요청하고, 수신된 식별자를 이용하여 디지털 증거에 대한 프로파일을 생성한다. 생성된 프로파일 및 디지털 증거는 TTP와 DEM에 전송하여 보관한다. TTP 및 DEM의 식별자는 DEC에 의해 생성되는 디지털 증거의 무결성을 보증하는 역할을 수행한다.

제안 메커니즘은 디지털 증거의 수사절차에 따라서 증거식별(1단계), 증거수집(2단계), 증거보존(3단계), 전송 및 저장(4단계)로 분류한다. 1/2/3단계는 기존 포렌식스 도구의 기능을 정책적으로 운영한 DEC에서 수행하고, 4단계는 DEM에서 수행한다. 이때 3단계의 증거보존을 위한 식별자 생성 및 프로파일 저장은 TTP에서 수행한다. 그림 1과 2는 증거물의 무결성 보증을 위한 처리 절차를 나타낸다.



(그림 1) 시스템 구성도



(그림 2) 무결성 보증 절차

(1) DEC는 TS에 접속하여 시스템 정보(SI)를 수집한다. 이때 수집되는 정보는 TS를 식별할 수 있는 H/W 및 S/W 고유값을 이용한다. 이후, DEC는 SI를 이용하여 CN_{DEC}(Case Number of DEC)을 생성하고, (2)DEM에 식별자를 요청한다. CN의 식별자 CN_{DEC}을 생성하여, (3)DEC 및 (3-1)TTP에 전송한다.

DEC는 수신된 CN_{DEC}을 보관하고, 프로파일 생성에 필요한 식별자를 사용한다. (4) DEC는 TTP에 식별자 및 TT(Time-sTamp)를 요청한다. TT는 TTP에서 발급하는 국가별 표준시간정보로서 증거식별을 위해 사용된다. TTP는 (3-1)에서 수신된 CN_{DEC}과 DEC에서 수신된 CN_{DEC}과 DEC에서 수

신된 CN_{DEC}을 확인하고 같으면 TTP 시스템의 고유값 CN_{TTP}(Case Number of TTP)를 생성하여 (5)DEC에 전송하고 (5-1) DEM에도 식별자를 전송한다.

DEC는 (6)TS로부터 디지털 데이터를 수집하여 DEO(Digital Evidence Object)를 생성한다. 이후, 수집된 DEO와 저장된 CN을 이용하여 PI(Profile Info)를 생성하고, PI와 DEO를 결합하여 DEI (Digital Evidence Item)를 생성한다. 이때, PI는 디지털 증거의 프로파일 정보로써 누가, 언제, 어디에서 생성되었는지에 대한 정보를 기록한다. 생성된 DEI는 (7)DEM에 전송되어 디지털 증거로써 저장되고, PI는 (7-1)TTP에 전송되어 저장한다.

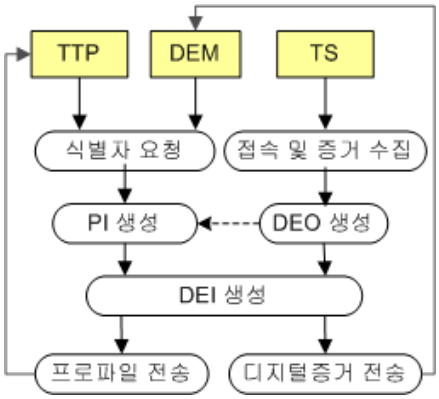
DEM은 DEI를 이용하여 보고서를 작성하여 법원에 제출하고, 프로파일을 이용하여 디지털 증거의 무결성을 보증한다. 이때, 법원으로부터 프로파일의 무결성 확인 요구가 발생하면, TTP에 저장된 PI값을 요청하여 프로파일의 무결성을 보증한다.

3.2 디지털 증거 수집 시스템

DEC는 DEM에 접수된 보안침해사고를 분석하기 위해 TS에 설치되고 해당 TS에 내포된 디지털 데이터를 분석하여 디지털 증거를 수집한다. DEC의 기능은 디지털 증거의 무결성 보증을 위해 DEM 및 TTP로부터 식별자를 요청하고 수집된 식별자를 적용한 디지털 증거의 프로파일을 생성하여 DEM 및 TTP로 전송한다. 그림 3은 DEC 구성도이다.

DEC는 다음과 같은 기능을 갖는다.

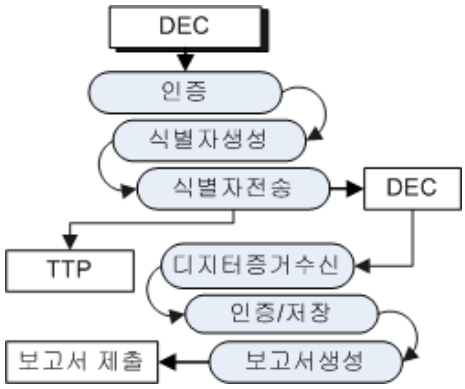
- 식별자 요청: TTP 및 DEM에 식별자 요청
- 증거수집: TS의 디지털 데이터를 읽어 디지털 증거 수집
- 프로파일 생성: 수집된 디지털 증거와 식별자를 적용한 디지털 증거 프로파일 생성
- 프로파일 전송: 생성된 프로파일을 TTP에 전송
- 디지털 증거 전송: 디지털 증거 및 프로파일을 DEM에 전송



(그림 3) DEC 구성도

3.3 디지털 증거 관리 시스템

DEM의 기능은 DEC 사용자 인증 및 디지털 증거 저장, 증거 제출 기능으로 분류한다. DEC 사용자 인증은 DEM에 의해 DEC가 TS에 설치된다. 이때, DEC는 TS의 시스템 정보를 이용하여 DEM에 정당한 권한을 가진 사용자인지를 인증한다. 저장 기능은 DEC로부터 신뢰된 인터페이스를 통하여 디지털 증거를 수신하고, 수신된 증거를 디지털 증거 DB에 저장 관리한다. 즉, 시스템 정보를 취합하여 침해 근거가 되는 디지털 증거의 프로파일을 보관한다. 그리고 저장된 디지털 증거를 법원에 제출하기 위한 보고서 생성기능도 제공한다. 그림 4는 DEM의 구성을 나타내며 각 시스템 구성요소의 기능을 보인다.



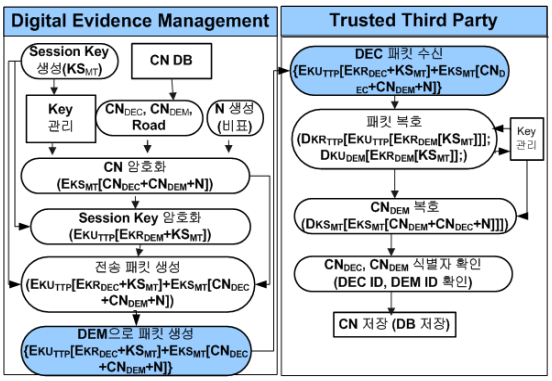
(그림 4) DEM 구성도

- 인증: DEC가 정당한 사용자인지 확인
- 식별자 생성: CNDEM 생성
- 식별자 전송: DEC에 식별자 전송
- 디지털 증거 수신: DEC에 식별자 전송
- 수신된 디지털 증거와 프로파일에 대한 무결성 검증과 저장
- 보고서 생성: 디지털 증거 DB로부터 디지털 증거 생성, 법원 제출

이때, DEM과 TTP사이에는 CN에 대한 식별자 인증이 필요하다. 즉, DEC에 의해 생성되는 프로파일의 식별자를 확인하는 기능을 제공한다.

3.3.1 DEM 식별자 인증

DEM은 그림 5와 같이 CN DB에서 CN_{DEC}, CNDEM을 읽어 TTP에 전송한다.



(그림 5) DEM 식별자 인증

- Packet=$EKU_{TTP}[EKR_{DEC}[KS_{MT}]]+EKS_{MT}[CN_{DEC}+CN_{DEM}+N]$

먼저, $EKU_{TTP}[EKR_{DEC}[KS_{MT}]]$를 이용하여 KS가 DEC로부터 TTP로 안전하게 전송되었음을 보증할 수 있다. 또한, KS로 암호화된 $EKS_{MT}[CN_{DEC}+CN_{DEM}+N]$는 기밀성을 보증할 수 있다.

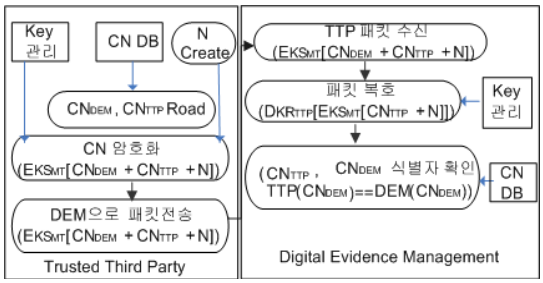
TTP는 자신의 개인키($DKR_{TTP}[EKU_{TTP}[EKR_{DEC}[KS_{MT}]]]$)와 DEC의 공개키($DKU_{DEC}[EKR_{DEC}[KS_{MT}]]$)로 KS를 획득하고, 암호문을 복호($DKS_{MT}[EKS_{MT}[CN_{DEC}+CN_{DEM}+N]]$)하여 CN을 획득한다.

3.3.2 TTP 식별자 인증

그림 6은 TTP 식별자 인증을 보인다. TTP는 CN DB에 저장된 CN_{DEM}, CN_{TTP}을 읽어 KS로 암호화하여 DEM에 전송한다.

- Packet=$EKS_{MT}[CN_{DEM}+CND_{TTP}+N]$

전송된 패킷은 KS로 복호($DKS_{MT}[EKS_{MT}[CN_{DEM}+CN_{TTP}+N]]$)하고, 이후 DEM의 CN DB에 저장된 CNDEM과 TTP로부터 수신된 CNDEM을 확인한다.

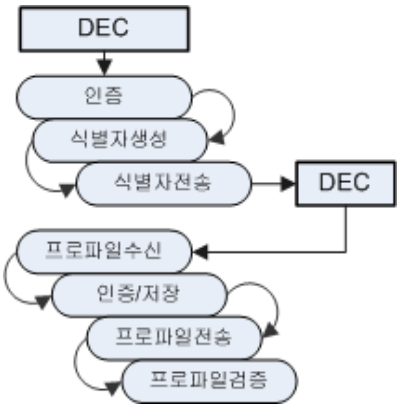


(그림 6) TTP 식별자 인증

3.4 신뢰할 수 있는 제 3기관

TTP의 기능은 식별자 생성 및 전송, 프로파일 관리, TimeStamp 생성 기능으로 분류한다. 먼저 식별자 생성 기능은 디지털 증거의 신뢰성 보증을 위해 CNDEC 및 TT 등을 이용하여 생성한다. 프로파일 관리 기능은 DEC로부터 수신된 프로파일 값을 프로파일 DB에 저장하고, 법원으로부터 디지털 증거에 대한 무결성 확인 요청시 프로파일을 전송한다. TimeStamp 생성 기능은 표준시간을 제공한다. 그림 7은 신뢰할 수 있는 제 3기관의 구성을 나타낸다. 각 시스템 구성요소의 기능은 다음과 같다.

- 인증: DEC가 정당한 사용자인지 확인
- 식별자 생성: DS_{TTP} 및 TT 생성
- 식별자 전송: DEC에 식별자 전송
- 프로파일 수신: DEC로부터 프로파일 수신
- 인증/저장: 수신된 프로파일에 대한 무결성 검증과 저장
- 프로파일 전송: 법원으로부터 디지털 증거의 무결성 검증 요청이 있을 때 해당 프로파일 전송



(그림 7) TTP 구성도

TTP는 기관 내부에 설치할 수도 있지만 가능하면 DEM을 운영하는 기관에서 임의로 접근할 수 없는 기관에 설치하고 이에 대한 접근을 제한하는 명백한 정책이 필요하다.

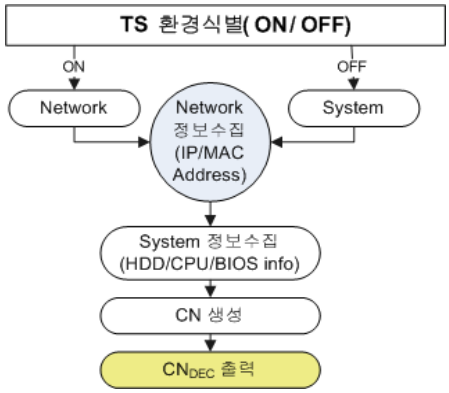
3.5 개체간 상호인터페이스

DEC와 TS, DEM, TTP의 세부운영 정책은 다음과 같다.

3.5.1 DEC와 TS

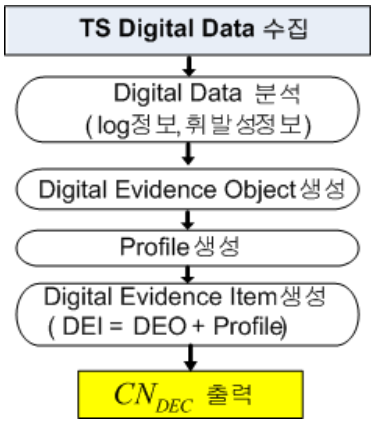
DEC와 TS는 TS의 환경에 따라 시스템정보를 획득하여 CN을 생성하고 생성된 CN은 TS를 식별하는 기능을 수행한다. 그리고 TS에 내포된 디지털 데이터를 분석하여 DEO를 생성한다. 그림 8는 TS와 DEC간의 CN 생성 절차를 보여준다.

DEC는 TS에 접속하여 디지털 데이터를 분석한다. 이때, TS는 네트워크 연결이 가능한 On-line 환경과 Off-line 환경으로 분류할 수 있으며 각 환경에 따라 네트워크 접속 및 시스템에 직접 접속하여 정보를 수집한다.



(그림 8) CN_{DEC} 생성

수집 정보는 크게 네트워크 정보 및 시스템 정보로 분류할 수 있다. 네트워크 정보는 TS의 고유 MAC 주소 및 IP 주소를 수집하고, 시스템 정보에서는 CPU 식별 번호나 HDD S/N 및 BIOS 정보를 수집한다. 이후, 수집된 정보는 DEC에 의해 생성되는 DEO가 TS로부터 생성된 데이터라는 것을 보증하는 식별자로 사용된다. 그림 9는 DEC와 TS 간의 DEO생성 절차를 보여준다.

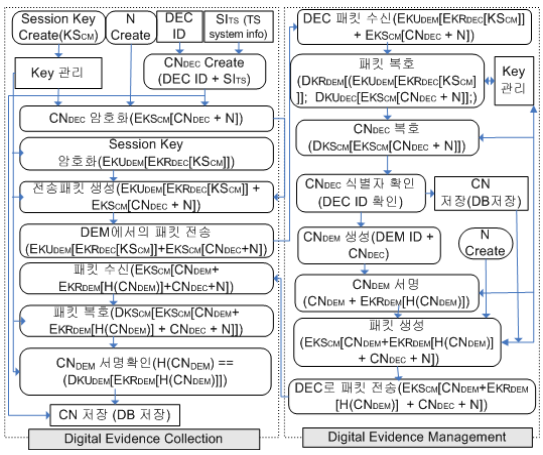


(그림 9) DEI 생성

DEC는 DEM 및 TTP로부터 프로파일에 필요한 식별자를 획득한다. 이후, TS에 접속하여 디지털 데이터를 수집·분석하고 DEO를 생성한다. 생성된 DEO는 식별자를 이용하여 프로파일링을 수행하고, 그 결과로 DEI를 생성한다. 이때 PI는 디지털 증거가 누가, 언제, 어디서, 무엇을 생성했는지에 대한 정보를 포함하고 있다.

3.5.2 DEC와 DEM

그림 10은 DEC와 DEM사이에 식별자 생성 절차를 보여준다.



(그림 10) DEC와 DEM 식별자 생성

TS의 환경에 따라 시스템정보를 획득하여 CN_{DEC}을 생성하고(생성된 CN_{DEC}은 TS를 식별하는 기능 수행) DEM으로 전송하여 확인한다. DEM은 CN_{DEC}값을 적용한 CN_{DEM}을 생성하여 안전하게 전송한다. 전송로 상의 보안을 위해 공개키 기반의 인증서를 사용한다.

(1) CN_{DEC} 생성/전송

CN_{DEC}은 그림 8과 같이 생성되어 관용암호화 방식을 이용하여 전송한다.

▪ $Packet=EKU_{DEM}[EKR_{DEC}[KS_{CM}]+EKS_{CM}[CN_{DEC}+N]]$

먼저 $EKU_{DEC}[EKR_{DEC}[KS_{CM}]]$를 이용하여 KS가 DEC로부터 DEM으로 안전하게 전송되었음을 보증할 수 있다. 또한, KS로 암호화된 $EKS_{CM}[CN_{DEC} + N]$는 기밀성을 보증할 수 있다. DEM은 자신의 개인키($DKR_{DEM}[EKU_{DEM}\ [EKR_{DEC}\ [KS_{CM}]]]$)와 DEC의 공개키($DKU_{DEC}[EKR_{DEC}\ [KS_{CM}]]$)로 KS를 획득하고, 암호문을 복호($DKS_{CM}[EKS_{CM}\ [CN_{DEC} + N]]$)하여 CN을 획득한다.

(2) CNDEM 생성/전송

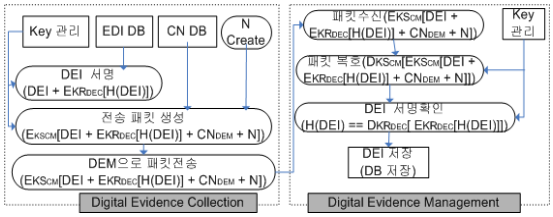
DEM은 CN_{DEC}를 적용하여 CN_{DEM}을 생성(DEM ID+CN_{DEC})하고 생성된 CN_{DEM}은 서명(CN_{DEM} + $EKR_{DEM}[H(CN_{DEM})]$)되어 DEC에 전송된다.

▪ $Packet=EKS_{CM}[CN_{DEM}+EKR_{DEM}[H(CN_{DEM})]+CN_{DEC}+N]$

DEC는 서명 확인을 통해 CN_{DEM}을 확인한다.

(3) DEI 전송/저장

그림 11은 DEI 전송 절차를 보여준다.



(그림 11) DEI 전송

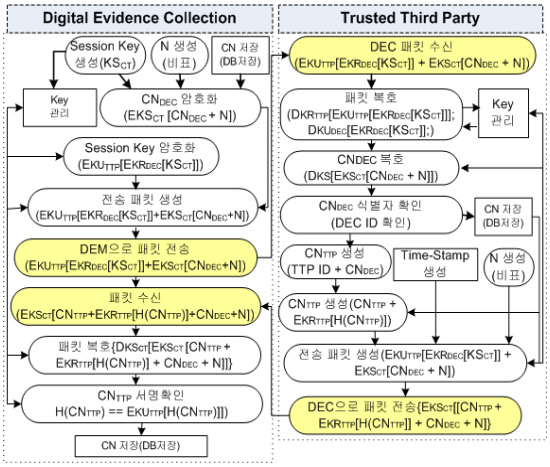
DEI DB에 저장된 DEI를 읽어 DEC의 개인키로 서명(DEI+$EKR_{DEC}[H(DEI)]$)하여 DEM에 전송한다.

▪ $Packet=EKS_{CM}[DEI+EKR_{DEC}[H(DEI)]+CN_{DEM}+N]$

전송된 패킷은 KS로 복호하고($DKS_{CM}[EKS_{CM}[DEI+EKR_{DEC}[H(DEI)]+CNDEM+N]]$), 이후 DEI 서명을 확인($H(DEI) == DKU_{DEC}[EKR_{DEC}[H(DEI)]]$)한다. 확인된 DEI는 DB에 저장된다.

3.5.3 DEC와 TTP

그림 12는 DEC와 TTP사이의 식별자 생성 절차를 보여준다.



(그림 12) DEC와 TTP 식별자 생성

먼저, TS의 환경에 따라 시스템 정보를 획득하여 CN_{DEC}를 생성하고 TTP로 전송하여 확인하는 기능이다. 둘째로, TTP는 CN_{DEC}값을 적용한 CN_{TTP}를 생성하고 안전하게 전송하는 기능을 갖는다. 또한 전송로 상의 보안을 위해 공개키 기반의 인증서를 사용한다. 마지막으로 DEC는 PI를 TTP에 전송한다.

(1) CN_{DEC} 생성/전송

CN_{DEc}는 그림 8과 같이 생성된다. 먼저, $EKU_{TTP}[EKR_{TTP}[KS_{CT}]]$를 이용하여 KS가 DEC로부터 TTP로 안전하게 전송되었음을 보증할 수 있다. 또한, KS로 암호화된 $EKS_{CT}[CN_{DEC}+N]$는 기밀성을 보증할 수 있다. TTP는 자신의 개인키 $(DKR_{TTP}[EKU_{TTP}[EKR_{DEC}[KS_{CT}]]])$ DEC의 공개키 $(DKU_{DEC}[EKR_{DEC}[KS_{CT}]]$로 KS를 획득하고 암호문을 복호$((DKS_{CT}[EKS_{CT}[CN_{DEC}+N]])$하여 CN을 획득한다.

(2) CN_{TTP} 생성/전송

TTP는 CN_{DEC}를 적용하여 CN_{TTP}를 생성(TTP ID $+CN_{DEC}$)하고 생성된 CN_{TTP}는 서명$(CN_{TTP}+EKR_{TTP}[H(CN_{TTP})])$되어 DEC에 전송된다.

▪ $Packet=EKS_{CT}[CN_{TTP}+EKR_{TTP}[H(CN_{TTP})]+CN_{DEC}+N]$

DEC는 서명 확인을 통해 CN_{TTP}를 확인한다.

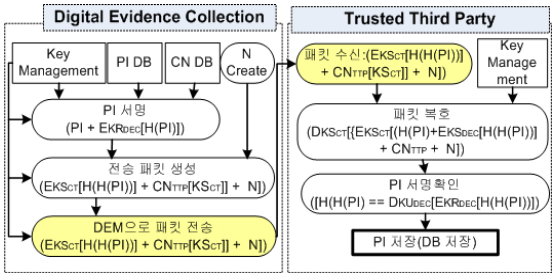
(3) PI 전송/저장

그림 13은 PI의 전송 절차를 보여준다.

먼저, PI DB에 저장된 PI를 읽어 DEC의 개인키로 서명$(H(PI)+EKR_{DEC}[H(H(PI))])$하여 TTP에 전송한다.

▪ $Packet=EKS_{CT}[H(PI)+EKR_{DEC}[H(H(PI))]+CN_{TTP}+N]$

전송된 패킷은 KS로 복호하고, 이후 PI 서명을 확인$(H(PI)$ == $DKR_{DEC}[EKR_{DEC}[H(H(PI))]])$한다. 확인된 PI는 DB에 저장된다.



(그림 13) PI 전송

4. 제안 메커니즘 평가

4.1 평가 요구사항

피해 시스템, 가해 시스템, 경유 시스템상에 존재하는 디지털 증거 자체에 대한 신뢰성, 디지털 증거의 수집 · 보관에 대한 신뢰의 요구사항을 갖는다. 이러한 신뢰성 보증 서비스를 제공하는 제안 시스템은 디지털 증거의 무결성 보증, 디지털

증거의 객관화, 침입증거의 무결성 보증을 위한 접근통제의 평가 요구사항을 갖는다.

평가 요구사항을 각 항목별로 분석하여 제안 모델의 타당성을 제시하고 현행 압수수색의 컴퓨터 포렌식스 절차 및 정책과 비교 분석한다.

4.2 침해 증거 무결성 보증 메커니즘 분석

4.2.1 침해 증거의 무결성 보증

디지털 증거의 무결성 보증은 디지털 증거의 프로파일이 변경되지 않고 잘 보존되어 있다는 사실을 객관적으로 입증할 수 있어야 한다.

무결성을 입증해야하는 사용자는 디지털 증거 프로파일 검증 메커니즘을 이용하여 검증할 수 있다. 즉, DEC에 의해 생성된 프로파일과 디지털 증거는 각각 TTP와 DEM에 안전하게 저장되어 있으므로, 저장된 프로파일 정보를 비교함으로써 디지털 증거의 무결성을 입증한다. 먼저, DEM에 저장된 내용은 다음과 같다.

- DEM = DEI
- DEI = PI ‖ DEO
- PIDEM = CN_{DEC} ‖ CNDEM ‖ CN_{TTP} ‖ TT ‖ H(DEO)

TTP에 저장된 내용은 다음과 같다.

- PI_{TTP} = H(CN_{DEC} ‖ CNDEM ‖ CN_{TTP} ‖ TT ‖ H(DEO))

즉, DEM에는 DEC에서 수집된 디지털 증거에 대한 프로파일과 디지털 증거를 보관하며, 디지털 증거의 무결성은 PI를 통하여 증명한다. 그러나 DEM에 저장된 PI는 신뢰성에 대한 문제가 발생할 수 있으며, 이를 해결하기 위하여 DEC에 의해 TTP에 저장된 PI값을 요청하여 PIDEM 값과 PI_{TTP} 값이 같음을 증명함으로 무결성을 보증한다.

- 무결성 보증 → if(H(PIDEM) == PI_{TTP}) CDI

4.2.2 디지털 증거의 객관화

디지털 증거와 관련한 기존 압수수색 방식에서는 매체에 의존하여 신뢰성을 보장하였다. 그러나 현재의 다중사용자 기반의 개방시스템 환경에서는 압수수색으로 인한 가용성 서비스 및 제 3자의 프라이버시 문제가 발생할 수 있다. 따라서 매체와는 독립하여 디지털 증거 자체가 임의로 변경되지 않았다는 사실을 입증하는 매체 독립적 접근 방식이 필요하다.

매체 독립적 접근 방식에서는 수집된 디지털 증거를 객관화하여 프로파일을 생성한다. 프로파일은 생성자로부터 분리시켜 생성자가 이를 변경할 수 없다는 사실을 법과학적으로 증명할 수 있는 구조를 갖추어야 한다. 이러한 객관화의 방법에는 관리 주제의 객관화, 생성 시간의 객관화, 내용의 객관화, 기록방식의 객관화, 저장방식의 객관화 등을 이용한다.

(1) 주체의 객관화

프로파일을 관리하는 주체를 생성자와 분리하고 생성자 이외의 주체로 하여금 프로파일을 관리하게 하는 방식이다. 본 논문에서는 이를 위하여 생성자인 DEC와 관리자인 DEM 및 TTP를 이용한다.

- DEC: 디지털 증거를 분석하여 DEI 생성
- DEM: DEI 관리
- TTP: PI 관리

즉, 생성되는 DEI를 생성자와 관리자로 분리하여 관리함으로써 주체를 객관화 시켰다.

(2) 생성시간의 객관화

디지털 증거를 생산한 시간과 프로파일을 생성한 시간을 확정함으로써 이후에 발생한 자료들과 구별하려는 노력이다. 디지털 증거의 생산시기가

객관화됨으로써 이를 생산한 주체가 임의로 사후에 변경하지 못하게 하기 위한 방책이다.

▪ PI: CN_{DEC} ‖ CNDEM ‖ CN_{TTP} ‖ TT ‖ H(DEO)

본 논문에서는 TTP에서 사건조사 및 증거 생성에 필요한 TimeStamp를 생성하여 객관화한다. TTP에서는 DEC로부터 식별자 요청시 식별자와 함께 TT를 제공한다.

(3) 내용의 객관화

디지털 증거의 내용을 더 이상 수정할 수 없도록 그 내용을 확정시키는 것으로 일반적으로 일방향 해쉬 함수가 이용된다.

▪ PI = CN_{DEC}‖ CNDEM ‖ CN_{TTP} ‖ TT ‖ H(DEO)

PI는 DEO를 포함한 식별자를 이용하여 생성한다.

(4) 기록방식과 저장방식의 객관화

디지털 증거를 기록하여 저장할 경우에 이를 어떠한 이유로도 변경할 수 없도록 하기 위한 것이다. 기록방식에서는 첨가기록방식(Append-Only)을 사용하여 이미 기록된 디지털 증거에 대해서 변경할 수 없도록 하는 방식을 말하고, 저장방식도 읽기전용방식(Read-Only)을 채택하는 방식을 사용하여 한번 기록된 디지털 증거가 다시 변경되는 일이 없도록 통제하는 방식이다.

4.2.3 침입증거의 무결성 보증을 위한 접근통제

피해시스템의 침입정보가 포렌식스 증거로 효용성을 발휘하기 위해서는 증거물의 원본 보호 무결성 기능을 제공해야 한다. 즉, 침입 흔적이 법적으로 효용성을 제공하기 위해서는 변경되거나 삭제로 부터 보호되어야 한다. 시스템을 사용하는 주체에 따라 보안 등급이 설정되고 자신의 보안 등급보다 높은 개체는 접근을 할 수 없다.

그러나 접근이 허용된 개체라도 포렌식스 정보로 활용되기 위해서는 등급과는 별개로 쓰기 및 수정으로부터 보호되어야 한다. 또한 같은 개체가 존재할 때, 새로 생성되는 개체는 기존 개체에 겹쳐 쓰지 못하도록 보호해야 한다. 주체의 집합(S), 개체의 집합(O), 주체의 보안등급(C(s)), 개체의 보안 등급(C(o))은 침입 증거를 보호하기 위하여 다음과 같은 보안 정책을 갖는다.

- 읽기 보안 성질: 주체 S는 객체 O를 C(s) >= C(o)일 경우 읽기 허가
- 쓰기 보안 성질: 객체 O에 대해서 주체 S는 쓰기 금지
- 생성 보안 성질: 객체 O에 대해서 읽기 참조가 있는 주체 S는 C(s) = C(o)일 경우, 새로운 객체 O에 생성 허가

(S: 주체의 집합, O: 주체의 보안 등급, C(s): 주체의 보안 등급, (Co): 객체의 보안 등급)

4.3 제안 메커니즘 평가

제안된 침해 증거 무결성 보증 모델의 평가는 4.1에서 도출된 요구사항을 바탕으로 현행 압수수색에 의한 컴퓨터 포렌식스 절차 및 정책과 비교하여 평가하였다. 제안된 방식은 디지털 증거에 대한 프로파일을 생성하여 누가, 언제, 어디서, 무엇을 했는가에 대한 정보를 포함하며, 이것은 대상시스템으로부터 디지털 증거에 대한 매체 독립적 분석을 가능하게 하였다. 수집된 디지털 증거는 TTP에 저장된 프로파일에 의해 무결성을 제공한다.

평가 요구사항을 각 항목별로 분석하여 제안 모델의 타당성을 제시하며 각 평가 항목(표 1)은 “컴퓨터 포렌식스 도구의 신뢰성”, “디지털 증거의 무결성 보증”, “가용성 서비스”, “디지털 증거의 객관화”이다.

현행 포렌식스 방식의 경우, 시스템 및 프로그램의 신뢰성을 검증할 수 있는 메커니즘은 없다. 단지, 몇몇의 프로그램의 경우 개발업체가 자체적으로 기준값을 만들어 제공한다. 또한 대상시스템

및 자원의 압수수색을 원칙으로 압수된 원본 데이터와 디지털 증거가 같음을 증명함으로써 무결성을 제공한다.

제안방식에서는 프로그램을 처음 설치에서부터 현재까지의 상태정보를 신뢰된 관리자에 의해 프로파일링 되고, TTP에 저장하여 프로그램의 신뢰성을 제공하고, 매체 독립적 방식으로 가용성을 제공하면서 디지털 증거를 수집할 수 있다. 디지털 증거의 신뢰성을 보증하기 위해 프로파일을 생성하고, 생성된 프로파일을 TTP에 저장되어 증거의 무결성 보증을 위해 사용된다.

(표 1) 증거 관리 모델 비교 분석

요구사항	현행 방식	제안 방식	비고
시스템 자체의 신뢰성 검증	X	Δ	TTP 이용
컴퓨터 포렌식스 도구의 신뢰성 검증	Δ	O	TTP 이용
가용성 서비스 제공	X	O	매체독립적
디지털 증거의 무결성 서비스 제공	Δ	O	디지털 증거 객관화
주체의 객관화	X	O	직무분리
생성시간의 객관화	X	O	TTP의 TimeStamp
내용의 객관화	O	O	Hash 함수

(O: 지원, Δ:부분적 지원, X:지원하지 않음)

침입 증거의 무결성 보증을 위한 접근통제의 경우, 현행방식에서는 일반적 접근 통제 모델을 사용함으로서 수정이 불가피한 것을 제안된 IEB 모델을 사용하여 정당한 권한을 가진 사용자의 불법적 변형을 제한할 수 있다.

제안된 방식에서는 디지털 증거 생성을 위한 DEC와 관리를 위한 DEM 그리고 검증을 위한 TTP로 구성되어 생성과 관리의 권한을 분리하였다. 또한, TTP를 통해 사건처리의 표준시간을 제공함으로써 생성시간의 객관화 및 프로파일링을 통해 내용의 객관화를 제공하였다. 즉, 제안 메커니즘은 기존 시스템 환경에서 매체 독립성을 적용하여 가용성 서비스를 제공하였으며 대상시스템에서 수집·생성된 디지털 증거를 객관화함으로써 신뢰성을 보증한다.

5. 결 론

본 논문에서는 디지털 컴퓨팅 환경의 시스템 오류 및 침해의 데이터를 법적대응 증거자료를 보호함으로써, 증거자료의 신뢰성을 높이기 위해 디지털 증거의 매체 독립적인 속성을 이용한 침해 증거 보증 메커니즘을 제안하였다.

제안한 메커니즘은 컴퓨팅 환경의 범죄에 대한 수사절차와 침해사고 대응과정에서 획득되는 디지털 증거의 신뢰성을 향상시켜 사법정의 실현과 정보보안 강화에 기여할 수 있다. 또한 범죄가 발생하기 이전에 사건 발생에 대비하여 시스템과 주요 프로그램에 대한 무결성 검증의 기준점 마련과 사건발생 이후에 시스템과 주요 프로그램에 대한 침해 사실을 확인하기 위한 목적으로 운용될 수 있다. 또한 디지털 자료처리의 전반적 분야에 적용함으로써 중요한 전자적 거래에 있어서 신뢰성을 보증하기 위한 인프라로 발전시켜 전자적 거래의 안전에 기여하는데 활용될 수 있다.

향후, 제안 메커니즘이 실무현장에서 널리 이용되기 위해서는 정부차원의 신뢰기관 구축을 필요로 한다. 또한 디지털 증거를 생성하고 처리 운영하는 대상시스템 및 주요 프로그램에 대한 신뢰성 보증을 위한 체계적인 연구가 필요하다.

참 고 문 헌

[1] Warren G.Kruse ii, Jay G.Heiser. "COMPUTER FORENSICS: Incident Response Essentials", Addison Wesley, Oct 2001.

[2] Albert J. Marcella Jr (Editor S. Greenfield, "Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes (Information Security)

(Hardcover)", Auerbach Publications, Dec 2007.
[3] Eoghan Casey, "Handbook of Computer Crime Investigation: Forensic Tools & Technology", Academic Press , Oct 2001.
[4] Braian Carrier, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers, International Journal of Digital Evidence", Vol 1, Issue 4,. Winder 2003.
[5] Gray Palner. "A Road Map for Digital Forensics Research. Technical Report DTR-T001-01. DFRWS", Report From the Fiest Digital Forensic Reserch Workshop(DFWS), November 2001.
[6] Lee Garber, "Encase: A Case Study in Computer-Forensics Technology", IEEE Computer Magazine Jan 2001.
[7] D.Farmer and W. Venema, "The Coroner Toolkit (TCT) v1.11", Available at: http://www. Porcupine.org/ forensics/tct.thml, September 2002.
[8] TCT: The Coroner's Toolkit, http://www.fish.com/tct

◐ 저 자 소 개 ◑

장 은 겸
2000년 대전대학교 컴퓨터공학과 졸업(학사)
2002년 대전대학교 대학원 컴퓨터공학과 졸업(석사)
2007년 대전대학교 대학원 컴퓨터공학과 졸업(박사)
2009년~현재 대전대학교 컴퓨터공학과 겸임교수
2008년~현재 (주)엠투엠코리아 연구소장
관심분야 : 컴퓨터 포렌식, DRM, 스마트 폰, 접근통제
E-mail : jangegu@nate.com