creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

이학석사 학위논문

디지털 증거의 특성을 고려한 압수수색방안 제안

2021년 1월

서울대학교 융합과학기술대학원

수리정보학과 디지털포렌식 전공

이 지 연

디지털 증거의 특성을 고려한 압수수색방안 제안

지도교수 이 병 영

이 논문을 이학석사 학위논문으로 제출함

2020년 12월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

이 지 연

이 지 연의 석사 학위논문을 인준함

2021년 1월

위 원 장	안 정 호	(인)
부 위 원 장	이 병 영	(인)
위 원	김 판 기	(인)

국문초록

압수수색영장 실무 및 법원의 증거능력과 관련된 현재 판례는 디지털 증거의 특성을 고려하지 않은 채 선별 압수수색의 원칙을 엄격하게 적용하고 있다.

예외적으로 저장매체 자체의 압수 또는 저장매체 전체의 이미징을 통해 수사기관으로 반출된 증거의 경우에도 이를 선별 또는 분석하는 과정에 피압수자 등의 참여권 보장을 엄격하게 요구하고 있어 디지털 증거가 증거로 사용되는 요건을 매우 제한적으로 좁혀 놓았다.

이에 따라 초기에 확보해야 할 디지털 증거는 흔적도 없이 사라지게 되고, 실체적 진실 발견을 위해 수사기관은 더욱 많은 시간과 비용을 들여야 하며, 상당한 시간이 소요되는 선별·분석과정에서의 참여권 보장은 그 제도의 정당성에도 불구하고 현실적으로는 피압수자 및 수사기관 모두에게 부담을 안겨주었고, 수사기밀의 유출 위험, 참여권 남용 등 많은 실무적 문제점들을 야기하였다.

이는 결과적으로 형사사법의 근간을 흔들고, 억울한 피해자를 양산하며, 사법제도에 대한 불신으로 이어질 수 있다. 이러한 실무상의 문제점을 해결하기 위해 본고에서는 디지털 증거의 특성을 고려한 압수수색방안을 제안해 보고자 한다.

우선 1단계로 현행 영장 실무에 따라 사용자가 작성한 문서, 메시지 등의 경우에는 현재와 같이 키워드 검색 등을 통해 범죄와 관련성이 인정되는 정보를 수집하고, 컴퓨터 생성 정보의 경우 디지털 증거의 진정 성립 입증에 필요한 증거인 간접증거로 보아 관련성의 범위를 보다 넓게 인정하여 컴퓨터 생성 증거 전체를 현장에서 이미징하여 함께 압수수색하는 방안이다.

다음으로 이와 같은 선별 압수수색과 더불어 저장매체 전체 이미지에 대하여 물리 이미징을 한 뒤 공개키로 암호화하여 신뢰계산 기술을 활용한 블랙박스 안에 저장하는 2단계 압수수색방안을 제안한다.

현장에서의 선별 압수수색만으로는 수사 및 재판 과정에서 추가 증거 확보가 필요함에도 이를 확보하기 어렵고, 은닉·삭제된 증거를 발견·복구하기 어려우며, 키워드 검색만으로는 관련성 있는 증거의 검출이 상당 부분 누락될 수 있으므로, 저장매체 전체의 물리 이미지를 확보할 필요성이 존재한다.

신뢰계산 기술을 활용한 블랙박스 안에 암호화된 상태로 보관되는 디지털 증거는 누구도 접근할 수 없고, 추가로 필요한 증거가 생기는 경우 담당 수사관이 이를 추출할 수 있는 계산 프로그램 및 이와 같은 증거의 필요성 등을 소명하면 담당 검사가 이를 확인한 뒤 승인하고, 해당 증거만을 비밀키로 복호화 시켜 증거로 사용하는 방안이다. 이와 같은 일련의 절차를 독립적인 제3의 검증기관에서 사후적으로 검증한다면 그 신뢰성을 보완할 수 있을 것이다.

신뢰계산 기술 방법은 Intel사의 Software Guard Extention과 같이 실무에서 이미 사용되고 있는 기술로, 동형암호에 비해 적은 시간과 비용으로 바로 구현 및 적용할 수 있다는 장점이 있다.

이와 같은 2단계 압수수색방안에 따르면 수사 초기에 확보할 수 있는 디지털 증거를 모두 확보하되, 피압수자의 개인정보를 보호하고, 사생활의 비밀 등 기본권 침해 가능성을 낮출 수 있으므로, 실체적 진실의 발견과 적법절차의 원칙 모두를 조화롭게 구현할 수 있을 것으로 예상된다.

주요어 : 디지털 증거, 선별 압수수색, 신뢰계산 기술, 관련성, 컴퓨터 생성 증거, 디지털 증거의 진정 성립, 참여권
학 번 : 2019-29478

목 차

제 1 장 서론 ····· 1

제 1 절 연구배경 ····· 1

제 2 절 연구방법 ····· 2

제 2 장 디지털 증거의 증거능력 ····· 3

제 1 절 디지털 증거의 의의 및 특성 ····· 3

제 2 절 디지털 증거의 무결성과 동일성 확보 ····· 5

제 3 절 디지털 증거의 진정성립 ····· 8

1. 전문법칙과 디지털 증거 ····· 8

2.「형사소송법」제313조 제2항 입법 경위 및 학설의 태도 9

3. 디지털 증거와 작성자 특정의 문제 ····· 11

4. 디지털 증거와 진정성립에 대한 판례의 태도 ····· 12

제 3 장 컴퓨터 생성 증거 수집의 중요성 ····· 17

제 1 절 개요 ····· 17

제 2 절 파일 시스템 ····· 18

제 3 절 메타 데이터 ····· 19

1. 메타 데이터의 정의 및 유형 ····· 19

2. 파일 시스템 메타 데이터 ····· 20

제 4 절 윈도우 레지스트리 ····· 22

제 5 절 이벤트로그 ····· 25

제 6 절 저널링 파일 시스템 ····· 26

제 7 절 볼륨 새도우 카피 ····· 27

제 8 절 슬랙 공간 ····· 27

제 9 절 프리패치 ····· 29

제 10 절 휴지통 ····· 30

제 11 절 바로가기 ····· 31
제 12 절 점프리스트 ····· 31
제 13 절 인터넷 접속 관련 기록 ····· 32
1. 쿠키 ····· 32
2. 히스토리 ····· 33
3. 웹 캐쉬 ····· 33

제 4 장 디지털 증거 압수수색 실무 및 문제점 · 33
제 1 절 선별 압수수색의 원칙 및 문제점 ····· 33
1. 관련 규정 ····· 33
2. 판례의 태도 ····· 34
3. 선별 압수수색 실무 ····· 37
4. 해외 입법례 ····· 41
5. 선별 압수수색과 관련된 문제점 ····· 42
제 2 절 참여권 보장과 관련된 실무 및 문제점 ····· 43
1. 관련 규정 ····· 43
2. 압수수색 집행 종료 시기에 대한 논의 ····· 44
3. 해외 입법례 ····· 48
4. 참여권 보장과 관련된 문제점 ····· 48

제 5 장 저장매체 전체 물리 이미지 확보 필요성 50
제 1 절 물리 이미징과 논리 이미징 ····· 50
제 2 절 안티포렌식 행위 ····· 51
1. 개요 ····· 51
2. 데이터 삭제 ····· 51
3. 데이터 은닉 ····· 52
제 3 절 삭제된 디지털 증거 복구 ····· 56
제 4 절 현장 키워드 검색의 한계 ····· 58

제 5 절 추가 증거 확보 필요성 ····· 60
제 6 절 소결 ····· 61

제 6 장 새로운 방법의 제안 ····· 62
제 1 절 기존 연구 방법 ····· 62
제 2 절 2단계 압수수색 방안 개요 ····· 65
제 3 절 관련성 있는 디지털 증거의 범위 확장 ····· 66
1. 관련성의 의미 ····· 66
2. 컴퓨터 생성 증거와 관련성 ····· 67
3. 소결 ····· 68
제 4 절 신뢰계산 기술 방법 ····· 69
1. 개인정보 보호 기술 ····· 69
2. 신뢰계산 기술 ····· 71
3. Intel SGX(Software Guard Extention) ····· 72
제 5 절 신뢰계산 기술을 활용한 디지털 증거 압수수색 76
1. 기본 아이디어 ····· 76
2. 실무에의 적용 검토 ····· 77
3. 비밀키 생성 및 보관 주체에 대한 검토 ····· 79
4. 구체적인 절차 ····· 81
5. 예상되는 효과 ····· 83

제 7 장 결론 ····· 85
참고문헌 ····· 88

표 목 차

[표 1] MFT Entry 속성 유형 ····· 21
[표 2] 단계별 압수수색 방안 ····· 66

그 림 목 차

[그림 1] 슬랙공간 이미지 ····· 29
[그림 2] 논리 이미지와 물리 이미지 ····· 50
[그림 3] 실링(Sealing) 프로세스 ····· 75
[그림 4] 신뢰계산 기술을 활용한 증거수집 및 암호화 ····· 79
[그림 5] 신뢰계산 기술을 활용한 디지털 증거 압수수색
방안 절차 ····· 83

제 1 장 서 론

제 1 절 연구배경

형사소송은 범인과 범죄사실을 밝혀내고, 이에 따라 국가의 형벌권을 집행하는 과정이므로 형사절차가 추구하는 최고의 이념은 실체적 진실의 발견에 있다. 이와 같은 실체적 진실의 발견은 수사기관의 수사에서부터 시작되어 법원의 재판, 판결 선고, 선고 결과에 따른 집행으로 이루어진다.

한편으로 실체적 진실을 발견하는 과정에서 국민의 부담 및 부당한 처우를 최소화하기 위해 국가의 활동은 적법한 절차에 따라 신속하게 이루어져야 한다.

현대 사회는 스마트폰, 인공지능, 자율주행, 슈퍼컴퓨터, 사물인터넷 등 디지털 정보가 모든 생활의 기본이 되는 최첨단 디지털 시대이다. 물건을 사고, 이동을 하고, 통화를 하고, 업무를 하는 등 대부분의 행동들은 우리도 모르는 사이에 디지털 정보로 저장되고 있다. 즉 우리의 일상은 일어나면서부터 잠이 들 때까지 심지어 자고 있는 동안에도 이메일, 문자메시지, 메신저 등이 오고가는 등 생활 전반이 디지털 정보로 점철되어 있다.

이와 같은 디지털 정보에서 확인되는 이벤트를 시간 순으로 나열하면 형사 사건의 흐름을 파악하고 재구성하는데 많은 도움이 되고, 디지털 정보의 분석을 통해 사건의 결정적인 증거를 확보할 수도 있다. 피해자와 범죄자의 SNS(카카오톡, 트위터, 페이스북 등), 계좌, 전화번호, 이메일, IP주소, GPS 정보, 업무 정보, 취미 정보 등을 분석함으로써 피해자와 범죄자, 범죄 현장 사이에 가능한 연결고리를 찾아 낼 수도 있다.

그러므로 이와 같은 디지털 정보를 잘 찾고 활용하는 것이 수사의 기본이자 사건관계인들의 인권을 보호하며 효율적이고, 스마트한 방식으로 수사를 할 수 있는 최고의 방법이라 할 것이다.

그러나 현재의 형사사법 체계는 발전하는 과학기술과 수사현실을 외면한 채 피의자와 사건관계인들의 사생활 보호 등 형식적인 논리에 치우쳐 디지털 증거의 수집 및 증거능력 인정에 매우 엄격한 기준을 두고 있고, 이로 인해 적법절차의 원칙을 오히려 실체적 진실의 발견보다 우위에 두는 결과를 초래하였다.

범죄를 밝혀내 억울한 사람이 없도록 하되, 범죄와 상관없는 사생활 등은 보장을 받으며, 피의자 또는 사건관계인들의 진술보다 명확하고 확실한 과학적인 증거를 통해 사건관계인들의 인권을 보호하고, 수사기관 및 사법부의 시간적, 인적 비용을 줄이는 방향이야말로 모두가 원하는 이상향일 것이다.

이에 따라 본고에서는 실체적 진실을 추구하되 적법절차의 원칙이 조화롭게 구현될 수 있도록 디지털 증거의 특성을 고려한 압수수색방안을 제안해 보고자 한다.

제 2 절 연구방법

본고에서는 우선 디지털 증거의 증거능력 인정과 관련된 학설 및 판례의 태도를 살펴보고, 증거능력 인정을 위해서 디지털 증거를 압수수색하는 경우 컴퓨터 생성 증거를 수집할 필요성 및 저장매체 전체의 물리이미지를 확보할 필요성 등에 대하여 검토해 보겠다.

다음으로 이와 같은 디지털 증거의 특성에도 불구하고 현행 실무는 선별 압수수색을 원칙으로 하고 있으므로 이로 인해 발생하는 참여권 등의 문제에 대하여 살펴보겠다.

마지막으로 앞서 살펴본 현행 실무의 문제점 및 디지털 증거의 특성상 컴퓨터 생성 증거의 수집 필요성과 저장매체 전체 물리 이미지의 확보 필요성을 바탕으로 새로운 압수수색방안을 제안하고자 한다.

기본적으로 현행와 같이 사용자가 생성한 관련성 있는 증거에 대해서는 키워드 검색 등으로 선별하고, 이에 더하여 컴퓨터 생성 증거 일체를 현

장에서 수집한 뒤 논리 이미징 형식으로 압수한다.

다음으로 저장매체 전체를 물리 이미징하여 동결한 뒤 이를 공개키로 암호화한다. 이와 같이 암호화 한 물리 이미지 전체를 신뢰계산 기술을 활용한 블랙박스 안에 업로드시킨 다음 필요한 경우 검사의 승인을 받아 복호화 시켜 증거로 활용하는 방안을 고안해 본다.

위 블랙박스는 Intel의 SGX(Sofeware Guard Eetention)의 기본구조에 착안하여 구현한 것으로 블랙박스 안에서만 계산, 복호화 되고, 블랙박스를 벗어나게 되면 검사의 승인이 있어야 복호화될 수 있으며 계산 과정 또한 암호화되어 진행된다. 그러므로 피압수자의 사생활을 보호할 수 있고, 범죄와 관련성 없는 정보들에 대한 수사기관의 임의적인 접근을 막을 수 있는 장점이 있다.

이와 같은 신뢰계산 기술을 바탕으로 디지털 증거를 수사 초기에 확보하고 범죄와 관련성 있는 증거만을 현출시켜, 실체적 진실 구현과 사생활 비밀의 보호를 조화롭게 구현할 수 있는 방안을 모색해 보고자 한다.

제 2 장 디지털 증거의 증거능력

제 1 절 디지털 증거의 의의 및 특성

디지털 증거란 '범죄를 입증하거나 피해자 또는 범죄자와 범죄 사이의 연결 고리를 제공할 수 있는 모든 디지털 데이터'로 정의되기도 하고, '범죄가 어떻게 일어났는지에 대하여 입증 또는 반박할 수 있거나, 범죄 의도나 알리바이와 같은 범죄의 핵심 요소들을 이끌어낼 수 있는 정보로 컴퓨터를 사용하여 저장되거나 전송되는 데이터'[1] 라고 정의되기도 한다.

또한 '디지털 형태로 저장 또는 전송되는 증거가치 있는 정보[2]', '법정

1) Eoghan Casey, Digital Evidence and Computer Crime(2nd ed.), Academic Press (2004), 12면

에서 신뢰할 수 있는 저장되거나 전송되는 이진수 형태의 정보[3]', '각종 디지털 저장매체에 저장되거나 네트워크 장비 및 유·무선 통신상으로 전송되는 정보 중 그 신뢰성을 보장할 수 있어 증거로서 가치를 가지는 디지털 정보'[4]로 정의되기도 한다.

디지털 증거는 기존의 유체물 증거들과는 달리 조작·훼손에 대한 취약성, 매체독립성, 원본과 사본 구분의 곤란성, 비가시성·비가독성, 대량성, 전문성, 익명성, 네트워크 관련성 등 고유의 특성을 갖고 있다.

이에 따라 디지털 증거를 출력한 출력문서가 증거능력을 갖추기 위해서는 원본과 출력문건 사이의 동일성 내지 무결성, 진정성, 신뢰성, 원본성 등이 증거능력 인정의 기본 전제로 논의된다.

대법원도 "압수물인 디지털 저장매체로부터 출력한 문건을 증거로 사용하기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력한 문건의 동일성이 인정되어야 하고, 이를 위해서는 디지털 저장매체 원본이 압수시부터 문건 출력시까지 변경되지 않았음이 담보되어야 한다. 특히 디지털 저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 **동일성도 인정**되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. 그리고 압수된 디지털 저장매체로부터 출력한 문건을 진술증거로 사용하는 경우, 그 기재 내용의 진실성에 관하여는 전문법칙이 적용되므로 형사소송법 제313조 제1항에 따라 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여

---

2) SWGDE(Scientific Working Group on Digital Evidence ; 미국 법무부의 마약수사청, 연방수사 관세청 및 국세청 등의 증거분석 연구소를 중심으로 구성된 디지털 증거에 관한 과학실무그룹)에서의 정의

3) IOCE(International Organisation on Computer Evidence ; 미국, 호주, 홍콩, 영국 등 각국의 실무자들을 중심으로 만들어진 디지털 증거에 관한 국제기구)에서의 정의

4) 탁희성·이상진, "디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보 방안", 한국형사정책연구원, 2006, 31~34면 참조

이를 증거로 사용할 수 있다."고 판시[5]하고 있다.

제 2 절 디지털 증거의 무결성과 동일성 확보

디지털 증거의 증거능력과 관련하여 가장 문제가 되고 있는 무결성과 동일성은 따로 떼어 놓고 판단할 수 없을 정도로 밀접한 연관성을 갖고 있으며 동전의 양면과도 같은 개념이다.

우선 무결성은 '절차적인 적정성의 준수 여부'라고 할 수 있는데 증거를 처음 확보하는 단계에서부터 법정에 증거자료로 제출될 때까지 훼손이나 변경이 없었음을 입증하는 것을 의미한다.

이에 따라 실무에서는 피압수자 등의 참여 하에 디지털 증거를 압수한 후 봉인하고, 봉인상태를 확인한 뒤 피압수자의 서명을 받고, 서명과 봉인 과정을 비디오카메라로 녹화하며, 재판 과정에서 무결성을 부인하는 경우에는 피압수자 등이 확인한 해시값과 증거로 제출된 이미지 파일 해시값의 동일성 여부를 비교·검증하여 무결성을 입증하고 있다.

실무상 원본 디지털 증거를 분석하게 되는 경우 그 증거는 원본성을 상실하게 되므로 이를 이미징하거나 하드카피한 뒤 그 사본을 분석의 대상으로 하고, 이를 출력한 문서를 증거로 제출한다. 그러므로 증거능력이 인정되기 위해서는 이 원본 디지털 증거와 사본 및 출력 문서 사이의 동일성이 필요하게 된다.

이와 같이 원본 디지털 증거와 사본 및 출력 문서간의 동일성을 판단함에 있어 법원은 "기술에 대한 신뢰와 정확성"을 그 기준으로 삼고, 세계적으로 인정받는 프로그램을 이용한 이미징 작업 및 쓰기방지장치를 부착한 이미징 작업, 디지털 저장매체 원본의 해쉬값과 이미징 작업을 통해 생성된 사본 파일 해쉬값의 동일성, 피고인·검사·변호인이 참여한 검증과정에서 산출한 해쉬값과 압수수색 당시 쓰기방지장치를 부착하여 '이미징' 작업을 하면서 산출한 해쉬값의 동일성, 사본파일 내용과 출력문서 사이

5) 대법원 2007. 12. 13. 선고 2007도7257 판결

의 동일성 확인을 위한 검증 등을 동일성 판단의 주요 기준으로 삼고 있다.[6]

이와 같은 무결성, 동일성의 입증은 압수수색의 과정을 비디오 촬영한 영상녹화물의 재생방법 이외에도 절차에 참여한 수사관이나 전문가 등의 증언 또는 법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법 등에 의해서도 가능하다는 것이 대법원 판례의 태도[7]이며 형사소송법 제313조 제2항[8]의 입법취지 또한 그러하다.

---

6) 대법원 2007. 12. 13. 선고 2007도7257 판결

7) 대법원 2013. 7. 26. 선고 2013도2511 판결 참조 ; "압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체(이하 '정보저장매체'라고만 한다)에 입력하여 기억된 문자정보 또는 그 출력물(이하 '출력 문건'이라 한다)을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다. 특히 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우에는 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이에 자료의 동일성도 인정되어야 할 뿐만 아니라, 이를 확인하는 과정에서 이용한 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인 기술능력과 정확성이 담보되어야 한다. 이 경우 출력 문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점은, **피압수·수색 당사자가 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체의 해쉬(Hash) 값이 동일하다는 취지로 서명한 확인서면을 교부받아 법원에 제출하는 방법에 의하여 증명하는 것이 원칙**이나, **그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우**에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피' 또는 '이미징' 등 일련의 **절차에 참여한 수사관이나 전문가 등의 증언**에 의해 정보저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 해쉬 값이 동일하다거나 정보저장매체 원본이 최초 압수 시부터 밀봉되어 증거 제출 시까지 전혀 변경되지 않았다는 등의 사정을 증명하는 방법 또는 **법원이 그 원본에 저장된 자료와 증거로 제출된 출력 문건을 대조하는 방법** 등으로도 그와 같은 무결성·동일성을 인정할 수 있으며, **반드시 압수·수색 과정을 촬영한 영상녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니다."**

8) 형사소송법 제313조 ② 제1항 본문에도 불구하고 진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다. <개정 2016. 5. 29.>

이러한 무결성 및 동일성은 디지털 증거의 증거능력 인정 요건에 해당하므로 검사가 그 존재에 대하여 구체적으로 주장・입증하여야 하지만, 이는 소송상의 사실에 관한 것이므로 엄격한 증명을 요하지 아니하고 자유로운 증명으로 족하다는 것이 대법원 판례[9]의 태도이다.

대검찰청 예규인「대검 디지털 증거 수집 및 분석 규정」에서도 이와 같은 디지털 증거의 무결성, 신뢰성, 보관의 연속성 유지 등에 대하여 규정[10]하고 있다.

원본이 소멸한 상황에서 동일성 입증이 필요한 경우에는 미리 추출하여 놓은 원본의 해쉬값이 있고 이를 신뢰할 수 있는 경우, 원본과 사본의 해쉬값을 비교하여 원본과 사본의 동일성을 확인하는 방법을 취할 수 있다.

그러나 원본이 소멸하였고 미리 추출하여 놓은 원본의 해쉬값도 없는 경우도 있을 수 있는데 이와 같은 경우 하급심 판례[11]에서는 비록 원본과

---

9) 대법원 2001. 9. 4. 선고 2000도1743 판결 ; 서울중앙지방법원 2014. 4. 25. 선고 2013고합805 판결

10) **「대검 디지털 증거 수집 및 분석 규정」<2021. 1. 1. 시행>**

제5조(디지털 증거의 원본성 유지) 디지털 증거는 법정에서 원본과의 동일성을 재현하거나 검증하는데 지장이 초래되지 않도록 수집·분석 및 관리되어야 한다.

제6조(디지털 증거의 무결성 유지) 디지털 증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다.

제7조(디지털 증거의 신뢰성 유지) 디지털 증거는 디지털포렌식 전문가에 의해 신뢰할 수 있는 도구와 방법으로 수집·분석 및 관리하여야 한다.

제8조(디지털 증거의 보관의 연속성 유지) 디지털 증거는 최초 수집된 상태 그대로 어떠한 변경도 없이 보관되어야 하고, 이를 위해 보관 주체들 간의 연속적인 승계 절차를 관리하는 등의 조치를 취해야 한다.

11) 서울중앙지방법원 2014. 4. 25. 선고 2013고합805 판결 참조 ; "디지털 증거를 압수・수색 영장의 집행에 의하여 압수한 것이 아니라 소유자, 소지자 내지 보관자로부터 임의제출 받아 압수한 경우는 영장 집행에 있어서와 같이 엄격한 절차를 요구하기는 어렵다. 하지만 임의제출 받는 경우 영장집행에 비하여 간략한 절차를 취한다고 하더라도 제출자로부터 원본이 조작되지 않았다는 취지의 확인을 받은 후 원본을 압수하여야 하고, 복사 등을 하는 경우 이로 인하여 작성된 사본을 봉인하여, 적어도 법원으로 하여금 그 무결성에 대한 합리적인 의심이 들지 않을 정도의 최소한의 조치를 취하여야 한다. (중략) 원본이 소멸하였더라도 미리 추출하여 놓은 원본의 해쉬값이 있고 이를 신뢰할 수 있는 경우, 원본과 사본의 해쉬값과 비교하여 원본과 사본의 동일성을 확인할 수 있다. 그러나 원본이 소멸하였고 미리 추출하여 놓은 원본의 해쉬값도 없는 경우에는 원본과 사본의 동일성에 관한 증명이 전혀 불가능하지 않다고 할지라도, 사본 파일에 대한 감정

사본의 동일성에 관한 증명이 전혀 불가능하지 않다고 할지라도, 사본 파일에 대한 감정 등을 통하여 인위적 개작의 흔적이 없다는 점이 밝혀지지 않은 이상 파일 복사에 관여한 수사관들의 진술과 사본에 대한 검증결과만으로는 동일성을 인정할 수 없으며, 디지털 저장매체에 대하여 수사관 계인이 임의제출을 하는 경우라도 차후에 증거로 채택되어 법정에서 증거능력이 인정되기 위해서는 그 무결성에 대한 합리적인 의심이 들지 않을 정도의 최소한의 조치를 취하여야 한다고 판시하고 있다.

제 3 절 디지털 증거의 진정성립

1. 전문법칙과 디지털 증거

전문법칙이란 '사실인정의 기초가 되는 경험사실을 경험한 사람이 직접 법원에 진술하지 않고 타인에 의하여 진술되거나 서면기재 형태로 제출하는 전문증거는 원칙적으로 증거능력이 없다'[12]는 법칙으로 형사소송법에서는 제311조부터 제316조까지 일정한 조건 하에서만 전문증거의 증거능력을 예외적으로 인정하고 있다.

그러나 문건의 존재 그 자체가 직접 증거로 되는 경우[13]나, 문건의 기재내용 자체가 요증 사실의 구성요소를 이루는 경우[14], 그 기재내용의 진실성과 관계없이 간접사실에 대한 정황증거로 사용되는 경우[15]에는 전문법칙이 적용되지 않는다. 즉 디지털 증거의 존재 또는 기재내용 자체가 요증 사실이 되는 경우에는 전문법칙의 문제가 적용되지 아니하나 그 기재내용의 진실성이 문제되는 경우에는 전문법칙이 적용[16] 되게 된다.

등을 통하여 인위적 개작의 흔적이 없다는 점이 밝혀지지 않은 이상 파일 복사에 관여한 수사관들의 진술과 사본에 대한 검증결과만으로는 동일성을 인정할 수 없다."

12) 형사소송법 제310조의2

13) 대법원 1999. 9. 3. 선고 99도2317 판결

14) 대법원 2008. 9. 25. 선고 2008도5347 판결

15) 대법원 2000. 2. 25. 선고 99도1252 판결

16) 대법원 2008. 11. 13. 선고 2006도2556 판결에서 판시한 바와 같이 불안감을

이와 같이 디지털 저장매체에서 출력한 문서가 진술자에 의한 진술을 구성하고, 그 진실성이 문제되는 경우에는 전문증거에 해당하므로 전문법칙의 예외가 인정되는 경우에 한해 증거능력이 인정된다.

2. 「형사소송법」 제313조 제2항 입법 경위 및 학설의 태도

전문법칙의 예외 규정에 따라 피고인 또는 피고인이 아닌 자가 작성한 진술서 또는 진술을 기재한 서류의 경우, 형사소송법 제313조 제1항에 의해 '그 작성자 또는 진술자의 진술에 의하여 성립의 진정함이 증명'된 때에 한하여 증거로 사용될 수 있다.

여기서 성립의 진정이란 형식적 진정성립과 실질적 진정성립으로 나누어지는데, 형식적 진정성립이란 '서명·날인과 같은 형식적 요건이 진술자의 것이 틀림없다'는 것을 의미하고, 실질적 진정성립이란 '진술내용이 서류에 기재된 내용과 일치한다'는 것을 의미한다.

그러나 디지털 증거의 경우 그 특성상 '자필·서명·날인'이 존재하지 않을 가능성이 높으므로 진정성립의 요건을 문서와 동일하게 보기보다는 디지털 증거의 특성을 고려하여 작성자 특정 등의 방식으로 진정성립 여부를 판단함이 상당할 것이다.

디지털 증거의 진정성립과 관련해서는 형식적 진정성립 요건이 불필요하다는 주장[17]부터, 조문상 명시적으로 형식적 진정성립 요건의 배제를 언급한 사실이 없으므로 법해석을 통해 형식적 진정성립 요건을 배제하는 것은 법 해석이 아닌 법 창조에 가까운 접근이라는 견해[18]까지 다양한 논란이 있어 왔다.

유발하는 문자메시지를 반복적으로 전송하였는지 여부가 요증 사실이고, '지금 내가 무슨 짓을 할 지 모른다'라는 문자메시지 내용의 진실성을 입증하려는 것이 아닌 경우 이를 전문증거라 할 수 없음

17) 오기두, "전자진술서의 증거능력(개정 형사소송법 제313조)", 사법(사법발전재단, 2016), 통권 제38호, 277면

18) 박민우, "전문증거 증거능력 인정요건의 변화와 이로 인한 새로운 문제에 대한 검토 : 형사소송법 제313조의 개정을 중심으로", 형사정책연구원(한국형사정책연구원, 2016), 제27권 제3호, 111면

이러한 실무상의 쟁점들을 반영하여 2016년 5월 형사소송법 제313조 제2항[19]이 개정되었고, 그 결과 진술서의 경우는 '과학적 분석결과에 기초한 디지털포렌식 자료나 감정 등 객관적 방법으로 성립의 진정을 증명'할 수 있도록 법률에 근거 규정을 두게 되었다.

개정법의 해석에 대해서도 전자진술서에 관해서는 디지털포렌식 등 객관적 방법에 의해 형식적 성립의 진정이 입증되면 그 진술자가 공판정에서 실질적 진정성립을 부인한다고 하더라도 이를 추정하라는 취지라는 견해[20]가 있고, 이에 반해 '전자정보 작성자의 특정'에 관한 형식적 진정 성립이 인정되는 경우에도 진술자가 부인하는 경우에는 제2항에 따라 별도로 '진술자의 진술 내용대로 기재되어 있음을 객관적 방법으로 증명한 때에 한하여' 증거로 사용할 수 있다고 해석[21]하는 견해, 디지털 증거의 경우 사후에 제출된 증거가 저장 및 수집 과정에서 오류가 없고, 특정한 사람의 행위 결과가 정확하게 표현되었으며, 그로 인해 생성된 자료임이 인정되어야 하므로 이는 결국 '실질적 진정성립'의 문제와 연결된다고 보는 견해[22]도 존재한다.

---

19) 형사소송법 제313조(진술서등) ① 전 2조의 규정 이외에 피고인 또는 피고인이 아닌 자가 작성한 진술서나 그 진술을 기재한 서류로서 그 작성자 또는 진술자의 자필이거나 그 서명 또는 날인이 있는 것(피고인 또는 피고인 아닌 자가 작성하였거나 진술한 내용이 포함된 문자·사진·영상 등의 정보로서 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체에 저장된 것을 포함한다. 이하 이 조에서 같다)은 공판준비나 공판기일에서의 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에는 증거로 할 수 있다. 단, 피고인의 진술을 기재한 서류는 공판준비 또는 공판기일에서의 그 작성자의 진술에 의하여 그 성립의 진정함이 증명되고 그 진술이 특히 신빙할 수 있는 상태 하에서 행하여 진 때에 한하여 피고인의 공판준비 또는 공판기일에서의 진술에 불구하고 증거로 할 수 있다.
② 제1항 본문에도 불구하고 **진술서의 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에는 과학적 분석결과에 기초한 디지털포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함이 증명되는 때에는 증거로 할 수 있다**. 다만, 피고인 아닌 자가 작성한 진술서는 피고인 또는 변호인이 공판준비 또는 공판기일에 그 기재 내용에 관하여 작성자를 신문할 수 있었을 것을 요한다.
20) 오기두, 앞의 논문, 379면
21) 강철하, "개정 형소법 제313조의 해석론", 이화여자대학교 법학논집 제22권 제4호 통권62호, 2018. 6. 269면

3. 디지털 증거의 작성자 특정의 문제

이와 같은 디지털 증거의 형식적 진정성립은 결과적으로 작성자를 특정하는 문제로 귀결될 수 있다.

작성자 특정이 가장 명확하게 이루어지는 경우로는 전자문서의 원본인 경우, 출력문서 자체에 문서작성자의 이름이 기재되어 있거나 전자서명 또는 날인이 있는 경우, 법령으로 인정되고 있거나 공사단체의 전산시스템으로 인정되는 전자서명이 있는 경우라 할 것이다.

또한 ID, PW, IP 정보, 메타 데이터 등을 분석해 보았을 때 피고인만 이용하는 컴퓨터, 휴대전화, 태블릿PC라는 사실이 인정되고, 그와 같은 기계에서 작성된 이메일, 문자 메시지, 문서 등의 경우에는 피고인이 작성했다고 인정할 수 있을 것이다.

피고인이 근무하는 회사, 가입한 단체나 ISP 업체가 운영하는 게시판, 블로그, 인터넷 카페, SNS에 피고인이 사용하는 계정으로 게시하거나 전송한 전자문서인 경우도 피고인이 작성하였다고 인정할 수 있다.

그 밖에 디지털 포렌식 과정에서 획득한 레지스트리와 캐시 내용, 메모리 내용, 네트워크 연결 상태, 실행 중인 프로그램 상태, 스왑 파일 시스템의 내용, 기타 하드디스크 등에 저장되어 있는 파일과 디렉토리에 대한 시간속성 정보 등과 같은 휘발성 데이터, 하드디스크, 프로피 디스크, CD, DVD, USB 메모리 등 비휘발성 장치로부터 획득된 데이터 분석자료, 프로그램의 원시코드나 프로그램 작동방식, 결과 등을 분석해내는 프로그램 소스분석 자료, 각종 디지털 전자기기에 대한 인식장치나 분석도구 등을 이용한 분석자료 등[23]에 의해서도 작성자를 입증할 수 있을 것이다.

이와 같이 컴퓨터 자체에서 확인할 수 있는 정황증거 이외에도 디지털 증거의 수색·검증, 압수과정에서 확보한 사건관계인의 입력장치에 있는

---

22) 노명선, “전자적 증거의 실효적인 압수·수색, 증거조사 방안연구”, 대검찰청 용역 보고서, 2007. 57면

23) 오기두, “피고인의 공판정 진술과 전자문서의 진정성립”, 사법 24호, 2013, 178면 참조

지문, 필적 메모, 꼬리표, 암호화된 데이터에 접근할 수 있는 손으로 쓴 암호, 그 밖의 모니터, 프린터 등 연결장치에서 확보한 자료[24] 등도 작성자 입증의 간접증거로 활용 가능할 것이다.

또한 우편물, 요금 고지서, 차량 등록 서류에 기재된 주소지 등 피고인이 해당 주거지에 단독으로 거주함을 입증할 수 있는 관련 서류들, 피고인의 출퇴근 시간, 발신지 기지국 위치, 피고인 명의로 인터넷에 가입하였는지 또는 그 명의로 이메일 계정이나 기타 서비스 제공 업체에 가입하였는지 여부 등[25]도 작성자 특정과 관련된 디지털 증거 분석의 중요한 자료가 될 수 있을 것이다.

다음으로 실질적 진정성립은 컴퓨터 시스템의 신뢰성과 밀접한 연관이 있다. 컴퓨터 시스템이 안정적으로 오작동 없이 돌아가는 상태에서는 작성자의 의사에 반한 입력, 저장, 전송, 출력 등이 존재하지 않으므로 작성자의 의사대로 작성되었다고 볼 수 있을 것이다.

오늘날과 같이 전자정보시스템의 안정성, 신뢰성 등에 기반한 IT 사회에서는 형식적 진정성립이 인정되는 이상 실질적 진정성립은 사실상 추정된다고 봄이 상당하다 할 것이다.

그러므로 형식적 진정성립이 인정되는 경우 디지털 증거의 증거능력을 인정하고, 작성자가 실질적 진정성립을 부인하는 경우에는 증명력의 문제로 보아 본안인 유무죄 판단을 위한 증거조사를 하면서 판단하면 족할 것이다.[26]

4. 디지털 증거의 진정성립에 대한 판례의 태도

가. 형사소송법 제313조 제2항 개정 전

24) USDOJ, Federal Guidelines for searching and seizing cimputers, IV. F. 2012
25) 한인검사협의회 디지털 증거 연구용역, “디지털 증거의 증거능력 및 압수수색에 관한 해외 실무례 연구”, 2016. 39면
26) 오기두, 전자증거법, ㈜박영사, 2015, 626～627면 참조

1) 공직선거법 위반 사건

1심에서는 압수된 디지털 저장매체로부터 출력한 문건을 진술증거로 사용하는 경우 그 진술의 진실성에 대해서는 전문법칙이 적용되므로 형사소송법 제313조 제1항에 따라 그 작성자 또는 진술자가 공판준비나 공판기일에서 그 성립의 진정함을 인정한 경우에 한해 이를 증거로 사용할 수 있다고 보아 위 각 문건의 작성자로 지목된 사람이 법정에서 위 각 문건의 진정성립을 묻는 질문에 대해 모두 진술거부권을 행사하여 그 성립의 진정함이 증명되지 아니하는 경우에는 이를 증거로 사용할 수 없다고 판시[27]하였고, 2심,[28] 3심 모두 같은 취지로 판단하였다.

다만 "USB 문건 중 선거운동원들이 실제로 선거운동을 하였는지 여부를 표시한 부분은 피고인이 선거운동원들을 모집, 관리하는 업무를 수행하기 위하여 선거운동원들이 실제로 선거운동을 하였는지 여부를 그때그때 일상적, 계속적, 기계적으로 확인하여 작성한 출결부를 근거로 작성되었다는 것이므로 형사소송법 315조 제2호의 '기타 업무상 필요로 작성한 통상문서'에 해당하고 따라서 USB 문건 중 선거운동원들이 실제 선거운동을 하였는지 여부를 표시한 부분도 위 출결부의 내용과 동일성을 유지한 상태에서 컴퓨터파일로 옮겨 적는 형태로 작성된 것임이 인정될 경우 역시 기타 업무상 필요로 작성한 통상문서에 해당한다고 볼 여지가 있다."고 판시하여 진정성립을 인정하는 피고인의 진술이 없음에도 형사소송법 제315조 제2호의 '기타 업무상 필요로 작성한 통상문서'로 보아 증거능력을 인정할 가능성 보여주었다.

2) 원세훈 사건[29]

이 사건에서는 "압수된 디지털 저장매체로부터 출력한 문서를 진술증거로 사용하는 경우, 저장매체의 사용자 및 소유자, 로그기록 등 저장매체에 남은 흔적, 초안 문서의 존재, 작성자만의 암호 사용 여부, 전자서

27) 수원지방법원 안산지원 2012. 8. 10. 선고 2012고합191, 231, 241, 242, 309 판결
28) 서울고등법원 2012. 12. 7. 선고 2012노2667 판결
29) 대법원 2015. 7. 16. 선고 2015도2625 판결

명의 유무 등 여러 사정에 의하여 동일인이 작성하였다고 볼 수 있고 그 진정성을 탄핵할 다른 증거가 없는 한 그 작성자의 공판준비나 공판기일에서의 진술과 상관없이 성립의 진정을 인정하여야 한다는 견해를 경청할 만하기는 하나 입법을 통하여 해결해야 한다."고 판시하여 해당 사건에서는 증거능력 인정을 부인하였으나, 향후 객관적 방법에 의한 진정성 성립 가능성을 열어 놓았다.

3) 전 대학교수 간첩사건[30]

피고인의 주거지에서 압수한 컴퓨터 내에 저장되어 있던 보고서 파일의 작성자가 누구인지가 쟁점이 되었던 사건에서 피고인이 작성사실을 부인하였음에도 파일 헤더정보 및 문건 내용을 종합하여 작성자를 피고인으로 인정한 판례이다.

위 판례에서 법원은 작성자를 피고인으로 인정했으나 피고인이 진정성립을 부인하여 증거능력을 인정하지 아니하였다. 그러나 현행 형사소송법 하에서는 진정성립이 인정되고 증거능력 또한 인정될 가능성이 있을 것이다.

작성자를 피고인으로 인정한 근거로는 파일 헤더 정보[31]에서 작성자와 마지막 저장자가 피고인의 손자 이름으로 입력되어 있고, 주거지에서 피고인이 사용하는 컴퓨터의 윈도우 운영체제 사용자도 피고인의 손자 이름으로 입력되어 있었으며, 피고인이 스스로 작성하였다고 인정한 일부 문서파일의 헤더 정보에도 그 작성자와 마지막 저장자가 피고인의 손자로 입력되어 있었다는 점이었다.

또한 보고서 파일의 내용이 피고인의 행적, 주소, 나이 등 객관적인 사실과 일치하는 점, 위 보고서 내용 중 '지난해 10월에 평양방문을 할 때' 부분은 피고인이 그 무렵 평양문화유적 참관 행사를 위해 평양을 방문한

30) 서울고등법원 2015. 6. 25. 선고 2014노2389 판결
31) 아래한글 문서파일(확장자가 hwp인 파일)의 헤더정보 중 작성자에는 문서를 최초로 생성하였을 당시 사용된 컴퓨터의 윈도우 운영체제 사용자 이름이 입력되고, 마지막 저장자에는 문서를 마지막으로 저장할 당시 사용된 컴퓨터의 윈도우 운영체제 사용자의 이름이 입력됨

것과 일치하고, ‘감옥을 나온 다음에 주로 청년학생들과 노동청년들을 만나 살아온 역사를 이야기 해주었다‘는 부분 또한 피고인의 행적과 일치한다는 점 등을 근거로 들고 있다.

4) 통진당 전 간부 특수잠입탈출 등 사건[32)]

법원은 피고인이 복호화 파일을 업로드한 사실을 부인하였음에도 웹하드 분석, 접속 아이피 분석, 휴대전화 기지국 분석 등을 종합하여 작성자를 피고인으로 인정하였으나, 피고인이 진정성립을 부인하여 결국증거능력은 인정되지 아니하였다.

작성자를 피고인으로 판단한 자료로 우선 웹하드 ID가 피고인의 이름을 추정하게 하는 이니셜과 나이로 구성되어 있고, 위 ID는 피고인이 사용하는 포털사이트인 다음, 네이버 등의 ID와 동일하며, 동일한 웹하드 ID로 업로드 되어 있는 이미지 파일에서 스테가노그라피 방식의 암호화 프로그램으로 위장된 문건이 발견된 점 등이 고려되었다.

다음으로 접속 아이피 분석 결과 이미지 파일이 업로드 될 당시 접속 IP 주소가 피고인의 주소지 광랜서비스 IP와 일치했다는 점, 휴대전화 기지국 분석 결과 이미지 파일 접속시간 대의 휴대전화 기지국 위치가 피고인 주거지 부근이었던 점, 복화화 파일을 분석한 결과 피고인이 활동하던 예술동지회에 대한 언급이 있어 피고인이 작성한 것으로 추론 가능하다고 판시하였다.

5) 새시대 교육운동 이적단체 구성 사건[33)]

이메일 발송시 접속 IP를 살펴보면 피고인들이 근무했던 학교에서 발송되었고, 압수된 이메일 등을 살펴보면 내용 자체로 피고인들이 작성할 수 있는 내용 포함되어 있는 점, 압수된 이메일에 피고인들이 통상 교사 업무를 수행하면서 수발신하였던 문건들도 함께 보관되어 있는 점 등을 종합하여 보면 피고인들이 작성한 것으로 추론 가능하다고 판시하였다.

---

32) 대법원 2015. 4. 23. 선고 2015도1278 판결
33) 서울고등법원 2016. 1. 19. 선고 2015노442 판결

법원은 피고인들이 이메일 작성사실을 부인하거나 기억나지 않는다고 진술하면 증거능력을 부정하였으나, 개정법 하에서는 접속 IP 분석, 이메일 내용 및 보관형태 분석 등을 종합하여 피고인들이 해당 문서를 작성하였다는 사실을 증명하는 것이 상당 부분 가능할 것으로 예상된다.

나. 개정 후

1) 국가보안법위반 사건

1심에서는 피고인들이 대북보고문 등의 문건에 대한 성립의 진정을 부인하더라도, 수사기관의 디지털 포렌식 절차에 의해 분석된 디지털 증거분석 보고서와 국립과학수사연구원의 감정결과를 통하여 피고인들이 해당 문건들을 작성한 사실을 인정[34]하였다.

항소심에서도 1심의 판단이 정당하다고 하며 설령 진정성립이 인정되지 않는다 하더라도 문서 파일이 작성되어 존재한다는 사실 및 그 기재내용의 진실 여부와는 관계없이 간접사실에 대한 정황증거로서의 증거능력은 인정할 수 있다[35]고 판시하였다.

2) 유흥주점조세포탈사건[36]

본 사건에서는 검사가 USB에 저장된 파일의 해시값과 논리적 이미징 작업을 한 파일의 해시값을 각각 피압수자 측에게 보여주면서 양자의 동일성을 확인하도록 하였음에도 불구하고 대법원은 이 사건 사실확인서에는 이 사건 USB 이미지 파일의 전체 해시값만 기재되어 있을 뿐 이미징을 한 이 사건 USB 내 개별 파일에 대한 해시값은 기재되어 있지 않으므로 해시값을 상호 비교할 수 없다는 이유로 동일성을 부정하였다.

또한 대법원에서는 "장부를 작성·관리한 경리직원이 '내가 작성한 것이 맞다'고 진술한 것만으로는 같은 것으로 보기에 충분하지 않다"고 하면서 "디지털 증거가 원본과 동일한 것인지는 '합리적 의심의 여지를 없앨

34) 서울중앙지방법원 2016. 12. 23. 선고 2016고합675 판결
35) 서울고등법원 2017. 7. 5. 선고 2017노146 판결
36) 대법원 2018. 2. 8. 선고 2017도13263 판결

정도'로 검찰이 입증해야 한다"고 강조하였으나 이는 디지털 증거의 특성을 충분히 고려하지 않은 판시로 보인다.

제 3 장 컴퓨터 생성 증거 수집의 중요성

제 1 절 개요

디지털 정보를 증거로 사용하기 위해서는 진정성립의 인정이 그 기본 전제이며 디지털 증거의 진정성립은 앞에서 살펴본 것과 같이 작성자의 입증에서부터 시작된다.

그러나 디지털 증거의 경우 파일 자체에 저장된 정보만으로는 작성자를 특정하기에 부족한 측면이 많다. 피고인 등 작성자가 진정성립을 인정하는 경우에는 문제되지 않으나 실무상 디지털 증거가 빛을 발하는 경우는 피고인이 부인하고 이를 입증할 증거가 부족할 때일 것이다.

피고인 등이 진정성립을 부인할 경우에 대비한다면 진정성립 증명에 활용빈도가 높은 컴퓨터가 직접 생성한 증거를 수집하여 진정성립 입증자료로 활용할 필요성이 높다 할 것이다.

컴퓨터에 저장된 데이터는 크게 컴퓨터가 자동 또는 임의로 생성한 데이터와 사람이 입력한 데이터, 다운로드, 복사, SW 설치 등에 의해 외부로부터 들어온 데이터로 나눌 수 있다. 컴퓨터 생성 증거(Computer Generated Evidence)[37]란 사용자가 생성한 증거가 아니라 사람의 개입 없이 컴퓨터가 프로그램에 따라 자체적으로 내장된 알고리즘을 통해 자동 또는 임의로 생성한 증거로 정의할 수 있다.

전자 문서, 이메일, 카카오톡 대화 내용, 진술서 등 사람이 입력한 데이터는 사람의 의사와 사상이 담긴 디지털 증거로 전문증거로 볼 수 있으므

37) Steven W Teppler, "Digital data as hearsay", Digital Evidence and Electronic Signature Law Review Vol. 6. 2009.

로 법정에서 진술 및 반대신문을 통해 진술의 신뢰성을 검증하는 절차가 필요하다.

이에 반해 메타 데이터, 시스템/응용 로그와 같은 아티팩트 등의 컴퓨터 생성 데이터의 경우 사람의 의사 및 사상과 관계없이 컴퓨터가 자동으로 생성한 증거로 비전문증거로 볼 수 있어 전문법칙이 적용되지 않는다.

대법원 또한 “정보저장매체에 기억된 문자정보 내용의 진실성이 아닌 그와 같은 내용의 문자 정보가 존재하는 것 자체가 증거로 되는 경우에는 전문법칙이 적용되지 아니한다.”라고 판시[38]하고 있다.

이와 같은 컴퓨터 생성 증거의 경우 데이터를 생성한 컴퓨터와 프로그램의 신뢰성에 의존할 수 밖에 없는데, 우리나라의 경우 컴퓨터 시스템의 정확성에 대하여 일반적인 신뢰가 형성되어 있다고 보이므로, 일응 컴퓨터 시스템이 정상적으로 작동하였음을 추정하고, 정확성을 부정하는 피고인이나 변호인 측에서 그 부정확성을 입증하여 신뢰성을 부정함이 상당하다 할 것이며, 미국의 실무도 그 정확성을 부정하는 당사자가 이를 입증하여야 한다는 것이 지배적인 의견[39]이다.

이와 같은 컴퓨터 생성 증거의 경우 진정성립을 입증하는 자료로 간접증거로 볼 수 있으므로 사용자가 직접 작성한 자료보다는 범죄사실과의 관련성 여부를 보다 넓게 인정함이 상당할 것이다.

제 2 절 파일 시스템

파일 시스템은 원하는 파일을 읽고 쓰며, 데이터를 검색, 저장, 관리하기 위한 규약으로 디지털 데이터를 효과적으로 관리하기 위해 파일을 체계적으로 기록하는 방식이다.

즉, 파일과 디렉토리와 같은 계층 구조로 데이터를 저장하도록 하는 메커니즘으로 파일이 어디에 저장되어 있는지 조직화하고, 사용자의 데이터

38) 대법원 2013. 2. 15. 선고 2010도3504 판결
39) 오기두, 앞의 책, 142면 참조

를 구조적으로 정의하기도 한다.

파일 시스템은 부팅 영역, 메타 영역, 데이터 영역으로 나눌 수 있다. 부팅 영역은 파티션의 Layout 정보를 저장하고, 메타 영역은 파일 관리를 위한 파일 이름, 위치, 크기, 시간 정보 등을 저장, 이와 같은 메타 정보를 이용하여 파일 시스템을 효과적으로 관리하며, 데이터 영역은 사용자가 생성한 파일의 내용을 기록한다.

파일 시스템의 종류로는 FAT, NTFS, UFS, ExT2/3/4 등이 있다. FAT 파일 시스템은 윈도우 9x의 기본 파일 시스템으로 최근에는 USB 메모리, 플래쉬 메모리 파일 시스템에서 주로 사용되고, 호환성이 좋아 윈도우, 맥, 리눅스에서도 읽기, 쓰기가 가능하나 접근 권한 제어 기능이 없어 보안에 취약하며 비교적 간단한 구조로 이루어져 있다.

NTFS(New Thchnology File System)은 윈도우 NT, 2000, XP 이후 버전에서 기본적으로 사용되는 운영체제로 하나의 파일이 다중 데이터를 저장할 수 있도록 지원하고, 빠른 암호화 복호화를 위해 FEK(File Encryption Key)를 통한 대칭키 방식[40]의 암호화를 수행하는 특징이 있다.

제 3 절 메타 데이터

1. 메타 데이터의 정의 및 유형

메타 데이터(Metadata)는 일정한 규칙에 따라 콘텐츠 또는 파일에 부여되는 데이터로, 속성 정보로 불리기도 한다. 데이터에 관한 정보를 저장하고, 데이터를 검색하거나 재구성하는데 큰 역할을 하므로 디지털 포렌식 증거 수집에 있어 매우 중요한 역할을 담당하고 있다.

메타 데이터의 유형으로는 파일 시스템 메타 데이터와 인터넷 메타 데이터가 있는데 인터넷 메타 데이터는 웹 페이지 메타 데이터와 브라우저

40) 박상준, 디지털포렌식 강의자료 II, 2020. 3. 396면 참조 ; 키관리는 RSA 공개키 암호 사용

메타 데이터로 나눌 수 있다. 파일 시스템 메타 데이터에 대해서는 항을 바꾸어 기술한다.

웹 페이지 메타 데이터는 웹 페이지의 이름, 헤더, 코드, 디스크립션 등에 관한 정보가 포함되어 있지만 대부분 웹 페이지를 제작하는 사용자가 통제할 수 있으므로 증거적인 가치는 상대적으로 낮다.

이에 반해 브라우저 메타 데이터의 경우에는 인터넷 브라우징 프로그램에 의해 저장된 검색 기록으로 사용자가 방문한 웹 사이트, 웹 페이지에 대한 정보를 확인할 수 있으므로 증거로 활용할 만한 가치가 높다.

2. 파일 시스템 메타 데이터

파일 시스템 메타 데이터에는 운영체제에 의해 기록된 파일의 저장위치, 파일 크기, 파일 생성시간, 수정시간, 접근시간, 마지막 쓰기 시간 등에 관한 정보가 포함되어 있다. 이와 같이 운영체제가 기록하는 메타 데이터는 시스템 내에 별도로 메타 데이터만 모아 놓은 파일로 존재한다.

한편, 응용 프로그램이 기록하는 메타 데이터는 파일 내부에 존재한다. 응용 프로그램에서 파일을 생성할 때는 반드시 운영체제를 통해 프로그램이 실행되므로 응용 프로그램에서 메타 데이터를 생성할 때는 운영체제에서 기록한 메타 데이터 파일도 함께 생성된다.

가. 운영체제에서 기록한 메타 데이터

NTFS 파일 시스템에서는 모든 데이터를 파일로 관리하는데, 파일이 생성, 수정 삭제될 때마다 파일과 관련된 정보가 MFT(Master File Table)에 기록된다. MFT는 모든 파일에 대응되는 MFT Entry들을 모아 놓은 배열이다. 각 MFT Entry에는 대응하는 파일의 메타 데이터를 저장한다.

MFT Entry 0~15번은 파일 시스템이 생성될 때 함께 생성되는 시스템 파일이다. 파일을 삭제하여도 MFT Entry는 남아 있고, 플래그 정보만 00으로 변하게 된다. MFT 파일에 남겨진 메타 데이터 정보를 분석하면, 파

일의 최근 접근·생성·수정 시간, 소유자의 정보, 파일명, 볼륨 이름, 파일 내용 등의 정보를 확인할 수 있다. MFT Entry 속성의 유형은 다음 표와 같다.

Entry number	Entry name	Description
0	$MFT	NTFS 상의 모든 파일들의 MFT Entry 정보
1	$MFTMirr	$MFT 파일 일부의 백업본
2	$LogFile	메타 데이터의 트랜잭션 저널 정보
3	$Volume	볼륨의 레이블, 식별자, 버전 등의 정보
5	\	볼륨의 루트 디렉토리
6	$Bitmap	볼륨의 클러스터 할당 정보
7	$Boot	볼륨의 부트 섹터 정보
11	$Extend	$Object, $UsnJrnl 등의 추가적인 파일 정보를 기록
12-15		예약 영역
16	$STANDARD_INFORMATION	파일의 생성, 접근, 수정 시간, 소유자 등의 일반적인 정보
48	$FILE_NAME	파일 이름(유니코드), 파일의 생성, 접근, 수정 시간
64	$VOLUME_VERSION	볼륨 정보(Windows NT 1.2 버전에만)
64	$OBJECT_ID	16바이트로 이루어진 파일, 디렉토리의 고유 값(3.0 이상에서만 존재)
128	$DATA	MFT 엔트리 파일 내용
144	$INDEX_ROOT	인덱스 트리의 루트 노드
160	$INDEX_ALLOCATION	인덱스 트리의 루트와 연결된 노드
176	$BITMAP	MFT Entry와 인덱스 레코드의 할당 정보 관리
256	$LOGGED_UTILITY_STREAM	암호화된 속성의 정보와 키 값

[표1] MFT Entry 속성 유형[41)]

나. 응용 프로그램에서 생성한 메타 데이터

응용 프로그램이 해당 파일을 관리하기 위해 저장하는 항목들로 응용 프로그램 별로 기록하는 정보의 항목들이 모두 다르다.

41) 박상준, 앞의 책, 397～405면 참조

1) 문서파일의 메타 데이터

MS Office, PDF 파일 등 문서 작성 또는 문서 보기 프로그램 경우 일정한 형식으로 문서에 관한 정보를 저장한다. 디지털 증거에서 가장 중요한 부분이라 할 수 있는 시간에 관한 정보도 메타 데이터를 통해 확인할 수 있다. 보통 'MAC시간'이라고 줄여서 부르는데, 수정된 시간(Modified), 접근된 시간(Acceessed), 생성된 시간(Created)을 의미한다.

이에 더하여 마지막 작성 시간(Last Written)도 디지털 증거 분석의 중요한 요소 중 하나이다. 이와 같이 컴퓨터가 생성한 타임스탬프를 분석하기 위해서는 우선 컴퓨터에 설정된 시간이 정확한지, 컴퓨터에 설정된 표준 시간대가 컴퓨터가 위치하고 있는 지역의 실제 시간과 일치하는지 여부에 대한 확인이 필요하다.

2) 사진파일의 메타 데이터

사진 촬영에 사용된 카메라의 제조사와 모델명이 기록되고, 사진이 수정된 경우에는 수정에 사용된 프로그램까지 메타 데이터로 확인이 가능하다. 그러나 해당 사진 파일을 'Adobe Photoshop' 프로그램을 사용하여 수정을 하게 되면 해당 사진을 찍는데 사용된 카메라에 관한 정보는 사라지지고, 편집 프로그램의 이름이 메타 데이터에 남게 된다.[42]

제 4 절 윈도우 레지스트리

윈도우 레지스트리는 마이크로소프트사에서 시스템과 응용프로그램 운영에 필요한 정보를 저장하기 위해 개발된 파일로 윈도우 포렌식의 보고라 할 만큼 포렌식에서 중요한 정보들을 많이 저장하고 있다.

윈도우 시스템 정보, 운영체제 정보, 사용자계정 정보, 시스템 정보, 응

42) Larry E. Daniel, Lars E. Daniel, Understanding Digital Evidence from the Warrant to the Courtroom(포렌식 전문가와 법률가를 위한 디지털 포렌식), 비제이퍼블릭, 2012. 232면

용프로그램 실행흔적, 최근 접근문서, 자동실행항목, 악성코드탐지, 저장매체 사용흔적 등을 확인할 수 있다.

레지스트리는 키(key), 값(value), 데이터(data)로 구성되어 있는데 '레지스트리 편집기'에서 그와 같은 값을 확인할 수 있다. 레지스트리 편집기에서 왼쪽에 트리 형태로 확인되는 부분이 키이고, 오른쪽에 이름이라는 항목으로 저장되어 있는 부분이 '값'이며, 그 옆으로 '값 저장 방식'과 '데이터'가 저장되어 있다.

하이브(Hive)는 레지스트리를 구성하는 키(key), 서브키(SubKey), 값(value) 등의 논리적인 집합을 말한다. 레지스트리 하이브 파일은 레지스트리를 저장하고 있는 물리적인 파일로, 데이터의 종류 별로 다양한 이름의 하이브 파일이 존재한다.

레지스트리 하이브 파일의 종류로는 SAM, SECURITY, SYSTEM, SOFTWARE, NTUSER.DAT, USERCLASS.DAT, BCD, COMPONENTS 등이 있다.

레지스트리에는 루트 키(Root Key)라는 것이 존재하는데 루트키는 레지스트리의 가장 상위에 있는 키로 총 6가지 종류의 루트키(HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG, HKEY_PERFORMANCE_DATA)가 있다.

HKEY_LOCAL_MACHINE은 시스템의 하드웨어와 소프트웨어의 설정 및 환경 정보를 저장하고 있는데 하이브 파일로는 SAM, SOFTWARE, BCD, COMPONENTS, SYSTEM이 있다. 위 하이브 파일의 저장 경로는 윈도우 운영체제 버전에 따라 달라질 수 있는데 %SystemRoot%[43] \System32\Config 경로에 주로 저장된다.

HKEY_USERS은 시스템에 등록된 사용자 및 그룹에 관한 정보를 저장하는데, 현재 로그인 된 사용자 계정과 관련된 정보를 관리하는 경우에는 HKEY_USERS 하위의 키를 직접 사용하지는 않고, 현재 로그인 된 사용

43) 윈도우 운영체제가 설치된 폴더 경로

자 계정과 연결된 HKEY_CURRENT_USER 키를 사용하게 된다. 또한 각 사용자 계정별로 부여된 SID(Security ID)를 서브 키로 가지고 있다. 주로 사용자 계정 하위 폴더에 저장된다.

HKEY_CURRENT_USER는 HKEY_USER 하위의 사용자 중에서 현재 로그인한 사용자에 대한 하이브를 보여준다. 하나의 시스템에 여러 개의 사용자 계정이 존재하지만, 현재 로그인한 사용자의 레지스트리를 연결하여 보여주며, 하위 키에는 운영체제에서 사용하는 설정 정보들이 저장되어 있다.

HKEY_CLASSES_ROOT는 시스템 운영을 위한 핵심 데이터를 저장하는데 실질적으로는 HKEY_LOCAL_MACHINE\Software\Classes와 HKEY_CURRENT_USER\Software\Classes가 논리적으로 결합한 형태이다.

HKEY_CURRENT_CONFIG는 시스템이 시작할 때 사용되는 시스템 하드웨어 설정 정보를 저장하고 있으며, 별도의 하이브 파일은 가지고 있지 않다.

HKEY_PERFORMANCE_DATA는 시스템 성능 관련 정보를 저장하는데 시스템의 성능을 측정하고 관리할 수 있으며, 레지스트리 편집기를 통해서는 접근이 불가능하고, 레지스트리 함수를 통해 접근할 수 있다.

레지스트리 하이브 파일 중 SAM(Security Accounts Manager) 하이브 파일에는 패스워드들의 해시 정보가 저장되므로 가장 중요한 하이브 파일이다. 패스워드 해시 정보들은 암호화되어 보호되는 경우가 많은데 이를 복호화하면 원본 패스워드의 해시 정보를 확인할 수 있다. 또한 'USER KEY'에서 마지막으로 로그온 한 시간, 로그온에 실패한 시간, 사용자의 계정(ID), 계정 정보 등을 확인할 수 있다.

그 밖에도 사용자 계정의 Default 폴더 경로, 최근 사용한 파일 및 프로그램 목록, 최근 실행하거나 수정한 문서파일 접근 기록, 사용한 USB 장치의 제조사, 모델명, 고유번호 정보, 설치 후 삭제한 프로그램 정보, 삭제된 사용자 계정 잔류정보, 메신저 사용 잔류 정보, 악성코드 감염 정보,

Windows 운영체제 설치 일시, 공유 폴더 기록 등을 확인할 수 있다.

컴퓨터 시스템에 외부 저장매체를 연결하면, 외부 저장 매체의 정보가 레지스트리에 등록이 되므로 레지스트리에 등록된 정보를 통해 외부 저장 매체의 제조사명, 제품 모델명, 시리얼넘버, 최초 연결시점, 마지막 연결시점 등의 정보를 확인할 수 있다. 이를 통해 최근 실행 파일, 각 응용프로그램별 레지스트리 사용 흔적, 파일의 접근·수정·생성 시간을 종합적으로 분석하여 사용자의 행위를 추적할 수 있다.

한글 프로그램은 레지스트리에 한글 설정 정보를 저장하고 있으므로 최근 열람한 파일 목록, 찾기/바꾸기 목록 등의 정보가 저장되어 있어 한글 프로그램의 사용 흔적을 찾을 수 있다.

MS Office 프로그램의 경우에도 레지스트리에 프로그램 설정 정보들을 저장하므로, 최근 사용한 폴더 경로, 최근 사용한 파일 경로 등의 정보가 저장되어 있어 MS Office 프로그램의 사용 흔적을 찾을 수 있다.

제 5 절 이벤트로그

이벤트로그란 윈도우에서 일어나는 특정 동작을 기록한 것으로 이벤트로그의 분석을 통해서 해당 시스템에서 일어난 동작들이 무엇이었는지 전반적으로 알 수 있다.

Windows Vista부터 윈도우 시스템에서 일어나는 일들을 구조화된 XML포맷을 기반으로 기록하게 되었고, 이와 같은 이벤트로그 분석을 통해 사용자 계정 로그온·오프, 응용 프로그램 실행 또는 종료, 시스템에서 발생한 문제와 보안 이벤트 등을 확인할 수 있다. 이벤트로그의 경우 사용자가 삭제할 수도 있으나, 복구도 가능하기 때문에 이와 같은 삭제 내역, 잔류하고 있는 정보 등은 디지털 포렌식에서 중요한 의미를 갖고 있다.

이벤트 로그는 Windows XP의 경우 %WINDIR%\System32\CONFIG 경로에 기록되며 확장자는 evt이었으나, Windows Vista 이후로는 이벤트 로그가 xml포맷으로 변환되면서 %WINDIR%\System32

\winevt\Logs 경로에 기록되며 확장자는 evtx이다.

이벤트 로그는 시스템 로그, 보안 로그, 응용 프로그램 로그, 기타 로그로 나눌 수 있는데 시스템 로그는 윈도우 시스템 구성요소가 기록하는 이벤트로 주로 운영체제 구성요소의 오류를 이벤트로 기록한다.

보안 로그는 로그인 시도 및 파일 생성, 열람, 삭제 등의 운영체제 리소스 사용에 관련된 이벤트를 기록하고, 응용프로그램 로그는 응용프로그램이 기록한 다양한 이벤트가 저장되는데 기록되는 이벤트는 해당 제품의 개발자에 의해 결정된다.

이벤트로그는 윈도우 운영체제에서 제공하는 이벤트 로그 뷰어[44]를 통해 열람할 수 있다.

이벤트로그는 운영체제에 따라 저장하는 항목이 다른데 윈도우XP에서는 종류(이벤트 심각도의 분류로 오류, 정보, 경고, 성공, 감사, 실패 감사로 분류), 날짜, 시간, 원본(이벤트를 기록한 소프트웨어 프로세스), 범주(이벤트의 원본에 의한 이벤트 분류로 주로 보안 로그에서 사용됨), 이벤트 ID(해당 원본의 특정 이벤트 유형을 식별하는 번호), 사용자(이벤트를 발생시킨 사용자의 이름), 컴퓨터(이벤트가 발생한 컴퓨터)를 저장하고, 윈도우 7이상의 경우 수준, 날짜 및 시간, 원본, 이벤트 ID, 작업 범주를 저장한다.

이벤트로그를 통해 저장장치의 연결·해제 시점, 제조사, 제품명, 시리얼 넘버 등을 확인할 수도 있으므로 이벤트로그의 확보도 디지털 포렌식에 있어 매우 중요한 부분이다.

제 6 절 저널링 파일 시스템

저널링 파일 시스템이란 디스크 데이터 영역에서 일어나는 모든 내용을 로그로 유지하면서 시스템 충돌이나 중단 시 로그에 있는 메타 데이터로 유실 데이터를 다시 만들어 충돌 전으로 데이터를 돌려주는 시스템을 말

44) 제어판 → 관리도구 → 이벤트뷰어

한다. 저널링 파일 시스템은 변경사항을 기록하는 특별한 구역을 저널로 할당하여 특정 데이터를 비정상적인 중간 상태로 남겨둘 수 있도록 설정한다. 즉 기록을 남겨두는 백업기능과 복구능력이 있는 파일시스템이다.

피압수자들이 압수현장에서 시스템을 인위적으로 다운시키고 오작동 시키는 방법으로 증거를 은닉하거나 삭제하는 경우에도 위 저널링 파일 시스템에 기록된 로그기록들을 통해 정보를 확인하고 복구할 수 있으므로 디지털 포렌식에서 유용하게 사용할 수 있는 기능이다.

제 7 절 볼륨 새도우 카피

Windows Vista 이후 버전부터는 시스템 보호를 위해 정기적으로 복원 지점을 만들고 저장한 뒤, 시스템이 오작동하는 경우에 그 복원 지점을 기준으로 그 이전 상태로 시스템 파일과 레지스트리값을 되돌리고 백업하는 VSC(Volume Shadow Copy) 기능을 보유[45] 하고 있다.

기본적으로 복구되는 항목은 레지스트리, filelist.xml 파일의 <include> 부분에 확장자가 포함된 파일이다. VSC 기능으로 인해 완전한 파일 내용의 복구가 가능하고, 덮어쓰기로 삭제된 파일의 복구도 가능하다. VSC로부터 과거의 폴더나 파일의 흔적을 찾을 수 있는데, 복구된 파일의 타임존은 기본적으로 국제표준시(UTC)라는 점을 유의해야 한다.

그러나 볼륨 섀도우 카피의 경우 그 보관 시간이 길지 않고 실시간으로 새로운 파일들이 업데이트 되고 있으므로 오래 전의 파일 저장 내역 등은 확인하기 어렵다.

제 8 절 슬랙 공간

슬랙 공간이란 논리적인 데이터의 구조와 실제 물리적인 저장 공간 간

45) 노명선, 구희진, 김영철, 배대한, 최대건, 최우석 공저, 「디지털포렌식 기술」, 미디어북, 2018, 211~213면 참조

의 차이로 생기는 낭비 공간으로 정의할 수 있다. 즉 표면상으로는 사용되는 공간으로 분류되나 실제로는 사용되지 않는 공간으로 주로 데이터 은닉 장소로 활용[46]된다.

파일을 저장할 때 실제 논리적 구조와는 무관하게 물리적으로는 섹터 단위(512Bytes)로 저장되는데, 이에 따라 데이터가 쓰여진 공간과 쓰여지지 않은 공간이 함께 존재하게 되어 필연적으로 이와 같은 슬랙 공간이 생기게 되는 것이다.

슬랙공간은 총 4가지로 나뉘는데, 램 슬랙(RAM Slack), 드라이브 슬랙(Drive Slack), 볼륨 슬랙(Volume Slack), 파일 시스템 슬랙(File System Slcak)으로 나눌 수 있다.

램 슬랙이란 메모리(RAM)에 저장되는 데이터가 디스크에 저장될 때 위와 같이 512Bytes 단위로 기록되는 특성에 의해 생기는 공간을 말하며 섹터의 남는 공간이기 때문에 섹터 슬랙이라 부르기도 한다. 데이터가 기록된 가장 마지막 섹터의 남는 공간이므로 파일의 마지막 부분과 구별하기 위해 0x00으로 초기화시켜여 한다.

클러스터[47]의 사용으로 인해 낭비되는 공간 중 램 슬랙을 제외한 나머지 부분을 파일 슬랙 또는 드라이브 슬랙이라 하며 램 슬랙과 달리 데이터가 그대로 남아 있다.

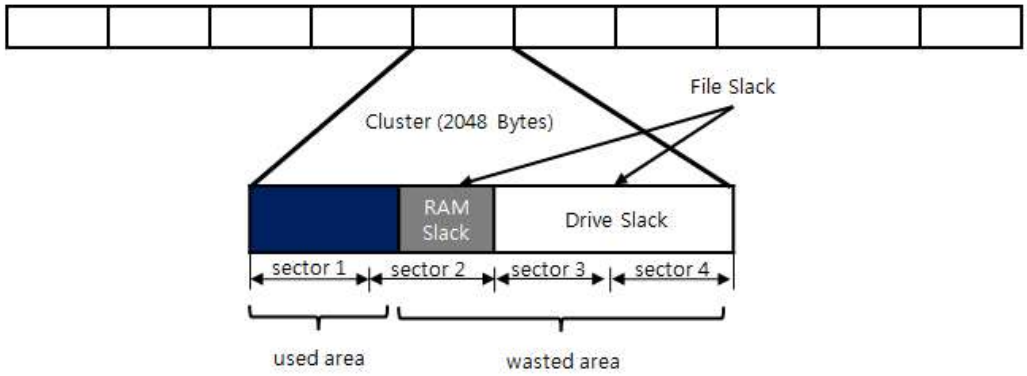
하드디스크를 논리적인 단위인 클러스터 단위로 할당한 뒤 남는 공간을 파일 시스템 슬랙 공간이라 하는데, 최근에는 악성코드를 이 파일 시스템 슬랙 공간에 숨겨두는 케이스가 많아 개인정보 침해 사건 수사 시 유의해서 살펴보아야 하는 부분이다.

마지막으로 전체 볼륨 크기와 할당된 파티션의 크기의 차이로 발생되는 공간을 볼륨 슬랙이라 한다. 다른 슬랙과 다르게 파티션 크기의 변경을 통해 임의로 생성 가능하기 때문에 데이터 은닉이 보다 쉽게 이루어질 수

---

46) 노명선, 구희진, 김영철, 배대한, 최대건, 최우석 공저, 앞의 책, 125면 참조
47) 클러스터(Cluster)란 운영체제가 저장장치에 데이터를 읽고 쓰는 논리적인 기본 단위로, 파일시스템이나 운영체제에 따라 그 크기가 다름

있다.



[그림1] 슬랙공간 이미지48)

제 9 절 프리패치

프리패치란 운영체제에서 제공하는 메모리 관리 정책 중 하나로 실행 파일을 메모리로 로딩할 때의 효율을 최대한 끌어올리기 위한 목적으로 개발되었다. 윈도우 운영체제는 실행 파일이 사용하는 시스템 자원 목록을 미리 저장하였다가 윈도우 부팅 시 프리패치 파일을 모두 메모리에 로드한 후 실제 사용할 때 메모리에 해당 정보를 가져올 수 있도록 하여 실행 속도를 향상시킨다.

부트 프리패치와 응용프로그램 프리패치로 구별되며 pf 확장자로 저장된다. 부트 프리패치는 윈도우 운영체제 부팅 시 하드 디스크의 부담을 줄이기 위해 사용하고, 응용 프로그램 프리패치는 실행 파일 실행 시, 프리패치에 해당 파일이 존재하지 않으면 생성된다.

실행 파일에 대한 정보를 프리패치 파일로 생성하고, 실행 파일을 다시 실행할 때 해당 프리패치를 사용함으로써 컴퓨터 시스템 자원을 관리한다.

48) http://forensic.korea.ac.kr/DFWIKI/index.php/Slack 참조

프리패치는 윈도우가 설치된 디렉토리 하위의 프리패치 폴더에 저장된다. 윈도우10부터는 프리패치 파일이 압축되어 저장되므로 w10pdfecomp.py[49]를 이용하여 압축을 해제한 후 분석을 하면 된다. 프리패치를 분석하게 되면 실행된 응용프로그램 이름, 실행 횟수, 마지막 실행 시간, 참조되는 목록, 프리패치 파일의 시간 정보, 경로 등의 데이터를 획득할 수 있다.

실행 경로에는 외부 경로도 기록되므로 저장매체에 연결된 외부 저장장치를 찾을 수 있다. 또한 프리패치에서 획득한 정보들을 분석하면 부팅 시 로드되는 악성코드나 응용 프로그램과 연결된 악성코드의 실행 프로그램을 발견할 수도 있다.

제 10 절 휴지통

휴지통이란 삭제된 파일 또는 디렉토리가 이동하는 영역으로, 파일을 삭제하는 경우 파일 시스템 메타 데이터만 변경되며, 실제 파일의 데이터는 변경되지 않으므로 원본 파일 복원을 위해 휴지통에는 다양한 정보가 저장되고, 사용자가 휴지통의 최대 크기를 설정할 수도 있다.

각 파티션 내 사용자 계정마다 한 개씩의 휴지통이 존재한다. 휴지통의 경로는 윈도우가 설정된 파티션에서 찾을 수 있는데 WindowsXP의 경우에는 %SystemDrive%:\Recycler\[사용자SID]에서, Windows7 이상의 경우에는 %SystemDrive%:\Recycle.Bin\[사용자SID]에서 찾을 수 있다.

WindowsXP의 경우 삭제된 파일의 형식은 D[원본 파일의 드라이브 이름][인덱스 번호].[원본 파일 확장자]의 형식으로 교체되어 휴지통에 저장된다.

Windows7 이상의 경우 삭제된 파일의 형식은 $R[임의 문자열].[원본 파일 확장자] 또는 $I[임의 문자열].[원본 파일 확장자] 쌍으로 존재하여 휴지통에 저장된다.

---

49) Github Gist, “Windows 10 Prefetch (native) Decompress”, 2018. 07. 04, https://gist.github.com/dfirfpi/113ff71274a97b489dfd#file-w10pfdecomp-py

제 11 절 바로가기

바로가기란 윈도우 운영체제에서 응용프로그램, 디렉토리, 파일, URL 등의 특정 객체를 참조하는 파일로 흔히 링크 파일이라고 불리우며, LNK 확장자를 가지며 바로가기 파일을 실행하면 대상 객체가 호출된다.

윈도우 운영체제 설치, 응용프로그램 설치 시 생성되고, 문서 파일 열람 시 생성되거나 사용자가 직접 생성할 수도 있다. 주로 바탕화면(Desktop), 최근문서(Recent), 시작 프로그램(Stast Menu), 빠른 실행(Quick Launch)에 생성된다. 저장경로는 윈도우가 설치된 드라이브이다.

최근 열람 문서를 확인하거나 외부 저장 매체를 통한 정보 유출을 확인할 때 유용하다.

바로가기 파일을 분석하면 대상 객체의 생성 시간, 수정 시간, 접근 시간, 대상 객체의 크기, 대상 객체의 경로(시작 위치), 볼륨 정보(시리얼 넘버, 실행파일, 네트워크 드라이브 정보 등) 등을 획득할 수 있다.

바로가기가 삭제된 경우에는 MFT 엔트리의 $OBJECT_ID 속성을 분석하여 파일의 접근 흔적을 식별할 수 있다.

제 12 절 점프리스트

Windows7부터 추가된 기능으로 응용 프로그램에서 특정 파일을 실행시키거나 어떤 행위를 했을 때 기록되는 것으로 실행 파일 마우스 오른쪽 버튼을 누르면 확인할 수 있는데 최근 항목, 자주 사용하는 목록/자주 방문한 페이지, 작업 가능한 목록, 사용자가 고정한 값 등을 확인할 수 있다. 사용자 계정의 하위 폴더에 저장되며 사용자별로 별도의 폴더가 존재한다.

점프리스트는 AutomaticDestications 폴더와 CustomDestications 폴더로 나눠지는데 AutomaticDestications 폴더에는 최근 사용한 목록이나 사

용자가 고정시키는 목록이 저장되고, CustomDestications 폴더에는 자주 사용되는 목록이나 작업 목록이 저장된다. 점프리스트에 사용되는 16자리 16진수는 응용프로그램별로 고유한 값을 가지고 있다.

점프리스트가 삭제된 경우에도 MFT 엔트리의 $OBJECT_ID 속성을 분석하여 파일의 접근 흔적을 식별할 수 있다.

제 13 절 인터넷 접속 관련 기록

인터넷 사용은 현대인들이 컴퓨터를 사용함에 있어 필수적이고 보편화되어 있으므로 수사기관에서는 피의자가 인터넷을 통해 어떤 행동을 했는지 확인하기 위해 웹 브라우저의 활동 기록을 분석하여 수사에 활용하기도 한다. 웹 브라우저는 웹 서버에 사용자가 방문하여 웹 서비스를 이용할 때 도와주는 응용프로그램으로 웹 서버에서 제공한 데이터는 사용자의 컴퓨터에 저장되므로 이러한 특성들을 이용하여 사용자의 인터넷 활동 이력을 찾고 분석할 수 있다.

1. 쿠키(Cookie)

웹 사이트에 접속할 때 자동적으로 만들어지는 임시파일로 이용자가 접속한 웹페이지의 도메인, 경로, 만기일, 보안속성, 상품 구매 내역, ID, PW, IP 주소 등의 정보를 담고 있는 파일을 말한다. 사용자가 웹 서비스를 이용하다가 웹 브라우저가 종료된다 하더라도 종료 직전에 사용자가 했던 행위들을 기록하는 기능이다.

쿠키는 이용자들의 홈페이지 접속을 용이하게 하기 위해 만들어졌으나, 최근에는 이와 같은 정보를 바탕으로 타깃 마케팅 등에 활용하기도 하고, 사생활을 침해하는 도구로 변칙 활용되면서 개인 정보가 위협을 받기도 한다. 이와 같은 쿠키를 이용하면 이용자가 어떤 웹 서비스를 이용하고, 그 안에서 어떠한 행위를 했는지 추적이 가능할 수 있다.

2. 히스토리(History)

히스토리란 웹 서비스를 방문한 기록을 의미한다. 이용자가 어떤 웹 서비스를 사용하던 중 다른 사이트로 이동했다가 다시 돌아가고 싶을 때 뒤로가기 버튼을 이용하게 되는데 이때 히스토리 기능을 이용하여 이전 사이트로 돌아갈 수 있다. 이와 같은 히스토리 기록을 통해서 이용자가 방문한 사이트 등을 확인할 수 있다.

3. 웹 캐쉬(Web Cache)

웹 서비스에 방문하는 경우 html, css, 자바스트립트, 이미지 등을 다운로드 하게 되는데 방문할 때마다 이와 같은 파일들을 새로 다운로드 받는다면 불필요한 시간이 많이 소모된다. 이에 따라 이를 절약하기 위해 이미 다운로드 한 파일이 새로 접속하는 웹 서비스에서 다운로드 받아야 하는 파일들과 다르지 않은 경우에는 기존에 다운로드 되어 있는 파일을 로드하여 신속하게 서비스를 이용할 수 있기 위해 만들어진 파일이다. 이와 같은 웹 캐쉬를 분석함으로써 피의자가 어떤 웹 서비스에 방문하였는지 방문 이력 등을 확인할 수 있어 수사에 용이하게 사용할 수 있다.

제 4 장 디지털 증거 압수수색 실무 및 문제점

제 1 절 선별압수수색의 원칙 및 문제점

1. 관련 규정

현행 형사소송법 제106조[50]에서는 원칙적으로 범죄사실과 관련성이 있

는 부분에 대해서만 선별적으로 압수를 하고, 예외적인 경우 매체 자체의 압수가 가능하며, 이와 같은 집행방법에 대하여 사전에 영장에 표기하고, 개인정보보호법에 따른 정보주체에게 통보 등의 조치를 하도록 규정하고 있다.

또한 법원의 수색에 대하여 형사소송법 제109조에서 '법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 피고인의 신체, 물건 또는 주거 기타 장소를 수색할 수 있다.'고 규정하고 있으며, 수사기관의 압수, 수색, 검증에 대해서는 형사소송법 제215조에서 '검사는 범죄수사에 필요한 때에는 피의자가 죄를 범하였다고 의심할만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 것에 한정하여 지방법원 판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.'라고 규정하고 있다.

이처럼 우리 형사소송법은 기본적으로 혐의사실과의 관련성을 압수수색의 요건으로 명시하고 있고, 정보저장매체를 압수하는 경우에도 원칙적으로는 혐의사실과 관련된 부분을 특정하여 이에 한해 정보의 범위를 정하여 출력하거나 복제하는 선별압수를 하도록 규정하고 있다.

2. 판례의 태도

---

50) 형사소송법 제106조(압수) ① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다.
② 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.
③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다.
④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다.

이와 같은 선별압수 원칙은 형사소송법 제106조 제3항이 2011. 7. 18. 개정되기 이전 소위 '전교조' 사건에서도 명시적으로 판시한 바 있으나, 2015년 종근당 사건 판례를 기점으로 디지털 증거 압수수색의 기본 원칙으로 자리 잡게 되었다.

전교조 사건[51]에서 대법원은 "전자정보에 대한 압수·수색 영장의 집행에 있어서는 원칙적으로 영장 발부의 사유로 된 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장의 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 그와 같은 경우에 그 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 예외적으로 허용될 수 있다."고 판시하였다. 또한 예외적으로 저장매체 자체를 직접 혹은 하드카피나 이미징 등의 형태로 반출하더라도 관련성 있는 정보만을 탐색하여 출력·복제해야 하며 그 과정 역시 전체적으로 압수·수색영장 집행의 일환이라고 보았다.

종근당 사건[52]에서 대법원은 "전자정보가 담긴 저장매체 또는 복제본을 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 일련의 과정에서, 피압수·수색 당사자나 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치가 취해지지 않은 경우, 압수·수색이 원칙적으로 부적법하다고 보았고, 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였더라도 이는 마찬가지라 판단"하였다.

또한 전자정보에 대한 압수・수색 과정에서 저장매체 압수·이미징·탐색·복제 및 출력행위 등 일련의 행위가 모두 진행되어 압수・수색이 종료된 후 전체 압수수색 과정을 단계적·개별적으로 구분하여 각 단계의 개별 처분의 취소를 구하는 준항고에 대해, "당해 압수·수색 과정 전체를 하나

51) 대법원 2011. 5. 26. 선고 2009모1190 결정
52) 대법원 2015. 7. 16. 선고 2011모1839 결정

의 절차로 파악하여 그 과정에서 나타난 위법이 압수·수색 절차 전체를 위법하게 할 정도로 중대한지 여부에 따라 전체적으로 압수·수색 처분을 취소할 것인지를 가려야 한다."고 판시하며 이때 위법의 중대성은 위반한 절차조항의 취지, 전체과정 중에서 위반행위가 발생한 과정의 중요도, 위반사항에 의한 법익침해 가능성의 경중 등을 종합하여 판단하여야 한다고 판시하였다.

범죄사실과의 관련성의 기준에 대해서 대법원은 "압수의 대상을 압수·수색영장의 범죄사실 자체와 직접적으로 연관된 물건에 한정할 것은 아니고 압수·수색영장의 범죄사실과 기본적 사실관계가 동일한 범행 또는 동종·유사의 범행과 관련된다고 의심할 만한 상당한 이유가 있는 범위 내에서는 압수를 실시[53]할 수 있다"고 보고 있다.

통신사실확인자료 제공요청과 관련된 판례에서는 "혐의사실과의 객관적 관련성은, 통신사실확인자료제공 요청허가서에 기재된 혐의사실 자체 또는 그와 기본적 사실관계가 동일한 범행과 직접 관련되어 있는 경우는 물론 범행 동기와 경위, 범행 수단 및 방법, 범행 시간과 장소 등을 증명하기 위한 간접증거나 정황증거 등으로 사용될 수 있는 경우에도 인정될 수 있다. 다만 통신비밀보호법이 위와 같이 통신사실확인자료의 사용 범위를 제한하고 있는 것은 특정한 혐의사실을 전제로 제공된 통신사실확인자료가 별건의 범죄사실을 수사하거나 소추하는 데 이용되는 것을 방지함으로써 통신의 비밀과 자유에 대한 제한을 최소화하는 데 입법 취지가 있다고 할 것이다. 따라서 그 관련성은 통신사실확인자료제공 요청허가서에 기재된 혐의사실의 내용과 당해 수사의 대상 및 수사 경위 등을 종합하여 구체적, 개별적 연관관계가 있는 경우에만 인정된다고 보아야 하고, 혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로 관련성이 있다고 할 것은 아니다. 그리고 피의자와 사이의 인적 관련성은 통신사실 확인자료 제공요청 허가서에 기재된 대상자의 공동정범이나 교사범 등 공범이나 간접정범을 물론 필요적 공범 등에 대한 피고사건에 대해서도 인정될 수 있다.[54]"고 판시하여 객관적 관련성, 주관적 관련성, 시간적 관련성을 그 기

53) 대법원 2009. 7. 23. 선고 2009도2649 판결

준으로 제시하고 있다.

한편 "저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수수색영장 집행에 포함된다고 보아야 하므로 그러한 경우 문서출력 또는 파일복사의 대상 역시 혐의사실과 관련된 부분으로 한정되어야 함은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의의 원칙상 당연하다"고 판시[55]하였다.

3. 선별 압수수색 실무

앞서 살펴본 바와 같이 우리 법원은 디지털 증거에 대하여 압수현장에서 혐의사실과 관련된 전자정보의 범위를 정하여 압수하되, 출력·복제가 불가능하거나 압수 목적을 달성하기 현저히 곤란한 경우에 한하여 저장매체에 들어 있는 전자정보 전체를 복제하거나 저장매체 자체의 압수를 허용하고 있다.

법원에서 발부하는 영장 별지 "압수 대상 및 방법의 제한" 부분에 따르면 전자정보 전체를 복제하는 예로 ① 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, ② 혐의사실과 관련된 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견되는 경우, ③ 출력·복제에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, ④ 그 밖에 위 각 호에 준하는 경우를 들고 있다.

최근 항소심 판례에서는 '전자정보가 삭제·폐기된 정황이 발견되었으므로 미할당영역에 존재하는 삭제된 파일을 복구하는 등의 과정에서 물리 이미징을 하여야 함에도 논리 이미징을 하였고, 그 과정에서 쓰기방지장치도 사용하지 않아 원본 파일과의 동일성을 인정할 수 없다'는 취지의 피고인의 주장에 대해 "이 사건 영장에는 정자정보가 삭제·폐기된 정황이

54) 대법원 2017. 1. 25. 선고 2016도13489 판결
55) 대법원 2015. 10. 29. 선고 2015도 9784 판결

발견되어 미할당역역에 존재하는 삭제된 파일을 복구하는 경우라도 반드시 저장매체 자체를 반출하거나 저장된 파일 전체를 물리 이미징할 것을 요구하고 있지 않으며, 쓰기방지장치를 반드시 사용해야한다고 명시하고 있지 않고, 관련 법령에서도 이에 대한 근거 규정이 없으며, 물리 이미징이나 논리 이미징 모두 정상 파일 뿐 아니라 삭제된 파일의 내용을 이루는 데이터 뿐만 아니라 파일 자신의 정보를 담고 있는 메타데이터 정보까지 동일하게 복원되어 복사되므로, 범죄 혐의와 관련된 내용만을 선별하여 압수, 즉 논리 이미징 한 것이 위법하다고 할 수는 없다"고 판시[56]하였다.

저장매체 자체를 압수할 수 있는 예외적인 상황으로 ① 집행현장에서 하드카피·이미징이 물리적·기술적으로 불가능하거나 극히 곤란한 경우, ② 하드카피·이미징에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우 ③ 그 밖에 위 각 호에 준하는 경우를 규정하고 있다.

이처럼 법원은 관련성이라는 기준을 근거로 디지털 증거를 압수수색하는 방법을 매우 제한적으로 해석하고 있다. 이에 따라 대검찰청에서도 영장 실무를 반영하여 2021. 1. 1.부터 단계적 압수수색검증방안[57]을 도입하여 선별압수수색을 원칙으로 하되, 이에 따른 압수가 불가능할 경우 전자정보 전체를 복제하여 반출[58]하고, 전체 복제가 불가능하거나 곤란한 경

56) 부산고등법원 2020. 2. 6. 선고 2018노121 판결 참조

57) 「디지털 증거의 수집·분석 및 관리 규정」<대검 예규 제1551호, 2021. 1. 1. 시행>
제20조(전자정보의 단계적 압수·수색·검증) ① 주임검사등은 정보저장매체등에 기억된 전자정보를 압수하는 경우에는 해당 정보저장매체등의 소재지에서 수색 또는 검증한 후 범죄사실과 관련된 전자정보의 범위를 정하여 출력하거나 복제하는 방법으로 한다.
② 제1항에도 불구하고 그에 따른 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우에는 압수·수색 또는 검증 현장에서 정보저장매체등에 들어 있는 전자정보 전부를 복제하여 그 복제본을 정보저장매체등의 소재지 외의 장소로 반출할 수 있다.
③ 제1항 및 제2항에도 불구하고 그에 따른 압수 방법의 실행이 불가능하거나 그 방법으로는 압수의 목적을 달성하는 것이 현저히 곤란한 경우에는 피압수자등이 참여한 상태에서 정보저장매체등의 원본을 봉인하여 정보저장매체등의 소재지 외의 장소로 반출할 수 있다.

우 저장매체 원본을 봉인하여 반출[59]하도록 규정하고 있다.

위와 같은 디지털 증거의 압수방법 각각의 장단점을 살펴보면 다음과 같다.

선별정보만을 압수하는 경우 빠르고 적은 비용으로 압수할 수 있고 장비 수집 책임과 위험성 논란에서 벗어날 수 있다는 장점이 있으나, 전문가만이 증거 선별을 할 수 있고, 시스템 관리자와 소유자(사용자)의 도움 필요하며 비전문가가 압수하는 경우 증거를 놓치거나 파괴, 잘못된 증거 수집이 이루어질 수 있어서 위험성이 큰 방법이다.

다음으로 저장매체 자체를 복제하는 경우인데, 압수 후에 통제된 환경에서 조사할 수 있고, 복제본으로 작업을 하면 원본 증거의 손상을 방지할 수 있으므로, 장비 손상과 영업 손실을 최소화 할 수 있다. 그러나 전문 장비와 전문적인 기술이 필요하고, 디스크가 암호화된 경우에는 드라이브 내 모든 증거에 엑세스하지 못할 위험이 존재하며, RAM과 같은 일부 증거는 파괴될 위험이 있다.

마지막으로 범죄 결과로서의 장비, 범죄도구로서의 장비, 증거로서의 장비, 대량의 디지털 증거를 포함하는 장비에 대해 장비 자체를 수집하는 경우, 장점으로는 전문 기술이 필요 없고, 상대적으로 간단하여 논란의 여

---

58) ① 파일 암호화 등으로 인해 범위를 정한 출력·복제가 불가능한 경우, ② 안티포렌식 등 범죄혐의와 개연성이 있는 디지털 정보가 조작 또는 삭제된 정황이 발견된 경우, ③ 정보저장매체등에 저장되어 있는 정보가 방대하여 현장에서 출력·복제 방식으로 압수하는데 많은 시간이 소요되어 피압수자의 사생활의 평온이나 영업 활동을 침해할 우려가 있는 경우, ④ 정보저장매체등이 사이버범죄 및 새로운 유형의 첨단범죄에 이용되는 등 수사 또는 공소의 제기 및 유지를 위하여 정보저장매체등에 기억된 디지털 증거의 종합적인 분석이 필요한 경우, ⑤ DB시스템이나 RAID시스템 등과 같이 분석 대상 시스템과 동일한 시스템을 구축하여 분석해야 하는 경우, ⑥ 그 밖에 위 각 호에 준하는 경우

59) ① 정보저장매체등이 물리적으로 손상된 경우, ② 정보저장매체등에 암호가 걸려 있고 피압수자등이 협조하지 않는 경우, ③ 현장에서 복제·출력할 수 있는 장비나 도구가 개발되어 있지 않거나 준비에 장시간이 소요되는 경우, ④ 현장에 전력 공급이 원활하지 않은 경우, ⑤ 피압수자가 위력을 행사하여 정상적인 압수·수색 집행이 불가능한 경우, ⑥ 전자정보의 전부 복제 반출을 위한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 현저히 침해하는 경우, ⑦ 정보저장매체등 또는 동 매체에 기억된 전자정보가 몰수대상인 경우, ⑧ 그 밖에 위 각 호에 준하는 경우

지가 적으며, 압수 후에 통제된 환경에서 조사될 수 있다는 점을 들 수 있다.

반면, 단점으로는 이송 중 장비 손상 위험, 디스크가 암호화 된 경우 드라이브 내 모든 증거에 엑세스하지 못할 위험의 존재, BIOS password 모르는 경우 부팅이 안 될 위험, RAM과 같은 일부 증거가 파괴될 위험이 있으며, 불필요한 영업 손실이 발생할 수 있다.

전자정보 선별을 위해 압수 현장에서 주로 사용되는 도구는 CFT(Computer Forensic Tool)이다.

CFT를 활용하여 증거를 선별하는 구체적인 절차를 살펴보면, 첫째로 CFT 프로그램이 저장된 USB를 대상 PC에 연결한다. CFT 프로그램이 연결되면 저장매체 내 파일들이 문서파일, 이메일, 압축파일 등 파일유형에 따라 자동으로 분류된다.

두 번째로 압수대상 가능성이 있는 파일을 지정하여 북마크로 이동시킨다. 세 번째로 북마크로 이동된 파일들 중 키워드를 입력하거나(Search Expression), 수색 대상 파일들 제한(Search Target), 파일 생성일시 등으로 제한(Search Filter) 등 다양한 조건으로 전자정보의 범위를 압축[60]시킨다. 네 번째로 키워드 검색 등 다양한 조건으로 압축된 파일들을 '미리

---

60) 파일 검색시 주로 활용하는 방법은 다음과 같다.
1. 파일명 검색 : 혐의사실과 관련되거나 영장에 기재된 '검색어'로 파일명을 검색하여 사건과의 관련성 여부를 확인할 수 있으나, 작성자가 파일명을 내용과 상관 없는 단어로 저장하였을 경우 검색이 불가능
2. 파일 시그니처 검색 : 파일 시그니처란 파일 헤더에 저장되어 있는 파일 종류 식별을 위한 정보로 같은 종류의 파일은 같은 시그니처 값을 갖고 있고, 파일 확장자와 달리 변경이 어렵다.(파일 확장자의 경우 OS시스템이나 응용프로그램이 파일의 종류를 식별하기 위해 파일 이름 뒤에 3byte 크기로 저장되는데 사용자가 이를 쉽게 변경할 수 있음)
3. 파일 확장자 검색 : 찾고자 하는 파일이 영상인 경우(avi, wmv, mp4), 사진인 경우(jpg, gif, bmp, png), 문서인 경우(hwp, docx, html, txt) 응용프로그램의 종류별로 해당 증거과 관련성 있는 확장자를 검색하여 파일 찾을 수 있음
4. 파일 시간별 검색 : 혐의사실과 근접한 시간에 생성, 수정, 접근한 파일을 검색하여 사건과의 관련성 여부 확인할 수 있음
5. 파일내용 검색 : 문서파일에 한해 가능하고, 데이터용량이 방대하거나 컴퓨터의 성능이 저성능인 경우, 문서파일을 스캔한 경우 등에는 검색이 어려울 수 있음

보기' 기능(Contents View)을 통해 최종 선별한 다음 논리 이미징을 한다. 마지막으로 자동 생성된 해시값을 피압수자 등에게 확인시킨 후 피압수자 등의 서명·날인을 받고, 전자정보 상세목록은 대상 PC, 노트북 등 디지털기기의 바탕화면에 파일로 저장해두는 방법으로 피압수자에게 교부하게 된다.

4. 해외 입법례

가. 미국

미국의 경우 다양한 현장상황 및 디지털 증거의 특수성을 고려하여 수사관에게 구체적인 압수수색방법에 대하여 합리적 재량을 부여[61]하고 있다.

또한 디지털 증거의 압수수색방법이 문제가 된 사건에서 "기술이 진보하고 수사기관의 경험이 발전하여 현장에서의 컴퓨터 기록 수색이 가능해지고 실효성을 갖추는 날이 오기 전까지는 (제3지로 이동한 후에 수색할 목적으로), 컴퓨터 하드웨어 전체를 압수하는 것은 적절히 안전장치를 갖춘 이상 필연적으로 수행되어야 하는 경우가 있다. 수정헌법 제4조에서도 이를 허용할 수 있지만, 수사기관은 피압수자의 영업이나 개인생활의 침해를 최소화하도록 가능한 한 빠른 시일 내에 복사를 수행하고 압수한 매체를 반환하여야 한다"고 판시[62]하여 관련성 유무에 대한 판단 전에 매체의 제3지로의 이동 가능성을 인정하고 있다.

나. 독일

독일은 일반적인 압수수색 규정에 더하여 형사소송법 제110조[63]에서 서류의 검열 규정을 두고 있다. 서류의 검열 규정이란 압수대상물에 해당

---

61) Dalia v. United States, 441 U. S. 238(1979) 영장을 집행함에 있어서 그 세부적인 절차는 일반적으로 이를 집행하는 수사관의 재량에 맡겨야 한다는 취지
62) United States v. Hunter, 13 F. Supp.2d 574(D. Vt., 1998)
63) 독일 형사소송법 제110조 ① 수사에 필요한 서류의 검열은 검사와 검사의 지시를 받은 사법경찰관의 권한이다.

하는지 여부를 구체적으로 확인하는 절차로, 현장에서 행해지는 경우도 있고, 수사기관의 사무실에서 행해지는 경우(임시적 보전)도 있다. 그 과정에서 소유자의 참여권을 보장하는 규정이 존재하였으나 2004년도 형사소송법 개정으로 삭제되었으며, 사건에 따라 검열에 의한 기본권 침해 정도와 소추기능 수행의 효율성을 비교하여 개별적으로 판단할 수 있다[64] 고 해석하고 있다.

이와 같은 규정은 디지털 증거에서도 유사한 논리로 적용되므로 범죄의 중대성, 혐의의 정도, 증거의 중요성, 기본권 침해 정도 등을 종합적으로 고려하여 개별 사건에 따라 탄력적으로 적용되고 있다.

5. 선별압수수색과 관련된 문제점

디지털 증거의 경우 비가시성, 비가독성, 대량성 등 디지털 증거의 고유한 특성으로 인해 사건 현장에서 관련성 있는 증거를 선별함에 많은 어려움이 있다. 또한 컴퓨터, 휴대폰 등의 디지털 정보 저장매체의 경우 개인에 대한 방대한 양의 정보가 저장되어 있어 무분별한 압수수색을 인정하게 되면 피압수자의 개인정보 및 프라이버시 등 인권침해를 야기할 수 있다.

그러므로 디지털 증거에 있어 관련성 인정은 비례의 원칙 하에서 개별적으로 사안에 따라 판단함이 상당하고 미국, 독일 등 각국의 디지털 증거에 대한 입장도 이와 유사하다.

그러나 현행 실무는 디지털 증거에 있어서도 '선별압수의 원칙'을 고집하여 현장에서 초기에 확보해야 할 증거의 상당 부분을 확보하지 못하는 우를 범하고 있다.

특히 컴퓨터가 자동으로 생성한 정보의 경우, 사용자가 직접 생성한 정보와는 다른 기준에서 관련성 여부를 판단해야 할 것이다.

컴퓨터 자동 생성 증거의 경우 형사소송법 제313조 제2항의 해석상 진

64) BVerfGE 124, 43, 96.

술서 작성자가 공판준비나 공판준비 기일에 진정성립을 부인하는 경우에 디지털 포렌식 등의 방법으로 성립의 진정을 증명할 수 있으므로, 작성자가 진정성립을 부인하지 않는 경우에는 관련성을 인정할 수 없다고 보는 견해[65]도 있다.

그러나 작성자가 공판단계에서 진정성립을 부인할지 여부는 압수수색 단계에서는 예측하기 어렵고, 이와 같이 진정성립을 부인하는 작성자의 경우, 압수수색 당시 진정성립과 관련된 컴퓨터 자동 생성 증거를 미리 확보해 놓지 않으면 이를 의도적으로 은닉, 삭제할 가능성이 더욱 높을 것이다.

피압수자의 의도적인 변경이 아니더라도 컴퓨터 자동생성 증거의 경우 열람, 탐색기에서의 선택 등 의도하지 않은 접근만으로도 디지털 증거의 속성 등이 쉽게 변할 수 있다.

또한 컴퓨터 자동 생성 증거의 경우 사용자 생성 증거와 달리 사생활 및 개인정보의 침해 가능성이 낮고, 디지털 전문증거의 진정성립의 자료로 사용될 가능성이 높으며, 압수수색 당시 수집하지 않으면 변경가능성이 높고, 진정성립 인정의 자료는 직접증거가 아닌 간접증거에 해당하므로 자유로운 증명의 대상으로 볼 수 있을 것이다.

즉 컴퓨터가 자동·임의로 생성한 증거의 경우, 관련성을 폭 넓게 인정하여 압수수색 대상 자체에서 제외시키는 방향이 아니라 임의적인 접근을 차단하는 방향으로 검토 함이 상당할 것이다.

제 2 절 참여권 보장과 관련된 실무 및 문제점

1. 관련 규정

형사소송법 제219조, 제121조에서는 '수사기관이 압수·수색영장을 집행

65) 김영철, "디지털 본래증거 수집 방안", 서울대학교 융합과학기술대학원 석사학위 논문, 2018. 33면 참조

할 때에는 피압수자 또는 변호인이 그 집행에 참여'할 수 있도록 규정하고 있고, 예외적으로 피압수자 등이 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 참여통지를 생략할 수 있도록 규정[66]하고 있다.

현장에서 관련성 있는 정보를 선별하여 해당 전자정보만 압수가 가능한 경우에는 영장 제시, 관련 정보의 무결성 입증 확인 등이 현장에서 바로 이루어지므로 참여권 행사의 문제가 발생할 소지가 낮다.

참여권 행사가 주로 문제가 되는 영역은 저장매체 자체를 반출하거나 하드카피나 이미징 등의 형태로 반출하여 수사기관 사무실 등에서 정보 탐색, 출력 등이 이루어지는 경우이다.

2. 압수수색 집행 종료 시기에 대한 논의

가. 선별 과정 또한 압수수색 집행의 연장선이라 보는 견해

압수수색의 대상은 전자정보 자체이므로 저장매체를 가져가거나 복제본을 만들어가는 단계는 아직 압수가 행해진 것이 아니며 그 저장매체나 복제본을 검색하여 범죄와 관련된 전자정보의 선별이 완전히 종료되었을 때 압수수색도 종료된 것으로 보는 견해이다.

이 견해에 따르면 수사기관이 분석실에서 전자정보의 선별을 모두 끝냈을 때 압수수색의 집행이 종료되고, 그때까지 피압수자 등의 참여권이 보

---

66) 형사소송법 제121조(영장집행과 당사자의 참여) 검사, 피고인 또는 변호인은 압수・수색영장의 집행에 참여할 수 있다.
제122조(영장집행과 참여권자에의 통지) 압수・수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.
제219조(준용규정) 제106조, 제107조, 제109조 내지 제112조, 제114조, 제115조제1항 본문, 제2항, 제118조부터 제132조까지, 제134조, 제135조, 제140조, 제141조, 제333조제2항, 제486조의 규정은 검사 또는 사법경찰관의 본장의 규정에 의한 압수, 수색 또는 검증에 준용한다. 단, 사법경찰관이 제130조, 제132조 및 제134조에 따른 처분을 함에는 검사의 지휘를 받아야 한다.

장되어야 한다고 본다.

나. 선별과정은 수사기관 내부의 분석과정이라 보는 견해

압수수색의 대상은 전자정보가 아닌 저장매체 등의 유체물이므로 수사관이 현장에서 저장매체 등을 발견하고, 저장매체 자체를 압수하거나 복제본을 만들어 압수하였을 때 압수수색이 종료된다고 보는 견해이다.

또한 수사기관의 분석실에서 행해지는 선별 작업은 압수물의 내용을 알기 위한 수사기관의 내부적인 확인행위[67]이므로 참여권이 반드시 보장될 필요는 없고, 증거분석을 위한 임의수사의 일종이자 무결성 확보하기 위한 기술적인 원형 보존조치[68]이므로 수사기관의 재량에 따라 이루어진다고 보는 견해도 있다.

다. 판례의 태도

판례는 저장매체 자체를 압수하거나 복제할 때부터 관련성 있는 정보를 선별하는 일련의 과정을 모두 압수수색 집행 과정으로 보고 피압수자 등의 참여권 보장이 필요하다는 견해이다.

구체적인 판례의 태도를 살펴보면, "형사소송법 제219조, 제121조는 '수사기관이 압수·수색영장을 집행할 때에는 피압수자 또는 변호인은 그 집행에 참여할 수 있다'는 취지로 규정하고 있다. 저장매체에 대한 압수·수색 과정에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 또는 하드카피나 이미징 등 형태(이하 '복제본'이라고 한다)를 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 경우에도, 그와 같은 일련의 과정에서 피압수자나 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다. 만약 그러한

---

67) 이완규, "디지털 증거의 압수수색 개념 및 증거능력 요건", 사법발전재단, 차한성 대법관 퇴임기념 논문집「형사재판의 제문제 제7권」, 박영사, 2014, 331~332면

68) 전승수, "디지털 정보에 대한 압수수색영장의 집행", 법조 통권 670호, 2012, 254면, 265면

조치를 취하지 않았다면 피압수자 측이 참여하지 아니한다는 의사를 명시적으로 표시하였거나 절차 위반행위가 이루어진 과정의 성질과 내용 등에 비추어 피압수자 측에 절차 참여를 보장한 취지가 실질적으로 침해되었다고 볼 수 없을 정도에 해당한다는 등의 특별한 사정이 없는 이상 압수·수색이 적법하다고 평가할 수 없고, 비록 수사기관이 저장매체 또는 복제본에서 혐의사실과 관련된 전자정보만을 복제·출력하였다고 하더라도 달리 볼 것은 아니다."[69]라고 판시하였다.

또한 "형사소송법 제219조, 제121조에 의하면, 수사기관이 압수·수색영장을 집행할 때 피의자 또는 변호인은 그 집행에 참여할 수 있다. 압수의 목적물이 컴퓨터용디스크 그 밖에 이와 비슷한 정보저장매체인 경우에는 영장 발부의 사유로 된 범죄 혐의사실과 관련 있는 정보의 범위를 정하여 출력하거나 복제하여 이를 제출받아야 하고, 피의자나 변호인에게 참여의 기회를 보장하여야 한다. 만약 그러한 조치를 취하지 않았다면 이는 형사소송법에 정한 영장주의 원칙과 적법절차를 준수하지 않은 것이다. 수사기관이 정보저장매체에 기억된 정보 중에서 키워드 또는 확장자 검색 등을 통해 범죄 혐의사실과 관련 있는 정보를 선별한 다음 정보저장매체와 동일하게 비트열 방식으로 복제하여 생성한 파일(이하 '이미지 파일'이라 한다)을 제출받아 압수하였다면 이로써 압수의 목적물에 대한 압수·수색 절차는 종료된 것이므로, 수사기관이 수사기관 사무실에서 위와 같이 압수된 이미지 파일을 탐색·복제·출력하는 과정에서도 피의자 등에게 참여의 기회를 보장하여야 하는 것은 아니다."[70]라고 판시하고 있다.

다만 통합진보당 내란음모에 관한 사건[71]에서는 "통상적으로 손상된 전자정보 저장매체의 복구나 암호의 해독, 삭제된 파일의 복원 과정 등은 그 성공 가능성을 미리 예측할 수 없고, 그 방법이나 소요시간 등도 가늠하기 어려워 이러한 조치가 수반되는 정보 분석 과정의 경우 피고인 등의

69) 대법원 2017. 9. 21. 선고 2015도12400 판결
70) 대법원 2018. 2. 8. 선고 2017도13263 판결
71) 대법원 2015. 1. 22. 선고 2014도10978 판결 / 서울고등법원 2014. 8. 11. 선고 2014노 762 판결 / 수원지방법원 2014. 2. 17. 선고 2013고합620, 624(병합), 699(병합), 851(병합) 판결

참여권을 완전히 보장하기란 현실적으로 어려움이 있고, 피고인들은 일부 현장 압수 수색 과정에 직접 참여하기도 한 점, 압수된 저장매체 중 증거로 제출된 것이 객관성이 인정되는 제3자의 서명에 의한 봉인조치에 의해 보존되어 있고, 해쉬값도 보존되어 있으며, 복호화 등 과정에 대한 참여통지 누락이 증거수집에 영향을 미쳤다고 보이지 않아 유죄 인정의 증거로 사용할 수 있는 예외적인 경우로 볼 수 있다."고 판시하였다.

그러나 이와 반대로 "이미지 파일을 파일변환, 복호화하는 작업에 피압수자 등을 참여시키지 않은 점과 관련하여, 원본 서버의 압수, 이미징 복제, 관련정보 출력 등 나머지 압수·수색 과정에는 참여의 기회가 보장되었고, 파일 탐색을 위한 준비과정에 불과하여 참여권이 가지는 의미가 상대적으로 크지 않으며, 파일변환 등 작업 시 참여 기회를 부여하지 않은 것이 참여를 배제하려는 의도로 보기 어려운 점 등을 종합하여 위법의 정보가 전체 압수·수색 과정 전체를 위법하게 할 정도로 중요하다고 보기 어려워 압수·수색 처분 취소를 청구하는 준항고인의 주장을 기각"한 사례[72]도 있다.

압수목록 교부와 관련해서도 우리 법원은 "형사소송법 제219조, 제129조에 의하면, 압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다. 그리고 법원은 압수·수색영장의 집행에 관하여 범죄 혐의사실과 관련 있는 정보의 탐색·복제·출력이 완료된 때에는 지체 없이 압수된 정보의 상세목록을 피의자 등에게 교부할 것을 정할 수 있다. 압수물 목록은 피압수자 등이 압수처분에 대한 준항고를 하는 등 권리행사절차를 밟는 가장 기초적인 자료가 되므로, 수사기관은 이러한 권리행사에 지장이 없도록 압수 직후 현장에서 압수물 목록을 바로 작성하여 교부해야 하는 것이 원칙이다. 이러한 압수물 목록 교부 취지에 비추어 볼 때, 압수된 정보의 상세목록에는 정보의 파일 명세가 특정되어 있어야 하고, 수사기관은 이를 출력한 서면을 교부하거나 전자파일 형태로 복사해 주거나 이메일을 전송하는 등의 방식으로도 할 수 있다.[73]"고 판시하여 압수된 정보의 상세목록 교부를 원칙적으로 요구하고

72) 대법원 2015. 10. 15. 선고 2013모1969 결정

있다.

3. 해외 입법례

독일, 미국 등의 경우에는 참여권이라는 제도가 존재하지 아니하고, 일본의 경우에도 형사소송법에서 법원의 압수·수색 과정에 피고인의 참여권을 인정하고 있으나, 수사기관의 압수·수색 과정에서 피압수자의 참여권을 인정하고 있지는 않다.

즉 디지털 증거를 현장에서 압수한 뒤 검색하고, 분석하여 최종적으로 분류하는 행위에 대해서 해외 입법례는 관련성의 정도, 비례성의 정도를 고려하여 일부 제한을 하고 있을 뿐이지, 우리나라와 같이 압수수색 집행 과정의 일환으로 보아 참여권을 인정하는 경우는 찾아볼 수 없다.

4. 참여권 보장과 관련된 문제점

대법원은 수사기관 사무실 등에서의 정보 탐색, 출력도 영장집행 과정의 일환이므로 피압수자 등의 참여권 보장이 필요하다고 판시하고 있으나, 수사실무상 이와 같은 참여권 보장에는 여러 가지 문제점이 존재한다.

우선 디지털 증거의 경우 일반 유체물 등에서 적용되었던 압수수색과 다른 법리가 적용되어야 할 이론적 및 법률적 근거가 존재하지 아니한다. 또한 실무상으로도 이와 같이 참여권을 보장함으로 인해 대법원이 기대하는 사생활 보호, 과잉압수의 제한 등의 목적을 달성하는데 실효성이 있는지 의문이며, 현실적으로도 그 시기 및 절차 등에 대해 다양한 문제점을 내포하고 있다.

대법원에서 기대하는 바는 피압수자의 참여권 보장으로 인해 무관정보의 압수, 열람 등을 방지하고자 함이나, 압수·수색영장의 집행은 강제수사로 피압수자가 이를 거부할 수 없는 것[74]이며, 압수처분이 위법하다고 판단하는 피압수자는 사후적으로 준항고 등으로 다투거나, 법정에서 위 증

73) 대법원 2017. 9. 21. 선고 2015도12400 판결
74) 백형구 등, 주석 형사소송법(I), 한국사법행정학회, 2009, 530면

거가 위법하게 수집되었으므로 유죄의 증거로 사용될 수 없다는 방법 등으로 다툴 수 밖에 없는 것이다.

또한 선별절차를 거친 후 무관한 정보를 폐기해야 한다는 판례의 태도 또한 무결성 확보의 측면에서는 많은 문제점을 내포하고 있다. 무관하다고 인정되는 증거를 폐기하게 되면 최초에 확보한 해쉬값의 변동이 생기기 때문이다. 오히려 수사기관이 관련성 있는 정보의 선별 후 이에 대한 목록을 사후적으로 교부하는 것이 보다 간명하고 무결성 확보 측면에서 바람직할 것으로 생각된다.

암호화된 파일의 복호화, 삭제된 파일 등의 복구, 관련성 있는 정보의 검색 등에는 장기간이 소요[75]되고, 분석 시간 또한 예측이 불가능하므로 피압수자 등의 입장에서 본인이 직접 참관을 하여도 전문가가 아닌 경우에는 무의미한 참여가 될 가능성이 높고, 변호인을 선임하여 참여하게 한다 하여도 이는 비용, 시간적인 측면에서 큰 부담으로 작용하고 있다.

수사기관의 입장에서도 피압수자 등을 수사기관 사무실에 장기간 대기하게 하면서 복호화, 검색, 분석의 전 과정을 참여시키는데 현실적인 어려움이 존재한다. 위와 같은 분석과정을 피압수자 등이 지켜보는 과정에서 수사기법, 기밀 등이 노출될 수 있으며, 다른 사건에 대한 수사 보안의 문제 등 시·공간적인 제약이 존재할 수 밖에 없다.

그러므로 디지털 증거의 저장매체 자체를 압수하거나 이미징 복제 방식으로 압수한 뒤 수사기관의 사무실에서 선별적으로 탐색하는 경우 그 과정 전부에 참여권을 보장하기에 현실적으로 많은 어려움이 존재하고 비효율적이므로 그 과정을 정확하게 기록 후 구체적인 파일목록을 압수목록으로 사후에 교부하면 충분할 것으로 생각된다.

---

75) 디지털 증거의 대량화, 디지털기기 사용의 전문화, 증거 은폐 시도의 고도화에 비해 디지털 포렌식 수사관의 수는 터무니없이 부족하여, 삭제된 데이터를 복원하고 분석하여 관련성 있는 데이터를 선별하는데 소요되는 작업의 양과 시간은 기하급수적으로 증가하였음, 종근당 사건에서는 이미징 사본을 이용하여 관련성 있는 정보를 검색하는데 11일이 소요되었음

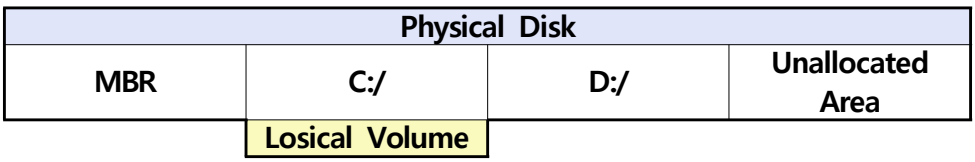
제 5 장 저장매체 전체 물리 이미지 확보 필요성

제 1 절 물리 이미징과 논리 이미징

디스크를 이미징하는 방식에는 물리 이미징과 논리 이미징이 있다. 물리 이미징이랑 원본 정보의 저장매체를 bit-by-bit로 복사하여 완벽히 동일한 사본을 만드는 것으로 파일 디렉토리 구조를 포함하여 하드디스크에서 사용하지 않는 공간인 볼륨 슬랙(Volume Slack), 비할당영역, 숨겨진 공간(HPA, Host Protected Area 등) 등 탐색기로 확인할 수 없는 부분까지 복제가 가능하다.

대표적인 이미지 파일 포맷으로는 dd(disk dump)와 EWX(Expert Witness Compression Format)이 있다. 포렌식 이미지 포맷을 사용하면 원본 비트스트림 데이터를 압축할 수 있기 때문에 사본 저장매체의 용량을 줄일 수 있고, 암호화를 통해 데이터를 보호하는 것도 가능하다.

이에 반해 논리 이미징은 사건 관련 파일과 폴더 또는 비할당영역에서 복구한 일정 데이터를 선별하여 이미징하는 것으로 관련 메타 데이터를 포함한 정보를 선별하여 복제하는 방법이다. 원본 파일 또는 디렉토리를 다른 저장매체에 단순히 복사하는 파일 복사[76]와는 구별되나 하드디스크에서 사용하지 않는 공간은 복제하지 않으므로 정밀한 분석은 불가능하다.



[그림2] 논리 이미지와 물리 이미지

76) 보통 Windows의 탐색기에서 마우스로 드래그 앤 드롭(Drag-and-drop)을 하거나 copy 명령어를 사용하는 방법으로 이루어지나, 삭제된 데이터를 복구할 수 없고, 복사 과정에서 원본파일의 시간정보가 변경될 수 있어 디지털 포렌식에서는 거의 사용되지 않는 방법이다.

제 2 절 안티포렌식 행위

1. 개요

안티포렌식이란 디지털 포렌식 기술에 대응하여 증거 획득 및 추적, 수사관의 분석 등을 방해하고 어렵게 하는 행위를 의미한다. 중요 데이터를 완전하게 삭제하거나 훼손하는 데이터 파괴, 데이터를 암호화하거나 특정 파일에 중요 정보를 숨기는 데이터 은닉, 테이터를 조작하여 분석을 방해하는 데이터 수정, 안티포렌식 도구나 기법의 흔적을 제거하는 방법 등으로 분류할 수 있다.

데이터 은닉 기술이 점차 발달함에 따라 다양한 방법의 파일 은닉이 이루어지고 있다. '파일속성'에 '숨김' 속성을 주어 Windows의 탐색기에서 보이지 않도록 하는 방법부터 디스크의 미사용 영역에 은닉하거나, 파일 확장자를 변경하는 방식, 파일 속에 다른 데이터를 은닉하는 방법 등 다양한 방법들이 있다.

2. 데이터 삭제

데이터를 삭제하는 방법으로는 저장매체를 물리적으로 파괴하는 방법과 하드디스크의 기존 데이터를 제거하고 모든 섹터의 내용을 0으로 만드는 디스크 와이프(Disk Wipe), 하드디스크나 테이프에 강력한 자기장을 노출시켜 기록된 데이터를 파괴하고 복구가 불가능하도록 하는 디가우저(Derausser) 방식 등이 있다.

최근에는 운영시스템에서 자동으로 생성되는 정보 중 시스템 관리에 불필요한 정보들인 사용하지 않은 임시 파일, 캐쉬 파일, 다운로드 파일 또는 불필요한 시스템 아티팩트, 어플리케이션 아티팩트 등을 자동으로 삭제하여 데이터 정리를 하고 시스템을 최적화하는 Window Washer, Evidence Eliminator 등의 제품도 등장하였다.

디스크 덮어쓰기(Data Wiping)란 파일을 삭제하였지만 삭제된 파일의 데이터 중 물리적으로 디스크에 남아있는 부분에 대해 덮어쓰고 삭제하는 과정을 반복하는 것으로 한 번의 덮어쓰기로는 이전 데이터의 부분 조각 등 작은 흔적들을 완전히 제거하기 어렵기 때문에 물리적 복구의 가능성이 잔존하게 된다.

3. 데이터 은닉

데이터 은닉은 물리적 수준, 파일 시스템 수준, 응용프로그램 수준으로 나눌 수 있다.

물리적 수준의 데이터 은닉은 운영체제가 인식 불가능한 영역에 데이터를 은닉하는 방법이다. 파티션 정의 영역, 비할당 영역[77], 복구 파티션 등에 데이터를 숨기면 운영체제가 인식하기 어렵게 된다.

다음으로 파일 시스템 수준의 데이터 은닉은 볼륨[78] 부팅 영역의 사용하지 않는 공간, 볼륨 슬랙, 파일 슬랙, 램 슬랙 등의 공간에 데이터를 은닉하는 방법이다.

파일은 클러스트 단위로 할당되므로 1개 클러스터가 4개의 섹터로 구성되었다고 하였을 때, 데이터가 섹터1의 일부에만 저장되고, 섹터1의 일부 영역 및 섹터2, 섹터3, 섹터4는 사용되지 않는 경우 램 슬랙 공간과 파일 슬랙 공간이 발생하고, 이와 같은 공간에 파일을 은닉하는 방식이다. 파일 슬랙에는 이전 데이터의 잔재가 남아 있고, 램 슬랙은 '0'으로 채워지게 된다. 이와 같은 슬랙 공간에 데이터를 은닉하는 경우 파일 자체를 지우지 않는 이상 은닉한 데이터가 삭제되는 경우는 없다.

---

77) 파일 시스템은 각 파일이 어디에 저장되어 있는지 기록을 하는데, 해당 파일에게 저장 장치의 일정 영역을 할당하는 것으로, 할당된 영역은 다른 파일들이 사용할 수 없고, 할당이 되지 않는 공간을 비할당 영역이라 함

78) 볼륨이란 운영체제나 응용프로그램이 데이터를 저장하여 사용하도록 주소가 지정된 섹터들의 집합으로 디스크 전체의 하위로서 C드라이브, D 드라이브와 같은 논리적 단위로 생각 할 수 있으며, ① 볼륨 부팅 영역, ② 메타 데이터 영역, ③ 데이터(파일 할당, 비할당), ④ 볼륨 슬랙 부분으로 구성됨

응용 프로그램 수준의 데이터 은닉 방법으로는 응용 프로그램 파일 내에 스테가노그래피(Steganography) 방법으로 은닉하거나, jpg파일 내 파일이 끝나는 푸터 부분에 은닉하거나 파일 헤더의 사용되지 않는 부분에 은닉하는 방법이 있다.

스테가노그래피 기법은 전달하려는 중요한 정보를 이미지, 오디오 등의 파일에 삽입하여 해당 정보의 존재를 은닉하는 방법이다. 사진, 오디오, 비디오 파일과 같은 다양한 디지털 파일의 경우 몇 개의 정보가 빠져도 육안으로 확인이 불가능한 경우가 많으므로, 이와 같이 빠진 공간에 은닉하고자 하는 데이터를 삽입하는 방식이다. 암호화의 경우 암호화된 사실만으로 수사기관의 관심을 끌 수 있기 때문에 암호화했다는 사실을 노출시키지 않기 위한 방법으로 사용되고 있다.

최근에는 복합문서파일의 구조적 특성과 문서작성 응용프로그램의 기능을 이용하여 데이터를 은닉하는 사례가 늘고 있다.

복합문서파일의 구조적 특성을 이용한 방법으로는 미할당·슬랙·예약 영역에 데이터를 은닉하거나 복합문서 파일의 형식을 조작하는 방법, 스테가노그래피 기법을 이용하여 데이터를 은닉한 멀티미디어 파일을 다시 문서에 삽입하는 방법 등이 있다.

jpg 파일 내에 데이터를 은닉하는 방법은 jpg뷰어가 jpg 파일의 마지막인 푸터 시그니쳐 이후 데이터를 무시하는 특성을 이용한 것으로 푸터 시그니처 이후 남는 공간에 데이터를 은닉하는 방식이다.

다음으로 파일 확장자를 변경하는 방식이 있다. 예를 들어 hwp 일의 확장자를 jpg 등으로 변경하여 파일을 은닉해두면, 변경된 jpg 파일을 실행할 경우에 사진 뷰어 프로그램이 실행되고, 한글 워드프로세서가 실행되지 않으므로 오류메시지가 나오면서 파일 내용의 확인이 불가능하게 된다. 또한 hwp, xls, pdf 등으로 끝나는 문서파일을 bin, sys 등 시스템 파일의 확장자로 변경시켜 관련 폴더에 저장하면 문서 파일을 찾기가 어렵다.

이와 같은 경우에는 파일 헤더 분석에 따른 확장자 유형을 파악해서 확장자 변경 여부를 확인해야 한다.

응용프로그램의 기능을 이용한 데이터 은닉 방법으로는 문서 속성정보에 데이터를 은닉하거나, 매우 작은 크기로 글자를 작성하거나, 글자색을 배경색과 같은 색으로 작성 또는 이미지 위에 텍스트를 숨기거나 문서에서 보이는 URL을 클릭해도 다른 링크로 연결되도록 하이퍼링크를 설정하는 방법 등이 있다.

이와 같이 비정상적인 방법으로 문서파일에 은닉된 데이터는 전문가가 아니면 쉽게 확인하기 어렵고, 웹 방화벽에서도 탐지가 어려워 국내외 범죄 조직에서 이와 같은 비밀 메시지 은닉 방법으로 사이버 교신을 하는 사례도 발견되었다.

파일 내 은닉된 데이터를 확인하기 위해서는 파일 구조상 발생할 수 밖에 없는 사용하지 않는 공간을 분류하고 임의로 추가되거나 수정된 스트림, 스토리지를 확인, 분석하여야 한다.[79]

가장 분석하기 어려운 방법은 암호 기술의 사용인데, 이는 파일 또는 폴더, 볼륨 또는 전체 디스크의 암호화로 구별된다.

사용자들이 많이 사용하는 마이크로소프트 사의 엑셀, 파워포인트, 워드, 한글과컴퓨터사의 한글, 이스트소프트사의 알집 등의 응용프로그램은 기본적으로 암호화 기능을 보유하고 있다.

또한 윈도우 운영시스템에서는 2000년도부터 자체적으로 암호화 파일시스템(Encypting File System, EFS)을 운영하고 있는데, 윈도우 파일 탐색기를 통해서 파일 폴더의 속성 안에서 암호화를 적용할 수 있고, 특정 폴더나 파일의 암호화가 가능하다. NTFS 드라이버에서 암호화와 복호화 진행이 가능한데, 암호화 키의 일부는 사용자가 접근 가능한 파일 내에

---

79) 김은광, 전상준, 한재혁, 이민욱, 이상진, “복합문서 파일에 은닉된 데이터 탐지 기법에 관한 연구”, 2015, 참조 ; “복합문서 파일의 미사용 영역을 검사하고 패딩 데이터가 아닌 다른 데이터가 존재한다면 데이터 추출 후 분석을 수행한다. 미사용 영역에 패딩 데이터 존재 시 복합문서 파일 내 존재하는 모든 스트림의 이름을 확인한 후 MS Office에서 지원하지 않는 스트림 이름이 존재할 경우 해당 스트림 내에 존재하는 데이터를 추출 후 분석을 수행한다. 마지막으로 스트림 내 미사용 영역을 확인하여 0x00이 아닌 다른 값이 존재한다면 추출 후 분석을 수행한다.”

저장되고, 다른 일부는 계정 비밀번호와 연계되어 계산된다.

볼륨 또는 전체 디스크 암호화는 하드디스크에서 자체적으로 기능을 제공하는 경우가 일반적이다. 이와 같은 운영체제 기반의 디스크 암호화로 PC의 경우 Windows BitLocker, OSX FileVault, 스마트폰의 경우 iOS 5.0. 이상, Android 7.0이상의 경우 볼륨 암호화가 기본적으로 이루어지고 있다. 그 밖의 볼륨 암호 프로그램으로 TrueCrypt, BitLocker, VetaCrypt 같은 프로그램들이 존재한다.

디스크 암호화의 경우 기기가 분실되어도 암호화되어 있기 때문에 안전하고, 해킹, 바이러스 및 악성 코드에 안전하다는 점과 사용자의 입장에서는 별도의 조치 없이 자동으로 암호화되기 때문에 편리하다는 장점이 있다. 그러나 많은 영역에 대해 암호화 과정을 거쳐야 하기 때문에 암호화 및 복호화에 상당한 시간이 소요된다. 복구키를 계정에 저장할 수도 있고 파일 또는 인쇄물로 관리할 수도 있는데 키를 손상하거나 분실할 경우 사용자도 데이터에 접근할 수 없다는 단점이 있다.

암호화된 정보를 복호화하기 위해서는 패스워드가 필요한데, 패스워드를 찾는 방법으로는 주로 키를 전수조사 하거나 패스워드 크랙, 암호키가 저장된 장소를 찾는 방법이 활용된다.

전수조사하는 방법은 많은 비용과 시간이 들기 때문에 주로 패스워드 크랙으로 패스워드를 추론하게 된다. 패스워드 크랙이란 다른 기기나 인터넷 계정 등에서 사용되는 패스워드의 패턴을 조사하고, 효과적인 추론 기법을 개발하여 추론 대상의 공간을 좁히고, 병렬·분산 처리 기술을 사용하여 패스워드를 찾아내는 방법이다.

다음으로 암호키가 저장된 장소를 찾는 방법이 있다. 암호키는 사용자가 패스워드를 암기하고 있는 경우, 컴퓨터 내부의 휘발성 메모리[80], 하드디스크, 메인보드의 암호칩[81] 등에 저장되어 있는 경우, 종이나 USB, 스

80) 암호화 및 복호화되는 경우 암호키가 메인 메모리에 일시적으로 저장되므로 라이브 포렌식으로 획득이 가능

81) 칩에 대한 역공학 기법으로 찾을 수 있으나 현실적으로 많은 비용과 시간이 소요되고 아이폰의 암호화, 윈도우 BitLocker가 그 대표적인 예임

마트카드, 키복구 서버 등 컴퓨터 외부에 저장되어 있는 경우로 나눌 수 있다.

이와 같은 안티포렌식 흔적을 조사하기 위해서는 우선 윈도우 레지스트리, 아티팩트 등을 조사하여 데이터 변조 도구 프로그램을 설치한 흔적이 있는지 확인해야 한다. 데이터 변조 프로그램이 설치된 사실이 확인되면 설치 시간을 중심으로 타임 라인을 구성하여 데이터를 분석할 필요가 있다.

또한 운영시스템에서 확인이 어려운 비할당 영역과 같은 곳에 은닉된 데이터 및 패스워드 등을 확인해야 은닉, 삭제된 데이터를 확인하거나 복구할 수 있게 된다.

안티포렌식 행위가 현장에서 바로 확인이 되는 경우에는 저장매체 자체 또는 전체 이미지의 압수수색이 가능할 것이나, 현장에서 제한된 시간 안에 안티포렌식 행위가 있었는지 여부를 확인하는 것은 매우 어려울 수 밖에 없다.

또한 비할당 영역을 비롯하여 컴퓨터가 자동으로 생성한 아티팩트, 메타 데이터 등을 모두 확보해야, 즉 저장매체 전체의 물리이미지를 확보해야 원래의 데이터 복구를 시도할 수 있으므로 현재의 선별 압수수색방법만으로는 안티포렌식 기법으로 훼손, 은닉된 데이터를 충분히 확보하기에 많은 어려움이 있다.

제 3 절 삭제된 디지털 증거 복구

디지털 파일은 클러스터 단위로 저장되는데 연속된 클러스터에 존재하거나 여러 곳에 분산되어 존재할 수 있으며, 각 클러스터에는 다음 클러스터를 가리키는 포인터(pointer)가 있어 이를 이용하여 연결된 클러스터를 조합하면 하나의 완성된 파일을 확인할 수 있다.

디지털 파일을 삭제하는 경우에는 이와 같은 클러스터에 존재한 파일들이 지워지는 것이 아니라, 파일의 정보를 담고 있던 메타 데이터의 할당 정보만 변경되어 비할당 영역으로 이동할 뿐이므로 나머지 파일의 정보

및 데이터 영역은 그대로 남아 있게 된다.

이와 같이 비할당 영역으로 이동한 파일은 덮어쓰기가 되거나 완전삭제(Wipe) 되기 전[82]까지는 비할당 영역에서 확인이 가능하나 이를 검색하는데 많은 시간이 걸리므로 현장에서의 키워드 검색만으로는 확인이 불가능하다.

FAT32 파일 시스템에서 파일을 복구하는 경우[83] 메타 데이터가 남아 있으면 메타 데이터를 이용하여 복구를 할 수 있다. 파일 삭제 시 FAT 테이블의 엔트리 할당 정보만 삭제되는데 이 디렉토리 엔트리의 첫 바이트만 헥사값 0xE5로 변경되므로 메타 데이터에서 파일 이름, 파일 생성시간, 파일 접근 시간, 파일 수정 시간, 파일 크기, 첫 번째 클러스터 할당 정보를 얻을 수 있다.

파일이 단편화 되지 않았다면 파일의 크기 정보와 첫 번째 클러스터 정보로부터 마지막 클러스터를 계산할 수 있을 것이다. 만약 메타 데이터가 삭제되었다면 삭제된 파일의 디렉토리 엔트리는 재할당 될 수 있으므로 파일의 시그니처, 헤더, 푸터 정보를 검색하여 영역을 결정하고 문자열 검색을 통해 해당 파일의 위치를 탐지한 뒤 푸터 정보와 램 슬랙 정보를 이용하여 마지막 클러스터의 위치를 파악하여 복구하게 된다.

NTFS 파일 시스템[84]에서는 파일 내용이 거주$DATA 속성에 있고 해당 파일의 MFT 엔트리가 재할당되지 않으면 복구가 가능하다. 만약 파일 내용이 비거주$DATA 속성에 있고 MFT 엔트리가 재할당되지 않았을 경우에는 파일에 할당된 클러스터 정보를 복구할 수 있으므로 해당 파일의 복구가 가능하고, MFT 엔트리가 재할당 되었을 경우에는 복구가 불가능하다.

이처럼 삭제된 파일을 복구[85]하기 위해서는 비할당 영역까지 포함한 저

---

82) 그밖에도 클러스터를 연결하는 포인터가 끊어진 경우, 디스크 모음 조각을 한 경우 등에도 복구가 불가능함
83) 박상준, 앞의 책, 390면 참조
84) 박상준, 앞의 책, 443면 참조
85) 삭제된 파일의 복구가 어려워도 파일이 존재했다는 사실 자체가 사건에서 중요한 단서가 되는 경우가 다수 존재함, 이미지를 삭제해도 Thumbs.db라는 숨김

장매체 전체의 물리 이미지가 필요하다.

제 4 절 현장 키워드 검색의 한계

검찰에서 주로 사용하는 포렌식 도구인 EnCase 프로그램의 경우 키워드 검색 기능을 제공하고 있다. 키워드 검색의 종류로는 Index Search와 Raw Keyword Search가 있는데 현장에서는 주로 Raw Keyword Search만이 가능하다.

Index Search의 경우 저장 장치에 대한 미리보기 단계에서는 활성화가 되지 않고, 저장 장치 전체를 증거 이미지 파일로 획득하여 인덱스를 생성한 이후에만 검색이 가능하기 때문이다. 인덱스를 생성하기 위해서는 파일 전체를 탐색해야 하므로 많은 시간이 소요되기 때문에 대용량 저장 장치에 대한 인덱스를 압수수색 현장에서 생성하기란 불가능한 것이 현실이다.

이에 반해 Raw Keyword Search의 경우 문서 내의 transcript가 아닌 파일시스템 Raw data에 대한 검색이므로 저장매체에 대한 이미징 없이도 바로 수행이 가능하고, 미리보기 단계에서도 검색이 가능하다. 또한 옵션의 'Search entry slack' 기능을 통해 파일 슬랙 부분의 검색이 가능하여 파일시스템에서 삭제된 파일명 또는 폴더명을 검색할 수 있으며, 'Undelete entries before searching' 기능을 통해 삭제 파일의 단편화된 키워드 검색 또한 가능하다.

그러나 Raw Keyword Search의 경우 복합문서와 압축파일의 검색이 불가능하다는 치명적인 단점이 존재한다. MS Office의 경우 2003년 이전 문서는 파일 확장자가 doc, ppt, xls로 Raw Keyword Search로 검색이 가능하나, 2007년 이후 문서의 경우 여러 파일들이 모인 복합문서로 파일 확장자가 docx, pptx, xlsx로 되어 있어 Index Search 방식을 통해서만

속성 파일을 통해 데이터베이스 파일을 확인할 수 있는데, 윈도우 자체에는 Thumbs.db파일을 열어볼 수 있는 프로그램이 없고, Thumbs.Viewer와 Thumbs.db.Explorer을 통해 확인이 가능함

검색이 가능하다.

또한 한글 파일의 경우에도 2013년 이전 버전의 경우 Raw Keyword Search로 검색이 가능하나, 그 이후 버전의 경우 복합문서로 구성되어 있어 Index Search로만 검색이 가능하며, 요약정보에 해당키워드가 있는 경우에 한해 Raw Keyword Search로 검색이 가능하다.

pdf 파일의 경우에도 Raw Keyword Search로 검색하면 파일 내용에 포함된 키워드들을 검색하지 못하는 문제가 있고, 압축 파일인 zip, rar 파일의 경우도 압축 파일 안에 포함되어 있는 파일들을 Raw Keyword Search 검색으로는 찾을 수가 없다.

이메일 본문에 첨부된 첨부파일의 경우 수사실무상 수사의 중요한 단서가 되거나 핵심키가 될 수 있는 경우가 많아 확인의 필요성이 높음에도 Raw Keyword Search 만으로는 첨부파일의 검색이 불가능[86]하다.

또한 기업용 DRM[87](Digital Right Management)을 도입하여 문서가 자동으로 암호화 되는 경우나 별도로 문서에 비밀번호를 설정한 경우 등에도 Raw Keyword Search만으로 파일 내용이 검색되지 않는다.

이와 같은 한계 중 일부는 EnCase와 함께 포렌식 도구로 많이 사용되는 CFT(Computer Forensic Tool)에서도 동일하게 나타난다. CFT에는 검색기능으로 Meta Index Search 방식과 Keyword Search 방식이 있는데, Index Search의 경우 Index를 만드는데 상당한 시간이 소요되어 현장에서는 Keyword Search 방식이 주로 이용된다.

CFT는 복합문서 파일과 PDF 파일에 대해서는 스크립트에서 텍스트를 추출하여 검색하므로 Encase 프로그램으로 추출할 수 없는 디지털 정보도 일부 검색이 가능하다. 그러나 압축 파일의 경우에는 압축파일 안에 들어 있는 정보들을 검색하지 못한다는 한계가 여전히 존재한다.

또한 검색어의 한계로 인해 관련성 있는 증거를 모두 탐색하는 것이 쉽

86) 김희균, “이메일 계정 속 첨부파일의 증거능력”, 한국형사소송법학회 형사소송 이론과 실무 제7권 제2호, 2015 참조
87) 디지털 콘텐츠의 지적재산권 보호와 디지털 콘텐츠의 관리 및 유통 효율화를 위해 사용되는 기술과 서비스를 의미함

지 않고, 폴더별, 파일별로 파일 내용을 확인해 가면서 키워드를 추가로 변경하는 경우 2배 이상의 시간이 소요되며, 대용량 저장매체의 경우 검색에 장시간이 소요되어 현장에서 이와 같은 키워드의 변경 또는 추가는 실질적으로 불가능하다.

제 5 절 수사과정 및 재판과정에서의 추가 증거 확보 필요성

압수수색영장을 발부받아 압수수색을 진행하는 단계는 수사의 초기 단계이고 압수수색을 통해 확보한 증거를 바탕으로 수사가 진행됨에 따라 혐의 사실이 변경될 가능성이 매우 높다. 수사는 결론을 정해 놓고 이를 입증하는 과정이 아니라, 혐의 사실을 바탕으로 관련 증거를 수집하여 실체적 진실을 밝혀나가는 과정이기 때문이다.

수사 단계에서는 혐의사실을 모두 인정하여 기본적인 증거만을 바탕으로 기소를 하였는데, 재판 단계에서 혐의를 모두 부인하여 뒤늦게 증거를 수집하는 것이 불가능해지는 상황이 실무에서는 종종 발생한다. 대부분의 중요한 증거들은 디지털 증거이고, 디지털 증거의 경우 그 특성상 사건관계인들이 의도하지 않더라도 사용 또는 접근만으로 아티팩트, 메타 데이터 등이 쉽게 변경되고, 보관기간을 놓치게 되면 더 이상 확보가 어려운 경우가 많다.

또한 선별 압수를 엄격히 적용하여 처음 수사가 시작된 단계에서는 관련성이 인정되지 아니하여 피의자 등에게 돌려준 디지털 증거의 경우 피의자 등이 사후에 이를 은닉하거나 삭제하게 되면 새로운 압수수색영장을 발부 받는다 하더라도 더 이상 이와 같은 증거를 확보하기는 곤란할 수 밖에 없다.

어쩌면 피의자와 변호인의 일종의 전략으로 볼 수도 있으나, 수사기관은 이에 속수무책일 수밖에 없다. 피의자가 수사단계에서 모든 혐의를 인정하고 자백하여도 부인할 경우를 대비하여 모든 증거를 완벽하게 수집해

놓을 수도 있겠지만 인력과 시간상의 한계로 현실적으로 불가능한 것이 사실이다.

수사기관에서는 성실하게 협조하였던 목격자나 참고인들도 법정에서는 피고인과 변호인의 회유, 법정 증언의 부담 등으로 인해 진술을 번복하거나 법정에 출석하는 것을 꺼리는 경우가 종종 발생한다.

수사나 재판이 진행되면서 범죄사실이 달라지고, 이에 따라 이를 입증하기 위한 증거도 달라지는 경우, 수사 단계에서는 필요성이 없어 보여 수집하지 않은 증거나 관련성이 인정되지 않았으나 재판 단계에서는 중요한 증거로 밝혀진 경우도 빈번하게 발생한다.

반면 압수수색 단계에서는 혐의사실과 관련성이 있고, 중요한 증거로 판단되어 압수수색이 진행되었으나 반대로 재판 단계에서 혐의사실과 관련성이 없고 무용한 증거로 밝혀진 경우도 실무에서는 어렵지 않게 찾아볼 수 있다.

즉 수사와 재판은 고정되어 있는 것이 아니라 끊임없이 변화하는 생물이므로 이와 같은 과정에 맞춰 추가 증거를 확보할 필요성이 발생하게 된다.

제 6 절 소결

이처럼 압수수색 현장에서 관련성 있는 증거들을 선별하여 논리 이미징 방법으로 압수수색하는 실무는 비할당 영역, 슬랙 공간 등에 저장되어 있는 아티팩트, 메타 데이터 등을 확보하기 어려우므로 안티포렌식 행위로 은닉, 삭제된 데이터를 검색하는데 한계가 있으며, 삭제된 데이터의 복구도 불가능하다.

또한 키워드 검색의 기술적인 한계로 인덱스 검색이 아닌, RAW DATA 검색의 경우 관련성이 있어도 검색이 불가능 해 현장에서 탐지가 어려운 증거들을 확보하지 못하는 한계가 있으며, 수사와 재판 과정에서 범죄혐의 및 쟁점이 변화하는 상황에 대한 적절한 대응이 불가능하다.

이와 같은 실무상의 기술적, 규범적인 한계를 반영하고 실체적 진실을 보다 효율적으로 발견하기 위해서는 디지털 정보 저장매체 전체의 물리적 이미징 확보가 필요하다 할 것이다.

물론 이와 더불어 사건과 관련성이 없고, 개인의 사생활의 비밀과 관련된 정보의 경우 수사기관의 과잉 압수와 임의적 접근을 막을 수 있는 제도적 기술적 장치의 필요성도 함께 논의되어야 할 것이다.

제 6 장 새로운 방법의 제안

제 1 절 기존 연구 방법

디지털 증거의 선별 압수수색 및 참여권 보장과 관련된 여러 가지 문제점들을 개선하기 위해 그 동안 여러 분야에서 많은 연구들이 진행되어 왔다. 우선 기존에 이루어진 선행연구들에 대하여 살펴보도록 하겠다.

피압수자의 참여권을 실질적으로 보장하기 위한 방법으로 시크릿 쉐어링 시스템을 활용하는 방안을 제안한 논문[88]이 있다. 위 논문에 따르면 비밀키를 한 사람이 아닌 여러 명이 나누어 보관하는 것으로 2개의 키가 맞아야만 봉인된 자료를 복호화하여 열람 가능하게 하는 시스템이다. 또한 이와 같이 봉인된 증거들은 수사기관·법원 등이 아닌 중립기관에 보관하도록 하였다. 즉 수사기관과 피압수자가 각자 키로 암호화하고, 암호화된 자료는 제3의 중립기관에 보관한 뒤 추가 열람이 필요한 경우 수사기관과 피압수자 쌍방의 동의하에 각자의 키를 내 놓고 중립기관이 이를 검증하여 이미지 파일을 열람하게 하는 방안이다.

위 방법은 사건과 관련이 없는 사생활 정보를 보호하기 위해 암호화 방식을 제안하였다는 점에서는 의미가 있으나, 제3의 중립기관을 설치하기

88) 강상현, “사생활 정보를 고려한 디지털 증거처리 모델”, 고려대학교 석사학위 논문, 2015.

위한 근거 법률의 부존재, 당사자가 열람을 거부할 때를 대비하여 제3의 중립기관에서 비밀키를 보유할 필요성이 있는데 이와 같은 제3의 중립기관에 의한 정보 유출의 위험 등이 존재한다. 또한 수사기관과 피압수자 쌍방의 동의 하에 복호화를 하는 경우 관련성 있는 정보가 아닌 선별을 거치지 않은 전체 정보가 복호화 되고, 이를 수사기관이나 제3의 기관이 열람, 유출할 수 있다는 문제가 있다.

이와 같은 문제점을 고려하여 집행현장에서 이미지 파일을 Shamir의 임계 암호 방식을 사용하여 암호화하고, 암호키를 3개로 나누어 수사기관, 피압수자, 법원에 분배한 뒤 이 중 2개의 암호키 조각만 있으면 복호화가 가능하도록 설계한 논문[89]도 있다.

기존의 형사사법망을 활용할 수 있고 입법의 문제없이 바로 실행이 가능하며, 피압수자의 참여권 남용의 경우에도 적극적인 대처가 가능하다는 장점이 있으나, 전자정보를 선별하는 과정은 상당한 시간이 필요하게 되어 이 과정에서 암호가 해제된 상태에 있는 이미지 파일이 유출되거나 암호파일이 해제되면 임시파일이 생성되는데 이와 같은 임시파일을 통해 임의적인 접근이 가능해지므로 임시파일 처리를 위한 추가 조치가 필요하다는 한계가 있다.

수사기관이 피압수자 등의 참여가 보장되지 않은 상태에서 압수 또는 복제된 저장매체 내의 전자정보를 무분별하게 열람 또는 복제, 출력하는 것을 방지하기 위해 DRM 방식으로 전자정보에 대한 사용 이력 관리 방안을 제안한 논문[90]도 있다.

구체적인 기술구조는 압수한 저장매체의 이미지 등은 대검찰청의 디지털통합수사업무시스템(D-NET)에 등록하고, 수사기관의 담당 직원이 자신이 업무용으로 사용하는 PC에서 관련 전자정보에 대한 다운로드 요청을 하게 되면, D-NET에서 이를 Server DRM[91] 시스템에 전송하게 된다.

---

89) 강석한, “전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구”, 서울대학교 융합과학기술대학원 석사학위 논문, 2016.
90) 김광호, “참여권 보장을 위한 전자정보 압수수색 집행 방안에 관한 연구”, 서울대학교 융합과학기술대학원 석사학위 논문, 2016.
91) 문진규, “내부정보유출방지를 위한 DRM 적용방법설계”, 한국컴퓨터종합학술

Server DRM에서는 전송받은 전자정보를 암호화하여 직원 PC에 전송하고, 직원은 다시 열람을 위한 복호화 키를 Server DRM에 요청하면 Server DRM은 사용자 인증과 권한을 확인한 후 복호화 키를 직원 PC에 전송하면서 그와 같은 사용 이력을 기록하게 된다는 것이다.

이와 같이 사용 이력을 남겨 비정상적이거나 무분별한 열람, 복제를 방지하고, 체계적으로 관리할 수 있다는 점에서 의미 있는 제안이라 할 것이다. 그러나 최초에 집행 현장에서 암호화되지 않은 채로 디지털수사통합업무시스템에 등록을 하고, 수사관 등의 요청이 있는 경우 사후적으로 암호화하는 방안은 완벽한 보안이 이루어지기에는 분명 한계가 존재한다.

압수한 디지털 데이터를 안전하게 관리하고 보관연속성을 증명하는 방안으로 블록체인을 이용하는 방식을 제안한 논문[92]도 있다. 위 논문에서는 검찰의 D-NET에서 생성되는 디지털 증거와 관련된 로그를 모아 블록체인 방식을 이용하여 관리하고, 범죄사실과 무관한 정보는 폐기하면서 폐기한 로그 자체에 대한 해시 값과 블록체인 안에 저장되어 있는 해시값을 비교 분석하여 보관연속성을 증명하는 방식이다.

이는 압수수색 후의 정보를 관리함에 있어 적법한 관리자만 접근이 가능하고, 보관의 연속성 증명 및 무관정보 폐기를 효율적으로 가능하게 한다는 장점이 있으나, 압수수색 단계에서 선별 압수 원칙과 관련된 문제를 해결하기에는 한계가 있다.

또한 최근 많은 분야에서 상용화가 이루어지고 있는 동형암호를 활용하여 디지털 증거를 압수수색하는 방안을 연구한 논문[93]도 있다.

위 논문에서는 디지털 증거의 경우도 유체물과 동일하게 디지털 증거의 범위를 매체 단위로 인정하여 저장매체 전체를 압수수색 시 확보하고 동

대회, 2007. 참조, 전자문서를 암호화하는 시점이 사용자 PC에 다운로드 전인 정보시스템 서버 내에서 이루어지고, 전자문서가 사용자 PC에 다운로드된 후에 열람, 인쇄, 저장 등 이용의 권한을 통제하는데 사용됨

92) 임성훈, “압수한 디지털 데이터의 안전한 관리 방식 제안”, 서울대학교 융합과학기술대학원 석사학위 논문, 2016.

93) 오미경, “디지털 증거 선별 압수·수색에 따른 문제점 해결을 위한 기술적 방안 연구”, 서울대학교 융합과학기술대학원 석사논문, 2019.

형암호를 통해 암호화하는 방안을 제시하고 있다. 동형암호 알고리즘을 이용하여 암호화된 상태에서 연산을 수행하고, 이를 통해 찾고자 하는 정보의 존재 여부를 확인한 뒤 복호화하는 방식이다. 또한 피압수자에게도 관련성 낮은 정보를 추출하게 하여 이를 수사기관이 검토한 뒤 관련성이 낮다고 판단되면 분리하여 암호화하여 암호화하는 대상 파일의 크기를 줄이는 방법도 병행하자고 제안하고 있다.

동형암호의 경우는 암호화된 상태에서 연산이 가능하고, 복호화 되기 때문에 개인정보 보호에 탁월하다는 장점이 있다. 그러나 동형암호는 복잡한 연산에서는 상당한 시간이 소요되어 상용화되기까지에는 보완 연구가 필요할 것으로 보인다.

제 2 절 2단계 압수수색방안 개요

본고에서는 압수수색의 절차를 2단계로 나누어 디지털 증거의 종류에 따라 2단계 압수수색방안을 적용하여 수사 초기에 필요한 디지털 증거를 충분히 확보하는 방안을 제안한다.

1단계는 사용자가 생성한 증거의 경우 관련성이 있는 증거를 선별하여 압수수색을 진행하되, 관련성의 범위를 직접증거뿐만 아니라 간접증거에 해당하는 증거도 포함하여 보다 넓게 인정하고, 이에 더하여 컴퓨터가 생성한 증거의 경우에는 생성 증거 전체를 현장에서 바로 압수수색 하여 암호화 없이 바로 D-NET에 업로드 시키는 방안이다.

이와 더불어 2단계는 저장매체 전체에 대해 물리 이미징을 한 뒤 이를 공개키로 암호화하는 방안이다.

공개키로 암호화한 저장매체 전체의 물리 이미지는 신뢰계산 기술을 바탕으로 고안된 블랙박스 안에 저장하고, 필요한 경우 해당 증거에 한해 복호화 시켜 증거로 사용하는 구조이다.

아래에서 단계별로 상세히 서술하도록 하겠다.

	압수수색 범위	압수수색 방법
1단계	사용자가 생성한 증거 중 관련성 있는 증거	논리 이미지 추출
	컴퓨터 생성 증거 일체	
2단계	저장매체 전체 복제	물리 이미지 추출 ⇒ 신뢰계산 기술 활용한 블랙박스 안에 보관하고 필요한 증거만 복호화

[표2] 단계별 압수수색 방안

제 3 절 관련성 있는 디지털 증거의 범위 확장

1. 관련성의 의미

수사 또는 재판 단계에서 압수수색을 하는 경우 해당 사건과의 관련성 유무를 그 기준으로 삼는데, '관련성'의 의미에 대해서는 수사와 재판에서 증거로 사용할 수 있는 개연성 또는 가능성 정도로 정의할 수 있다. 그러나 증거로 사용될 수 있을지 여부는 수사와 재판이 진행됨에 따라 계속 변하여 재판을 통해 최종적으로 결정될 수밖에 없는 것이 수사와 재판의 속성이다.

결국 수사 단계에서 '관련성' 유무의 판단 시점은 압수수색 당시를 기준으로 해야 하므로 압수수색 당시에 해당 사건과 관련성이 있다고 인정되는 경우라면 재판 단계에서 관련성이 없다고 밝혀진다 하더라도 위법한 증거로 볼 수는 없을 것이다.

이처럼 압수수색은 수사와 재판에서 증거로 사용할 수 있는 개연성 또는 가능성을 의미하는 바, 여기서 '증거'란 요증사실의 존부를 직접적으로

증명하기 위해 사용되는 직접증거와 정황증거인 간접증거로 구별된다. 범죄의 성립 요소인 구성요건 해당사실, 위법성과 책임조각 사유의 부존재, 처벌조건은 엄격한 증명의 대상이 되므로, 증거법상 증거능력이 인정되는 증거로 증명을 하여야 한다.

그러나 정상관계와 관련된 사실, 증거능력 입증을 위한 진정성립과 관련된 자료, 증거의 증명력을 탄핵하는 데 사용하는 탄핵 증거 등은 간접증거로 보아 자유로운 증명의 대상이 되고, 증거능력을 요하지 않는다.

즉 범죄사실과 밀접한 관련이 있는 증거뿐만 아니라 수사 진행에 있어 도움이 되는 피의자의 소재를 확인할 수 있는 자료, 피의자의 동종 범행 자료, 비행 자료, 범행의 동기, 준비, 계획 등을 위한 자료를 비롯하여 양형자료, 증거능력 입증을 위한 진정성립 자료 등도 압수대상인 증거물이 될 수 있다고 판단함이 상당하다.

2. 컴퓨터 생성 증거와 관련성

디지털 증거의 경우 정보의 대량성, 비가독성이라는 특성으로 인해 일반 압수수색 절차와는 다른 절차가 실무에서 형성되고 있다.

저장매체 안에 저장되어 있는 정보들은 그 대량성으로 인해 압수수색 현장에서 모두 열람, 확인하여 관련성 여부를 판단하기는 거의 불가능에 가까우며, 안티포렌식 행위로 인해 데이터가 삭제, 은닉, 암호화된 경우에는 이를 복구, 복호화하는 과정을 거친 뒤 관련성 여부를 확인해야 하므로 소요되는 시간과 복구 장비 등의 부존재로 인해 현장에서 모든 정보를 선별하는 것이 현실적으로 어렵다.

또한 저장매체 안에 들어 있는 정보를 확인하기 위해서는 일정한 프로그램 등을 통해 가독성 있는 상태로 변환해야 하는 과정을 거쳐야 한다는 점도 실무상 많은 어려움을 초래하는 요소 중 하나이다.

저장매체 안에는 범죄와 관련성 있는 증거부터 내밀한 사생활의 영역과 관련되어 있어 보호의 필요성이 높고 범죄와의 관련성은 낮은 증거들도 많이 존재한다.

이에 따라 디지털 저장매체 안에 저장된 정보의 경우 실체적 진실의 발견과 사생활의 비밀, 개인정보 보호 등의 기본권 보호라는 두 이념을 비교 형량하여 조화롭게 그 기준을 설정해야 할 것이다.

이와 같은 측면에서 보았을 때 혐의사실과 관련성 있는 증거를 판단함에 있어 사용자가 직접 생성한 문서를 위주로 그 내용만을 주된 기준으로 관련성 여부를 판단하는 것은 디지털 증거의 특성상 여러 가지 중요 증거를 놓칠 수 있다는 면에서 적절하지 못하다.

사용자의 행동 양식은 범행을 저지른 방법에 반영되고, 특정 훈련 또는 지식 분야에 대한 특성은 오랜 시간 진화되고 발전되어 습득된 행위이므로 범인을 특정하는데 많은 도움을 준다. 이와 같은 사용자의 행동 양식은 컴퓨터가 생성한 증거를 종합적으로 분석해야만 밝혀낼 수 있다.

또한 사용자가 생성한 증거가 아니라 사람의 개입 없이 컴퓨터가 프로그램에 따라 자체적으로 내장된 알고리즘을 통해 자동 또는 임의로 생성한 컴퓨터 생성 증거는 디지털 증거의 진정성립을 인정하는 기초 자료로 주로 활용된다. 컴퓨터가 자동으로 생성한 증거로는 앞서 살펴본 바와 같이 아티팩트, RAM 정보, 슬랙 공간에 저장된 정보, 레지스트리 상에 존재하는 정보 등을 그 예로 들 수 있다.

이와 같은 컴퓨터 생성 증거의 경우 작성자가 공판준비나 공판기일에서 그 성립의 진정을 부인하는 경우에 한해 관련성을 인정할 수 있다고 해석[94]하는 견해도 있으나, 작성자의 의사에 따라 관련성 인정 여부가 달라진다고 볼 수 없으며, 디지털 증거의 경우 그 특성상 컴퓨터 생성 증거와 결합하였을 때 그 증거능력 및 신빙성이 높아지는 점 등에 비추어 보면 관련성을 의미를 넓게 해석할 필요가 있다 할 것이다.

3. 소결

혐의사실과의 관련성 문제는 수사와 재판 과정에서 계속 변화하며, 이와 같은 관련성은 '수사와 재판에서 증거로 사용될 가능성'을 일응의 기준

94) 김영철, 앞의 논문 33면 참조

으로 볼 수 있으며, 증거는 직접증거뿐만 아니라 간접증거도 포함한다고 봄이 상당하다 할 것이다.

사용자가 작성한 문서, 메시지 등과 같은 디지털 증거의 경우 그 내용이 혐의사실과 관련성 있는지 여부를 판단해야 할 것이다. 여기서 관련성도 앞서 살펴본 바와 같이 압수수색 당시 향후 수사나 재판에 사용될 가능성이 있는 직접증거를 포함한 간접증거 일체에 대해 관련성을 인정할 필요가 있을 것이다.

또한 컴퓨터가 자동 또는 임의로 생성하는 MFT와 같은 메타 데이터, 로그기록, 윈도우 레지스트리 등은 해당 파일의 내용이 기록되는 공간과는 별도의 공간에 기록되고, 관련 내용이 있는 정보, 특정 시기의 정보만을 분리하는 것이 쉽지 않으며, 안티포렌식 행위 등에 대응하기 위해서는 이를 전체적으로 압수하여 분석할 필요성이 높다 할 것이다.

컴퓨터 생성 증거의 경우 디지털 증거의 진정성립을 인정하는 기초 자료 또는 간접증거, 정황증거로 볼 수 있고, 압수수색 당시 수집하지 않으면 사용자의 의도적 또는 비의도적인 접근 등에 의해서 변경가능성이 높은 점, 컴퓨터 생성 정보의 특성상 사용자가 작성한 디지털 데이터와 비교해 보았을 때 개인정보 침해 가능성은 낮은 점 등을 고려해 보았을 때 관련성의 범위를 보다 폭 넓게 인정할 필요가 있다 할 것이다.

제 4 절 신뢰계산 기술 방법

1. 개인정보 보호 기술

디지털 증거를 안전하게 보호하면서 필요할 때 활용하기 위한 방안으로 데이터 비식별화(Data anonymization), 차등보호(Differential Privacy), 동형암호(Homorphic Encryption), 신뢰계산 기술(Hardware-Assisted Trested Computing) 등이 있다.

비식별화란 개인정보의 일부 또는 전부를 삭제하거나 다른 정보로 대체

함으로써 다른 정보와 결합하여도 특정 개인을 식별하기 어렵게 하는 일련의 조치[95]를 의미한다. 개인정보 중 일부를 특정 개인에 대하여 식별이 어려운 다른 데이터로 바꾸는 방법인 가명처리 방법, 전체 또는 부분적인 통계값을 적용하는 총계처리 방법, 개인정보의 식별이 어렵도록 데이터 전부 또는 일부를 삭제하는 데이터 삭제 방법, 데이터를 그룹화하여 그룹의 대표값, 구간값으로 범주화하는 데이터 범주화 방법, 데이터의 전부 또는 일부를 노이즈, 공백 등의 다른 값으로 대체하는 데이터 마스킹 방법이 있다.

차등보호[96]란 하나의 데이터 안에 있는 여러 개의 정보들을 원래 데이터가 가지고 있는 평균, 편차 등을 유지하면서 정보의 값을 변경시키는 방법이다. N-1명의 평균과 N명의 평균을 안다면 한 명의 데이터 값을 복원할 수 있다는 것이 관찰됨에 따라 데이터 분석의 결과 값으로 특정인의 정보가 유출되는 것을 방지하기 위해 차등보호가 필요하게 되었다.

차등보호란 기본적으로 통계적인 특성만을 유지하도록 노이즈를 추가하는 방식인데 Global DP와 Local DP의 두 가지 방식으로 나눠진다. Global DP는 데이터를 분석한 후 결과 값에 노이즈를 추가하는 것으로 결과값의 정확도가 상대적으로 높으나 신뢰할 수 있는 제3의 기관(Trusted Third Party, TTP)이 필요하다는 단점이 있다.

Local DP는 데이터를 분석하기 전에 노이즈를 추가하는 것으로 TTP는 필요 없으나 결과 값의 정확도가 낮다는 단점이 있다. Google Chrome이 사용자 데이터를 수집할 때 Local DP 방식을 사용하고 있다.

그러나 차등보호 방식은 평균, 합 등 구하고자 하는 목표함수에 따라 이에 맞는 데이터 변환이 필요하고, 기계학습 등과 같은 복잡한 분석은 수행하기 어려우며, 분석 결과 값의 정확도가 손실된다는 단점이 존재한다.

다음으로 동형암호[97]는 암호화된 데이터를 복호화 없이도 연산할 수 있

95) 미래창조과학부·NIA·빅데이터 전략센터, 빅데이터 활용을 위한 개인정보 비식별화 사례집92014), 14면 참조
96) 천정희, 2019정보보호이론, 2019, 139~140면 참조
97) 천정희, 앞의 책, 18~21면 참조

는 암호 기술로 암호화된 상태에서 컴퓨터로 하는 모든 연산이 가능[98]하고, 암호화 후 검색, 통계처리, 머신러닝이 가능하며, 해커의 데이터 유출을 원천 봉쇄할 수 있다는 장점이 있다. 동형암호는 임의의 연산을 무한하게 계속할 수 있는 완전동형암호와 제한된 연산만 할 수 있는 제한동형암호로 구분된다. 그러나 속도가 느리고, 연산의 종류에 따라 속도 차이가 커서 아직은 용량이 큰 데이터에서 사용하는 데는 한계가 있어 실질적으로 활용하는 분야는 많지 않다. 그러나 실용성을 보완하는 연구가 계속되고 있어 향후 많은 분야에서 사용될 것으로 예상된다.

본고에서 검토하려는 신뢰계산 기술은 일부 클라우드 컴퓨터에서 이미 사용되고 있는 기술로 신뢰할 수 있는 하드웨어를 기반으로 데이터를 보호하는 방법이다. 자세한 내용은 다음 항에서 기술하겠다.

2. 신뢰계산 기술(Hardware-Assisted Trested Computing)

신뢰계산 기술은 하드웨어를 기반으로 CPU 이외에는 접근이 불가능한 안전한 실행영역을 만든 뒤 사용자의 프로그램 등이 해당 안전 영역 안에서만 수행되도록 구현하여 수행 과정과 그 결과의 보안이 보장되는 기술이다.

데이터 보안 이슈의 중요성이 강조됨에 따라 주요 클라우드 업체에서 제공하고 있는 서비스로 Microsoft Azure[99]의 경우 Intel SGX(Software Guard Extention)를 기반으로 보안이 유지되는 기밀 컴퓨팅(confidential computing) 서비스를 제공하고 있다. Google Cloud의 경우에도 AMD SEV(Secure Encrypted Virtualization ; 보안 암호화 가상화)를 기반으로 하여 보안 클라우드 서비스를 제공하고 있다.

기밀 컴퓨팅이란 데이터 계산을 하드웨어를 기반으로 한 신뢰할 수 있

---

98) 곱셈만 가능한 곱셉동형암호, 덧셈만 가능한 덧셈동형암호와 같이 일부 연산만 수행이 가능한 부분동형암호도 존재함[천정희·어윤희·김재윤, “개인정보가 보호되는 동형암호기반 금융데이터분석”, 금융정보연구 제7권 제1호, 한국금융정보학회(2018. 2.), 39면 참조

99) azure.microsoft.com 참조

는 실행 환경(Thrusted Execution Environment ; TEE) 안에서 수행하도록 하여 사용 중인 데이터를 보호하는 것이다. 데이터는 일반적으로 미사용 및 전송 중에는 암호화되지만 계산이 이루어지는 중에는 암호화 되지 않는 것이 일반적인데 반해 기밀 컴퓨팅은 처리 중인 데이터도 암호화 된 상태로 보호된다.

즉, TEE는 하드웨어의 프로세서 및 메모리 일부를 보호하여 보호된 컨테이너를 제공하고, 보호된 환경 위에서 소프트웨어를 실행하여 TEE 외부에서 코드와 데이터 부분을 보거나 수정하지 못하도록 보호할 수 있다.

기밀 컴퓨팅을 사용하면 클라우드에서 처리하는 동안 중요한 데이터를 격리 할 수 있어 금융 데이터 보안, 환자 정보 보호, 중요한 정보에 대한 기계 학습 프로세스 실행, 여러 원본에서 암호화된 데이터 세트에 대한 알고리즘 수행 등 여러 분야에서 기밀 컴퓨팅을 사용하여 데이터를 보호하려고 하는 것이 최근의 추세이기도 하다.

3. Intel SGX(Software Guard Extention)[100]

가. 개요

Intel사에서 개발한 SGX는 하드웨어를 기반으로 보안 기능을 제공하는 것으로 CPU 내부에 보안 및 암호화 메커니즘의 도움을 받아 신뢰할 수 없는 사용자로부터 민감한 데이터를 보호하는 기술이다.

디스크 암호화, 네트워크 트래픽 암호화 등의 기술은 전송 중인 데이터나 스토리지 내에서의 데이터를 보호하는 데는 유용하지만 메모리에서 사용 중인 데이터에 대한 가로채기와 변조에 취약할 수 있다는 점에 착안하여 개발된 기술이다.

사용 중인 환경에서 엔클레이브(Enclave)라고 부르는 프라이빗 메모리를 만들어 그곳에 데이터를 저장하여 프라이버시 침해 가능성을 없애는

100)https://medium.com/magicofc/the-magic-of-intels-sgx-how-to-hello-it-sec-world-fd0295d6c33b 참조 (2020. 12. 6. 최종 방문)

방식이다.

기밀성과 무결성을 유지하면서 민감한 데이터를 보호할 수 있도록 암호화된 앤클레이브를 만드는데, 이러한 앤클레이브는 내부에서만 접근할 수 있으며, 일반 텍스트는 CPU 내부에서 처리되는 동안에만 표시되므로 응용프로그램이나 신뢰할 수 없는 당사자가 정보를 얻거나 데이터 및 코드를 조작하지 못하도록 보호할 수 있다.

Intel은 이와 같은 SGX 기능과 더불어 기밀성 향상 및 데이터 무결성을 위한 전체 메모리 암호화(Total Memory Encryption ; TME[101]), 플랫폼 펌웨어 레질리언스(Platform Firmware Resilience ; PER[102]), 새로운 암호화 가속기 기능을 지원하는 인텔 3세대 제온 플랫폼을 곧 출시할 예정이다.

나. SGX의 Enclave[103]

SGX는 외부의 공격이 가능한 디바이스에 안전한 샌드박스를 구현하는 것인데, 이와 같은 샌드박스 기능을 하는 것이 앤클레이브(Enclave)이다. SGX 기능을 사용하는 응용프로그램은 신뢰할 수 있는 영역과 신뢰할 수 없는 영역으로 구분되는데, SGX 기능을 사용하는 응용프로그램이 시작되면 신뢰할 수 있는 메모리 영역에 앤클레이브가 생성되면서 SGX 동작이 실행된다.

앤클레이브는 메모리 영역에 PRM(Processor Reserved Memory)이라는 영역을 지정하여 독점적으로 사용하는데, PRM은 CPU에 의해 운영체제, 하이퍼바이저, 커널 등의 모든 접근으로부터 보호된다.

PRM에는 EPC(Enclave Page Cache), SECS(SGX Enclave Control

---

101) TME란 고객 자격 증명, 암호화 키 및 기타 IP 또는 외부 메모리의 개인정보를 포함해 인텔 CPU에서 접근하는 모든 메모리가 암호화되도록 하는 기능을 의미함

102) PER은 프로그래머블반도체(FPGA)를 신뢰성 플랫폼 루트로 사용하여, 펌웨어 코드가 실행되기 전 부팅시 위험이 있는 플랫폼의 펌웨어 구성 요소를 검증하는 기능을 의미함

103) Intel Corporation, "Intel® Software Guard Extention,", 2015 참조

Srtucture), EPCM(Enclave Page Cache Map) 영역이 존재하는데, EPC는 앤클레이브 내부의 코드 및 데이터를 저장하는 페이지이다. EPCM은 EPC의 페이지 정보를 가지고 있는 가상의 주소 공간이고, SECS는 앤클레이브 자체의 속성 정보가 담긴 메타 데이터가 저장되는 곳으로 앤클레이브의 메모리 주소에 연결되지 않고 CPU의 SGX 구현에 의해 독점적으로 사용된다.

SGX 기능을 사용하는 응용프로그램이 운영체제로부터 앤클레이브 페이지를 요구하게 되면 실제 응용프로그램이 동작하기에 앞서 보호하고자 하는 데이터 및 코드를 앤클레이브 페이지에 추가하여 초기화한다.

앤클레이브의 모든 페이지가 EPC 영역에 로드되면 시스템 소프트웨어는 CPU에 앤클레이브가 초기화되었다는 신호를 보내고, 응용프로그램은 앤클레이브 내부의 데이터 및 코드를 안전하게 사용할 수 있게 된다.

다. 암호화(Sealing)[104]

앤클레이브 내부의 데이터는 외부 플랫폼으로부터 안전하나 시스템이나 어플리케이션이 갑자기 종료되는 등 앤클레이브 내부의 데이터가 외부로 나가게 되는 경우, 데이터를 앤클레이브 밖의 신뢰할 수 없는 영역에 저장해 두어야 한다. 이 과정에서 외부의 공격이나 내부의 악의적인 접근을 막고 데이터를 안전하게 보호하기 위해 앤클레이브를 벗어나기 전에 인증된 암호화 키를 이용하여 암호화 시키는 기술이 실링(Sealing)이다.

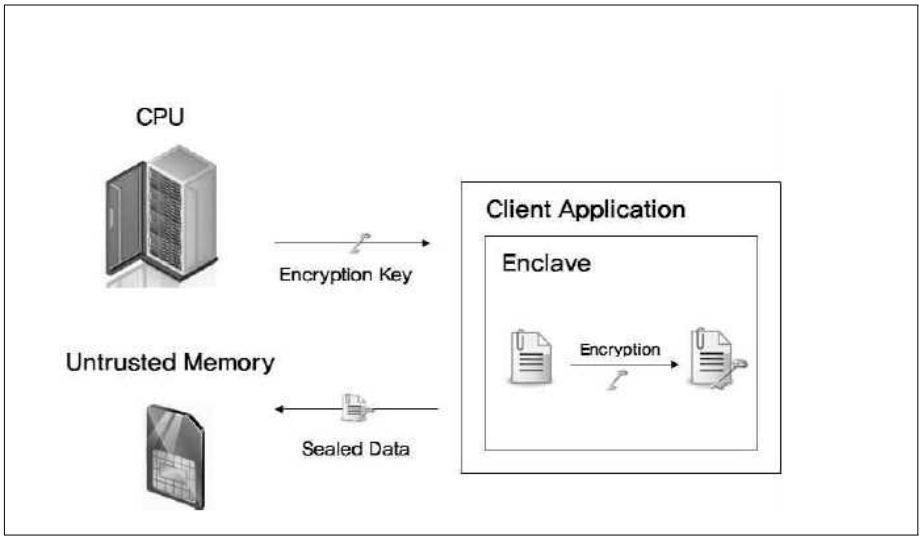
이때 사용되는 암호화키는 CPU로부터 획득한 것으로 이렇게 암호화된 데이터는 동일한 시스템에서만 복호화 될 수 있으므로, 앤클레이브 내부에 있던 중요 데이터들이 암호화되어 기밀성 및 무결성을 유지한 채로 앤클레이브 외부에 저장되는 것이다.

즉 암호화된 데이터들은 비신뢰영역에 저장되지만 복호화 키는 앤클레이브 안에 저장되어 있기 때문에 기밀성이 유지되고, 이와 같이 실링된

104) 노영욱, 김동규, “Intel SGX Sealing 기법에 기반한 메모리 보호기법”, 한국정보과학학회 학술발표논문집, 2018. 6. 1214~1216 참조

데이터를 복호화 하기 위해서는 앤클레이브 내부로 옮겨 복호화 해야 하므로 데이터가 보호된다. 이 과정에서 무결성 검사가 진행되어 실링을 통해 많은 양의 데이터들을 안전하게 디스크에 저장되고, 필요한 데이터 및 코드만 앤클레이브 내부에서 처리할 수 있다.

실링을 통해 디스크에 저장된 데이터를 처리할 필요가 있는 경우에는 다시 앤클레이브 내부로 옮겨 와 실링에 사용하였던 암호화 키를 사용하여 데이터를 복호화 하여 처리하게 된다.



[그림3] 실링(Sealing) 프로세스105)

라. 무결성 검사106)

암호화된 데이터를 앤클레이브 내에서 복호화 하기 위해서는 데이터가 변조된 사실이 없는지 여부를 확인하는 무결성 검사가 필요하다. 각 앤클레이브에는 무결성 검사를 위한 특정 해쉬값이 저장되는 SECS가 포함되어 있다. 이 해쉬값은 EPC 내부에 저장된 앤클레이브에 저장되며 앤클레

105) 노영욱, 김동규, 앞의 글 참조
106) https://medium.com/magicofc/the-magic-of-intels-sgx-how-to-hello-it-sec-world-fd0295d6c33b 참조 (2020. 10. 20. 최종 방문)

이브 모드에서 CPU 내부의 MEE(Memory Encryption Engine)를 통해 실시간으로 복호화된다.

SGX 장치에는 칩 제조 공정에서 생성된 고정 비밀 키가 포함되어 있고, 암호 해독은 비밀 키로만 가능하다. 암호화된 데이터가 앤클레이브 내부에 도착하면 이를 비밀 키로 복호화하여 해쉬값을 계산하고, 앤클레이브 내부에 저장되어 있는 해쉬값과 비교하여 변조 여부를 확인하게 된다.

마. 이용 사례

컴퓨터 서버와 스토리지, 네트워크 장비 등의 IT 인프라 장비를 빌려주는 IaaS(Infrastructure as a Service) 사업자[107]들은 고객의 데이터를 보호하기 위해 Intel SGX 기능을 사용한다.

게임회사에서도 게임 어플리케이션의 변조와 악용을 막기 위해, 보안회사의 경우에는 데이터의 기밀성 유지, 암호 키의 안전한 보관 등을 위해 SGX 기능을 사용한다. 블록체인에서도 개인 정보 보호 및 보안 강화를 위해 거래 처리, 합의, 스마트 계약 및 키 저장 등에 SGX 기능을 사용하고 디지털 지갑에서도 안전한 지불 및 거래를 위해 SGX 기능이 사용되고 있다.

발신자와 수신자 간의 안전한 화상회의 환경을 지원하기 위한 Zoom, Google Meet와 같은 커뮤니케이션 및 메시징 관련 사업에서도 Intel SGX 기능이 이용되고 있다.

제 5 절 신뢰계산 기술을 활용한 디지털 증거 압수수색

1. 기본 아이디어

앞서 살펴본 것과 같이 현장에서 선별한 사용자 작성 데이터 및 컴퓨터

107) 넷플릭스가 대표적인 사례로 넷플릭스는 아마존웹서비스(AWS)의 IaaS 서비스를 이용하여 데이터센터 구축 없이 클라우드 환경에서 필요한 인프라를 꺼내서 사용함

가 생성한 디지털 증거 일체는 논리 이미징 형태로 추출하여 압수수색을 진행한다.(1단계)

이와 같은 선별 압수수색과 함께 저장매체 전체에 대한 물리 이미지를 공개키로 암호화하여 동결한 뒤 압수하여 신뢰계산 기술을 이용한 블랙박스 안에 보관하는 방안을 제안한다.(2단계)

앞서 살펴본 Intel의 SGX 기능을 활용하여 물리 이미지 전체를 암호화 시킨다. 여기서 암호화 과정은 마스터키와 CPU가 제공하는 암호화 키가 함께 묶여 항상 SGX 안의 블랙박스 내에서만 증거데이터가 복호화 되고 접근할 수 있도록 구현한다.

2. 실무에의 적용 검토

대검찰청은 2012년에 전국디지털수사망(D-NET)을 구축하여 디지털 데이터의 압수, 분석, 관리 및 폐기에 이르기까지 디지털 증거와 관련된 전반적인 업무 지원 및 정보시스템을 구축하였다.

D-NET은 디지털 데이터의 압수, 분석 및 분석 결과를 확인할 수 있는 디지털수사통합업무관리시스템(DFIS II), 디지털 증거 압수물을 보관 및 관리하는 디지털 증거 압수물관리시스템, 디지털 증거 압수물의 폐기와 관련된 디지털 증거 폐기관리시스템, 통화내역, 계좌내역, 회계 등 디지털 증거를 담당 수사관, 검사 등이 직접 분석할 수 있는 통합디지털분석시스템(IDEAS), 모바일포렌식 증거를 수집하고 분석하는 MFA운영시스템 등으로 구성되어 있다.

검찰수사관이 현장에서 디지털 증거를 압수하면 압수한 자료를 대검 디지털수사망(D-NET)에 업로드하게 되는데 디지털증거관리시스템은 이와 같은 디지털 증거 압수물의 생성부터 관리, 보관, 폐기에 이르는 생명주기 전체를 관리하고 있다.

디지털 증거의 경우 보관연속성 확보가 증거능력을 입증하는데 있어 매우 중요한 요소이며, 증거능력 입증의 성부를 가를 수 있는 문제이므로 각 지역별 디지털포렌식 수사지원팀과 대검 디지털수사과를 연결하여 압

수된 모든 디지털 증거를 대검에서 관리할 수 있도록 시스템을 설계하였다.

위 시스템은 사건 정보와 디지털 증거의 정보를 연계하여 조회 가능하도록 디자인하여 수사관 및 검사의 접근 권한을 설정할 수 있고, 권한이 없는 사람들의 접근 및 정보 수정을 차단하고 있다. 또한 디지털 증거 압수물에 접근하거나 열람, 다운로드 받은 이력 등 모든 변경 기록을 저장하여 증거보관의 연속성 입증이 가능하도록 하였다.

이와 같은 디지털 증거 관리시스템 안에 Intel SGX의 기본아이디어를 활용하여 블랙박스를 고안한 뒤 그 안에 암호화 된 저장매체 전체의 물리 이미지를 보관하는 방안을 설계해 볼 수 있다.

압수수색 현장에서 공개키로 암호화를 시키고, 공개키로 암호화된 비밀키(마스터키)는 신뢰기관만이 독점하며 신뢰기관이 보관하고 있는 비밀키로만 암호화 되는 것이 아닌 SGX의 CPU가 제공하는 암호화키와 바인딩되어 항상 SGX의 블랙박스 내에서만 증거 데이터가 복호화되고 접근할 수 있도록 설계한다.

위 블랙박스 안에 저장된 디지털 증거는 암호화된 상태로 보관되고, 블랙박스 안에서는 신뢰계산 기술에 근거하여 데이터의 처리가 이루어지므로, 임의적인 접근 및 열람이 불가능하다.

수사 또는 재판 과정에서 추가 증거 확보가 필요한 경우, 디지털 증거의 진정 성립과 관련된 아티팩트, 메타 데이터 등 직·간접 증거가 필요한 경우, 현장에서 키워드 검색 등으로 추출이 되지 않았던 증거가 추가로 필요한 경우 등 추가 증거 확보의 필요성이 생기면 위 블랙박스 안에 저장된 암호화된 디지털 증거를 복호화하여 활용할 수 있다.

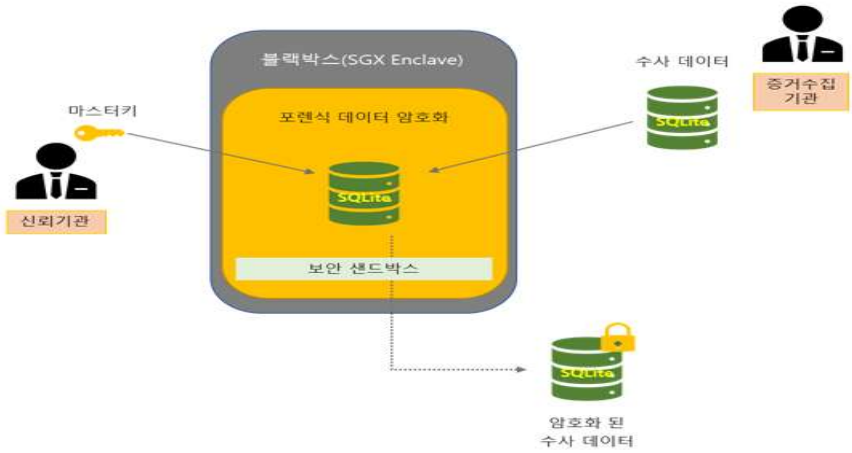
위 블랙박스 안에 저장된 디지털 증거는 저장매체 전체의 물리 이미지이므로 인덱스 추출이 가능하여 인덱스 검색을 통해 관련성 있는 추가 증거의 확보도 가능하다.

구체적인 절차는 우선 담당 수사관이 필요한 디지털 증거의 종류와 이를 추출할 수 있는 계산식, 계산 결과로 출력하고자 하는 바를 스크립트

형식으로 기술하여 마스터 키를 보관하고 있는 신뢰기관에 제출을 한다.

신뢰기관은 증거 확보의 필요성, 범죄 혐의와의 관련성 여부 등을 검토한 뒤 필요성이 인정된다고 판단한 경우 마스터 키를 이용하여 해당 포렌식 스크립트를 서명하는 방식으로 결재를 한다.

이와 같은 승인을 받은 담당 수사관은 이를 SGX 블랙박스 안에서 수행하게 되고, 암호화되어 있던 데이터는 블랙박스 내에서 계산되고 복호화되어 최종 계산 결과인 추가 디지털 증거만을 담당 수사관이 획득할 수 있게 된다.



[그림4] 신뢰계산 기술을 활용한 증거수집 및 암호화

3. 비밀키 생성 및 보관 주체에 대한 검토

그렇다면 과연 이와 같은 신뢰기관의 역할을 누가 할 것인지에 대한 판단이 필요하다. 상정할 수 있는 방식으로는 수사기관, 법원, 제3의 중립기관에서 비밀키를 보관하거나, 피압수자 등 다중이 보관하는 방식 등을 생각해 볼 수 있다.

우선 법원이 비밀키를 생성하여 관리하고, 추가 증거 확보가 필요한 경

우 수사기관에서 이와 같은 필요성 등을 소명하여 법원의 허가를 다시 받아 비밀키로 복호화 하는 방안을 생각해 볼 수 있다.

이와 같은 방식은 증거능력과 관련하여 불필요한 논쟁을 종식시키고 디지털 증거를 관리, 암호화, 복호화 하는 과정의 신뢰를 담보할 수 있다는 장점이 있을 수 있다. 그러나 범죄와 관련된 혐의가 인정되어 발부된 압수수색 영장으로 압수수색이 이루어졌고, 이에 근거하여 암호화된 상태에서 보관하는 증거를 다시 법원의 허가 등을 받아야만 증거로 사용할 수 있다는 것은 최초 발부받은 압수수색 영장의 효력에 의문을 갖게 하고, 법원의 입장에서도 이와 관련된 예산 및 전문가를 도입해야하며 관련 규정 또한 마련해야 한다는 현실적인 장애가 존재한다.

다음으로 제3의 중립기관에서 비밀키를 생성하여 관리하는 방안에 대해서 생각해 볼 수 있는데, 이와 같은 중립적인 기관의 신뢰성을 무엇으로 담보할 수 있는지 여부 및 제3의 중립기관을 통한 정보 유출 위험, 법적 근거 미비 등의 문제점이 존재한다.

피압수자 등 다중이 참여하여 비밀키를 공유하는 방식은 수사기관의 정보에 대한 임의적 접근을 막을 수 있고, 법원의 강제처분을 추가로 요하지 않는다는 장점은 있으나, 피압수자 등이 관련성이 없는 정보라며 협조하지 않는 경우 이를 해결할 방안이 존재하지 않아 현실적으로 구현이 어려울 것으로 예상된다.

마지막으로 수사기관, 즉 사건 담당 검사가 비밀키를 생성하여 보관하는 방안이다. 수사기관에서 아무런 제한 없이 비밀키를 생성하여 필요시 복호화 한다면 전자정보에 대한 임의적 접근을 배제할 수 없다는 측면에서 남용의 가능성이 문제될 수도 있다.

그러나 앞에서 제시한 신뢰계산 기술 방식에 따르면 블랙박스 내에서는 보관 및 연산 과정이 모두 암호화되기 때문에 담당 수사관은 이에 접근할 수가 없다. 관련성이 인정되고, 필요성이 입증된 정보에 한해 그 필요성과 그와 같은 정보를 추출할 수 있는 프로그램을 담당 검사에게 제시하면, 담당 검사는 이를 검토한 뒤 승인하고, 검사의 승인으로 마스터 키를 얻

어 복호화 한다면 수사기관의 임의적 접근을 막을 수 있을 것이다.

이와 같은 절차를 거쳐 획득한 증거의 경우, 복호화, 열람, 다운로드 등 제반 절차가 시스템에 기록되므로 이를 남용하기는 어려울 것으로 예상된다.

또한 저장매체 전체의 이미지를 수사기관에 반출 후 선별하는 과정은 수사기관의 분석행위의 일환으로 볼 수 있으므로 담당 검사의 승인 아래 집행하도록 함이 상당하다 할 것이다.

다만 이와 같은 일련의 절차를 독립된 디지털 검증기관에서 사후적으로 검증하여 압수수색 시부터 법정에 증거로 제출될 때까지 디지털 증거의 무결성을 보증하는 방안을 함께 도입하는 방법도 생각해 볼 수 있을 것이다.

수사의 경우 증거가 인멸되기 전에 신속하게 증거를 수집하고, 수사과정의 보안을 유지하는 것이 중요하므로 디지털 검증기관에서 사전적으로 이와 같은 마스터키 작동에 대한 적법성 여부를 확인하는 것은 실무상 많은 어려움이 존재한다.

그러므로 독립적인 디지털 검증기관을 두어 관련성 있는 증거가 적법하게 압수수색 되었는지 여부, 즉 담당검사가 신뢰계산 기술에 근거하여 관련성 있는 증거에 대해서만 마스터키를 이용하여 복호화하였는지 여부에 대하여 사후적으로 제3자로서의 감시자 역할을 담당하게 하는 방안이 보다 효율적인 방안이 될 것으로 생각된다.

4. 구체적인 절차

디지털 증거의 2단계 압수수색은 기본적으로 현장에서 저장매체 전체를 물리 이미징한 후 이를 암호화하여 보관하는 것을 기본으로 하되, 기술적인 문제로 현장에서 물리 이미징이 어려운 경우는 예외적으로 저장매체 전체를 반출하여 수사기관의 분석실에서 물리 이미징을 하여 암호화한 뒤 블랙박스 안에 저장하는 방법으로 진행할 수 있을 것이다.

저장매체 전체를 반출하는 경우에는 현장에서 봉인한 후, 피압수자의 서명을 받고, 수사기관의 분석실에서 봉인을 해제하는 과정 및 물리 이미징하여 블랙박스 안에 보관하는 과정을 모두 영상녹화하여 무결성을 보장할 수 있을 것이다.

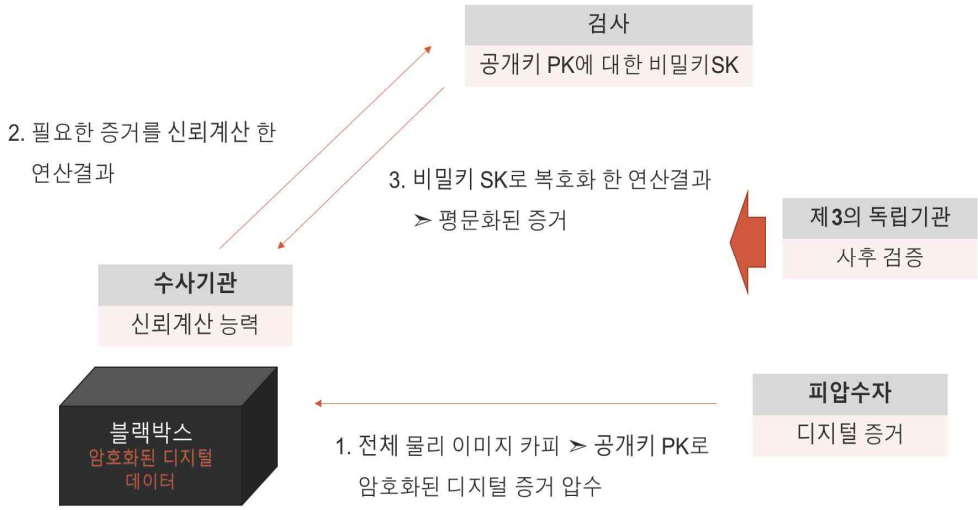
담당 수사관은 필요한 디지털 증거의 종류와 계산의 종류, 결과로 출력하고자 하는 바를 스트립트 형식으로 기술한 뒤, D-NET 시스템 내에서 담당 검사를 결재권자로 지정한 후 전자결재의 방식으로 기안하여 올린다.

담당 검사는 필요성, 관련성 여부 등을 검토한 뒤 적절한 경우 마스터 키를 이용하여 해당 포렌식 스크립트를 서명하는 방식으로 결재를 하게 된다. 결재를 받은 담당 수사관은 획득한 마스터 키로 SGX 블랙박스 안에서 암호화된 증거를 추출할 수 있는 프로그램을 돌리고, 필요한 디지털 증거를 획득할 수 있게 된다.

이와 같이 수사관이 담당 검사에게 결재를 올리고, 담당 검사가 이를 승인하고, 관련 정보가 복호화된 뒤 수사관이 정보에 접근하여 이를 증거로 제출하는 일련의 과정은 모두 D-NET 시스템에 남게 되고, 무결성 및 보관연속성을 증명하는 증거로 사용되기 때문에 법정에서 증거능력을 인정받기 위해서라도 관련성 없는 증거에 무분별하게 접근하거나 권한을 남용하는 경우는 없을 것이다.

또한 관련성 있는 증거는 법원에서 적법하게 발부한 압수수색 영장에 의해 당연히 압수할 수 있는 증거이므로 이와 같은 추가적인 정보 탐색 및 압수는 수사기관의 증거분석행위의 일환이자 영장집행 종료 이후의 행위이므로 임의수사로 볼 수 있을 것이다. 즉 법원의 추가적인 허가나 강제처분 없이도 당연히 획득할 수 있는 정보로 봄이 상당하다.

이와 같이 신뢰계산기술을 통해 추가로 획득된 정보에 대해서는 그 승인 절차나 열람, 다운로드 상황 등을 사후적으로 독립된 검증기관에서 확인함으로써 임의적인 접근을 예방할 수 있을 것으로 생각된다.



[그림5] 신뢰계산 기술을 활용한 디지털 증거 압수수색 방안 절차

5. 예상되는 효과

위와 같은 신뢰계산 기술방식을 사용하게 되면 디지털 증거의 복호화는 블랙박스 내에서만 이루어지고, 평문형태의 디지털 증거가 블랙박스를 벗어나지 않도록 보장되므로 수사기관에서 임의로 수사 관련 데이터를 열람할 수 없다.

또한 암호화된 상태로 보관되는 증거는 필요 시 저장매체 전체 이미지를 복호화 하는 것이 아니라 관련성이 인정되어 검사의 승인을 받은 증거만 추출하여 복호화 하기 때문에 피압수자의 사생활의 비밀과 자유 등이 침해될 가능성이 줄어들고, 과잉압수의 위험도 낮아지게 된다.

이와 같은 일련의 절차는 모두 전자적으로 남아서 위법성을 담보할 수 있고 디지털 증거의 보관 연속성, 무결성을 입증할 수 있으며, 그 과정에서 검사 및 수사관 모두 무관한 정보는 확인 불가능하므로 개인의 프라이버시를 보호하며 수사를 진행할 수 있다.

저장매체의 물리 이미지 전체를 복사하여 암호화된 상태로 저장하므로

키워드 검색뿐만 아니라 인덱스 검색도 가능하므로 현장에서 추출하지 못한 관련성 있는 정보를 사후적으로 추출할 수 있게 된다.

다음으로 참여권 보장과 관련된 여러 가지 문제도 해결할 수 있다. 현재는 저장매체 전체를 이미징하는 경우 현장에서 전체 이미징에 대한 해쉬값을 구한 뒤 봉인하고, 피압수자의 서명을 받아 수사기관의 분석실로 가져오게 된다. 수사기관의 분석실에서 사후적으로 관련성 있는 정보를 탐색하게 되는데 이 과정에서 피압수자의 참여권 등이 보장되어야 했기 때문에 참여권 보장과 관련된 다양한 문제가 존재하였다.

그러나 신뢰계산 기술을 이용하게 되면 현장에서 수집한 전체 물리이미지를 블랙박스 안에 암호화된 상태로 보관하고, 필요한 증거만 사후에 추출하게 되어 참여권 보장과 관련된 다양한 문제 해결할 수 있게 된다. 피압수자의 참여 없이도 검사의 승인에 따라 추출된 관련성 있는 증거들을 그 무결성, 보관연속성을 증명하여 법원에 증거로 제출하게 되므로 오랜 시간의 탐색과정을 지켜만 보아야 했던 피압수자의 불편을 줄일 수 있다. 참여 과정에서 수사기관의 포렌식 기법, 포렌식 도구 등 수사기밀의 유출 위험을 낮출 수 있으며, 참여하기로 하고 약속된 시간에 나타나지 않거나 부당하게 수사절차를 지연시키는 행위 등을 방지할 수 있다.

디지털 증거의 경우 초기에 확보하기 못하면 사건관계인들의 의도적 또는 비의도적 접근으로 인해 변경되거나 조작될 가능성이 높다.

수사 과정은 결론이 난 사건에 대한 검증 과정이 아닌 사건의 실체를 밝혀내 가는 과정이므로 압수수색을 거쳐 기소에 이르기까지 혐의사실이 변경될 가능성이 매우 높다는 점도 함께 고려해야 한다.

재판 실무에서도 피고인 또는 사건관계인들의 진술번복 등으로 추가 증거의 확보가 필요한 사례를 자주 접할 수 있다. 신뢰계산 기술을 이용하여 압수수색을 한다면 이와 같은 초기 증거의 확보 필요성 및 추가증거 확보 필요성의 문제를 상당 부분 해결할 수 있을 것으로 보인다.

수사나 재판 과정에서 범죄사실이 추가되거나 변경되는 경우 새로운 압수·수색 영장을 발부받아 이와 같이 암호화된 상태로 동결된 디지털 증거

를 압수하여 증거로 활용할 수 있을 것이다.

위 방식은 현재 구축되어 있는 D-NET 안에 Intel SGX의 기본아이디어를 활용하여 블랙박스를 고안한 뒤 그 안에 암호화된 저장매체의 물리 이미지를 보관하는 방법이므로 이를 개발하는데 많은 비용과 노력 없이도 구현이 가능하다.

또한 신뢰계산 기술은 복잡한 연산의 경우에도 빠른 속도로 처리가 가능하므로 잘 정의된 특정 연산의 진행에만 효과적인 동형암호에 비해 다양한 디지털 증거에 실용적으로 활용할 수 있다는 장점이 있다.

제 7 장 결 론

디지털 증거의 경우 무결성, 동일성 등의 요건을 갖춘 경우에 한해 증거능력이 인정되고, 디지털 증거 중 그 내용의 진실성이 문제되는 경우에는 전문법칙이 적용되므로 작성자에 의해 그 진정성립이 인정되는 경우 증거능력이 인정되고 있다.

그러나 디지털 증거의 특성상 형사소송법 제313조 제2항에서 작성자가 진정성립을 부인하는 경우에도 과학적 분석결과에 기초한 디지털 포렌식 자료, 감정 등 객관적 방법으로 성립의 진정함을 증명할 수 있도록 규정하고 있다.

이와 같은 디지털 증거의 진정성립은 주로 컴퓨터가 자동으로 생성한 증거를 통해 확인이 가능하고, 디지털 증거는 그 특성상 데이터에서 담고 있는 문서의 내용뿐만 아니라, 생성, 수정, 저장 등과 관련되어 컴퓨터가 자동 생성한 여러 정보도 함께 분석할 필요가 있다.

또한 실무에서 빈번하게 발견되고 있는 안티포렌식 행위, 삭제되거나 은닉된 데이터의 복구, 수사와 재판 과정에서 필요한 추가 증거의 확보 필요성, 현장에서의 키워드 검색의 한계 등의 문제를 극복하기 위해서는

저장매체 전체의 물리 이미지 확보가 절실하다.

이와 같은 디지털 증거의 특성에도 불구하고 현행 실무는 선별 압수수색의 원칙을 엄격하게 적용하고 있어 초기에 확보해야 하는 중요한 증거들을 놓치고 있으며, 이와 함께 피압수자에 대한 참여권 보장으로 인해 실무상 많은 어려움을 초래하고 있다.

또한 디지털 저장매체 안에는 관련성 있는 증거와 관련성 없는 증거가 함께 저장되어 있고, 문서 파일 안에도 관련성 있는 정보와 관련성 없는 정보가 혼재되어 있는 경우가 상당하다.

본고에서는 실체적 진실의 발견과 피압수자 등 사건관계인의 사생활의 비밀, 개인정보 등의 기본권 보호를 조화롭게 구현시키기 위한 방법으로 2단계 압수수색 방안을 제안하였다.

1단계에서는 사용자가 생성한 관련성 있는 증거와 이에 더하여 컴퓨터 생성 증거 일체를 현장에서 수집한 뒤 논리 이미징 형식으로 압수하여 대검 D-NET에 업로드 하여 분석한다. 관련성 판단의 시점은 압수수색 당시이고, 관련성의 범위는 시시각각 변화하는 수사와 재판 과정을 고려하여 직접증거 뿐만 아니라 간접증거도 포함하는 개념으로 해석함이 상당할 것이다.

다음으로 2단계에서는 저장매체 전체를 물리 이미징하여 동결한 뒤 이를 암호화하여 신뢰계산 기술을 바탕으로 한 블랙박스 안에 업로드 시키는 방안이다. 위와 같이 암호화된 증거는 블랙박스 안에서만 계산, 복호화되는데, 검사의 승인이 있어야 복호화될 수 있으며, 계산 과정 또한 암호화되어 진행되므로 피압수자의 사생활 보호 및 수사기관의 범죄와 관련성 없는 정보들에 대한 접근을 막을 수 있다는 장점이 있다.

또한 선별을 거치지 않은 물리 이미지 전체가 복호화되는 것이 아니라 관련성이 있는 증거만 복호화 되므로 피압수자들의 사생활의 비밀, 개인정보 등이 침해될 우려도 낮을 것으로 예상된다.

이와 같은 신뢰계산 기술을 바탕으로 디지털 증거가 사라지기 전에 필요한 증거들을 확보하고, 그 중 범죄와 관련성 있는 증거만을 현출시켜,

관련성 기준 위반으로 인한 위법성 문제와 컴퓨터 생성 증거의 멸실 가능성을 조화롭게 보장할 수 있기를 기대해 본다.

참 고 문 헌

1. 논문

강상현, “사생활 정보를 고려한 디지털 증거처리 모델”, 고려대학교 석사학위논문, 2015.

강석한, “전자정보 압수수색에서의 참여권 보장을 위한 기술적 조치 연구”, 서울대학교 융합과학기술대학원 석사학위 논문, 2016.

강철하, “개정 형소법 제313조의 해석론”, 이화여자대학교 법학논집 제22권 제4호 통권62호, 2018. 6.

김광호, “참여권 보장을 위한 전자정보 압수수색 집행 방안에 관한 연구”, 서울대학교 융합과학기술대학원 석사학위 논문, 2016.

김영철, “디지털 본래증거 수집 방안”, 서울대학교 융합과학기술대학원 석사학위 논문, 2018.

김은광, 전상준, 한재혁, 이민욱, 이상진, “복합문서 파일에 은닉된 데이터 탐지 기법에 관한 연구”, 2015.

김희균, “이메일 계정 속 첨부파일의 증거능력”, 한국형사소송법학회 형사소송 이론과 실무 제7권 제2호, 2015.

노명선, “전자적 증거의 실효적인 압수·수색, 증거조사 방안연구”, 대검찰청 용역 보고서, 2007.

노영욱, 김동규, “Intel SGX Sealing 기법에 기반한 메모리 보호기법”, 한국정보과학학회 학술발표논문집, 2018. 6.

박민우, “전문증거 증거능력 인정요건의 변화와 이로 인한 새로운 문제에 대한 검토 : 형사소송법 제313조의 개정을 중심으로”, 형사정책연구원, 제27권 제3호, 2016.

오기두, “전자진술서의 증거능력(개정 형사소송법 제313조)”, 사법(사법발전재단), 통권 제38호, 2016.

오기두, “피고인의 공판정 진술과 전자문서의 진정성립”, 사법 24호

오미경, “디지털 증거 선별 압수·수색에 따른 문제점 해결을 위한 기술적 방안 연구”, 서울대학교 융합과학기술대학원 석사논문, 2019.

이완규, “디지털 증거의 압수수색 개념 및 증거능력 요건”, 사법발전재단, 차한성 대법관 퇴임기념 논문집「형사재판의 제문제 제7권」, 박영사, 2014.

임성훈, “압수한 디지털 데이터의 안전한 관리 방식 제안”, 서울대학교 융합과학기술대학원 석사학위 논문, 2016.

전승수, “디지털 정보에 대한 압수수색영장의 집행”, 법조 통권 670호, 2012.

진종민, “데이터베이스 은닉행위 식별을 위한 system artifacts 조사 기법에 대한 고찰”, 석사학위 논문, 서울대학교, 2016.

탁희성·이상진, “디지털 증거분석 도구에 의한 증거수집절차 및 증거능력 확보 방안”, 한국형사정책연구원, 2006.

천정희·어윤희·김재윤, “개인정보가 보호되는 동형암호기반 금융데이터분석”, 금융정보연구 제7권 제1호, 한국금융정보학회, 2018. 2.

2. 단행본, 자료집

노명선, 구희진, 김영철, 배대한, 최대건, 최우석 공저,「디지털포렌식 기술」, 미디어북, 2018.

대검찰청, 과학수사 실무 매뉴얼, 2014. 12.

미래창조과학부·NIA·빅데이터 전략센터, 빅데이터 활용을 위한 개인정보 비식별화 사례집 2014. 9.

박상준, 디지털포렌식 강의자료, 서울대학교 융합과학기술대학원 수리정보과학과, 2020. 3.

백형구 등, 주석 형사소송법(I), 한국사법행정학회, 2009.

오기두, 전자증거법, ㈜박영사, 2015.

한인검사협의회 디지털 증거 연구용역, 디지털 증거의 증거능력 및 압수수색에 관한 해외 실무례 연구, 2016.

천정희, 2019정보보호이론, 서울대학교 융합과학기술대학원 수리정보학과, 2019. 9.

3. 판례

대법원 1999. 9. 3. 선고, 99도2317판결
대법원 2000. 2. 25. 선고 99도1252판결
대법원 2001. 9. 4. 선고 2000도1743 판결
대법원 2007. 12. 13. 선고 2007도7257 판결
대법원 2008. 9. 25. 선고 2008도5347판결
대법원 2008. 11. 13. 선고 2006도2556 판결
대법원 2009. 7. 23. 선고 2009도2649 판결
대법원 2011. 5. 26. 2009모1190 결정
대법원 2013. 2. 15. 선고 2010도3504 판결
대법원 2013. 7. 26. 선고 2013도2511판결
대법원 2015. 1. 22. 선고 2014도10978 판결
대법원 2015. 4. 23. 선고, 2015도1278 판결
대법원 2015. 7. 16. 선고 2015도2625 판결
대법원 2015. 10. 15. 선고 2013모1969 결정
대법원 2017. 9. 21. 선고 2015도12400 판결
대법원 2018. 2. 8. 선고 2017도13263 판결
서울고등법원 2012. 12. 7. 선고 2012노2667 판결
서울고등법원 2014. 8. 11. 선고 2014노762 판결
서울고등법원 2015. 6. 25. 선고, 2014노2389 판결
서울고등법원 2016. 1. 19. 2015노442 판결
서울고등법원 2017. 7. 5. 선고 2017노146호 판결
부산고등법원 2020. 2. 6. 선고 2018노121 판결
서울중앙지방법원 2014. 4. 25. 선고 2013고합805판결
서울중앙지방법원 2016. 12. 23. 선고 2016고합675 판결

수원지방법원 안산지원 2012. 8. 10. 선고 2012고합191, 231(병합), 241(병합), 242(병합), 309(병합) 판결
수원지방법원 2014. 2. 17. 선고 2013고합620, 624(병합), 699(병합), 851(병합)

4. 웹문서

http://forensic.korea.ac.kr/DFWIKI/index.php/Slack
https://medium.com/magicofc/the-magic-of-intels-sgx-how-to-hello-it-sec-world-fd0295d6c33b
Intel Corporation, "Intel® Software Guard Extention,", 2015
azure.microsoft.com

5. 외국 문헌 및 판례

Eoghan Casey, Digital Evidence and Computer Crime(2nd ed.), Academic Press , 2004.
Larry E. Daniel, Lars E. Daniel, Understanding Digital Evidence from the Warrant to the Courtroom 2012.
Dalia v. United States, 441 U. S. 238, 1979.
United States v. Hunter, 13 F. Supp.2d 574(D. Vt., 1998)

Abstract

A Study on the Effective Investigation and Management of Digital Evidence

Jiyeon Lee
Master of Science in Digital Forensics
Department of Mathematical Information Science
The Graduate School of Convergence Science and Technology
Seoul National University

The precedents related to the practice of seizure and search warrants and the court's ability to prove evidence strictly apply the principle of selective seizure and search without considering the characteristics of digital evidence.

As a result, digital evidence to be secured in the beginning disappears without a trace, and investigative agencies have to spend more time and money to discover the actual truth, causing many practical problems such as the risk of leakage of investigative secrets and abuse of the right to participate.

To solve these practical problems, this study proposes a second-stage seizure and search plan that considers the characteristics of digital evidence.

In the first step, the relevant evidence generated by the user and all

the computer-generated evidence is collected in the field, confiscated in a logical imaging format, and uploaded to D-NET for analysis.
In the second step, the entire storage medium is physically imaged and then encrypted and uploaded into a black box based on the hardware-assisted trusted computing.

As above, the encrypted evidence is calculated and decrypted only in the black box, but it can be decrypted only with the approval of the prosecutor, and the calculation process is also encrypted.

In addition, since the entire physical image that has not been screened is not decoded, but only relevant evidence is decoded, the fear of infringing the secrets of the confiscated people's privacy and personal information is expected to be low.

Based on such hardware-assisted trusted computing technology, it is possible to secure necessary evidence before the disappearance of digital evidence, and display only evidence relevant to crime among them, harmoniously ensuring the illegality problem caused by the violation of the relevance standard and the possibility of loss of computer-generated evidence.

keywords : Digital Evidence, Selective acquisition of the information, Hardware-assisted Trusted Computing, Relevance, Computer generated evidence, The true establishment of digital evidence, The right to participate and observe

Student Number : 2019-29478