https://doi.org/10.35147/knpsi.2019.33.2.091

디지털 포렌식 분석을 통한 온라인 음란물 최초 유포자 확인 연구
- 클라우드, 카카오톡, 텔레그램을 중심으로 -

A Study on the Identification of the First Person to Distribute Online Pornography through Digital Forensics Analysis
- In Focus on Cloud, KakaoTalk, Telegram -

천성덕* · 강구민**

차 례

● 국문요약 ●

2019년 초 한 연예인이 여러 명이 참여한 대화방에 한 여성을 성폭행하는 장면을 불법 촬영하여 올리는 사건이 발생하면서 대한민국의 성범죄에 대한 경종을 울리는 계기가 되었다. 특히 전파성이 매우 강한 온라인상에 음란물을 유포하는 것은 한 사람의 인격권과 생명권까지 침해한다는 점에서 치유될 수 없는 범죄행위이다. 더욱이 사건을 통하여 유포된 음란물을 찾아 파기하여도 복사하여 재유포된 음란물까지 모두 찾아 파기하기에는 수사 현실상 어려웠다. 본 논문에서는 불법 음란물의 마지막 한 개까지 찾아 파기하기 위한 방법에 대하여 고민하였다. 특히 스마트폰을 이용하여 불법 촬영하고 클라우드앱이나 메신저앱을 통하여 주로 음란물이 유포된다는 점에서 클라우드앱, 카카오톡, 텔레그램을 통해 음란 동영상을 유포한다는 가설을 두고 실험을 하였다. 다만 여러 경우의 수를 산정하여 실험을 해야 하지만, 본 논문에서는 아이폰8(v12.3.1)만을 이용하여 제한적인 실험을 진행하였다. 연구결과 클라우드앱상에서는

* 서울 광진경찰서 보안과, 성균관대학교 일반대학원 과학수사학과 박사과정, 제1저자.
** 성균관대학교 일반대학원 과학수사학과 초빙교수, 법학박사, 교신저자.

원본 동영상과 내려 받은 파일 모두 변화가 없었고, 메신저앱상에서는 최초 동영상을 응용프로그램 공급업체에서 지원하는 코덱으로 변환되어 메신저를 통해 재배포되었음에도 어떠한 변화도 일어나지 않았다. 이러한 연구 결과를 바탕으로 유포된 것으로 의심되는 동영상 파일의 원본파일과 유포된 파일을 상대로 파일의 해쉬함수를 이용하여 해당 동영상 파일만을 추출하는 것이 가능하다는 사실을 알게 되었다. 그리고 이러한 분석방법을 통하여 수집된 디지털 증거가 법적인 증거능력을 갖기 위해서는 우선 수사기관의 적법한 절차에 의하여 수집 분석되어야 하고, 디지털 증거에 대한 원본성·무결성 등의 진정성 요건을 충족하여야 한다. 마지막으로 전문법칙 관문을 통과해야 하는데, 본 논문에서 진행된 실험으로 얻은 결과값들은 컴퓨터에 의해 자동 생성된 기록들로서 전문법칙의 예외에 해당되어 당연 증거능력이 인정된다.

◈ 주제어 : 온라인 음란물, 디지털포렌식, 디지털증거, 클라우드, 카카오톡, 텔레그램

Ⅰ. 서론

우리의 문명사회는 컴퓨터와 정보통신기술의 발달로 현실 세계에서 할 수 있는 일들을 스마트폰을 이용하여 온라인상에서도 할 수 있게 되었다. 우리의 이러한 삶이 가능한 것은 바로 '사이버 공간'의 출현, 즉 네트워크로 연결된 온라인이 있었기에 가능한 것이다. 한국은 스마트폰 보유율 95%로 세계 1위의 국가이다.[1] 이러한 결과는 우리 대한민국이 스마트폰 관련 기술의 선구자이면서 스마트폰 문화를 이끌고 있다는 방증이라 생각된다. 그렇다면 범죄의 양상은 어떨까.

스마트폰을 이용하여 온라인상에서의 범죄의 양상은 현실 세계와 별반 차이가 없다. 우선 온라인이라는 특성상 상대방에 대한 인식이 없는

1) Pew Researcher Center, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally", 2019. 2. 5. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/(2019. 8. 3. 검색).

비대면성 또는 익명성이라는 특성을 지닌다. 그렇다 보니 범죄자를 특정함에 있어 고도의 전문적인 기술력이 필요하기 때문에 적발하기가 매우 어렵고, 피해자 역시 본인이 피해를 당하였는지를 인식하기까지 시간이 오래 걸린다. 뿐만 아니라 네트워크로 연결된 곳이면 언제 어디서든 시간과 공간의 제약을 받지 않으며 클릭 하나로 전 세계적으로 전파된다. 이처럼 온라인상에서의 범죄는 우리의 상상을 초월하고, 이를 수사하는 수사기관에게는 커다란 부담일 수밖에 없다.

온라인상에서 발생하는 여러 성범죄가 모두 중대하겠지만, 그 중 음란 동영상을 온라인상에 불법 유포[2]함으로써 피해 여성이 자살까지 하는 기사를 종종 접하곤 한다. 한 사람의 성적수치심과 인격권 더 나아가 생명권까지 침해한다는 점에서 피해자가 사회적으로 회복할 수 없을 정도의 심각한 범죄가 바로 온라인상에 성 관련 동영상을 불법적으로 유포하는 범죄라 생각된다.

최근 투자자들에게 성 접대를 하였다는 한 연예인의 기사가 사회적 이목이 집중되었다. 그러나 해당 연예인의 카카오톡 대화를 조사하던 중 또 다른 연예인이 단체 대화방에 불법 촬영한 동영상을 유포하였다는 언론의 보도 후 세간의 떠들썩한 관심이 다시 집중되었다.[3] 뿐만 아니라 한 남성이 지하철에서 여성 승객의 치마 속을 몰래 찍어 온라인 커뮤니티와 SNS에 해당 몰카영상을 올리는 일도 있었다.[4]

---

2) 여성가족부, 2018년 디지털 성범죄 피해 유형별 현황, 2018 : 여성가족부가 운영 중인 '디지털 성범죄 피해자 지원센터'에 의하면, 2018년 8월 현재 센터에 접수된 피해건수 2,358건 중 유포피해가 998건(42.3%)으로 가장 많다. 그 뒤로 불법촬영이 795건(33.7%), 유포협박이 202건(8.6%), 사진합성이 64건(2.7%)으로 뒤를 이었다.

3) 김종원, "[단독] 정준영, 불법촬영 후 카톡방에 전송...피해자 최소 10명", SBS뉴스, 2019. 3. 1.

4) 장경운, "지하철서 '스마트폰'으로 여성 치마 속 '몰카'찍다 딱 걸린 변태남",

이처럼 현대의 음란물들은 과거 청계천 일대에서 포르노 비디오를 구하는 방식과 전혀 다른 양상을 보인다. 클릭 하나로 온라인상에서 누구나 때와 장소를 가리지 않고 음란물을 서로 주고받을 수 있는 환경이 되었고, 피해자가 이를 인식하고 경찰에 신고하여 수사가 진행되는 와중에도 해당 동영상은 일파만파 번지고 있을 것이다. 현재 해당 음란 동영상을 유포한 사건에 있어서 관련자들만 처벌할 뿐 수사의 한계상 음란 동영상의 원본이나 복제본까지 찾아내어 전량 파기하는 일은 매우 어려운 현실이다. 이러한 수사 현실 속에서 복제된 음란 동영상이 온라인상에 또다시 유포된다면, 피해 여성의 생활은 만신창이가 될 것이고, 수사기관에서는 억울한 한 명의 피해여성을 위해서라도 새로운 수사방법에 대한 고민이 필요하다.

본 논문에서는 클라우드 어플리케이션, 국내에서 가장 많이 사용되어지고 있는 카카오톡, 보안성이 강한 텔레그램을 이용하여 음란 동영상을 유포한 경우를 산정하였다. 그리고 각 유포과정에서 발생되는 음란 동영상 파일시스템 및 구조의 변화를 비교함으로써 최초 촬영자 및 유포자를 특정하고, 재공유를 차단하기 위한 디지털 포렌식 수사기법을 제안한다. 그리고 이러한 디지털 포렌식 분석을 통하여 수집된 디지털 정보들이 증거능력을 갖추기 위한 요건들은 무엇인지를 함께 검토한다.

인사이트, 2019. 5. 28.

Ⅱ. 선행 연구 및 연구의 한계점

1. 선행 연구

기존 '온라인상에 유포된 음란물' 관련 논문들을 살펴보면, 주로 음란물에 대한 형사법적 책임과 정책적인 문제들을 다루고 있으며,[5] 기술적으로 수사기법이나 추적기법과 관련하여서는 스마트폰 내에 있는 저장정보나 클라우드 상에 있는 정보에 대한 수집 방법 및 저작권과 관련된 동영상에 대한 단속 등을 연구한 논문들[6]이 대다수이다.

5) 김수아·장다혜, "온라인 피해 경험을 통해 본 성적 대상화와 온라인 성폭력 문제", 미디어 제던&문화, 제34권 제1호, 한국여성커뮤니케이션학회, 2019; 홍태석, "일본에 있어 아동음란물 다운로드 행위의 가벌성 논의", 법학연구, 제17권 제4호, 한국법학회, 2017; 서승희, "사이버성폭력 피해의 특성과 근절을 위한 대응방안 -비동의 유포 성적촬영물을 중심으로-", 이화젠더법학, 제9권 제3호, 이화여자대학교 젠더법학연구소, 2017; 박준석, "음란물의 저작물성 및 저작권침해금지청구 등의 가능성 -대법원 2015. 6. 11. 선고 2011도10872판결-", 법조, 제65권 제9호, 법조협회, 2016; 이동훈, "사이버 음란물 규제 방안에 대한 고찰 -'SNS 앱'을 중심으로-", 글로벌 기업법무 리뷰, 제9권 제2호, 경희대학교 법학연구소, 2016; 이흔재, "아동음란물소지죄에 관한 형사정책 및 형법상의 문제점", 형사정책연구, 제25권 제4호, 한국형사정책연구원, 2014; 류진철·이형일, "사이버음란물 유포행위의 형사법적 규제", 법학논총, 제14권 제1호, 조선대학교 법학연구소, 2007; 박희영, "사이버 음란물 유포행위와 형사책임", 법학연구, 제43권 제1호, 부산대학교 법학연구소, 2002.

6) 최민석·최성욱, "저작권 보호를 위한 대표 색상 시퀀스를 이용한 동영상 복사 검출 방법", 디지털융복합연구, 제10권 제5호, 한국디지털정책학회, 2012; 이정훈·천우성, "디지털 증거 수집과 분석을 위한 스마트폰 포렌식 적용 연구", 정보보호학회지, 제21권 제6호, 한국정보보호학회, 2011; 손현구 외,"트래픽 모니터링을 통한 P2P 및 웹 하드 다운로드응용의 파일이름 식별 방법", 정보통신, 제37권 제6호, 한국정보과학회, 2010; 최윤기, "'해운대'류 불법복제 동영상 검색-단속 기법", 경찰연구논집, 제6권, 한국경찰이론과실무학회, 2010.

본 논문과 유사한 방법으로 음란물 유포자에 대한 추적 기법을 제시한 연구에서 P2P(Peer to Peer)나 웹하드를 통하여 음란물이 유통된다는 점에 착안하여 Torrent를 이용하여 아동·청소년 음란물을 유포하는 최초 유포자 외 중간 유포자들까지 포함하여 아동·청소년 음란물 유포자를 추적하는 방안에 대하여 연구하였다.[7] 동 논문은 음란물을 유포한 자에 대한 추적기법이라는 점에서 동일하나, 과거 P2P 방식으로 파일을 주고받던 시대에 이루어진 기법이라는 점에서 현 시점에서 이루어지는 파일 공유 방식과는 현저한 차이가 있다. 뿐만 아니라 스마트폰을 이용하여 카카오톡이나 텔레그램 등을 이용하여 파일을 주고받는 음란물에 대한 추적기법을 제시하지 못하고 있다.

메타데이터를 이용하여 파일에 대한 추적 기법을 연구한 논문[8]에서는 MS Office의 PowerPoint, Word, Excel과 훈글 파일을 대상으로 하였고, 이들 파일의 메타데이터를 분석하여 파일의 동일성과 원본을 판단하여 추적하는 방법을 제시하였다. 일반적으로 디지털 증거의 진정성 여부를 판단할 때 해쉬값을 통하여 동일성 여부를 판단하는데, 위 논문에서는 해쉬값이 변화더라도 메타데이터를 통하여 동일성을 입증하려 시도하였다. 그리고 분석의 대상은 일반 문서파일을 대상으로 하였다. 파일의 해쉬값을 통하여 최초 유포자를 식별하고 문서파일이 아닌 동영상 파일을 대상으로 하였다는 점에서 본 논문과 차이가 있다.

7) 최아영, "아동·청소년 음란물 유포자자 추적 방안에 관한 연구 : 비트 토렌트에 대한 포렌식 중심으로", 동국대학교 국제정보대학원 석사학위 논문, 2014.
8) 진경아 외, "메타데이터를 이용한 파일 유출 추적에 관한 연구", 한국통신학회 학술대회논문집(2018년도 동계종합학술발표회), 한국통신학회, 2018.

2. 연구의 한계점

본 연구에서는 불법 촬영된 동영상이 주로 스마트폰을 이용하여 촬영되고 클라우드 어플리케이션을 이용하여 해당 스토리지에 저장한 후 스마트폰 내에 있는 채팅 어플리케이션을 통하여 유포된다는 점에 착안하여, 여러 변수를 설정하지 않고 하나의 스마트 폰을 정하여 해당 스마트폰으로 촬영하고 클라우드에 저장한 후 채팅앱을 통하여 유포한다는 상황으로 설정하였다.

우선 스마트폰의 운영체제는 애플의 iOS, 구글의 Android, MS의 Windows로 나뉜다. 본 논문에서는 Apple사의 iPhone8(v.12.3.1)만을 이용하여 동영상을 촬영하고 관련 어플리케이션을 다운 받아 실험하였다. 구글의 Android와 MS의 Windows 운영체제를 이용한 연구는 하지 않았다.

본 논문에서 이용한 클라우드 어플리케이션은 Naver Mail, Naver Band, Naver Cloud, Daum Mail, Evernote 등이다. 클라우드 서비스 방식에는 일반 기업에서 제공하는 방식과 최근에는 개인이 사적으로 클라우드를 구성하여 이용하기도 한다. 본 연구에서는 개인 클라우드에 대한 접속권한의 문제로 연구 대상에서 제외하고 기업에서 제공하는 5개의 클라우드 어플리케이션만을 이용하여 연구하였다.

모바일 메신저 대상으로 카카오톡과 텔레그램만을 이용하였다.[9] 이외에도 라인, 페이스북 메신저, 인스타그램 등 다양한 모바일 메시전가 있지만 본 논문에서는 일반적으로 가장 많이 사용하는 카카오톡과 보안

9) KT경제연구소·DMC미디어의 '2019 모바일 메신저 앱 이용 행태' 보고서에 의하면, 사용순위로 카카오톡, 네이트온, 페이스북메신저, 라인, 텔레그램, 위챗, 스카이프 등의 순으로 나타났다.

성이 강한 해외 메신저인 텔레그램을 중심으로 연구를 하였다. 또한 모바일 상의 메신저를 일반PC에서도 사용 가능하다는 점에서 PC상의 메신저를 통하여 음란물을 유포하였을 때의 파일 변화값을 비교하면 좋겠지만, 이 역시 본 논문에서는 다루지 못하고 향후 연구로 남겨둔다.

Ⅲ. 클라우드(Cloud)를 이용한 음란물 유포 확인

1. 클라우드 어플리케이션을 통한 음란물 파일 유포 특징

〈표 1〉 실험에 사용한 클라우드 애플리케이션 정보

서비스명	방식	어플 버전	사용기기
Naver Mail	Cloud	v2.3.6	iPhone 8 (v12.3.1) / KOR SK Telecom
Daum Mail	Cloud	v1.0.6	iPhone 8 (v12.3.1) / KOR SK Telecom
Naver Band	Cloud	v7.3.5	iPhone 8 (v12.3.1) / KOR SK Telecom
Evernote	Cloud	v8.22.370013	iPhone 8 (v12.3.1) / KOR SK Telecom
Naver Cloud	Cloud	v5.3.0	iPhone 8 (v12.3.1) / KOR SK Telecom

클라우드 제공업체 Naver, Daum, Evernote에서 지원하는 5가지 어플리케이션(Application) 응용프로그램을 대상으로 최초 촬영된 동영상을 upload, download 함으로써 동영상 파일의 내부 구조와 파일시스템의 변화를 비교하였다.

실험 결과는 5가지 클라우드 방식의 어플리케이션 모두 원본 동영상과 저장 후 내려 받은 파일 모두 변화가 없었다는 것이다. 이것은 디지털 포렌식 프로그램 EnCase v8.08 도구로 파일의 해쉬함수(Hash Function)값의 변화를 통해 확인하였다.

〈그림 1〉 클라우드 환경에 따른 원본파일의 해쉬값 변화

(1) Naver Mail

Name	File Ext	Logical Size	MD5
IMG_0187_original file.MOV 원본 파일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3
video_0_naver mail.MOV 네이버 메일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3

(2) Daum Mail

Name	File Ext	Logical Size	MD5
A4FA82F3-EA7F-45BF-B146-C2216B2319DE_다음 메일.MOV 다음 메일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3
IMG_0187_original file.MOV 원본파일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3

(3) Naver Band

Name	File Ext	Logical Size	MD5
IMG_0187_naver band.MOV 네이버 밴드	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3
IMG_0187_original file.MOV 원본 파일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3

(4) Evernote

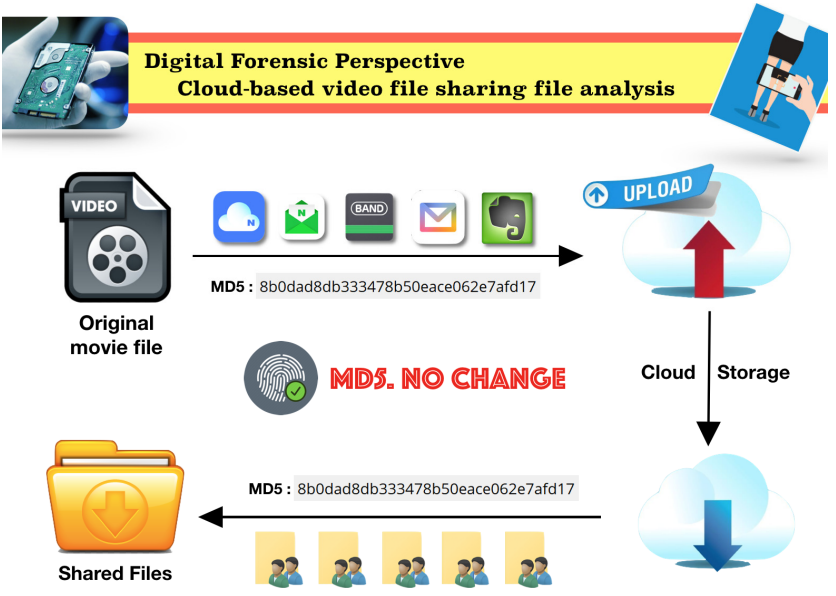
Name	File Ext	Logical Size	MD5
IMG_0187_Evernote.MOV 에버노트	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3
IMG_0187_original file.MOV 원본 파일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3

(5) Naver Cloud

Name	File Ext	Logical Size	MD5
IMG_0187_naver cloud.MOV 네이버 클라우드	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3
IMG_0187_original file.MOV 원본 파일	MOV	519,171	2c3ecb917be0e7481aadb358f65812d3

위 실험결과는 피의자 또는 피고인 본인이 소지하고 있는 스마트폰을 통해 음란물 동영상을 촬영한 후 같은 스마트폰에 설치된 어플리케이션을 통해 클라우드 서비스에 접속하고 upload 한 상황을 가정하고 실험한 것이다. 경우에 따라 스마트폰이 아닌 PC에 동영상을 옮긴 후 upload 하는 경우도 있는 만큼 향후 추가적이고 세부적인 연구가 필요할 것으로 생각된다.

〈그림 2〉 클라우드 방식의 공유파일 MD5 변화 개요도



위와 같은 환경에서 피해자를 검거하고 유포된 동영상 파일을 신속하게 찾아 삭제하기 위해 어떠한 부분을 확인하고 증거로서 수집해야 할 것인가 생각해봐야 할 것이다. 이러한 견지에서 온라인 성범죄의 경우 피의자 또는 피고인을 찾아 처벌하는 형벌적 행위보다 피해 여성의 동영상이 제3자에게 무차별적으로 유포되어 겪는 정신적 피해에 대한 고민을 먼저 해야 할 것이다.

그렇다면 수사기관 원본 동영상 파일을 디지털 포렌식을 통해 분석하여 최초 촬영자와 유포자를 찾아야 한다면, 특히 대용량 저장장치에 불특정 다수의 파일과 혼재되어 있는 경우 원본 파일의 파일시스템 분석은 필수라 할 것이다.

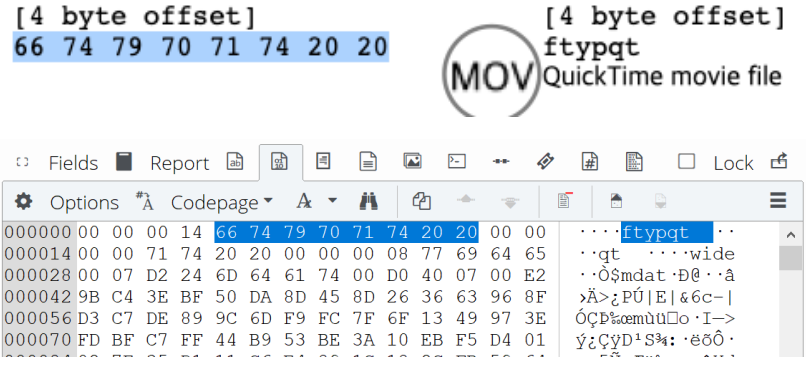
2. 원본 파일에 대한 디지털 포렌식 분석 (iOS : iPhone MOV File 분석)

iPhone의 동영상 포맷은 MOV(Quick Time Movie) 형태를 가지고 있다. 안드로이드폰(겔럭시)의 동영상 포맷은 mp4(MPEG-4)의 형태를 가지고 있는 것과 비교되는 경우가 많이 있다. iPhone MOV 비디오 파일에는 촬영 당시의 정보를 많이 가지고 있다.

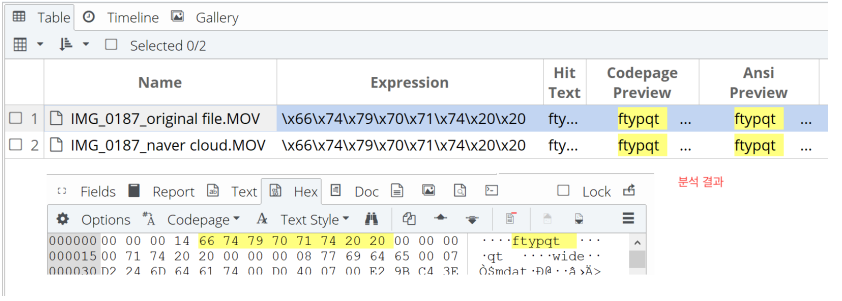
그중 사건을 처리하기 위해 유용하게 사용될 정보는 촬영 당시의 ① 기기정보, ② 날짜정보, ③ 위치정보를 들 수 있을 것이다. 하지만 이러한 정보 역시 일반적인 방법이 아닌 디지털 포렌식 과정을 통해 무결성과 원본성 등을 갖추어 정보를 수집해야 하며 차후 유효한 증거로써 공판과정에 사용하고자 하면 재현성까지 갖추어야 할 것이다.

1) MOV File Signature 분석

〈그림 3〉 Mov file Hex Code



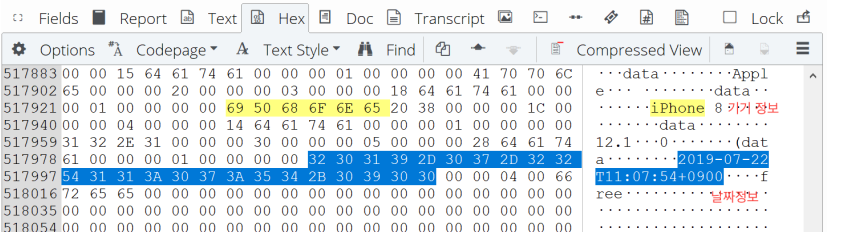
〈그림 4〉 EnCase Raw Search Selected 결과



원본파일을 찾기 위해 포렌식 수사를 진행할 때, 아이폰에서 기본값으로 설정되어 있는 파일의 offset 값을 확인하여 분석한다면 많은 양의 증거파일로부터 아이폰에서 촬영된 파일을 추출하는 것이 가능해진다.

2) Metadata 촬영정보 분석 : 촬영기기(기종), 촬영날짜 정보

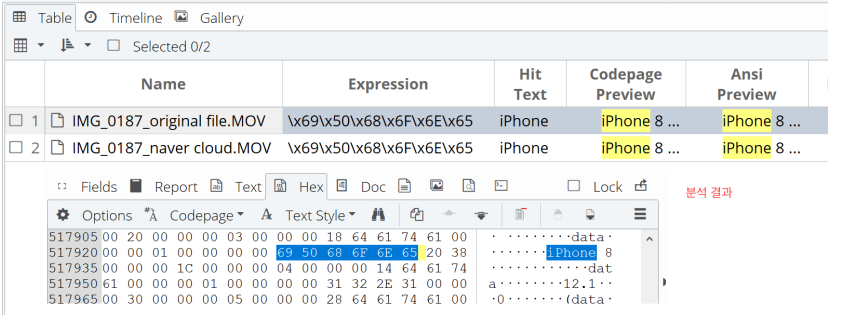
〈그림 5〉 iPhone 촬영 사진의 Metadata 정보



동영상이나 사진과 같은 미디어 디지털 증거의 경우 촬영기기에 따라 파일명이 임의로 작성되고 있다. 그래서 촬영자는 촬영이후 저장하는 과정에 파일명을 변경하는 경우가 대부분으로 만약 이러한 정보만을 선별한다는 것은 파일명만으로는 불가능한 상황이다. 이런 경우 위 내용처럼 피의자 또는 피고인의 촬영기기와 날짜 정보를 가지고 분석하면, 관련성

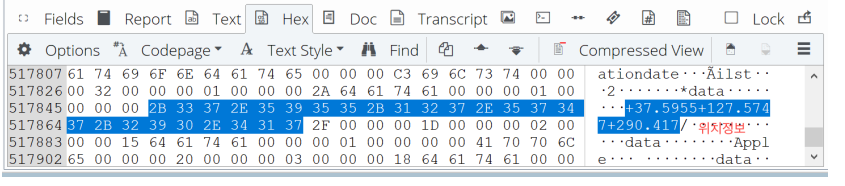
없는 많은 양의 불필요한 데이터를 제외하는 효과가 있을 것이다.

〈그림 6〉 EnCase Raw Search Selected 결과



3) 촬영위치 정보 분석

〈그림 7〉 사진파일에 저장된 촬영 위치 정보



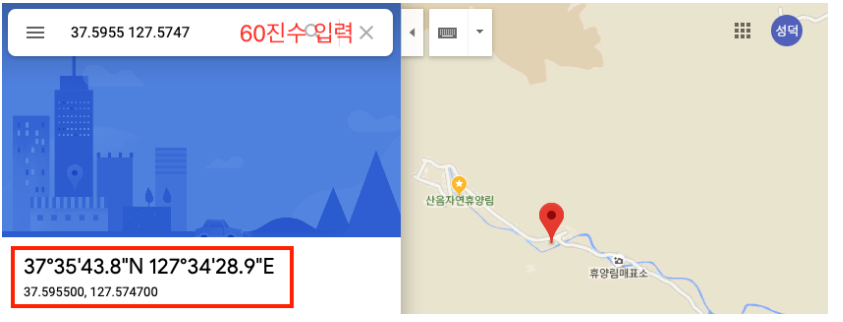
위 데이터를 지도에서 찾기 위해서는 60진수를 표기된 좌표값을 10진수로 변환하여야 하는데 계산식은 아래와 같다.

〈표 2〉 60진수 위치정보 10진수 변환 계산식

구분	60진수	계산식	10진수
위도	+37.5955	0.5955*60 = 35.73 / 0.73*60 = 43.8	37° 35′ 43.8″
경도	+127.7547	0.5747*60 = 34.482 / 0.482*60 = 28.92	127° 34′ 28.9″

디지털 포렌식 관점에서는 계산식을 통한 위도·경도를 파악하여 증거로 사용하는 것이 맞지만 보다 정확하고 촬영자의 장소를 가독성 있게 확인하기 위한 방법으로 60진수의 데이터를 그대로 구글 웹사이트(https://www.google.com/maps)에 지도 검색란에 입력하게 되면 촬영장소를 도식화하여 보여준다.

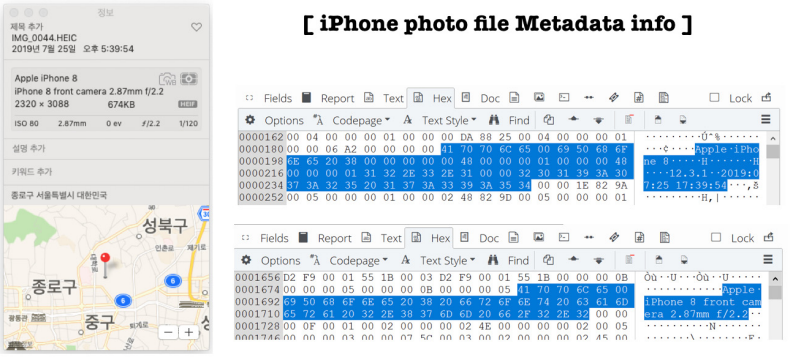
〈그림 8〉 분석된 위치정보(위경도)의 실제위치 결과



iPhone에서 촬영한 사진의 경우에도 많은 정보를 내부에 가지고 있는데 최근 iOS11 업데이트 이후 '고효율 이미지 파일형식'인 HEIF (High Efficiency Image File Format) 의 경우 아직까지 파일 내부구조 연구가 되어 있지 않아 포렌식 관점에서 접근하기 어려운 실정이다.

하지만 기본적인 정보들은 확인 가능하며 이 역시 손쉽게 확인이 가능하도록 하기 위해서는 Mac OS에서 기본으로 지원하는 응용프로그램 <그림 9>를 통해 내부정보를 확인할 수 있다.

〈그림 9〉 아이폰 촬영 사진에 존재하는 메타데이터 분석 결과



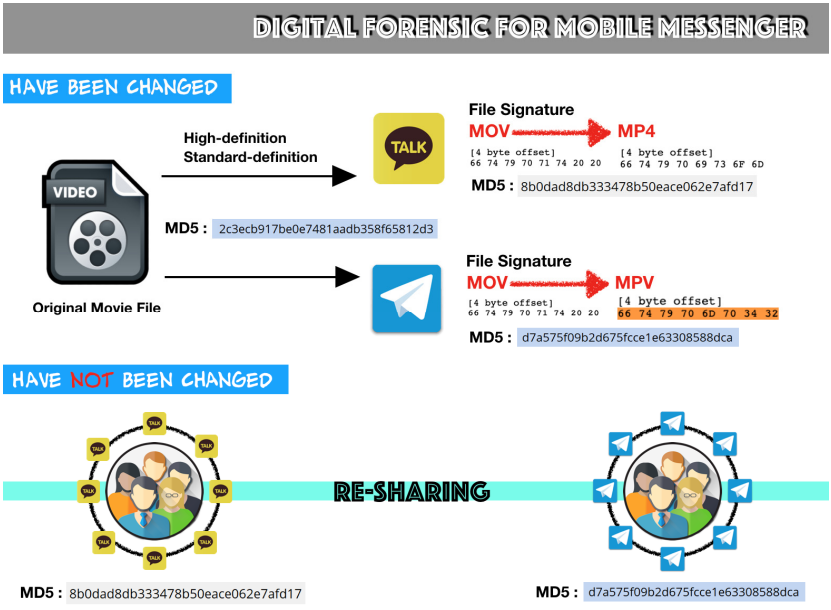
Ⅳ. 모바일 메신저(Mobile Messenger)를 이용한 음란물 유포 확인

〈표 3〉 실험에 사용한 모바일 메신저 정보

서비스명	방식	어플 버전	사용기기
KakaoTalk	Messenger	Mobile v8.4.8 Computer v2.6.3	iPhone 8 (v12.3.1) / KOR SK Telecom
Telegram	Messenger	Mobile v5.9.1 Computer v1.7.14	iPhone 8 (v12.3.1) / KOR SK Telecom

국내에서 가장 많이 사용하는 모바일 메신저는 ‘카카오톡’과 ‘텔레그램’이다. 이 두 가지 응용프로그램을 통해 동영상을 유포한다는 가설을 두고 실험한 결과 전혀 생각하지 못했던 결과를 가지게 되었다. 최초 동영상을 응용프로그램 공급업체에서 지원하는 코덱으로 변환되는 것을 알게 되었고, 이후 같은 메신저를 통해 재배포한다는 전제로 연구한 결과 재배포 과정에서는 어떠한 변화도 일어나지 않는다는 것을 알게 되었다.

〈그림 10〉 모바일 메신저 공유파일 MD5 변화 개요도

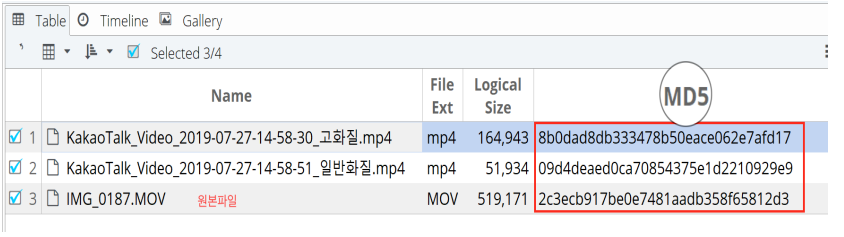


1. 카카오톡 메신저 분석

카카오톡 메신저의 경우 스마트폰에서 촬영된 동영상을 대화방을 통해 제3자에게 전송이 가능하다. 전송되는 동영상의 화질을 사용자가 직접 선택(일반화질, 고화질) 할 수 있으며 응용프로그램 설치 후 아무런 설정을 하지 않은 default 값은 일반화질이 될 것이다.

원본파일 기준으로 고화질, 일반화질 2가지 방식으로 전송한 후 데이터의 변화를 확인한 결과 모두 데이터의 변화가 일어났다. 이것은 수사과정에서 원본파일 정보만으로 유포된 동영상이 누구를 거쳐 몇 번에 재유포가 일어났는지 확인할 방법이 없다는 것을 뜻한다.

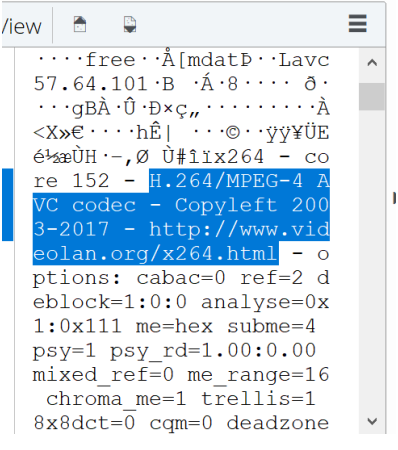
〈그림 11〉 카카오톡 메신저 파일전송에 따른 해쉬값 변화



연구과정에서 알게 된 사실은 카카오톡 스마트폰에서는 원본 그대로 전송하는 기능이 없다는 것이다. 만약 피의자 또는 피고인이 스마트폰에서 촬영한 동영상으로 바로 제3자에게 전송하였다면 아이폰에서 촬영된 동영상 파일(MOV)을 자체 동영상 포맷(MP4) 형태로 변환되어 전송될 것이다.

※ 카카오톡 PC 응용프로그램을 사용하는 동영상 원본(MOV) 형태 그대로 전송이 가능하다

〈그림 12〉 카카오톡 메신저 파일전송 이후 encoding 메타데이터



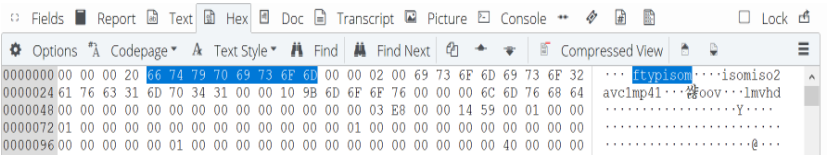
H.264 / MPEG-4 AVC 압축 형식으로 인코딩 하는 무료 소프트웨어 및 응용프로그램을 사용하고 있는 것을 알 수 있다

(디코딩되는 프로그램은 지원하지 않고 있다)

모바일 카카오톡 응용프로그램에서 인코딩 되는 mp4의 File Signature는 아래와 같다.

〈그림 13〉 EnCase 도구에 출력된 MP4 Hex Code 정보

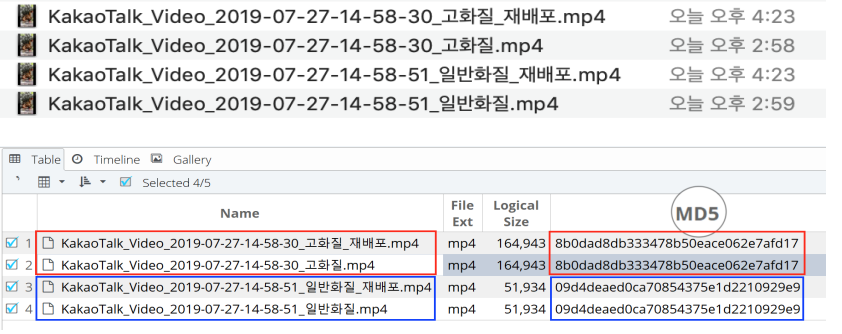
```
[4 byte offset]                    [4 byte offset]
66 74 79 70 69 73 6F 6D            ftypisom
                                MP4 ISO Base Media file (MPEG-4) v1
```



그렇다면 스마트폰에 설치된 카카오톡으로 대화방에서 제3자들에게 동영상을 공유하였고 공유 받은 사람들은 자신의 친구들에게 다시 동영상을 재공유한 이후 피해자가 이런 상황을 알게 된 경우, 동영상 유포로 인한 형벌적 수사 이외에 계속되는 재공유를 막기 위하여 동영상 소지자 전체에 대한 파악이 불가능 한 것일까.

연구결과, 카카오톡 대화방에서 공유된 동영상 파일의 경우 위 내용과 같이 최초 촬영된 동영상 파일의 값이 변하지 않았다. 즉 카카오톡 대화방을 통해 인코딩된 파일을 전송받은 사람이 재배포하고 재배포된 파일을 다시 재재배포하는 경우 모든 파일의 변화가 없다는 것이다. (즉, 최초 카카오톡에서 지원하는 비디오 코덱으로 인코딩된 이후부터 파일의 변화가 없음)

〈그림 14〉 카카오톡을 통한 파일전송시 해쉬함수 변화

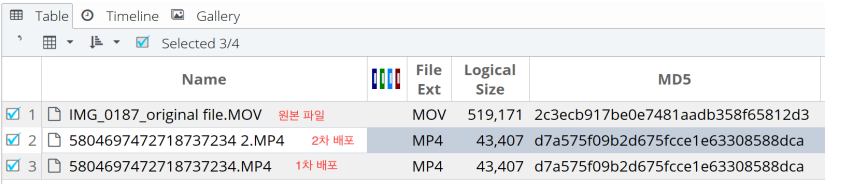


위 분석 결과, 대화방을 통해 전송받은 파일을 2시간 뒤 제3자에게 다시 전송한 결과 2개 파일 모두 어떠한 데이터 변화없이 전송되었음을 확인 할 수 있었다.

2. 텔레그램 메신저 분석

국내에서 보안 메신저로 알려져 있는 모바일 메신저 응용프로그램 「텔레그램」 역시 「카카오톡」과 동일하게 스마트폰에서 제3자에게 전송하는 경우 원본 파일(MOV)이 아닌 자체 인코딩된 mp4 파일 형태로 전송되었으며, 제3자가 다시 재전송하는 경우 데이터 변화 없이 변환된 mp4 파일 형태 그대로 전송됨을 알 수 있었다.

〈그림 15〉 배포순서에 따른 해쉬함수 변화(텔레그램)



3. 모바일 메신저를 통한 음란물 유포 시 동일파일 추출 분석

최근 온라인상에 불법 촬영한 음란물을 유포한 사건에서 범죄자의 처벌뿐만 아니라 불법 유포로 인하여 가장 큰 피해를 받는 피해여성의 회복을 위하여 모든 영상물을 찾아 삭제하는 기법이 필요하다. 하지만 현실적으로 유포된 범위를 정확히 알지 못하고 설사 유포된 곳을 특정 할 수 있다고 하여도 방대한 디지털 파일 중 범죄와 관련된 자료만을 추출하는 것은 상당히 많은 시간과 수사인력이 필요한 현실이다.

그렇다면 이러한 상황에서 가장 좋은 방법은 위에서 연구한 내용과 같이 메신저를 이용한 경우 재배포시 데이터 변화 없이 진행된다는 사실을 바탕으로 유포된 것으로 의심되는 동영상 파일의 원본파일과 유포된 파일을 상대로 파일의 해쉬함수를 이용한다면 전체 데이터 중에서 타겟이 되는 파일만을 추출하는 것이 가능하다고 할 것이다.

다음 3가지 파일에 대해 「해쉬함수」를 이용한 추출 방법은 아래와 같다.

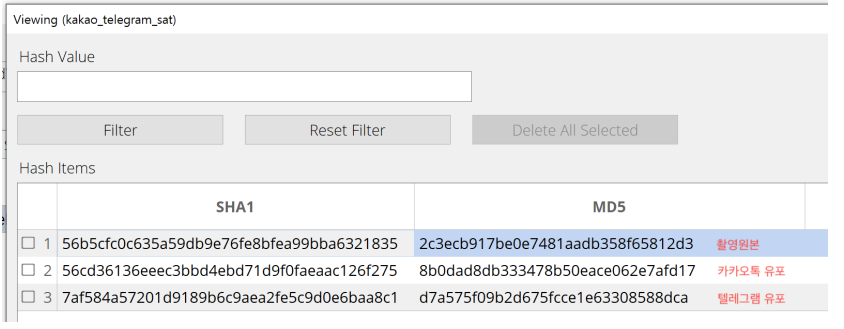
〈표 4〉 유포자 확인을 위한 타겟 파일 해쉬 분석 결과

순번	구 분	md5	sha-1
1	카카오톡	8b0dad8db333478b50eace062e7afd17	56cd36136eeec3bbd4ebd71d9f0faeaac126f275
2	텔레그램	d7a575f09b2d675fcce1e63308588dca	7af584a57201d9189b6c9aea2fe5c9d0e6baa8c1
3	원본파일	2c3ecb917be0e7481aadb358f65812d3	56b5cfc0c635a59db9e76fe8bfea99bba6321835

분석도구는 EnCase Forensic v8.08의 Hash 분석 기능으로 연구하였다.

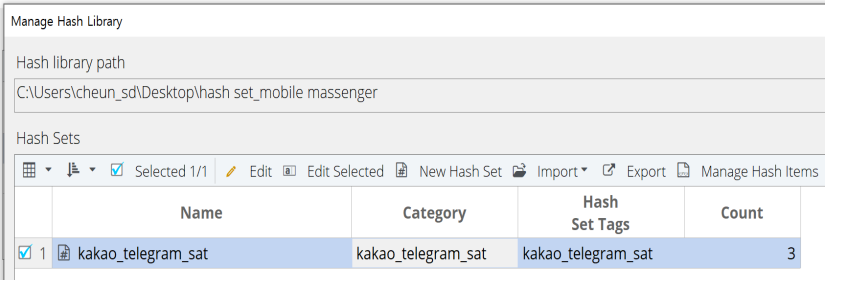
[1. 유포된 것으로 의심되는 파일에 대한 해쉬함수 정보를 입력]

〈그림 16〉 Hash 파일 선택



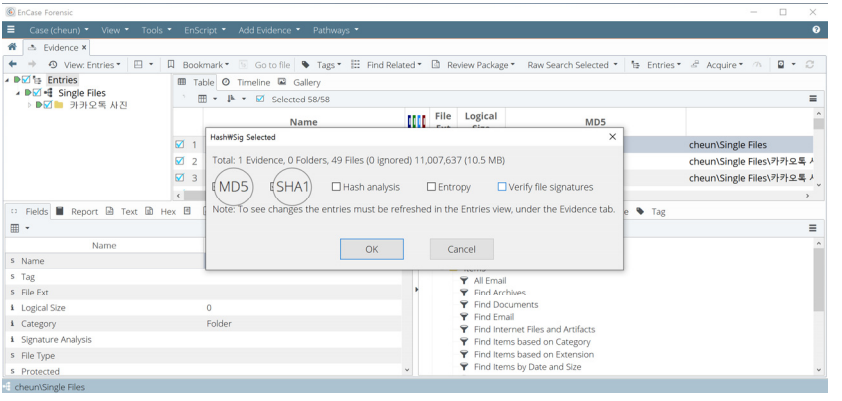
[2. Hash library 생성]

〈그림 17〉 Hash library 생성



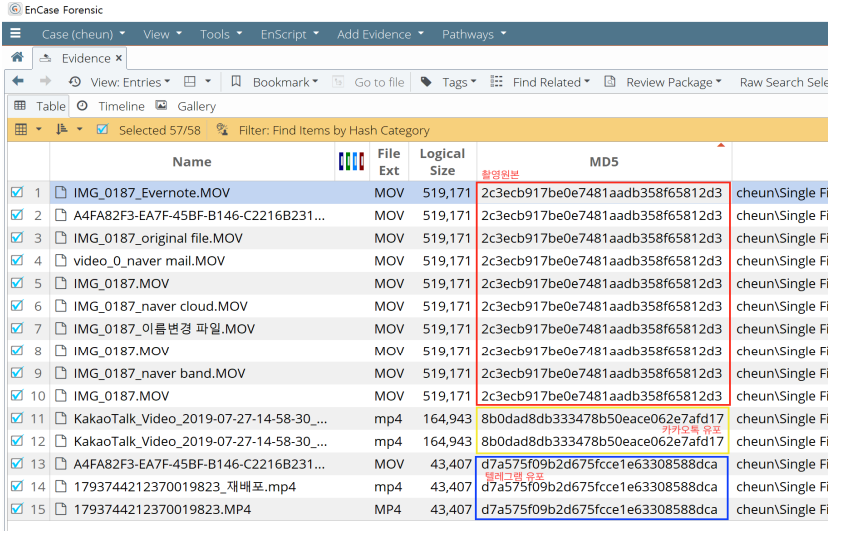
[3. 조사대상 파일들의 해쉬함수 계산]

〈그림 18〉 조사대상이 되는 파일에 대한 해쉬값 계산



[4. 조사대상 해쉬함수 비교 : 조사결과]

〈그림 19〉 조사 데이터 중 유포가 의심되는 파일 추출 결과



위 연구결과, 방대한 양의 디지털 증거파일들 중에서 해쉬함수 값이 동일한 파일만이 선별되었으며 <그림 19>(4. 조사결과)와 같이 선별된 파일들의 파일명이 각각 다르지만 배포된 동영상만을 추출하는데 성공하였다. 위 결과는 가장 대표적인 카카오톡, 텔레그램 2가지 메신저에 대해서만 연구한 결과이며 응용프로그램 설정에 따라 다른 결과 나올 수 있다.

하지만 온라인 음란물의 재배포로 인한 피해자의 또 다른 정신적 피해회복을 위해 대용량의 디지털 증거에서 일정한 조건의 파일만을 빠르게 추출하여 삭제하는 것만으로도 많은 도움이 될 것으로 생각된다.

Ⅴ. 디지털 포렌식 분석 자료에 대한 증거능력

클라우드, 카카오톡, 텔레그램 등 대표적인 메신저상에 불법적으로 음란물을 유포하는 자에 대한 처벌과 해당 음란물에 대한 효과적인 수집과 파기가 성공적으로 이루어지기 위해서는 수사기관의 적법절차, 디지털 증거의 진정성 요건 충족, 그리고 해당 디지털 증거가 전문법칙의 적용을 받는 지에 대한 검토가 필요하다.

1. 압수·수색의 적법성

「헌법」 제12조 제1항에서 “모든 국민은 신체의 자유를 가진다. 누구든지 법률에 의하지 아니하고는 체포·구속·압수·수색 또는 심문을 받지 아니한다.”고 규정하고, 제3항에서는 “체포·구속·압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다.”고 규정하여 헌법상 영장주의를 천명하고 있다.

이러한 영장주의를 구체화한「형사소송법」제199조 제1항에서는「수사에 관하여는 그 목적을 달성하기 위하여 필요한 조사를 할 수 있되, 강제처분은 법률에 특별한 규정이 있는 경우에 한하여, 필요한 최소한도의 범위 안에서 하여야 한다.」규정하고, 제215조에서「검사는 범죄수사에 필요한 때에는 지방법원 판사에게 청구하여 발부받은 영장에 의하여 압수·수색·검증을 할 수 있다.」고 규정하였다.

피고인의 스마트폰은 많은 개인정보 및 프라이버시적인 내용을 포함하고 있는 개인소유의 사유물로서 수사기관은 이에 대한 압수·수색 시 헌법과 형사소송법 규정에 따라 법원에서 발부한 영장에 근거하여 압수·수색을 실시하여야 한다. 영장을 집행함에 있어서도「형사소송법」제106조 제3항에 따라 압수의 범위를 정하여 관련된 정보만을 선별하여 압수·수색하여야 한다.

만약 수사기관이 이러한 적법절차 규정을 준수하지 않으면,「형사소송법」제308조의2 "적법한 절차에 따르지 아니하고 수집한 증거는 증거로 할 수 없다."는 위법수집증거배제의 법칙에 따라 증거로 인정되지 않게 된다. 위법수집증거배제법칙은 위법한 절차에 의하여 수집된 증거의 증거능력을 부정하는 법칙을 말하며, 미국 연방대법원의 판례[10]에 의하여 형성된 미국의 증거법칙이다.[11]

우리의 법제에는 2007년 개정「형사소송법」에 편입되었으며, 당시 증거수집 절차의 적법성을 제고하고 위한 입법취지로 '위법하게'라는 문구 대신 '적법한 절차에 의하지 아니하고'라는 문구를 사용함으로써 '헌법상의 적법절차에 의하지 않은 것'이라고 해석하여 법원의 재량에

10) Silverthorne Lubmer Co. v. U.S., 251 U.S. 385(1929)(독수독과이론을 처음으로 인정한 사건); Nardone v. U.S., 308 U.S. 338(1939)('Fruit of the Poisonous Tree'라는 용어를 처음 사용).

11) 노명선·이완규, 형사소송법(제5판), 성균관대학교 출판부, 2017, 449쪽.

의한 증거배제 여부 결정 가능성을 부여하였다.[12] 그리고 동 규정은 진술증거 뿐만 아니라 비진술증거에도 적용되어 판례실무를 입법적으로 수정하였다는 의미를 갖는다.[13]

하지만 개정 「형사소송법」 제308조의2에서 말하는 '적법한 절차'와 관련하여 해석상의 논란이 있다.[14] 해석과 관련하여 이를 법률에 합치한다는 의미로 해석해야 할지, 「헌법」 제12조 제1항 및 제3항에 규정된 '적법한 절차'의 의미로 해석할지, 아니면 두 의미를 포괄하는 개념으로 해석할지가 명확하지 않다. 또한 경중을 불문하고 모든 위법을 배제사유로 하는 것인지, 법관에게 배제여부를 결정할 재량을 부여하는 것인지, 미국과 같은 예외이론을 인정하고 있는 것인지에 대해서도 분명하지 않다는 문제점이 제기된다.[15]

대법원[16]은 "증거능력배제를 인정하기 위해서는 수사기관의 절차위반행위가 '적법절차의 실질적인 내용'을 침해하는 경우에 해당해야 한다."고 판시하고 있다. 대법원 판결 내용에 따라 제308조의2가 규정한 '적법한 절차'의 광범위한 내용의 범위를 제한하여 실질적 내용의 적법절차를 의미한다고 해석하여야 할 것이다.

이와 관련하여 개정 이전의 학설은 중대하고 본질적 절차규정을 위반한 경우에 위법수집증거배제법칙이 적용된다고 보았다.[17] 무엇이 중대

12) 법무부, 개정 형사소송법, 2007, 226쪽.; 법원행정처, 형사소송법 개정법률해석, 2007, 124쪽.
13) 이완규, 개정형사소송법의 쟁점, 탐구사, 2007, 407쪽.
14) 이에 자세한 내용은 이완규, 앞의 책, 428쪽.
15) 이완규, 앞의 책, 409쪽.; 안성수, "각국의 위법수집증거배제법칙과 우리법상 수용방안", 저스티스, 제96호, 한국법학원, 2007. 02, 235쪽.
16) 대법원 2007. 11. 15. 선고 2007도3061 판결.
17) 이재상, 신형사소송법, 박영사, 2006, 531쪽.; 배종대·이상돈, 형사소송법, 홍문사, 2001, 535쪽.

하고 본질적인 내용인가에 대해서는 ① 영장제도나 적법절차를 규정하고 있는 헌법에 위반하는 경우, ② 수사기관의 수사활동이 형벌 법규에 위반하는 경우, ③ 형사소송법의 효력규정에 위배하여 압수·수색 등이 무효인 경우를 제시하였다.[18]

적법절차의 실질적 내용에 관해서는 기존학설과 법문규정으로는 알 수 없지만, 대법원 판례에 비추어 볼 때 법원은 제308조의2 적용여부를 적법절차의 '실질적 내용'을 기준으로 법관이 판단할 문제로 해석하고 있다. 즉 적법절차의 실질적 내용에 대한 위반이 있는지의 여부는 절차위반행위와 관련된 모든 사정[19]을 전체적이고 종합적으로 살펴서 판단하여야 한다.[20]

2. 디지털 증거의 진정성

대법원[21]은 "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 저장매

18) 김한균 외, 압수·수색과 위법수집증거배제법칙에 관한 연구, 연구총서07-23, 한국형사정책연구원, 2008, 3, 46쪽.
19) ① 절차 조항의 취지와 그 위반의 내용 및 정도, ② 구체적인 위반 경위와 회피가능성, ③ 절차 조항이 보호하고자 하는 권리 또는 법익의 성질과 침해 정도 및 피고인 관련성, ④ 절차 위반행위와 증거수집 사이의 인과관계 등 관성성의 정도, ⑤ 수사기관의 인식과 의도 등.
20) 그 밖의 실무현실상 문제점에 대한 지적은 안성수, 앞의 논문, 236쪽.
21) 대법원 2007. 12. 13. 선고 2007도7257 판결.

체 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."고 판시하였다.

원본성 및 무결성의 입증에 관련하여 대법원[22]은 "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 해쉬값이 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 출력문건을 대조하는 방법 등으로도 그와 같은 무결성·동일성을 인정할 수 있다."고 판시하였다.

대법원은 디지털 증거에 대한 원본성과 무결성 입증방법을 각 단계별 해쉬값을 확보하여 비교하는 방법을 제시하고 있지만, 반드시 이러한 방법만으로 무결성·동일성을 입증하기 보다는 봉인, 봉인해제, 재봉인 절차의 준수 및 관계자의 참여, 포렌식 전문가의 입회 등으로 보관의 연속성이 담보되어 있거나 그밖에 증거 조작 가능성을 의심할 만한 사

22) 대법원 2013. 7. 26. 선고 2013도2511 판결.

정이 없음을 밝힘으로써 디지털 증거의 무결성 및 동일성을 증명할 수도 있다.

그리고 디지털 증거의 동일성 및 무결성 요건에 더하여 디지털 포렌식 절차를 진행하는 수사관(분석관 및 조사관 포함)의 전문성과 디지털 포렌식 도구(포렌식 기계 및 프로그램 등)에 대한 정확성과 신뢰성을 종합적으로 고려하여 디지털 증거에 대한 진정성을 판단하여야 한다.

디지털 증거의 진정성 요건을 정리하면 다음과 같이 정리할 수 있다.[23]

① 디지털 증거는 조작 가능성이 있기 때문에 동일성, 무결성이 인정되어야 한다.
② 디지털 증거에 대한 동일성과 무결성은 해쉬값, 조사관 및 전문가에 의한 증언, 검증·감정 등의 다양한 방법으로 확인할 수 있다.
③ 디지털 증거를 다루는 조작자의 전문성, 포렌식 도구 및 프로그램에 대한 정확성과 신뢰성이 담보되어야 한다.

3. 전문법칙의 적용 여부

대법원[24]은 1999년 "컴퓨터 디스켓에 들어 있는 문건이 증거로 사용되는 경우 그 컴퓨터 디스켓은 그 기재의 매체가 다를 뿐 실질에 있어서는 피고인 또는 피고인 아닌 자의 진술을 기재한 서류와 크게 다를 바 없고, 압수 후의 보관 및 출력과정에 조작의 가능성이 있으며, 기본적으로 반대신문의 기회가 보장되지 않는 점 등에 비추어 그 기재내용

23) 강구민, "대공사건에 있어 전자적 증거의 증거능력", 형사소송 이론과 실무, 제8권 제2호, 한국형사소송법학회, 2016, 12, 147쪽.
24) 대법원 1999. 9. 3. 선고 99도2317 판결.

의 진실성에 관하여는 전문법칙이 적용된다고 할 것이고, 따라서 형사소송법 제313조 제1항에 의하여 그 작성자 또는 진술자의 진술에 의하여 그 성립의 진정함이 증명된 때에 한하여 이를 증거로 사용할 수 있다."라고 판시하면서 최초로 디지털 증거에 대하여 판단을 함과 동시에 전문법칙의 적용 대상임을 확인하였다.

우리의 「형사소송법」은 범죄수사에 있어 중요 증거가 종이문서가 아닌 디지털 정보의 형태로 각종 저장매체에 저장하고 있는 것이 일상화되었음에도 불구하고 아직까지 1961년 '종이문서'에 대해서만 예상한 증거능력 규정을 두어 현실을 반영하지 못한 채 수사 및 재판에 혼선을 준다는 비판이 있었다.[25]

그 결과 유죄 입증의 중요 디지털 증거가 진정성 요건을 충족하여도 전문법칙의 적용을 받아 증거로써 인정받지 못하는 상황이 발생하자 2015년 19대 국회에서 디지털 정보의 형태로 되어 있는 디지털 증거의 증거능력 인정에 관한 규정을 신설하고, 디지털 증거는 서류로 된 증거와 달리 고도의 진정성을 담보할 수 있는 기술적 방법에 의하여 성립의 진정함을 인정하는 것이 가능하므로 이러한 점을 "디지털 전문증거의 증거능력 확대"등을 주요 내용으로 하는 「형사소송법」 개정안에 반영[26]하여 「형사소송법」 제313조 제2항으로 신설되었다.

「형사소송법」 제313조 제2항의 신설로 인하여 정보저장매체에 저장된 진술의 내용을 담은 문건에 대하여 작성자로 추정되는 사람이 '모르는 문건'이라고 주장하여 성립의 진정을 인정하지 않더라도, 디지털 포렌식 등의 객관적 방법으로 디지털 증거에 대한 진정성을 입증할 수 있다.[27]

25) 강구민, "전자적 증거와 관련한 미국의 전문법칙", 형사법의 신동향, 통권 제52호, 대검찰청, 2016. 9, 139쪽.
26) 김진태 의원 대표발의 형사소송법 일부개정법률안(2015. 5. 15).
27) 강구민, 앞의 논문, 155쪽.

4. 컴퓨터로 생성된 기록에 대한 증거능력

디지털 포렌식을 통하여 컴퓨터 분석 시, 다양한 유형의 디지털 정보를 접하게 된다. 이를 3가지로 범주화 하면, (1) 사람의 주장, 감정, 사상이 담긴 기록(hearsay), (2) 컴퓨터 처리 결과 자동적으로 발생된 기록(non-hearsay), (3) 컴퓨터 기록이 앞의 (1)과 (2)가 혼재되어 그 결과 부분적으로 전문증거인 경우로 분류할 수 있다.[28] (1)과 (3)의 경우 사람의 진술이나 주장 등이 담긴 기록은 전문법칙의 적용을 받겠지만, (2)의 경우 컴퓨터 처리과정에서 자동 생성되었기 때문에 전문법칙의 적용을 받지 않게 된다. 컴퓨터 시스템에 의해 자동적으로 생성된 기록은 사람의 인식작용과 관련 없이 컴퓨터 프로그램에 자체적으로 내재되어 있는 알고리즘에 의하여 자동적으로 생성된 정보[29]를 말한다.[30]

미국의 United States v. Hamilton[31] 사건에서 피고인은 약 44장의 아동포르노 사진을 인터넷 토론방에 올려 기소되었다. 피고인은 아동포르노 이미지파일과 관련된 헤더정보에 대하여 전문증거에 해당되기 때문에 증거능력이 배제되어야 한다고 주장하였다. 이미지 파일의 헤더정보에는 주제, 게시된 이미지의 날짜, 그리고 Hamilton의 화면상 이름과 IP주소를 보여줌으로써 인터넷 토론방(newsgroup)에 아동포르노 사진을 게시한 사람이 피고인 Hamilton임을 정황적으로 식별해주고 있

28) Courtroom Evidence, 2nd, Article VIII, United States Department of Justice, OLE. (2001); Steven Goode and Olin G. Welborn, *Courtroom Evidence Handbook,* Ch. 2, pp. 226-280, 2005-2006.

29) 예를 들어 컴퓨터 접속 로그기록, 웹 히스토리, 휴대폰 송·수신정보, 이메일 헤더정보, 전자금융정보, GPS기록, ISP 또는 인터넷 토론방의 로그기록 등

30) 박현준, "이메일 헤더 분석을 통한 전자문서의 작성자 특정과 형사소송법 제315조 전문법칙 예외", 서울대학교, 석사학위논문, 2015, 23쪽.

31) United States v. Hamilton, 413 F.3d 1138 (10th Cir. 2005).

었다. 제10 순회 항소법원은 헤더정보가 토론방에 이미지를 업로드할 때 토론방을 호스팅하는 컴퓨터에 의해 자동적으로 생성된다는 점에 주목하였다. 그리고 항소법원은 컴퓨터 처리과정에 의해 독립적으로 생성된 헤더정보이기 때문에 진술자에 의한 진술이 없을뿐더러 전문증거를 정의하고 있는 연방증거법 제801(c)[32]의 예외에 해당한다고 보았다.[33]

마지막으로 컴퓨터 기록 중 진술이 담긴 기록과 컴퓨터에 의해 생성된 기록이 혼재된 경우 전문법칙을 적용할지 여부가 쟁점이 된다. 이와 관련하여 미국의 많은 법원에서는 연방증거법 제803(6)[34] 규정에 근거하여 컴퓨터에 저장된 기록을 업무상 정기적 활동에 대한 기록으로 허용하고 있다.[35] 이 때 법원은 제803(6)의 요건을 엄격하게 해석하기 보

32) Rule 801(c) Hearsay.—"Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.

33) United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003): "header information automatically generated by a fax machine was not hearsay as "nothing 'said' by a machine … is hearsay."

34) Rule 803(6) Records of regularly conducted activity.—A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

35) United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991); United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988).

다는 폭넓게 해석하여 컴퓨터 기록을 증거로 인정하고 있다.

United States v. Cestnik[36] 판결에서 "컴퓨터에 저장된 업무상 기록은 (1) 기록의 정확성을 보장하기 위해 고안된 기계적인 절차에 따라서 지속적으로 그 기록이 유지되어야 하고, (2) 소송준비를 염두에 두지 않은 기록들이어야 하고, (3) 기록자체가 단지 전문진술의 축적(accumulations of hearsay)이 아닌 기록이어야 한다."는 요건을 제시하고 있다.

United States v. Briscoe[37] 판결에서 "업무상 기록은 정기적으로 행해지는 업무활동의 과정에서 기록된 것이고, 이러한 기록은 사업상 관례이며, 기록 보관자(custodian) 또는 자격을 갖춘 다른 증인의 증언에 의하여 입증될 때, 컴퓨터에 저장된 기록은 업무상 기록으로 허용되어 전문법칙의 예외에 해당된다."고 판시하였다.

특히 email이나 대화기록(chat logs)과 같은 컴퓨터 기록은 범죄와 관련된 일종의 피고인의 고백을 담고 있거나 범죄 관련 일부 내용을 담고 있어 연방증거법 제801(d)(2)[38]에 의해서 전문진술이 아니다. 위 규

36) United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994).
37) United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990).
38) Rule 801(d)(2) Statements which are not hearsay.—A statement is not hearsay if— Admission by party-opponent.—The statement is offered against a party and is (A) the party's own statement, in either an individual or a representative capacity or (B) a statement of which the party has manifested an adoption or belief in its truth, or (C) a statement by a person authorized by the party to make a statement concerning the subject, or (D) a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship, or (E) a statement by a coconspirator of a party during the course and in furtherance of the conspiracy. The contents of the statement shall be considered but are not alone sufficient to establish the declarant's authority under subdivision (C), the agency or employment relationship and scope thereof under subdivision (D), or the existence of the

정의 해석에 따라 United States v. Burt[39] 판결에서 법원은 “피고와 증인이 주고받은 대화기록은 전문진술에 해당되지 않는다.”고 보았다.[40] 또한 United States v. Safavian[41] 판결에서도 법원은 피고인에 의해서 다른 사람들에게 전송된 이메일 전문(the full text of some emails)을 증거로 허용하였다.[42]

이메일에 첨부된 파일이나 대화기록은 진술이 담긴 전문증거로써 원칙적으로 전문법칙이 적용된다. 소위 ‘전 국정원장에 대한 선거법위반 사건’ 원심[43]에서는 쟁점이 된 2개의 첨부파일에 대하여 「형사소송법」 제313조 제1항을 적용하여 배척되었다. 하지만 항소심[44]과 대법원[45]에서는 2개의 첨부파일의 이름, 작성된 일자, 내용, 활동내역, 통화내역, 이메일 헤더정도, IP주소 등 제반사정들을 종합하여 2개 파일의 작성자로 특정하여 「형사소송법」 제315조 제2호 ‘상업장부, 항해일지 기타 업무상 필요로 작성한 통상문서’로 보아 증거능력을 인정하였다.

Ⅵ. 결론

온라인상에 불법 촬영된 동영상이 유포되어 피해자가 이를 인지하고

conspiracy and the participation therein of the declarant and the party against whom the statement is offered under subdivision (E).

39) United States v. Burt, 495 F.3d 733, 738-39 (7th Cir. 2007).

40) 증인이 피고의 대화내용을 고백의 문맥(context)으로 받아들이고 있는 동안 피고의 대화는 고백이 된다.

41) United States v. Safavian, 435 F. Supp. 2d 36, 43-44 (D.D.C. 2006).

42) 전문의 내용은 피고인의 진술이 진실하다는 것을 명백히 보여줬다.

43) 서울중앙지방법원 2014. 9. 11. 선고 2013고합577, 2013고합1060(병합) 판결.

44) 서울고등법원 2015. 2. 9. 선고 2014노2820 판결.

45) 대법원 2015. 7. 16. 선고 2015도2625 판결.

경찰에 수사요청을 하지만, 해당 동영상에 대해서만 삭제하고 게시한 피의자만을 처벌하는 데 그치고 만다. 이후에 같은 내용의 또 다른 동영상이 온라인상에 재유포되더라도 원본이나 해당 동영상 전부를 삭제·파기하기에는 현실적으로 한계가 있어 어쩌면 피해자에게 평생 치유할 수 없는 상처로 남게 된다. 이러한 고민에서 시작된 본 논문에서의 연구는 온라인상에 돌아다니는 모든 음란물에 대한 완벽한 삭제를 위한 단초를 제공한다는 점에서 본 연구의 의의를 두고 싶다.

본 연구는 불법 촬영된 음란물을 나의 스마트폰으로 찍고 여러 클라우드 어플리케이션 및 카카오톡과 텔레그램 메신저상에 유포·재유포함으로써 파일 내부구조와 파일시스템의 변화를 비교하는 것이다. 이러한 실험을 통하여 최초 원본파일과 재유포된 파일의 해쉬함수를 이용하여 타겟이 되는 파일만을 추출하여 완전 삭제를 도모하였다. 그리고 이러한 디지털 포렌식 과정으로부터 획득한 디지털 증거가 법정에서 증거능력을 갖기 위한 요건들을 함께 제시하였다.

우선 클라우드를 통한 음란물 유포과정에서는, 클라우드 제공업체인 Naver, Daum, Evernote가 지원하는 앱 응용프로그램을 대상으로 최초 촬영한 동영상을 업로드한 후 다시 다운로드 함으로써 동영상 파일의 변화를 비교하였다. 실험 결과는 모두 변화가 없었다. 이러한 특징으로 최초 원본파일에 대한 분석을 통하여 구분할 필요가 있다.

다음으로 모바일 메신저를 통한 음란물 유포의 경우, 이용자가 가장 많은 '카카오톡'과 '텔레그램'을 선정하여 이 두 가지 앱 응용프로그램을 통해 동영상을 유포하고 그 과정에서 동영상 파일의 변화를 비교하였다. 기본적으로 원본파일은 응용프로그램 공급업체에서 지원하는 코덱으로 변환되어 자체 인코딩된 'MP4' 파일 형태로 전송된다. 전송 받은 동영상을 재전송하는 경우에도 데이터 변화 없이 변환된 'MP4' 파

일 형태 그대로 재전송되었다.

카카오톡과 텔레그램을 통하여 전송한 동영상은 원본이 아닌 MP4 파일 형태로 전환되고, 재전송하더라도 해쉬값의 변화가 없음을 확인하였다. 이러한 연구결과를 바탕으로 원본파일과 유포된 파일의 해쉬함수를 이용하여 방대한 데이터로부터 타겟이 되는 동영상 파일만을 찾아 삭제하는 수사기법을 제안한다.

마지막으로 디지털 포렌식 분석을 통하여 수집된 디지털 증거가 법정에서 유효한 증거가 되기 위해서는 수사기관의 적법절차, 디지털 증거의 진정성, 전문법칙의 관문을 통과해야만 비로소 증거능력을 갖추게 된다. 디지털 증거는 새로운 형태의 증거로써 기존의 물적 증거에 대한 압수·수색 방법보다 더 면밀한 주의가 필요하다. 포렌식에 대한 전문지식과 경험을 가진 분석관은 검증된 포렌식 도구를 사용하여 디지털 증거의 수집부터 법정에 증거로 제출하기까지 위변조 없이 동일성과 무결성을 유지하여야 한다. 그리고 디지털 증거에 진술이 담겨 있다면 전문법칙의 적용을 받겠지만, 본 논문의 실험결과는 모두 컴퓨터 시스템에 의해 자동 생성된 기록에 해당되기 때문에 전문법칙의 예외에 해당되어 당연 증거로 활용할 수 있다.

〈논문접수 : 2019. 8. 4, 심사개시 : 2019. 8. 7, 게재확정 : 2019. 9. 9.〉

참 고 문 헌

Ⅰ. 국내 문헌

1. 단행본

김진태 의원, 형사소송법 일부 개정법률안, 2015. 5. 15.

김한균 외, 압수·수색과 위법수집증거배제법칙에 관한 연구, 연구총서 07-23, 한국형사정책연구원, 2008.

노명선·이완규, 형사소송법(제5판), 성균관대학교 출판부, 2017.

법무부, 개정 형사소송법, 2007.

법원행정처, 형사소송법 개정법률 해석, 2007.

배종대·이상돈, 형사소송법, 홍문사, 2001.

이완규, 개정형사소송법의 쟁점, 탐구사, 2007.

이재상, 신형사소송법, 박영사, 2006.

2. 논문

강구민, “대공사건에 있어 전자적 증거의 증거능력”, 형사소송 이론과 실무, 제8권 제2호, 한국형사소송법학회, 2016.

강구민, “전자적 증거와 관련한 미국의 전문법칙”, 형사법의 신동향, 통권 제52호, 대검찰청, 2016.

김수아·장다혜, “온라인 피해 경험을 통해 본 성적 대상화와 온라인 성폭력 문제”, 미디어 제더&문화, 제34권 제1호, 한국여성커뮤니케이션학회, 2019.

류진철·이형일, “사이버음란물 유포행위의 형사법적 규제”, 법학논총, 제14권 제1호, 조선대학교 법학연구소, 2007.

박준석, “음란물의 저작물성 및 저작권침해금지청구 등의 가능성 -대법원 2015. 6. 11. 선고 2011도10872판결-”, 법조, 제65권 제9호, 법조협회, 2016.

박현준, “이메일 헤더 분석을 통한 전자문서의 작성자 특정과 형사소송법 제315조 전문법칙 예외”, 서울대학교, 석사학위논문, 2015.

박희영, “사이버 음란물 유포행위와 형사책임”, 법학연구, 제43권 제1호, 부산대학교 법학연구소, 2002.

서승희, “사이버성폭력 피해의 특성과 근절을 위한 대응방안 -비동의 유포 성적촬영물을 중심으로-”, 이화젠더법학, 제9권 제3호, 이화여자대학교 젠더법학연구소, 2017.

손현구 외, “트래픽 모니터링을 통한 P2P 및 웹 하드 다운로드응용의 파일이름 식별 방법”, 정보통신, 제37권 제6호, 한국정보과학회, 2010.

안성수, “각국의 위법수집증거배제법칙과 우리법상 수용방안”, 저스티스, 제96호, 한국법학원, 2007.

이동훈, “사이버 음란물 규제 방안에 대한 고찰 -‘SNS 앱’을 중심으로-”, 글로벌 기업법무 리뷰, 제9권 제2호, 경희대학교 법학연구소, 2016.

이정훈·천우성, “디지털 증거 수집과 분석을 위한 스마트폰 포렌식 적용 연구”, 정보보호학회지, 제21권 제6호, 한국정보보호학회, 2011.

이흔재, “아동음란물소지죄에 관한 형사정책 및 형법상의 문제점”, 형사정책연구, 제25권 제4호, 한국형사정책연구원, 2014.

진경아 외, “메타데이터를 이용한 파일 유출 추적에 관한 연구”, 한국통신학회 학술대회논문집(2018년도 동계종합학술발표회), 한국통신학회, 2018.

최민석·최성욱, “저작권 보호를 위한 대표 색상 시퀀스를 이용한 동영상 복사검출 방법”, 디지털융복합연구, 제10권 제5호, 한국디지털정책학회, 2012.

최아영, “아동·청소년 음란물 유포자자 추적 방안에 관한 연구 : 비트 토렌트에 대한 포렌식 중심으로”, 동국대학교 국제정보대학원 석사학위 논문, 2014.

최윤기, "'해운대'류 불법복제 동영상 검색-단속 기법", 경찰연구논집, 제6권, 한국경찰이론과실무학회, 2010.

홍태석, "일본에 있어 아동음란물 다운로드 행위의 가벌성 논의", 법학연구, 제17권 제4호, 한국법학회, 2017.

3. 기타

김종원, "[단독] 정준영, 불법촬영 후 카톡방에 전송...피해자 최소 10명", SBS 뉴스, 2019. 3. 11.

장경운, "지하철서 '스마트폰'으로 여성 치마 속 '몰카'찍다 딱 걸린 변태남", 인사이트, 2019. 5. 28.

KT경제연구소·DMC미디어, '2019 모바일 메신저 앱 이용 행태' 보고서, 2019. 6. 3.

Ⅱ. 외국 문헌

Courtroom Evidence, 2nd, Article VIII, United States Department of Justice, OLE (2001).

Steven Goode and Olin G. Welborn, *Courtroom Evidence Handbook,* Ch.2, 2005-2006.

< ABSTRACT >

A Study on the Identification of the First Person to Distribute Online Pornography through Digital Forensics Analysis

- In Focus on Cloud, KakaoTalk, Telegram -

Cheun, Seung-Deuk · Kang, Gu-Min

In early 2019, there was an incident that a celebrity illegally filmed a scene of sexual assault and shared it with other celebrities in SNS group chat in South Korea. People has been aware of the seriousness of sexual crimes after learning of this report. Especially, distributing obscene materials is a one of incurable crimes because it is highly contagious. In addition, it can infringe on a one's life and personal rights. Moreover, it is difficult to find and destroy all pornographic materials under investigation because some materials can be reproduced and then issued again. This study suggests the method to find and destroy all illegal pornography materials to prevent the occurrence of victims. In particular, the experiment is conducted on the hypothesis that pornographic videos are spread out through Could app, Kakaotalk, and Telegram because given obscene materials are usually filmed and distributed in messenger apps by smartphones. Although the number of cases has been calculated and tested, this study has been proceeded with using iPhone 8 (v12.3.1) only in limited experiment. The study finds that neither the original video nor the downloaded file changed on cloud app. Furthermore, original video convert into codec supported by application vendor and redistribute

through messenger, but no change occurs. Based on research, it is possible to extract only relevant video files through using distributed videos' hash value and original file's hash value. In addition, digital evidence collected through this method of analysis can have legal ability of evidence when method meets the requirements such as legitimate procedures of the investigative agency, authenticity of digital evidence, and hearsay rule.

◈ Key words : Online Pornographic, Digital Forensic, Digital Evidence, Cloud, Kakaotalk, Telegram