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

삭제 후 복구된 디지털 파일의 증거능력 인정 요건에 관한 연구

A Study on Requirements for Recognizing Evidence of Digital File Recovered after Deletion

2020년 2월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

김방글

삭제 후 복구된 디지털 파일의 증거능력 인정 요건에 관한 연구

A Study on Requirements for Recognizing Evidence of Digital File Recovered after Deletion

지도교수 이중식

이 논문을 이학석사 학위논문으로 제출함

2020년 2월

서울대학교 융합과학기술대학원

수리정보과학과 디지털포렌식학 전공

김방글

김방글의 석사 학위논문을 인준함

2020 2월

위 원 장 _____ 김 명 환 (인) _____

부위원장 _____ 이 중 식 (인) _____

위 원 _____ 이 병 영 (인) _____

요약 (국문초록)

세계에서 생성되는 정보의 약 90% 이상이 디지털 형태로 만들어지고 있다고 한다. 민사소송, 증거개시절차에서도 전자적 자료의 중요성이 커지고 있고, 수사 및 형사소송에서도 디지털 형태의 증거가 더욱 중요해 지고 있다. 그런데 디지털 증거는 기존의 물리적 증거와는 다른 특징들을 가지고 있어서 형사소송에서 디지털 증거에 대한 적법성, 압수·수색과 증거 분석의 방법 및 증거능력 인정 요건 등의 중요성이 더욱 커지고 있다.

피압수자가 디지털 파일을 작성하여 정보저장매체에 저장한 후 실수로 이를 삭제해 버리거나 정보저장매체 용량의 부족 또는 디지털 파일 보관의 필요성이 없다는 이유로 디지털 파일을 삭제하는 경우가 존재한다. 또한 최근 안티포렌식을 목적으로 디지털 파일을 삭제하는 경우가 증가하고 있고, 이를 위해 디가우징 등 전문적인 방법까지 이용되고 있다.

디지털 포렌식은 이러한 디지털 증거를 수집, 복원, 분석, 보고서 작성 및 증거 보존하는 일련의 작업을 의미하는데, 기존의 디지털 포렌식은 정보저장매체의 비할당된 영역에서 삭제된 파일을 복구하는 것보다는 할당된 영역에 존재하는 파일을 수집하고 분석하는데 초점을 맞추고 있었다. 그런데 위와 같이 디지털 파일이 다양한 이유로 삭제되는 경우가 증가하고 있어 향후 비할당된 영역에서 삭제된 파일을 복구하는 것이 중요해질 것으로 보이는데, 삭제된 파일의 복구와 이에 대한 논의는 부족하였다.

사용자가 정보저장매체에서 저장되어 있던 디지털 파일을 삭제하고 나면, 사용자의 입장에서는 삭제 처리된 디지털 파일이 보이지 않아

완전히 사라진 것처럼 보인다. 그런데 정말 삭제 처리된 디지털 파일은 정보저장매체에서 영구 삭제, 완전히 사라진 것일까. 정답은 그렇지 않다. 삭제된 디지털 파일의 정보는 정보저장매체의 비할당된 영역에 저장되어 있는 경우가 많고, 복구가 가능하다. 물론, 안티포렌식 기술의 발달과 HDD 등 새로운 정보저장매체의 등장 등으로 디지털 파일의 복구가 어렵거나 불가능한 경우도 증가하고 있지만, 이로 인하여 수사기관이 삭제된 파일을 발견해 복구해 내는 것은 더 중요해지고 있고, 삭제된 디지털 파일의 복구 기법도 역설적으로 활발히 연구되어 발달하고 있다.

그렇다면 수사기관에서 삭제된 디지털 파일을 복구하여 그 복구된 디지털 파일을 형사소송에서 증거로 사용되는 경우, 증거능력을 어떻게 인정받을 것인지 여부가 문제된다.

기존 실무와 판례에서는 할당된 영역에 존재하는 파일을 압수하여 이를 증거로 사용하는 경우가 대부분이었기 때문에 증거능력에 대한 논의는 정보저장매체에 저장된 디지털 파일과의 동일성, 무결성을 입증하는데 집중되어 왔다. 또한, 디지털 증거의 대량성 특징으로 인하여 관련성이 중요시됨에 따라 '원칙적 선별 압수, 예외적 매체 압수'가 강조되었고, 개별 디지털 파일을 단위로 하여 범죄사실과 관련성이 있는 개별적 디지털 파일만을 선별하여 압수하면서 동일성, 무결성의 입증도 정보저장매체 전체에서 개별 디지털 파일로 확장되어 왔다.

디지털 파일이 삭제 후 복구된 경우에는, 복구 이후의 시점부터는 기존과 동일하게 압수된 복구 파일이 복구 시점 이후에 변경되지 않고 동일하다는 것에 대한 입증은 가능하다. 그런데 피압수자의 입장에서 삭제되었던 디지털 파일은 실제 정보저장매체의 비할당영역에

존재했던 것이지만 전문적인 디지털 복구 도구를 이용하지 않고는 접근할 수 없고, 삭제되기 전 디지털 파일을 존재하지 않으며, 삭제되기 전 디지털 파일의 해시값도 알 수 없기 때문에 삭제되기 전 디지털 파일을 원본으로 본다면 기존과 같이 단순히 해시값의 비교로 증거능력을 인정할 수 없다. 이에 삭제 후 복구된 디지털 파일의 증거능력의 인정 요건, 즉 무엇을 원본으로 볼 것인지, 원본과의 동일성, 무결성을 입증하는 방법 및 그 입증 정도 등이 문제된다.

디지털 증거가 무엇인지 살펴보면, 디지털 증거는 '디지털 형태로 저장되거나 전송되는 정보'를 의미하므로, 한컴오피스, Microsoft Word, Excel, Powerpoint 등 각종 소프트웨어 프로그램을 통해 보고 읽을 수 있는 개별 디지털 파일이 아니라 정보저장매체에 저장된 데이터, 정보 그 자체로 보아야 한다. 삭제 후 복구된 디지털 파일의 경우, 삭제되기 전이 아닌 삭제되고 난 이후, 압수 시점에서의 정보저장매체에 저장된 디지털 형태의 정보를 원본으로 보아야 한다.

또한, 증거능력의 인정 요건으로 원본과의 동일성, 무결성 및 신뢰성이 있다. 수사 실무적으로 디지털 증거 중 삭제 후 복구된 디지털 파일을 압수하는 방법으로 정보저장매체에서 삭제된 디지털 파일들을 복구한 후 선별하여 관련성이 있는 복구된 디지털 파일들만을 이미징하여 압수하는 방법('복구 후 선별 압수 방법'이라 한다)과 정보저장매체 자체를 이미징한 후 삭제된 디지털 파일들을 복구한 이후에 선별하여 압수하는 방법('전체 이미징 후 복구 및 선별 압수 방법'이라 한다)이 있다. 각각의 경우에 따라 해시값 비교의 대상을 무엇으로 볼 것인지, 재현가능의 입증 정도도 달라진다.

먼저 복구 후 선별 압수 방법에서는 삭제 후 복구된 디지털 파일들과 다른 파일들을 이미징하여 복사한 것이기 때문에 정보저장매체 전체가

아닌 복구된 디지털 파일들을 포함한 압수된 디지털 파일들과 그것을 이미지한 파일의 해시값을 비교하는 방법으로 동일성, 무결성을 증명할 수 밖에 없다. 이미징 이전의 단계, 즉 복구 과정이 문제된다면 재현가능성을 입증하기 위하여 저장저장매체나 그 정보저장매체 전체에 대한 이미지 파일이 필요한데, 정보저장매체나 그 정보저장매체 전체에 대한 이미지 파일 모두 없는 상황에서 복구가 제대로 이루어졌는지 여부를 증명하기 곤란한 상황이 발생한다. 따라서 재현가능성에 대한 입증의 정도를 완화하여 디지털 증거 분석 도구의 신뢰성, 디지털 포렌식 수사관의 전문성 등으로 이를 보완하는 것이 필요하다.

다음으로, 전체 이미징 후 복구 및 선별 압수 방법에서는 정보저장매체 자체를 이미징하였기 때문에 정보저장매체에 저장되어 있던 전체 정보를 원본으로 보고, 정보저장매체 전체의 해시값과 이미지 파일의 해시값을 비교한 후, 이미지 파일에서 삭제된 디지털 파일이 복구되었고, 그 복구된 파일의 사본이라는 것을 증명하여야 한다. 이 경우, 재현가능성을 입증하기 위하여 원본 정보저장매체나 이미지 파일이 필요하다. 보통 원본 정보저장매체는 피압수자에게 반환하고 이미지 파일은 복구 및 선별 압수 후 삭제하나 이러한 경우 재현가능성 입증을 위해 이미지 파일을 보관하는 것이 필요하고, 이미지 파일의 보관 방법 등을 논의할 필요성이 있다.

현재까지 삭제 후 복구된 파일의 증거능력 인정 요건에 대해 명시적으로 판결한 판례가 존재하지 않는다. 판례는 디지털 증거의 증거능력 인정 요건에 대하여 종합판단설의 입장을 취하고 있으므로, 비할당영역에 압수할 데이터가 존재하였고, 전문성을 갖춘 디지털포렌식 수사관이 신뢰할 수 있는 복구 도구를 이용하여

복구하였으며, 이를 재현할 수 있음을 종합적으로 증명함으로써 동일성, 무결성 및 신뢰성을 인정받을 수 있다고 생각한다. 구체적으로, 디지털 증거분석 도구의 신뢰성, 디지털 포렌식 수사관의 법정 증언 및 재현가능성 검증, 저장매체에 저장되어 있는 디지털 정보 자체의 확인, 부수데이터의 분석, 제3의 전문기관 등에 의한 감정 등 다양한 방법으로 이를 효과적으로 입증할 수 있다.

앞으로도 정보저장매체 원본이 존재하지 않거나 HDD 등 저장매체의 특성상 해시값이 변경되는 상황이 존재할 것이다. 과학기술은 계속적으로 발전하면서 변화하고 있고, 디지털 포렌식 및 이에 대응하는 안티포렌식도 계속적으로 발전하면서 변화하고 있다. 따라서 디지털 증거의 특징을 고려하여 다양한 방법으로 증거능력의 인정 요건인 진정성, 무결성 및 신뢰성을 입증할 수 있도록 해야 하는 방안이 계속적으로 연구되어야 할 것이라고 생각한다.

주요어 : 디지털포렌식, 디지털 증거, 디지털 파일, 삭제, 복구, 증거능력, 동일성, 무결성, 신뢰성, 전문성, 해시값, 이미지 파일

학 번 : 2018-49612

<목차>

I. 서론 ····· 1

II. 디지털 증거와 증거능력 인정 요건 ····· 4

제1장 디지털 증거의 의의 ····· 4

제2장 디지털 증거의 특징 ····· 5

제1절 매체독립성 ····· 5
제2절 변경가능성(취약성) ····· 6
제3절 비가시성 및 비가독성 ····· 7
제4절 전문성 ····· 7
제5절 복구가능성 ····· 8
제6절 부수데이터의 존재(정보의 풍부성) ····· 9

제3장 디지털 증거의 증거능력 ····· 10

제1절 일반 ····· 10
제2절 동일성, 무결성, 신뢰성 ····· 11
제3절 판례의 태도 ····· 12
1. 일심회 사건 ····· 13
2. 왕재산 사건 ····· 16
3. 이석기 사건 ····· 18
4. 원세훈 사건 ····· 19
5. 조세범처벌법위반 사건 ····· 21
6. 소결 ····· 23

제4절 미국 판례의 태도 ····· 24
1. 진정성 ····· 24
2. 최량증거법칙 ····· 26
제5절 실무의 태도 ····· 28

Ⅲ. 디지털 파일의 삭제와 삭제 파일의 복구 ····· 33

제1장 파일시스템과 데이터의 저장 구조 ····· 33

제1절 파일시스템 ····· 33
1. FAT 파일시스템 ····· 33
2. NTFS 파일시스템 ····· 34
제2절 하드 드라이브의 데이터 저장 구조 ····· 34
1. 데이터 저장에 이용되는 수학적 개념 ····· 35
2. 할당영역과 비할당영역 ····· 36

제2장 디지털 파일의 삭제 및 복구방법 ····· 38

제1절 디지털 파일의 삭제 ····· 38
제2절 삭제된 디지털 파일의 복구 원리 ····· 38
제3절 삭제된 디지털 파일의 복구 방법 ····· 39
1. 포렌식 소프트 웨어를 이용한 파일 복구 ····· 39
2. 메타 정보를 이용한 파일 복구 ····· 40
3. 데이터 카빙 복구 ····· 41
제4절 실무상 삭제 파일 복구 및 압수 절차 ····· 41
1. 디스크 이미징 ····· 41
2. CFT, Encase 등 프로그램을 통한 복구 및 선별 파일 등록 ····· 43
3. 이미지 파일 보관 또는 삭제 ····· 46

Ⅳ. 삭제 후 복구된 디지털 파일의 증거능력 인정 요건 ····· 49

제1장 기존 실무 및 판례의 태도와 문제점 ····· 49

제2장 미국 판례의 태도 ····· 50

제1절 복구, 복제절차의 진정성 문제 ····· 50

제2절 신뢰성의 문제 ····· 51

1. 포렌식 도구의 유효성 ····· 51

2. 디지털 증거 분석관의 전문성 검증 ····· 52

제3절 원본성의 문제 ····· 53

제3장 삭제 후 복구된 디지털 파일의 원본 ····· 54

제4장 증거능력 입증 방법 ····· 55

제1절 디지털 증거 분석 도구의 신뢰성 ····· 56

1. 국내 기준 ····· 56

2. NIST의 CFTT ····· 56

3. 국내 실험 ····· 58

4. 대검찰청의 CFT ····· 59

5. Encase 등 프로그램 ····· 61

제2절 디지털 포렌식 수사관의 법정 증언 ····· 61

제3절 재현가능성 ····· 63

제4절 저장매체에 저장되어 있는 디지털 정보 자체의 확인 ····· 65

제5절 부수데이터의 분석 ····· 66

제6절 제3의 전문기관 등에 의한 감정 ····· 66

Ⅴ. 결론 ····· 68

참고문헌 ····· 72

<그림 차례>

그림 1. 2019. 5. 20.부터 사용된 검찰 '현장조사확인서' 서식 ····· 31
그림 2. NTFS 파일 시스템에서의 파일 저장 개념도 ····· 35
그림 3. 2015. 8.부터 사용된 압수·수색·검증영장 별지 ····· 45

<표 차례>

표 1. 삭제 파일 복구 기능의 필수적인 요구사항 ····· 58
표 2. Selected Test Cases ····· 60

I. 서론

세계에서 생성되는 정보의 약 90% 이상이 디지털 형태로 만들어지고 있다고 한다.[1] 민사소송, 증거개시절차에서도 전자적 자료의 중요성이 커지고 있고, 수사 및 형사소송에서도 디지털 형태의 증거가 더욱 중요해 지고 있다. 그런데 디지털 증거는 기존의 물리적 증거와는 다른 특징들을 가지고 있어서 형사소송에서 디지털 증거에 대한 적법성, 압수·수색과 증거 분석의 방법 및 증거능력 인정 요건 등의 중요성이 더욱 커지고 있다.

피압수자가 디지털 파일을 작성하여 정보저장매체에 저장한 후 실수로 이를 삭제해 버리거나 정보저장매체 용량의 부족 또는 디지털 파일 보관의 필요성이 없다는 이유로 디지털 파일을 삭제하는 경우가 존재한다. 또한 최근 안티포렌식을 목적으로 디지털 파일을 삭제하는 경우가 증가하고 있고, 이를 위해 디가우징 등 전문적인 방법까지 이용되고 있다. 이는 디지털 증거를 삭제했을 시 수사기관에 적발되지 않을 가능성이 있고, 만약 디지털 증거를 삭제한 것이 적발되더라도 증거인멸죄로 인한 형사 처벌이 수사기관에 핵심적인 증거가 압수되어 유죄로 인정되는 경우의 형사 처벌 및 그로 인한 민사상의 배상보다 더 나을 수 있다는 계산에도 기인한 것으로 보인다.

디지털 포렌식은 이러한 디지털 증거를 수집, 복원, 분석, 보고서 작성 및 증거 보존하는 일련의 작업을 의미하는데, 기존의 디지털 포렌식은 정보저장매체의 비할당된 영역에서 삭제된 파일을 복구하는 것보다는 할당된 영역에 존재하는 파일을 수집하고 분석하는데 초점을

1) Peter Lyman and Hal R.Varian, U.C. Berkely, “How Much Storage is Enough?”, ACM Queue vol.1, no.4 June 2003.(양근원, “증거법상의 새로운 화두 : 디지털 증거와 디지털 포렌식”, 경찰법연구 제5권 제1호, 2007, 2면에서 재인용)

맞추고 있었다. 그런데 위와 같이 디지털 파일이 다양한 이유로 삭제되는 경우가 증가하고 있어 향후 비할당된 영역에서 삭제된 파일을 복구하는 것이 중요해질 것으로 보이는데, 삭제된 파일의 복구와 이에 대한 논의는 부족하였다.

사용자가 정보저장매체에 저장되어 있던 디지털 파일을 삭제하고 나면, 사용자의 입장에서는 삭제 처리된 디지털 파일이 보이지 않아 완전히 사라진 것처럼 보인다. 그런데 정말 삭제 처리된 디지털 파일은 정보저장매체에서 영구 삭제, 완전히 사라진 것일까. 정답은 그렇지 않다. 삭제된 디지털 파일의 정보는 정보저장매체의 비할당된 영역에 저장되어 있는 경우가 많고, 복구가 가능하다. 물론, 안티포렌식 기술의 발달과 HDD 등 새로운 정보저장매체의 등장 등으로 디지털 파일의 복구가 어렵거나 불가능한 경우도 증가하고 있지만, 이로 인하여 수사기관이 삭제된 파일을 발견해 복구해 내는 것은 더 중요해지고 있고, 삭제된 디지털 파일의 복구 기법도 역설적으로 활발히 연구되고 있다.

그렇다면 수사기관에서 삭제된 디지털 파일을 복구하여 그 복구된 디지털 파일을 형사소송에서 증거로 사용되는 경우, 증거능력을 어떻게 인정받을 것인지 여부가 문제된다.

기존 실무와 판례에서는 할당된 영역에 존재하는 파일을 압수하여 이를 증거로 사용하는 경우가 대부분이었기 때문에 증거능력에 대한 논의는 저장매체에 저장되어 있던 디지털 파일과의 동일성, 무결성을 입증하는데 집중되어 왔다. 또한, 디지털 증거의 대량성 특징으로 인하여 관련성이 중요시됨에 따라 '원칙적 선별 압수, 예외적 매체 압수'가 강조되었고, 개별 디지털 파일을 단위로 하여 범죄사실과 관련성이 있는 개별적인 디지털 파일만을 선별하여 압수하면서 동일성,

무결성의 입증도 정보저장매체 전체에서 개별 디지털 파일로 확장되어 왔다. 구체적으로, 디지털 파일의 증거능력은 정보저장매체 전체의 해시값 비교하는 방법을 넘어 정보저장매체에 저장되어 있고 한컴오피스, Microsoft Word, Excel, Powerpoint 등 각종 소프트웨어 프로그램을 통해 보고 읽을 수 있는 개별 디지털 파일을 원본으로 보아 위 개별 디지털 파일과 압수한 디지털 파일의 해시값을 비교하는 방법으로 동일성, 무결성을 증명하는 방법으로 확장되고 있다.

디지털 파일이 삭제 후 복구된 경우에는, 복구 이후의 시점부터는 기존과 동일하게 압수된 복구 파일이 복구 시점 이후에 변경되지 않고 동일하다는 것에 대한 입증은 가능하다. 그런데 피압수자의 입장에서 삭제되었던 디지털 파일은 실제 정보저장매체의 비할당영역에 존재했던 것이지만 전문적인 디지털 복구 도구를 이용하지 않고는 접근할 수 없고, 삭제되기 전의 디지털 파일은 존재하지 않으며, 삭제되기 전 디지털 파일의 해시값도 알 수 없기 때문에 삭제되기 전 디지털 파일을 원본으로 본다면 기존과 같이 단순히 해시값의 비교로 증거능력을 인정할 수 없다. 이에 삭제 후 복구된 디지털 파일의 증거능력의 인정 요건, 즉 무엇을 원본으로 볼 것인지, 원본과의 동일성, 무결성을 입증하는 방법 및 그 입증 정도 등이 문제되고, 아래에서 이에 대해서 논의해 보겠다.

II. 디지털 증거와 증거능력 인정 요건

제1장 디지털 증거의 의의

디지털 포렌식은 '컴퓨터용 디스크, 그 밖에 이와 비슷한 정보저장매체로부터 디지털 증거를 수집·보존·분석·현출하는데 적용되는 과학기술 및 절차'[2]를 의미하여, 디지털 포렌식의 대상은 디지털 증거(Digital Evidence)이다. 디지털 증거에 관한 국제 조직 IOCE(International Organization on Computer Evidence)[3]에서는 '2진수 형태로 저장 혹은 전송되는 것으로서 법정에서 신뢰할 수 있는 정보'라 정의하고, 전자적 증거에 관한 과학실무 그룹 SWGDE(Sciencetific Working Group on Digital Evidence)[4]에서는 '디지털 형태로 저장되거나 전송되는 증거가치 있는 정보'라고 정의하며, 대검찰청은 '범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보'라고 정의하고 있다.[5] 디지털 증거에 대한 어떠한 정의에서든 '디지털 형태'와 '정보'를 요건으로

---

2) 디지털 증거의 수집 분석 및 관리규정(대검찰청 예규 제991호)
제3조(정의) 이 규정에서 사용되는 용어의 뜻은 다음과 같다.
2. "디지털포렌식"이란 디지털 증거를 수집·보존·분석·현출하는데 적용되는 과학기술 및 절차를 말한다.

3) 미국, 호주, 홍콩, 영국 등 각국의 실무자들을 중심으로 만들어진 디지털증거에 관한 국제기구

4) 미국 법무부의 마약수사청(Drug Enforcement Administration : DEA), 연방수사국(Federal Bureau of investigation : FBI), 국세청 범죄수사단(Internal Revenue Service Criminal Investigation Department : IRS-CID), 관세청(US Customs), 항공우주국(National Aeronautics and Space Administration : NASA) 등 연방기관의 증거분석 연구소를 중심으로 구성된 디지털증거에 관한 과학실무그룹

5) 디지털 증거의 수집 분석 및 관리규정(대검찰청 예규 제991호)
제3조(정의) 이 규정에서 사용되는 용어의 뜻은 다음과 같다.
1. "디지털 증거"란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다.

하고 있다.

디지털 증거란 전자적으로 기록되거나 그 내용이 현출되고 있는 증거를 통틀어 말한다. 일반적으로 컴퓨터의 입력장치, 연산·제어·기억장치, 출력장치 등 컴퓨터의 기본구조에 관련된 증거방법, 컴퓨터 통신에 관련된 증거방법, 디지털 방식에 의한 전자적 기억매체에 수록된 전자정보나 그 전자기억매체 내지 그 전자정보의 출력물 등을 총칭하고, 그 전자정보 전부나 일부를 복제한 자기디스크, 그 데이터를 새로이 가공처리한 데이터 내지 그와 같이 가공처리된 데이터를 저장한 자기디스크, 컴퓨터 모니터에 떠 있는 문자나 화상, 동화상, 컴퓨터 스피커에 출력되는 소리 또는 음악, 전선이나 광섬유를 통해 전자적 방식으로 이동되거나 무선방식으로 이동하는 컴퓨터 통신 데이터나 음성, 데이터베이스, 전자우편, 전자게시판에 있는 데이터 등을 일컫는 용어[6]이다.

제2장 디지털 증거의 특징

디지털 증거는 매체독립성, 변경가능성(취약성), 비가시성·비가독성, 전문성, 복원가능성, 부수데이터의 존재(정보의 풍부성), 대량성, 네트워크관련성 등 여러 가지 특징을 가지고 있다. 여기서는 삭제 후 복구된 전자파일의 증거능력과 관련된 특징들에 대해서 살펴보도록 하겠다.

제1절 매체독립성

디지털 증거는 '유체물'이 아니고 각종 디지털 저장매체에 저장되어

6) 오기두, "전자증거법", 박영사, 2015, 5면

있거나 네트워크를 통하여 0과 1의 2진수 형태로 전송 중인 정보 그 자체를 의미한다. 전자적 증거는 매체와 독립된 정보의 내용이 증거로 되는 특성을 지니고 있고, 어떠한 정보든 내용이 같다면 어느 매체에 저장되어 있든지 동일한 가치를 가진다. 즉, 컴퓨터 하드디스크에 저장되어 있는 특정한 한글 파일은 이를 USB 저장매체나 다른 하드디스크에 복사를 하더라도 동일한 정보와 해시값을 가지고 있어 동일한 가치를 가지고,[7] 원본과 사본의 구별 또한 불가능하다.

제2절 변경가능성(취약성)

물리적 증거의 경우 증거물을 조작하면 조작 흔적이 남게 되므로 조작이 비교적 쉽게 판별할 수 있으나, 디지털 증거는 간단한 조작이나 단순한 명령어 입력만으로도 디지털 자료를 삭제하거나 변경시킬 수 있고, 자료의 일부만을 쉽게 조작할 수 있다.[8] 하나의 명령만으로 하드디스크 전체를 포맷하거나 특정 파일을 삭제할 수도 있다. 즉, 디지털 증거는 위·변조 및 삭제가 용이하다는 변경가능성, 취약성의 특징을 가지고 있다.

따라서 수사기관에 의한 증거조작 가능성도 배제할 수 없으므로 수사기관이 디지털 증거를 수집하는 경우에 수집 이후부터는 디지털 증거가 변조되지 않았다는 것을 입증할 수 있도록 무결성을 확보하는 절차와 기술이 필요로 되고,[9] 여기에서 디지털 증거에 대한 무결성의 문제가 대두된다.[10]

---

7) 노명선·구희진·김영철·배대한·최대건·최우석, “디지털포렌식 이론”, 미디어북, 2018, 51면

8) 권양섭, “디지털증거수집에 관한 연구”, 군산대학교 박사학위논문, 2009, 12면

9) 탁희성·이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보 방안, 형사정책연구원, 2006, 36면

10) 노명선·구희진·김영철·배대한·최대건·최우석, “디지털포렌식 이론”, 미디어북, 2018, 53면

제3절 비가시성 및 비가독성

디지털 저장매체에 저장된 디지털 증거 그 자체는 이진수 형태의 전자적인 신호로 존재하는 특성상 사람의 지각으로 바로 인식할 수 없고, 일정한 변환절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되었을 때 가시성과 가독성을 가지게 된다. 예를 들어 종이 문서가 증거인 경우 이를 제시하는 방법으로 곧바로 그 정보의 내용을 인지할 수 있는데 반하여, 디지털 증거의 경우 컴퓨터 하드디스크 등 정보저장매체 자체를 제시하는 것만으로는 그 정보의 내용을 인지할 수 없고, 정보저장매체에 저장된 내용을 한컴오피스, Microsoft Word, Excel, Powerpoint와 같은 소프트웨어 프로그램이나 각종 분석 프로그램 등을 통하여 모니터 상에 나타나게 하거나 인쇄를 통하여 제시될 때 비로소 가시성·가독성을 가지게 된다.[11)]

따라서 디지털 증거는 가시성·가독성이 없는 매체독립적인 전자정보이므로 법정에서 증거로 사용하기 위해서는 가시성·가독성이 있는 형태로 변환하여 제출하여야 한다.

제4절 전문성

디지털 방식으로 자료를 저장하고 이를 출력하는 데는 많은 컴퓨터 기술과 프로그램이 사용된다. 따라서 저장되어 있는 자료가 어떤 소프트웨어를 사용하여 저장되었는지 여부가 정확하게 규명하지 않으면 자료에 접근하기조차 어려운 문제가 발생한다. 또한 접근하여 수집된 자료라 할지라도 이를 가독성·가시성 있는 자료로 제시하고 그 내용을 해석하는 데는 해당 분야에 대한 전문적 지식 없이는 불가능한

11) 노명선·구희진·김영철·배대한·최대건·최우석, “디지털포렌식 이론”, 미디어북, 2018, 52면

경우가 많고, 법정에 제시된 최종 산출물이 원본 증거에 대한 정확한 해석인지 검증하는 것도 필요하다.[12)]

따라서 디지털 방식으로 자료를 저장하고 이를 출력하는데 많은 컴퓨터 기술과 프로그램이 되고, 디지털 증거의 수집, 복구 및 분석에도 전문적인 기술이 사용되므로, 디지털 증거의 압수, 복구 및 분석 등에 있어 포렌식 전문가의 도움이 필수적이다. 여기에서 전자적 증거에 대한 신뢰성 문제, 특히, 디지털 수사관의 증언능력과 사용된 디지털포렌식 도구의 신뢰성이 문제된다.[13)]

제5절 복구가능성

종래의 유체물 형태의 자료는 한 번 훼손되거나 소멸되는 경우 이를 복원하는 것이 매우 어렵거나 불가능한 경우가 대부분이다. 하지만 디지털 정보의 경우는 유체물 형태와 달리 데이터가 삭제되더라도 복구될 수 있는 가능성이 높다.

사용자가 'Delete 명령어' 또는 '윈도우의 휴지통 비우기'를 통하여 디지털 파일을 삭제하여도 컴퓨터 운영체제는 실제 물리 디스크 영역에서 곧바로 그 디지털 파일의 데이터를 삭제하지 않는다. 이는 컴퓨터 작동의 효율성을 위한 기술로서, 컴퓨터 파일관리시스템은 사용자가 삭제되었다고 믿는 데이터가 저장된 영역에 다시 데이터를 기록할 수 있는 영역이라고 표시만 하고, 새로운 데이터가 덮어씌워지는 순간까지 어떠한 작업도 하지 않는다. 달리 말하면 컴퓨터 파일시스템이 기존 데이터가 저장되어 있던 영역에 다른 데이터를 다시 기록하지 않는 한 해당 영역에 있는 데이터는 실제로 삭제되지 않고

12) 양근원, "형사절차상 디지털 증거의 수집과 증거능력에 관한 연구", 박사학위논문, 경희대학교, 2006, 139면

13) 노명선·구희진·김영철·배대한·최대건·최우석, "디지털포렌식 이론", 미디어북, 2018, 54면

정보저장매체에 남아있게 된다. 그 결과 디지털포렌식 기법을 활용하여 해당 영역에 있는 데이터를 복구할 수 있다. 물론 삭제된 데이터의 복구가능성은 사용자의 컴퓨터 사용 습관, 정보저장매체의 종류 등에 따라 달라지지만 유체물 형태의 자료에 비하여 복구가능성이 높고, 복구시 삭제 전과 동일한 내용을 복구할 수 있다는 것을 감안한다면 복구가능성은 디지털 증거의 중요한 특성이 된다.

제6절 부수데이터의 존재(정보의 풍부성)[14]

디지털 증거는 해당 응용 프로그램의 운용 목적에 따라 다양한 데이터를 보관하게 되고, 운영체제는 파일 등의 효율적인 관리를 위하여 일정한 규칙에 따라 데이터를 관리(파일시스템)하게 된다. 따라서 유체물 형태의 자료는 작성자, 작성일시, 수정일시 등이 직접적으로 기재되어 있지 않다면 자료에 기재된 내용의 정보만을 가지고 있는 반면에, 디지털 증거는 소프트웨어 프로그램을 통해 모니터 상에 현출되는 내용 이외에도 증거로 사용될 수 있는 주요한 부수데이터들을 포함하고 있다.

각 소프트웨어 프로그램은 데이터를 저장하기 위해 고유한 저장 형식을 사용하는데, 크게 헤더(header), 메타데이터(metadata), 데이터(body data)로 구성된다. 헤더에는 해당 파일의 유형을 나타내는 시그니처(signiture)가 포함되고, 전체 파일의 크기, 메타데이터의 시작위치 등의 부가 정보가 저장된다. 메타데이터는 사용자가 입력한 데이터를 설명하거나 관리하기 위한 데이터로 사용자가 입력하는 것이 아니라 응용 프로그램에서 자동적으로 생성된다. 그래서 메타데이터를 데이터에 관한 데이터(data about data)라고 말한다. 그리고

14) 이상진, “디지털 포렌식 개론”, 이룬출판사, 2015

데이터(body data)는 파일의 내용을 구성하는 실제 컨텐츠가 저장되는 영역으로, 디지털 파일의 내용이 증거로 사용되는 경우 위 데이터 영역에 저장되어 있는 컨텐츠가 가시성·가독성이 있는 형태로 현출되는 것이다.

디지털 파일의 삭제는 데이터(body data)를 삭제하는 것이 아니라 메타데이터(metadata)만을 일부 수정하는 것이기 때문에 나머지 파일 정보 및 데이터(body data) 영역은 다른 파일에 의해 '덮어쓰기'가 되기 전까지 그대로 남아있게 되고, 남아있는 위 나머지 파일 정보 및 데이터 영역으로 인해 복구가 가능하게 된다.

제3장 디지털 증거의 증거능력

제1절 일반

디지털 증거는 매체독립성, 변조의 용이성 등 다양한 특성을 가졌고, 이러한 특성 때문에 매체와 상관없이 독립하여 매체를 옮겨 다닐 수 있으며, 간단한 조작 또는 명령어만으로 내용이 변경될 수 있다. 따라서 디지털 증거가 증거로서 기능하기 위해서는 디지털 정보가 수사기관에 의해 압수될 때 그 내용이 압수 전과 동일하고 변경되지 않았다는 것 등 증거가치로서의 자격이 보증되어야 한다.

이와 관련하여 기록 관리를 위한 국제표준 ISO 15489는 디지털 증거가 증거로서 가치를 가지기 위한 요건으로 '진정성', '신뢰성', '무결성' 등을 들고 있다.[15)]

15) 강승훈, "행정조사를 위한 디지털증거 수집의 적법성 강화 방안", 석사학위논문, 서울대학교, 2019, 11면

제2절 동일성, 무결성, 신뢰성

디지털 증거의 증거능력 인정을 위한 요건 중 핵심은 증거의 원본과의 동일성, 무결성 및 신뢰성이다.

'동일성'이란 디지털 증거의 원본이 아닌 사본 또는 출력물이 증거로 제출된 경우 그 원본과 사본, 출력물이 서로 일치해야 한다는 것을 의미한다. 형사소송법상 디지털 증거를 압수할 때에는 범죄 혐의와 관련된 부분을 출력 또는 복제하는 방식으로 압수하는 것이 원칙[16]이므로, 디지털 증거의 원본과의 동일성이 문제된다.

'무결성'이란 디지털 증거가 원본으로부터 수집되어 운반·보관·분석되는 과정에서 수정·변경·손상 등이 없음을 보증하는 것을 의미한다. 디지털 파일은 복제(이미징) 후 그 증거를 분석하는 과정에서 디지털 기기에 기록된 사실들을 삭제하거나 그 사실이 일어난 날짜와 시각, 내용 등을 변경할 수 있으므로, 최초 수집된 이후부터 법정에 제출되기까지 수정, 변경이나 훼손이 없었다는 점에 대한 입증이 필요하다.

'신뢰성'이란 디지털포렌식 수사관과 디지털 증거의 수집·분석 도구의 전문성을 의미한다.

디지털 정보가 수사기관에 의해 압수될 때 그 내용이 압수 전과 동일하고 변경되지 않았다는 것 등 증거가치로서의 자격이 보증되어야 하는데, 디지털 파일은 조작이 용이하므로 원본과의 동일성 판단은

---

16) 형사소송법 제106조(압수)
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.

해시값을 비교하여 파일 위·변조 여부를 확인하는 것이 기본적인 방법으로 이용되고 있다. 암호학적 해시함수(Hash function)는 디지털 증거의 무결성 유지와 원본 동일성 유지(위·변조 검사)의 중요한 기술적 요소로 활용되고 있으며, 현재 가장 비용 효율적이고 안전한 방법으로 인식되어 활용되고 있다. 해시함수의 연산결과인 해시값은 인간의 DNA와 같이 디지털 데이터의 정보에 조금이라도 차이가 있으면 다른 해시값을 가지게 된다.

수사기관은 1990년대 중후반부터 사이버수사와 디지털 포렌식 분야에서 해시함수를 사용하기 시작하였고, 2007년 대법원에서 처음으로 디지털 증거의 증거능력 인정의 근거 중 하나로 '디지털 저장매체 원본의 해시값과 이미징 작업을 통해 생성된 파일의 해시값이 동일하다'는 것을 설시하면서, 해시값이 증거법적 측면에서 중요한 증거능력 인정 수단이 되었다. 이어 왕재산 사건과 이석기 사건 등에서 해시값을 동일성 입증 수단의 원칙적 방법으로 인정함에 따라 현재까지 압수·수색 및 재판과정에서 해시값 비교가 많이 활용되고 있다. 한편 2011년 형사소송법에서 디지털 증거에 대한 출력·복제를 압수원칙으로 규정(제106조 제3항)하면서 정보저장매체 자체를 압수하는 것이 아니라 복제하여 압수하는 사례가 증가하여 해시함수는 동일성 입증의 주요한 기술로 자리를 잡아가고 있다.[17]

그러나 해시함수만으로 디지털 증거의 증거능력의 인정 문제를 해결할 수 없어 디지털 증거의 증거능력 인정 여부에 대한 논란은 끊이지 않고 있다.

제3절 판례의 태도

17) 김기범, "해시함수의 형사법적 고찰", 형사정책연구, 29(2), 한국형사정책연구원, 2018, 200면.

1. 일심회 사건

일심회 사건에서 제1심은 디지털 저장매체로부터 수사기관이 출력하여 제출한 문건들의 증거능력에 대하여, 변호인들은 검찰이 위 저장매체의 데이터가 본래 존재하였던 상태와 전혀 다름이 없이 수집, 제출되었다는 사실과 위 디지털 증거의 분석처리과정에 대한 신뢰성에 대하여 그 입증책임을 다하지 못하였고, 이 법원의 검증절차에 참여하여 이를 주도적으로 진행한 증인의 디지털 증거 분석능력과 그 증언은 신뢰할 수 없으므로, 위 문건들은 독립적인 증거로 사용할 수 없다고 주장하며 동일성, 무결성, 신뢰성을 문제삼았으나, 디지털 저장매체에 대한 압수과정부터 법원의 검증절차에 이르기까지의 제반사정에 비추어, 보관과정의 신뢰성, 데이터의 동일성, 처리과정의 정확성 등의 요건이 인정된다고 보아 컴퓨터기록 자체로서의 증거능력을 인정하였다.

구체적으로 살펴보면, “컴퓨터 디스켓 등 디지털 저장매체에 들어 있는 컴퓨터기록이 증거로 사용되기 위해서는, 디지털 저장매체에 들어 있는 무체정보인 컴퓨터기록 그 자체로서는 가시성과 가독성이 없으므로 법원에서의 검증절차를 통해 디지털 저장매체에 수록된 컴퓨터기록의 내용이 확인되어야 하고, 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는, 법원에서의 검증절차를 통해 디지털 저장매체에 수록된 컴퓨터기록의 내용이 출력된 문건에 기재된 것과 동일하다는 것이 입증되어야 한다. 한편, 컴퓨터기록의 증거능력이 인정되기 위해서는, 컴퓨터기록이 입력된 후 법원의 검증절차에 이르기까지 변경되지 않았음이 인정되어야 할 것이고, 이를 위해서는 컴퓨터기록의 보관상황에 대한 신뢰성이 담보되어야 한다. 그리고

디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 보존된 데이터를 '하드카피' 또는 '이미징'한 매체가 법원의 검증에 사용될 경우에는 디지털 저장매체 원본과 '하드카피' 또는 '이미징'한 매체 사이의 데이터의 동일성이 증명되어야 한다. 또한 검증과정에 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력, 처리, 출력의 각 단계에서의 컴퓨터 처리과정의 정확성, 조작자의 전문적 기술능력 등이 갖추어질 때, 컴퓨터기록은 디지털 저장매체에 대한 법원의 검증절차를 통해 증거능력이 인정될 수 있다."고 하면서 "압수물인 디지털 저장매체 원본에 액세스할 경우 원본에 변화가 일어나게 되므로, 압수물인 디지털 저장매체 원본에 쓰기방지장치를 사용하고 이미징 장비를 통해 '이미징' 작업을 하였고, 그렇게 작성된 이미지가 법원에서의 검증절차의 대상이 된 사실을 인정할 수 있고, 또한 위 이미지 파일은 전세계적으로 많이 사용되고 있는 엔케이스 프로그램을 이용하여 작성되었는데, 디지털 저장매체 원본의 해쉬값과 이미징 작업을 통해 생성된 이미지 파일의 해쉬값은 동일한 점이 인정된다. 살피건대, 압수수색영장에 의해 피고인들의 주거지 또는 사무실 등에서 압수된 각 디지털 저장매체 원본들은 피고인들의 참여 하에 이미징 작업을 하는 경우를 제외하고는 계속 봉인되어 있었으므로, 압수된 이후 법원에서의 검증절차에 이르기까지 보관과정의 신뢰성이 인정되고, 또한 디지털 저장매체 원본과 이미지 파일 사이에 디지털 기기 등의 데이터가 서로 일치함을 증명하는 방법으로 일반적으로 이용되는 해쉬값이 동일하므로 디지털 저장매체 원본과 이미지 파일 사이의 데이터의 동일성이 인정되며, 한편 피고인들 및 검사, 변호인들이 모두 참여한 가운데 이 법원의 전자법정시설 및 인케이스 프로그램을 이용하여

법원의 검증절차가 이루어졌는바, 검증 당시 규격에 적합한 컴퓨터와 인케이스 프로그램을 이용하여 적절한 방법으로 검증절차가 진행되었으므로, 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력, 처리, 출력의 각 단계에서의 컴퓨터 처리과정의 정확성, 조작자의 전문적 기술능력 등의 요건이 구비되었다고 보이고, 달리 그 요건의 흠결을 의심하거나 신뢰성을 배척할 만한 사정은 보이지 아니하며, 위와 같은 검증절차를 거쳐, 디지털 저장매체 원본을 이미징한 파일에 수록된 컴퓨터 파일의 내용이 압수물인 디지털 저장매체로부터 수사기관이 출력하여 제출한 문건들에 기재된 것과 동일하다는 점이 확인되었으므로, 증거능력이 적법하게 부여되었다"고 판시하였다.[18)]

대법원은 "압수물인 디지털 저장매체로부터 출력된 문건이 증거로 사용되기 위해서는 디지털 저장매체 원본에 저장된 내용과 출력된 문건의 동일성이 인정되어야 할 것인데, 그 동일성을 인정하기 위해서는 디지털 저장매체 원본이 압수된 이후 문건 출력에 이르기까지 변경되지 않았음이 담보되어야 하고 특히 디지털 저장매체 원본에 변화가 일어나는 것을 방지하기 위해 디지털 저장매체 원본을 대신하여 디지털 저장매체에 저장된 자료를 '하드카피'·'이미징'한 매체로부터 문건이 출력된 경우에는 디지털 저장매체 원본과 '하드카피'·'이미징'한 매체 사이에 자료의 동일성도 인정되어야 한다. 나아가 법원 감정을 통해 디지털 저장매체 원본 혹은 '하드카피'·'이미징'한 매체에 저장된 내용과 출력된 문건의 동일성을 확인하는 과정에서 이용된 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력의 각 단계에서 조작자의 전문적인

18) 서울중앙지방법원 2007. 4. 16. 선고 2006고합1365, 2006고합1363(병합), 2006고합1364(병합), 2006고합1366(병합), 2006고합1367(병합) 판결

기술능력과 정확성이 담보되어야 한다.”고 하면서, “디지털 저장매체가 봉인된 상태에서 서울중앙지방검찰청에 송치된 후 피고인들이 입회한 상태에서 봉인을 풀고 세계적으로 인정받는 프로그램을 이용하여 이미징 작업을 하였는데, 디지털 저장매체 원본의 해쉬(hash) 값과 이미징 작업을 통해 생성된 파일의 해쉬 값이 동일한 사실, 제1심법원은 피고인들 및 검사, 변호인이 모두 참여한 가운데 검증을 실시하여 이미징 작업을 통해 생성된 파일의 내용과 출력된 문건에 기재된 내용이 동일함을 확인한 사실을 알 수 있는바, 그렇다면 출력된 문건은 압수된 디지털 저장매체 원본에 저장되었던 내용과 동일한 것으로 인정할 수 있다“고 보아 증거능력을 인정하였다.[19]

이처럼 법원은 최초 디지털 증거의 증거능력 인정 요건을 원본과의 동일성, 무결성, 신뢰성으로 보고 있다. 또한 원본을 디지털 저장매체에 저장된 개별 디지털 파일이 아닌 정보저장매체 자체로 보아 정보저장매체 원본과 이를 이미징한 파일의 해시값을 비교하여 디지털 증거의 동일성을 인정하였다.

2. 왕재산 사건

왕재산 사건에서 대법원[20]은 “압수물인 컴퓨터용 디스크 그 밖에 이와 비슷한 정보저장매체에 입력하여 기억된 문자정보 또는 그 출력물을 증거로 사용하기 위해서는 정보저장매체 원본에 저장된 내용과 출력 문건의 동일성이 인정되어야 하고, 이를 위해서는 정보저장매체 원본이 압수 시부터 문건 출력시까지 변경되지 않았다는 사정, 즉 무결성이 담보되어야 한다. 특히 정보저장매체 원본을

19) 대법원 2007. 12. 13. 선고 2007도7257 판결
20) 대법원 2013. 7. 26. 선고 2013도2511 판결

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 원칙이나, 그와 같은 방법에 의한 증명이 불가능하거나 현저히 곤란한 경우에는, 정보저장매체 원본에 대한 압수, 봉인, 봉인해제, '하드카피'또는 '이미징' 등 일련의 절차에 참여한 수사관이나 전문가 등의 증언에 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."라고 판시하였다.

왕재산 사건에서 법원은 기존 일심회 사건에서와 동일하게 디지털 증거의 원본과 사본과의 동일성, 무결성, 신뢰성을 증거능력을 인정하기 위한 요건으로 보면서, 동일성과 무결성의 입증방법에 대한 원칙과 예외를 설시하고 있다.

구체적으로 살펴보면, 정보저장매체 자체를 원본으로 보면서 정보저장매체의 이미지 파일과 정보저장매체 원본 사이의 동일성, 압수시부터 문건 출력시까지 변경되지 않았다는 무결성이 입증되어야 하는데, 그 방법으로 피압수·수색 당사자로부터 원본과 이미지 파일의 해시값이 동일하다는 취지의 확인서면을 받아 해시값 확인서의 해시값과 이미지 파일의 해시값을 비교하여 동일성, 무결성을 입증하는 것이 원칙이라고 설시하여 해시값 비교의 방법을 구체적으로 제시하였고, 그와 동시에 그와 같은 방법이 불가능한 경우에는 예외적으로 일련의 압수절차에 참여한 수사관이나 전문가 등의 증언으로 해시값의 동일성을 증명하거나 정보저장매체 원본이 압수시부터 밀봉되어 변경되지 않았음을 증명하는 방법 또는 법원이 원본에 저장된 자료와 출력 문건을 대조하는 방법 등으로 증명할 수 있고, 반드시 압수·수색 과정을 촬영한 영상녹화물 재생 등의 방법으로만 증명하여야 한다고 볼 것은 아니라고 판시하였다.

따라서 법원은 정보저장매체 자체를 원본으로 보고, 피압수·수색 당사자로부터 해시값 확인서를 받는 방법으로 그 원본과 이미징 파일의 해시값을 비교하는 방법을 동일성, 무결성 입증의 원칙으로 하지만, 그러한 방법이 불가능한 경우에는 예외적으로 다양한 입증방법을 허용하고 있다고 판단된다.

3. 이석기 사건

이석기 사건에서 디지털 증거로서 녹음파일의 증거능력이 문제되었는데, 항소심은 “녹음파일도 디지털방식으로 저장된 디지털 정보이므로 디지털 증거에 해당한다. 그러므로 그 파일이 원본임을 밝히거나 원본과 동일한 사본임을 증명하는 가장 유효·적절한 수단은

원본파일이나 사본파일 생성 직후 해시값을 산출하여 추후 이를 비교하는 방법일 것이다. 그러나 그와 같은 방법에 의한 증명이 불가능하거나 곤란한 경우에는, 녹음파일의 수집·보관·복제 등의 절차에 관여한 사람의 증언이나 진술 또는 녹음파일에 대한 검증·감정 결과 등 제반 사정을 종합하여 그 원본성이나 원본과의 동일성 유무를 판단할 수도 있다. 그러므로 반드시 원본이 보존되어 있어야 한다거나, 디지털 포렌식 절차를 준수하였어야 한다거나, 봉인조치에 의해 보관의 연속성이 증명되어야 한다고 볼 것은 아니다.[21]"라고 판시하였고, 대법원은 "증거로 제출된 녹음파일이 대화 내용을 녹음한 원본이거나 혹은 복사 과정에서 편집되는 등 인위적 개작 없이 원본 내용을 그대로 복사한 사본이라는 점은 **녹음파일의 생성과 전달 및 보관 등의 절차에 관여한 사람의 증언이나 진술, 원본이나 사본 파일 생성 직후의 해쉬(Hash)값과의 비교, 녹음파일에 대한 검증·감정 결과 등 제반 사정을 종합하여 판단**할 수 있다."라고 판시하였다.

법원은 이석기 사건에서 증거능력 인정 요건을 원본과의 동일성, 무결성으로 동일하게 보았다. 그런데 원본의 대상을 정보저장매체가 아닌 정보저장매체에 저장된 디지털 파일을 단위로 보고, 정보저장매체에 저장된 디지털 파일 원본과 동일한 사본 파일임을 해시값 비교를 통하여 증명하는 것이 원칙이나, 예외적으로 압수절차에 참여한 수사관이나 전문가 등의 증언, 검증·감정 등을 종합하여 증명할 수 있다고 판단하였다.

4. 원세훈 사건

원세훈 뇌물 사건에서 대법원은 "전자문서를 수록한 파일 등의

21) 서울고등법원 2014. 8. 11. 선고 2014노762 판결

디지털 전자매체의 경우에는, 그 성질상 작성자의 서명 혹은 날인이 없을 뿐만 아니라 작성자·관리자의 의도나 특정한 기술에 의하여 그 내용이 편집·조작될 위험성이 있음을 고려하여, 원본임이 증명되거나 혹은 원본으로부터 복사한 사본일 경우에는 복사 과정에서 편집되는 등 인위적 개작 없이 원본의 내용 그대로 복사된 사본임이 증명되어야만 하고, 그러한 증명이 없는 경우에는 쉽게 그 증거능력을 인정할 수 없다. 그리고 증거로 제출된 전자문서 파일이 그 원본이거나 혹은 복사 과정에서 편집되는 등 인위적 개작 없이 원본 내용을 그대로 복사한 사본이라는 사실은 그 전자문서 파일의 생성과 전달 및 보관 등의 절차에 관여한 사람의 증언이나 진술, 원본이나 사본 파일 생성 직후의 해쉬(Hash)값과의 비교, 전자문서 파일에 대한 검증·감정 결과 등 제반 사정을 종합하여 판단할 수 있다."라고 하면서 "포렌식 분석결과에 의하면, 엑셀 프로그램으로 작성된 각 시재금고파일의 해시값이 일치하지 않지만, 이는 본문 내용이 달라서가 아니라 위 각 파일을 마지막으로 열어본 시간과 당시 사용하였던 컴퓨터의 사용자 계정명이 다르기 때문이고 본문 내용이 다르기 때문은 아니다. 그 외에 이 사건 각 시재금고파일의 생성일시, 최종 저장일시, 최종 수정일시의 해시값은 서로 동일하므로, 이 사건 각 시재금고파일은 모두 동일한 원본파일의 사본이라고 추단할 수 있다"[22]고 판시하였다.

법원은 원세훈 사건에서도 계속적으로 종합판단설의 입장을 유지하면서 증거능력 인정 요건을 원본과의 동일성, 무결성으로 보고 있다. 그런데 원본의 대상을 전자문서 파일, 즉 디지털 파일로 보고 전자문서 파일 원본과 그 사본 파일의 해시값을 비교하는 것을 원칙으로 하고 있으나, 해시값이 일치하지 않는 경우에도 본문 내용이

22) 대법원 2016. 9. 28. 선고 2014도9903 판결

일치하는 점, 생성일시, 최종 저장일시, 최종 수정일시의 해시값이 동일한 점 등을 종합하여 동일성을 인정하고 있다.

5. 조세범처벌법위반 사건

조세범처벌법위반 사건에서 대법원은 "① 이 사건 CD에는 이 사건 판매심사 파일을 포함하여 이현정이 작성한 것으로 보이는 4,458개의 파일(이하 '이 사건 개별 파일들'이라고 한다)과 DirList[20160407-213826].html 파일(이하 '이 사건 목록 파일')이 저장되어 있다. 원심 감정결과에 의하면, 이 사건 개별 파일들은 포렌식 이미징 작업을 거친 이미지 파일이 아니어서 이 사건 USB 이미지 파일과 동일한 형태의 파일이 아닌데, 이 사건 USB 이미지 파일이 어떠한 형태의 변환 및 복제 등 과정을 거쳐 이 사건 CD에 일반 파일 형태로 저장된 것인지를 확인할 자료가 전혀 제출된 바 없다. 더욱이 이 사건 목록 파일에는 이 사건 개별 파일들 숫자보다 많은 4,508개의 파일 관련 이름, 생성·수정·접근 시각, 파일 크기, MD5 해시값, 경로 정보가 저장되어 있고, 원심 감정결과에 의하면, 이 사건 개별 파일들의 해시값과 이 사건 목록 파일상 해당 파일별 해시값을 비교해 보았을 때 20개 파일의 해시값이 동일하지 않다는 것이다. 따라서 이 사건 목록 파일이 생성·저장된 경위에 대하여 아무런 주장·증명이 없는 이 사건에서 이 사건 목록 파일 자체의 파일명 및 그 파일 속성을 통해 알 수 있는 수정 일자 등에 비추어 이 사건 목록 파일이 이 사건 압수 집행 당시가 아닌 그 이후에 생성되었을 가능성을 배제할 수 없다. ② 이 사건 사실확인서에는 이 사건 USB 이미지 파일의 전체 해시값만이 기재되어 있을 뿐 이미징을 한 이 사건 USB 내 개별 파일에 대한 해시값은 기재되어 있지 않으므로, 이 사건 사실확인서를

가지고 이 사건 판매심사 파일과 이 사건 USB 내 원본 파일과의 개별 해시값을 상호 비교할 수도 없다.”고 하면서 “이 사건 판매심사 파일이 이 사건 USB 내 원본 파일을 내용의 변개 없이 복제한 것이 확인되지 않은 이상, 이 사건 판매심사 파일과 대조한 결과 그 출력물에서 과세표준의 기초가 되는 부분의 변조내용을 찾아볼 수 없었다는 사정이 이 사건 USB 내 원본 파일의 인위적 개작 없이 그 출력물이 복제·출력되었음을 뒷받침한다고 볼 수도 없다.”[23]‘고 판시하였다.

위 판례는 정보저장매체에 저장된 개별 파일들의 사본이 증거로 제출된 경우의 동일성, 무결성의 입증에 대해 설시하고 있는 것으로 보인다. 이 사건은 정보저장매체에 저장된 파일을 선별을 한 후 이미징하여 정보저장매체 이미지 파일을 압수한 사례이다. 정보저장매체에 저장된 파일들이 전체적으로 이미징된 파일과 정보저장매체에 저장된 개별 디지털 파일을 구별하여, 피압수·수색 당사자에게 교부된 사실확인서에 개별 디지털 파일들의 해시값이 아닌 정보저장매체 이미지 파일의 전체 해시값만이 기재된 경우에는 개별 파일들이 이미지 파일로부터 어떠한 형태의 변환 및 복제 등 과정을 거쳐 개별 파일로 된 것인지 여부도 증명해야 되는 것으로 보았고, 이 사건 목록 파일과 개별 파일들의 해시값이 일부 일치하지 않는 점 등을 이유로 동일성이 충분히 증명되었다고 볼 수 없다는 취지로 판시하였다. 결국, 법원은 피압수자에게 교부된 사실확인서에 기재된 해시값, 즉 전체 이미지 파일의 해시값을 해시값 비교의 대상으로 보면서, 위 해시값의 비교에서 더 나아가 압수된 이미지 파일에서 개별 파일들이 변환 및 복제된 사실, 즉 이미지 파일에서 개별 파일로 전환 및 복제되는 과정의 동일성, 무결성까지 증명하여야 된다고 본 것으로

23) 대법원 2018. 2. 8. 선고 2017도13263 판결

보아 증거능력 인정 요건을 더욱 강화한 것으로 보인다. 다만, 원심 감정 결과에 의해 일부 개별적 디지털 파일들의 해시값이 다른 사정이 발견되어 더욱 엄격하게 판단하였을 가능성이 있으므로, 위 판례만으로 판례의 태도가 변경되었다거나 디지털 파일의 증거능력에 대한 일반 원칙을 선언하였다고 볼 수는 없을 것이다.

6. 소결

박진환은 "우리나라 대법원은 동일성 입증에 엄격한 태도를 취하고 있어 해시값이 다르거나 기술적인 이유 등으로 해시값 산출이 곤란한 경우 다른 특별한 입증이 없는 한 증거능력을 인정하지 않으려는 경향이 강하다. 판례에서 해시값의 비교를 동일성을 입증하기 위한 원칙적인 방법으로 제시하고 있기 때문이다. 반면 해시값으로 동일성을 증명할 수 없는 경우에도 대법원에서는 다양한 입증방법을 허용하고 있어 증거능력을 인정받을 수 있는 여지가 생겼다고 보여진다."[24]고 한다.

판례는 앞서 살펴본 바와 같이 증거능력 인정 요건으로 디지털 증거의 원본과 사본과의 동일성, 무결성, 신뢰성을 들면서, 동일성, 무결성을 증명하는 방법으로 피압수자에게 교부된 확인서에 기재된 원본의 해시값과 사본의 해시값을 비교하는 방법을 원칙으로 하고, 예외적으로 수사관이나 전문가의 증언, 검증·감정 등 다양한 입증방법을 종합적으로 판단할 수 있다고 판시하고 있다. 원본의 대상과 관련하여, 판례는 기존 정보저장매체 자체를 원본으로 보고 정보저장매체의 이미지 파일의 해시값을 비교하였으나 최근에는 개별

24) 박진환, "해시값의 비교에 의한 디지털 증거의 동일성 입증에 관한 연구", 석사학위논문, 서울대학교, 2019, 87면

디지털 파일로 단위를 확장하고 있고, 최근에는 이미지 파일에서 개별 디지털 파일들로의 변환, 복제하는 과정에서의 동일성, 무결성에 대한 증명도 요구하는 것으로 보인다. 이는 판례의 각각의 사건에서 제출된 증거의 형태가 다르고, 압수 방법이 다른 것이 원인으로 인한 것일 수도 있으나, 판례의 경향은 동일성, 무결성에 대한 입증을 강화하는 것으로 보인다.

제4절 미국 판례의 태도

1. 진정성[25)]

디지털 정보가 어떠한 매체를 통하여 작성되면 그 매체에 독립성을 가지게 되고, 일단 생성된 디지털 정보는 다른 저장매체 또는 인터넷 등을 통하여 이동할 수 있다. 그러한 과정에서 디지털 정보는 사람에 의해서 의도적으로 혹은 시스템에 의하여 자동적으로 변경될 수 있는데, 변경되지 않았다는 것을 증명하는 것을 '진정성'이라고 한다. 우리나라 판례에서 요구하는 동일성과 무결성은 미국 증거법상 증거능력의 요건인 진정성의 개념에서 유래한 것으로 보이고, 연방증거규칙 제901조(a)항은 "일반 규정. 진정성과 동일성 확인의 인정요건에 있어서, 증거로 채택함에 선행하는 조건은, 그 증거의 신청자가 진정하고 동일한 것이라고 구장하는 것이 그 원본인 것과 같다는 점을 충분히 인정할 만한 증거에 의하여 성취된다"고 규정하고 있다. '증거의 진정성'과 동일성(identification) 요건을 충족시키기 위하여, 증거신청인은 해당 증거가 증거신청인이 주장하는 바로

25) 박진환, "해시값의 비교에 의한 디지털 증거의 동일성 입증에 관한 연구", 석사학위논문, 서울대학교, 2019, 68-70면을 정리하였음

그것이라는 사실을 뒷받침하기에 충분한 증거를 제출하여야 한다고 규정하고 있다. 연방증거규칙(FRE)과 이를 기초한 미국 각 주의 증거법에 규정된 진정성의 문제는 '과연 해당 증거가 당해 문서 또는 자료가 맞는지의 문제'로서 전문법칙 적용 여부의 이전의 단계이고, 진정성에 대한 입증은 공소사실에 대한 입증정도인 합리적으로 의심의 여지가 없을 정도라는 엄격한 증명이 아닌 자유로운 증명으로 족하다고 규정되어 있다.

미국에서도 그 증명을 위한 심증의 정도는 그리 높지 않고 증명방법도 아무런 제한이 없다. 미국연방증거규칙은 후술하는 바와 같이 관련자 증언으로도 그 증명을 할 수 있다고 명시적으로 선언하였다.(제901조의(b)). 언뜻 보기에(prima facie) 진정할 정도이면 증거로 받아들이고, 이후에는 증명력(weight)의 문제로 보아 피고인으로 하여금 그 신빙성을 공격할 것을 요구한다. 미국 법원은 증거가 변개되지 않았음을 모든 의심의 여지가 없도록 증명할 필요가 없고 조작 흔적이 없음을 합리적인 정도로 증명하는 것으로 충분하다고 본다. 증거능력을 부여할지 여부는 사실심 법원에 광범위한 재량의 문제로 보았다.

미국 Maryland 지방법원의 Paul Grimm 치안판사는 2007년 Lorraine v. Markel 사건[26]에서 전자적 저장정보(Electronically Stored

26) Lorraine v. Markel American Ins. CO., PWG-06-1893 (D. Md May 4. 2007); [사실관계] 원고 Jack Lorraine과 Beverly Mack은 2004. 5. 17. 자신의 보트가 번개에 맞아 피해를 입자 피고 보험사(Markel American Insurance社)에 보험금을 청구하였고, 피고 보험사는 자신의 정책에 따라 보험금을 지급하였다. 그런데 원고는 몇 달 후에 자신의 보트 외부가 손상되었음을 발견하고 보트 손상시 수리에 관한 특약 36,000달러에 대한 지급을 요청하였는데, 피고는 이에 불응하였고, 이로 인해 Lorraine 등과 피고 보험사 사이에 분쟁이 발생하였다. 그런데 당사자들은 이메일을 통해 보험금 지급에 관한 중재협약을 하여 미연방중재법(§9 of the Fedral Arbitration Act, 9 U.S.C.. §1 et seq.[2006])에 따라 위 분쟁이 우선 중재에 회부되었는데, 그 중재에서 중재위원은 보트외부에 대한 손해 중 일부가 번개로 인한 것으로 판단, 손해액을 14,100달러로 제한 결정했다. 그런데 원고는 이에 불복하고

Information)의 증거능력 허용여부에 대한 의미 있는 판결을 내놓았다. 즉 디지털 증거를 받아들일지 평가할 때 고려해야 할 5가지 이슈를 정리하였는데, 디지털 증거의 증거능력 인정요건으로, ① 당해 증거가 연방증거규칙 제401조에 따른 사실관계의 존재에 관한 관련성(Relevant)이 인정될 것, ② 외부적 증거에 의하거나 독립적 증명방법을 통해 그 진정성(Authentic)이 인정될 것, ③ 전문증거가 아니거나 그 예외사유에 해당할 것(Not hearsay or admissible hearsay), ④ 연방증거규칙 제1001조(3)의 원본(the original)이거나 동 규칙 제1003조의 '원본과 동일하게 인정되는 사본'일 것, ⑤ 부당한 편견의 부재(Unfair Prejudice)를 제시하였는데,[27] 여기에서 위 ②의 진정성(Authentic) 증명 방법으로 해시값[28]과 메타데이터를 언급하였다.[29]

2. 최량증거법칙(The Best Evidence Rule)

미국 연방 증거법 제1002조는 '서류, 기록물 또는 사진의 내용을 증명하기 위하여 문서, 기록물, 사진의 원본이 요구된다.'라고 규정하고

중재는 그 손해가 번개로 인한 것인지 여부만 판단할 뿐 그 손해액을 감액할 권한이 없음을 이유로 지방법원에 위 소를 제기하였다. 그런데 위 소송과정에서 당사자 모두 '중재협약 범위'에 관한 당사자들의 의도에 대한 증거로 상담시 주고받은 이메일 사본을 제출하였는데 이와 관련하여 이메일이라는 전자적 저장정보가 증거로서 허용될 수 있는지 여부가 쟁점으로 부각되었다(강철하, "美 Loraine v. Markel American Insurance Company 事件에 나타난 電子的貯藏情報의 證據能力許容要件", 아주법학 2권 1호, 아주대학교 법학연구소, 2008, 10~11면, 박진환, "해시값의 비교에 의한 디지털 증거의 동일성 입증에 관한 연구", 석사학위논문, 서울대학교, 2019, 73면에서 재인용).

27) Eoghan Casey, "Digital Evidence and Computer Crime : Forensic Science, Computers and the Internet", Third Edition, 1999, 57면.

28) 전현욱·김기범·조성용·Emilio C. VIANO, "사이버범죄의 수사 효율성 강화를 위한 법제 개선방안 연구", 경제·인문사회연구회 미래사회 협동연구총서 15-17-01, 2015, 355~356면

29) Lorraine v. Markel American Ins. CO., 241 F.R.D. 534, 546-47 & n.23 (D. Md. 2007); 김기범, "해시함수의 형사법적 고찰", 형사정책연구, 한국형사정책연구원, 2018, 212면

있다. 이것이 최량증거법칙 규정이다. 또한 연방증거규칙 제1001조 제1호에 의하면 디지털 증거는 자기적 혹은 전기적 방식에 의한 기록물로서 제1002조의 '서류, 기록물 등'에 포함된다. 따라서 디지털 증거도 당연히 원본으로 제출 될 것을 요구받는다.

그런데 미국에서는 증거규칙 제1001조 제3호에 "원본(original). 서면이나 기록의 '원본'은 서면이나 기록 그 자체 또는 그것을 발행하거나 집행하는 사람이 그와 동일한 효력을 가지게 할 의도로 작성한 것을 말한다. 사진의 '원본'은 네가티브(negative) 필름 또는 그것으로부터 인화된 것을 포함한다. 데이터가 컴퓨터나 이와 유사한 장치에 의해 저장되어 있는 경우 육안에 의하여 읽을 수 있는 인쇄물이나 어떠한 형태의 출력물이라도 자료를 정확히 반영하고 있는 경우에는 '원본'이다"라고 규정함으로써 원본의 출력물도 원본으로 인정하는 규정을 두고 있다. 나아가 제1001조 제4호에서는 "사본(duplicate). '사본'은 원본과 동일한 내용을 표현하도록 만들거나, 동일한 매트릭스(matrix)로부터 작성되거나, 확대와 축소를 포함한, 사진, 기계적 또는 전기적인 재기록(re-recording), 화학적인 재생산, 또는 원본을 정확히 재생할 수 있는 기타의 동등한 기술에 의하여 작성된 것을 말한다"고 규정하고, 제1003호에서는 "사본은 (1) 원본에 대한 진정성에 대하여 이의가 제기된 경우 또는 (2) 사본으로 원본을 대체하는 것이 불공평한 것으로 인정되는 정황이 있을 경우를 제외하고는 원본과 동일하게 증거로 할 수 있다"고 규정하고 있다.[30]

우리나라의 판례 및 학설의 태도에서는 원본을 정보저장매체 자체에 저장되어 정보로 보고, 원본을 동일한 내용으로 재생산, 복제 및 출력한 것들을 모두 사본으로 보고 있으나, 미국에서는 원본의 개념을

30) 김현선, "미국의 디지털 증거 활용 실태", 해외연구검사 연구논문, 2008, 72-73면

넓게 보아 원본을 동일하게 반영하고 있는 것, 출력물까지도 모두 원본으로 보고 있음을 알 수 있다.

제5절 실무의 태도

우리나라 수사 실무의 태도를 살펴보면, 검찰에서는 '디지털 증거의 수집·분석 및 관리 규정'(대검 예규 제991호, 전부 개정 2019. 5. 20.)을 통해 정보저장매체 등으로부터 디지털 증거를 수집·보존·분석·현출하는 과정에서 준수하여야 할 사항을 규정하였는데, 디지털 증거의 무결성, 신뢰성 및 보관의 연속성 유지를 요건[31]으로 하고 있다.

디지털 증거의 압수·수색·검증은 수사에 필요한 범위에서 실시하고, 모든 과정에서 적법절차를 엄격히 준수하여야 하며, 디지털 증거의 압수·수색·검증은 디지털 포렌식 수사관이 하여야 하며, 피압수자 등의 참여기회를 보장하여야 하도록 규정하고 있다.[32]

---

31) 디지털 증거의 수집·분석 및 관리규정(대검 예규 제991호)

제4조(디지털 증거의 무결성 유지)

디지털 증거는 압수·수색·검증한 때로부터 법정에 제출하는 때까지 훼손 또는 변경되지 아니하여야 한다.

제5조(디지털 증거의 신뢰성 유지)

디지털 증거는 그 수집 및 분석 과정에서 이용된 도구와 방법의 신뢰성이 유지되어야 한다.

제6조(디지털 증거의 보관의 연속성 유지)

디지털 증거는 최초 수집된 상태 그대로 어떠한 변경도 없이 보관되어야 하고, 이를 위해 보관한 주체들 간의 연속적인 승계 절차를 관리하는 등의 조치를 취해야 한다.

32) 디지털 증거의 수집·분석 및 관리규정(대검 예규 제991호)

제14조 (압수·수색·검증 시 유의사항)

디지털 증거의 압수·수색·검증은 수사에 필요한 범위에서 실시하고, 모든 과정에서 적법절차를 엄격히 준수하여야 한다.

제15조 (압수·수색·검증의 실시자)

디지털 증거의 압수·수색·검증은 디지털포렌식 수사관이 하여야 한다. 다만, 부득이한 사유가 있는 경우 포렌식 도구 교육 등 제7조제2항에 의한 디지털포렌식 관련 교육을 받은 수사관이 할 수 있다.

제17조 (압수·수색·검증의 참여)

① 주임검사 등은 디지털 증거를 압수·수색·검증하는 과정에서 피압수자 등에게 참여의 기회를 보장하여야 한다.

구체적으로, 압수의 목적물이 정보저장매체 등인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 압수하여 하나, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 경우 또는 피압수자 등의 동의가 있는 경우에는 정보저장매체 등을 압수하거나 정보저장매체 등에 기억된 전자정보 전부를 복제할 수 있다. 사건과 관련성이 있는 정보를 수색하여 디지털 증거를 압수하는 경우에는 진정성, 무결성, 신뢰성을 확인하기 위하여 해시값(Hash Value)을 생성하고 "현장조사확인서"를 작성하여 확인·서명을 받거나 다음 해시값 등이 포함된 확인서를 작성하여 피압수자 등의 확인·서명을 받아야 한다.[33]

---

② 피압수자 등의 참여가 곤란한 사정 등이 있는 경우에는 다음 각 호에 따라 필요한 조치를 할 수 있다.

1. 피압수자의 소재불명, 참여지연, 참여불응 등의 사유로 피압수자 또는 변호인의 참여 없이 압수·수색·검증을 해야 하는 경우에는 「형사소송법」 제123조에서 정하는 참여인을 참여하게 한다.
2. 피압수자 또는 변호인 등이 압수·수색·검증에 참여 중 정당한 사유 없이 참여를 중단하여 그 집행을 계속하기 어려운 경우에는 「형사소송법」 제123조의 참여인을 참여하게 한 후 집행을 재개한다. 집행을 중지한 경우 필요한 때에는 압수·수색·검증 장소의 출구를 별지 제5-3호 서식의 "압수장소 봉인지" 등으로 봉인하여 집행재개 시까지 그 장소를 폐쇄할 수 있다.
3. 피압수자 또는 변호인 등이 압수·수색·검증에 참여한 후 별지 제2호 서식의 "현장조사확인서"에 서명을 거부하는 때에는 피압수자 또는 변호인 등이 서명을 거부하였음과 그 사유를 위 확인서에 기재한다.

33) 디지털 증거의 수집·분석 및 관리 규정(대검 예규 제991호)

제18조 (디지털 증거의 압수·수색·검증)

① 압수의 목적물이 정보저장매체 등인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 압수하여야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 경우 또는 피압수자 등의 동의가 있는 경우에는 정보저장매체 등을 압수하거나 정보저장매체 등에 기억된 전자정보 전부를 복제할 수 있다.

② 사건과 관련성이 있는 정보를 수색하여 디지털 증거를 압수하는 경우에는 해시값(Hash Value)을 생성하고 별지 제2호 서식의 "현장조사확인서"를 작성하여 확인·서명을 받거나 다음 각 호의 내용이 포함된 확인서를 작성하여 피압수자 등의 확인·서명을 받아야 한다. 이 경우, 확인서는 디지털포렌식 도구에 의해 자동 생성된 자료로 갈음할 수 있다.

1. 확인서 작성일시 및 장소
2. 정보저장매체 등의 종류 및 사용자
3. 해시값, 해시함수

디지털 증거의 수집·분석 및 관리 규정'(대검 예규 제991호, 전부 개정 2019. 5. 20.)에서는 제19조(확인서 인계 및 전자정보상세목록 교부)가 신설되었는데, "디지털포렌식 압수·수색·검증이 종료되면 압수한 파일의 상세목록을 작성하여 서면의 형태로 교부, 파일의 형태로 복사 또는 전자메일로 전송하는 등의 방법으로 피압수자 등에게 교부하여야 한다."[34]고 규정하고 있다.

이에 따라 아래와 같이 디지털 증거의 수집 분석 및 관리 규정(대검 예규 제991호, 전부 개정 2019. 5. 20.) [별지 2] 현장조사확인서 서식을 규정하고 있는데, 위 현장조사확인서에는 이미지파일의

---

4. 확인자의 인적사항 및 연락처, 확인자와 피압수자와의 관계
5. 기타 진정성·무결성·신뢰성을 확인하는데 필요한 사항

③ 정보저장매체 등을 압수하는 경우에는 제11조제3항을 준용하여 별지 제5-1호 서식의 "압수물 봉인지" 및 별지 제3호 서식의 "정보저장매체 제출 및 이미징 등 참관여부 확인서"를 작성하여야 한다.

④ 정보저장매체 등에 기억된 전자정보 전부를 다른 정보저장매체에 복제하는 경우에는 별지 제5-1호 서식의 "압수물 봉인지" 및 별지 제4호 서식의 "정보저장매체 복제 및 이미징 등 참관여부 확인서"를 작성하여야 한다.

⑤ 제3항 내지 제4항의 경우에 대한 참관여부 확인은 피압수자 등의 참관 의사를 확인한 수사보고서로 갈음할 수 있다.

⑥ 압수·수색·검증의 대상인 정보저장매체와 정보통신망으로 연결되어 있고 압수·수색·검증의 대상이 되는 디지털 증거를 저장하고 있다고 인정되는 다른 정보저장매체에 대하여 압수·수색·검증 대상인 정보저장매체의 시스템을 통하여 접속한 후 수색을 할 수 있다. 이 경우 압수·수색·검증 대상 정보저장매체가 정보통신망에 연결되어 있고, 압수·수색·검증 대상자가 정보통신망으로 접속하여 기억된 정보를 임의로 삭제할 우려가 있을 경우에는 정보통신망 연결 케이블을 차단할 수 있다.

⑦ 정보저장매체의 피압수자 등에게 디지털 증거의 출력, 복제, 정보저장매체의 작동, 정보통신망으로 연결되어 있는 다른 정보저장매체의 접속, 기타 필요한 협력을 요구할 수 있다.

34) 디지털 증거의 수집·분석 및 관리 규정(대검 예규 제991호)

제19조 (확인서 인계 및 전자정보상세목록 교부)

① 디지털포렌식 수사관은 피압수자 등이 작성한 각종 확인서를 주임검사 등에게 인계하여 압수목록 작성, 참여기회 보장 등 후속 절차진행에 참고할 수 있도록 한다.

② 디지털포렌식 수사관은 디지털포렌식 압수·수색·검증이 종료되면 압수한 파일의 상세목록을 작성하여 피압수자 등에게 교부하여야 한다. 다만, 다음 각 호와 같이 상세목록 작성이 곤란한 경우는 예외로 한다.

1. 범위를 정하여 출력 또는 복제하는 방법이 불가능하여 정보저장매체 등을 압수한 경우
2. 정보저장매체에 저장된 전자정보를 파일 단위로 온전하게 압수할 수 없는 경우

③ 제2항에 따른 상세목록의 교부는 서면의 형태로 교부하는 방법 이외에 파일의 형태로 복사해주거나 전자메일로 전송하는 등의 방법으로 갈음할 수 있다.

해시값뿐만 아니라 전자정보상세목록의 해시값도 기재하여 피압수자에게 교부하도록 하고 있다.

[별지 제2호 서식] 현장조사확인서

National Digital Forensic Center

【 현장조사확인서 】

이미지파일 정보

사건번호	2019지원0000_1호_○○주식회사
증거번호	증1호 홍길동(대표이사)의 노트북
압수장소	서울 서초구 반포대로
사 용 자	홍길동
조 사 자	조사자
시간설정	PC 설정시간 : 2019. 01. 01. 00:00:00 KST 시간 : 2019. 01. 01. 00:00:00
이미지파일 생성일시	2019. 01. 01. 00:00:00
이미지파일명	증1호_홍길동(대표이사)_노트북.dd

해시값

이미지파일	
전자정보상세목록 파일	

※ Hash Value : 해시값은 데이터를 고유하게 식별하는 고정 길이의 값으로 해시함수의 결과로 생성된다. 해시함수는 입력 데이터의 크기와 무관하게 일정한 길이를 가진 값을 출력하며, 입력이 다른 경우 다른 결과가 나타난다. 만약 원본에서 조금이라도 변경이 되면 계산되는 해시값이 완전히 달라지기 때문에, 일반적으로 디지털증거의 무결성을 입증하는 수단으로 사용되고 있다.

- 위 해시값은 홍길동(대표이사)의 디지털기기(노트북)에서 압수한 전자정보에 대한 해시값이고, 그에 대한 전자정보상세목록을 교부(□출력 □복사) 받았음을 확인합니다.
- 위 압수·수색·검증 절차에서 압수한 전자정보는 수사 또는 재판 목적 소멸 시 폐기됨을 고지받았음을 확인합니다.

확인 일시 및 장소 :

확인자 성명 : (서명)

확인자 생년월일 :

확인자 연락처 :

피압수자(임의제출자 등)와의 관계 : 본인, 기타 ( )

그림 1. 2019. 5. 20.부터 사용된 검찰 '현장조사확인서' 서식

기존 실무에서는 현장조사확인서에 이미지파일의 해시값만을 기재하여 교부하였으나, 판례의 태도가 해시값 비교의 대상을 정보저장매체에서 개별 디지털 파일로 확대하고 있는 경향에 따라 개별 디지털 파일의 해시값이 기재된 전자정보상세목록을 교부하면서 위 전자정보상세목록의 동일성, 무결성을 입증하기 위해 전자정보상세목록 파일의 해시값도 제공하도록 신규 개정한 것으로 보인다.

따라서 2019. 5. 20. 전부 개정된 디지털 증거의 수집·분석 및 관리 규정에 의하면, 전문적인 디지털포렌식 수사관이 디지털 증거의 압수·수색·검증을 하게 함으로써 전문성, 신뢰성을 인정받고, 피압수자 등에게 현장조사확인서에 기재된 해시값과 전체 이미지 파일의 해시값 및 전자정보상세목록 파일의 해시값을 비교하고, 피압수자에게 교부된 전자정보상세목록에 기재된 개별 디지털 파일들의 해시값과 법정에 제출한 개별 디지털 파일들의 해시값을 비교하는 방법으로 동일성, 무결성을 입증하는 방법으로 증거능력을 인정받을 수 있도록 규정한 것으로 보인다.

III. 디지털 파일의 삭제와 삭제 파일의 복구

제1장 파일시스템과 데이터의 저장 구조[35)]

제1절 파일시스템

컴퓨터 안에는 수백만 개에서 수천만 개의 파일이 있고, 이러한 파일을 제대로 관리하기 위해서 사용하는 방법을 파일 시스템(File System)이라 한다. 즉, 파일 시스템은 데이터의 효과적인 관리·저장 목적으로 파일을 체계적으로 저장하는 규칙을 정한 것이다. 광학 저장 장치의 경우 ISO 9660, UDF 등의 파일시스템으로 데이터를 저장하고, 디스크 저장 장치의 경우 운영체제에 따라 다양한 파일시스템이 활용되는데, 이하에서는 윈도우 운영체제에서 많이 사용되는 파일시스템인 FAT(File Allocation Table)및 NTFS(New Technology File System)를 개략적으로 확인하겠다. 주로 FAT은 USB 메모리에, NTFS는 하드디스크에 사용된다.

1. FAT 파일시스템

FAT파일시스템은 Directory 표현을 위하여 트리구조를 사용하고 있고, Root Directory가 데이터 영역의 제일 앞부분에 위치하게 된다. FAT12, FAT16은 Root Directory가 FAT Entry 2번에 위치하고, FAT32는 Root Directory가 특별히 설정하지 않는 한 FAT Entry

35) Larry E. Daniel, Lars E. Daniel, “포렌식 전문가와 법률가를 위한 디지털 포렌식”, 비제이퍼블릭, 2012, 247-256면과 John Sammons, "이제 시작이야 디지털 포렌식“, 비제이퍼블릭, 2012, 34-42면을 정리하였음

2번에 위치하게 된다. 개별 Directory 및 파일들은 파일의 이름, 확장자, 시간정보 등을 표현하기 위하여 Directory Entry를 구성하는데, 특히 파일들의 Directory Entry 0x000E~000F에 생성시간(Created Time), 0x0010~0011에 생성날짜(Created Date), 0x12~13에 마지막 접근 날짜(Accessed Date), 0x16~17에 마지막 수정시간(Written Time), 0x18~19(Written Date)에 마지막 수정날짜가 기재된다. 따라서 FAT파일시스템으로 저장된 파일을 증거조사할 때, 해당 Directory Entry에 저장되어 있는 시간정보를 확인할 필요가 있을 수 있다.

2. NTFS 파일시스템

NTFS 파일시스템은 메타데이터 역할을 하는 MFT Entry 0~15($MFT, $LogFile, $Volume 등) 및 기타 MFT Entry를 가지고 있다. MFT Entry는 1,024바이트 크기를 가지고 있고, 그 중 $STANDARD_INFORMATION 속성(속성헤더 0x0010)에 파일 생성시간(0x0000~0007), 파일 변경시간(0x0008~000F), MFT 변경시간(0x0010~0017), 파일 접근시간(0x0018~0x001F) 등의 정보가 저장되고, $FILE_NAME 속성(속성헤더 0x0030)에 파일 생성시간(0x0008~0x000F), 파일 변경시간(0x0010~0x0017), MFT 변경시간(0x0018~0x001F), 파일 접근시간(0x0020~0x0027) 등의 정보가 중복 저장되므로, 위 각 데이터를 증거조사하여 시간정보의 내용 및 변개여부를 확인할 수 있다.

제2절 하드 드라이브의 데이터 저장 구조

1. 데이터 저장에 이용되는 수학적 개념

디지털 파일은 클러스터(Cluster)[36] 단위로 저장되고, 저장될 위치를 할당하여야 한다. 예를 들어서 6566바이트 크기의 파일을 가지고 있다고 가정해보면, 컴퓨터의 운영체제(OS)가 이 파일을 저장하기 위해서는 먼저 4096바이트의 크기인 1개의 클러스터를 전부 사용하고 나머지 2560바이트는 다른 클러스터에 저장한다. 파일 시스템에 파일이 저장되는 개념은 아래와 같다.

A hard drive with no data																
Sectors	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512
Clusters	4096								4096							
File Data	Unallocated Space															
A hard drive with file data																
Sectors	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512
Clusters	4096								4096							
File Data	**Used By Fide Data**													Slack		
A hard drive after deleting the file data																
Sectors	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512
Clusters	4096								4096							
File Data	**Delected Data(Old File)**													Slack		
A hard drive with new file data and old file data left over																
Sectors	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512	512
Clusters	4096								4096							
File Data	**Used By New File**					**Delected Data(Old File)**								Slack		

그림 2. NTFS 파일 시스템에서의 파일 저장 개념도[37]

36) 저장장치에 데이터를 읽고 쓰는 논리적인 기본 단위

37) Larry E. Daniel, Lars E. Daniel, “포렌식 전문가와 법률가를 위한 디지털 포렌식”, 비제이 퍼블릭, 2012, 252면, 그림 29-6

그림을 보면, 첫 번째 칸은 아무런 데이터가 저장되어 있지 않음(Unallocated Space)을 알 수 있고, 두 번째 칸은 1개의 클러스터 전체와 또 다른 클러스터의 일부분이 파일을 저장하는데 이용되고 있음을 알 수 있으며, 세 번째 칸은 파일이 삭제되었음을 알 수 있는데, 이렇게 파일이 삭제되었다고 하더라도 윈도우즈에서는 눈으로 볼 수 없을 뿐, 하드 드라이브에서는 여전히 파일이 남아있게 되는 것을 알 수 있다. 네 번째 칸은 이전에 저장했던 큰 파일이 남아있는 클러스터에 이보다 작은 새로운 파일이 저장되었음을 볼 수 있다. 이와 같이 파일이 삭제되고 난 후 새로운 파일이 저장된 경우라 하더라도 이전에 저장했던 파일의 크기가 더 큰 경우에는 이전에 저장했던 파일의 일부분은 여전히 하드 드라이브에 남아있게 되고, 이러한 잔여 파일은 '파일 카빙(File Carving)' 기업을 통해서 복구해 낼 수 있음을 알 수 있다.

2. 할당영역과 비할당영역

파일 시스템은 하드 드라이브에 있는 공간을 할당영역과 비할당영역, 2가지로 분류된다.

할당영역이란 컴퓨터가 사용 중에 있고 기록 및 유지하고 있는 데이터, 즉, 윈도우에서 볼 수 있고 열 수 있는 모든 파일을 의미한다. 컴퓨터의 파일 시스템은 이러한 파일을 모니터하고 이러한 파일에 대한 다양한 정보를 기록한다.

그런데 파일이 삭제되거나 파일시스템이 포맷된 경우에는 파일시스템의 파일메타정보들이 변경되거나 사라졌기 때문에 해당 파일에 접근할 수 없고, 일반적으로 파일시스템의 파일메타정보가 정상적으로 존재하여 접근할 수 없는 저장매체의 영역을

비할당영역이라 한다.

파일시스템은 운영체제가 디지털 데이터를 저장, 탐색, 삭제, 조작 등을 쉽게 하기 위해 구조적으로 유지 관리하는 방식으로, 디지털 데이터는 파일의 형태로 파일시스템에 기록되는데, 각 저장매체의 파일시스템은 저장된 파일들에 대한 접근을 쉽게 하기 위해 파일데이터와 이름, 크기, 위치 등의 파일메타정보를 별도로 관리한다. 따라서 특정 파일에 접근하고자 할 경우 저장매체 전체를 검색할 필요 없이 파일메타정보를 이용해 빠르게 접근이 가능하다. 파일메타정보는 파일의 생성/수정/삭제 등의 작업이 발생할 때마다 갱신되어 실제 저장되어 있는 파일데이터와 일관성이 유지된다. 따라서 파일시스템의 파일메타정보를 획득하게 되면 현재 저장된 모든 파일에 접근할 수 있다. 파일이 삭제되거나 파일시스템이 포맷된 경우에는 파일메타정보가 변경되거나 삭제된다. 따라서 이전에 저장되었던 파일에 대한 접근이 불가능하지만 파일메타정보에만 영향을 미쳤기 때문에 실제 파일데이터는 새로운 파일로 덮어 써지거나 완전삭제되기 전에는 그대로 존재한다. 비할당영역은 파일메타정보를 통해 접근할 수는 없지만 해당 영역이 새로운 파일로 덮어 써지거나 완전삭제(Wipe)되지 않았다면 이전 파일데이터가 그대로 존재하게 된다.

결론적으로, 운영체제에 의해 파일시스템이 구성된 후 파일이 저장되면 파일시스템 상에 파일메타정보가 기록되게 되는데, 파일메타정보가 정상적으로 존재하여 접근이 가능한 저장매체의 영역을 할당영역이라 하고(저장매체에 저장되는 파일데이터들은 항상 연속된 공간에 저장되는 것이 아니라 운영체제의 할당 알고리즘에 의존한다), 파일이 삭제되었거나 파일시스템이 포맷된 경우

파일메타정보가 변경되거나 사라진 경우 논리적으로 파일데이터에 대해 접근할 수 없는데 파일메타정보를 참조하여 접근할 수 없는 저장매체의 영역을 비할당영역이라 한다.

제2장 디지털 파일의 삭제 및 복구 방법

제1절 디지털 파일의 삭제

앞서 살펴본 바와 같이 디지털 파일은 클러스터(Cluster) 단위로 저장되고, 파일시스템 구조 상에서 삭제 명령시 메타데이터만 일부 수정하는 것이 데이터 영역 전체, 클러스터 전부를 삭제하는 것보다 간이하고, 하드디스크에 수시로 파일 쓰기, 삭제가 반복된다면 굳이 삭제 시 데이터 영역을 지우는 것이 비효율적이기 때문에 파일을 삭제하면 메타데이터에 삭제되었음을 표시만 할 뿐 나머지 파일 정보 및 데이터 영역의 파일 내용은 다른 파일에 의해 덮어쓰기가 되기 전까지 그대로 남아있게 된다.

제2절 삭제된 디지털 파일의 복구 원리

디지털 파일을 삭제한 경우, 파일정보를 담고 있던 메타데이터에 '저장매체의 공간이 필요하면 새롭게 할당 가능하다'(비할당영역) 표시만 바뀌는 것이기 때문에 메타데이터 영역에서 삭제되었다고 표기된 것을 찾아 원상복구를 하는 것이 복구의 기초이다. 즉, 데이터 영역(body data, 파일의 내용)은 남아있고 메타데이터 영역의 파일 정보만 삭제된 것으로 표시되는 것이므로 삭제표시만 정상으로 변경해 주고, 만약 메타데이터의 복구가 어려운 경우에는 데이터 영역에

저장된 기존 데이터에 직접 접근하여 삭제된 데이터를 복구한다.

앞서 살펴본 바와 같이 파일 시스템은 하드 드라이브에 있는 공간을 할당영역과 비할당영역으로 분류되는데, 할당영역은 컴퓨터가 사용 중에 있고 기록 및 유지하고 있는 데이터를 의미하고, 비할당영역은 하드디스크상 현재 파일이 할당되지 않은 공간으로, 다른 파일에 의해 덮어씌워지지 않아 예전 데이터가 그대로 남아있을 수 있다(파일이 삭제되면 파일에 대응되는 메터데이터 엔트리만 비할당상태로 변경되는 것이 아니라 파일에 대응하는 해당 데이터 유닛들도 비할당상태로 변경된다. 이 경우 해당 데이터 유닛의 내용은 지워지지 않는다.) 하드디스크의 비할당영역에는 잠재적 증거가 남아있을 수 있고, 디지털포렌식 관점에서 하드디스크의 할당영역뿐만 아니라 비할당영역의 데이터를 분석하는 것은 삭제된 데이터를 조사할 수 있다는 점에서 의미가 있다.

제3절 삭제된 디지털 파일의 복구 방법

1. 포렌식 소프트웨어를 이용한 파일 복구

컴퓨터 포렌식 소프트웨어로 Guidance Software의 Encase, AccessData의 FTK(Forensic Tool Kit), 국가보안기술연구소(대검찰청 공동개발)의 CFT(Computer Forensic Tool), X-ways의 X-Ways Forensic, WinHex, R-Tools Technology의 R-Studio, Piriform의 Recuva 등 다양한 프로그램이 존재한다. 이러한 포렌식 소프트웨어 프로그램을 사용하여 삭제된 파일을 복구할 수 있다. 이러한 소프트웨어를 이용하면 파일 복구를 위한 특별한 절차를 실행할 필요가 없어 삭제된 파일을 손쉽게 찾아낼 수 있다.

검찰은 과거 Encase 프로그램을 사용하다가 국가보안기술연구소와 CFT 프로그램을 개발하면서 CFT를 주로 사용하면서 다양한 프로그램을 상호 보완하며 사용하고 있다. Encase 프로그램은 이미지 파일의 해시값을 확인할 수 있고, CFT 프로그램은 이미지 파일뿐만 아니라 이미지 파일에 포함된 개별 디지털 파일의 해시값까지 확인할 수 있다. 또한 CFT 프로그램에서는 디지털 파일의 삭제 여부와 관련하여 'is delected' 항목에서 'TRUE, FALSE'로 구분되어 삭제 후 복구된 파일인지 여부를 알 수 있다.

2. 메타 정보를 이용한 파일 복구

메타 정보를 이용한 파일 복구는 복구를 위해 파일시스템의 메타 정보를 이용한다. 앞서 살펴본 바와 같이 파일 시스템은 다수의 파일을 효과적으로 관리하기 위해 파일명, 크기, 위치, 특성 등을 메타 영역에 구조적으로 저장한다. 그리고 실제 파일의 내용 데이터는 데이터 영역에 저장된다.

일반적인 파일시스템은 파일 삭제 작업이 발생하면 파일의 실제 데이터를 지우는 것이 아니라 메타 영역의 일부 정보만 변경하여 파일이 삭제되었다는 것을 표시하는 것이기 때문에 삭제된 파일의 메타 영역이 새로운 파일로 덮어써지지 않는다면 메타 영역의 파일 위치 및 크기 정보를 이용해 데이터 영역에 저장된 파일의 실제 데이터를 비교적 쉽게 획득할 수 있다. 이렇듯 파일시스템의 메타정보를 이용하여 파일을 복구하는 기법을 메타 정보를 이용한 파일 복구라 한다.[38]

38) 이상진·김진국·방정흠, "디지털 포렌식 관점의 데이터 복구 및 분석 프레임워크", 한국정보처리학회, 한국정보처리학회논문지 17(5), 2010

3. 데이터 카빙 복구

데이터 카빙 복구는 파일시스템의 특성을 이용하는 것이 아니라 파일의 특성을 이용하는 것이다. 파일이 삭제된 후 메타 영역에 존재하는 파일 정보까지 삭제된 경우 파일의 위치, 크기 등을 알 수 없기 때문에 더 이상 파일시스템이 제공해 주는 정보는 사용하기 어렵다. 이 경우에는 데이터 영역에서 현재 사용되지 않는 영역(비할당영역)을 복구하고자 하는 특성을 이용해 복구할 수 있는데, 비할당영역에 있는 삭제된 파일의 조각을 찾아 이를 전자적으로 조합하는 것으로, 이러한 기법을 데이터 카빙 복구라 한다.

일반적으로 데이터 카빙 복구는 파일이 조각나지 않은 경우에 복구하는 기법과 조각난 경우에 복구하는 기법으로 나눌 수 있다. 조각나지 않은 파일 카빙 기법은 헤더/푸터 시그니처를 이용하거나 램슬랙(Ram Slack)을 이용하여 복구하는 기법이다.[39] 조각난 파일 카빙 기법은 파일 구조체, 내용 엔트로피에 기반하여 복구하는 방법으로 아직까지 가능한 포맷이 제한이고 많은 시간이 요구된다.[40]

제4절 실무상 삭제 파일 복구 및 압수 절차

1. 디스트 이미징[41]

디스크 이미징은 원본 정보저장매체(또는 정보저장매체 내 파일)과

39) 김진국·이승봉·방정흠·방제완·이상진, “파일카빙 기법에 한 연구”, 디지털 포렌식연구 2호, 2008. 6.

40) Joachim Metz, Bas Kloet and Robert-Jan Mora, “Analysis of 2007 DFRWS Forensic Carving Chllenge - The 07 smart carving approach,” Digital Forensic Research Workshop (DFRWS), July, 2007.

41) 노명선·구희진·김영철·배대한·최대건·최우석, “디지털포렌식 이론”, 미디어북. 2018, 107면

정확히 똑같은 사본을 만드는 것을 가리킨다. 대검찰청은 예규에서 '포렌식 이미지'(이하 '이미지 파일'란 법률적으로 유효한 증거로 사용될 수 있도록 '정보저장매체 등에 저장된 전자정보를 포렌식 도구를 사용하여 비트열 방식으로 동일하게 복사하여 생성한 파일'로 정의하고 있다.[42)]

디스크 이미징은 Disk to Disk 방식의 하드카피(복제, Duplication), Disk to File 방식의 이미징(Imaging), File to File 방식의 복사(Copy)가 존재하고, 이미징에는 물리 이미징과 논리 이미징이 있다.

물리 이미징은 원본 정보저장매체의 모든 물리적인 섹터를 파일 형태로 만드는 방식으로, 모든 물리적 데이터를 bit-by-bit로 복사하여 완벽히 동일한 사본을 만든다. *.dd(disk dump)와 *.EWF(Expert Witness Compression format)와 같은 특정한 포맷의 이미지 파일로 변환하여 저장한다. 탐색기로 확인할 수 있는 파일과 디렉터리 구조 이외에 슬랙 공간과 비할당영역까지 모두 저장된다.

논리 이미징은 물리 이미징과 달리 사건 관련 파일과 폴더 또는 비할당 영역에서 복구한 데이터만을 선별하여 이미징하는 것을 말한다. 단순 파일 복사와는 달리 저장매체에 저장된 파일명, 시간 정보(생성, 수정, 접근, MFT Entry 변경 시간), 저장경로, 해시값, 파일 크기, 권한 정보 등 메타데이터를 포함한 모든 정보를 복제하는 방법이다. 이 경우 하드디스크에서 사용하지 않는 공간인 Unused Area, 볼륨 슬랙(Volume Slack), 숨겨진 공간(HPA, Host Protected Area 등)은

---

42) 디지털 증거의 수집·분석 및 관리 규정(대검찰청 예규 제991호)
제3조(정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.
6. "포렌식 이미지"(이하 '이미지 파일'이라고 한다)란 법률적으로 유효한 증거로 사용될 수 있도록 정보저장매체 등에 저장된 전자정보를 포렌식 도구를 사용하여 비트열 방식으로 동일하게 복사하여 생성한 파일을 말한다.

복제하지 않는다. 따라서 정밀분석이 필요한 사건의 경우 물리 이미징이 더 적절하다.

2. CFT, Encase 등 프로그램을 통한 복구 및 선별 파일 등록

실무에서는 물리 이미징과 논리 이미징이 혼용되어 사용되고 있다. 주로 회사 등 대규모의 장소를 압수수색하는 경우 선별 대상이 되는 정보저장매체가 많기 때문에 현장용 도구인 CFT(Computer Forensic Tool) 프로그램을 이용하여 사건 관련 키워드, 파일생성일자 등 다양한 조건을 검색하여 현장에서 관련성이 있는 전자정보를 선별한 후 논리 이미징하는 방식이 사용되고 있고, 개인의 PC, USB, 외장하드 등은 물리 이미징 후 선별하는 방식이 사용되고 있다.

구체적으로 CFT 프로그램을 사용하여 선별 이미징하는 방법을 살펴보면, ① CFT 프로그램이 저장된 USB를 대상 PC에 연결하여 저장매체 내 파일들을 문서파일, 이메일, 압축파일 등 파일 유형에 따라 자동 분류하고, ② 압수대상 가능성이 있는 파일을 지정하여 북마크(Add Bookmark)로 이동하며, ③ 북마크에 이동된 파일들 중 키워드를 입력, 수색 대상 파일들 제한, 파일 생성일시 등으로 제한하는 등 방법으로 전자정보의 범위를 압축하고, ④ 위와 같이 키워드 검색 등 다양한 조건으로 압축된 파일들을 최종 선별한 다음 복제(논리이미징)한 후, ⑤ 자동생성된 해시값을 피압수자 등에게 확인시킨 후 피압수자 등의 서명·날인을 받고, 전자정보 상세목록은 대상 PC, 노트북 등 디지털기기의 바탕화면에 파일로 저장해 두는 방법으로 피압수자에게 교부한다.

다음으로, 물리 이미징을 하는 경우를 살펴보면, 정보저장매체 자체나 전체를 물리 이미징한 후, ① 하드카피·이미징, ② 전자정보 탐색, ③

전자정보 복제·출력으로 참관 범위를 세분화하여 참관 여부를 확인받고, 피압수자의 의사에 따라 참관을 하거나 참관을 하지 않고 디지털 파일들을 최종 선별한 다음 피압수자 등에게 전자정보 상세목록을 교부하거나 이메일 등으로 전송해 주고 있다.

디지털포렌직 수사관은 최종적으로 선별한 디지털 파일을 디지털수사통합업무관리시스템(DFIS Ⅱ)에 등록하고, 사건을 수사하는 검사와 수사관은 위 통합디지털증거분석시스템에 접속하여 최종적으로 선별되어 압수된 디지털 파일을 확인하여 수사하고 있다.

그런데 삭제 후 복구된 디지털 파일을 압수하는 방법으로는 2가지 경우를 가정할 수 있다. 정보저장매체에서 삭제된 디지털 파일들을 복구한 후 선별하여 관련성이 있는 복구된 디지털 파일들만을 논리이미징하여 압수하는 방법('복구 후 선별 압수 방법'이라 한다)과 정보저장매체 자체를 물리이미징한 후 삭제된 디지털 파일들을 복구한 이후에 선별하여 압수하는 방법('전체 이미징 후 복구 및 선별 압수 방법'이라 한다)이 존재한다.

법원은 원칙적으로 저장매체의 소재지에서 수색·검증 후 혐의사실과 관련된 전자정보만을 범위를 정하여 문서로 출력하거나 수사기관이 휴대한 저장매체에 복제하는 방법으로 압수할 수 있다고 하면서, ① 피압수자 등이 협조하지 않거나 협조를 기대할 수 없는 경우, ② 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견되는 경우, ③ 출력·복사에 의한 집행이 피압수자 등의 영업활동이나 사생활의 평온을 침해하는 경우, ④ 기타 이에 준하는 경우 등 출력·복사에 의한 집행이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 경우에 한하여 저장매체 전부를 하드카피 또는 이미징 방법으로 복제하는 것이 허용된다고 보고,

압수·수색·검증영장의 별지에 기재하였다.

압수 대상 및 방법의 제한

1. 문서에 대한 압수

가. 해당 문서가 몰수 대상물인 경우, 그 원본을 압수함.

나. 해당 문서가 증거물인 경우, 피압수자 또는 참여인[1](이하 '피압수자 등'이라 한다)의 확인 아래 사본하는 방법으로 압수함 (다만, 사본 작성이 불가능하거나 협조를 얻을 수 없는 경우 또는 문서의 형상, 재질 등에 증거가치가 있어 원본의 압수가 필요한 경우에는 원본을 압수할 수 있음).

다. 원본을 압수하였더라도 원본의 압수를 계속할 필요가 없는 경우에는 사본 후 즉시 반환하여야 함.

2. 컴퓨터용 디스크 등 정보저장매체에 저장된 전자정보에 대한 압수・수색・검증

가. 전자정보의 수색・검증

수색·검증만으로 수사의 목적을 달성할 수 있는 경우, 압수 없이 수색·검증만 함.

나. 전자정보의 압수

(1) **원칙** : 저장매체의 소재지에서 수색·검증 후 **혐의사실과 관련된 전자정보만을 범위를 정하여 문서로 출력하거나 수사기관이 휴대한 저장매체에 복제하는 방법으로 압수할 수 있음.**

(2) **저장매체 자체를 반출하거나 하드카피·이미징 등 형태로 반출할 수 있는 경우**

(가) 저장매체 소재지에서 하드카피·이미징 등 형태(이하 "복제본"이라 함)로 반출하는 경우

– 혐의사실과 관련된 전자정보의 범위를 정하여 출력·복제하는 위 (1)항 기재의 원칙적 압수 방법이 불가능하거나, 압수 목적을 달성하기에 현저히 곤란한 경우[2]에 한하여, 저장매체에 들어 있는 전자파일 전부를 하드카피·이미징하여 그 복제본을 외부로 반출할 수 있음.

(나) 저장매체의 원본 반출이 허용되는 경우

1) 위 (가)항에 따라 집행현장에서 저장매체의 복제본 획득이 불가능하거나 현저히 곤란할 때[3]에 한하여, 피압수자 등의 참여 하에 저장매체 원본을 봉인하여 저장매체의 소재지 이외의 장소로 반출할 수 있음.

2) 위 1)항에 따라 저장매체 원본을 반출한 때에는 피압수자 등의 참여권을 보장한 가운데 원본을 개봉하여 복제본을 획득할 수 있고, 그 경우 원본은 지체 없이 반환하되, 특별한 사정이 없는 한 원본 반출일로부터 10일을 도과하여서는 아니됨.

(다) 위 (가), (나)항에 의한 저장매체 원본 또는 복제본에 대하여는, 혐의사실과 관련된 전자정보만을 출력 또는 복제하여야 하고, 전자정보의 복구나 분석을 하는 경우 신뢰성과 전문성을 담보할 수 있는 방법에 의하여야 함.

(3) **전자정보 압수시 주의사항**

(가) 위 (1), (2) 항에 따라 혐의사실과 관련된 전자정보의 탐색·복제·출력이 완료된 후에는 지체 없이, 피압수자 등에게 **① 압수 대상 전자정보의 상세목록을 교부하여야 하고, ② 그 목록에서 제외된 전자정보는 삭제·폐기 또는 반환하고 그 취지를 통지하여야 함**[위 상세목록에 삭제·폐기하였다는 취지를 명시함으로써 통지에 갈음할 수 있음].

(나) 봉인 및 개봉은 물리적인 방법 또는 수사기관과 피압수자 등 쌍방이 암호를 설정하는 방법 등에 의할 수 있고, 복제본을 획득하거나 개별 전자정보를 복제할 때에는 해시 함수값의 확인이나 압수·수색과정의 촬영 등 원본과의 동일성을 확인할 수 있는 방법을 취하여야 함.

(다) **압수·수색의 전체 과정(복제본의 획득, 저장매체 또는 복제본에 대한 탐색·복제·출력 과정 포함)에 걸쳐 피압수자 등의 참여권이 보장되어야 하며**, 참여를 거부하는 경우에는 신뢰성과 전문성을 담보할 수 있는 상당한 방법으로 압수·수색이 이루어져야 함.

---

1) **피압수자** – 피의자나 변호인, 소유자, 소지자 // **참여인** – 형사소송법 제123조에 정한 참여인

2) ① 피압수자 등이 협조하지 않거나, 협조를 기대할 수 없는 경우, ② 혐의사실과 관련될 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 말한다.

3) ① 집행현장에서의 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 말한다.

그림 3. 2015. 8.부터 사용된 법원의 압수·수색·검증영장 별지

따라서 디지털 파일의 삭제된 경우, 정보저장매체 자체를 하드카피·이미징 등 형태로 반출할 수 있는 위 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견되는 경우에 해당되므로, 앞에서 설시한 압수·수색의 위 2가지 방법이 모두 허용된다고 하겠다. 또한 데이터 카빙 복구 등은 많은 시간이 소요되는 복구 방법으로 위와 같은 복구가 필요한 경우에는 저장매체 소재지에서 압수가 불가능하여 저장매체 자체를 반출하거나 하드카피·이미징 등 형태로 반출할 수 밖에 없다고 보아야 한다.

그런데 아래에서 살펴보는 바와 같이 압수·수색의 방법에 따라 해시값 비교의 대상, 증거능력 인정 요건과 관련된 입증방법 및 그 정도가 달라진다.

피압수자는 증거인멸의 의사로 혐의사실과 관련될 개연성이 있는 전자정보를 삭제하였을 수 있고, 일상적인 삭제의 일환이었을 수도 있다. 예외적으로 정보저장매체 자체의 하드카피·이미징 등 형태로 반출이 허용되는 전자정보 삭제·폐기 정황에 위 2가지 경우가 모두 포함되는지 문제될 수 있으나, 혐의사실과 관련될 개연성이 있는 전자정보가 삭제·폐기된 정황이 발견된 경우 디지털포렌식 수사관이 집행현장에서 이를 구분하는 것은 굉장히 어렵고, 물리적 증거를 압수하는 경우에도 증거를 발견하기 위한 압수장소에 대한 광범위한 수색이 가능하며, 정보저장매체 자체를 하드카피·이미징 등 형태로 반출한 이후 선별하여 관련성이 있는 정보들을 압수하기 때문에 모두 포함된다고 해석하는 것이 바람직한 것으로 보인다.

3. 이미지 파일의 보관 또는 삭제

디지털포렌식 수사관은 최종적으로 사건과 관련성이 인정되는

전자정보만을 선별하여 이를 디지털수사통합업무관리시스템에 등록하고, 전자정보 전부에 대하여 생성한 이미지 파일을 삭제한다.

그러나 사건 관련 전자정보를 선별하여 압수하는 과정에서 발생하는 전자정보의 변경·손실이 증거가치를 훼손할 우려가 있는 경우에는 이미지 파일을 삭제하지 않도록 한다.[43]

앞서 살펴본 바와 같이 삭제 후 복구된 디지털 파일을 압수하는 방법으로는 정보저장매체에서 삭제된 디지털 파일들을 복구한 후 선별하여 관련성이 있는 복구된 디지털 파일들만을 이미징하여 압수하는 방법과 정보저장매체 자체를 이미징한 후 삭제된 디지털 파일들을 복구한 이후에 선별하여 압수하는 방법이 존재한다.

전자의 경우의 이미지 파일은 삭제 후 복구된 디지털 파일들만을 이미징한 것이기 때문에 사건과 관련성이 없는 정보들이 저장되어 있지 않고, 이미지 파일 자체를 압수의 대상으로 볼 수 있다.

그러나 후자의 경우의 이미지 파일은 정보저장매체 전체를 이미징하였기 때문에 사건과 관련성이 없는 정보들도 저장되어 있고, 추후 위 이미지 파일에서 관련성이 있는 정보들을 수색한 후 선별하여 압수하게 된다. 위 이미지 파일은 정보저장매체 전체가 이미징된

---

43) 디지털 증거의 수집·분석 및 관리 규정(대검찰청 예규 제991호)

제24조 (이미지 파일 등의 등록)

① 제18조제1항에 따라 생성된 이미지 파일과 증거파일(이하 '이미지 파일 등'이라고 한다) 및 제23조에 따라 생성된 이미지 파일은 다음 각 호의 구분에 따라 업무관리시스템에 등록한다. 다만, 정보저장매체 등으로부터 기억된 전자정보 전부에 대하여 생성한 이미지 파일의 등록은 다음 각 호의 절차에 따른다.

1. 정보저장매체 등으로부터 기억된 전자정보 전부에 대하여 생성한 이미지 파일을 업무관리시스템에 등록한다.
2. 제1호와 같이 생성한 이미지 파일에서 사건과 관련성이 인정되는 전자정보만을 선별하여 이미지 파일을 생성한 경우에는 제1호에 따라 등록된 이미지 파일을 삭제하고 선별하여 생성한 이미지 파일을 등록한다.
3. 제2호에도 불구하고 사건관련 전자정보를 선별하여 압수하는 과정에서 발생하는 전자정보의 변경·손실이 증거가치를 훼손할 우려가 있는 경우에는 제1호에 따라 등록된 이미지 파일을 삭제하지 않도록 한다.

것이기 때문에 선별하여 압수하는 작업이 종료된 이후 이를 삭제하는 것이 원칙이나, 아래에서 살펴보는 바와 같이 삭제 후 복구된 파일의 증거능력을 입증하기 위한 방법으로 재현가능성, 부수데이터의 분석 등을 증명하기 위해서는 위 이미지 파일이 필요하여 디지털 증거의 수집·분석 및 관리 규정에서도 위와 같은 경우 예외적으로 이미지 파일을 삭제하지 않도록 규정하고 있다.

그런데 정보저장매체 전체를 이미징한 경우 위와 같이 관련성이 없는 정보들도 포함되어 있기 때문에 정보저장매체 전체 이미지 파일 보관이 문제될 여지가 있다. 위 이미지 파일은 대검찰청에 별도로 보관되고 사건을 수사하는 검사와 수사관이 별개의 절차를 거치지 않고 접근할 수 없고, 전문적인 디지털 증거 분석 도구를 이용하지 않고 이미지 파일 안에 있는 개별 디지털 파일을 가시화·가독화할 수 없기는 하지만, 법원의 증거보전 절차 등을 이용하거나 법원 또는 제3의 기관에 이를 보관하고 증거능력이 문제될 때 이를 활용할 수 있는 방법을 규정하거나 암호화 등으로 피압수자의 기본권 침해를 최소화하는 방안을 고려하는 것도 바람직할 것으로 생각된다.

IV. 삭제 후 복구된 디지털 파일의 증거능력 인정 요건

제1장 기존 실무 및 판례의 태도와 문제점

디지털 포렌식 절차 중 복구 절차는 독특하다. 의도적이든, 비의도적이든 논리적으로 응용소프트웨어에서는 더 이상 관련 데이터로 인식될 수 없도록 삭제·손상시킨 파일일지라도 일정한 조건하에서는 저장매체의 일정한 부분, 예컨대 데이터 저장 공간, Slack Space 등에 남아 있게 되고 그것이 만약 증거가치가 있다면 분석과정에서 되살려 증거로 사용하게 된다. 즉, 잠재적 증거를 현실화시키는 절차인 것이다.[44]

삭제 후 복구된 디지털 파일의 경우, 일반인의 입장에서 정보저장매체에 저장된 디지털 파일이 삭제에 의하여 사라졌고, 수사기관이 정보저장매체에 어떠한 조작을 가하여 삭제된 디지털 파일을 되살려낸 것이라고 생각하기 쉽다. 그래서 삭제되기 전 정보저장매체에 저장되어 있던 개별 디지털 파일을 원본이라고 생각한다면, 삭제 처리 전 디지털 파일은 존재하지 않으므로 원본과의 동일성, 무결성을 증명할 대상이 부존재하는 문제가 생겨난다.

나아가 무결성과 동일성의 측면에서 디지털 증거가 획득, 증거제출까지의 모든 과정에서 변경되지 않았음과 해당 디지털 증거가 피압수자의 저장매체에서 획득된 데이터임을 입증해야 한다. 판례는 원칙적으로 해시값을 비교하는 방법을 이용하고, 예외적으로 증언, 감정 및 검증 등의 방법으로 종합적으로 판단하고 있다.

삭제 후 복구된 디지털 파일의 경우, 복구된 이후의 디지털 파일에

44) 탁희성, “전자증거에 관한 연구”, 박사학위논문, 이화여자대학교, 2004, 193면

대하여는 종전과 동일한 방법으로 동일성, 무결성을 증명할 수 있다. 그런데 삭제되기 전 디지털 파일을 원본으로 본다면, 판례에서 동일성, 무결성의 입증방법으로 여겨지는 개별 디지털 파일의 해시값 비교가 불가능하고, 복구 과정이 문제된다면 이를 증명하는 방법이 문제된다.

현재까지 삭제 후 복구된 파일의 증거능력에 대해 명시적으로 판결한 판례가 존재하지 않는다. 그렇다면 삭제 후 복구된 디지털 파일의 경우 무엇을 원본으로 볼 것인지, 어떠한 방법 또는 요건 하에 삭제 후 복구된 파일의 증거능력을 인정할 것인지 여부에 대해서 살펴보도록 하겠다.

제2장 미국 판례의 태도

제1절 복구, 복제절차의 진정성 문제

미국에서 1996.경 Gates Rubber Co v. Bando Chemical Indus., Ltd 사건[45]에서는 법원은 소송당사자 혹은 잠재적인 소송당사자가 적정한 컴퓨터 포렌식 조사를 수행해야 할 법적 책임이 있다고 하면서, 한쪽 당사자의 분석관은 하드 디스크 매체의 이미지 복사본을 만드는데 실패하였고 대신 파일 복사 방식을 수행하였는데, 그 결과 중요한 정보의 손실을 입는 결과를 야기하였다. 반대 당사자는 당시인 1992. 2.경에도 이미지 복사본을 만드는 기술이 가능하였다는 점에 주의하였고 법원은 이미지 복사에 실패한 분석관을 비난하면서 당사자들은 법적 증거 분석과 제출에 필요한 기법들이 정확한 결과를 가져오도록 할 책임이 있다고 하였다.

45) Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90(D.C. Col., 1996).

한편 Bray v. Bi-State Development Corp. 사건[46]에서는 전문 분석관은 사용한 컴퓨터 소프트웨어의 신뢰성을 입증할만한 충분한 입증자료를 증언해야 한다고 판시하고 있다. 삭제된 증거의 복구 등에 있어서 입력 자료와 결과간의 연관성·정확성이 입증되어야만 증거 자체의 진정성을 인정할 수 있다는 것이다.

이렇듯 미국에서는 판결을 통하여 특별한 응용 소프트웨어를 사용하여 증거 복구 기타의 작업을 수행하여 증거로 제출한 경우 응용 소프트웨어의 성능과 기능에 대한 전문가들의 증언, 자료 등 간접적인 방법을 통해 그 진정성을 인정하고 있다.[47]

제2절 신뢰성의 문제

1. 포렌식 도구의 유효성

피고인 측에서 디지털 증거를 분석하는데 사용된 장비나 컴퓨터 프로그램의 신뢰성에 의문을 제기할 경우에 어떤 과정을 통해서 그 신뢰성이 입증되어야 하며 분석관은 그 신뢰성을 입증하기 위해 어떻게 해야 하는지 여부가 문제된다.

미 연방대법원은 Daubert v. Merrel Dow(1993) 판결[48]에서

46) Bray v. Bi-State Development Corp., 949 S.W.2d 93(1997).

47) 김현선, “미국의 디지털 증거 활용 실태”, 해외연구검사 연구논문, 2008, 68면

48) Daubert는 선천적 장애를 가진 아이의 엄마로서, 임신중 복용한 Merrell Dow사의 anti-nausea(임신중 헛구역질 방지) 약물인 Bendectin에 의해 아이의 장애가 초래되었으며, Bendectin의 포장지에는 임산부에 대한 경고나 복용금지 등의 문구가 인쇄되어 있지 않았다는 이유로 Merrell Dow 사를 상대로 소송을 제기했다. 이에 대해 Merrell Dow 사는 Bendectin이 아이의 장애를 초래하지 않았다고 주장하면서 Dr. Steve H. Lamm을 전문가 증인으로 진술하게 하였다. Dr. S.H. Lamm은 Bendectin과 인간의 선천성 기형에 관한 다양한 연구 문헌을 검토한 결과, 임신초기단계에서 Bendectin의 복용이 태아의 건강에 위험을 초래한다고 예측되지 않는다고 진술하였다. 이에 대하여 Daubert 측은 약리학·병리학·생리학 등 전문가 8인을 통해 실험실에서의 물질반응 테스트와 동물에 대한 임상실험결과 Bendectin이 기형을 유발시킬 수 있는 화학물질과 구성성분 및 화학적 구조가 유사하다

연방규칙하에서 법관은 과학적 증거에 대하여 관련성뿐만 아니라 신뢰성도 확보할 수 있어야 한다고 전제하면서, 다음과 같은 4가지의 기준을 사용하여 과학적 증거의 허용성을 판단하였다. 첫째, 그 이론이나 기술이 검증될 수 있는지, 그리고 검증되었는지의 여부, 둘째, 거기에 잘 알려진 혹은 잠재적인 오류율이 있는지, 그리고 기술의 운용을 통제하는 기준이 존재하는지, 지속되고 있는지의 여부, 셋째, 그 이론이나 기술이 비평과 발표의 관심대상이 되는지의 여부, 넷째, 그 이론이나 기술이 관련된 과학적 커뮤니티 내에서 광범위한 승인을 받고 있는 것인지 여부가 그것이다.

Daubert test는 현재 미국에 있어서 과학적 증거의 허용성 여부와 관련하여 보편적인 신뢰성 판단기준으로 확고히 자리잡고 있다.

2. 디지털 증거 분석관(Forensic Examiner or Investigator)의 전문성 검증

증거분석을 수행한 사람이 사람이 전문적인 지식을 바탕으로 적절한 자격을 갖춘 사람인지의 문제이다. 미연방증거규칙 제702조는 “만약 과학적, 기술적, 다른 전문적인 지식이 사실인정권자가 증거를

는 약리학적 검사결과 그리고 Merrell Dow사가 제시한 임상실험결과를 재분석한 결과를 토대로, Bendectin과 기형아 출산가능성에 대한 상관성을 긍정하는 감정결과를 제출하였다. 법원은 Daubert의 전문가 증언이, 그것이 속한 분야에 있어서 일반적인 승인을 받았다고 하는 충분히 입증되지 못한 증거에 의거했다고 판단했다. 또한 법원은 Bendectin에 관한 의생태학분야로부터 나온 데이터에 근거를 두지 않은 전문가 의견이 배심원에게 법률상 인과관계에 관한 문제를 제기하도록 허용될 수는 없다고 판시했다. 더욱이 Daubert의 전문가 증언이 이미 이전에 출간된 의생 태학 연구로부터 얻은 데이터를 재계산했을지라도 그들의 조사결과나 분석방법이 정식으로 출간된 것이거나 논평에 준할 만한 것도 아니기 때문에 허용될 수 없다고 판단했다. 원고는 그 판결에 항소하였으나 항소법원도 Frye 판결을 인용하여 항소를 기각했다. 이에 원고가 다시 미 연방대법원에 상소를 제기하였고, 연방대법원은 원고의 상소가 이유있다고 하여 사건을 파기환송하였다. 이 판결에서 다수의견은 연방증거규칙이 Frye test를 대체하며, 과학적 증거의 허용성은 연방증거규칙을 통해 제한된다고 판시하였다.(김현선, “미국의 디지털 증거 활용 실태”, 해외연구검사 연구논문, 2008, 69면에서 재인용)

이해하거나 쟁점을 이루는 사실을 확정하는데 도움을 주는 것이라면, 지식, 기술, 경험, 훈련 또는 교육에 의한 전문가로서 자격 있는 증인은 의견의 형태로 증언할 수 있고, 만약 그렇지 않으면, (1) 증언이 충분한 사실이나 자료에 근거하고, (2) 증언이 믿을 수 있는 원칙이나 방법의 결과물이며, (3) 증인이 사실에 대해 위 원칙과 방법을 신뢰할 수 있게 적용한 경우에 의견의 형태로 증언할 수 있다"고 규정하고 있다.

또한, United States v. Scott-Emuakpor 사건[49]에서 피고는 컴퓨터 포렌식을 수행한 분석관인 미 재무성 특별수사국(USSS) 수사관의 전문성을 문제 삼았고 법원은 수사관이 자기들의 입증사실을 제출하기 위해서는 컴퓨터 과학 분야에서 자격 있는 전문가여야 할 필요가 있다고 판시한 바 있다.

제3절 원본성의 문제

디지털 증거 자체는 가시성과 가독성이 없으며 매체독립적인 정보이기 때문에 매체에 저장된 상태 그대로 매체와 함께 형사소송의 증거로 제출되는 경우보다는 가시성, 가독성 있는 형태로 변환시켜 제출하게 된다. 이 경우 증거 원본이 제출되어야 하는 증거법칙의 원칙상 제출되는 사본 증거, 그리고 가시성·가독성 있는 형태로 변환된 증거를 원본으로 인정할 수 있는가가 문제된다.

일반적인 논리적인 프로그램으로는 인식할 수 없는 슬랙스페이스에서 자료를 축출한 경우 최량증거법칙이 적용될 수 있는 여지가 있는지가 문제된다.

앞서 살펴본 바와 같이, 미국에서는 원본의 개념을 넓게 인정하고

49) United States v. Scott-Emuakpor, supra, 2000 WL 288443.

있고, 유사한 사례로 United States v. Seifert 사건[50]에서 디지털방식으로 성능이 개선된 비디오테이프가 문제가 되었는데 방화 혐의를 받고 있던 피고는 불속에서 복구된 비디오테이프를 디지털 방식으로 질을 높였을 경우 최량증거가 될 수 있는지 의문을 제기했다. 화질을 조정하기 위해 밝기나 선명도를 조정하게 되면 원본으로서의 가치를 상실하는 것이라고 주장한 것이다. 그러나 법원은 전문가에 의해 수행된 과정이 적절하다면 화질이 개선된 테이프는 원본에서 정확하게 재생산된 사본에 해당한다고 판시하였다.

또한, galaxy computer Services, INC. V. Baker 사건[51]에서 삭제 후 복구된 파일의 증거능력을 인정한 바 있다

제3장 삭제 후 복구된 디지털 파일의 원본

우리는 기존 디지털 증거의 압수·수색 및 증거능력에 대하여 물리적 증거의 관점에서 접근해 왔다. 소프트웨어 프로그램을 통하여 보고 읽을 수 있는 개별 디지털 파일을 마치 하나의 유체물인 서류와 같이 보고, 증거능력의 요건인 동일성, 무결성을 입증하는 구조를 취해 오면서 해시값 비교가 가장 중요하게 여겨졌고, 해시값 비교의 대상도 정보저장매체 전체에서 개별 디지털 파일을 단위로 점차 확장되어 왔다.

삭제 후 복구된 디지털 파일의 경우, 원본과의 동일성, 무결성을 입증하여야 하므로 무엇이 원본인지 여부가 문제된다. 디지털 증거의 개념을 살펴보면, 디지털 증거는 '디지털 형태로 저장되거나 전송되는

50) United States v. Seifert, 2005 WL44749(D.Minn. Jan 7, 2005)(김현선, "미국의 디지털 증거 활용 실태", 해외연구검사 연구논문, 2008, 73면에서 재인용)

51) galaxy computer Services, INC. V. Baker, 325 B.R.544(E.D.va.2005)

정보'를 의미하므로, 한컴오피스, Microsoft Word, Excel, Powerpoint 등 각종 소프트웨어 프로그램을 통해 보고 읽을 수 있는 개별 디지털 파일이 아니라 정보저장매체에 저장된 데이터, 정보 그 자체로 보아야 한다. 삭제 후 복구된 디지털 파일의 경우, 삭제되기 전이 아닌 삭제되고 난 이후, 압수 시점에서의 정보저장매체에 저장된 디지털 형태의 정보를 원본으로 보아야 한다.

디지털 파일을 삭제하는 경우, 디지털 파일의 삭제는 메타데이터만을 일부 수정하는 것이기 때문에 나머지 파일 정보 및 데이터 영역은 다른 파일에 의해 '덮어쓰기'가 되기 전까지 그대로 남아있게 되고, 남아있는 위 나머지 파일 정보 및 데이터 영역을 가시화·가독화하는 것이 복구이기 때문에 정보저장매체에 저장된 디지털 형태의 정보를 변경하는 것이 아니다. 데이터 중 일부가 덮어쓰기가 된 경우에도 데이터 카빙 등의 방법으로 정보저장매체에 일부 남아있는 데이터를 모아 가시화·가독화한 경우에도 정보저장매체에 남아있는 정보 자체를 변경한 것이 아니라 부분적으로 남아 있는 정보를 가시성·가독성있는 형태로 변환하기 위해 조합한 것에 불과하므로 동일하게 보아야 한다.

따라서 삭제 전 정보저장매체에 저장된 디지털 파일을 원본으로 생각하기 쉬우나, 삭제 전이 아닌 '삭제되고 난 이후의 압수 시점에서의 정보저장매체에 저장된 디지털 형태의 정보'를 원본으로 보아야 하고, 복구된 디지털 파일은 정보저장매체에 남아있는 정보를 가시화·가독화한 것에 불과하고 정보 자체를 변경시킨 것이 아니므로 원본과 동일한 사본으로 보아야 한다.

제4장 증거능력 인정 요건

제1절 디지털 증거 분석 도구의 신뢰성 검증

1. 국내 기준

한국정보통신기술협회(Telecommunications Technology Association. 이하 TTA)는 2007년부터 현재에 이르기까지 디지털포렌식과 관련하여 다양한 국가 표준을 제정하였다. 이들 중 디지털포렌식 도구들과 관련된 것은 다음과 같다.

· 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 요구사항(TTAS.KO-12.0057)

· 컴퓨터 포렌식을 위한 디지털 데이터 수집도구 검증규격(TTAK.KO-12.0075)

· 컴퓨터 포렌식을 위한 디지털 증거 분석도구 요구사항(TTAK.KO-12.0081)

· 컴퓨터 포렌식을 위한 디지털 분석도구 검증(TTAS.KO-12.0012)

2. NIST의 CFTT

미국표준기술연구소(National Institute of Standards and Technology, NIST)는 미국 상무성(Department of Commerce) 소속의 정부기관으로 디지털 포렌식 프로젝트를 국가적인 사업으로 수행하고 있다.[52)]

미국 상무부 산하의 NIST(National Institute of Standards and

52) 김민서·이상진, “윈도우 포렌식 도구의 검증용 데이터 세트의 개발”, 한국정보보호학회, 정보보호학회논문지 제25권 제6호, 2015. 12., 1,422면

Technology)에서 진행되고 있는 CFTT(Computer Forensic Tool Testing) 프로젝트는 대표적인 디지털 포렌식 도구 테스트 프로젝트로, 포렌식 조사에서 사용되는 모든 도구들에 대해 신뢰성 기준을 제공하기 위한 방법을 연구하며, NIJ(National Institute of Justice)와 법무부 산하 연구 개발 조직 및 OLES(Office of Law Enforcement Std.). ITL(Information Technology Lab.)에 의해 공동으로 진행되고 있다. 또한 FBI. 사이버 범죄 예방 센터 및 U. S Security Service를 포함한 여러 관련 기관들에 의해 지원되고 있다.

연구에 대한 결과물로는 2008년 1월에는 포렌식 수사 시 사용되는 문자열 검색 도구를 위한 요구사항들을 정의한 Forensic String Searching Tool Requirements Specification을 발행하였으며, 2009년 3월에는 삭제된 파일에 대한 인식과 복구를 위해 파일시스템의 메타데이터를 조사하는 포렌식 도구들의 요구사항을 정의한 Active File Identification & Deleted File Recovery Tool Specification 문서를 발행하였다.

이 프로젝트에서는 도구의 주요 기능을 검증 및 보장하기 위하여 각각의 도구들의 요구사항, 검증 방법 및 테스트 절차를 수립하는 것을 주된 목적으로 한다. CFTT 프로젝트를 소개하고 있는 홈페이지(www.cftt.nist.gov)에서는 디지털 증거의 수집과 관련된 기능인 디스크 이미징 기능과 증거 훼손을 방지하기 위한 쓰기 방지 기능, 증거 파일들을 복구하는 데이터 복구 기능과 증거 파일들을 검색할 수 있는 키워드 검색 기능 등이 소개되어 있고, 각각의 기능이 충족되어야 할 요구사항, 테스트 방법을 상세히 기술한 문서, 대표적인 도구들에 대한 테스트 결과 등을 공개하고 있다.

3. 국내 실험(디지털 증거 분석 도구 요구사항 및 신뢰성 검증)[53]

디지털 데이터는 변경이나 복제가 용이하다는 특수성으로 인해 적법한 형태의 증거로 인정을 받기 위해서는 이를 다루는 증거 획득 및 분석 도구가 정확하고 결정적이어야 하며 검증 가능하게 동작해야 함을 의미하다.

표준에서는 디지털 증거 분석 도구가 시스템 상에서 동작하는 소프트웨어로써 기본적으로 갖추어야 할 일반적인 요구사항 이외에도 포렌식 조사 단계에서 증거 데이터 분석을 수행하기 위한 핵심 요소 3가지에 중점을 두어 해당 기능별 요구사항을 제시하고 있다.

· 도구는 분석 대상이 되는 증거 디스크 또는 데이터 이미지 내의 모든 영역에 대해 일체 누락 없는 분석을 수행해야 한다.

· 도구는 삭제되거나 변조된 데이터 또는 파일들에 대한 탐지와 복구 기능을 제공해야 한다.

· 도구는 특정 문자열 또는 파일들을 탐색할 수 있어야 한다.

[표 1] 삭제 파일 복구 기능의 필수적인 요구사항[54]

구분	요구사항
DFR_M_01	삭제 파일 복구 기능은 도구에 의해 제공되는 문서들(사용법, 목적, 동작, 시스템 요구사항 등을 기술하는 자료들의 집합)에 의해 확인된 파일 시스템에서 복구 기능을 지원해야 한다.
DFR_M_02	삭제 파일 복구 기능은 파일 시스템 객체가 삭제된 이후에 유지되는 메타데이터에서 복구

53) 이태림·신상욱, “디지털 포렌식을 위한 증거 분석 도구의 신뢰성 검증”, 한국정보보호학회, 정보보호학회논문지 제21권 제3호, 2011. 6., 167-175면

54) 이태림·신상욱, “디지털 포렌식을 위한 증거 분석 도구의 신뢰성 검증”, 한국정보보호학회,

	가능한 모든 삭제된 파일 시스템 객체들을 식별해야 한다.
DFR_M_03	삭제 파일 복구 기능은 복구된 객체를 구성하는데 있어 발생한 오류를 보고해야 한다.
DFR_M_04	삭제 파일 복구 기능은 잔여 메타 데이터에서 각각의 삭제된 파일 시스템 객체에 대해 복구된 객체를 구성해야 한다.
DFR_M_05	각각의 복구된 객체는 잔여 메타 데이터에서 식별된 모든 할당되지 않은 데이터 블록들을 포함해야 한다.
DFR_M_06	각각의 복구된 객체는 삭제된 블록 풀로부터 데이터 블록들만으로 구성되어야 한다.

위 논문에서는 Encase 등 다양한 프로그램을 통해 MSoffice.docx 등 다양한 종류의 파일들을 복구하여 실제 복구 기능을 검증한 바 있다. 디지털 파일의 해시값은 파일의 콘텐츠를 기초로 추출되기 때문에[55] 삭제된 디지털 파일이 완전히 복구된다면 복구된 디지털 파일은 삭제 전 디지털 파일과 동일한 해시값을 가지게 되고, 일부 덮어쓰기된 부분이 있거나 완전히 복구되지 않는다면 삭제 전 디지털 파일과 다른 해시값을 가지게 된다.

4. 대검찰청의 CFT

검찰은 2010년 이래로 전자증거 압수수색 도구 CFT(Computer Forensic Tool의 약칭)를 현장에서 PC의 HDD, SSD 등에 대하여

정보보호학회논문지 제21권 제3호, 2011. 6., 168면

55) 박진환, “해시값의 비교에 의한 디지털 증거의 동일성 입증에 관한 연구”, 석사학위논문, 서울대학교, 2019, 63면

증거획득시에 널리 사용하고 있다. 국가보안기술연구소(NSR)가 2007년부터 개발하기 시작하였고 2009. 7. 검찰에 제공한 이래로 지금도 업그레이드를 담당하고 있다.

CFT(version 3. 4. 1)는 2018. 2. 미국의 CFTT 프로그램을 통해 이미징에 대하여 테스트를 받았다. 5가지 경우의 테스트 결과가 완료(completed)되었다.

[표 2] Selected Test Cases[56)]

Case	Description	Status
FT-DI-01-SATA28	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-01-SATA48	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately and correctly hash the data while creating an image file.	completed
FT-DI-01-USB	Acquire drive of a given type using a given write blocker connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given drive type accurately	completed

56) Test Results(Federated Testing) for Disk Imaging Tool : Computer Forensic Tool(CFT) version 3. 4. 1.(February 2018)

	and correctly hash the data while creating an image file.	
FT-DI-03-SD	Acquire removable media of a given type using a given media reader connected to a computer with a given interface to an image file and compute selected hashes for the acquired data. Test the ability to read a given removable media type accurately and correctly hash the data while creating an image file.	completed
FT-DI-05-NTFS	Acquire partition of a given type to an image file and compute given partition type accurately and correctly hash the data while creating an image file.	completed
FT-DI-13	Compute the hash value of the acquired data within an image file. Test the ability of the tool to recompute the hash of an existing	completed

5. Encase 등 프로그램

ILooKIX v.2.2.3.1.151, The Sleuth kit(TSK)/Autopsy v3.2.2./2.24, X-ways Forensicx v16.0 SR-4, Linux v2011-02-02, Encase Forensics v6.18.0.59, FTK v.3.3.0.33124는 미국의 CFTT 프로그램을 통해 삭제된 파일 복구에 대하여 테스트를 받았다.[57]

제2절 디지털 포렌식 수사관의 법정 증언

57) Test Results for Delected File Recovery and Active File Listing Tools[ILooKIX v2.2.3.151.(9/22/2014), The Sleuth Kit(TSK)/Autopsy v3.2.2.(7/2/2014), X-ways Forensics v16.0 SR-4(7/2/2014), SMART for Linux v2011-02-02, Encase Forensic v6.18.0.59(6/23/2014), FTK v3.3.0.33124(6/23/2014)](www.cftt.niv.gov)

우리 법원은 일심회 사건[58]에서 “법원의 검증절차에 참여하여 이를 주도적으로 진행한 증인 정○○의 전자적 정보 분석능력과 그 증언은 신뢰할 수 없으므로, 위 문건들은 독립적인 증거로 사용할 수 없다”는 피고인 측의 주장에 대해서 “이 법원의 검증조서, 증인 정○○의 증언 및 기타 이 사건 변론에 나타난 제반 사정을 종합하면, … 피고인들 및 검사, 변호인들이 모두 참여한 가운데 이 법원의 전자법정시설 및 Encase 프로그램을 이용하여 법원의 검증절차가 이루어졌는바, 검증 당시 규격에 적합한 컴퓨터와 Encase 프로그램을 이용하여 적절한 방법으로 검증절차가 진행되었으므로, 컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력, 처리, 출력의 각 단계에서의 컴퓨터 처리과정의 정확성, 조작자의 전문적 기술능력 등의 요건이 구비되었다고 보이고, 달리 그 요건의 흠결을 의심하거나 신뢰성을 배척할 만한 사정은 보이지 아니하며, 위와 같은 검증절차를 거쳐, 디지털 저장매체 원본을 이미징한 파일에 수록된 컴퓨터파일의 내용물이 압수물인 디지털 저장매체로부터 수사기관이 출력하여 제출한 문건들에 기재된 것과 동일하다는 점이 확인되었으므로, 앞서 본 ‘증거의 요지’란에 거시된 문건들은 증거능력이 적법하게 부여되었다고 할 것이어서 변호인들의 이 부분 주장은 이유 없다”고 하여 사건 담당 디지털 포렌식 수사관의 사용도구와 엔케이스 프로그램 등에 관한 전문적인 증언능력과 증언에 대한 독립한 증거로서의 가치를 인정하였다.[59]

다만, 위 판례에서는 “각 디지털 저장매체가 봉인된 상태에서 서울중앙지방검찰청에 송치된 후 피고인들이 입회한 상태에서 봉인을

58) 서울중앙지방법원 2007. 4. 16. 선고 2006고합1365 판결

59) 천영준, “디지털 포렌식 수사관의 법정증언과 분석결과의 신뢰성 확보 방안 연구”, 석사학위 논문, 서울대학교, 2017, 30-31면

풀고 세계적으로 인정받는 프로그램을 이용하여 이미징 작업을 하였는데, 디지털 저장매체 원본의 해쉬(Hash) 값과 이미징 파일을 통해 생성된 파일의 해쉬값이 동일한 사실, 제1심 법원은 피고인들 및 검사, 변호인이 모두 참여한 가운데 검증을 실시하여 이미징 작업을 통해 생성된 파일의 내용과 출력된 문건에 기재된 내용이 동일함을 확인한 사실을 알 수 있는바, 그렇다면 출력된 문건은 압수된 디지털 저장매체 원본에 저장되었던 내용과 동일한 것으로 인정할 수 있어 증거로 사용할 수 있다"고 하여 삭제 후 복구된 디지털 파일에 대한 것은 아니었다.

삭제 후 복구된 파일의 경우 원본과 사본의 동일성에 대한 증명뿐만 아니라 정보저장매체에서 디지털 파일이 삭제되었고, 이를 과학적 방법으로 복구하였다는 것을 추가적으로 입증하여야 하는바, 이는 재현가능성에서 후술하겠다.

제3절 재현가능성

일반적으로 재현성(Reproducibility)의 원칙이란, 동일한 조건과 동일한 상황 아래에서의 디지털포렌식의 분석 결과는 항상 같은 결과가 나와야 한다는 원칙이다. A라는 분석관이 Encase를 사용하여 얻은 분석결과는 FTK를 이용하여 분석해도 동일한 결과가 나와야 하고, B라는 분석관이 Encase를 사용하여 분석해도 같은 결과가 나와야 한다는 원칙이다.[60]

그러나 파일 이미징이나 복제와는 다르게, 삭제된 파일의 복구와 관련하여서 분석 도구와 디지털 포렌식 수사관의 능력 차이로 인해 복구의 정도에 차이가 있다.

60) 노명선·구희진·김영철·배대한·최대건·최우석, "디지털포렌식 이론", 미디어북, 2018, 33면

따라서 삭제된 파일의 복구와 관련된 재현가능성은 모든 경우에 같은 결과물이 나오는지 보다는 디지털 포렌식 수사관이 동일한 상황에서 특정한 포렌식 프로그램을 이용하여 복구를 하였을 때 같은 결과가 나오는지 여부, 즉 반복가능성에 가깝다고 할 것이다. 물론, 다른 포렌식 도구, 다른 수사관이 분석을 한 복구 결과가 동일하다는 것도 삭제 후 복구된 파일의 신뢰성, 진정성을 입증하는 하나의 요소가 될 수 있다.

판례의 태도와 같이 증거로 제출된 개별 디지털 파일의 증거능력의 인정과 관련하여, 압수된 이미지 파일에서의 개별 디지털 파일의 변환·복제를 동일성의 관점에서 중시 여기게 된다면, 삭제 후 복구된 디지털 파일의 증거능력에서도 삭제된 디지털 파일의 복구 과정 및 위 복구 파일의 변화되지 않고 복사된 것임을 증명하는 것, 즉, 재현가능성이 향후 중시될 것으로 보인다.

그런데 앞서 살펴본 바와 같이 삭제 후 복구된 디지털 파일을 압수하는 방법으로는 2가지 경우를 가정할 수 있다. 정보저장매체에서 삭제된 디지털 파일들을 복구한 후 선별하여 관련성이 있는 복구된 디지털 파일들만을 논리이미징하여 압수하는 방법(‘복구 후 선별 압수 방법’이라 한다)과 정보저장매체 자체를 물리이미징한 후 삭제된 디지털 파일들을 복구한 이후에 선별하여 압수하는 방법(‘전체 이미징 후 복구 및 선별 압수 방법’이라 한다)이 존재한다. 각각의 경우에 따라 해시값 비교의 대상을 무엇으로 볼 것인지, 재현가능의 입증 정도도 달라진다.

먼저 복구 후 선별 압수 방법에서는 삭제 후 복구된 디지털 파일들만을 논리이미징하여 복사한 것이기 때문에 정보저장매체 전체가 아닌 복구된 디지털 파일들을 포함한 압수한 파일들의 해시값과

이미지 사본 파일의 해시값을 비교하는 방법으로 동일성, 무결성을 증명할 수 밖에 없다. 그런데 만약 이미징 이전의 단계, 즉 복구 과정이 문제된다면 재현가능성을 입증하기 위하여 저장저장매체나 그 정보저장매체 전체에 대한 이미지 파일이 필요한데, 정보저장매체나 그 정보저장매체 전체에 대한 이미지 파일 모두 없는 상황에서 복구가 제대로 이루어졌는지 여부를 증명하기 곤란한 상황이 발생한다. 따라서 재현가능성에 대한 입증의 정도를 완화하여 디지털 증거 분석 도구의 신뢰성, 디지털 포렌식 수사관의 전문성 등으로 이를 보완하는 것이 필요하다.

다음으로, 전체 이미징 후 복구 및 선별 압수 방법에서는 정보저장매체 자체를 이미징하였기 때문에 정보저장매체에 저장되어 있던 전체 정보를 원본으로 보고, 정보저장매체 전체의 해시값과 이미지 파일의 해시값을 비교한 후, 이미지 파일에서 삭제된 디지털 파일이 복구되었고, 그 복구된 파일의 사본이라는 것을 증명하여야 한다. 이 경우, 재현가능성을 입증하기 위하여 원본 정보저장매체나 이미지 파일이 필요하다. 보통 원본 정보저장매체는 피압수자에게 반환하고 이미지 파일은 복구 및 선별 압수 후 삭제하나 이러한 경우 재현가능성 입증을 위해 이미지 파일을 보관하는 것이 필요하다.

제4절 저장매체에 저장된 디지털 정보 자체의 확인

앞서 살펴본 바와 같이, 디지털 증거는 0과 1의 2진법적인 데이터가 저장되어 있는 구조이다. 디지털 증거는 비가시성·비가독성의 특징을 가지지만, 헥스 편집기(Hex Editor[61])는 이러한 2진수 파일을

61) 대표적으로 디지털 포렌식 소프트웨어 개발 및 교육 회사인 X-ways에서 개발된 WinHex 등이 있다.

16진수로 읽을 수 있는 프로그램이다.

이러한 헥사편집기를 이용하여 2진수 파일 자체를 16진수로 읽을 수 있고, 삭제된 파일의 복구, 카빙 복구가 가능하다. 삭제된 디지털 파일 중 저장매체에 남아있는 데이터의 구조 및 그 내용을 입증할 수 있을 것으로 보인다.

제5절 부수데이터의 분석

디지털 증거의 특징에서 살펴본 바와 같이 디지털 증거에는 풍부한 부수데이터가 존재한다. 윈도우 아티팩트 및 메타데이터 분석 등을 통해 디지털 파일의 생성 시간, 수정 및 삭제 시간, 파일의 크기, 파일명, 소유자 정보 등 다양한 정보를 확인하여 디지털 파일의 삭제에 대한 간접 증거로 활용할 수 있을 것으로 보인다.

제6절 제3의 전문기관 등에 의한 감정

디지털포렌식을 전문적으로 하는 전문기관이 존재하고, 디지털포렌식팀을 운영하고 있는 법무법인이 증가하고 있다. 실제 증거인멸·은닉죄 등으로 기소된 사건에서 변호인은 수사기관에서 압수한 저장매체의 이미지 파일의 열람·등사를 요청하여, 변호인이 자체적으로 대검찰청이 보관하고 있던 이미지 파일에 대하여 Encase 등 프로그램을 이용하여 삭제 데이터 분석 및 복구 작업을 실시한 바 있다. 자체적으로 분석 및 복구한 자료와 검찰이 증거로 제출한 자료가 동일함을 확인한다면 피고인의 권익 보호와 방어권 행사에도 유리하고, 형사소송에서도 증거능력과 관련한 공방을 조기에 종결할 수 있어 유익한 방법인 것으로 보인다.

또한, 법원은 민사소송에서 소송관계를 분명하게 하거나

소송절차(증거조사 등)를 원활하게 진행하기 위하여 전문심리위원을 지정하여 소송절차에 참여하게 할 수 있고(민사소송법 제146조의2), 디지털증거 관련 전문심리위원(비상임)도 활용된다.[62] 형사소송에서도 이러한 디지털증거 관련 전문심리위원도 증거조사에 활용될 수 있을 것으로 보인다. 따라서 객관적이고 전문성을 갖춘 제3의 기관인 국가디지털포렌식센터, 한국포렌식학회 등을 통해 감정을 하는 것도 좋은 방법인 것으로 보인다.

62) 김유성, “디지털증거의 효과적인 증거조사 및 증거관리 방안에 대한 연구”, 석사학위논문, 서울대학교, 2019, 34면

V. 결론

디지털 증거는 기존의 물리적 증거와는 다른 특징들을 가지고 있다. 그러므로 디지털 증거의 압수·수색 및 증거능력에 대하여 물리적 증거의 관점에서 접근을 해서는 안 된다.

정보저장매체에 저장된 디지털 파일을 삭제하는 것은 실제 물리적 증거를 폐기하는 것과는 다르다. 삭제된 디지털 파일은 눈에 보이지 않기 때문에 완전히 없어진 것처럼 보이고, 복구 작업을 통해 새롭게 재생성된 것처럼 여겨질 수 있으나, 앞서 살펴본 바와 같이 정보저장매체에 남아있는 데이터를 가시성·가독성이 있는 형태로 변환한 것에 불과하다.

따라서 디지털 증거는 정보저장매체에 저장된 데이터, 정보 그 자체를 의미하고, 삭제 후 복구된 디지털 파일의 경우, 삭제되기 전이 아닌 삭제되고 난 이후, 압수 시점에서의 정보저장매체에 저장된 디지털 형태의 정보를 원본으로 보아야 한다. 또한 개별 디지털 파일은 한컴오피스, Microsoft Word, Excel, Powerpoint 등 각종 소프트웨어 프로그램을 통해 보고 읽을 수 있도록 변환된 것이기 때문에 원본의 단위를 개별 디지털 파일 단위로 보기 보다는 정보저장매체나 전체 이미지 파일의 단위로 보아야 한다.

또한, 증거능력의 인정 요건으로 원본과의 동일성, 무결성 및 신뢰성이 있다. 수사 실무적으로 디지털 증거 중 삭제 후 복구된 디지털 파일을 압수하는 방법으로 정보저장매체에서 삭제된 디지털 파일들을 복구한 후 선별하여 관련성이 있는 복구된 디지털 파일들만을 이미징하여 압수하는 방법(‘복구 후 선별 압수 방법’이라 한다)과 정보저장매체 자체를 이미징한 후 삭제된 디지털 파일들을 복구한

이후에 선별하여 압수하는 방법(‘전체 이미징 후 복구 및 선별 압수 방법’이라 한다)이 있다. 각각의 경우에 따라 해시값 비교의 대상을 무엇으로 볼 것인지, 재현가능의 입증 정도도 달라진다.

먼저 복구 후 선별 압수 방법에서는 삭제 후 복구된 디지털 파일들과 다른 파일들을 이미징하여 복사한 것이기 때문에 정보저장매체 전체가 아닌 복구된 디지털 파일들을 포함한 압수된 디지털 파일들과 그것을 이미지한 파일의 해시값을 비교하는 방법으로 동일성, 무결성을 증명할 수 밖에 없다. 이미징 이전의 단계, 즉 복구 과정이 문제된다면 재현가능성을 입증하기 위하여 저장저장매체나 그 정보저장매체 전체에 대한 이미지 파일이 필요한데, 정보저장매체나 그 정보저장매체 전체에 대한 이미지 파일 모두 없는 상황에서 복구가 제대로 이루어졌는지 여부를 증명하기 곤란한 상황이 발생한다. 따라서 재현가능성에 대한 입증의 정도를 완화하여 디지털 증거 분석 도구의 신뢰성, 디지털 포렌식 수사관의 전문성 등으로 이를 보완하는 것이 필요하다.

다음으로, 전체 이미징 후 복구 및 선별 압수 방법에서는 정보저장매체 자체를 이미징하였기 때문에 정보저장매체에 저장되어 있던 전체 정보를 원본으로 보고, 정보저장매체 전체의 해시값과 이미지 파일의 해시값을 비교한 후, 이미지 파일에서 삭제된 디지털 파일이 복구되었고, 그 복구된 파일의 사본이라는 것을 증명하여야 한다. 이 경우, 재현가능성을 입증하기 위하여 원본 정보저장매체나 이미지 파일이 필요하다. 보통 원본 정보저장매체는 피압수자에게 반환하고 이미지 파일은 복구 및 선별 압수 후 삭제하나 이러한 경우 재현가능성 입증을 위해 이미지 파일을 보관하는 것이 필요하고, 이미지 파일의 보관 방법 등을 논의할 필요성이 있다.

현재까지 삭제 후 복구된 파일의 증거능력 인정 요건에 대해 명시적으로 판결한 판례가 존재하지 않는다. 판례는 디지털 증거의 증거능력 인정 요건에 대하여 종합판단설의 입장을 취하고 있으므로, 비할당영역에 압수할 데이터가 존재하였고, 전문성을 갖춘 디지털포렌식 수사관이 신뢰할 수 있는 복구 도구를 이용하여 복구하였으며, 이를 재현할 수 있음을 종합적으로 증명함으로써 동일성, 무결성 및 신뢰성을 인정받을 수 있다고 생각한다. 구체적으로, 디지털 증거분석 도구의 신뢰성, 디지털 포렌식 수사관의 법정 증언 및 재현가능성 검증, 저장매체에 저장되어 있는 디지털 정보 자체의 확인, 부수데이터의 분석, 제3의 전문기관 등에 의한 감정 등 다양한 방법으로 이를 효과적으로 입증할 수 있다. 미국은 원본의 개념을 폭넓게 인정하고 있고, 증거능력의 증명과 관련하여서도 엄격한 증명이 아닌 자유로운 증명으로 족하다는 태도이다. 그러나 우리나라의 판례 및 실무는 증거능력의 증명과 관련하여서 점차 엄격한 증명의 방향으로 가고 있는 것처럼 보인다. 피압수자의 기본권 보호, 피고인의 방어권 행사에 유리한 방향이기는 하나 과학기술이 계속적으로 발전하면서 변화하고 있는 상황에서 증거능력과 관련하여 다양한 방법을 통해 자유로운 증명을 가능하게 하고, 법원에 폭넓은 재량을 인정하는 것이 바람직해 보인다.

기존 증거능력 인정 요건과 관련하여 해시값 비교가 중요하게 여겨졌으나, 앞으로 정보저장매체 원본이 존재하지 않거나 HDD 등 저장매체의 특성상 해시값이 변경되는 상황이 존재할 것이다. 과학기술은 계속적으로 발전하면서 변화하고 있고, 디지털 포렌식 및 이에 대응하는 안티포렌식도 계속적으로 발전하면서 변화하고 있다. 따라서 디지털 증거의 특징을 고려하여 다양한 방법으로 증거능력의

인정 요건인 진정성, 무결성 및 신뢰성을 입증할 수 있도록 해야 하는 방안이 계속적으로 연구되어야 할 것이라고 생각한다.

[참고문헌]

□ 국내 단행본

오기두, “전자증거법”, 박영사, 2015.

노명선 · 구희진 · 김영철 · 배대한 · 최대건 · 최우석, “디지털포렌식 이론”, 미디어북, 2018.

이상진, “디지털 포렌식 개론”, 이룬출판사, 2015.

Larry E. Daniel, Lars E. Daniel, “포렌식 전문가와 법률가를 위한 디지털 포렌식”, 비제이퍼블릭, 2012.

John Sammons, "이제 시작이야 디지털 포렌식“, 비제이퍼블릭, 2012.

□ 국내 논문

권양섭, “디지털증거수집에 관한 연구”, 박사학위논문, 군산대학교, 2009.

탁희성·이상진, 디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보 방안, 형사정책연구원, 2006.

양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 박사학위논문, 경희대학교, 2006.

양근원, ‘증거법상의 새로운 화두 : 디지털 증거와 디지털 포렌식, 경찰법연구 제5권 제1호, 2007.

강승훈, “행정조사를 위한 디지털증거 수집의 적법성 강화 방안”, 석사학위논문, 서울대학교, 2019.

김기범, “해시함수의 형사법적 고찰”, 형사정책연구, 29(2), 한국형사정

책연구원, 2018.
박진환, “해시값의 비교에 의한 디지털 증거의 동일성 입증에 관한 연구”, 석사학위논문, 서울대학교 2019.
전현욱 · 김기범 · 조성용 · Emilio C. VIANO, “사이버범죄의 수사 효율성 강화를 위한 법제 개선방안 연구”, 경제·인문사회연구회 미래사회 협동연구총서 15-17-01, 2015.
김현선, “미국의 디지털 증거 활용 실태”, 해외연구검사 연구논문, 2008
이상진·김진국·방정흠, “디지털 포렌식 관점의 데이터 복구 및 분석 프레임워크”, 한국정보처리학회, 한국정보처리학회논문지 17(5), 2010.
탁희성, “전자증거에 관한 연구”, 이화여자대학교 박사학위논문, 2004
김진국 · 이승봉 · 방정흠 · 방제완 · 이상진, “파일카빙 기법에 한 연구”, 디지털 포렌식연구 2호, 2008. 6.
김민서 · 이상진, “윈도우 포렌식 도구의 검증용 데이터 세트의 개발”, 한국정보보호학회, 정보보호학회논문지 제25권 제6호, 2015. 12.
이태림 · 신상욱, “디지털 포렌식을 위한 증거 분석 도구의 신뢰성 검증”, 한국정보보호학회, 정보보호학회논문지 제21권 제3호, 2011. 6.
천영준, “디지털 포렌식 수사관의 법정증언과 분석결과의 신뢰성 확보 방안 연구”, 석사학위논문, 서울대학교, 2017.
김유성, “디지털증거의 효과적인 증거조사 및 증거관리 방안에 대한 연구”, 석사학위논문, 서울대학교, 2019.
강철하, “美 Loraine v. Markel American Insurance Company 事件에 나타난 電子的貯藏情報의 證據能力許容要件”, 아주법학 2권 1호, 아주대학교 법학연구소, 2008.

□ 외국 자료

Peter Lyman and Hal R.Varian, U.C. Berkely, “How Much Storage is Enough?”, ACM Queue vol.1, no.4 June 2003.

Lorraine v. Markel American Ins. CO., PWG-06-1893 (D. Md May 4. 2007)

Eoghan Casey, "Digital Evidence and Computer Crime : Forensic Science, Computers and the Internet", Third Edition, 1999

Joachim Metz, Bas Kloet and Robert-Jan Mora, “Analysis of 2007 DFRWS Forensic Carving Chllenge - The 07 smart carving approach,” Digital Forensic Research Workshop (DFRWS), July, 2007.

Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90(D.C. Col., 1996).

Bray v. Bi-State Development Corp., 949 S.W.2d 93(1997).

United States v. Scott-Emuakpor, supra, 2000 WL 288443.

United States v. Seifert, 2005 WL44749(D.Minn. Jan 7, 2005).

galaxy computer Services, INC. V. Baker, 325 B.R.544(E.D.va.2005)

Test Results(Federated Testing) for Disk Imaging Tool : Computer Forensic Tool(CFT) version 3. 4. 1.(February 2018)

Test Results for Delected File Recovery and Active File Listing Tools[ILooKIX v2.2.3.151.(9/22/2014), The Sleuth Kit(TSK)/Autopsy v3.2.2.(7/2/2014), X-ways Forensics v16.0 SR-4(7/2/2014), SMART for Linux v2011-02-02, Encase Forensic v6.18.0.59(6/23/2014), FTK

v3.3.0.33124(6/23/2014)]
www.cftt.nist.gov

□ 판결

대법원 2007. 12. 13. 선고 2007도7257 판결
대법원 2013. 7. 26. 선고 2013도2511 판결
대법원 2016. 9. 28. 선고 2014도9903 판결
대법원 2018. 2. 8. 선고 2017도13263 판결
서울고등법원 2014. 8. 11. 선고 2014노762 판결
서울중앙지방법원 2007. 4. 16. 선고 2006고합1365, 2006고합1363(병합), 2006고합1364(병합), 2006고합1366(병합), 2006고합1367(병합) 판결