Report

‘디지털 흔적’을 수사하는 ‘디지털 포렌식’

디지털 포렌식의 사례, 절차, 단점을 중심으로

과목명 : Forensic 기법 및 Evidence 이론

담당교수 : 최연준

전공 : 경영학과

학번 : 20180494

이름 : 김지원

목차

Ⅰ. 서론

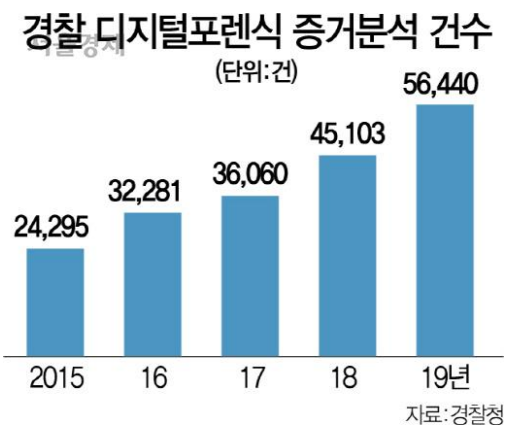
1. 주제 및 주제선정이유

오늘날 범죄는 살인 같은 잔혹한 범죄 뿐만 아니라 그 밖의 범죄들도 사회변화와 함께 점점 지능화, 광역화 되어가는 중이다. 범죄가 남긴 흔적은 유/무형의 결과물이자 인간의 행동이기 때문에 사회적 징표를 남기면서 필연적인 자연현상을 수반한다. 프랑스의 법학자 에드몽 로카르의 "모든 접촉은 증거를 남긴다."의 의미와 일맥상통하다. 즉, 디지털 범죄는 '디지털 흔적'을 남겨 디지털 기기 사용시 저장장치에 '흔적'이 남는다. 그리고 이러한 '디지털 흔적'이 최첨단 범죄 등의 실마리를 푸는 역할을 한다.

우리나라에서 유명한 미국 드라마 제목인 CSI의 의미를 아는가? CSI는 범죄현장수사, Crime Scene Investigation의 약자이며, 범죄에 대한 증거를 수집하기 위해 최첨단 장비를 사용하여 과학적 분석으로 미궁의 사건을 해결하는 수사를 의미한다. 우리는 해당 드라마를 통해 포렌식의 개념을 친근하게 접할 수 있었다. CSI에 나올 법한 미궁에 빠진 사건들 뿐만 아니라 스마트 기기 사용량이 늘어나는 오늘날에는 디지털 감식과 범죄 증거 확보가 중요하기에 과학수사도 디지털 포렌식으로 확장되었다. 이슈가 된 사건들 중에서 정준영의 '버닝썬' 사건은 디지털 포렌식 수사기법을 활용해 치부를 밝혀낸 바 있으며 이에 따라 본인은 디지털 포렌식이 어떠한 특징을 갖는지, 어떠한 수사절차와 원칙을 적용하여 법정에서 증거로 채택되는지 살펴보고 디지털 포렌식이 범죄 수사에 어떻게 활용되었는지, 그리고 심화하여 어떠한 허점을 가지고 있는지 알아보고자 본 레포트를 작성한다.

Ⅱ. 본론

1. 디지털 포렌식이란?

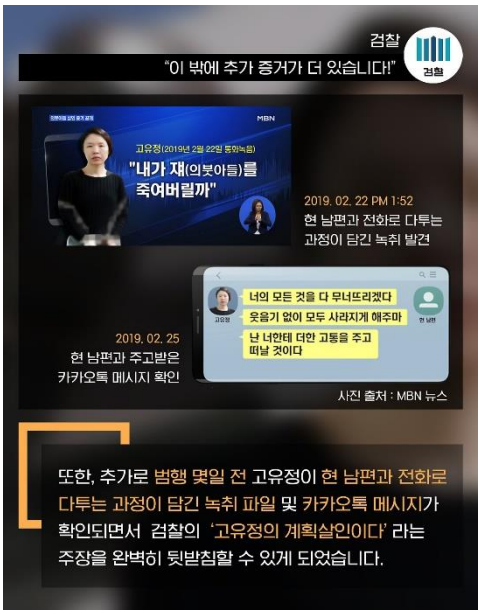


디지털 포렌식은 디지털 시대의 명탐정이다. PC나 노트북, 휴대전화 등 각종 저장매체 또는 인터넷상에 남아 있는 각종 디지털 정보를 분석하여 범죄 단서를 찾는 수사기법을 의미하며 디지털 증거의 의미를 해석하기 때문에 범죄 수법을 추론하는 역할을 한다. 오늘날 수사 영역에서 디지털 포렌식의 수요가 급증하고 있는 추세이고, 일반 기업에서도 디지털 포렌식 활용이 늘어나고 있다.

디지털 포렌식은 특정 제품은 포렌식이 불가하다는 속설이 있는 반면, 사용자가 어떻게 설정했느냐, 특정 제품에 따라 달라지기 때문에 확실한 대답이 불가하며 상대적이라는 특징이 있다. 두번째, 전자레인지에 돌리면 증거가 인멸될까? 정답은 없다. 이도 마찬가지로 상대적인 질문이다. 금속으로 이뤄진 제품은 전자레인지에 돌리면 불꽃도 튀고, 손상이 되기에 그런 반응을 하는 물질을 넣는다면 문제가 생길 수 있다. 하지만, 데이터가 들어있는 칩이 손상되지 않고 유용한 증거가 나온다면 복구가 가능하다. 세번째, 10년 전 자료도 복구가 되는지에 대한 의문이다. 지문이나 DNA는 환경적 요인에 따라 멸실이 되고 이처럼 디지털 증거도 물론 물리적 영향을 받을 수 있지만 물리적인 손상 없이 잘 보관만 된다면 사실상 영구불변의 보존력을 가지고 있기 때문에 큰 장점을 가지고 있다.

2. 디지털 포렌식 활용 사례

(1) 고유정 살인 사건



지난해 남편과 의붓아들을 잔인하게 살해하고 시신을 훼손한 일이 고유정 사건으로 세상에 공개되었다. 디지털 포렌식을 통해 경찰은 고유정이 제주-완도행 여객선 탑승후기 블로그를 확인 한 것, 카카오톡 메신저에서 의붓아들의 친모와 가족 3인의 프로필을 삭제한 것, 스마트폰에 자동녹음 된 전화내역을 증거로 수집하였다. 수집한 증거 중 녹취기록에서 현남편과 전화로 다투는 과정에서 "내가 쟤(의붓아들)을 죽여버릴까" 라고 말한 것, 카카오톡에서 남편에게 "모두 사라지게 해주마", "난 너한테 더한 고통을 주고 떠날 것이다"라고 주고받은 메시지를 확인하였다. 해당 증거를 통해 검찰은 고유정의 계획적 살인이라는 주장을 완벽히 뒷받침할 수 있었다.

(2) 데이트 폭력

지난 25일에는 데이트 폭력이 흉악범죄로 이어져 "헤어지자"는 여자친구를 잔인하게 살해한 20대 남성에게 중형이 선고되었다. 피의자는 조사 과정에서 "이성 문제로 다툼이 있었고, 이에 우발적으로 살해하게 됐다" 며 억울함을 호소했으나 디지털 포렌식 수사 결과 범행 전 온라인에서 '살인 안 들키는 법' 등 입에 담기 어려운 말을 검색한 것이 밝혀져 가중양형이 적용됐다. 해당 사건은 검색기록을 디지털 포렌식 하여 범죄의 단서를 얻을 수 있었는데, 일반적으로는 데이트 폭력 관련한 카카오톡이나 사진, 동영상이 증거자료로 활용된다. 하지만 데이트 폭력과 관련한 내용이 들어있는 카톡 대화내용이나 사진, 영상 등을 스스로 삭제하거나 상대의 억압에 의해 삭제하는 경우가 있어 주의를 요한다.

(3) 딥페이크

2018년, 약 8천 개의 딥 페이크 영상이 발견될 정도로 딥 페이크 영상 생성이 점점 증가하고 있다. 연예인 영상, 대통령의 얼굴을 합성한 가짜뉴스 영상 등 사회에 혼란을 야기한 다양한 사건에 악용하는 것이다. N번방 사건 또한 딥 페이크를 악용한 사진이 유포되었다. 이에 법무부는 딥 페이크 처벌 강화법을 국회 본회의에 통과시켰으며, 해당 법안에 따르면 딥 페이크 포르노를 제작 및 배포한 자는 5년 이하의 징역 혹은 5천만 원 이하의 벌금형을 선고받는다. 영리 목적이었다면 가중 처벌을 받기에 이 경우 7년 이하의 징역에 처해질 수도 있다. 디지털 포렌식은 이러한 딥 페이크 악용여부를 판단하는 대표적인 기술로, 악용이 의심되는 영상을 탐지하고 위·변조 여부를 판별하여 사건의 스모킹 건을 찾아낸다.

(4) 보이스피싱

지난 8월, 코로나로 인해 2차긴급재난지원금 지급가능성이 높아지면서 1차지급 때 발생했던 보이스피싱 등의 금융범죄가 다시 증가하였다. 가족을 사칭한 뒤 휴대폰이 망가져 전화를 할 수 없다는 핑계를 대고 카카오톡으로 연락하여 금액을 요구하거나 악성 URL을 클릭하도록 유인하는 메시지를 보내기도 한다. 때때로는 보이스피싱에 연루되기도 하는데 그러한 경우 범죄의사가 없었음을 입증하기 위해서 보이스피싱 직원과 했던 대화를 분석하고 위/변조가 일어나지 않았다는 것을 활용하여 자신의 무죄를 입증할 수 있다.

2. 디지털 포렌식의 수사 절차

(1) Preliminaries

어떤 기업에서 일어난 범죄 행위를 수사한다고 가정해보자. 당연히 기업에 있는 컴퓨터나, 전자기기에 대한 디지털 포렌식을 진행하게 될 것이다. 이를 위해 사전 준비를 해야 한다. 디지털 기기의 압수수색을 위한 영장을 준비하고 피 조사 대상에 대한 규모 등을 파악하여 자료 수집을 위해 필요한 인원이나 수집할 자료에 대한 우선순위를 정한 뒤, 필요한 증거수집 장비들을 준비한다.

(2) Collection

준비를 마쳤으면 증거수집을 위한 절차를 거친다. 현장에 도착하면 증거가 훼손됨을 방지하기 위해 폴리스 라인으로 현장을 통제하고 보존한다. 이후, 본격적으로 조사 대상이 될 디지털 기기들을 확보해야 하는데 가장 먼저 휘발성 데이터를 확보해야 한다. 휘발성 데이터는 전원공급이 끊기거나 시간이 지나면 사라지는 데이터이다. 예를 들어, 현재실행중인 파일이나 프로세스 리스트, 현재 네트워크 연결상태, 접속중인 사용자 목록이 이에 해당된다. 이러한 데이터들은 굉장히 중요하지만 시간의 흐름에 따라 변할 수 있기에 빠른 확보가 중요하다. 휘발성 데이터를 수집하는데, 시스템의 전원이 꺼져 있다면 시스템 자체를 확보하기도 하고 전원이 켜져 있을 경우 이미지 획득이 가능한 경우에 물리메모리와 가상메모리를 수집한다. 여기서 말하는 이미지는 데이터 전체를 하나의 파일로 만드는 것을 의미한다. 메모리 자체를 하나의 파일로 만드는 것이다. 이미지 획득이 불가능한 경우에는 그 자리에서 증거를 수집해야 한다. 시스템의 기본정보, 네트워크 정보, 실행중인 프로세스 정보, 마지막으로 비휘발성 데이터를 수집한다. 디지털 기기를 그대로 압수하여 확보할 수 있지만, 굳이 원본을 확보할 필요가 없을 때에는 사본 이미지를 만들 수 있다.

(3) Analysis

모든 증거물을 확보했다면 증거물을 안전하게 포장하고 밀봉한 후 분석실로 가져간다. 분석에 앞서 원본의 훼손을 방지하기 위해 획득한 디지털 기기들을 Opentext Inc. TX1같은 장비를 활용해 디스크 이미징 시킨다. 이와 같은 장비들의 동작 방식은 ssd를 이미징 한다고 가정하에, 한쪽에는 이미징 할 SSD를 장착하고 다른 한쪽에는 데이터를 저장할 하드디스크를 장착한다. 그러면 SSD에 있는 데이터들이 이미징되어 하드디스크에 그대로 들어간다. 이때 원본 SSD를 그대로 분석하면 원본이 훼손될 수 있기에 디스크를 이미징하여 분석하는 것이다. 이미징한 데이터에서 사건에 필요한 증거를 찾기 위해 Opentext 사의 Encase, Accessdata의 FTK를 사용한다. 오늘날에는 PC카톡을 분석해주는 MAGNET AXIOM 3.6도 뜨고 있다. 이제 데이터 분류작업을 통해 조사에 필요한 데이터를 선별한다. 그래야 더 효율적이고

빠르게 증거 분석이 가능하다. ARTIFACT, 시스템이나 어플리케이션이 자동으로 생성한 사용자의 흔적의 데이터 복구를 수행해야한다. 용의자가 데이터를 삭제했을 가능성이 있거나 복구가 필요하다고 판단하는 경우 진행한다. 일반적으로 아는 파일복구와 포렌식의 복구는 다르다. 일반적 복구는 온전하게 복구해야 하지만, 포렌식의 복구는 온전하게 복구가 되던 안되던 간에 증거물로 사용할 부분만 복구하거나 증거물의 가치만 존재하면 된다.

(4) Create Report -> (5) Submit to court

범죄 증거를 찾았다면, 혹은 찾지 못했다면 이에 대한 보고서를 작성해야 한다. 무엇을 분석, 어떻게 분석했는지 행동을 객관적이고 명확하게 기록하며 전문적 용어보다는 쉬운 용어로 작성하여 법정에 제출한다.

3. 디지털 포렌식의 단점

(1) 개인정보 유출의 위험

디지털 포렌식 시장이 커진 이후, 디지털 포렌식의 단점도 그만큼 부각되고 있다. 포털 검색창에 포렌식과 연관된 단어를 검색하면, 백 여개의 포렌식 업체를 찾아볼 수 있다. 높은 수준은 아니지만 스마트폰 복원과 관련된 개방 소프트웨어도 찾을 수 있다. 주부 A씨는 자신의 핸드폰을 한 사설 포렌식 업체에 맡기게 되었다. 하지만, 업체 담당자가 돌변하더니, 외도가 의심되는 문자를 지인들에게 유포하겠다는 협박을 받아 곤욕을 치렀다. 신분증을 확인하거나 다른 인증 절차를 거치는 업체의 경우도 있었지만, 지인이나 가족이라 얼버무려도 남의 스마트폰이나 컴퓨터를 복원업체가 적지 않기에 걱정되는 점이 크다. 이처럼, 사설업체가 요청된 개인 정보를 안전하게 보호하는지, 직원이 해코지나 협박을 하지 않는지에 대해 불안하다는 시각이 많다. 이에 대해, 권양섭 '한국 디지털 포렌식 학회' 이사는 개인정보가 아무리 문제가 있더라도 불법으로 가로챈 자료를 바탕으로 협박하는 것은 증거능력이 없으며, 관련 업계 윤리 규정자체가 전무한데다 영세업체가 대부분이기에 법적제재를 가하기 힘든 사각지대에 놓여있다고 말했다.

(2) 법관이 자유심증주의로 판단한 증거의 '증명력' 문제

디지털 증거는 디지털 포렌식을 통해 수집되어, 법적으로 증거의 가치를 인정받기 위해 기본적으로 형사소송법 등에 디지털 증거가 포섭되어야 한다. 포렌식에서는 증거를 찾는 것 만큼 중요한 것이 증거를 찾는 방식이다. 포렌식에서 얻은 증거가 법정 효력을 갖기 위해서 적법한 절차를 준수하여 정당하게 증거를 획득하는 정당성의 원칙, 데이터가 위/변조 되지 않고 정확한 데이터를 유지하는 무결성의 원칙, 증거 획득 과정에서 지체 없이 신속하게 진행되는 신속성의 원칙, 똑같은 환경에서 똑같은 조건과 똑같은

과정으로 재현할 경우 결과가 항상 동일한 재현의 원칙, 마지막으로 모든 과정에 대해 해당 증거물이 어떠한 변경도 발생하지 않았다는 것에 대해 보장하고 과정에 대한 추적이 가능해야 하는 연계보완성의 5원칙을 따라야한다.

그러나, 위법 수집 증거 및 전문증거 배제 법칙 등 분석조사 과정에서 객관적이고 엄격한 요건에 따라 판단되는 증거의 증거능력이 인정되었더라도 증명력 판단은 법관의 자유로운 심증에만 맡겨져 있어 '증명력'에 문제가 있다고 판단하면 해당 증거를 기각할 수 밖에 없다. 자유심증주의는 법관의 판단에 맡긴다는 의미가 아닌 법관의 판단에 법이 간섭할 수 없음을 의미한다. 유죄 판결을 내리기 위해 필요한 '합리적 의심을 배제' 할 정도의 증명력에 대한 법관의 심증의 정도와 심증 형성 기준에 대해 보편타당하고 구체적인 방법론이 마련되어야 한다.

Ⅲ. 결론

오늘날 정보통신 및 디지털 기기 확장과 동시에 수집되는 디지털 증거가 증가함에 따라 범죄 수사에 있어서 디지털 포렌식의 중요성은 더욱 부각되고 있다. 앞서 말한 '고유정' 사건과 'N번방' 사건은 최근 디지털 포렌식을 활용한 대표적인 사례로 꼽히고 있다. 디지털 포렌식을 활용하여 증거가 될 만한 자료들을 수집하였지만, 증거로 채택되지 못한다면 완벽한 검거를 하지 못하였을 것이다. 그만큼 우수한 디지털 포렌식 기술 뿐만 아니라 수집된 디지털 증거가 법적으로 인정받을 수 있는 요건들을 충족하는 것이 중요하다. 디지털 포렌식만으로는 아무 의미도 존재하지 않을 것이다. 즉, 범죄수사의 특성상 과학적 기술 외에도 법적/ 제도적 측면들이 함께 고려되어야 한다. 앞서 말한 디지털 포렌식의 특징(매체독립성, 무체정보성, 복제용이성, 비가독성, 대량성 등)을 잘 살리고, 5대 원칙의 적법한 절차를 거쳐 수집한 증거의 가치를 완전하게 보존하여 법정에 제출할 필요가 있다. 마지막으로, 위에서 말했던 개인정보 유출의 문제, 자유심증주의로 인해 '증명력'을 인정 받지 못하는 문제를 최소화하기 위해서 관련 법안을 만들기 위해 힘 쓸 필요가 있으며 디지털 기술은 매우 빠르게 진화하고 있기에 필자는 필요한 디지털 포렌식 수집 및 분석 도구에 대한 정부의 기술적 지원도 함께 이루어졌으면 하는 바람이다.

Ⅳ. 참고문헌

2015, 임정완, 살인사건 수사에서의 디지털 포렌식 활용방안에 관한 연구
https://www.youtube.com/watch?v=s44bCPjESDA

디지털타임스, 신종흥, 2015.08.24, http://www.dt.co.kr/contents.html?article_no=2015082502102251607001

아시아경제, 2020.07.29, 경찰, '디지털포렌식' 수사 규정 싹 바꾼다,
https://www.asiae.co.kr/article/2020072911284405796

고려대학교 정보보호대학원, 임종인, 디지털 포렌식 활용사례 및 발전전망

광병선, 2011.11.05, 디지털 포렌식 수사의 문제점과 개선방안

황현석 ,디지털 증거 압수·수색에 관한 디지털 포렌식 수사 관점의 고찰

한국디지털정책학회, 2015, 오세연, 사이버범죄의 대응강화를 위한 디지털 포렌식 수사 활용방안

뉴스워커 , 2020.11.27, 급증하는 데이트 폭력 해법은…디지털 포렌식으로 피해사실 입증하는 KDFT 한국 디지털 포렌식 기술표준원㈜. http://www.newsworker.co.kr/news/articleView.html?idxno=93565

뉴스워커, 2020.11.16, “딥페이크 사진·영상 가려낸다”…디지털 포렌식의 범용화에 앞장서는 KDFT 한국 디지털 포렌식 기술표준원㈜, http://www.newsworker.co.kr/news/articleView.html?idxno=91029

매일경제, 박수호, 2019.04.15, https://www.mk.co.kr/news/business/view/2019/04/230324/

경기대학교, 김민수, 2018.08, 디지털 포렌식 증거 채택 기준의 한계와 개선 방안