Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.4, Aug. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.4.609

DJI 드론 모델별 삭제 비행기록 복구 가능성 분석*

윤 여 훈,[1†] 윤 주 범[2‡]
[1,2]세종대학교 (대학원생, 교수)

Analysis of the Possibility of Recovering Deleted Flight Records by DJI Drone Model*

YeoHoon Yoon,[1†] Joobeom Yun[2‡]
[1,2]Sejong University (Graduate student, Professor)

요 약

최근 IoT 산업 중 하나인 드론을 사용한 범죄가 지속적으로 보고되고 있다. 특히 드론은 손쉽게 접근하여 자유롭게 움직이는 특징이 있어 폭발물 운반, 마약 운반, 불법 촬영 등 다양한 범죄에 사용된다. 이러한 범죄 행위를 분석하고 수사하기 위해 드론 포렌식 연구가 매우 강조되는 상황이다. 드론에서 획득할 수 있는 대표적인 디지털 포렌식 아티팩트로는 미디어 데이터, PII, 비행기록 등이 있으며 특히 비행기록은 드론의 행적을 추적할 수 있는 중요한 아티팩트가 된다. 따라서 본 논문에서는 DJI 드론의 삭제된 비행기록 파일이 갖는 특징을 제시하고 특징의 차이점이 발생하는 세 가지 드론인 Phantom3, Phantom4, Mini2 드론을 이용하여 검증하였다. 또한 비행기록 파일이 갖는 특징을 이용하여 파일 카빙 기법을 통해 복구 정도를 분석하고 최종적으로 드론 모델별로 비행기록의 복구 가능성이 존재하는 드론과 그렇지 않은 드론 모델들을 분류한다.

ABSTRACT

Recently, crimes using drones, one of the IoT industries have been continuously reported. In particular, drones are characterized by easy access and free movement, so they are used for various crimes such as transporting explosives, transporting drugs, and illegal recording. In order to analyze and investigate these criminal acts, drone forensic research is highly emphasized. Media data, PII, and flight records are digital forensic artifacts that can be acquired from drones, in particluar flight records are important artifacts since they can be used to trace drone activities. Therefore, in this paper, the characteristics of the deleted flight record files of DJI drones are presented and verified using the Phantom3, Phantom4 and Mini2 models, two drones with differences in characteristics. Additionally, the recovery level is analyzed using the flight record file characteristics, and lastly, drones with the capacity to recover flight records for each drone model and drone models without it are classified.

Keywords: Drone Forensic, DJI, Drone, Recoverability, Flight Log

I. 서 론

IoT(Internet of Things) 기기란 스마트 워치, 카메라, 자동차와 같이 사물에 네트워크가 연결되어 실시간으로 통신이 가능한 임베디드 기기를 의미한다. 이러한 IoT 기기 중 하나인 드론은 무인 항공기

Received(04. 18. 2023), Modified(07. 05. 2023), Accepted(07. 06. 2023)
* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2023-2018-0-01423)
† 주저자, yeohoon1991@naver.com
‡ 교신저자, jbyun@sejong.ac.kr(Corresponding author)

(Unmanned Aerial Vehicle)라고도 불린다. 또한 농업, 임업, 배송, 군사 분야를 넘어 촬영, 레이싱 등의 취미용 드론까지 다양한 편의성을 제공함에 따라 세계적으로 폭발적인 추세로 증가하고 있다.

하지만 드론의 증가에 따라서 드론을 사용한 불법적 문제 또한 지속적으로 보고되고 있으며 미국 연방항공처(Federal Aviation Administration)에서 발표한 무인 항공기 불법 통계를 보면 2020년 1637건, 2022년 1811을 기록하여 약 10%가 증가한 수치이다[1]. 하지만 현재의 드론 디지털 포렌식 연구는 현저히 부족한 수준이며, 다양한 드론 제조회사와 모델에 따른 통합된 디지털 포렌식 프레임워크를 적용하기 어려운 점도 존재하다[2][3]. 그렇기 때문에 드론 포렌식 연구의 필요성이 매우 강조된다.

본 논문에서는 세계적으로 드론 시장의 80% 이상의 점유율를 가진 DJI(Da Jiang Innovation)의 Phantom3 Standard, Phantom4 Standard 드론과 미국의 NIST와 협약하여 포렌식 연구를 진행하는 VTO Labs[4]에서 제공한 드론 포렌식 데이터 셋을 이용하여 포렌식 분석을 진행하였다[5]. 드론 포렌식의 중요 아티팩트 중 하나인 비행 기록(Flight Record)은 내부 SD카드에 기록되는데, 각각의 드론 모델별로 삭제된 비행기록의 콘텐츠(Contents)가 비할당 영역에 잔존하는 경우와 잔존하지 않는 경우가 존재한다. 이때 드론 모델마다 삭제된 파일의 특징이 다르다는 것을 검증하기 위해 특징의 차이가 발생하는 사례 중 Phantom3 드론과 Phantom4 드론, Mini2 드론을 통해 직접 비행하여 비행기록이 할당되는 방식과 삭제되는 방식을 분석하고 그 차이점을 검증하였다. 그 후, 비할당 영역에 콘텐츠가 잔존하는 특징을 이용하여 파일 카빙 기법을 적용하여 비행기록 복구 정도를 분석하였다. 최종적으로는 비할당 영역에 데이터가 잔존하는 특징에 따라서 비행기록의 복구가 가능한 드론과 그렇지 않은 드론을 분류한다.

본 논문은 총 5장으로 구성되어 있으며 2장에서는 드론 포렌식과 관련된 연구를 서술하고 3장에서는 모델별로 비할당 영역에 데이터가 잔존하는 차이를 보여주고 3가지 특징에 따른 드론을 보여준다. 또한 Phantom3 모델과 4 모델의 사례를 통해 비행기록의 할당과 삭제의 특징을 검증한다. 4장에서는 드론의 비행을 통해 얻은 비행 기록 복구 정도와 분석한 결과를 설명하고 복구 가능성이 존재하는 드론 모델을 분류한 뒤, 마지막 5장에서 결론을 통해 본 논문을 정리하고 끝맺는다.

II. 관련연구

드론 제조업체로는 DJI, SenseFly, Parrot, Yuneec 등이 있으며, 각 업체마다 다양한 모델을 생산한다. 또한 드론에서 얻을 수 있는 아티팩트 종류는 매우 다양하기 때문에 아티팩트를 저장하는 저장소도 제조업체마다 상이하다. 본 논문에서는 시장 점유율이 높은 DJI 기업의 드론을 통해 연구하였다. 이영우 등[6]은 DJI 드론의 아티팩트 저장소를 크게 내부 저장소, 외장 저장소, 모바일 저장소 3가지로 분류하였으며, 각 저장소별로 획득할 수 있는 아티팩트의 종류를 제시하였다. Stanković 등[7]은 DJI Mini2 모델을 이용하여 포렌식 분석을 진행하였으며 iPhone, Samsung, SD card를 대상으로 아티팩트를 획득하였고 각 분석 결과를 Autopsy, Cellebrite, Magnet AXIOM 3가지 포렌식 도구를 통한 최종 평가를 제시하였다. 대표적으로 도구 평가에 사용된 드론의 아티팩트로는 PII(Personal Identifiable Information), 미디어 데이터, 비행 기록이었다. 이와 비슷하게 Salamh 등[8]은 DJI Phantom4와 Matrice 210 모델을 사용하여 PII, 미디어 데이터, 비행 기록을 분석하였고 Autopsy, Cellebrite, Magnet AXIOM 3가지 포렌식 도구를 비교하였다. 이때 Autopsy와 Cellebrite를 이용하여 복호화한 비행 기록이 동일한 데이터를 추출하지 못하였으며 이는 법의학적으로 문제가 될 수 있다고 강조하였다.

이처럼 드론 아티팩트는 크게 PII, 미디어 데이터, 비행기록 3가지로 구분되어진다. 이때 비행기록은 드론이 비행한 날짜, 시간, 풍속, 컨트롤러 일련번호, GPS(경도, 위도, 고도)정보 등 다양한 비행 정보를 갖고 있는 매우 중요한 아티팩트이다. [9]와 [10]의 저자들은 Phantom4 드론과 Spark 드론에서의 범죄 시나리오를 기획하여 이때의 비행기록을 통한 포렌식 분석 결과를 보여준다. [11]의 저자 또한 Mavic Air 드론을 이용하여 각 저장소에서 획득할 수 있는 아티팩트들의 종류와 분석 결과를 제시한다. 그리고 [8]의 제시점처럼 DJI의 비행기록은 암호화가되어 .DAT 확장자를 가진 채 내부 SD카드에 저장된다. 이때 암호화된 비행기록을 복호화하는데 필요한 여러 도구가 존재하는데 일반적으로 사용되는 복호화 도구는 DatCon[12]이다. DatCon은 다양

한 DJI 드론의 비행기록 복호화 알고리즘을 구현하여 비행기록을 CSV 형태로 추출해주는 도구이다. 이와 비슷하게 CsvView[13]는 DatCon을 통해 추출된 CSV 파일이나 암호화되어진 비행기록을 입력으로 받아 드론 비행기록을 시각적으로 쉽게 파악할 수 있는 도구이다. 또한 [8]에서 제시하고 있는 내용을 참조하면, Autopsy[14]나 Cellebrite[15] 포렌식 도구를 통해서도 복호화하여 비행기록을 확인할 수 있다. 이러한 도구들 외에도 DJI와 협약하여 비행기록의 단편적인 정보를 확인할 수 있는 드론 비행기록 관리 사이트 Airdata[16], Phantomhelp[17]를 통해서도 복호화가 가능하지만, 이러한 사이트를 통한 확인은 조종사에게 충돌 방지 정보 혹은 관리적인 측면에서의 정보 제공 목적이 크기 때문에 포렌식 분석적으론 다소 한계점이 있다[6]. [18]의 저자들은 DatCon과 CsvView 두 가지 도구에서 얻을 수 있는 포렌식 아티팩트들을 비교한 결과를 제시하고 드론 포렌식 절차를 자동화할 수 있는 기계학습의 중요성을 언급하였다. 또한 [19]의 저자들은 DFLER 이름의 비행기록 엔티티를 이용한 비행 기록 분석 도구를 제안했다. 마지막으로 Clark 등의 저자는[20] DatCon 도구를 역공학을 통해 분석하여 Phantom3 드론의 내부 SD카드에 존재하는 비행기록 파일 .DAT 파일의 구조를 제시하고 비행기록 암호화 알고리즘을 분석하였다. 또한 DatCon의 기능을 발전시킨 DROP(DRone Opensource Parser) 도구를 제안하였다. 하지만 DROP은 Phantom3 드론에서만 동작한다는 한계점이 있다. 그리고 저자들은 내부 SD카드에 대한 몇 가지의 실험 결과를 제시하였는데 첫 번째로 드론을 동작할 때마다 비행기록을 하나씩 기록한다는 사실과 두 번째로 내부 SD카드의 용량 문제로 삭제되는 비행기록은 제일 오래된 비행기록부터 삭제가 된다는 사실이다. 세 번째로 삭제된 비행기록은 단순히 삭제된 것이 아니라 드라이브 공간 자체가 “00” 값으로 채워지기 때문에 모든 복구 가능성이 사라졌다는 사실이다. 본 논문에서는 검증을 위해서 실제로 Phantom3 드론의 내부 SD카드의 비행기록 실험을 진행하였으며, 그 결과 삭제된 비행기록 파일의 메타데이터 뿐만 아니라 데이터 영역이 모두 “00” 값으로 채워짐을 확인하였다. 하지만 실험을 통해 Phantom4 모델에서는 삭제된 비행기록의 데이터가 “00” 값으로 채워지지 않고 잔존하는 특징을 발견하였으며 이는 Phantom 4에서는 삭제된 비행기록 파일의 복구 가능성이 존재한다. 또한 드론 모델마다 비행기록의 복구 가능성의 존재 여부가 다를 수도 있음을 암시한다. 하지만 현재까지 드론에서 삭제된 비행기록 파일의 복구에 관해 확인된 연구는 없었으며 DJI 드론의 비행기록을 활용한 MD-Drone[26], 확장 DROP[27] 등의 디지털 포렌식 도구가 지속적으로 제안되어지고 있음에 따라 불법 촬영, 불법 행위 등의 분석에 필요한 아티팩트로써 중요도는 날로 증가하고 있다. 따라서 본 연구를 통한 삭제된 비행기록 파일 복구는 다양한 산업, 분야에 매우 중요한 기여가 될 것을 기대한다.

III. 삭제된 비행기록 파일 특징 분석

예시로 비행기록 파일은 Fig. 1과 Fig. 2와 같이 Phantom3 Standard 드론 모델과 Phantom4 Standard 모델의 비행 제어 보드에 위치한 SD 카드에서 추출 가능하다[21].

두 드론의 비행기록 파일을 저장하는 SD 카드는 FAT32 파일 시스템을 사용하였다. 또한 우리는 비행기록이 할당되는 방식과 삭제되는 방식을 검증하기 위해 각 드론을 수 차례 비행을 한 뒤, 각 비행마다 내부 SD카드를 추출하여 FTK Imager[22] 도구를 사용하여 이미징을 진행하였다. 따라서 본 3장에서는 드론 모델별 삭제된 비행기록 파일이 갖는 3가지 유형을 제시하고 각 유형에 해당하는 드론 모델인 Phantom 3 모델, 4모델, Mini 2 모델을 선정하여 특징을 검증하였다. 또한 각 유형의 공통점과 차이점을 제시하고 기존의 FAT32 파일 시스템에서 동작하는 삭제 방식과 DJI 드론에서의 삭제 방식의

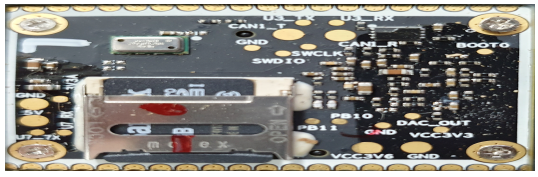


Fig. 1. Phantom3 Internal SD Card

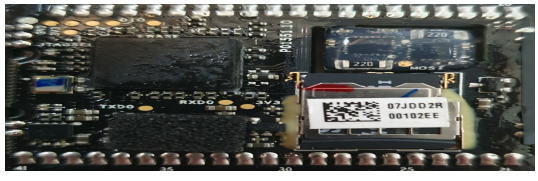


Fig. 2. Phantom4 Internal SD Card

차이점을 보여준다.

3.1 드론 모델별 삭제 파일 특징 분석

FAT32 파일 시스템에서 삭제된 파일은 비할당 영역에 파일의 콘텐츠가 남는 특징이 있다. 포렌식 수사관은 콘텐츠가 남아있는 특징을 이용하여 파일 카빙 기법 등을 이용해 파일 복구가 가능하다[23]. 이때 비행기록 파일 복구 가능성 관점에 따라 우리는 DJI 드론을 3가지 유형으로 나누었다. 분석에 사용된 드론 모델은 총 15개이며 각 특징이 나타나는 드론 모델은 Table 1과 같다. 먼저 Type Ⅰ은 삭제된 파일의 콘텐츠가 비할당 영역에도 그대로 잔존하는 특징을 가진 드론이다. Type Ⅱ는 삭제된 파일의 콘텐츠가 모두 "00" 값으로 채워지는 특징을 지닌 드론이다. 마지막 Type Ⅲ는 내부 SD 카드가 드론에 존재하지 않거나 내부 SD 카드에 비행기록 파일이 할당되지 않는 특징을 가진 드론들이다.

모든 드론에 대한 실험을 진행하는 것은 연구적으로 한계가 있어, 각 유형을 대표하는 드론 모델을 선정하여 검증하였다. Type Ⅰ의 드론은 Phantom4 Std 모델, Type Ⅱ의 드론은 Phantom3 Std 모델, Type Ⅲ 드론으론 Mini2 드론을 선정하였다. 동시에 Mini2 드론을 분해하였지만 내부 SD 카드가 존재하지 않았으며 이와 마찬가지인 Type Ⅲ 드론들은 결과적으로 내부 SD카드를 대상으로 비행기록 파일이 존재하지 않았기 때문에 복구 가능성과는 무관하다.

3.2 Phantom3 비행기록 할당 및 삭제 방식

Phantom3를 비롯한 DJI의 다른 드론 모델들에서도 비행기록은 "FLY###.DAT" 파일 명으로 저장된다. 즉, 드론의 첫 비행 시 FLY 000.DAT부터 시작하여 FLY 001, FLY 002 순서로 저장된다. 삭제될 경우는 제일 오래된 파일인 FLY 000.DAT 파일부터 삭제가 된다. 이때 삭제 없이 새로운 비행기록 파일만 할당되는 경우가 있고, 삭제와 할당이 함께 이뤄지는 경우 두 가지가 존재한다. 우선 새로운 파일이 기록되는 파일 할당 과정을 살펴보면, 드론의 전원이 켜질 때 비행기록 할당을 위해 드론 내부 SD카드에 존재하던 비할당 영역(Unallocated Space)의 클러스터 영역 중 제일 낮은 번지수부터 데이터를 기록하기 시작한다. 하지만 드론을 오랜시간 비행하여 비행기록 파일의 크기가 기존의 남아있던 비할당 영역의 연속된 클러스트 영역의 크기를 넘긴다면, 이때 파일의 단편화가 이루어지며 다음의 비할당 클러스트 영역에 데이터가 할당된다. 이때 삭제되는 파일이 없이 비행이 종료된다면 파일의 할당 과정은 여기서 멈춘다.

하지만 용량 문제로 파일의 할당 과정 진행 중 삭제되어야 하는 파일이 발생하는 경우가 있다. 이때의 경우 파일의 할당 과정은 동일하게 진행되며 이는 Pal, A 등[23]에서 설명하는 FAT32 파일 시스템에서의 데이터 할당 과정과 동일하다. 하지만 삭제 방식에서 차이점을 보인다. Phantom3에서 삭제된 비행기록의 처리되는 특징은 Fig.3와 같다.

Fig 3 그림을 보게되면, 내부에 위치한 SD 카드에 "FLY161.DAT"부터 "FLY182.DAT"까지 있다고 가정한다. 비행을 시작하기 전 "FLY161.DAT"라는 이름을 가진 비행기록은 파일의 콘텐츠가 실제로 저장되는 클러스터 영역과 해당 파일을 관리하기 위한 메타데이터 영역으로 구분된다. 또한 FAT32 파일 시스템의 파일을 관리하는 메타데이터인 디렉터리 엔트리(Directroy Entry)는 파일의 시작 위치, 파일 크기, 파일의 이름 등의 정보를 갖고 있어 파일 복구에 중요한 역할을 한다[24]. 이때, FAT32 파

Table 1. Type classification of DJI Drones

	Type Ⅰ		Type Ⅱ	Type Ⅲ	
Drone Model	Phantom4 Std	Inspire2	Phantom3 Std	Mini2	Mavic2 Pro
	Phantom4 Pro	Matrice 210	Matrice 600	Spark	Mavic2 Zoom
	Phantom4 Pro+	Mavic Pro		Mavic Air	
	Agras MG-1S			Mavic2 EnterPrise	

Type Ⅰ : The contents of a deleted file remained in unallocated space
Type Ⅱ : The contents of a deleted file do not remain in unallocated space
Type Ⅲ : No existing internal SD card or Flight record did not store in SD card

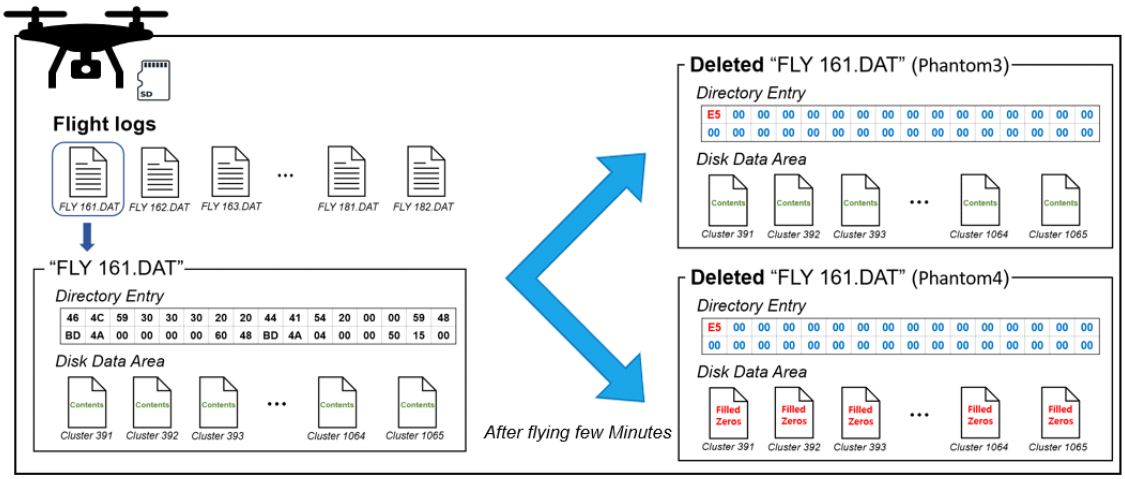


Fig. 3. Phantom3 and Phantom4 Flight Records Deletion Procedure

일 시스템에서 파일이 삭제되는 경우엔 디렉터리 엔트리의 첫 바이트만 "E5" 값으로 변경되고 기존의 값은 유지된다. 또한 파일의 콘텐츠를 저장되는 클러스트 영역은 비할당 영역으로 변경되지만 기존의 내용들은 삭제되지 않고 잔존하게 되어 파일 카빙 등의 방법을 통해 복구가 가능하다[23][25]. 하지만 Fig. 3에서 Phantom3의 삭제된 "FLY161.DAT" 비행기록의 디렉터리 엔트리의 첫 바이트는 "E5"로 정상적으로 변경되었지만 그 외의 디렉터리 엔트리 값들은 "00" 값으로 덮여 쓰이기 때문에 디렉터리 엔트리를 참조한 파일 복구는 불가능하다. 그리고 파일의 콘텐츠가 저장되어진 클러스트 영역 또한 모두 "00" 값으로 덮어 쓰이기 때문에 파일 카빙을 이용한 복구 또한 어려워진다. 결과적으로 팬텀 3에서 삭제된 비행기록 파일은 저장소 내부에서 완전히 사라지게 된다.

3.3 Phantom4 비행기록 할당 및 삭제 방식

Phantom4 드론 또한 3 모델과 마찬가지로 내부 SD 카드에 비행기록이 "FLY###.DAT" 이름 형식으로 저장되며, 삭제 순서 또한 오래된 비행기록부터 삭제된다. 또한 새로운 비행기록이 쓰여질 때, 할당되는 방식 또한 Phantom3와 마찬가지로 내부 SD 카드에 비할당 영역으로 존재하던 클러스트 영역 중 제일 낮은 번지수의 클러스트부터 데이터가 쓰여지기 시작한다. 하지만 이때 새로운 비행기록이 할당되는 방식은 Phantom3와 동일하였지만 삭제되는 특징에서 큰 차이점이 존재한다.

마찬가지로 Fig 3는 Phantom4 드론에서 비행기록이 삭제되는 특징이며 내부 SD 카드에 위치한 비행기록이 "FLY161.DAT"부터 "FLY182.DAT"까지 있다고 가정한다. 이때 Phantom4에서도 161번 비행기록이 삭제될 때 파일의 디렉터리 엔트리의 첫 바이트가 "E5"로 변경된다. 또한 나머지 값들도 "00" 값으로 덮어 쓰여진다. 하지만 Phantom 3와는 다르게 161번 비행기록 파일의 콘텐츠를 저장하는 클러스트 영역은 "00" 값으로 덮어 쓰이지 않고 그대로 잔존하게된 채, 비할당 영역으로 변경된다. 이때 삭제된 비행기록을 관리하는 메타데이터는 덮어 쓰였기 때문에 디렉터리 엔트리를 이용한 파일 복구는 3 모델과 마찬가지로 어렵지만, 콘텐츠가 잔존하는 특징을 이용하여 파일 카빙 기법을 이용한 비행기록 파일 복구 가능성이 존재하게 된다.

3.4 파일 카빙을 위한 비행기록 특징 파악

파일 카빙 기법은 파일 구조와 콘텐츠를 이용하여 파일을 복구하는 기법으로서 비할당 영역에서 파일을 복구하는데 가장 많이 사용되는 방법이다[23]. 대표적으로 파일의 헤더와 푸터를 이용하여 파일의 시작과 끝을 지정하여 파일을 복구하는 방법이 있다. 본 논문에서는 파일 카빙을 이용하기 위해 3.4.1~3 절에 해당하는 세 가지 절차를 분석하였다.

3.4.1 Phantom4 드론 비행기록 파일 분석

Phantom4 드론의 비행기록 파일의 분석을 위해 FTK Imager 도구와 HxD 도구를 이용하였다. Clark 등[20] 저자들이 언급한대로 Phantom 3모델처럼 4모델 마찬가지로 BUILD 지시자가 포함된 헤더로 비행기록 파일이 시작된다.

이때 3모델과 4모델에서 각각 펌웨어 버전 3가지에서 100개 정도의 비행기록을 분석한 결과, 비행기록 파일이 저장된 첫 번째 섹터의 첫 16Bytes 값은 Fig 4와 같이 항상 동일한 값을 갖는다. 또한 VTO Labs에서 제공하는 드론 포렌식 데이터 셋을 통해 비교 검증한 결과, 비행기록의 첫 16Byte 값은 드론 모델에 종속적인 특징을 갖고 있었다. 이를 통해 DJI 드론이 기록하는 비행기록 파일의 첫 16 Bytes 값은 모델에 종속적이며 동일한 모델은 동일한 시그니처인 16Bytes 값을 갖는 특징이 있다.

또한 파일의 끝을 나타내는 푸터 시그니처는 따로 존재하지 않았지만, 공통적으로 비행기록 파일의 마지막 클러스트 영역에서 남은 영역의 헥사 값이 Fig 5와 같이 항상 "FF" 값으로 채워졌으며, 이는 3만 Byte 이상의 길이를 가지고 있었다. 이를 통해 비행기록의 첫 시그니처가 항상 동일한 값으로 시작되는 특징과 비행기록 파일의 끝은 항상 "FF" 값으로 마무리 된다는 특징을 이용하여 본 논문에서는 파일 카빙 기법을 적용했으며 이는 4장 실험을 통해 복구 정도를 분석한 결과를 보여준다.

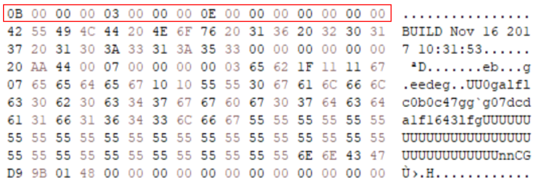


Fig. 4. Phantom4 Flight Log's Header

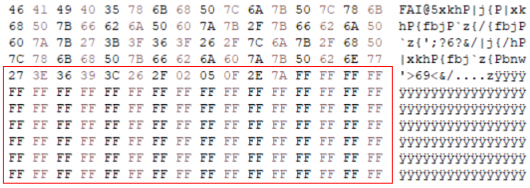


Fig. 5. Phantom4 Flight Log's Footer

3.4.2 DJI 드론의 비행기록 시그니처 분석

DJI의 드론의 비행기록 헤더의 첫 16 Bytes가 항상 동일하다는 특징을 이용하여 삭제된 비행기록의 복구가 가능하다. Table. 2는 9가지 드론 모델의 비행기록 파일의 첫 16 Bytes를 분석한 결과이다.

3.4.3 복호화 도구를 통한 시그니처 검증

각 드론 모델의 비행기록 헤더의 첫 16 Bytes 값은 드론 모델에 종속적인 특징을 검증하기 위해 DatCon과 CsvView 두 도구를 통해 16Bytes 값의 역할을 알아보았다. 정상적인 비행기록 파일의 첫 16Bytes 값을 다른 드론 모델의 16Bytes 값으로 변조한 뒤 출력되는 드론 모델 명을 확인하여 검증하였다. 예를 들어, 정상적인 Phantom4 Std 비행기록 파일의 처음 16Bytes를 Phantom4 Pro 비행기록 파일의 16Bytes 값으로 변조한 뒤, 복호화를 진행하여 결과를 지켜보았다. 먼저 변조되지 않은 Phantom4 Std의 비행기록을 복호화하면 두 도구는 모두 마찬가지로 Phantom4 Std 모델의 비행

Table 2. DJI Drone's First 16bytes of Flight Log Header

Drone Model	The first 16 bytes of the header
Phantom3 Std	06 00 00 00 03 00 00 00 09 00 00 00 00 00 00 00
Phantom4 Std	0B 00 00 00 03 00 00 00 0E 00 00 00 00 00 00 00
Phantom4 Pro	12 00 00 00 03 00 00 00 15 00 00 00 00 00 00 00
Phantom4 Pro+	24 00 00 00 03 00 00 00 27 00 00 00 00 00 00 00
Matrice 210	19 00 00 00 03 00 00 00 1C 00 00 00 00 00 00 00
Matrice 600	17 00 00 00 03 00 00 00 1A 00 00 00 00 00 00 00
Agras MG-1S	0A 00 00 00 03 00 00 00 0D 00 00 00 00 00 00 00
Mavic Pro	10 00 00 00 03 00 00 00 13 00 00 00 00 00 00 00
Inspire 2	11 00 00 00 03 00 00 00 14 00 00 00 00 00 00 00

기록으로 모델 명을 출력한다. 하지만 변조된 값을 넣은 비행기록의 복호화를 진행하면 Phantom4 Std가 아닌 Phantom4 Pro 모델 명을 갖는 비행기록 결과를 출력한다. 마찬가지로써, Table. 1에서 보여주는 8 가지 드론 모델들의 16Bytes 값을 Phantom4 Std 모델의 헤더에 변조한 결과 8개 드론 모두 변조한 드론의 모델명으로 결과를 출력하였다. 즉, 비행기록 파일의 첫 16Bytes를 이용하여 DatCon과 CsvView 도구는 입력으로 받은 비행기록 파일의 드론 모델에 종속적인 특징이 있음을 알 수 있다.

IV. 실험 및 결과

4.1 복구 정도 분석

삭제된 비행기록 파일의 복구 정도를 알아보기 위해 Phantom4 Standard 드론을 5분에서 10분 사이의 비행을 10번 진행한 뒤, 각 비행마다 내부 SD 카드를 추출하여 이미징을 진행하여 결과를 분석하였다. 드론은 4GB의 SD 카드를 사용하며, 각 이미징 데이터의 비할당 영역에서 비행기록을 복구한 뒤 원본 파일과 복구한 비행기록 파일의 해시 값 검사를 통해 무결성을 확인하였다. 또한 삭제된 비행기록 개수와 복구한 비행기록 개수 분석을 비교하여 복구 정도를 파악하였다. Table. 3.를 보게되면 Flight Recrods 필드는 각 비행에서 발견된 총 비행기록 개수이며 Deleted Flight Records 필드는 직전에 비행한 데이터와 비교하여 삭제되어진 비행기록의 개수이다. 그리고 Found Flight Record 필드는 비행기록의 시그니처 검색을 통해 발견된 과거의 삭제된 비행기록의 개수이다. 마지막 필드는 각 비행의 비할당 영역 크기를 보여준다. 실험 결과를 분석하자면 첫 번째로 드론은 일정 크기 이상의 비할당 영역 공간을 유지하는 것을 알 수 있다. 본 실험에선 비할당 영역의 최저 크기는 약 504.34 MB이며 최대 크기는 약 738.34 MB였다. 앞서 언급한 삭제된 비행기록 파일이 비할당 영역으로 변경되는 특징과 드론 내부 SD 카드에서 일정 크기 이상의 비할당 영역이 유지되는 특징을 이용하여 불법적으로 사용된 드론의 내부 SD카드에서 추가적인 범죄 증거를 발견하거나 보충 증거가 될 수 있는 파일의 발견 가능성이 높다. 두 번째로는 비행기록이 삭제된 경우 대부분 비할당 영역에서 파일을 복구할 수 있었지만, 2번 비행과 같이 삭제된 비행기록이 있었음에도 비할당 영역에선 삭제된 기록이 발견되지 않은 경우가 존재하여 복구가 불가능했던 경우도 존재하였다. 이는 삭제된 비행기록 파일의 콘텐츠가 저장된 클러스터 영역에 새로운 비행기록 파일의 콘텐츠로 덮어 쓰였기 때문이다. 이렇게 10번의 비행 중 최저 0개에서 최고 3개의 비행기록 파일을 복구할 수 있었다. 세 번째로는 삭제된 비행기록 파일은 직전에 비행한 비행기록 파일만 발견된 것이 아닌, 더 이전에 비행한 비행기록 파일이더라도 데이터가 덮어 쓰이지만 않았다면 원본 비행기록 파일과 동일한 해시 값을 가진 비행기록 파일을 복구할 수 있었다. 마지막 네 번째로는 Phantom4 Standard 모델은 4GB의 내부 SD 카드를 사용하지만 Phantom4 Pro 모델과 Pro + 모델은 8GB의 내부 SD카드를 사용한다. 또한 Pro 모델의 비할당 영역에선 28개의 삭제된 비행기록을

Table 3. Flight Test

Flight Count (File Number)	Flight Records	Deleted Flight Records	Found Flight Record in unallocated space	Size of Unallocated Space
1 (146 ~ 176)	31	-	-	-
2 (147 ~ 177)	31	1	0	529.81 MB
3 (149 ~ 178)	30	2	2	711.68 MB
4 (149 ~ 179)	31	0	2	626.06 MB
5 (150 ~ 180)	31	1	1	738.34 MB
6 (150 ~ 181)	32	0	1	628.96 MB
7 (151 ~ 182)	32	1	1	551.09 MB
8 (152 ~ 183)	32	1	2	629.78 MB
9 (153 ~ 184)	32	1	3	504.34 MB
10 (154 ~ 185)	32	1	1	545.71 MB

발견할 수 있었다. 이렇듯 더 높은 용량의 내부 SD 카드를 제공하는 드론 모델에선 더 많은 비행기록 파일을 복구할 가능성이 존재한다.

4.2 내부 SD카드 테스트

Phantom 3모델과 4모델의 내부 SD 카드는 기본적으로 FAT32 파일 시스템을 사용하며 클러스터 당 64개의 섹터, 섹터 당 512 Bytes로 포맷된다. 우리는 DJI만의 정해진 환경에 따라 비행기록 파일을 처리하는지 검증을 위해 SD카드 실험을 진행하였다. 드론 모델마다 혹은 SD 카드의 포맷에 따라 상이한 방법으로 데이터를 처리하는지 검증을 위해 실험하였으며 우선 FAT16, NTFS로 포맷된 SD 카드 두 종류를 각 드론에 삽입하고 비행을 하였다. 그 결과 3모델과 4모델 모두 서로 다르게 포맷된 SD 카드가 FAT32 파일시스템, 클러스터 당 섹터 수, 섹터 크기 등 기존과 동일한 포맷으로 드론에서 자체적으로 재포맷이 되었으며 FLY000.DAT부터 새롭게 비행기록 파일을 할당하기 시작했다. 삭제되는 방식 및 특징 또한 3장에서 제시한 특징과 동일하였다. 본 실험은 팬텀3와 팬텀4에서 한정적으로 진행되었으며, Table. 1의 Type Ⅲ 드론을 제외한 총 9 가지 드론 모델의 내부 SD 카드 환경을 포렌식 분석을 하였다. 그 결과 모두 동일한 FAT32 파일 시스템을 사용하고 있었으며, 클러스트 당 64개의 섹터, 섹터 당 512 Bytes 크기를 갖는 동일한 특징을 확인하였다. 이를 통해 9개 드론의 내부 SD 카드는 모두 동일한 환경을 갖고 있음을 확인하였고 팬텀3와 팬텀4의 내부 SD카드 실험 결과처럼 다른 드론 모델들 또한 FAT32 파일 시스템 환경에서만 동작할 것임을 유추할 수 있다.

4.3 비행기록 파일 복구 가능성에 따른 드론 분류

본 논문에서는 비행기록 파일 복구 가능성의 존재 여부 관점에 따라 15개의 드론 모델에 대하여 공통적으로 적용할 수 있는 3 가지 특징을 제시하였다. 이때 각각의 특징에 해당하는 드론을 선정하여 특징을 자세하게 검증하였다. 사례 연구 중 Phantom3 Standard 모델과 Phantom4 Standard 모델을 사용하였으며 두 드론의 내부 SD 카드에서 비행기록 파일의 삭제 방식과 특징을 분석하였다. 이때 발생하는 특징의 차이점인 비할당 영역에 데이터가 잔존하는 차이점을 통해 파일 카빙 기법을 이용한 비행기록 복구를 보였다. 결과적으로 DJI 드론은 비행기록 파일의 삭제될 때, Phantom3 드론과 같이 비할당 영역에 비행기록 콘텐츠가 잔존하지 않는 드론과

Table 4. Classification of drones according to recoverability

Type	Description	Drone Model
Type Ⅰ	Exist chance for recovery flight logs	Inspire 2 Mavic Pro Matrice 210 Agras MG-1S Phantom4 Standard Phantom4 Professional Phantom4 Professional +
Type Ⅱ	No chance for recovery flight logs	Phantom3 Standard Matrice 600
Type Ⅲ	No existing internal SD card or Flight record did not store in SD card	Mavic 2 enterprise Mavic 2 Pro Mavic 2 Zoom Mavic Air Mini 2 Spark

Phantom4 드론과 같이 콘텐츠가 잔존하는 드론으로 특징의 분류가 가능하다. Table. 4는 앞서 제시한 Table. 1의 3 가지 유형에 맞게 DJI 드론을 3 가지 Type으로 분류하였다. Type Ⅰ은 드론 내부에 비행기록 파일이 존재하며 마찬가지로 복구 가능성 또한 존재하는 드론이며, Type Ⅱ는 드론 내부에 비행기록 파일이 존재하지만 복구 가능성은 존재하지 않는 드론이다. 마지막 Type Ⅲ는 Mini2나 Spark 모델과 같이 내부 SD카드가 존재하지 않는 드론이거나, Mavic 2 Pro와 같이 내부 SD카드에 사진과 같은 미디어 데이터만 저장되고 비행기록 파일은 존재하지 않는 경우이다. 또한 Phantom3 계열의 Adv 모델이나 Pro 모델도 Std 모델과 마찬가지로 복구 가능성이 존재하지 않을 것으로 추측되지만 데이터 셋을 구하지 못하여 본 연구를 통해서는 분석하지 못하였다.

V. 결 론

본 연구에서는 드론의 비행기록 파일이 삭제되는 특징을 비할당 영역에 데이터가 잔존하는 여부에 따라 2 가지 제시하였다. 또한 15 가지 드론 모델에서 복구 가능성을 분석한 결과, 3 가지 Type으로 분류할 수 있었으며 이때, Type Ⅰ의 드론에서 비행기록 파일의 복구 가능성이 존재하였다.

또한 Type Ⅰ,Ⅱ에 해당하는 9 가지의 드론 모델의 내부 SD카드는 모두 동일한 FAT32 파일 시스템의 환경을 가지고 있었다.

최종적으로 본 논문에선 드론 모델별 비행기록 복구 가능성이 존재하는 드론을 제시하였으며 이는 학문적인 영역을 넘어서 다양한 산업, 분야에 있어 예방, 보안, 사고대응 등 다양하게 발생하는 문제점들에 충분한 기여가 될 것을 기대한다.

하지만 연구를 진행하며 비행기록이 삭제될 때 발생하는 특징의 차이점에 있어서 원인을 파악하는 것에 한계가 있었다. 그 이유로는, DJI는 기본적으로 비행기록과 관련된 정보를 전혀 공개하지 않고 있으며 펌웨어와 같은 시스템 정보 또한 공개하지 않고 있다. 마찬가지로 드론 펌웨어를 이용하여 그 차이점을 분석하기에도 한계가 있었으며 에뮬레이터와 같은 분석 환경도 제공되지 않기 때문이다.

향후 연구에서는 분석한 드론 모델 이외의 다른 모델에 대한 연구가 필요하다. 또 다른 드론 모델에선 삭제된 비행기록이 갖는 특징이 다를 수도 있기 때문에 그에 따른 비행기록 복구 방법에 대한 연구가 진행될 필요가 있다.

References

[1] UAS Sightings Report, “FAA”, https://www.faa.gov/uas/resources/public_records/uas_sightings_report, Jan 2023

[2] U. Jain, M. Rogers and E. T. Matson, ″Drone forensics framework: Sensor and data identification and verification,″ IEEE Sensors Applications Symposium (SAS), pp. 1-6, March. 2017

[3] Al-Dhaqm, Arafat, et al. ″Research challenges and opportunities in drone forensics models.″ Electronics, vol. 10, no. 13, June 2021

[4] VTO Labs, “Drone Datasets Forensic”, https://www.vtolabs.com/drone-forensics , June 2023

[5] DJI Drones Market. “Drone Market”, https://view.asiae.co.kr/article/2023020907151774288, June 2023

[6] Y. Lee, J. Kim, J. Yu and Yun, J., “Classification of DJI Drones Based on Flight Log Decryption Method”, Journal of The Korea Institute of Information Security & Cryptology, 32(1), Feb 2022

[7] Stanković,M.,Mirza, M. M.,Karabiyik, U. “UAV forensics: DJI mini 2 case study” Drones, Vol 5, no.2, June 2021

[8] Salamh, F. E., Mirza, M. M., Karabiyik, U., “UAV forensic analysis and software tools assessment: DJI Phantom 4 and Matrice 210 as case studies”, Electronics, Vol 10, no. 6, March 2021

[9] Iqbal, F.; Alam, S.; Kazim, A.; MacDermott, Á.; Hamdi, D.A., “Drone forensics: A case study on DJI phantom 4”, In Proceedings of the 2019 IEEE/ACS 16th International

Conference on Computer Systems and Applications (AICCSA), pp. 1-6 Nov 2019

[10] Kao, Da-Yu, et al. "Drone forensic investigation: DJI spark drone as a case study." Procedia Computer Science,Vol.159,pp.1890-1899,Sep 2019

[11] Yousef, Maryam, and Farkhund Iqbal. "Drone forensics: A case study on a DJI Mavic Air." 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, pp.1-3, Nov 2019

[12] DatCon Tool Documentation, "DatCon" https://datfile.net/DatCon/intro.html, June 2023

[13] CsvView Documentation, "CsvView" https://datfile.net/CsvView/intro.html, June 2023

[14] Autopsy Forensic Tool, "Autopsy", https://www.basistech.com/autopsy/, June 2023

[15] Cellebrite Forensic Tool, "Cellebrite", https://cellebrite.com/en/home/, June 2023

[16] Airdata UAV Flight Record, "Airdata", https://app.airdata.com/, June 2023

[17] Phantom Help, "Phantom Help", https://www.phantomhelp.com/getting-started/, June 2023

[18] Mohammed, Abdul Sami, et al. "A Comparative Study of Drone Forensic Tools and Techniques." International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 752-758, Jan 2023

[19] Silalahi, et. al. "DFLER: Drone Flight Log Entity Recognizer to support forensic investigation on drone device." Software Impacts, Vol. 15, Mar 2023

[20] Clark, D. R., Meffert, C., Baggili, I., and Breitinger, F. "DROP (DRone Opensource Parser) your drone: Forensic analysis of the DJI Phantom III" Digital Investigation, Vol. 22, pp. 3-14, Aug 2017

[21] dji-firmware-tools, "DJI Hardware" https://github.com/o-gs/dji-firmware-tools/wiki/DJI-Hardware, June 2023

[22] FTK Imager. "FTK Imager Forensic" https://www.exterro.com/ftk-imager, June 2023

[23] Pal, Anandabrata, and Nasir Memon. "The evolution of file carving." IEEE signal processing magazine, Vol. 26, No. 2, pp. 59-71, March 2009

[24] Lee, Seokjun, and Taeshik Shon. "Improved deleted file recovery technique for Ext2/3 filesystem." The Journal of Supercomputing, Vol. 70, No. 1, pp. 20-30, Sep 2014

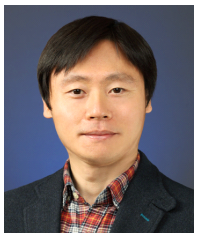
[25] Povar, Digambar, and V. K. Bhadran, "Forensic data carving." Digital Forensics and Cyber Crime: Second International, Vol. 53, pp. 137-148, Oct 2011.

[26] MD-Drone Tool. "Forensic Tool Drone" ,https://www.gmdsoft.com/product/digital-forensics-software/ , June 2023

[27] Latzo, Tobias, et al. "Maraudrone's Map: An Interactive Web Application for Forensic Analysis and Visualization of DJI Drone Log Data." Nordic Conference on Secure IT Systems, pp. 329-345, Jan 2022.

〈저 자 소 개〉

윤 여 훈 (YeoHoon Yoon) 학생회원
2022년 2월: 대전대학교 컴퓨터공학과 졸업
2022년 3월~현재:세종대학교 일반대학원 정보보호학과, 지능형 드론 융합전공 석사과정
〈관심분야〉 정보보호, 드론 포렌식



윤 주 범 (Joobeom Yun) 종신회원
1999년 2월: 고려대학교 컴퓨터학과 학사
2001년 2월: 서울대학교 컴퓨터공학과 석사
2012년 2월: KAIST 전산학과 박사
2001년 3월~2015년 2월: ETRI부설연구소 선임연구원
2015년 3월~현재: 세종대학교 정보보호학과, 지능형 드론 융합전공 부교수
〈관심분야〉 네트워크 보안, 시스템 보안, 인공지능 보안