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

포맷프리 저장 방식 블랙박스의 효율적인 영상 복구 방안에 관한 연구

오 영 주*, 이 상 진**
경기남부지방경찰청 (디지털증거분석관)*, 고려대학교 정보보호대학원 (교수)**

A Study on Efficient Image Recovery For Format-free Technology in black box

Young-Joo Oh*, Sangjin Lee**
Gyeonggi Nambu Provincial Police Agency (Digital Forensic Investigator)*
Graduate School of Information Security, Korea University (Professor)**

요 약

차량용 블랙박스에서 사용하는 포맷프리 저장 방식은 충격 또는 갑작스런 전원 차단에도 녹화 영상이 손실되지 않게 하기 위해 개발된 저장 방식이다. 기존 차량용 블랙박스 분석은 미할당 영역과 슬랙 영역에서 삭제된 영상을 복구하였으나, 차량용 블랙박스의 포맷프리 저장 방식은 기존 분석 도구에서 지원하지 않아 미할당 영역과 슬랙 영역을 분리하여 삭제된 영상을 복구할 수 없다. 따라서, 전체 영역에서 영상을 복구해야 하므로 많은 시간이 소요된다. 본 논문에서는 포맷프리 저장 방식이 적용된 블랙박스를 선정하여 저장 구조를 분석하고 기존 영상 복구 방식의 한계점을 확인하였다. 이를 통해 미할당 영역과 슬랙 영역을 분리하는 영상 복구 방식을 제안하고, 이 방식에 적용된 포렌식 분석 도구를 설계 및 구현하였다.

주제어 : 디지털포렌식, 포맷프리 파일시스템, 임베디드 영상 촬영장치, 포렌식 분석도구

ABSTRACT

Format-free technology used in car black boxes is a new storage technique to protect recording images from being lost when physical shocked or sudden power-off. When analysing a black box, the ordinary analysis usually recovers lost images from unallocated space and slack space. However, existing analysis tools do not support the Format-free technology, it is impossible to extract unallocated space and slack space from the memory. As a result, it takes a lot of time to recover lost images with carving in whole memory. In this paper, we selected black boxes using Format-free technology, analyzed it's storage structure and confirmed the limitations of the existing image recovery method. Through this, we propose an efficient image recovery method that separates unallocated space and slack space. we also designed and implemented the forensic analysis tools supporting Format-free technology.

Key Words : Digital Forensics, Format Free File System, Embaded Movie capture, Forensic Tool

1. 서 론

차량용 영상 기록 장치(이하 블랙박스)는 차량 내부에 장착되는 임베디드 영상 기록 장치로 충격 또는 갑작스런 전원 차단시에 영상이 정상적으로 저장되지 않는 문제점이 있다. 블랙박스의 포맷프리(Format Free) 저장 방식은 이런 문제점을 극복하고자 적용된 영상 저장 방식이다.[1] 현재 출시된 블랙박스 중에는 포맷프리 저장 방식을 적용한 제품이 많이 있다. 2018년 1월부터 2019년 10월까지 경기남부지방경찰청에서 디지털포렌식 조사를 한 블랙박스를 확인한 결과, 265개 중 102개(38.4%)가 포맷프리 파일시스템을 사용하고 있었다.

초기의 포맷프리 저장 방식인 TAT(Time Allocated Table) 저장 방식과 NxFS 저장 방식은 제조사에서 제공하는 전용 프로그램으로만 영상 데이터에 접근할 수 있다. 이러한 단점을 보완하고자 제조사에서 제공하는 전용 프로그램 없이도 영상 파일을 탐색 및 저장할 수 있는 FAT32 파일시스템 기반 포맷프리 저장 방식(이하 FAT32 포맷프리 저장 방식)이 블랙박스에 적용되는 사례가 표 1과 같이 증가했다. 경기남부지방경찰청 관할 경찰서에서 디지털포렌식계로 분석 의뢰된 블랙박스

▪ Received 14 November 2019, Revised 24 November 2019, Accepted 17 December 2019
▪ 제1저자(First Author) : Young-Joo Oh (Email : osmartuo@naver.com)
▪ 교신저자(Corresponding Author) : Sangjin Lee (Email : sangjin@korea.ac.kr)

건수를 살펴보면 TAT 저장 방식은 2018년도에 11건(7.4%)에서 2019년도에 3건(2.5%)으로 계속하여 줄고 있다. 따라서, 본 논문에서는 NxFS 포맷프리 저장 방식과 FAT32 포맷 프리 저장 방식을 분석 대상으로 하였다.

표 1. 경기남부지방경찰청 디지털포렌식 조사한 블랙박스의 포맷프리 저장 방식 비율
Table 1. Percentage of format free storage of black boxes surveyed by the Gyeonggi nambu provincial police agency

기 간	非 포맷프리	포맷프리	합 계
2018.1. ~ 2018. 12.	92(61.7%)	57(38.3%)	149
2019.1. ~ 2019. 10.	71(61.2%)	45(38.8%)	116

기존 블랙박스에서 삭제된 영상을 복구하는 방법은 정상 저장된 영상 파일이 존재하는 할당 영역을 제외한 미할당 영역과 슬랙 영역에서 삭제된 영상 데이터를 복구하였으나, 블랙박스의 포맷프리 저장 방식은 기존 분석 도구에서 지원하지 않아 미할당 영역과 슬랙 영역을 분리해주지 않는다. 따라서 블랙박스 메모리의 전체 영역에서 삭제되지 않은 영역까지 탐색, 복구해야 하므로 많은 시간이 소요된다.

본 논문에서는 포맷프리 저장 방식이 적용된 파일시스템을 선정하여 저장 구조를 분석하고, 슬랙 영역을 분리하여 동영상 파일 포맷으로 복구하며, 동영상으로 재조립이 불가능한 프레임은 사진 파일 포맷으로 복구하는 방식을 제안한다.

2. 관련 연구

디지털 영상 데이터를 복구하거나 분석 및 복구 시간을 절약하기 위한 연구는 다양하게 진행되었다. 나기현 등은 블랙박스내 영상 데이터가 삭제된 경우 영상 데이터와 영상 데이터 내부에 저장되는 시간정보를 이용하여 삭제된 데이터를 복구하는 방법을 제시하였다.[2] 박정흠 등은 삭제되거나 손상된 영상 데이터가 저장 장치 내에 파편화되어 저장되어 있는 경우 이를 재조합하여 영상 데이터를 복구하는 연구를 진행하였다.[3] D.Suresh 등은 미할당 영역에 순차적으로 저장되지 않은 프레임을 시간 순으로 연결하여 영상 데이터를 복구하는 방법을 제안하였다.[4] 이국헌 등은 파일 시스템 구조에 기반을 둔 복구 방법을 이용하여 미할당 영역에서 삭제된 영상을 복구하고, 파일 시스템 구조를 이용하여 복구할 수 없는 경우에는 전체 영역에서 파일 포맷 구조에 기반을 둔 복구 방법을 이용하거나 바이트 스캔하는 방법을 제안하였다.[5]

이렇듯 블랙박스 영상에 대한 연구는 다방면으로 진행되어왔다. 그러나 블랙박스의 영상데이터가 대용량화하고 있어 필요한 영역의 데이터만을 선별하는 연구가 필요하다. 차인환 등은 블랙박스에서 사고 발생 시간과 GPS 위치 정보를 이용하여 필요한 영상 데이터를 선택적으로 복구하는 방식을 제안하였다.[6] 안휘향 등은 영상정보와 시간 정보, GPS 등의 비영상정보를 활용하여 영상 데이터를 선별하여 분석하는 방식을 제안하였다.[7]

그러나 포맷프리 저장 방식은 FAT32에서 변형된 파일 시스템 구조이므로, FAT32 파일 시스템 구조에 기반을 둔 복구 방법을 이용하여 미할당 영역에서 삭제된 영상을 복구할 수 없다. 또한 전체 영상의 프레임 데이터에서 비영상정보인 시간 정보를 검색하고, 필요한 프레임을 시간 순으로 정렬하여 재조합하는 기존 복구 방식은 시간이 많이 소요되는 문제점이 있으며, 프레임 단위의 시간정보를 저장하지 않는 경우도 존재한다. 본 논문은 영상 데이터가 시간 순으로 저장되는 포맷프리 저장 방식의 특성과 파일 포맷 구조를 이용하여 삭제된 블랙박스 영상 데이터의 프레임을 선별 수집하고, 자동화된 분석 시스템을 구현하는 방식을 제안한다.

3. 동영상 파일 포맷 구조

일반적인 동영상 파일은 컨테이너(Container)와 코덱(Codec)으로 구성된다. 컨테이너는 AVI, MP4 등 파일의 확장자 종류에 따라 어떤 규격을 가졌는지 알 수 있다. 컨테이너는 하나 이상의 압축된 데이터를 가지고 있으며 데이터의 종류는 비디오, 오디오, 텍스트 등이 있다.

비디오 데이터는 프레임 단위로 저장되며, 프레임의 종류에는 I프레임, P프레임이 있다. 일반적으로 비디오 데이터는 SPS(Sequence Parameter Set), PPS(Pic Parameter Set), I 프레임, P 프레임 순으로 저장된다. SPS는 해상도, 비디오 포맷 등이 포함되는 헤더 정보이고, PPS는 부호화 정보를 저장하는 헤더 정보이다.[8] I 프레임은 IDR(Instantaneous Decoding Refresh) Picture라고도 불리며, 다른 이미지를 참조하지 않고 독립적으로 복구가 가능한 정지 영상이 저장된 프레임이다. P 프레임은 프레임 사이의 예측(Predictive)을 의미하는 것으로 이전의 I 프레임 및 P 프레임을 참조하여 프레임을 부호화하므로, 그 자체만으로는 정지 영상 복구가 불가능하다.

H.264 코덱은 NAL 헤더를 이용하여 프레임을 구분하고, NAL은 1Byte값으로 사용하며 데이터를 구분하기 위해 Sync word라 불리는 0x000000001값을 결합하여 사용한다.[5] 포맷프리 저장 방식에서 MP4 파일 포맷의 Sync word는 데이터의 크기가 사용되고, 포맷프리 저장 방식에서 SPS, PPS, 프레임의 NAL헤더값과 Sync word가 결합된 시그니쳐는 표 2와 같다.

표 2. 포맷프리 저장 방식의 프레임 시그니쳐 종류
Table 2. Frame signature type of format free storeage

NAL type	NAL Header value(hex)	Signature(hex)	
		AVI	MP4
SPS	**27**, 47, **67**	00 00 00 01 **67**	EF E1 00 30 **27**(Data Size + **27**)
PPS	**28**, 48, **68**	00 00 00 01 **68**	00 01 00 04 **28**(Data Size + **28**)
I Frame	**25**, 45, **65**	00 00 00 01 **65**	00 02 1D 66 **25**(Data Size + **25**)
P Frame	01, **21**, 41, **61**	00 00 00 01 **61**	00 00 55 E4 **21**(Data Size + **21**)

3.1. AVI 파일 포맷 구조

AVI 파일 포맷의 스트림은 비디오, 오디오, 텍스트로 분류된다. 각 스트림의 식별자는 '00dc', 01wb', '02tx'와 같이 2 byte의 스트림 번호 문자와 2 byte의 비디오, 오디오, 문자열 표시가 합쳐진 총 4 Byte의 식별자로 구성 된다. 첫 번째 스트림이 비디오 데이터일 경우 스트림 번호가 '00'이 되고, 비디오 인덱스가 'dc' 이므로, '00dc'가 데이터 식별자이다. 두 번째 스트림이 오디오 데이터일 경우 스트림 번호가 '01'이 되고, 오디오 인덱스가 'wb'이므로 '01wb'로 표시된다. 세 번째 스트림이 텍스트 데이터일 경우 스트림 번호가 '02'가 되고, 문자열 인덱스가 'tx'이므로 '02tx'로 표시된다. 각 스트림의 식별자 뒤에는 스트림 데이터 크기가 4Byte로 저장된다.[8]

3.2. MP4 파일 포맷 구조

MP4 영상 파일 포맷 구조는 크게 3개의 컨테이너(ftyp, mdat, moov) 영역으로 구성된다. 컨테이너의 헤더는 처음 4Byte에 데이터 크기를 저장하고, 다음 4Byte에 컨테이너 시그니쳐가 저장된다.

첫 번째 컨테이너인 ftyp 컨테이너는 파일 타입과 파일 호환 포맷에 대한 내용을 저장하고, 두 번째 컨테이너인 mdat 컨테이너는 영상, 음성자료를 프레임 단위로 저장한다, 세 번째 컨테이너인 moov 컨테이너는 영상의 실행에 필요한 싱크정보를 저장한다.[8]

4. 포맷프리 저장 구조

일반적인 차량용 블랙박스는 메모리에 30초 ~ 1분 단위의 영상을 보관한 후, AVI, MP4와 같은 파일 포맷를 이용하여 파일 단위로 저장한다. 파일 단위로 저장되는 방식의 블랙박스에서 사고나 충격으로 전원 공급이 중단되는 경우 메모리에 보관된 영상이 정상적으로 파일에 저장되지 않는 문제점이 있다. 하지만 포맷프리 저장 방식은 프레임 단위의 영상 데이터를 순차적으로 저장하는 방식이다.

FAT32에서 데이터에 메모리를 할당하는 논리적인 최소 단위가 클러스터이다.[9] 하지만 NxFS 포맷프리 저장 방식에서 메모리를 할당하는 최소 단위는 Chunk 단위이고, FAT32 기반 포맷프리 저장 방식은 제조사마다 상이한 고정된 영상 파일의 크기 단위로 할당된다.

파일 슬랙은 파일을 저장하기 위해 파일시스템에서 메모리가 할당되었으나 실제로는 파일의 데이터가 저장되지 않은 영역이다.[9] 따라서 NxFS 포맷프리 저장 방식은 파일의 데이터 끝부터 파일에 할당된 마지막 Chunk의 끝까지이고, FAT32 기반 포맷프리 저장 방식은 파일의 데이터 끝부터 파일에 할당된 크기의 끝까지이다. 그리고 파일 슬랙의 끝부터 다음 파일의 시작 위치 또는 메모리의 끝까지가 미할당 영역이다.

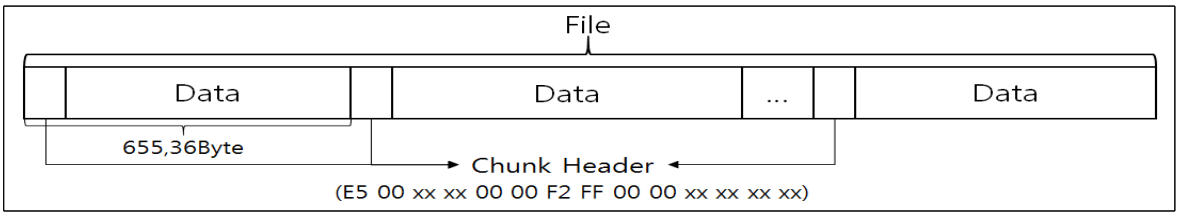

그림 1. NxFS 포맷프리 저장 방식의 Chunk 구조
Fig. 1. NxFS Format Free Storage Chunk Structure

영상 데이터를 저장하기 위해 할당된 영역에 영상 데이터가 모두 저장되면, 앞부분의 파일부터 순차적으로 데이터가 덮어 써진다. 따라서 덮어써진 영상 데이터가 이전 영상 데이터보다 크기가 작으면, 그림2와 같이 슬랙 영역에 이전 영상 데이터가 저장되어 있다.[9]

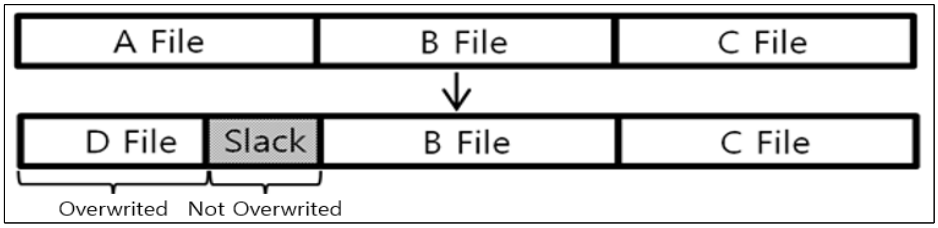

그림 2. 슬랙 생성 원리
Fig. 2. Slack Generation Priciple

4.1. NxFS 포맷프리 구조

NxFS 포맷프리 저장 방식은 AVI 파일 포맷으로 저장되나 윈도우 탐색기에서 영상 파일들을 탐색 및 재생할 수 없고, 제조사에서 제공하는 전용 프로그램으로만 영상 파일을 탐색 및 재생할 수 있다.

NxFS 포맷프리 파일시스템은 Offset 3에서 NxFS 시그니처가 존재하므로, NxFS 시그니처로 NxFS 포맷프리 저장 방식임을 알 수 있다.

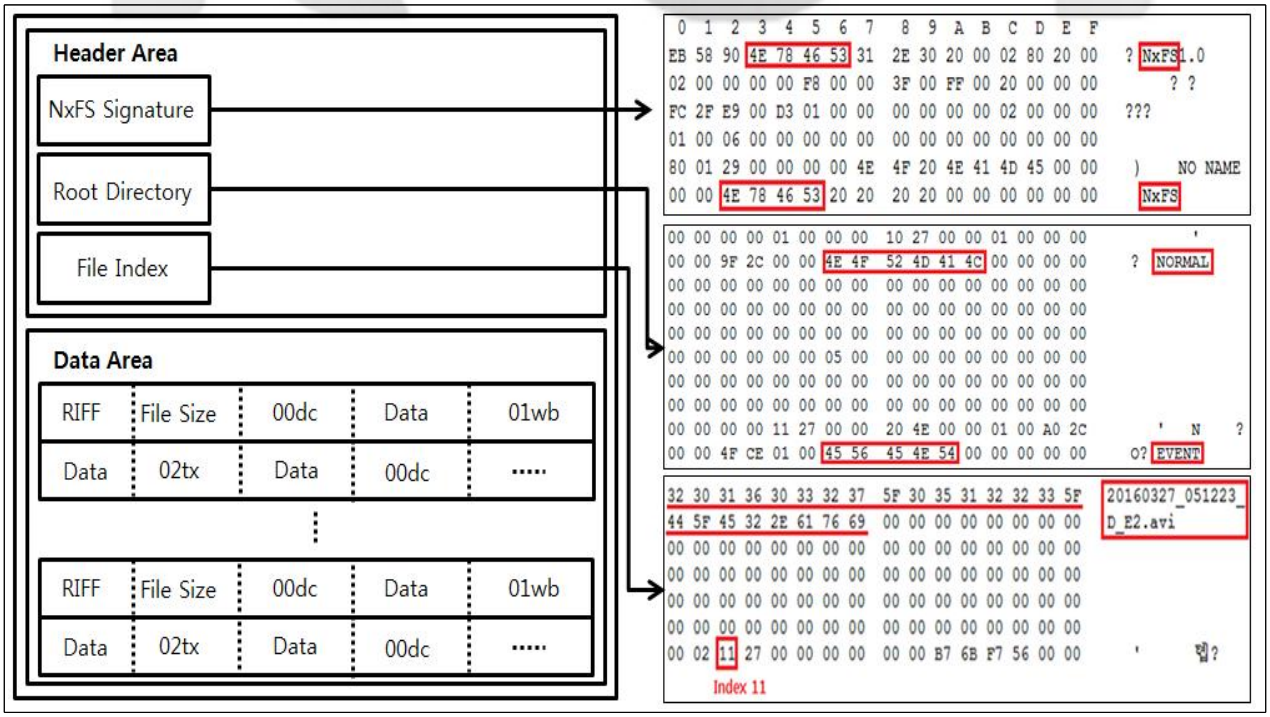

그림 3. NxFS 포맷프리 영상 데이터 저장 구조
Fig. 3. NxFS format free image data storage structure

4.2. FAT32 파일시스템 기반 포맷프리 구조

FAT32 파일시스템을 이용한 포맷프리 영상 저장 방식은 영상 파일의 크기와 생성 시간이 동일한 AVI 파일 포맷 또는 MP4 파일 포맷으로 생성하고. 기존 분석 도구나 윈도우 탐색기에서 영상 파일을 탐색 및 재생할 수 있다. 따라서 FAT32 파일시스템의 포맷 프리 영상 저장 방식에서 영상 파일의 생성 시간은 포맷 시간이고, 수정 시간은 영상이 저장된 시간이다.

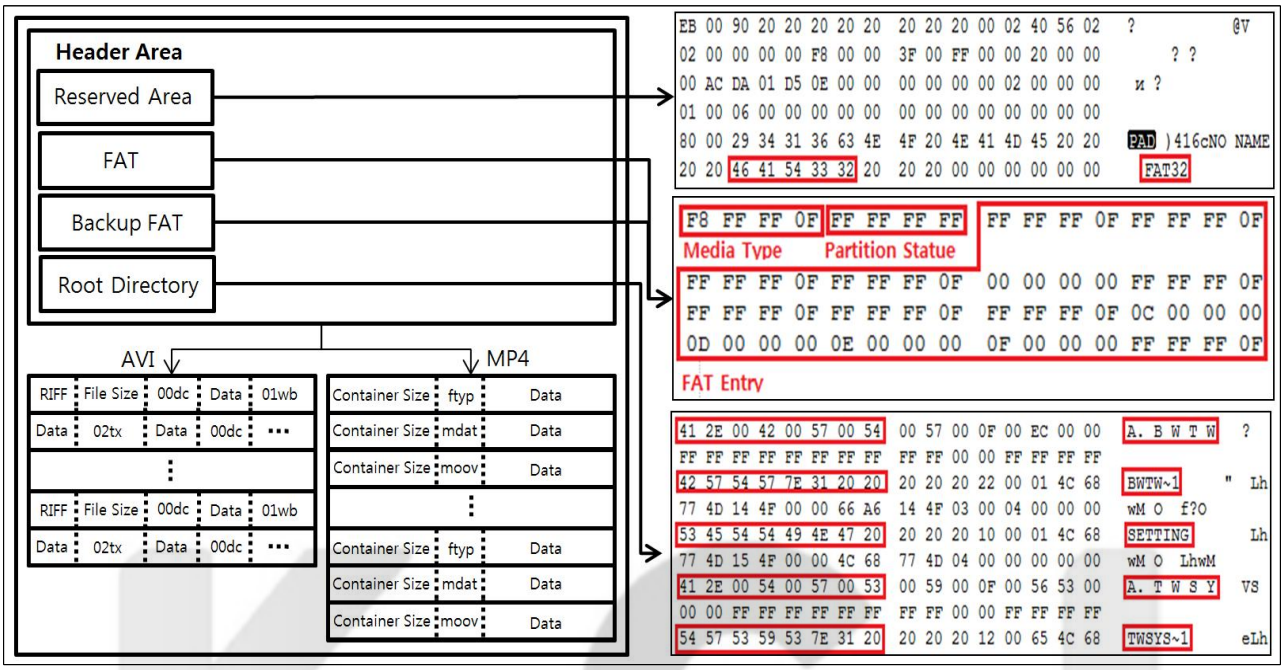

그림 4. FAT32 포맷프리 영상 데이터 저장 구조
Fig. 4. FAT32 format free image data storage structure

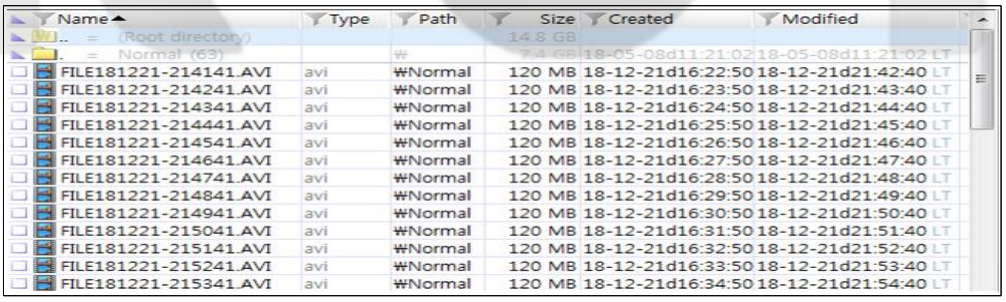

그림 5. X-Way 분석 프로그램에서 FAT 32 포맷프리 방식의 파일 목록
Fig. 5. FAT32 format free file list in X-Way analysis program

영상 파일 목록에서 파일의 크기가 동일하나 다른 파일들에 비해 영상의 길이가 작은 파일들을 확인할 수 있다. 영상의 길이가 작은 파일들은 뒷부분에 파일 슬랙 영역이 존재한다.

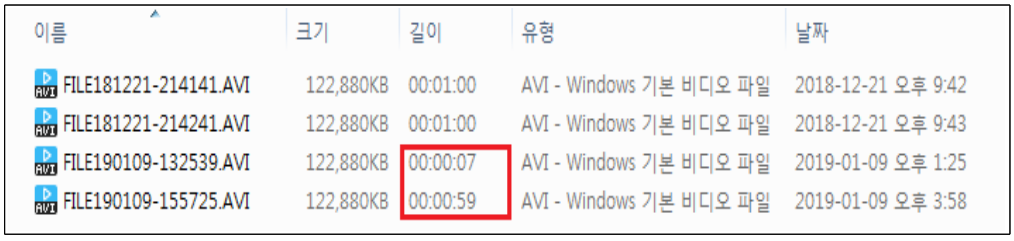

그림 6. 윈도우 탐색기에서 FAT32 포맷프리 방식의 영상 파일 목록
Fig. 6. FAT32 format free video file list in Windows Explorer

5. 포맷프리 저장 방식에서 영상 복구 방법 제안

현재 수사기관에서는 포맷프리 저장 방식에 대해 그림7 과 같이 분석 하고 있다. 미할당 영역과 슬랙 영역을 구분하지 못할 경우, 전체 영역을 검색하여 프레임 단위로 영상 데이터를 추출하는데 많은 시간이 소요된다는 문제점이 발생한다.[4] 또한, 전체 영역에서 추출한 프레임은 삭제된 영역의 프레임인지 여부를 알 수 없기 때문에 많은 시간을 소요하여 모든 프레임을 보고 선별하여야 한다는 문제점이 있다.

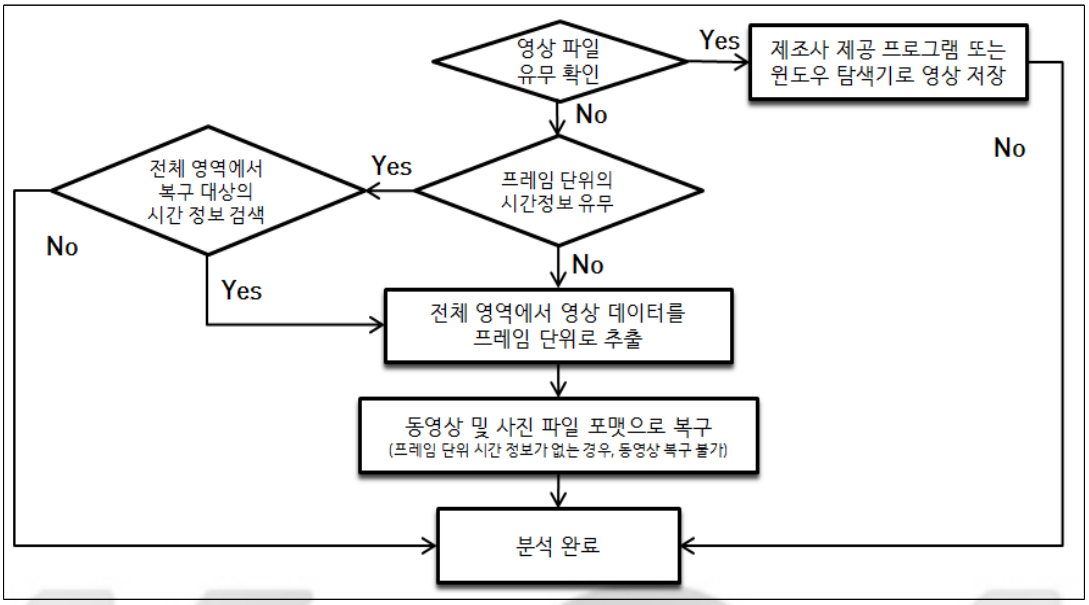

그림 7. 현재 수사기관의 포맷프리 저장 방식 영상 복구 방법 순서도
Fig. 7. Flowchart of how to recover format free storage method of current investigative agency

블랙박스 영상에서 디지털 포렌식이 필요한 부분은 정상적으로 접근할 수 없는 삭제된 영역이다. 따라서 포맷프리 저장 방식으로 저장된 메모리카드의 전체 영역이 아닌 파일 슬랙 영역에서 시간 정보를 검색하고, 복구하고자 하는 시간대의 파일 슬랙을 선별할 필요가 있다. 복구할 필요가 있는 파일 슬랙을 선별했다면, 동영상, 음성, 사진 파일 포맷, 인코딩, 디코딩하는 FFMPEG 프로그램을 사용하여 해당 영역에서 프레임 단위로 복구할 수 있다. 기존 분석 방법인 프레임 단위로 추출하여 동영상으로 변환하는 경우에는 음성 데이터의 손실이 발생하지만, 파일 슬랙 영역을 FFMPEG 프로그램으로 복구하는 경우에는 음성 데이터의 손실을 방지할 수 있다.

그러나 파일 슬랙에 존재하는 프레임의 수가 적은 경우, 동영상 복구 시 프레임이 누락되거나 동영상의 재생시간이 짧아 영상을 식별할 수 없는 문제점이 발생할 수 있다. 이러한 문제점을 해결하기 위해 동영상 파일 포맷으로 복구하고, 데이터가 적을 경우에는 프레임 단위에서 사진 파일 포맷으로 복구한다.

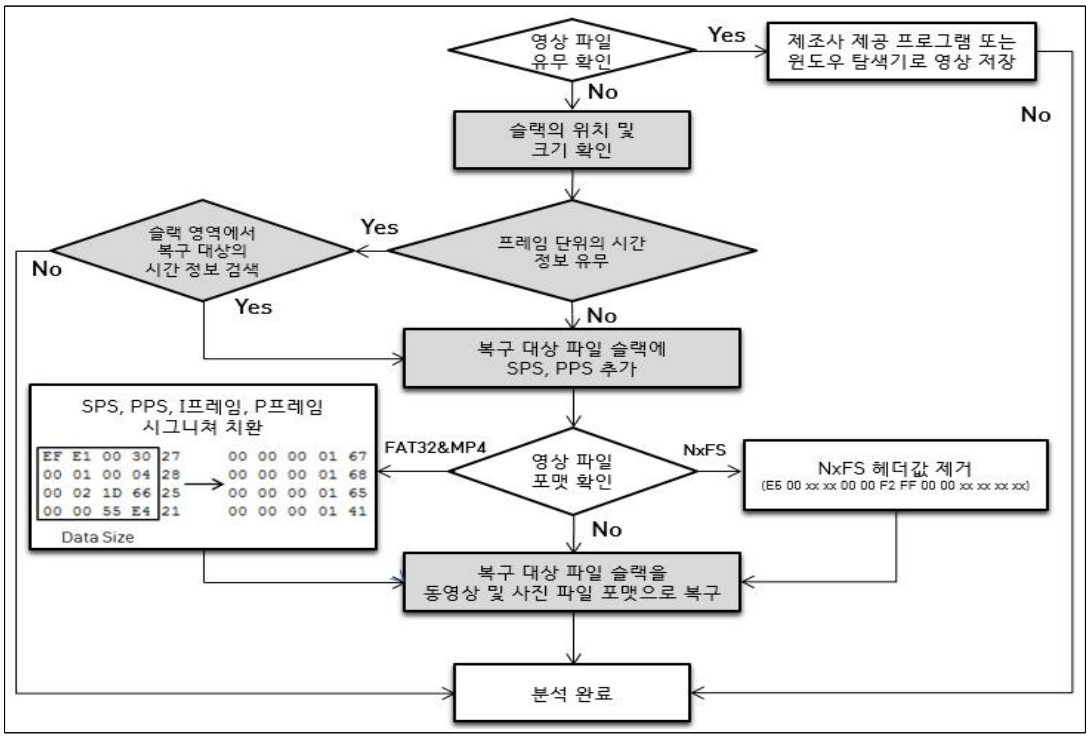

그림 8. 포맷프리 저장 방식 영상 복구 방법 제안 순서도
Fig. 8. Suggested flowchart for format free storage image recovery

5.1. 파일 슬랙에서 시간 정보 검색

NxFS 포맷프리 저장 방식에서는 AVI 파일 포맷의 문자열 스트림에 제조사 정의 시간 정보가 저장되거나 Unix Time 시간 정보로 저장된다. 첫 번째 유형인 제조사 정의 시간 정보는 표 3과 같이 텍스트 스트림 시그니쳐에서 Offset 15에 위치하며, 2Byte씩 연, 월, 일, 시, 분, 초 순으로 저장되어 있다.

표 3. NxFS 저장 방식의 제조사 정의 시간 정보 구조
Table 3. Menufacture defined time information structure for NxFS storage

위치	헥사 값	해석	의미
0	30 32 74 78	02tx	텍스트 스트림
4	0F 00 00 00	0Fh(15)	데이터 크기
15	12	18	2018년
16	0B	11 + 1	12월
17	1B	27	27일
18	07	7	7시
19	2A	42	42분
20	37	55	55초

두 번째 유형인 Unix Time 시간 정보는 표 4와 같이 텍스트 스트림 시그니쳐에서 Offset 15에 위치하여, 4Byte의 크기에 Unix Time(Big Endian) 시간 정보로 저장되어 있다.

표 4. NxFS 포맷프리의 Unix Time(Unix Time: 32 bit Hex Value - Big Endign) 시간 정보 저장 방식
Table 4. How to store Unix Time(Unix Time: 32 bit Hex Value - Big Endign) information in NxFS format free

위치	헥사 값	해석	의미
0	30 33 74 78	03tx	텍스트 스트림
4	0C 00 00 00	0Ch(12)	데이터 크기
15	5C DA A3 28	2019. 5. 14. 11:14:48 (Unix: 32 bit Hex Value - Big Endian)	시간 정보

FAT32 포맷 프리 저장 방식은 AVI 파일 포맷의 문자열 스트림에 Unix Time(Little Endian) 시간 정보가 저장된다. Unix Time 시간 정보는 표 5와 같이 텍스트 스트림 시그니쳐에서 Offset 15에 위치하며, 4Byte의 크기에 Unix Time 시간 정보로 저장되어 있다.

표 5. FAT32 포맷프리 Unix Time (Unix Time : 32 bit Hex Value - Little Endian) 시간 정보 저장 방식
Table 5. How to store Unix Time(Unix Time : 32 bit Hex Value - Little Endian) information in FAT32 format free

위치	헥사 값	해석	의미
0	30 33 74 78	03tx	텍스트 스트림
4	48 00 00 00	48h(72)	데이터 크기
20	EE 43 F6 5A	2018. 5. 12. 01:31:26 (Unix: 32 bit Hex Value - Little Endian)	시간정보
34	6B 00	6Bh(107)	시간정보(ms)

FAT32 포맷 프리 저장 방식에서 MP4 파일 포맷은 프레임 단위의 시간 정보가 텍스트 데이터로 저장되지 않는다. 또한, NxFS 저장 방식과 FAT32 저장 방식에서도 시간 정보가 저장되지 않을 수 있다. 따라서 시간 정보를 저장하지 않는 경우에는 시간 정보의 텍스트 데이터를 검색하여 선별할 수 없으므로, 모든 파일 슬랙의 프레임을 사진 파일 포맷과 동영상 파일 포맷으로 복구해야 한다.

5.2. 파일 슬랙에서 동영상 복구 또는 사진 데이터 추출

포맷 프리 저장 방식의 AVI 파일 포맷은 인덱스 시그니쳐(idx)로부터 인덱스 크기만큼 이동하면, 파일 슬랙의 시작 위치를 찾을 수 있고, 다음 AVI 파일 시그니쳐까지가 파일 슬랙이다. 포맷 프리 저장 방식의 MP4 파일 포맷은 ftyp, mdat, moov 컨테이너 크기만큼 이동하면, 파일 슬랙의 시작 위치를 찾을 수 있고, 다음 MP4 파일의 시그니쳐까지가 파일 슬랙이다.

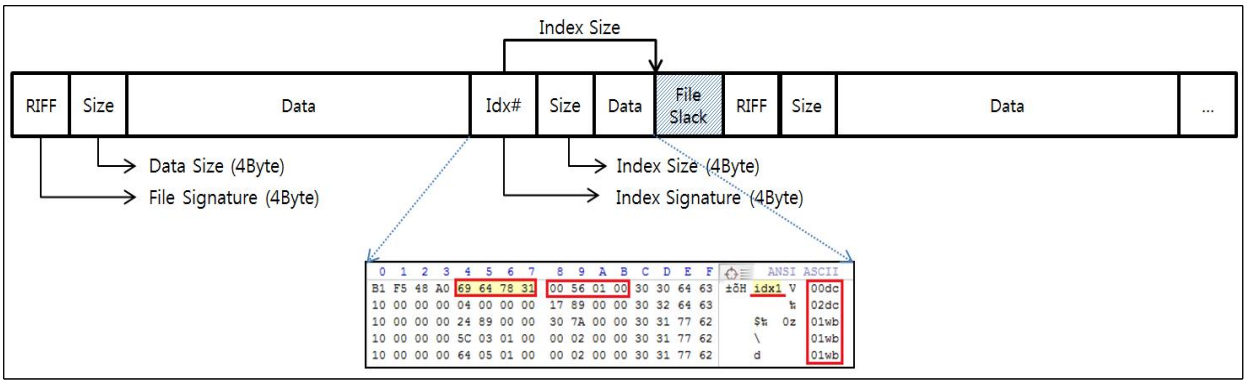

그림 9. AVI 파일 포맷 슬랙 위치
Fig. 9. AVI location in the AVI file format

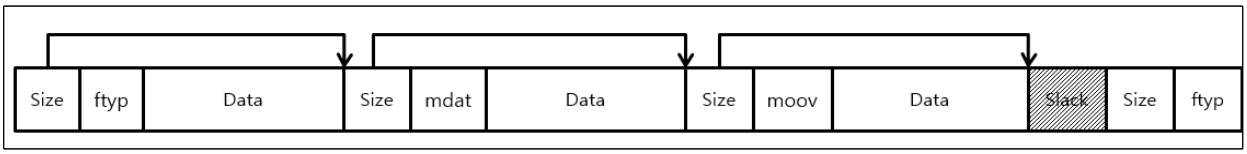

그림 10. MP4 파일 포맷 슬랙 위치
Fig. 10. Slack location in the MP4 file format

FFMPEG 프로그램으로 영상 데이터를 복구하는 경우에는 Offset 0의 위치에 SPS, PPS, 프레임 순으로 저장되어야 한다.

파일 슬랙의 앞에 존재하는 프레임의 헤더와 데이터 일부가 덮어 쓰여졌을 수 있다. 따라서, 프레임의 헤더가 존재하지 않는 데이터부터 제일 먼저 검색되는 I프레임의 헤더 앞까지 제거하고, 제일 먼저 검색된 I 프레임의 헤더 앞에 SPS와 PPS를 추가한다. FAT32 포맷 프리 저장 방식에서 MP4를 사용하면 그림 11과 같이 치환한 SPS와 PPS를 추가하였다. 표 6은 치환한 예이다.

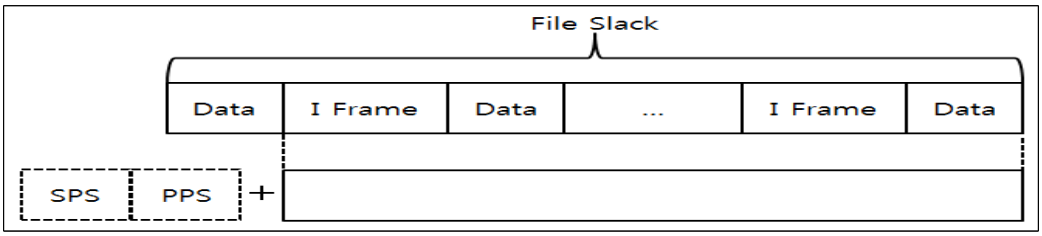

그림 11. 슬랙 데이터에 SPS와 PPS를 추가
Fig. 11. Add SPS and PPS to slack data

표 6. SPS와 PPS 치환
Table 6. SPS and PPS substition

Item	Value
치환 전 SPS와 PPS	**EFE1003027**4D00339A6402802DD35010101400000FA40003A983A18005B900005B8DAEF2E343000B720000B**71B5DE5C28**000000001000428EE3C8
치환 후 SPS와 PPS	**0000000167**4D00339A6402802DD35010101400000FA40003A983A18005B900005B8DAEF2E343000B720000B0**0000000168**000000001000428EE3C8

FFMPEG 프로그램으로 포맷프리 저장 방식의 파일 슬랙을 추출하여 저장한 파일을 대상으로, 그림 12와 같이 프레임 단위를 사진 파일 포맷으로 복구한다.

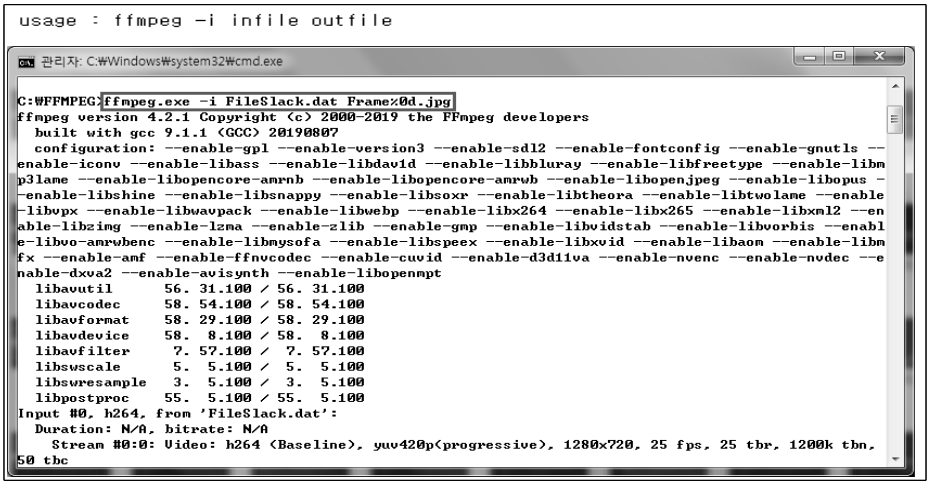

그림 12. FFMPEG 프로그램을 이용하여 사진 파일 포맷으로 복구
Fig. 12. Recover photo file format using FFMPEG program

그림 13. 슬랙 영역에서 사진 파일 포맷으로 복구한 프레임
Fig. 13. Frame recovered from slack area to photo file format

FFMPEG 프로그램으로 FAT32 포맷프리 저장 방식의 AVI 파일 포맷에서 슬랙 영역을 동영상 파일 포맷으로 복구한다. 그림 14와 같이 복구할 경우에는 음성 데이터가 손실되지 않아 동영상 파일 포맷을 동영상 플레이어로 재생 시에 음성도 청취할 수 있다.

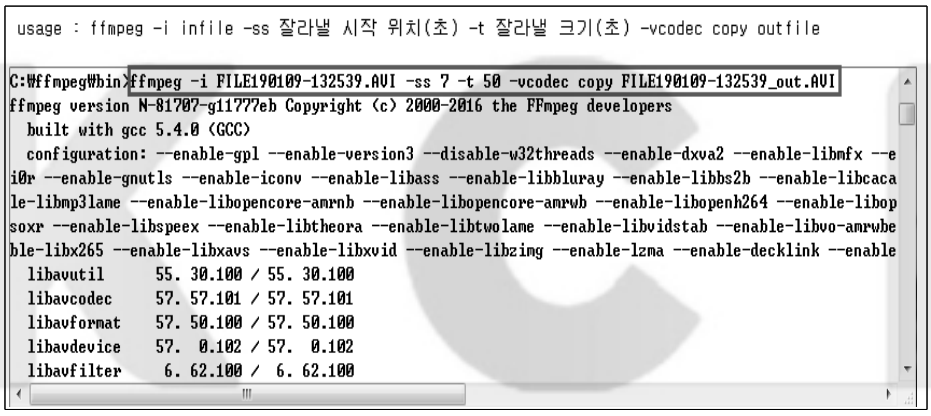

그림 14. FFMPEG 프로그램으로 FAT32 저장 방식의 AVI 파일 포맷 슬랙 영역 동영상 복구
Fig. 14. AVI file format slack area video recovery with FAT32 storage with FFMPEG program

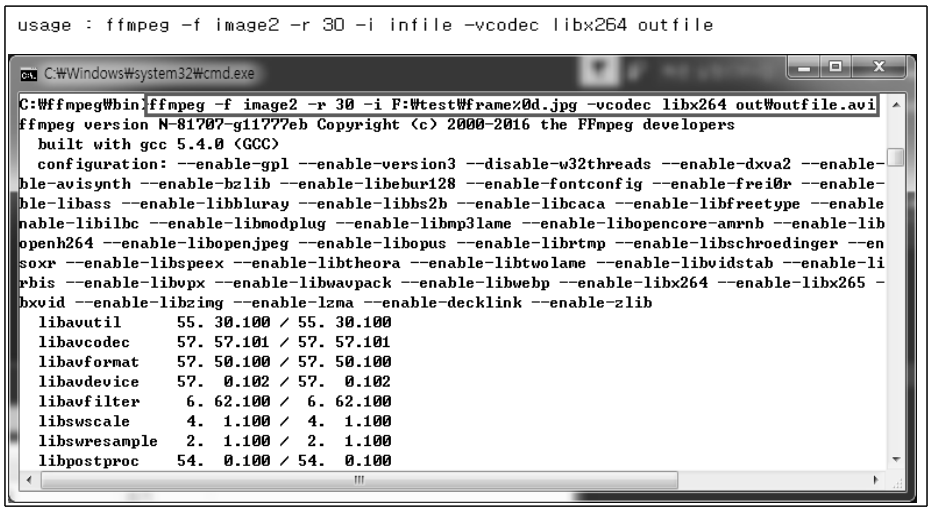

그림 15. FFMPEG 프로그램으로 NxFS 와 FAT32 저장 방식의 슬랙 영역 동영상 복구
Fig. 15. FFMPEG program recovers slack area video with NxFS and FAT32 storage

그림 16. 슬랙 영역에서 동영상 파일 포맷으로 복구한 영상
Fig. 16. Image recovered from video file format in slack area

6. 구현 결과

블랙박스 포맷프리 분석 도구는 C#을 이용한 GUI 환경으로 그림 17, 그림 18와 같이 개발하였다. 이 도구는 슬랙 영역 위치 및 크기, 시간 정보 검색, 파일 슬랙 선별, SPS와 PPS 등을 검색하여 치환 및 추가하는 기능이 구현되었으며, 동영상 및 사진 파일 포맷으로 복구하는 기능은 FFMPEG 프로그램을 호출하여 구현하였다. 구현 결과를 확인하기 위하여 표 7과 같이 실험을 진행하였다.

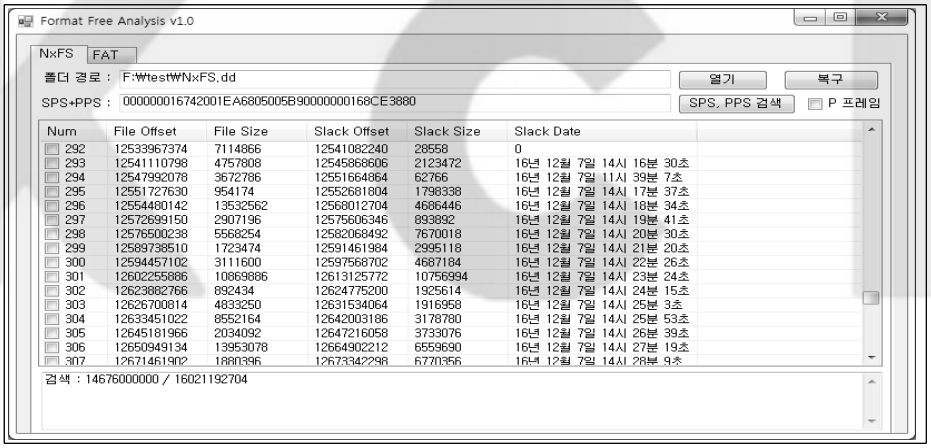

그림 17. NxFS 포맷프리 저장 방식 영상 분석 프로그램
Fig. 17. NxFS format free storage video analysis program

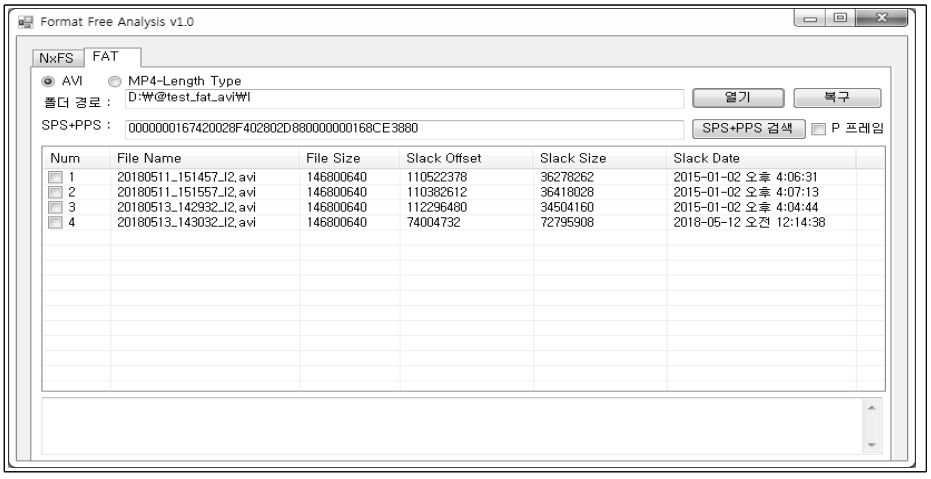

그림 18. FAT32 포맷프리 저장 방식 영상 분석 프로그램
Fig. 18. FAT32 format free video analysis program

표 7. 포맷프리 분석 도구의 구현 결과 실험 대상 제품
Table 7. Result of implementation of format free analysis tool

포맷 프리	파일 포맷	제조사	모델명
NxFS	AVI	URIVE	albatross A3
		VUGERA	VG-701V2
FAT32	AVI	루카스	LK-9100 Duo
		만도	GH100
	MP4	아이나비	V900

일반적으로 데이터 복구 시 미할당 영역과 슬랙 영역이 복구할 영역이다. 그러나 차량용 블랙박스에서 포맷프리 저장 방식은 기존 분석 도구로는 미할당 영역과 슬랙 영역을 제대로 구분해 주지 않아, 전체 영역에서 영상 데이터를 복구해야 했다. 그림 19과 같이 16GB 메모리의 전체 영역에서 I 프레임을 추출하는데 소요되는 시간보다 슬랙 영역에서 I 프레임을 추출하는데 소요되는 시간이 적게 소요되었다. 전체 영역에서 추출된 프레임에서 삭제된 영역의 프레임을 선별에 소요되는 시간은 평가 시간에서 제외하였다. 그럼에도, 삭제된 영역의 프레임을 자동화 프로그램으로 선별하면 큰 차이로 분석 시간을 줄일 수 있는 것을 확인하였다.

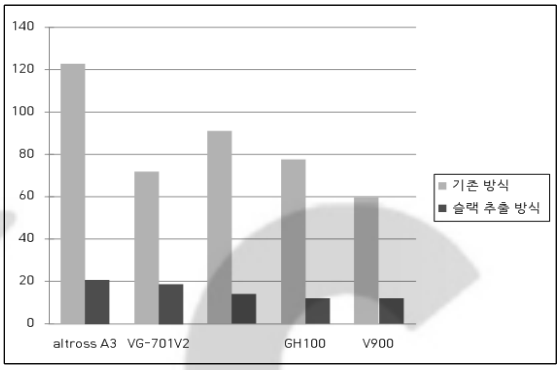

그림 19. 기존 방식과 슬랙 추출 방식 소요 시간 비교
Fig. 19. Comparing the time required for the convetional method and the slack extraction method

7. 결론 및 향후 연구

본 논문에서는 포맷프리 저장 방식의 블랙박스에서 점유율이 높은 NxFS 포맷프리 저장 방식과 FAT32 포맷프리 저장 방식을 선정하여 삭제된 데이터만을 구분하여 복구하는 방법에 대해 분석하였고, 이러한 저장 방식에서 슬랙 내의 영상 프레임을 동영상과 사진 파일 포맷으로 복구하는 포렌식 분석 도구를 개발하여 효과를 확인하였다.

다만, 점유율이 높은 NxFS 포맷프리, FAT32 포맷프리만을 대상으로 하였으며, TAT 포맷프리 저장 방식이 본 방식에 효과가 있는지는 확인하지 못하였다. 또한, 향후 증가할 것으로 보이는 H.265 코덱 방식의 영상에 대해서도 대응이 필요하다. 본 논문에서 충분히 연구하지 못한 이 두 가지 방식에 대해서도 연구가 필요할 것으로 보인다.

참 고 문 헌 (References)

〔1〕 http://cctvnews.co.kr/news/articleView.html?idxno=22438

〔2〕 G. D. Na. S. Shim, J. S. Byun, E. S. Kim, and J. Lee, "Recovery corrupted Video Files using Time Information", Journal of Korea Multimedia Society, Vol.18, No.12, pp. 1492-1500, 2015.

〔3〕 J. H. Park and S. J. Lee, "Data frament forensics for embbedded DVR systems", Digital Investifation, Vol.11, No.3, pp.187-200, 2014.

〔4〕 D.Suresh, D.V.Ramana, D.Arun Kumar, "FRAME BASED RECOVERY OF CORRUPTED VIDEO FILES", pp. 193-198, 2015.

〔5〕 이국헌, 박아란, 조성혜, 백현우, 박찬순, 이한형, "손상된 CCTV, 블랙박스의 복원대상기기 확대 및 통합뷰어 개발", 고려대학교 산학협력단 연구개발 결과보고서, pp. 193-198, 2015.

〔6〕 I. H. Cha, K. H. Lee, S. J. Lee, "Design and implementation of Car Blackbox Forensic Analysis Tool Though the Analysis of Data Structure", KIPS Tr. Comp. and Comm. Sys, Vol.5, No.11, pp.427-438, 2016.

〔7〕 H. H. An, S. J. Lee, "The analysis of data structure to digital forensic of dashboard camera", Journal of The Korea Insititute of Information Security & Cryptology, Vol.25, No.6, pp. 1495-1502, 2015.

〔8〕 박기현, "이론과 실무의 조화 코덱의 세계로의 초대", pp. 4-6, pp. 172, pp. 320-338, 2006.

〔9〕 Phil Nabity. Brett J. L. Landry, "Recovery Deleted and Wiped FIles: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator", University of Dallas, pp. 3-5, 2009.

저 자 소 개

오 영 주 (Youngjoo Oh)
준회원
2010년 2월 : 호서대학교 정보보호학과 졸업
2016년 5월~현재 : 경기남부지방경찰청 사이버안전과 디지털포렌식계
2019년 2월~현재 : 고려대학교 정보보호대학원 디지털포렌식학과 석사과정
관심분야 : 디지털포렌식, 모의해킹, 악성코드, 정보보호 등

이 상 진 (Sangjin 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