민간 디지털포렌식 업체의 데이터 유출방지

김 희 주
(성신여자대학교 융합보안공학과 학사 과정)
이 은 민
(성신여자대학교 융합보안공학과 학사 과정)

민간 디지털포렌식 업체의 데이터 유출방지

김희주**
이은민***

< 요 약 >

디지털 자료에 대한 중요도가 늘며 법정에서는 민간에서 분석한 디지털 증거가 채택되고 있다. 산업 기술 유출 범죄 발생 시 자체 디지털 포렌식 부서를 가지고 있는 대기업과 달리 중소기업은 민간 디지털 포렌식 업체에 기업의 정보를 맡겨야 한다. 디지털 포렌식은 디지털 기기에 저장되어 있는 모든 정보를 하나의 파일로 제작하여 분석하는 것이기에 포렌식을 진행하는 모든 데이터에 대해 열람이 가능하다. 기밀 문서의 저장 시점부터 암호화를 통한 데이터 보호 조치가 이루어지지 않으면 복구 과정에서의 정보 유출은 불가피하다. 따라서 미리 암호화를 진행하지 않은 파일의 포렌식을 진행할 경우 디지털 포렌식 과정에서 데이터에 대한 보호가 가능하도록 위탁 데이터 보호 시스템을 제안한다. 또한, 최근 발의된 '디지털포렌식 산업 육성 및 지원 법안 발의'와 관련하여 국가의 민간 디지털 포렌식에 대한 대처와 향후 민간 디지털 포렌식 업체가 나아가야 하는 방향성에 대해서도 추가적으로 논의하고자 한다.

주제어: 디지털 포렌식, 산업 기밀 유출, 개인 정보 보호, 포렌식 워터마킹, 암호화

** Undergraduated, Sungshin Women's University
*** Undergraduated, Sungshin Women's University

목 차

Ⅰ. 서론
Ⅱ. 관련 연구
Ⅲ. 위탁 데이터 보호 시스템
Ⅳ. 법적 개선방향
Ⅴ. 결론

Ⅰ. 서 론

디지털 포렌식이란 범죄사실을 규명하기 위해 디지털 데이터를 규정된 절차에 의해서 수집하고 분석 및 안전하게 보관하여 수사에 활용하는 과학수사 기법을 말한다. 정보화 시대로 인해 디지털 기기를 통한 데이터의 생성은 가속화되고 있는 범죄사실 또는 혐의를 입증하기 위한 디지털 증거의 중요성은 날로 증가하고 있는 상황이다.

<표 1> 2010년 - 2020년 디지털 증거분석 현황

구분	소계	컴퓨터 기기 (PC, 노트북 등)	디지털기기 (CCTV, 네비)	모바일기기 (스마트폰, 휴대폰)	파일/기타 (개인정보, DB 등)
'10년	6,247	3,664	276	1,611	496
'11년	7,288	3,356	479	3,352	201
'12년	10,426	3,830	393	5,870	333
'13년	11,200	3,138	483	7,332	247
'14년	14,899	3,079	510	10,656	654
'15년	24,295	3,357	712	19,526	700
'16년	32,281	3,923	794	26,408	1,156
'17년	36,060	4,198	867	30,238	757
'18년	45,103	6,239	1,065	36,986	813
'19년	56,440	7,259	1,412	46,551	1,182
'20년	63,953	9,113	1,557	52,479	786

※ 출처: 경찰청(2020)

경찰청의 디지털 포렌식 증거 분석 건수 통계 자료를 확인하면 3년간 경찰이 실시한 디지털 포렌식 분석 건수는 2018년 4만 5103건에서 2019년 5만 6440건, 2020년 6만 3935건으로 1년마다 대략 만 건씩 증가하고 있는 모습을 볼 수 있다. 이는 2010년 6247건이라는 수치와 비교했을 때 10배 이상 늘어난 것을 확인할 수 있다. 이를 통해 법적 증거로서의 디지털 포렌식 수요는 지속해서 증가하고 있으며, 개인 민간업체와 같은 소규모 사업장을 통한 디지털 포렌식 수요 역시 확대될 것으로 예측 가능하다.

(1) 수사기관에서의 위탁 데이터 보호 규제

경찰, 검찰과 같은 국가수사기관은 해당 기관의 신뢰성 아래 적법한 절차를 걸쳐 디지털 포렌식을 진행한다. 국가에서 진행되는 포렌식 과정은 전문성을 갖춘 증거분석관 아래 이루어져야 하며, 시행하는 디지털 포렌식은 수사목적을 달성하는 데 필요한 최소한의 범위에서 이루어져야 한다 (디지털 증거의 처리 등에 관한 규칙 제 9조). 디지털 증거를 압수・수색・검증할 경우에는 피의자 또는 변호인, 소유자, 소지자, 보관자의 참여를 보장하여 무결성을 보장한다(디지털 증거의 처리 등에 관한 규칙 제 13조). 또한 디지털 증거 수집 시 암호화 프로그램 사용을 의무화함으로써 디지털 포렌식 데이터의 유출을 방지하고 있다 (개인정보보호법 제29조). 분석이 종료되면 해당 개인정보는 삭제・폐기함으로써 수사 전 과정에서 개인정보를 보호하고 있다(디지털 증거의 처리 등한 관한 규칙 제 35조).

(2) 민간 디지털 포렌식 업체의 위탁 데이터 보호 방안에 대한 한계

디지털 기록의 중요성이 커짐에 따라 국내의 민사 사건에서는 형사 사건과 달리 민간 디지털 포렌식 업체에서 발급하는 포렌식 증명서가 증거로 채택되는 경우가 존재한다. 따라서 국내 대형 법률회사에서는 자체 민간 디지털 포렌식 운영을 통해 의뢰자들의 디지털 증거물을 제작해주며 다른 로펌과의 차별성을 강조한다. 하지만 민간 디지털 포렌식 업체에서 진행하는 디지털 포렌식 과정은 법적으로 규정되어 있지 않기 때문에 증거 무결성을 보장할 수 없고, 발급한 포렌식 분석 보고서와 감정서 또한 규격이 존재하지 않기에 확실한 증거 채택 여부는 불확실하다. 포렌식 과정에서 정보의 안전성 또한 보장할 수 없다. 민간 디지털 포렌식 업체에서는 CCTV와 보안 각서 유지 등을 통해 보안유지를 제공한다고 주장하지만 정보 통제 수단이 전무한 현 상황에서는 민간 데이터 포렌식 업체가 개인정보를 마음만 먹으면 열람 가능하

며 개인 정보 파기의 의무 또한 없기 때문에 포렌식을 시행한 데이터 파기 여부 또한 불분명하다.

실제로 국내의 사회고발 프로그램에서는 의뢰자의 개인정보를 따로 소장하거나 돈을 받고 판매한다는 동종 업계 관계자의 증언이 보도된 바 있다. 2019년 버닝썬 사건의 시초가 된 가수 정모씨의 카카오톡 기록은 2016년 정모씨의 휴대폰을 맡긴 민간 디지털 포렌식 업체에서 카카오톡 기록을 보관하고 있다가 3년 후에 공익적으로 제보한 것으로 추측되고 있다.

(3) 국제 디지털 포렌식 표준 가이드라인

현재 민간 디지털 포렌식 업체에 대한 법률을 제정한 국가는 없다. 다만 국제형사기구인 INTERPOL에서 제시한 국제표준 디지털 포렌식 랩 가이드라인과 ISO 17025와 같은 국제 디지털 포렌식 표준 가이드라인을 통해 안전한 디지털 포렌식을 위한 방향을 제시하고 있다. ISO 17025는 실험실의 운영과 관련된 업무절차 및 관리체계에 대한 국제표준이다. 해당 국제표준에서는 시설 및 환경, 장비, 데이터 및 정보관리 통제, 직원의 역량 등의 규제를 기술하고 있다. 따라서 국내 민간 포렌식 업체에서는 국내 공공기관인 KOLAS에서 진행하는 ISO 17025의 인증을 통해 업체의 신뢰성을 증명하고 있다. INTERPOL에서 제작한 국제표준 디지털 포렌식 랩 가이드라인은 ISO 17025와 다르게 디지털 포렌식에 초점을 맞추어 디지털 포렌식의 권고사항을 제시하고 있다. 하지만 ISO 17025와 INTERPOL의 가이드라인 두 가지 다 권고 사항일 뿐 강제적으로 지켜야 하는 법은 아니므로 디지털 포렌식의 정보 유출에 대해 규제하기는 어려울 것으로 사료된다.

(4) 민간 디지털 포렌식 업체에서의 산업 기술 정보 유출 시나리오

대기업이 아닌 중소 기업은 자체 포렌식 부서를 만들기는 힘들기 때문에 기술 유출 시 민간 포렌식 업체에 의뢰를 맡기는 경우가 많다. 민간 포렌식의 중요도가 늘어나며, 민간 포렌식 업체로 포렌식 의뢰를 했다가 산업 기밀이 유출되는 경우가 발생 가능하다. 민간 디지털 포렌식 업체에서 기술 유출이 일어날 수 있는 시나리오는 다음과 같다.

먼저 중소기업에서 기술 유출로 인해 피해를 입은 기업이 피해 사실을 입증하기 위해 자료 포렌식을 맡겼을 때, 민간 포렌식 업체에서 2차 유출을 하는 경우이다. 두 번째로는 중소 기업의 기술 관리자가 휴대폰과 같은 개인 전자기기 포렌식을 의뢰할 경우, 민간 포렌식 업체에서

저장되어 있는 기술을 유출하는 경우이다.

두 가지 모두 당사자는 기술이 어디서 유출되었는지 가늠하기 힘들고, 민간 디지털 포렌식 업체의 체계가 만들어져 있지 않기 때문에 유출에 대한 책임을 묻기도 어렵다.

II. 관련연구

포렌식 과정에서 정보 유출을 최소화하기 위해 제안된 소프트웨어적 데이터 보호 방안으로 블록체인 또는 클라우드 기반의 위탁 데이터 이력 관리 시스템[1]이 있다.

(1) 블록체인 기반

블록체인은 이전 블록에 새로운 블록이 연결되며 이전 블록에 저장된 데이터의 변조가 불가하므로 무결성을 보장한다는 특징이 있다. 따라서 블록체인을 통해 기기의 관련 정보들을 블록체인에 등록하고 관리하는 시스템을 도입한다면 개인이 위탁한 정보에 대한 무결성을 보장받을 수 있다. 민간 포렌식 업체에서는 위탁 데이터의 분석을 개시한 후, 이미징 파일의 업로드 시간, 분석 이미지 파일명, 분석자 ID, 업체명, 이미지 파일의 해시값 산출 후 이를 블록체인의 블록에 저장하게 된다. 분석 대상이 추가될 때마다 새로운 블록이 연결되기 때문에 분석 데이터에 대한 이력이 계속 남게 되므로 분석 담당자나 책임자에게 개인정보 처리자와 개인정보보호 책임자의 의무를 수행하도록 강제할 수 있다.

(2) 클라우드 기반

클라우드 기반의 위탁 데이터 이력 관리 시스템은 민간 업체에게 수정 권한을 제외한 읽기, 쓰기 권한만을 부여하고 클라우드 상의 DB에 분석 기기에 대한 정보를 등록한다. 이후 읽기, 쓰기를 시도할 때마다 태그 기록을 남기는 방식이다. 데이터 처리에 대한 이력을 태그 기록으로 남길 시 개인정보 처리자와 책임자가 각자의 책임을 이행하므로 최종적으로 데이터의 파기까지 입증이 가능하다.

(3) 한계점

기존 포렌식 과정은 복구하는 기기의 드라이브 파일을 모두 이미징하여 복구자의 컴퓨터에서 분석하는 방식이었다. 해당 과정은 대상 드라이브 파일을 손쉽게 다른 저장매체 저장할 수 있다. 분석 과정에서 의뢰자는 모르는 사이에 분석자가 대상자의 중요 파일을

열람하고, 이를 유포하는 것도 가능하다. 현재로서는 디지털 포렌식을 진행하기 위해 대상 드라이브의 이미징을 뜨는 과정이 필수이기 때문에, 해당 드라이브 내의 원하는 파일만 골라내어 유출을 막는 것 또한 불가능하다. 앞서 제안된 블록체인과 클라우드 기반 시스템 또한한 민감 정보 열람에 대한 기록을 남김으로써 데이터의 무결성, 책임소재 명확화 측면에서는 효과가 있을 수 있으나, 민감한 데이터를 타인이 열람하는 것을 원천적으로 방지할 수 없다. 블록체인과 클라우드를 통한 이력 관리 시스템은 데이터에 접근한 사람의 정보와 데이터의 무결성만을 보장하기 때문에 포렌식 복구 과정에서 분석 담당자 즉, 제 3자가 위탁된 데이터 중 사건과 무관한 데이터에 대한 열람을 막기엔 한계가 있다. 이는 포렌식 과정 중 해당 데이터나 파일을 열람해보기 전에는 저장된 데이터의 내용을 알 수 없으므로 일정 범위 안의 데이터는 모두 복구를 통해 열람하여 관련된 데이터를 디지털 증거로써 사용하기 때문이다. 따라서 해당 방법을 사용한다면 현재 문제가 되고 있는 민간 업체에서의 개인정보 유출에 대한 피해를 막는 것은 어려울 것으로 보인다.

앞서 내용을 종합하면, 민간 포렌식 업체에 위탁된 데이터는 법적인 규제를 통한 사후적 보호 수단만 존재할 뿐 근본적으로 데이터의 유출을 막는 사전적 보호 수단은 부재한 상황이다. 저자자는 사전에 데이터를 저장할 때 후킹과 마스킹을 통해 정보를 암호화하고 복호화하는 과정을 추가함으로써, 파일을 복구하더라도 분석자가 이를 열람할 수 없는 아이디어를 제시하고자 한다.

Ⅲ. 위탁 데이터 보호 시스템

(1) 후킹(Hooking)

후킹(Hooking)이란 운영체제(OS)가 어떤 코드를 실행하려고 할 때 이를 낚아채 다른 코드가 실행되게 하는 것을 뜻한다. 이때 실행되는 코드를 훅(Hook)이라 칭한다. 후킹은 windows에서 크게 사용자 모드(User Mode)와 커널 모드(Kernel Mode)로 나뉜다. 이렇게 분리되는 이유는 보안상의 이유가 가장 크다. 사용자 모드에서 쓰이는 메시지 후킹을 예로 후킹이 진행되는 전반적인 과정을 이해해보고자 한다.

윈도우 운영체제는 사용자에게 GUI(Graphic User Interface)를 제공하고 사용자는 이 GUI를 이용하여 원하는 동작을 한다. 동작에는 마우스를 움직이거나 클릭, 키보드 버튼을 누르는 등이 해당된다. 이러한 동작으로 이벤트로 발생시켜 운영체제는 그 이벤트에 적합한 메시지를 해당 응용 프로그램에게 전달하여 처리한다.

사용자의 특정 행위는 이벤트를 발생시키고 이벤트 발생은 OS로 하여금 응용 프로그램에게 관련 메시지들을 보낸다. 이때, 해당 메시지들은 OS Message Queue에 존재하고 있다. 운영체제는 해당 이벤트가 어느 응용프로그램에서 발생했는지 파악 후 큐에서 메시지를 꺼내 해당 응용프로그램의 메시지 큐에 전달한다. 그럼 해당 응용프로그램은 본인의 Application Message Queue에 추가된 메시지를 확인하고 해당 이벤트 핸들러를 호출한다. 이런 방식으로 윈도우 메시지를 전달하고 동작하며 이를 메시지 후킹이라 부른다.

(2) 데이터 마스킹(Data Masking)

데이터 마스킹(Data Masking)이란 민감한 데이터의 보호를 위해 만들어진 프로세스이다. 해당 민감 정보를 문자나 숫자와 같은 다른 가상의 값으로 변경함으로써 인가되지 않은 사용자나 해커가 사용할 수 없도록 한다. 따라서 데이터 마스킹은 기업이 제 3자에게 중요한 데이터를 공유할 때 유용하며, 민감 데이터를 변경하더라도 해당 데이터의 고유한 특성은 그래도 유지되는 특성을 지니고 있다.

Fig1에서의 데이터 이미징을 위해 데이터 마스킹 기법 종류 중 암호화(Encryption) 방법을 사용한다. 오직 키가 있는 인가된 사용자만이 암호화 상태의 데이터를 복호화할 수 있다. 암호화 방법으로는 Encase에서도 지원하는 AES-256을 따르며 무결성 검증을 위해 수집 파일의 MD5와 SHA-1 해쉬를 사용한다.

(3) 제안 프로그램

저자는 앞서 설명한 후킹과 데이터 마스킹 기술을 통해 민간 디지털 포렌식 업체에서 정보를 보호하기 위한 대책을 제안하고자 한다.

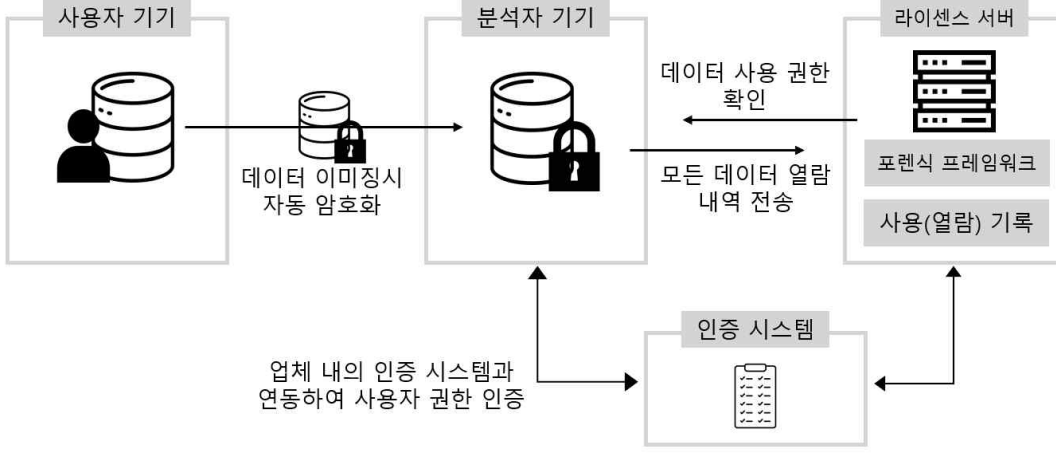

Fig1. 전체 플로우

제안하는 시스템의 전체적인 플로우는 Fig.1과 같다. 먼저 사용자의 데이터를 포렌식 담당 분석자 기기로 가져와 이미징 파일을 제작하는 과정에서 이미지 파일을 암호화한다. 이는 DRM(Digital Rights Management, 디지털 권리 관리)의 패키징 과정과 유사하다. 암호화 과정에서 기기 속 데이터가 불법 복제 및 유통되었을 때를 고려하여 해당 경로를 감지하기 위한 워터마킹도 함께 삽입된다. 워터마킹은 해당 업체를 식별할 수 있는 고유 사업자 번호로 한다.

앞서 언급한 DRM은 복구자가 데이터를 열람하기 위해 사전적으로 복호화 모듈이 단말기에 설치되어 있어야 한다는 불편함이 존재한다. 이에 반해 제안 시스템은 제어 알고리즘을 통해 복호화 모듈이 설치되어 있지 않더라도 암호화된 파일의 복호화가 가능하다. 동적으로 호출할 수 있는 복호화 모듈은 사용자 인증과 라이센스 정보를 발급받아 이미징한 데이터를 복호화 한다. 이때 사전에 설정한 키를 복호화 모듈에 가져오는 과정이 필요하다.

안전한 복호화 과정을 위해서는 인증 및 라이센스 절차가 선행되어야 한다. 인증 시스템의 인증 서버는 민간 디지털 포렌식 업체 내에서 해당 케이스 담당 분석자임을 인증하는 역할을 수행한다. 그 후 라이센스 서버를 통해 신뢰할 수 있는 기관으로부터 인증받은 업체인지, 의뢰자의 데이터를 절절한 절차에 따라 넘겨받았는지 등의 여부를 심사받고 이러한 절차에 통과하면 라이센스 정보를 획득한다. 라이센스 정보 안에는 데이터를 복호화하기 위한 키 정보가 들어있다. 복호화 키를 받아오면 정상적으로 데이터 사용 권한 확인을 받은 것이며 분석자 기기에서 데이터를 클릭했을 때 원본 데이터가 출력되게 된다. 또한, 포렌식 절차를 투명하게 하고 책임 소재를 명확히 하기 위해서 데이터에 접근 및 열람했던 기록들을 모두 라이센스 서버로 전송된다.

본래 암호화되어서 제안 프로그램 위에 올라온 이미징된 데이터로부터 원본 데이터를 출력하기 위해서는 제어 알고리즘이 필요하다. 제어 알고리즘은 어플리케이션 프로세스가 생성될 때 자동으로 dll 모듈이 로딩되도록 하는 기술(injection)과 로딩된 dll이 프로세스의 특정 메모리 영역을 변조하여 API 호출을 가로채는 기술(hooking), 이렇게 2가지 기술을 이용하여 구현된다.

우선 정상적으로 데이터를 읽어오기 위한 프로세스는 다음과 같다.

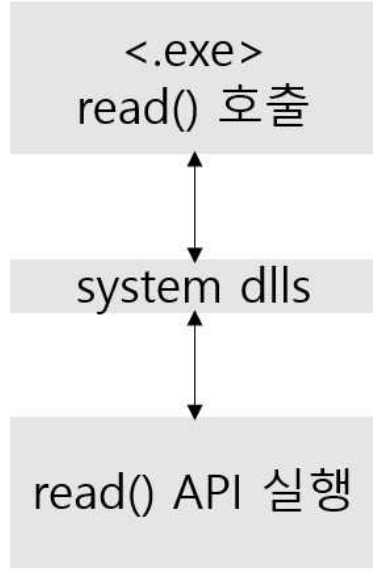

Fig2. 정상적인 API 호출

어플리케이션은 사용자(복구자)의 시스템 자원(데이터)을 사용하고자 시스템 커널에게 API(Application Programming Interface)를 이용하여 요청한다. Fig2에서도 그렇듯 이미징한 데이터 값을 프로그램에서 읽어오기 위해서 read() 함수를 요청하여 read() 함수에 해당하는 시스템 라이브러리(dll)가 로딩되고 알맞은 경로로 타고 들어가다가 커널 모드로 진입하여 요청한 함수를 실행시킬 수 있다.

반면 제안하는 제어 알고리즘의 프로세스는 다음과 같다.

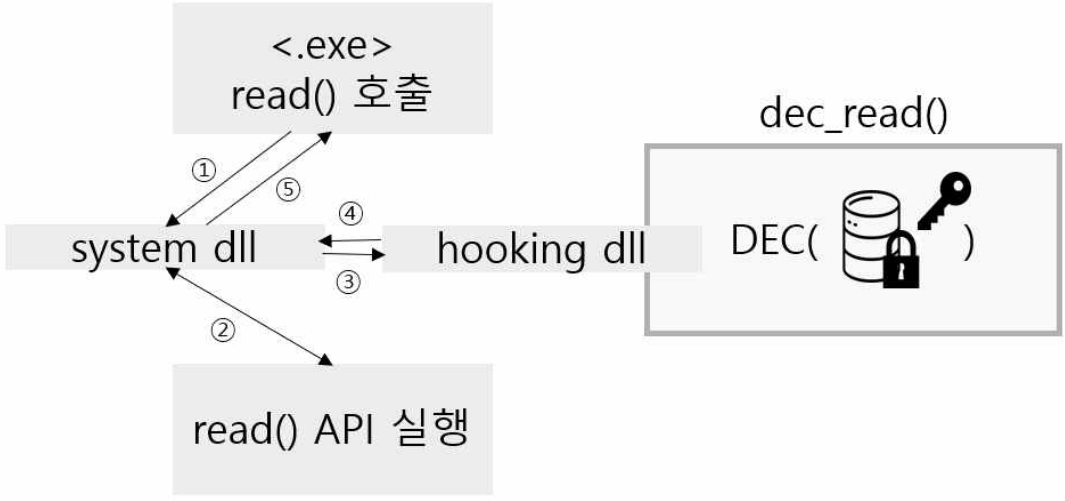

Fig2. 정상적인 API 호출

Fig3에서는 dll injection과 hooking을 이용한 제어 알고리즘으로 사용자 코드 실행 흐름을 변경한다. Fig1에 따라 인증 서버와 라이센스 서버로부터 정상적인 인증을 받고 데이터 접근 권한을 획득했을 때를 전제로 한다.

데이터 열람 이벤트가 발생하면 read() 함수가 호출되어 시스템 자원을 사용하기 위한 프로세스가 생성될 때 복호화할 수 있는 로직으로 가기 위한 라이브러리 함수(hooking dll)가 다른 원본 dll들과 함께 로딩된다. 이렇게 dll injection이 일어나고 난 뒤 로딩된 후킹 dll을 read() API를 실행 후 거쳐갈 수 있도록 하기 위한 작업을 수행한다. 프로세스 메모리에 로딩되어 있는 dll 코드에 read() API의 결과값을 내보내기 전 dec_read() 함수를 거치도록 하는 dll 함수 주소 값을 삽입한다. dec_read()에는 라이센스 서버로부터 받아온 키 값과 앞서 read() 함수로 불러온 암호화 상태의 데이터가 입력으로 들어가며 해당 함수가 바로 앞에서 언급한 동적 복호화 모듈을 의미한다. 결과적으로 제어 알고리즘의 목표인 암호화 되어 있는 데이터를 키와 결합해 복호화 상태의 리턴 값으로 가져오는 절차를 수행할 수 있다.

만약 적절한 인증과 허가를 받지 못해 복호화 키 값을 가지고 있지 않다면 dec_read 함수의 입력 값으로는 임의의 default의 값이 전달될 것이며 원하는 복호화 결과를 얻을 수 없게 된다.

Ⅳ. 법적 개선방향

(1) 디지털포렌식 산업 육성 및 지원 법안 발의

민간 디지털 포렌식 업체에서 발생할 수 있는 정보 유출을 방지하기 위해 국내에서는 2022년 9월 20일 조수진 국민의힘 의원이 '디지털포렌식산업 육성 및 지원에 관한 법률안'을 발의하였다. 해당 법률안은 늘어가는 디지털 포렌식 수요에 맞추어 국가가 직접 신기술 연구, 개발의 육성 및 지원에 앞장서기 위해 발의되었다. 발의된 법률안을 개괄적으로 살펴보면 다음과 같다.

우선, 디지털포렌식 산업 육청 추진을 위해 과학기술정보통신부장관(이하 과기정통부장관)은 3년마다 디지털포렌식산업 육성 기본 계획을 수립하고 실행해야 하며, 매년 해당 계획에 따라 실행 계획을 시행해야 한다. 국무총리 소속으로 디지털포렌식산업 육성위원회를 만들어 중요사항을 심의하고 과기정통부 장관은 디지털포렌식산업의 기술 개발을 위해 기술협력 및 인력, 정보 교류 사업을 추진하여야 한다. (안 제5조부터 8조까지)

다음으로 디지털 포렌식산업육성을 위해 국가에선 사업자의 관리와 처벌을 통해 국민에게 믿음과 수준 높은 서비스를 지원하여야 한다. 이를 위해 디지털포렌식사업자는 과기정통부장관의 허가를 받아야 하고, 결격이 있을 시 해당 사업을 할 수 없다 (안 제9조 및 제10조). 과기정통부 장관은 디지털포렌식 사업자가 부정한 방법으로 허가를 받거나 개인정보 보호 관련 법령을 위반할 경우, 허가를 취소하거나 영업 정지를 명할 수 있다 (안 제12조). 국가 및 지방자치단체는 재정 지원, 조세 감면, 창업 지원 등을 통해 디지털포렌식산업의 육성을 돕는다 (안 제13조부터 제 16조).

마지막으로 디지털포렌식산업의 기반을 조성하기 위해 국가에서 주도적으로 사업을 실시하는 법안을 제시하였다. 과기정통부장관은 디지털포렌식 산업의 육성을 위해 관계 중앙행정기관의 장과 협의하여 국내외 표준의 조사·연구·개발 등 표준화 사업을 추진할 수 있도록 한다(안 제17조). 또한 과기정통부장관은 디지털포렌식산업의 육성을 위하여 전문인력 양성 교육프로그램의 개발 및 보급, 양성기관 지원 등 전문인력의 양성에 힘써야 한다(안 제18조). 과학기술정보통신부장관은 디지털포렌식산업의 육성 정책의 수립·시행에 필요한 기초 자료를 확보하기 위하여 디지털포렌식산업 실태조사를 매년 실시하고, 그 결과를 공개해야 한다(안 제19조).

(2) 해당 법안의 문제점

현재 디지털포렌식산업 육성 및 지원에 관한 법률안은 소관위원회의 심사를 받고 있다.

하지만 과학기술정보통신보는 해당 제정안이 현행 「정보보호산업의 진흥에 관한 법률[1](이하 “정보보호산업법”이라 한다) 」의 “정보보호” 의미에 포함되므로 중복 입법의 우려가 있다는 의견을 내보이며 기존의 정보보호산업법에 디지털포렌식산업 육성 및 지원에 관한 법률안에서 제안한 내용을 반영해야 한다는 입장을 보이고 있다. (실제로 동 제정안과 현행 「정보보호산업법」을 비교하면, 제정안에서 디지털포렌식의 대상이 되는 “디지털기기나 인터넷에 있는 데이터”가 「정보보호산업법」에서 정보보호의 대상이 되는 정보에 포함된다는 점과, 제정안에서 “데이터를 수집·분석하여 범죄 또는 사고의 증거 등을 확보”하는 부분을 「정보보호산업법」 상 “정보의 수집 중에 발생할 수 있는 정보의 훼손, 변조 등을 복구”하는 부분과 유사하다고 볼 수 있다.)이 외에도 안 6조의 국무총리 육성위원회에 대해 중복된 위원회의 설치 지적, 안 제9조의 디지털포렌식사업자의 자격 검정은 높은 진입장벽 때문에 신규 사업자가 들어오기 힘들다는 과학기술정보통신부의 의견이 있었다.

이처럼 현재 디지털포렌식산업 육성 및 지원에 관한 법률안은 기존의 「정보보호산업법」과 겹치는 부분이 많고 과한 제재로 인해 실제 법안으로 채택되기는 어렵다고 보인다.

(3) 제안 사항

민간 디지털 업체에서 후킹과 마스킹을 통해 제3자가 데이터 파일을 열람하지 못하도록 하는 해당 방식은 물리적으로 데이터 유출을 막는 것임으로, 분석 기관이 해당 방식을 쓰지 않으면 물리적 유출을 방지할 수 없다. 현재 무엇보다 중요한 것은 민간 데이터 업체의 정보보호 결여에서 발생하는 포렌식 과정을 통해 이전된 개인정보 데이터 유출로 인한 이용자들의 불안감임으로, 기술의 발전에 앞서 법 제도의 마련이 시급하다고 보여진다.

현재 개인이 민간 디지털 포렌식 업체를 운영할 때 국가는 아무런 전문 사항도 요구하지 않는다. 의뢰자는 분석자의 양심에 의존하여 중요 정보의 분석을 의뢰하고 있다. 이를 방지하기 위해 국가에서는 민간 디지털 포렌식 업체를 운영하기 위한 최소 조건을 요구하며, 민간 디지털 업체를 국가에서 관리하고 업체마다 고유 번호를 부여해야 한다. 이를 통해 업체는 발급받은 번호를 디지털 포렌식 프로그램에 등록함으로써 디지털 포렌식을 실시할 때 책임을 질 수 있도록 한다. 프로그램을 사용하여 디지털 포렌식을 진행하는 내내 사진을 클릭하면 워터마크가 자동으로 표시되고, 이를 통해 업체가 임의로 정보의 사진을 찍어 유출할 경우 해당 업체를 추적하여 책임을 물 수 있다. 고유 번호 워터마크는 프로그램 밖으로 내보낼 때 키를 입력하여 없앨 수 있음으로 의뢰자는 복구 과정에서 정

보 유출에 대한 불안감을 덜고 안전한 디지털 포렌식 서비스를 제공받을 수 있다.

민간 디지털 업체를 국가에서 관리 및 감시하는 업무는 과학기술정보통신부에서 담당하도록 한다. 과학기술 및 정보통신 관련 중앙행정기관인 과학기술정보통신부는 과학기술 정책의 수립·총괄·조정·평가 및 과학기술 연구 개발 업무를 담당하고 있다. 따라서 과학기술정보통신부로 하여금 민간 디지털 포렌식 업체는 본 논문에서 제안하는 포렌식 프로그램처럼 암호화 기능을 충족하는 포렌식 프로그램 설치 여부 및 업데이트 현황을 확인하고 자격 미달의 업체에 대해서는 영업 중지 등의 제한을 가할 수 있는 권한을 부여한다. 또한 사전에 디지털 포렌식 업체의 개시는 등록제를 통해 최소 요구 조건을 법적으로 규정하여 이에 만족하는 기업에 한해 과기부에서 관리하도록 한다.

대형 로펌 사무실의 디지털 포렌식 부서와 같은 민간 포렌식 업체는 민사 소송 시 기기의 포렌식을 진행하여 증거 자료로 제출하고 있다. 하지만 증거 자료의 양식이 정해져 있지 않기 때문에 민간 디지털 포렌식 업체에서 제작된 증거의 효력은 판사의 증거능력 인정에 따라 달라진다. 따라서 민간 디지털 포렌식 업체를 이용해야만 하는 급박한 피해자들에게 도움을 주기 위해 민간 디지털 포렌식 업체를 이용하여 제작된 증거가 효력이 있을 수 있도록 증거 인정 요건에 맞게 해당 정보를 처리하도록 동일한 양식을 제작해야 할 필요성이 있다. 이를 통해 판사에게 증거의 적법함을 신속하고 자세하게 알려주며 증거 채택의 가능성 향상을 기대할 수 있다. 민간 디지털 포렌식 업체에서 디지털 포렌식을 진행할 때 포함해야 하는 증거 인정 요건은 다음과 같다.

증거 인정 요건

- 분석의 목적
- 의뢰자가 분석을 요구한 일시
- 분석의 시작 시간과 종료 시간
- 원본값과 해시값의 비교
- 디지털 포렌식을 진행한 기기
- 디지털 포렌식 의뢰자
- 포렌식 대상 기기 소유주와의 관계
- 포렌식 진행 시 해당 암호화 프로그램 사용 인증

- 분석 담당자의 전문성(자격증 및 이력) 인증

위의 내용을 포함하여 증거를 제작한다면 디지털포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집·분석 및 관리로 인해 증거의 무결성과 동일성을 입증 가능하다.

마지막으로 경찰의 “디지털 증거 수집 및 처리 등에 관한 규칙”, 검찰의 “디지털 증거의 수집·분석 및 관리 규정”과 같은 정보보호에 관련된 규정을 활용하여 민간 디지털 포렌식 업체에서 정보를 다루는 과정에 대한 법규를 제정할 필요성이 존재한다. 산업기밀 유출범죄의 경우 징역 15년 이하 혹은 15억원 이하의 처벌을 내리고 있다. 현재 아직까지 민간 디지털 포렌식 업체에서 정보 유출로 인한 피해 사례는 존재하지 않지만, 민간 디지털 포렌식 업체에서서 개인정보를 유출할 경우 해당 유출자를 엄히 처벌하는 법과 선례를를 제시하여 민간 업체 이용자들이 개개인 간의 신뢰가 아닌 법 아래 개인의 정보를 타인에게 맡길 수 있는 환경을 조성해야 한다.

Ⅴ. 결론

본 논문에서는 현재 증가하고 있는 민간 포렌식 디지털 업체의 수요에 비해 구체화 되어있지 않는 국내의 제도에 대해 검토하고, 도출된 문제점에 관한 법적, 기술적 개선방향을 제시하고 있다. 민간 포렌식 디지털 업체의 주요 쟁점은 주요 정보의 유출을 막을 기술적 방안이 전무하고, 국가에서 진행하는 디지털 포렌식과 다르게 법적 제재도 존재하지 않는다는 것이었다. 디지털 포렌식은 저장되어 있는 자료를 미리 볼 수 없음으로, 자료의 분석을 통해서는 파일을 일일히 검토해야 하기 때문에 해당 과정에서 정보의 유출 가능성이 있고 정보 유출 시 유출 사실을 추적하기 힘들며 강한 형량을 내리기 어렵다는 문제점이 있다.

본 논문에서 제안한 프로그램은 앞서 서술한 법적 기술적 한계로 일어나는 민간 디지털 포렌식 업체에서의 중소기업 기술 유출 문제해결을 목표로 한다. 해당 프로그램을 통해 저장된 데이터를 프로그램 상에서 암호화 및 복호화를 진행하며 데이터의 무단복제로 인한 유출을 막고 포렌식 워터마크를 통해 휴대폰으로 사진을 찍어 유출 시 범인 추적이 가능하다. 법적 측면에서는 처벌 강화 및 디지털 포렌식 민간업체 관련 등록제를 도입하여 보다 신뢰성 있는 민간 디지털 포렌식 업체 환경을 유지한다. 또한 2022년 9월 발의된 &디지털포렌식 산업 육성 및 지원 법안 발의&의 문제점에 대해 분석한 후 해당

법안이 앞으로 나아가야 할 실효성 있는 방향성을 제시하였다. 해당 법안에서 제시한 인증 요건과 처벌의 수위를 구체적으로 제시한 후 과학기술정보통신부장관 산하 민간 디지털 포렌식 업체를 관리하며 고유 번호를 부여함으로써 지속적인 기술의 지원과 업체의 효용성을 신뢰성을 증가시켜 늘어나는 디지털 포렌식의 수요에 효과적이고 안전하게 대응할 수 있다. 민사소송에서 민간 디지털 포렌식 업체가 분석한 디지털 증거 자료가 증거물로 채택이 될 수 있도록 기존의 디지털 포렌식 관련 법률과 국제 가이드라인을 참고하여 민간 디지털 포렌식 업체에서 분석한 증거도 인정받기 위한 공인 증명서를 제시하였다. 본 눈문은 현재 진행되고 있는 민간 포렌식 업체에서 발생 가능한 정보 유출 및 대응 방안에 대한 연구를 통해 증가하고 있는 민간 디지털 포렌식 수요의 실효성 있는 발전에 기여하고자 하였다. 디지털 정보의 생성은 현재 지속되고 있고 , 방대한 데이터의 양에서 분실된 중요 정보를 찾기위해 많은 이들이 민간 디지털 포렌식 업체를 방문할 것이다 . 안전한 디지털 포렌식 제공을 위해 디지털 포렌식 과정에서 정보 유출을 근본적으로 막을 수 있는 다양한 후속 연구들이 필요하다고 판단된다 .

참 고 문 헌

국내문헌

[1] 남기욱 and 이상진. (2021). 디지털 포렌식 사설 업체에 위탁된 데이터 보호 방안에 관한 연구 (디지털 포렌식 랩(시설)이 구비해야 할 요건 제시). 디지털포렌식연구, 15(1), 12-25.

[2] 권양섭. (2021). 한국형 디지털포렌식 수사절차 및 검증체계 구축방안. 디지털포렌식연구, 15(1), 67-82.

[3] 홍표길 and 김도현. (2021). 이동식 저장매체의 은닉 영역에 대한 안티 포렌식 대응 기술 연구. 디지털포렌식연구, 15(3), 72-84.

기타

경찰청 (2021. 09. 29). “디지털증거분석 현황”. https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1025&q_bbscttSn=20210929074259890&q_tab=&q_code=005015&q_detailCode=&q_searchKeyTy=&q_searchVal=%EB%94%94%EC%A7%80%ED%84%B8%EC%A6%9D%EA%B1%B0%EB%B6%84%EC%84%9D&q_rowPerPage=10&q_currPage=2&q_sortName=&q_sortOrder=& (검색일자: 2023. 04. 11)

【Abstract】

Prevention of data leakage by private digital forensics firms

Kim, Hee-Joo*
Lee, Eun-Min**

The importance of digital data has been increasing, and in legal proceedings, digitally analyzed evidence from private sources is being adopted. Unlike large corporations that have their own in-house digital forensics departments, small and medium-sized enterprises (SMEs) have to rely on private digital forensics firms to handle their corporate information. Digital forensics involves creating a single file from all the information stored on a person's digital devices for analysis, making it possible to access all the data involved in the forensic process. If encryption and data protection measures are not implemented from the moment confidential documents are stored, the risk of information leakage becomes unavoidable during the recovery process. Therefore, I propose the implementation of a delegated data protection system to ensure data security during the digital forensics of files that were not encrypted in advance. Furthermore, I would like to discuss the recent proposal of the "Digital Forensics Industry Promotion and Support Act" and additional considerations regarding how the country should handle private digital forensics and the future direction that private digital forensics firms should pursue.

Key Words: Digital forensics, Industrial espionage, Personal data protection, Forensic watermarking, Encryption

* Undergraduated, Sungshin Women's University
** Undergraduated, Sungshin Women's University