보안공학연구논문지 *Journal of Security Engineering*
Vol.11, No.6 (2014), pp.605-614
http://dx.doi.org/10.14257/jse.2014.12.05

안티포렌식 기법 분석을 통한 안티포렌식 대응 방안

신원[1)]

Countermeasures against Anti-forensics by Analyzing Anti-forensics Techniques

Weon Shin[1)]

요 약

최근 다양한 포렌식 기술이 널리 알려짐에 따라 개인 정보나 중요 정보를 보호하기 위한 안티포렌식 도구들이 많이 사용되고 있다. 그러나 디지털 포렌식에 있어 안티포렌식 도구는 디지털 증거 수집을 어렵게 함으로써 수사를 방해할 수 있는 문제점을 가지고 있다. 본 논문에서는 다양한 안티포렌식 기법을 분류하고, 이에 대한 각각의 대응 방안을 제안한다. 또한, 안티포렌식을 고려한 수사 절차 상의 수정 방안도 제시한다. 본 연구의 결과는 안티포렌식 기법을 분석한 후 안티포렌식 대응 방안을 마련하는데 도움이 될 것으로 판단한다.

핵심어 : 디지털포렌식, 안티포렌식, 안티포렌식 대응

Abstract

Since forensics technologies are widely known, various anti-forensics tools are used widely to protect personal information and sensitive information recently. But anti-forensics tools also are able to frustrate the investigation by making it difficult to collect digital evidences on computer systems. In this paper, we classify anti-forensics techniques and propose the anti-anti-forensics countermeasures against them respectively. We also suggest a revised procedure of the investigation considering the use of anti-forensics tools. The results of this study help to develop the corresponding anti-anti-forensics against anti-forensics technologies by analyzing anti-forensics techniques.

Keywords : Digital Forensics, Anti-forensics, Anti-anti-forensics

1. 서론

디지털 포렌식(Digital Forensics)은 “범죄 현장에서 확보한 컴퓨터 시스템이나 전자 장비에서 수집할 수 있는 디지털 증거물에 대해 보존(Preservation), 수집(Collection), 확인(Validation), 식별(Identification), 분석(Analysis), 해석(Interpretation), 기록(Documentation), 현출(Presentation) 등을

접수일(2014년08월18일), 심사의뢰일(2014년08월18일), 심사완료일(1차:2014년09월10일, 2차:2014년10월23일)
게재일(2014년12월31일)

[1]608-711 부산광역시 남구 신선로 428 (용당동), 동명대학교 정보보호학과.
email: shinweon@tu.ac.kr

ISSN: 1738-7531 JSE

과학적으로 도출되고 검증된 방법으로 수행하는 일련의 과정"으로 정의한다[1]. 디지털 포렌식은 해킹, 사이버 범죄에서 사용되는 컴퓨터, 노트북, 스마트폰 등의 메모리, 운영체제, 애플리케이션, 네트워크 등에 존재하는 다양한 디지털 증거를 분석함으로써, 사이버 범죄의 추적과 조사에 적극 활용되고 있다[2][3]. 한편, 디지털 포렌식이 다양한 환경에서 적용되고 보편화됨에 따라 이에 대한 대응으로 안티포렌식 도구들이 등장하고 있다. 개인이 자신의 개인정보를 삭제하거나 기업에서 중요 기밀정보를 안전하게 파기함으로서 중요 데이터 보호나 개인정보 보호를 위한 정당한 파괴 행위에 안티포렌식 도구들을 활용하고 있다. 최근에는 추적 및 증거물 획득을 원천적이고 자동화된 방법으로 막아주는 전문 제품들이 등장하고 있으며, 다양한 안티포렌식 기법들이 소개되고 있는 실정이다. 특히, 이들 도구를 활용하여 수사를 방해하기 위한 목적으로 증거가 될 가능성이 있는 데이터를 의도적으로 파괴하는 행위는 엄연히 범법 행위가 된다.

본 논문에서는 이러한 문제점을 인식하고 현존하는 다양한 안티포렌식 기법에 대한 각각의 대응 방안을 제안하고자 한다. 또한, 이 결과를 활용하여 포렌식 조사 모델에서 안티포렌식을 고려한 수사 절차 상의 수정 방안도 제시한다. 본 논문의 구성은 다음과 같다. 2장에서는 안티포렌식의 정의와 목적에 대해서 살펴보고 해당 기술을 분류하고, 3장에서는 각각의 안티포렌식과 해당하는 대응 방안을 설명한다. 4장에서는 본 논문에서 제안한 안티포렌식 기법 각각의 대응 방안과 수정된 수사 절차를 제시하고, 마지막 5장에서 결론을 맺는다.

2. 안티포렌식 개요

2.1 안티포렌식의 정의

안티포렌식(Anti-Forensics)은 "포렌식 도구, 수사 및 수사관의 분석을 방해하기 위한 도구와 기술"로 정의한다[4]. 즉, 디지털 포렌식 기술에 대응하여 자신에게 불리하게 작용될 가능성이 있는 디지털 증거를 훼손하거나 숨기려는 일련의 행위를 의미한다. 데이터 파괴, 데이터 암호화, 데이터 은닉, 데이터 조작, 흔적 최소화 등이 대표적이며, 포괄적으로 디지털 증거의 획득을 방해하는 모든 행위가 포함된다. 가장 일반적인 안티포렌식 행위는 수사관들이 수집할 수 없도록 증거물이 될 수 있는 데이터를 삭제하거나 훼손하는 것인데, 예를 들면 파일을 단순 삭제, 하드디스크의 파티션 삭제나 하드디스크 포맷, 파일 또는 하드디스크 암호화 도구 사용, 파일의 확장자 변경, 웹 브라우저 사용 흔적 삭제 등과 같은 행위가 해당된다. Liu et al[5]은 이러한 방식을 사용하는 안티포렌식의 주요 목적을 다음과 같이 정의하였다.

- 어떤 종류의 사건이 발생한 사실을 탐지하는 것을 회피
- 정보의 수집을 방해
- 하나의 경우에 대해 수사관이 필요한 시간을 증가
- 포렌식 보고서나 증언에 대한 의혹을 제기

2.2 안티포렌식 기술 분류

안티포렌식 기술은 디지털 증거의 분석을 방해하기 위하여 디지털 증거가 될 수 있는 데이터를 훼손하거나 숨기기 위해 사용하는 모든 방법으로, 사용하는 기법과 세부 내용에 따라 표 1과 같이 분류할 수 있다[4][5][[6][7].

[표 1] 안티포렌식 기술 분류
[Table 1] Classification of anti-forensics technologies

분류	세부	내용
데이터 파괴 (Destruction)	완전삭제	분석을 방해하기 위해 중요 데이터를 삭제하거나 훼손
데이터 은닉 (Hiding)	암호화	데이터를 암호화하여 디지털 증거 분석을 방해
	심층암호	특정 파일에 중요 정보를 은닉
데이터 수정 (Modification)	조작	데이터를 수정 또는 조작하여 분석이 어렵도록 처리
흔적 최소화 (Minimizing the footprint)		사용한 안티포렌식 도구나 기법의 흔적을 제거

3. 안티포렌식 대응 방안

안티포렌식에 대한 일반적인 대응 방안은 다음과 같다[4]. 첫째, 공격자가 데이터를 접근할 수 장소에 데이터를 저장하는 방법이다. 로그를 남기거나 CD-R 또는 DVD-R 등 한번 기록하면 수정할 수 없는 읽기 전용 매체에 데이터를 저장하는 방법이다. 최근 널리 사용하는 클라우드 컴퓨팅(Cloud Computing)을 활용하는 것도 좋은 방법이다. 둘째, 기존 디지털 포렌식 도구들은 안티포렌식에 대응하기에는 기능이 부족한 것들이 많은데, 이들의 기능을 개선하는 방법이다. 현실적으로 쉽지는 않으나 새로운 방법들을 적용하여 지속적으로 기능을 개선하여야 한다. 셋째, 안티포렌식에 대응하기 위한 전문 도구들을 새롭게 개발하는 방법이다. 데이터 암호화에 대응하기 위하여 키로거(Keylogger)를 개발하여 설치하거나 네트워크 트래픽 분석을 위하여 스니퍼(Sniffer)를 보강하거나 로그를 활용하여 사용자 행위를 모니터링하는 방법이 여기에 속한다. 그러나 이러한 방법은 부수적인 제약 조건이 따르거나 제한적인 환경에서만 적용할 수 있는 단점이 있다. 따라서, 안티포렌식에 적극적으로 대응하기 위해서는 안티포렌식 대응 기술(Anti-Anti-Forensics)을 적용해야만 하는데, 안티포렌식 대응 기술은 표 2와 같이 분류할 수 있다.

ISSN: 1738-7531 JSE

[표 2] 안티포렌식 기술 분류
[Table 2] Classification of anti-forensics technologies

분류	내용
데이터 복구	분석을 방해하기 위해 중요 데이터를 삭제하거나 훼손
데이터 검색 및 탐지	데이터를 암호화하여 디지털 증거 분석을 방해
암호 크래킹	특정 파일에 중요 정보를 은닉
은닉 데이터 탐지	데이터를 수정 또는 조작하여 분석이 어렵도록 처리
물리 메모리 분석	사용한 안티포렌식 도구나 기법의 흔적을 제거
기타 분석	시간 정보 분석, 일관성 분석, 연관 관계 분석 방법 등

안티포렌식 기술 분류에 따른 안티포렌식 대응 기술에 대한 세부 내용은 다음과 같다.

3.1 데이터 복구 방안

삭제한 데이터가 어떤 형태로든 저장 매체에 남아 있다면 이론적으로 복구가 가능하지만, 안티포렌식 전용 도구를 이용한 삭제는 일반적으로 복구가 불가능하다. 데이터 복구는 물리적인 복구와 논리적인 복구로 분류할 수 있는데, 물리적인 복구는 저장매체를 파괴하지 않은 경우 복구가 가능하고 이후 논리적인 복구를 수행할 수 있다. 논리적인 복구는 안티포렌식 도구를 이용하여 데이터를 완전삭제하지 않았다면 여러 복구 기법을 동원하여 복구가 가능하다. 단, 데이터 복구율은 저장매체의 상태, 파일 시스템 유형, 데이터 저장 방식에 따라 많은 차이가 존재한다. 참고로 그림 1은 국내 무료 백신 프로그램 내에 포함되어 있는 완전삭제 기능이다.

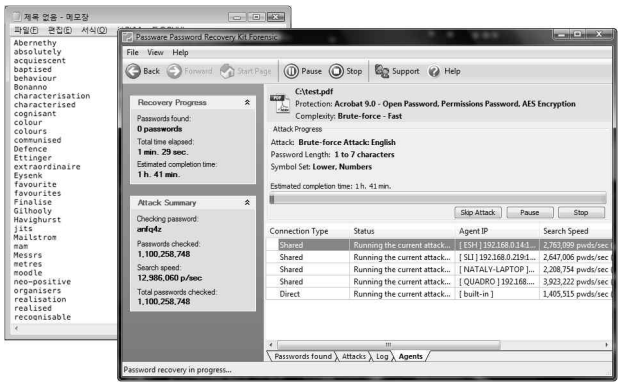
[그림 1] 백신 프로그램 내의 완적산제 기능
[Fig. 1] Wiping function in anti-varus programs

3.2 데이터 검색 및 탐지 방안

데이터 검색 및 탐지 기술은 하드디스크 및 파일 시스템 기반 조사와 파일 기반 조사로 나눌 수 있다. 첫째, 하드디스크 및 파일 시스템 기반 조사에는 Index 기반 탐색과 Bitwise 방법이 있다. Index 기반 탐색은 포렌식 도구에서 키워드에 의존하여 일반 드라이브, 이미지, 파티션 등의 모든 영역을 모두 검색하는 방법으로, 파일 포맷과는 독립적인 조사가 가능하고 속도가 빠른 장점이 있다. Bitwise 방법은 디스크 내의 섹터나 슬랙 공간(Slack Space)에서 찾을 수 있는 비 할당 영역에 존재하는 간단한 텍스트나 특정 표현들을 찾는 방법으로, 텍스트 뿐만 아니라 이진수 표현 검색 가능하지만 단편화가 심하게 되어 있는 경우 조사가 어렵다. 둘째, 파일 기반 조사에는 파일 포맷 분석과 해쉬 검증이 있다. 파일 포맷 분석은 파일 시그니처(Signature)에 의존하여 원하는 대상 검색하는 방법으로, 파일 포맷에 의존하므로 파일의 이름 또는 확장자를 변경하더라도 분석이 가능하다. 해쉬 검증은 해쉬 값을 분석함으로써 해당 파일을 찾는 경우로, 이미 알려진 파일의 해쉬값은 NSRL(National Software Reference Library)의 RDS(Reference Data Set) 해쉬셋에 테이블 형태로 제공하고 있다[8].

3.3 암호 크래킹 방안

암호 크래킹은 암호화된 데이터의 키를 알아내어 이를 복호화하는 기법으로 암호 알고리즘으로 암호화된 데이터의 키(Key)를 무차별 대입 하는 경우 많은 시간을 소요한다. 그러나 패스워드 기반 암호 체계를 사용하는 경우 복구를 위해서 크래킹 전용 도구를 사용한 사회공학 공격(Social Engineering Attack), 사전 공격(Dictionary Attack), 무차별 대입 공격(Brute Force Attack) 등을 사용할 수 있다. 그림 2는 패스워드 사전과 패스워드 크래킹 도구이다.



[그림 2] 패스워드 사전과 패스워드 크래킹 도구

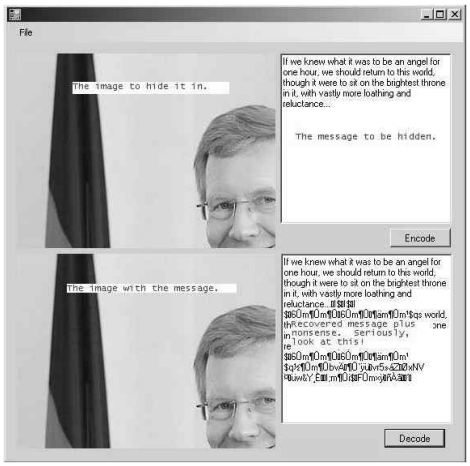
[Fig. 2] Password dictionary and password cracking tool

데이터를 암호화할 때 AES, RSA 등 널리 사용되는 표준 암호 알고리즘을 이용하여 암호화하는 경우가 많은데, 일반적으로 이들 표준 암호 알고리즘에서는 권장하는 키 크기(AES는 128/192/256 비트, RSA는 1024/2048 비트)와 IV(Initial Vector)를 사용하여 데이터를 암호화한다. 이 경우에 암호화 키와 IV를 안전한 장소에 보관하여 알아낼 수 없다면 암호 크래킹은 사실상 불가능하다. 그러나 로그온 패스워드나 파일 암호화는 대부분 사람의 기억에 의존하여 패스워드 또는 암호화키를 관리하는 경우가 많으므로 사회공학 공격, 사전 공격 등을 사용하여 크래킹 시간을 충분히 단축할 수 있으며, 필요에 따라 전용 도구를 사용하거나 직접 개발하여 암호 크래킹을 수행할 수 있다.

3.4 은닉 데이터 탐지 방안

은닉 데이터 탐지 및 분석 기법은 이미지와 같은 멀티미디어 파일 또는 문서 파일 등에 숨겨 놓은 데이터를 탐지하고 분석하는 방법이다. 대상에 따라 멀티미디어 파일 분석과 문서 파일 분석이 있다. 멀티미디어 파일 분석은 데이터를 이미지/오디오/비디오 파일 등에 암호화해 숨기는 기술인 심층암호(Steganography)를 탐지하는 방법인데, 영상 분석, 색상 분석, 통계 분석 기법을 이용한다. 문서 파일 분석은 오피스 문서 등에서 많이 사용하는 문서 파일에 은닉한 데이터, 악성 코드 등을 탐지하는 방법으로, 포맷 분석, 저장 형식 분석 기법을 이용한다.

은닉된 데이터를 탐지하는 기법으로는 영상 분석, 색상 분석, 통계 분석, 포맷 분석, 저장 형식 분석 등을 이용하여 은닉 데이터를 탐지해내거나 데이터 은닉에 사용될 수 있는 영역을 검사하는 방법을 사용한다. 그림 3은 이미지 내에 비밀 데이터를 삽입할 수 있다는 것을 보여주는 사례이다.



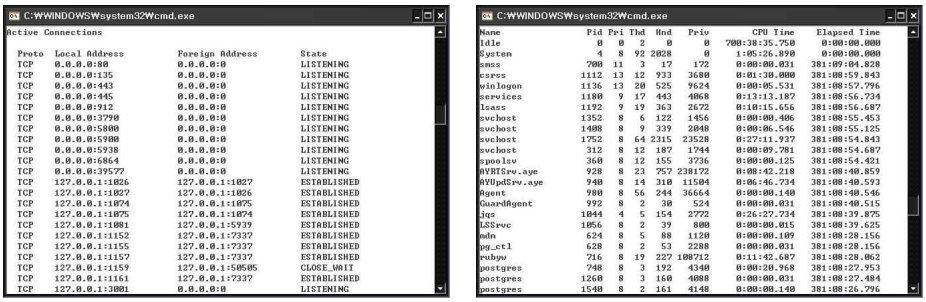
[그림 3] 이미지 내의 비밀 데이터

[Fig. 3] Secret data in an image

3.5 물리 메모리 분석 방안

휘발성 메모리 분석은 저장매체를 이용하지 않고 메모리 영역에서만 실행되는 기법과 그 흔적을 탐지하기 위한 방법이다. 이는 물리 메모리 영역은 일반적으로 완전삭제 프로그램의 영향을 받지 않는 것으로 알려져 있기 때문이다. 그림 4는 컴퓨터가 켜진 상태에서 수집할 수 있는 네트워크 포트 정보와 프로세스 정보이다.

메모리 관련 항목은 물리 메모리, 페이지 파일, 스왑(Swap) 파일, 하이버네이션 파일 (최대 절전 모드 파일) 등이 포함될 수 있고, 구체적인 추출 대상 항목은 운영체제 정보, 프로세스 정보, 네트워크 연결 정보, 로그인 정보, 메모리 내 텍스트 정보 등이 해당된다.



[그림 4] 네트워크 포트 리스트와 프로세스 리스트

[Fig. 4] Network port list & process list

3.6 기타 분석 방안

기타 분석 방법으로는 파일 내부의 시간 정보 분석, 일관성 분석, 연관 관계 분석 방법이 있다. 파일 내부의 시간 정보 분석은 어플리케이션의 의해 저장되는 파일 내부에 저장된 시간 정보를 분석하는 방법이고, 일관성 분석은 파일, 메타데이터, 로그 등의 정보를 활용하여 시간의 연속성에 따른 일관성을 분석하는 것이다. 연관 관계 분석은 확률 및 통계 기법을 적용하여 서로 다른 이벤트 사이의 연관 관계를 이용한 분석 방법이다.

4. 안티포렌식 대응 기술과 대응 절차

지금까지 살펴본 각 안티포렌식에 대해 대응하는 안티포렌식 대응 기술은 다음과 같다. 그림 5는 이들 사이의 대응 관계를 보여준다.

① 데이터를 삭제하거나 훼손하는 데이터 파괴는 데이터 복구 기법을 통하여 복구하는 것이 최선의 방법이고 이를 위하여 데이터 검색 및 탐지 기법을 적용한다.

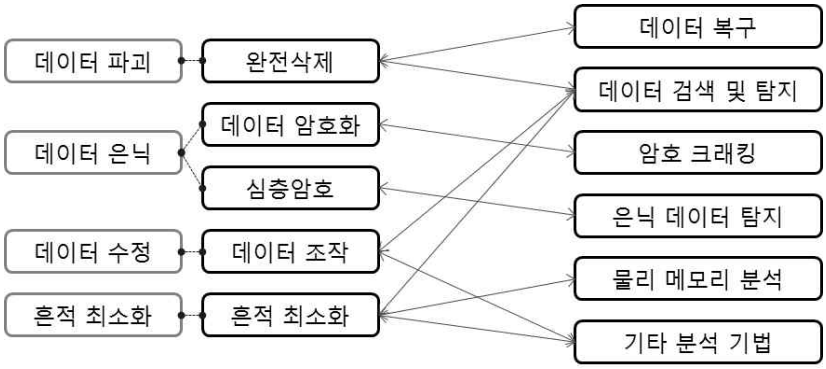
② 암호화를 적용하여 데이터 암호화하는 데이터 암호화는 암호 크래킹 기법을 적용하여 데이

터를 복호화할 수 있다.

③ 특정 파일에 중요 정보를 은닉하는 데이터 은닉은 유형에 따라 별도의 은닉 데이터 탐지 기법을 이용하여 중요 데이터를 추출할 수 있다.

④ 데이터를 수정 및 조작하여 분석이 어렵도록 처리하는 데이터 조작은 데이터 검색 및 탐지 기법을 적용하여 데이터 유무를 판단하고 기타 분석 기법을 사용하여 분석이 가능하다.

⑤ 사용한 안티포렌식 기법의 흔적을 제거하는 흔적 최소화에 대응하기 위해서는 안티포렌식 영향을 덜 받는 물리 메모리 분석 기법이 필요하고 기타 분석 기법을 사용한다.



[그림 5] 안티포렌식에 대응하는 안티포렌식 대응 기술

[Fig. 5] Anti-anti-forensics against anti-forensics

디지털 포렌식을 수행하기 위한 디지털 포렌식 조사 모델은 그림 6과 같이 여섯 단계로 구성되는데[1], 조사 및 분석 단계에서 데이터 분류 및 분석이 이루어진다.

[그림 6] 디지털 포렌식 조사 모델

[Fig. 6] Digital forensics investigation model

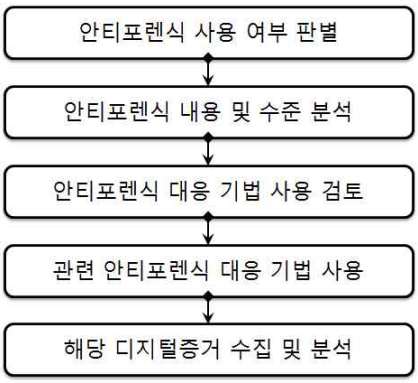
조사 및 분석 단계는 다시 데이터 추출, 데이터 분류, 상세 분석의 3단계로 구성되는데[1], 기존의 디지털 포렌식 절차는 안티포렌식에 대한 고려없이 구성되어 있으므로 이를 반영한 대응이 필요하다. 조사 및 분석 단계에서 안티포렌식을 함께 고려한 수정된 절차는 표 3과 같다.

[표 3] 수정된 조사 및 분석 단계

[Table 3] Modified investigation & analysis phase

단계	내용 및 특징
데이터 추출	• 조사를 필요한 데이터를 추출할 수 있도록 사본을 생성해서 수행 • 응용 프로그램 파일, 운영체제 사용 정보 등을 분석에 유용한 데이터를 추출 • **안티포렌식 사용 여부 확인**
데이터 분류	• 효과적인 분석과 소요 시간을 줄이기 위해 데이터를 특정 기준으로 분류 • 시간 흐름, 응용 프로그램 종류 등에 따라 데이터를 분류하고 결과 검토 • 안티포렌식 수준 확인 및 안티포렌식 대응 도구 사용 검토
상세 분석	• 분류된 데이터를 바탕으로 사건 유형에 맞게 본격적인 분석을 수행 • 인터넷 사용 흔적 분석, 사용자 활동 정보 분석, 시스템 사용 정보 분석, 응용 프로그램 사용 흔적 분석, 파일 분석 등 • **안티포렌식 대응 기법 사용을 통한 상세 분석**

안티포렌식을 고려한 경우 조사 및 분석 단계에 안티포렌식 도구에 대한 판별과 내용 및 수준 등을 반영하고 이에 대한 대응도 포함되어야 하므로 이를 고려한 세부 절차는 그림 7과 같다.



[그림 7] 안티포렌식을 고려한 절차 수정

[Fig. 7] A new procedure considering anti-forensics

3. 결론

최근 급증하는 해킹, 악성코드 등 사이버 범죄에 대응하기 위한 방안으로 디지털 포렌식이 다양하게 적용되고 있다. 그러나 이에 대항하기 위해 안티포렌식 기법들이 등장하여 디지털 포렌식을 방해하는 사례가 증가하고 있는 추세이고, 새로운 컴퓨팅 환경을 고려한 새로운 안티포렌식 기법들이 소개되고 있는 실정이다.

본 논문에서는 이러한 문제점을 인식하여 다양한 안티포렌식 기법을 분류하고 각각의 대응 방

안을 제시하였다. 또한, 포렌식 조사 모델에서 안티포렌식을 고려한 수사 절차 상의 수정 방안도 제안하였다. 본 논문은 향후 등장이 예상되는 안티포렌식 기술의 다양한 측면을 고려한 안티포렌식 대응 기술 개발에 도움이 될 것으로 판단한다.

References

[1] Sang-Jin Lee, Introduction to Digital Forensic, Eroon Press, Seoul **(2010)**.

[2] Young Sun Shim, "Incident Response Procedure using Digital Forensic Methods," Samsung SDS Journal of IT Services, **(2012)**, Vol.9 No.1, pp.128-141.

[3] http://blog.handlerdiaries.com/?p=363, Jan 29 **(2014)**.

[4] Simson Garfinkel, "Anti-Forensics: Techniques, Detection and Countermeasures," Proceedings of the 2nd International Conference on i-Warfare and Security, **(2007)** March 8-9; California, USA.

[5] Vincent Liu and Francis Brown, "Bleeding-Edge Anti-Forensics," Infosec World Conference & Expo, MIS Training Institute, **(2006)** Apr 3-5, Florida, USA.

[6] http://forensic-proof.com/archives/4689, Jan 21 **(2013)**.

[7] Noemi Kuncik and Andrew Harbison, "Counter forensics techniques - a brief overview," Grant Thornton Ireland, **(2010)**, Forensic & Investigation Services.

[8] http://www.nsrl.nist.gov/Downloads.htm, Aug 8 **(2014)**.

Authors

신원 (Shin, Weon)

2001년 8월 : 부경대학교 전자계산학과 이학박사 졸업
2002년 3월 ~ 2005년 1월 (주)안철수연구소 선임연구원
2005년 3월 ~ 현재 동명대학교 정보보호학과 전임강사, 조교수, 부교수
관심분야 : 소프트웨어 보안, 악성코드 확산, 디지털 포렌식