ISSN : 1976-5304
https://kdfs.jams.or.kr

EXO 파일 재조합을 통한 영상 데이터 획득 방법에 대한 연구

한 용 현*, 이 상 진**
경기남부지방경찰청 (디지털증거분석관)*, 고려대학교 정보보호대학원 (교수)**

A Study on Video Data Acquisition Method through EXO File Recombination

Yonghyun Han*, Sangjin Lee**
Gyeonggi Nambu Provincial Police Agency (Digital Forensic Investigator)*
Graduate School of Information Security, Korea University (Professor)**

요 약

많은 사람들이 스마트폰을 이용해 스트리밍 동영상을 시청하고 있다. 스트리밍 동영상을 시청할 경우에 스마트폰 이용자가 어떤 동영상을 시청했는지 알 수 있는 방법이 없다. 페이스북, 인스타그램, 트위터, 텀블러 등과 같이 전세계적으로 사용되는 다수의 앱들은 ExoPlayer를 이용하여 스마트폰 이용자들에게 스트리밍 동영상을 제공하고 있다. ExoPlayer를 이용해 동영상을 재생할 경우, 빠른 재생을 위해 캐시 파일(.exo)이 분할되어 스마트폰에 저장되는데 분할 캐시 파일(.exo)을 재조합하여 스마트폰 이용자가 재생한 스트리밍 영상이 무엇인지 알 수 있도록 복원할 수 있다면 포렌식 관점에서 유의미하게 사용될 수 있을 것이다. 본 논문에서는 ExoPlayer에 의해 생성된 분할 캐시 파일(.exo)을 재조합하는 방법을 제안하며, 디지털포렌식 업무에 활용할 수 있도록 재조합 도구를 함께 개발하였다.

주제어 : 디지털 포렌식, EXO 파일 재조합, 분할 영상 캐시 파일 재조합, ExoPlayer

ABSTRACT

Many people are watching streaming videos using their smartphones. When watching streaming video, there is no way for a smartphone user to know what video they watched. Many apps around the world, such as Facebook, Instagram, Twitter, and Tumblr, use ExoPlayer to provide streaming video to smartphone users. When playing a video using ExoPlayer, the c ache file (.exo) is divided and stored in the smartphone for fast playback. If it can be restored, it can be used significantly from the forensic point of view. In this paper, we studied the method of recombining the split cache file (.exo) created by ExoPlayer and developed the recombination tool to be used for digital forensic.

Key Words : DigitalForensics, Exo file recombination, Split image cache file recombination, ExoPlayer

Ⅰ. 서 론

미국의 여론조사 기관인 퓨 리서치(Pew Research Center)가 2019년 전세계 스마트폰 보급률을 조사한 결과에서 한국이 95%로 1위를 차지했다[1]. 스마트폰 보급률이 높은 만큼 한국에서는 스마트폰을 이용하여 소셜 네트워크 서비스 앱인 페이스북, 인스타그램, 네이버 밴드 등과 메신저 앱인 카카오톡, 페이스북 메신저, 라인, 텔레그램을 이용하여 사람들과 소통하는 비율이 증가하고 있다. 그리고 소통하는 방식이 문자나 사진이 아닌 동영상을 통해 소통하는 비율이 증가하고 있다. 이에, 소셜 네트워크 서비스 앱들은 사용자들에게 끊김 없는 실시간 스트리밍 동영상을 제공해주기 위해 구글에서 개발한 ExoPlayer를 자신들의 앱에 적용하고 있다. 과거에는 스마트폰을 이용해 스트리밍 동영상을 재생하면 버퍼링이 생기면서 빠른 재생이 어려운 경우가 있었지만 ExoPlayer를 이용할 경우, 버퍼링을 최소화하면서 스마트폰 이용자들에게 스트리밍 동영상을 제공할 수 있게 되었다.

스마트폰 이용자들이 스트리밍 동영상을 많이 이용함에 따라 디지털포렌식 관점에서 어떤 스트리밍 동영상이 스마트폰 내에서 재생되었는지 알 필요성이 있다. 만약, 범죄가 발생한 시각에 재생된 스트리밍 동영상이 스마트폰 내 존재하고, 해당 영상을 복원할 수 있다면 범죄 혐의를 입증할 수 있는 중요한 단서가 될 수 있기 때문이다.

ExoPlayer에서는 재생된 스트리밍 동영상에 대해 exo 확장자를 갖는 캐시 파일(이하 'exo 파일'이라 한다.)로 저장하고 있고,

▪ Received 07 November 2019, Revised 28 November 2019, Accepted 17 December 2019
▪ 제1저자(First Author) : Yonghyun Han (Email : yh.john85@gmail.com)
▪ 교신저자(Corresponding Author) : Sangjin Lee (Email : sangjin@korea.ac.kr)

exo 파일은 분할된 형태로 저장되는 특징이 있다. 본 논문에서는 분할된 형태로 저장된 exo 파일에 대한 분석 및 재조합을 통해 재생된 스트리밍 동영상이 어떤 동영상이었는지 확인할 수 있는 방안을 제안한다. 특히, 국내 사용자들이 많이 사용하고 있는 밴드, 인스타그램, 페이스북, 페이스북 메신저, 텀블러를 대상으로 분석을 진행하였으며, 이 앱들이 생성한 exo 파일들의 재조합을 통해 재생되었던 스트리밍 동영상이 무엇인지 확인할 수 있도록 분석하였다. 더불어 exo 파일들을 재조합 할 수 있는 자동화 도구를 개발함으로써 디지털포렌식 분석에 활용될 수 있도록 하였다.

Ⅱ. 기존 연구 동향

2014년 Kang Sheng은 PC 디스크 내 존재하는 부분 동영상 파일과 분할된 동영상 파일에서 SPS(Sequence Parameter Set RBSP syntax), PPS(Pic Parameter Set RBPS syntax)에 대한 구조 분석 및 재구성을 통해 IDR 프레임을 복구한 결과를 발표하였다[2]. Kang Sheng은 분할된 동영상 파일에서 IDR 프레임을 복구하는 방안에 대해 분석하였지만 어떤 형태의 분할된 동영상을 연구 대상으로 할 것인지 명확히 하지 않았고, 실제 복구된 결과를 보여주지 않았다.

2018년 Graeme Horsman은 스트리밍된 동영상 파일 복구에 대한 연구 결과를 발표하였다[3]. Graeme Horsman은 PC를 이용하여 Youtube와 Facebook의 스트리밍 동영상을 재생할 때 생성되는 캐시 파일의 흔적을 분석하였으며, 스트리밍 동영상의 재조합 형태를 분석하였다. 다만, PC 내 크롬 브라우저를 통해 재생된 스트리밍 동영상에 대해서만 분석하였고, 분할된 동영상들의 재조합 구조를 보여줬을 뿐 재조합하는 방법에 대한 분석은 이루어지지 않았다.

본 논문에서는 PC가 아닌 안드로이드 스마트폰을 대상으로 진행하였으며, 국내 스마트폰 이용자들이 다수 사용하고 있는 앱들이 ExoPlayer를 이용하여 스트리밍 동영상을 재생할 경우 생성되는 exo 파일의 구조를 분석하고, 다수의 exo 파일로 분할되어 저장될 경우, 스트리밍된 동영상이 무엇이었는지 알 수 있도록 exo 파일을 재조합하는 영상 복구 기법을 제안한다.

Ⅲ. ExoPlayer 사용현황

3.1. ExoPlayer 개요

2014년 구글에서는 안드로이드 기반의 오픈 소스 미디어 재생 라이브러리인 ExoPlayer를 오픈 소스로 공개하였다[4]. ExoPlayer는 YouTube나 Google Play Movies와 같은 구글의 Android 앱에서 사용하기 위해 개발된 라이브러리이며, 표준 오디오 및 비디오 구성 요소는 Android 4.1(API Level 16)에서 출시된 Android's MediaCodec API를 기반으로 하고 있다. Android 운영체제 내 종속되어 있는 Android MediaPlayer와는 달리 ExoPlayer는 라이브러리 형태로 공개되어 있기 때문에 개발자들이 앱에 포함하여 개발할 수 있어 버전 관리가 용이하며, 사용 목적에 따라 확장 및 수정이 용이하다. 또한, Android MediaPlayer에서 제공하지 못했던 DASH, SmoothStreaming, HLS 등의 다양한 동영상 포맷들에 대한 지원이 가능하다. 이와 같은 장점으로 인해, ExoPlayer는 구글 플레이스토어에 등록된 약 140,000개의 앱에서 사용 중이다.[4]

스마트폰을 이용하는 사용자들은 한 곳에서 스마트폰을 사용하는 경우보다 이동하면서 사용하는 경우가 다수이다. 또한, 이동 중에 스마트폰을 사용할 경우, 인터넷 연결 형태가 바뀌는 상황이 발생한다. 예를 들어, 이동 중인 지하철에서 제공하는 와이파이를 이용하다가 지하철에서 하차 후, 도보로 이동하면서 통신사의 데이터 통신을 이용한다. 이와 같은 물리적 위치 변경에 따른 인터넷 연결 형태의 변화는 모바일 기기의 인터넷 접속 속도에 영향을 준다.

ExoPlayer는 인터넷 접속 속도에 따른 실시간 동영상 재생 속도 지연을 방지하기 위해, exo 파일을 생성하여 스마트폰 내 저장하고 있다. 인터넷 속도가 느린 곳에서는 약 2초의 재생시간을 갖는 exo 파일을 생성하여 스마트폰 이용자로 하여금 재생이 지연되지 않을 수 있도록 해주며, 비교적 인터넷 속도가 빠른 곳에서는 긴 재생시간을 갖는 exo 파일을 생성한다. exo 파일은 인터넷 접속 속도 및 스트리밍 동영상의 크기에 따라 생성되는 개수와 파일 크기가 달라진다.

SNS 앱 중 다수가 스트리밍 동영상을 재생하기 위해 ExoPlayer를 이용하고 있으며, 이 앱들이 사용하는 특정 영역에 exo 파일들이 저장되어 있다. 만약, exo 파일들의 특징을 분석하고, 분할된 형태의 exo 파일들을 재조합하여 스마트폰 이용자가 재생한 스트리밍 동영상이 무엇인지 알 수 있다면 디지털 포렌식 관점에서 유의미하게 사용될 수 있을 것이다. 대표적인 메신저 및 SNS 앱들을 대상으로 ExoPlayer를 사용하는지 조사한 결과, 페이스북 메신저, 페이스북, 인스타그램, 밴드, 텀블러가 스트리밍 동영상 재생을 위해 ExoPlayer를 사용하고 있음을 확인하였다. 위 앱들의 최신 버전에서 사용되는 ExoPlayer 버전은 [표 1]과 같다.

Table 1. ExoPlayer version by app
표 1. 앱 별 ExoPlayer 버전

앱 이름	앱 버전	ExoPlayer 버전
밴드	7.5.2.0	ExoPlayerLib 2.9.6
인스타그램	114.0.0.38.120	ExoPlayerLib 2.8.1
페이스북	244.0.0.0.15	ExoPlayerLib 2
페이스북 메신저	236.0.0.14.120	ExoPlayerLib 2.8.1
텀블러	14.4.0.00	ExoPlayerLib 2.7.1

3.2. exo 파일 연구의 필요성

〔그림 1〕은 2009년부터 2018년 사이 디지털증거분석 현황이다〔5〕. 스마트폰을 포함한 모바일 기기의 2018년 디지털증거분석 건수는 36,986건으로 전체 45,103건의 82%를 차지하고 있다.

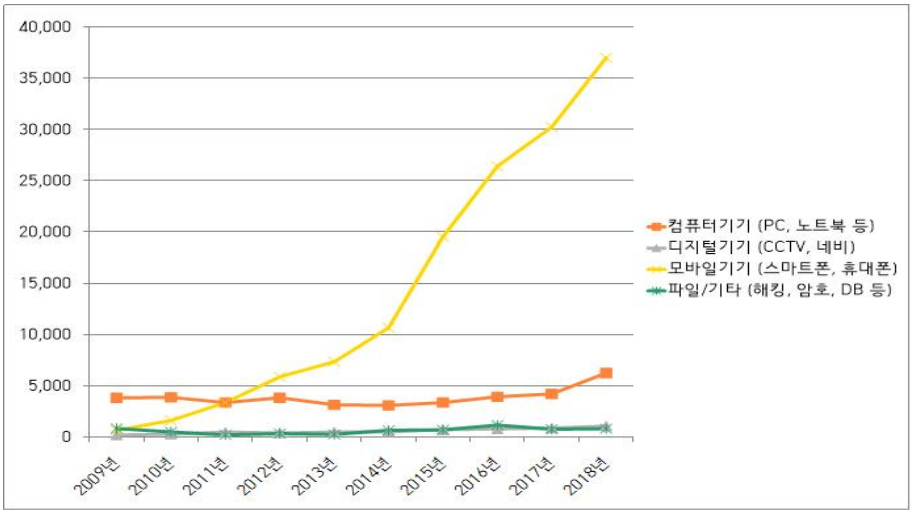


그림 1. 2009년 ~ 2018년 매체별 디지털증거분석 현황 (출처 :경찰청)
Fig. 1. Status of digital evidence analysis by media in 2009 ~ 2018

과학기술정보통신부와 한국인터넷진흥원은 2018년 인터넷이용실태조사를 통해 인터넷 이용자의 95%가 모바일 메신저를 사용하고 있고, 인터넷 이용자의 65%가 SNS를 사용하고 있다고 발표하였다. 또한, 위 인터넷이용실태조사에서는 모바일 기기 사용자들이 여가활동의 87%를 이미지, 동영상, 영화를 보고 있으며, 밴드, 인스타그램, 페이스북, 페이스북 메신저, 텀블러가 전체 사용률 중 상당히 높은 비율로 국내 모바일 기기 이용자들에 의해 사용되고 있다고 발표하였다〔6〕.

이 통계들을 통해, 동영상을 재생했던 모바일 기기들이 수사기관에 디지털증거분석 의뢰될 가능성이 상당히 높음을 알 수 있다. 만약, 범죄와 관련된 피해자, 피의자, 참고인들이 밴드, 인스타그램, 페이스북, 페이스북 메신저, 텀블러를 통해 스트리밍 동영상을 재생한 적이 있고, 그 동영상이 범죄 혐의 입증에 단서가 될 수 있다면, exo 파일에 대한 분석은 사건 수사에 필요한 주요 단서를 제공할 수 있다.

Ⅳ. exo 파일 특성 분석

4.1. mp4 파일 포맷과 H.264 코덱

exo 파일들은 MP4(MPEG-4 파트 14) 파일 포맷을 사용하면서 H.264 코덱으로 프레임들을 압축하고 있다. MP4 포맷은 MPEG-4 파트 12(ISO Base Media File Format)의 기능을 확장하여 만들어졌으며, 음성 데이터, 영상 데이터를 독립적으로 또는 혼합하여 저장할 수 있다〔7〕〔8〕. MP4 포맷은 ftyp, moov, mdat이라는 3개의 주요 컨테이너를 비롯하여 여러 종류의 컨테이너들과 컨테이너 내 실제 데이터, 메타 데이터 등을 저장하는 아톰으로 구성된다. 주요 컨테이너 중의 하나인 ftyp 컨테이너는 파일의 종류, 호환이 가능한 포맷 및 버전 정보 등을 저장하고 있고, moov 컨테이너는 아톰들로 구성되어 있으며, 비디오, 오디오 데이터에 대한 메타 정보 등이 저장된다. mdat 컨테이너에는 실제 재생되는 음성, 영상 데이터가 프레임 단위로 저장되어 있다〔9〕〔10〕.

MP4 포맷의 동영상 파일 내에는 영상 재생을 하기 위해 다수의 프레임들이 저장되어 있다. 만약, 저장된 다수의 프레임들이 가공 없이 그대로 저장될 경우, 동영상 파일의 크기가 커지게 된다. 이에, 동영상 파일들은 코덱으로 프레임들을 압축하여 저장하는데, 본 연구의 대상이 되는 앱들의 exo 파일들은 프레임 압축 시, 모두 H.264 코덱을 사용하고 있다.

H.264 코덱 내에서 가장 기본이 되는 프레임을 I 프레임 혹은 IDR 프레임이라 하고, 앞, 뒤 프레임들의 데이터를 비교하여 변경되는 부분만 인코딩하는 프레임을 B 프레임, P 프레임 혹은 non-IDR 프레임이라 한다. H.264 코덱은 네트워크 전송을 목적으로 개발되었으며, 효율적인 동영상 재생을 위해 NAL(Network Abstraction Layer)로 구성된다. NAL은 NAL unit이라고 하는 일종의 Header 값과 Payload로 구성되고, NAL Unit은 다시 forbidden_zero_bit(1bit), nal_ref_idc(2bit), nal_unit_type(5bit)로 구성된다. NAL Unit 앞에는 〔그림 2〕와 같이 4byte 혹은 3byte의 시작 패턴이 존재한다〔11〕.

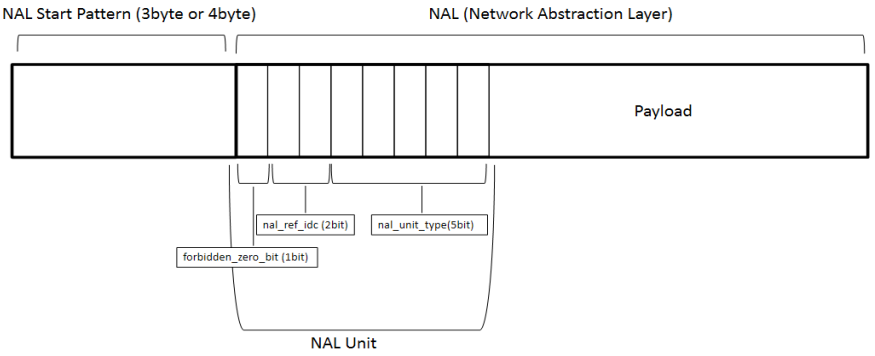


그림 2. NAL(Network Abstraction Layer) 구조
Fig. 2. NAL(Network Abstraction Layer) Structure

H.264 데이터의 시작점에는 프레임들의 디코딩에 필요한 정보를 가지고 있는 SPS(Sequence Parameter Set RBSP syntax)와 PPS(Pic Parameter Set RBPS syntax)가 위치하고, SPS와 PPS 이후에는 IDR 프레임 및 non-IDR 프레임이 위치한다[11][12]. SPS, PPS 값은 MP4 파일에서 디코딩 정보를 가지고 있는 stbl 컨테이너의 avcC 아톰에 저장되어 있으며, SPS는 해상도, 비디오 포맷 등 파일 전체에 대한 정보를 가지고 있고, PPS는 부호화 정보 등 상세한 정보를 가지고 있다. SPS, PPS, IDR 프레임, non-IDR 프레임은 각각의 NAL 구조를 가지고 있으며, [표 2]와 같이 서로 다른 nal_unit_type 을 가지게 된다[13].

Table 2. SPS, PPS, IDR, non-IDR NAL Unit Type
표 2. SPS, PPS, IDR, non-IDR NAL Unit Type

NAL Unit Type(5bit)	NAL Unit의 내용 및 구조
1 (00001)	non-IDR 프레임
5 (00101)	IDR 프레임
7 (00111)	SPS (Sequence Parameter Set RBSP syntax)
8 (01000)	PPS (Pic Parameter Set RBPS syntax)

H.264 코덱은 2016년도에 79%, 2017년에는 81%, 2018년에는 82%로 사용률이 증가하고 있고, 온라인 비디오 코덱들(H.264, HEVC, VP9, FLV, WebM) 사이에서 압도적으로 사용률이 높다[14].

4.2. exo 파일 구조 및 저장 경로

ExoPlayer를 사용하는 스마트폰 앱들을 통해 스트리밍 동영상을 재생할 경우, H.264 코덱을 사용하는 MP4 파일 포맷 형태의 exo 파일이 1개 혹은 여러 개의 파일로 분할되어 저장되며, exo 파일은 기본적으로 [그림 3]과 같이 3가지 컨테이너(ftyp, moov, mdat)를 가진 형태로 저장된다. ftyp, moov, mdat 3가지 컨테이너는 첫 번째 exo 파일 내부에 필수적으로 존재한다. 미디어 데이터를 저장하고 있는 mdat 컨테이너는 각각의 분할된 exo 파일들에 모두 존재할 수도 있다.

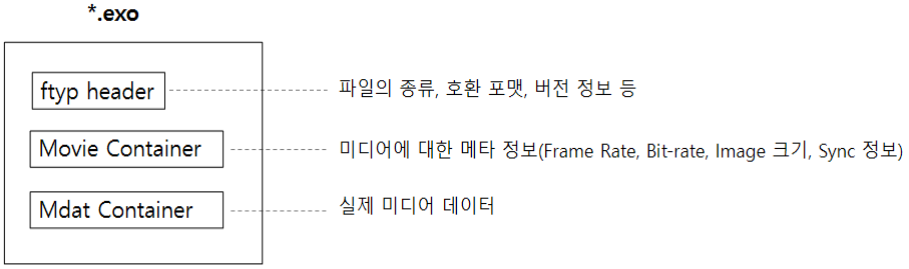


그림 3. exo 파일 기본 형태
Fig. 3. exo file basic form

exo 파일은 분할되지 않고 1개의 파일로 저장될 수도 있으나, 스트리밍 동영상이 클 경우, 다수의 파일로 분할되어 저장된다. 스트리밍 동영상이 처음부터 끝까지 재생될 경우 [그림 4]와 같이 mvhd 아톰 내 전체 재생 시간(M초) 정도의 동영상 재생이 가능한 분할된 exo 파일들이 생성된다.

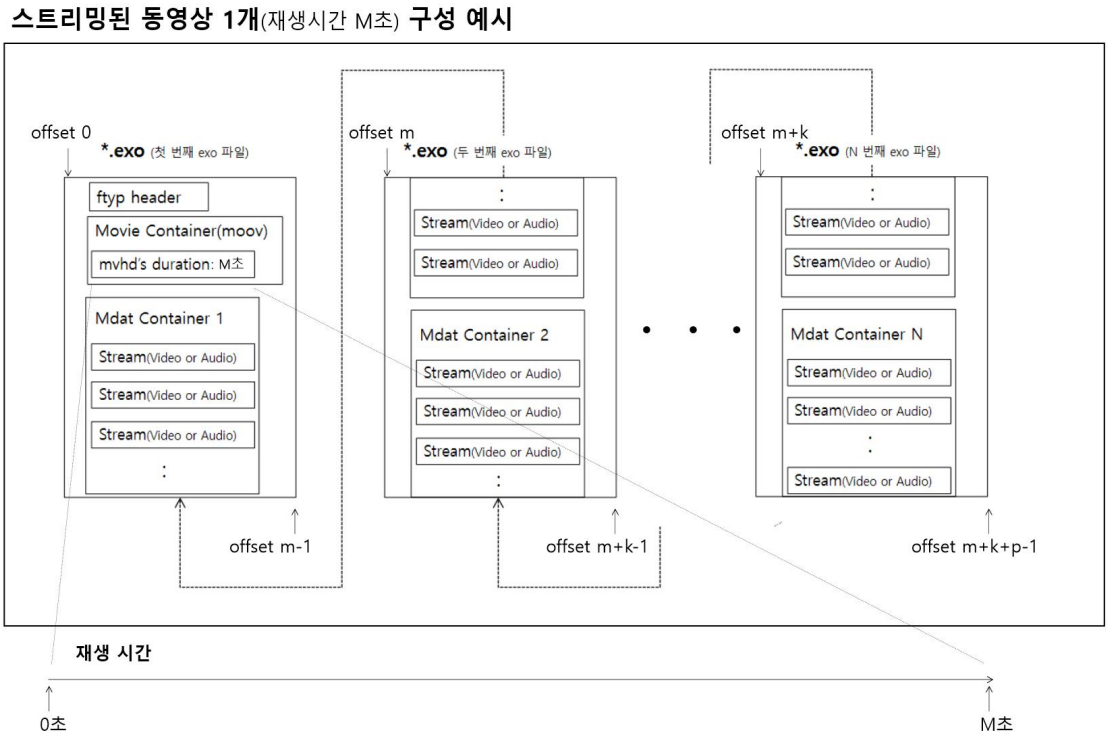


그림 4. 분할된 exo 파일들의 구성(스트리밍된 동영상의 크기가 t byte(t=m+k+p)인 경우)
Fig. 4. Composition of split exo files(If the size of the streamed video is t byte(t=m+k+p))

만약, 스트리밍 동영상이 재생 중 중단된 경우에는 재생을 멈춘 시점까지의 exo 파일들이 생성되는데 이는 Graeme Horsman이 연구한[3] PC 내 페이스북을 통해 스트리밍 동영상을 이용한 경우 생성되는 분할된 캐시 파일들의 구조적 특징에서도 발견되는 부분이다.

exo 파일들 내부에는 공통적으로 비디오 혹은 오디오 형태의 미디어 데이터가 존재하지만, 첫 번째 exo 파일만 [그림 3]과 같은 mp4 파일 형태의 구조를 가진다. 이와 같은 exo 파일 구조로 인해, 모바일 디지털 포렌식 분석 도구에서는 exo 파일의 대다수를 mp4 파일 형태의 동영상 파일 타입으로 분류하지 않고 있다. 대표적으로 사용되는 모바일 디지털 포렌식 분석 도구들이 exo 파일에 대해 획득, 분석 및 동영상 파일 타입으로 분류하고 있는지 여부를 확인하기 위해 스마트폰(SM-G930L)의 이미징 데이터를 획득 후, 분석 도구 별로 확인한 결과는 [표 3]과 같다.

Table 3. Whether to acquire and analyze exo files in mobile digital forensics tools and whether it is classified as a movie file type
표 3. 모바일 디지털 포렌식 도구에서 exo 파일 획득, 분석 및 동영상 파일 타입으로의 분류 여부

제작사	분석 도구	exo 파일 획득	exo 파일 분석	exo 파일 동영상 파일 타입 분류
경찰청	KDF-Mobile v3.0.20191028.42085D8	가능	가능	일부 분류 (첫 번째 exo 파일)
FINALDATA	FINALMobile Forensics 2019. 03. 06.	가능	가능	분류하지 않음

컴퓨터 디지털 포렌식 분석 도구들에서도 exo 파일에 대해 획득, 분석 및 동영상 파일 타입으로 분류하고 있는지 여부를 확인하기 위해 분석 도구 별로 컴퓨터 내 exo 파일들이 저장된 미디어를 읽어 들이는 방식으로 확인한 결과는 [표 4]와 같다.

Table 4. Whether to acquire and analyze exo files in computer digital forensics tools and whether it is classified as a movie file type
표 4. 컴퓨터 디지털 포렌식 도구에서 exo 파일 획득, 분석 및 동영상 파일 타입으로의 분류 여부

제작사	분석 도구	exo 파일 획득	exo 파일 분석	exo 파일 동영상 파일 타입 분류
Guidance Software	Encase v8.08.00.140	가능	가능	분류하지 않음
X-Ways Software Technology AG	X-Ways Forensics 19.8	가능	가능	분류하지 않음

〔표 3〕과 〔표 4〕와 같이 확인된 내용을 볼 때, 디지털 포렌식 분석 도구에 의해 정상적으로 획득된 exo 파일이라 할지라도 분석관이 exo 파일의 특성을 모를 경우, 디지털 포렌식 분석 도구에서 동영상 파일 타입으로 분류되지 않은 exo 파일들에 대한 분석이 이루어지지 않을 수 있다.

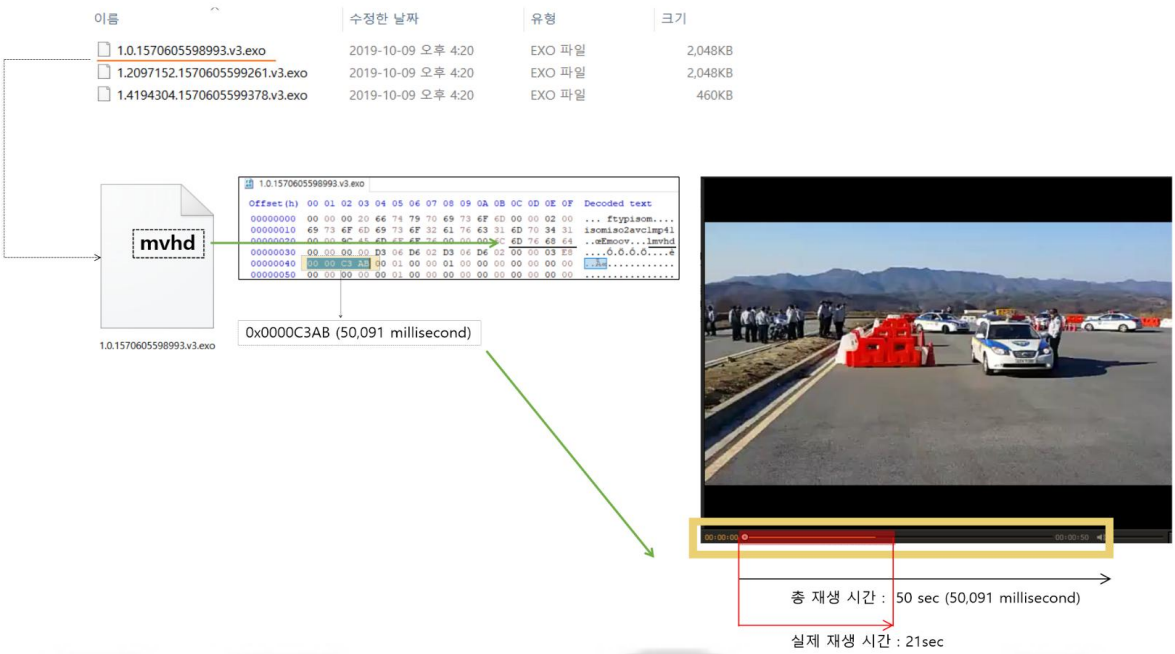


그림 5. 첫 번째 exo 파일을 재생할 경우, mvhd 아톰 내 재생시간 및 실제 재생했을 경우 확인되는 재생시간
Fig. 5. Play time in mvhd atom when the first exo file is played and play time when it is actually played

네이버 밴드(버전 7.5.2.0)를 이용하여 스트리밍 동영상을 재생하고, 〔그림 5〕와 같이 재생 후 생성된 3개의 exo 파일들 중 첫 번째 exo 파일(1.0.1570605598993.v3.exo)을 재생한 결과, 실제 약 50초의 재생시간을 가지는 동영상 파일이 21초간 재생되는 것을 알 수 있다. 결국, 첫 번째 exo 파일만 동영상 파일로 분류되어 분석될 경우, 나머지 약 29초에 대한 동영상을 확인할 수 없다.

안드로이드 스마트폰에서 동작하는 각 앱들은 실행 중 생성되는 캐시 파일을 '/data/패키지이름/cache/' 경로 하위에 저장한다. 〔표 1〕의 앱에서 사용하는 exo 파일의 경우도 '/data/패키지이름/' 하위 경로에 생성되는데, 앱의 특성에 따라 일부 경로는 〔표 5〕와 같이 변경되어 저장된다.

Table 5. Path to saving exo files by app
표 5. 앱 별 exo 파일 저장 경로

앱 이름	exo 파일 저장 경로
밴드	/data/com.nhn.android.band/cache/EXO/
인스타그램	/data/com.instagram.android/cache/ExoPlayerCacheDir/videocache/
페이스북	/data/com.facebook.katana/files or cache/ExoPlayerCacheDir/videocache/
페이스북 메신저	/data/com.facebook.orca/files/ExoPlayerCacheDir/videocache/
텀블러	/data/com.tumblr/app_video_cache/

4.3. exo 파일 이름 생성 규칙

ExoPlayer를 사용하는 앱들은 각 앱이 지정한 경로에 exo 파일들을 저장하고, 새로운 스트리밍 동영상들이 재생될 때마다 같은 경로에 exo 파일들을 저장한다. 스트리밍된 동영상들에 의해 생성된 exo 파일들이 모두 한 경로에 저장되어 있기 때문에 스마트폰에서 재생된 스트리밍 동영상들을 복원하기 위해서는 각 스트리밍 동영상 재생을 통해 생성되는 exo 파일들을 구분할 수 있어야 한다. ExoPlayer를 사용하는 앱들은 exo 파일을 생성할 때, 각 앱이 정한 규칙에 따라 exo 파일의 이름을 만드는데, exo 파일 이름을 통해 스트리밍 동영상 별 생성되는 exo 파일들을 구분할 수 있다.

밴드, 텀블러는 동일한 규칙으로 〔그림 6〕과 같은 형태의 exo 파일 이름을 만들다. 〔그림 6〕의 exo 파일들의 이름을 분석해보면, 점(.)을 구분자로 하여 5개의 값으로 구분되는 것을 알 수 있다. 첫 번째 자리에는 스트리밍 동영상이 재생되는 순서가 10진수 숫자 형태로 입력되게 되는데, 첫 번째 자리의 10진수 숫자를 통해 스트리밍 동영상들을 서로 구분할 수 있다. 두 번째 자리에는 재생된 스트리밍 동영상의 offset 값이 10진수 형태로 입력된다. 0.0.1570093298239.v3.exo 파일의 마지막 offset 값(0x200000)이 0.2097152.1570093298971.v3.exo 파일 이름의 두 번째 자리 값인 2097152 값(0x200000)과 동일하다는 특징을 통해 그 사실을 알 수 있다. 세 번째 자리의 13자리 숫자는 유닉스 시간으로 표현된 파일 생성 시각 값이다. 결국, 밴드, 텀블러에 의해 생성된 exo 파일들의 이름은 〔스트리밍 동영상 생성 순서(10진수)〕.〔스트리밍 동영상 offset(10진수)〕.〔13자리 시각 값(유닉스 시간)〕.v3.exo 형태로 만들어진다.

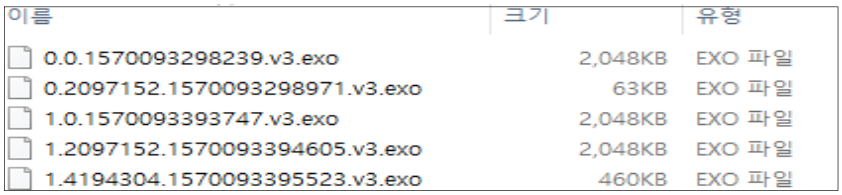


그림 6. 밴드 앱에 의해 생성된 exo 파일들
Fig. 6. Exo files generated by band app

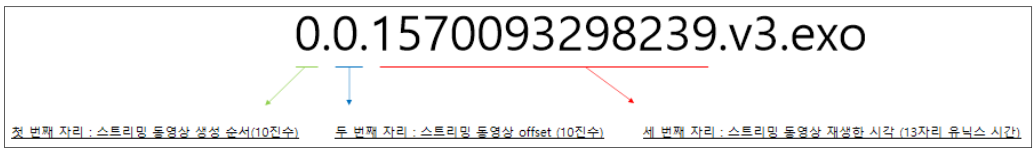


그림 7. 밴드 앱에 의해 생성된 exo 파일 이름 포맷 분석
Fig. 7. Analyzing exo file name format generated by band app

위와 같은 exo 파일들 이름 생성 규칙에 대한 분석을 통해 2가지 사실을 알 수 있다. 첫 번째, 각 앱에 의해 실행된 스트리밍 동영상의 개수를 알 수 있다. 두 번째, 앱을 이용해 각 스트리밍 동영상을 시청한 시각과 스트리밍 동영상들을 시청한 기간을 알 수 있다. 이 2가지 사실을 〔그림 6〕의 exo 파일들에 대입하여 분석해보면, 〔그림 6〕의 exo 파일들은 2019. 10. 3. 18:01:38 (KST)부터 2019. 10. 3. 18:03:15(KST) 사이에 2개의 스트리밍 동영상을 시청했음을 알 수 있다. 5개의 exo 파일들 이름의 첫 번째 자리에 0과 1만 갖고 있다는 사실을 통해 2개의 스트리밍 동영상임을 알 수 있고, 0.0.1570093298239.v3.exo 파일과 1.4194304.1570093395523.v3.exo 파일의 세 번째 자리 값('스트리밍 동영상 재생 시각)의 시각 변환을 통해 시청 기간 및 시청 시각이 추정 가능하다.

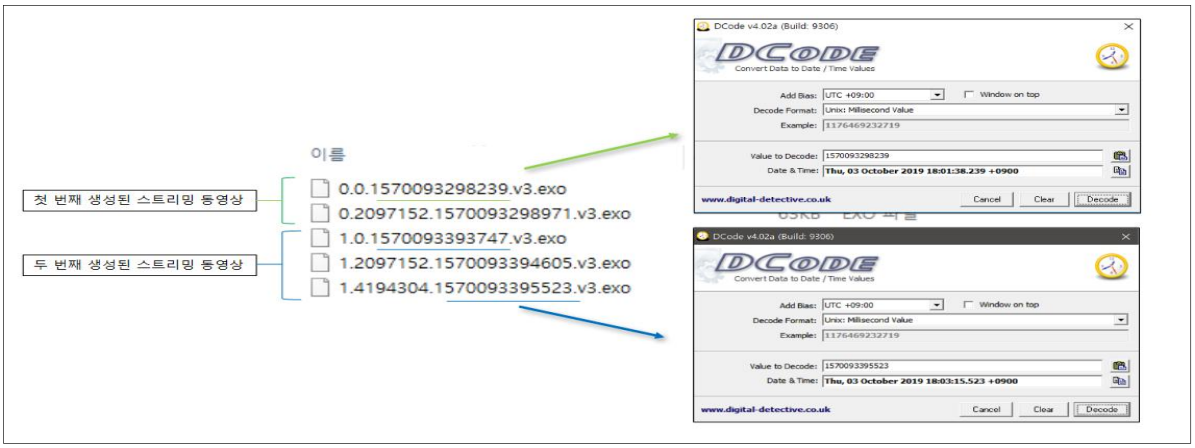
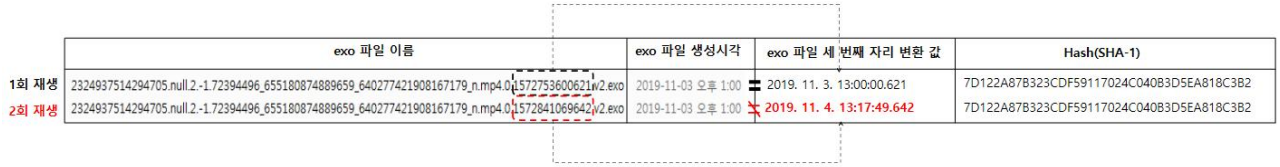


그림 8. exo 파일들에서 영상 개수와 영상 시청 시간 추정 값 확인
Fig. 8. Confirmation of video count and video viewing time estimate in exo files

스트리밍 동영상이 1회 재생됐을 때, exo 파일 이름의 세 번째 자리 값은 exo 파일의 생성 시각과 동일할 수 있다. 그러나 스트리밍 동영상을 1회 이상 재생할 경우, 파일 이름의 세 번째 자리 값과 exo 파일의 생성 시각은 달라질 수 있다. ExoPlayer는 과거 재생했던 스트리밍 동영상을 다시 재생할 때, 과거에 생성했던 exo 파일들을 재사용하는데 exo 파일을 재사용할 경우 파일 이름 중 세 번째 자리 값이 최근 재생했던 시각으로 변경된다. 이로 인해 스트리밍 동영상이 1회 이상 재생될 경우에 exo 파일의 생성 시각과 exo 파일 이름의 세 번째 자리 값이 달라지게 된다. 결국, exo 파일의 생성 시각을 해당 스트리밍 동영상을 처음 재생한 시각으로 생각할 수 있으며, exo 파일 이름의 세 번째 자리 값은 스트리밍 동영상의 마지막 재생 시각으로 볼 수 있다. 〔그림 9〕은

페이스북 메신저에서 동일한 스트리밍 동영상을 1회 재생(2019. 11. 3. 13:00)했을 때의 exo 파일과 2회 재생(2019. 11. 4. 13:17)했을 때의 exo 파일을 비교한 것이다. 2개의 exo 파일은 해시 값, 파일 생성 시각은 같지만 파일 이름(세 번째 자리 값)이 다름을 알 수 있다.



	exo 파일 이름	exo 파일 생성시각	exo 파일 세 번째 자리 변환 값	Hash(SHA-1)
1회 재생	2324937514294705.null.2.-1.72394496_655180874889659_6402774219081671 79_n.mp4.0.1572753600621.v2.exo	2019-11-03 오후 1:00	= 2019. 11. 3. 13:00:00.621	7D122A87B323CDF59117024C040B3D5EA818C3B2
2회 재생	2324937514294705.null.2.-1.72394496_655180874889659_6402774219081671 79_n.mp4.0.1572841069642.v2.exo	2019-11-03 오후 1:00	≠ 2019. 11. 4. 13:17:49.642	7D122A87B323CDF59117024C040B3D5EA818C3B2

그림 9. 과거 재생한 스트리밍 동영상을 다시 재생할 경우, exo 파일 이름의 세 번째 자리 값(스트리밍 동영상 재생 시각)의 갱신
Fig. 9. If you play a previously played streaming movie again, update the third digit value of the exo file name(time to play streaming video)

페이스북 메신저에서 생성한 exo 파일의 이름은 〔그림 7〕에서 확인한 파일 이름 포맷의 첫 번째 자리에 페이스북만이 가지는 규칙으로 이름을 덧붙여서 〔그림 10〕과 같은 exo 파일을 만들고 있다. 〔그림 6〕과 달리 파일 이름 포맷의 첫 번째 자리가 10진수 형태의 동영상 생성 순서는 아니나 각 스트리밍 동영상마다 서로 다른 값을 가지고 있기 때문에 페이스북에서 생성한 exo 파일들의 이름만으로도 스트리밍 동영상 개수를 알 수 있다.

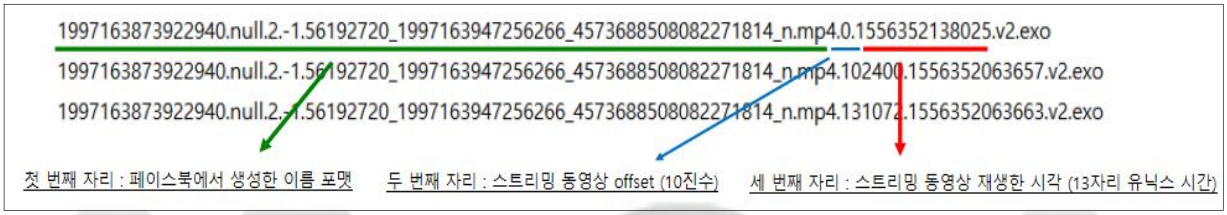


그림 10. 페이스북 및 페이스북 메신저에 의해 생성된 exo 파일 이름 포맷 분석
Fig. 10. Analyze the format of the exo file name generated by Facebook and Facebook Messenger

2019년 8월 동영상 앱 사용 순위 1위인 유튜브(com.google.android.youtube)와 3위인 네이버 TV(com.nhn.android.naverplayer), 6위인 넷플릭스(com.netflix.mediaclient)〔15〕에서 생성된 exo 파일의 이름과 플레이스토어(com.android.vending)에서 생성된 exo 파일의 이름, 쇼핑몰 관련 앱(com.buzzvil.buzzscreen.wemakeprice)에서 생성하는 exo 파일의 이름을 〔표 6〕과 같이 확인한 결과, 앞서 살펴본 앱들과 동일한 형태로 exo 파일의 이름을 생성하고 있다.

Table 6. Exo file storage path and generated exo file name for YouTube, Naver Player, Netflix, Play store, Wemakeprice app
표 6. 유튜브, 네이버 플레이어, 넷플릭스, 플레이스토어, 위메프체크 앱의 exo 파일 저장경로 및 생성된 exo 파일 이름

앱 이름 (버전)	exo 파일 저장 경로	exo 파일 이름
유튜브 (14.43.55)	/data/com.google.android.youtube/cache/exo/	0.2888041.1572886805082.v3.exo
네이버 플레이어 (v4.1.1)	/data/com.nhn.android.naverplayer/cache/prismplayer_cache/	0.0.1572887209689.v3.exo 13.0.1572887211132.v3.exo
넷플릭스 (7.32.0 build 19 34546)	/data/com.netflix.mediaclient/cache/fragment or header/	1.0.1572924167152.v3.exo
구글 플레이스토어 (17.2.13-all 〔0〕〔PR〕 276332444)	/data/com.android.vending/cache/explayer_cache/	0.0.1571798710055.v3.exo 0.48.1571798710059.v3.exo
위메프체크 (1.0.16)	/media/0/Android/data/com.buzzvil.buzzscreen.wemakeprice/cache/bs-videos	0.0.1555621812035.v3.exo

Ⅴ. exo 파일 재조합 프로그램 설계 및 구현

exo 파일을 재조합하기 위해서는 4단계가 필요하다. 첫 번째, exo 파일들을 〔그림 4〕와 같이 1개의 파일로 병합한다. 프레임이 exo 파일 사이에 걸쳐서 저장되어 있을 경우, 병합하여 비디오 데이터를 추출해야 정확한 프레임을 추출할 수 있다. 두 번째, 병합된 exo 파일 내 IDR 프레임과 non-IDR 프레임을 추출하고, NAL Unit의 시작 패턴 기본 값인 0x00000001을 추출된

프레임들의 nal_unit_type 값 앞에 추가한다. H.264 코덱으로 압축된 데이터에서 IDR 프레임과 non-IDR 프레임을 추출하기 위해 사용한 주요 값(Signature)은 〔표 7〕과 같다.

Table 7. Frame extraction main part(Signature)
표 7. 프레임 추출 주요 부분(Signature)

구분	프레임 사이즈 (4byte)	forbidden_zero_bit (1bit)	nal_ref_idc (2bit)	nal_unit_type (5bit)	slice_type
non-IDR 프레임	00 00 xx xx	0	00	00001	1, 3, 5, 6, 8
	00 00 xx xx	0	01	00001	1, 3, 5, 6, 8
	00 00 xx xx	0	10	00001	1, 3, 5, 6, 8
	00 00 xx xx	0	11	00001	1, 3, 5, 6, 8
IDR 프레임	00 00 xx xx	0	01	00101	2, 4, 7, 9
	00 00 xx xx	0	10	00101	2, 4, 7, 9
	00 00 xx xx	0	11	00101	2, 4, 7, 9

세 번째, 추출된 프레임들을 동영상 형태로 재생성 하기 위해서는 해상도, 비디오 포맷, 부호화 정보 등을 가지고 있는 SPS NAL Unit과, PPS NAL Unit이 있어야 한다. 이를 위해, 병합된 exo 파일의 avcC 아톰 내 존재하는 SPS NAL Unit의 값과 PPS NAL Unit 값을 각각 추출한 뒤, NAL Unit의 시작 패턴 기본 값인 0x00000001을 앞에 추가하여 기본 SPS, PPS NAL Unit 값을 만든다.

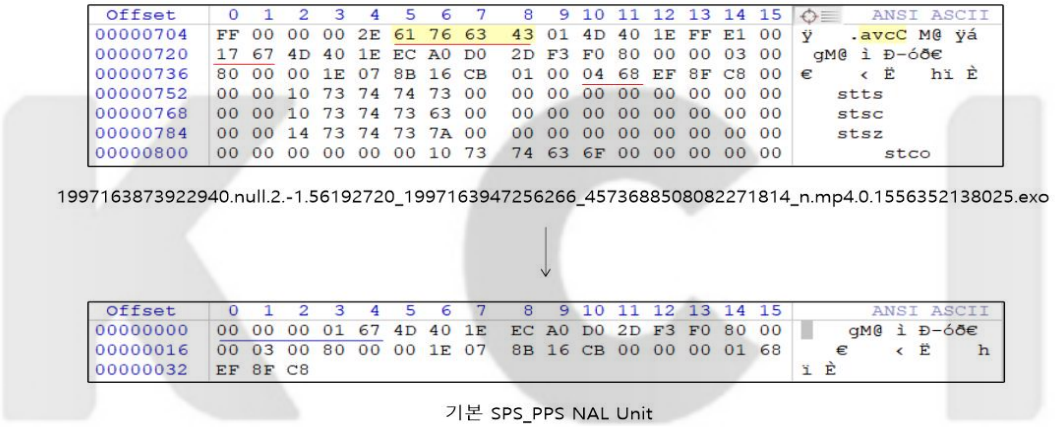


그림 11. 페이스북 메신저에 의해 생성된 첫 번째 exo 파일에서 기본 SPS, PPS NAL Unit 추출
Fig. 11. Extract basic SPS, PPS NAL Unit from the first exo file created by Facebook Messenger

네 번째, 기본 SPS, NAL Unit 값과 추출된 프레임들을 병합한 뒤, FFmpeg 프로그램으로 병합된 프레임들을 인코딩하여 avi 동영상 파일을 생성한다.

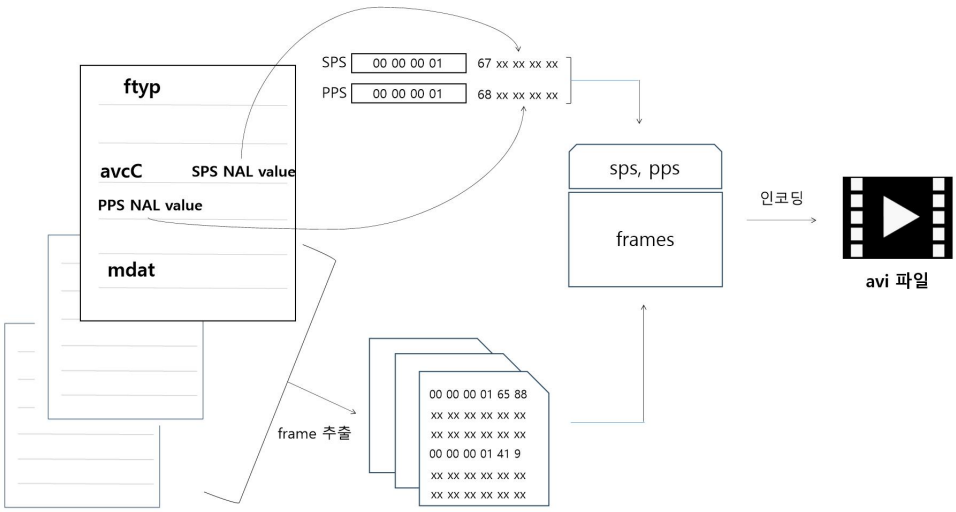


그림 12. exo 파일 재조합 원리
Fig. 12. Principle of exo file reombination

본 연구에서는 〔그림 12〕와 같이 도식화된 재조합 과정을 바탕으로, python(3.7.4 버전), FFmpeg(N-81707-g11777eb 버전)〔16〕을 사용하여 exo 파일 재조합을 위한 프로그램을 개발하였으며, 프로그램의 주요 흐름도는 〔그림 13〕과 같다.

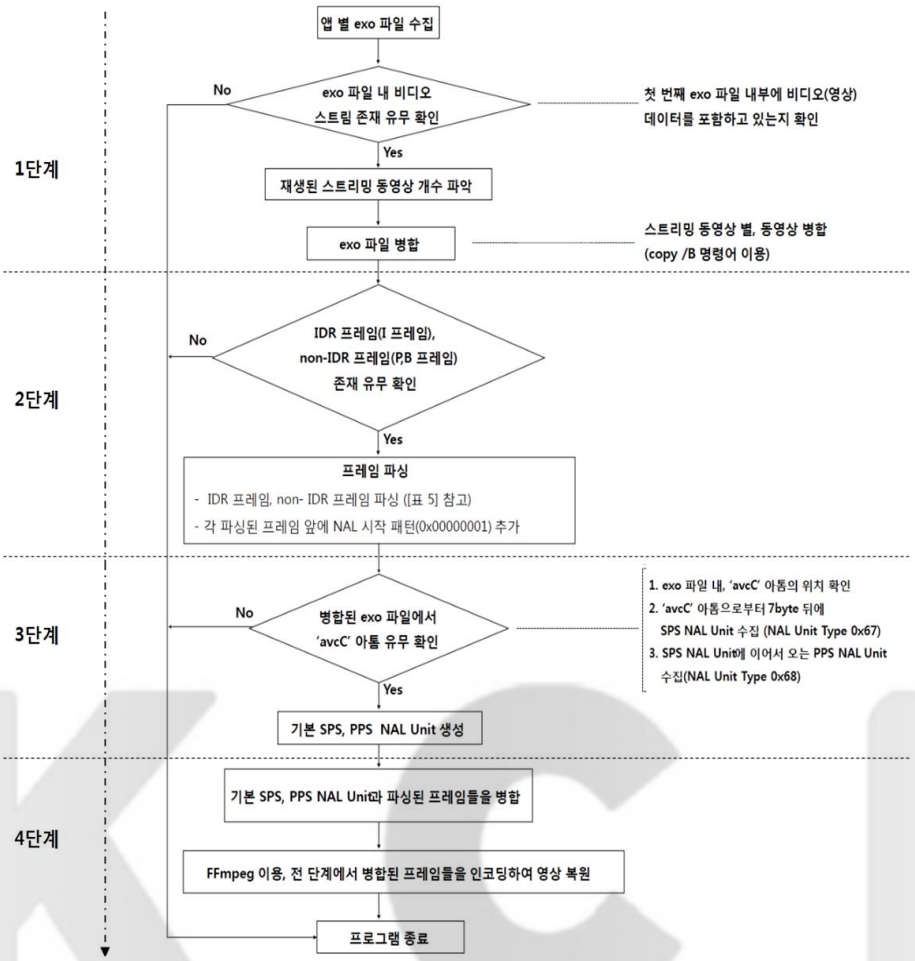


그림 13. exo 파일 재조합 프로그램의 순서도
Fig. 13. Flowchart of exo file recombination program

Ⅵ. exo 파일 재조합을 통한 포렌식 분석 적용 사례

6.1. 불법 촬영 동영상 유포 협박 사례

불법 촬영 범죄는 2011년 1,523건에서 2017년 6,470건으로 증가하고 있다〔17〕. 또한, 불법 촬영된 동영상을 인터넷상에 유포하겠다고 피해자를 협박하는 2차 피해도 증가하고 있다. 불법 촬영된 동영상으로 피해자를 협박하는 사건의 경우, 피의자가 불법 촬영된 동영상을 소지하고 있는지 여부가 혐의를 입증하는데 중요한 단서로 사용될 수 있다. 피의자가 불법 촬영 동영상을 가지고 있지 않다고 부인하고 있는 가운데 exo 파일 재조합을 통한 영상 복원으로 피의자의 범죄 혐의를 입증할 수 있었던 사건이 있었다. 이 사건에서 exo 파일 재조합을 통한 영상 데이터 복원의 실효성을 확인할 수 있었다.

2019. 3.경 피의자가 피해자와의 성관계 장면을 불법 촬영하고, 불법 촬영된 동영상의 유포를 빌미로 협박을 한 사건이 발생하였다. 전형적인 불법 촬영 범죄에 의한 2차 가해 유형 범죄로, 피의자는 범행 일체를 부인하고 있었던 사건이다. 피의자의 스마트폰(SM-OOOOO, 안드로이드 8.0)이 분석 의뢰되어 불법 촬영된 성관계 동영상이 스마트폰 내에 존재하는지 여부, 불법 촬영 동영상이 문자메시지 및 SNS 메신저 등을 통해 송·수신된 이력이 존재하는지 여부 확인 등을 확인하여 피의자의 범죄 혐의를 입증하는 단서를 찾는데 주안점을 두고 분석 진행하였다.

범죄 일시 경에 생성된 동영상 파일 중 범죄 혐의와 관련된 동영상이 확인되지 않는 상황에서 /data/com.facebook.orca/files/ExoPlayerCacheDir/videocache 경로에 범죄 일시 경에 생성된 38개의 exo 파일들이 존재함을 확인하였다. 페이스북 메신저를 통해 범죄 일시 경에 주고받은 스트리밍 동영상이 존재할 것으로 판단되었고, 분할된 exo 파일 중 offset 0 값을 갖는 1997163873922940.null.2.-1.56192720_1997163947256266_4573688508082271814_n.mp4.0.1556352138025.exo 파일을 실행한 결과 〔그림 14〕처럼 2초간 방 안이 비치는 영상이 재생되었다.

그림 14. 사례1 - 약 2초간 재생되는 exo 파일
Fig. 14. Case1 - exo file playing for about 2 seconds

이에, /data/com.facebook.orca/files/ExoPlayerCacheDir/videocache 하위에 존재하는 exo 파일들을 〔그림 15〕와 같이 수집하고, exo 파일 재조합 프로그램을 실행하여 동영상을 복원한 결과, 〔그림 16〕과 같이 성관계 장면이 촬영된 동영상(1분 14초 재생)을 획득할 수 있었다.

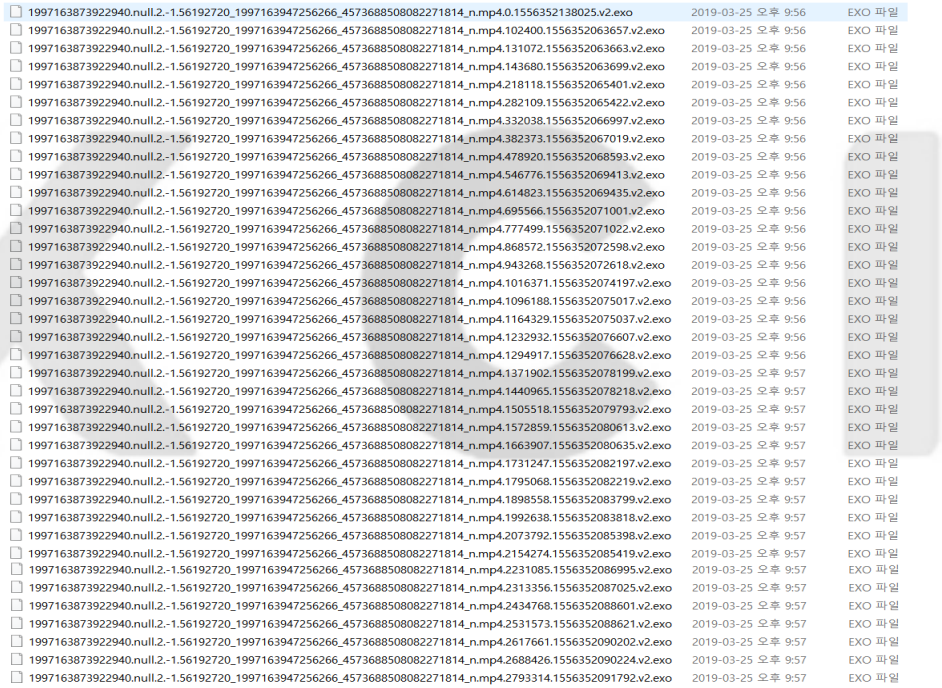


그림 15. 사례1 - com.facebook.orca/files/ExoPlayerCacheDir/videocache에 저장된 38개의 exo 파일들
Fig. 15. Case1 - 38 exo files stored on com.facebook.orca/files/ExoPlayerCacheDir/videocache

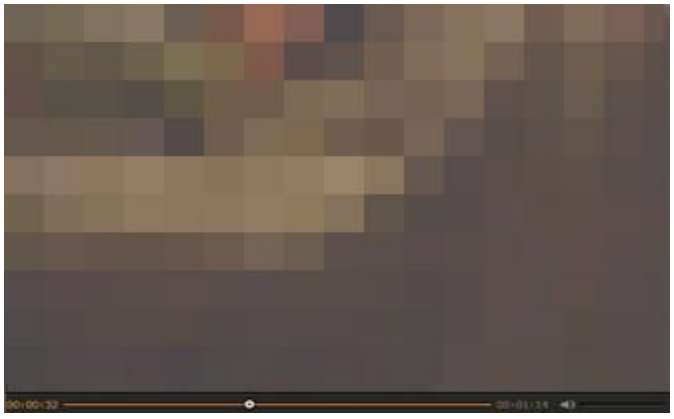


그림 16. 사례1 - exo 파일 재조합 프로그램을 통해 복구한 성관계 영상
Fig. 16. Case1 - Video restored through exo file recombination program

획득된 성관계 동영상에는 피의자의 얼굴이 식별 가능하였고, 피해자의 성관계 거부 의사 및 불법 촬영을 원치 않는 의사가 확인되는 영상이 확인되어 피의자의 범죄 혐의를 입증할 수 있는 단서로서 사용 가능하였다. 수집된 exo 파일들을 추가 분석한 결과, exo 파일의 생성 시각(2019. 3. OO.)과 exo 파일 이름의 세 번째 자리 값(스트리밍 재생 시각. 2019. 4. OO.)의 비교를 통해 피의자가 2019. 3. OO.과 2019. 4. OO.에 최소 2차례에 걸쳐 페이스북 메신저 내에 존재하는 성관계 동영상을 재생했다는 사실을 확인할 수 있었다. 이는, 피의자가 페이스북 메신저 내에 저장되어 있는 성관계 동영상을 약 1개월 이상 소지하고 있었다는 사실을 알 수 있게 해주었다.

이 사례는 ExoPlayer를 사용하는 앱에 의해 재생되는 불법 스트리밍 동영상에 대한 분석이 필요함을 인식시켜줌과 동시에 exo 파일 이름에 대한 분석과 exo 파일 재조합 프로그램이 디지털증거분석에 유용하게 사용될 수 있음을 보여준다.

6.2. 음란 동영상 실시간 방송을 통한 유포 사례

페이스북, 인스타그램, 유튜브, 카카오톡 등 국내외 주요 앱들은 사용자들에게 실시간으로 방송을 할 수 있도록 라이브 스트리밍 서비스를 제공한다. 스마트폰 하나만으로 자신이 원하는 영상을 다수가 볼 수 있도록 방송할 수 있기 때문에 많은 사람들이 이러한 라이브 스트리밍 서비스 기능을 이용하고 있다. 라이브 스트리밍 서비스 기능은 지식 공유, 취미 공유 등 긍정적인 영향이 많이 있으나, 특별한 규제없이 누구나 스마트폰을 이용해 방송을 할 수 있기에 라이브 스트리밍 서비스로 인한 사회적 문제가 발생하고 있다. 대표적인 사례로 2019년 뉴질랜드에 있는 이슬람 사원에서 발생한 총격사건에서 페이스북 앱으로 약 17분간 총격 장면이 방송된 적이 있다[18].

국내에서 페이스북 라이브 스트리밍 서비스를 이용해 성관계 장면이 방송된 사건이 신고되었다. 페이스북을 이용하던 사용자가 성관계 장면이 실시간 재생되는 것을 확인하여 경찰에 신고하였고, 이로 인해 수사가 개시된 사례이다. 담당 수사관은 남·녀 피의자들을 검거하면서 페이스북 실행 이력이 확인되는 남자 피의자의 스마트폰(SM-OOOOO, Android 8.0)을 압수하였고, 해당 스마트폰을 증거분석 의뢰하였다. 피의자들은 성관계를 한 것은 사실이나 촬영한 사실이 없다고 부인하고 있었다.

스마트폰 내 페이스북이 삭제된 흔적이 없는 가운데 스마트폰 카메라를 통해 동영상을 촬영한 이력, 페이스북에 성관계 동영상이 업로드된 이력이 확인되지 않았고, 증거분석 프로그램에서 동영상으로 분류한 동영상 파일들에서도 성관계를 하는 동영상이 확인되지 않았다. 남자 피의자가 페이스북을 이용한다는 사실이 확인되고, 라이브 스트리밍 서비스에 의해 재생되는 동영상도 exo 파일 형태로 동영상들을 저장할 것으로 판단되어 페이스북 내 /data/com.facebook.katana/files/ExoPlayerCacheDir/videocache 경로 확인한 결과, 범죄 일시에 [그림 17]과 같이 다수의 exo 파일이 생성되어 있음을 확인하였다. 이에, exo 파일 재조합 프로그램을 통해 동영상 복원을 진행한 결과, 피의자들이 성관계하는 동영상을 복원할 수 있었다.

/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.0.1572930087662.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.1002319.1572930093893.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.117275.1572930087718.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.157706.1572930088469.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.199624.1572930088973.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.245226.1572930089351.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.287139.1572930089732.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.314810.1572930090114.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.339985.1572930090496.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.359157.1572930090870.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.382407.1572930091244.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.410529.1572930091633.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.504724.1572930092007.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.646821.1572930092379.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.749894.1572930092774.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.791048.1572930093143.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.80411.1572930087709.v2.exo
/data/com.facebook.katana/cache/ExoPlayerCacheDir/videocache/3040186929342084.null.4328920240866696vd.-1.76773844_268254634071370_7748162305941759581_n.mp4.887364.1572930093513.v2.exo

그림 17. 사례2 - 범죄 일시에 페이스북에 의해 생성된 exo 파일 목록
Fig. 17. Case2 - List of exo files created by Facebook at the time of the crime

이 사례에서 복원된 동영상이 성관계 영상이었다고 하지만 피의자들이 성관계하는 동영상이 페이스북에 실시간 스트리밍 재생 되었다는 사실 여부까지는 확인할 수 없었다. 그렇지만 피의자들의 진술과 exo 파일의 생성 시각, 기타 수사된 사항과 더불어 결정적으로 exo 파일 재조합 프로그램에 의해 복원된 동영상의 영상 내용 등을 종합하여 피의자들의 범죄 혐의를 입증할 수 있었던 사례였다. exo 파일 재조합 프로그램에 의해 복원된 영상만으로 라이브 스트리밍 서비스를 이용한 범죄 피의자의 혐의를 입증하는데는 어려움이 있을 수 있다. 그러나 수사 과정에서 확보된 기타 단서, 증거와 더불어 exo 파일 재조합 프로그램에 의해 복원된 영상이 활용된다면 향후 라이브 스트리밍 서비스를 이용하는 범죄자들을 추적하고, 그들의 범죄 혐의를 입증하는데 도움이 될 것이다.

Ⅶ. 결론 및 향후 계획

본 논문에서는 안드로이드 OS 기반 스마트폰에서 ExoPlayer에 의해 생성되는 exo 파일들의 특징과 재조합 방법을 연구하였으며, exo 파일들을 자동으로 재조합하여 영상으로 복원하는 프로그램을 개발하여 포렌식 업무에 적용할 수 있도록 제안하였다. 업무 적용 가능 사례에서 살펴보았듯이 exo 파일 재조합 프로그램을 통한 동영상 복원은 나날이 증가하는 불법 촬영 관련 범죄와 그에 따른 2차 범죄를 예방하는데 기여할 수 있다.

스마트폰을 이용한 실시간 동영상 제작, 실시간 동영상 시청 등이 증가함에 따라 향후 증거분석 의뢰된 스마트폰에서 재생된 실시간 동영상이 무엇이었는지 여부를 판별하는 것이 범죄 혐의를 입증하는 단서 중의 하나로 사용될 수 있다. 이에, 스마트폰 내에서 재생되었던 실시간 동영상이 무엇이었는지 판별하고, 입증하는 연구는 향후 디지털포렌식 관점에서 필요한 연구이다.

ExoPlayer는 구글에서 제작한 오픈 소스로, 개발자에 따라 본 논문에서 살펴본 exo 파일과 다른 형태로(예. 파일 확장자의 변경, 난독화 등) 실시간 동영상 관련 파일을 저장하거나 exo 파일 내부를 암호화하여 저장할 수 있을 것이다. 따라서, 향후 본 논문에서 연구되지 못한 exo 파일 외 다른 형태로 저장된 실시간 동영상 관련 파일들을 추출하고, 분석하는 연구를 진행할 예정이다. 또한, 안드로이드 기반 스마트폰의 exo 파일과 같이 iOS 기반 스마트폰에서도 실시간 동영상이 분할된 형태의 캐시 파일로 저장되는 사례가 있는지 분석하여, 분할된 형태의 캐시 파일이기 때문에 디지털포렌식 분석 과정에서 놓칠 수 있는 범죄 혐의 관련 동영상을 복원하는데 사용될 수 있도록 하고자 한다.

참 고 문 헌 (References)

〔1〕 KBS News, "국민 95%가 스마트폰 사용…보급률 1위 국가는?", Available:http://mn.kbs.co.kr/news/view.do?ncd=4135732, 2019.2.11.

〔2〕 Kang Sheng, "Video Forensic of Fragmented Video Based on H.264/AVC Video Compression Standard", International Conference on Mechatronic, Industrial and Control Engineering (MEIC 2014), 2014

〔3〕 Graeme Horsman, "Reconstructing Streamed Video Content – A Case Study on Youtube and Facebook Live Stream Content in the Chrome Web Browser Cache", Digital Investigation, 2018

〔4〕 ExoPlayer: Adaptive video streaming on Android, Available:https://www.youtube.com/watch?v=6VjF638VObA, 2014.6.25.

〔5〕 National Police Agency Digital Evidence Analysis(2009~2018), Available:https://www.police.go.kr/portal/bbs/view.do?nttId=71723&bbsId=B0000136&searchCnd=&searchWrd=&section=&sdate=&edate=&useAt=&replyAt=&menuNo=200525&viewType=&delCode=0&option1=&option2=&option4=&option5=&deptId=&pageIndex=1

〔6〕 Ministry of Science and ICT, Korea Internet & Security Agency, "2018 인터넷이용실태조사", Available:https://www.kisa.or.kr/public/library/etc_View.jsp?regno=0011998&searchType=&searchKeyword=&pageIndex=1, 2019.

〔7〕 Wikipedia, MPEG-4 Part 14, Available:https://en.wikipedia.org/wiki/MPEG-4_Part_14

〔8〕 G. H. Park, "이론과 실무의 조화 코덱의 세계로의 초대", Hongreung, Seoul, pp. 356, 2006.

〔9〕 G. H. Park, "이론과 실무의 조화 코덱의 세계로의 초대", Hongreung, Seoul, pp. 362, 2006.

〔10〕 Supreme Prosecutor's Office, Korea University Industry-Academic Cooperation Foundation, "손상된 CCTV, 블랙박스의 복원대상기기 확대 및 통합뷰어 개발", pp. 47-52, 2015.

〔11〕 Supreme Prosecutor's Office, Korea University Industry-Academic Cooperation Foundation, "손상된 CCTV, 블랙박스의 복원대상기기 확대 및 통합뷰어 개발", pp. 53-57, 2015.

〔12〕 G. H. Park, "이론과 실무의 조화 코덱의 세계로의 초대", Hongreung, Seoul, pp. 316-412, 2006.

〔13〕 ITU-T, Advanced video coding for generic audiovisual services, pp. 65, 2019.

〔14〕 Shanhong Liu, Online video codecs and containers share worldwide 2016-2018, Available:https://cdn.statista.com/statistics/710673/worldwide-video-codecs-containers-share-online, 2019.

〔15〕 wiseapp, "〔와이즈앱 비교하기 #166〕 2019년 8월 동영상 앱 사용자 동향", Available:https://platum.kr/archives/128645, 2019.9.26.

〔16〕 FFmpeg, About FFmpeg, Available:https://www.ffmpeg.org/about.html

〔17〕 The Kyunghyang Shinmun, "불법촬영 7년 새 4배 급증에도 구속은 고작 2%대", Available:http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201903221608001, 2019.3.22.

〔18〕 Korea JoongAng Daily, "생중계로 게임하듯 탕 ·탕·탕…뉴질랜드 '테러 라이브' 경악", Available:https://news.joins.com/article/23412066, 2019.3.15.

저 자 소 개

한 용 현 (Yonghyun Han)
준회원
2010년 8월 : 한국기술교육대학교 인터넷미디어공학부 정보보호전공 졸업
2017년 1월~2019년 1월 : 수원서부경찰서 사이버범죄수사팀
2019년 1월~현재 : 경기남부지방경찰청 사이버안전과 디지털포렌식계
2019년 2월~현재 : 고려대학교 정보보호대학원 디지털포렌식학과 석사과정
관심분야 : 디지털포렌식, 악성코드, 정보보호 등

이 상 진 (Soonsin Lee)
종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
관심분야: 디지털포렌식, 심층암호, 해쉬함수