Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.1, Feb. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.1.77

비행 로그 복호화 방식에 따른 DJI 드론 분류*

이 영 우,[1†] 김 주 환,[1] 유 지 현,[1] 윤 주 범[2‡]
[1,2]세종대학교 (대학원생, 교수)

Classification of DJI Drones Based on Flight Log Decryption Method*

Youngwoo Lee,[1†] Juhwan Kim,[1] Jihyeon Yu,[1] Joobeom Yun[2‡]
[1,2]Sejong University (Graduate student, Professor)

요 약

드론(Drone)의 제작기술이 발전하고 대중화되면서 주로 산업, 농업, 군사 등에 치우쳐 있던 드론 시장은 개인·상업 시장에서도 큰 성장세를 보인다. 그중에서 DJI는 개인·상업용 드론 시장에 높은 점유율을 보이고, 이에 따라 DJI 드론의 포렌식 분석이 주목받고 있다. 특히, 범죄행위에 사용된 드론을 탈취·획득하여 분석할 때, 드론의 비행 경로 및 하드웨어 정보를 기록한 비행 로그를 해석하는 기술이 필요하고, 이는 DJI의 드론 모델마다 복호화 방식의 차이로 인해 드론 모델별로 다르게 적용할 수밖에 없다. 따라서, 디지털 포렌식 조사관의 관점에서 불상의 드론을 획득하였을 때, 분석할 수 있는 드론 모델에 대한 명확한 분류가 필요하다. 본 논문에서는 포렌식을 통해 DJI 드론의 아티팩트를 추출하여 분석하는 방법을 제안하고, DJI의 출시 연월이 다른 세 가지 드론 모델에 대해서 미디어 데이터의 분석 및 비행 로그 분석 결과와 복호화 방식에 대해서 분석한다. 마지막으로, 상용화된 DJI 드론 비행 로그의 복호화 여부에 따라 DJI 제품군의 드론을 분류한다.

ABSTRACT

With the development and popularization of drone manufacturing technology, the drone market, which was mainly focused on industry, agriculture, and military, is also showing great growth in individual and commercial markets. Among them, DJI has a high share in the personal and commercial drone market, and accordingly, forensic analysis of DJI drones is drawing attention. In particular, when stealing and analyzing drones used in criminal acts, a technology to interpret flight logs recording drone flight paths and hardware information is needed, which inevitably applies drone models due to differences in decryption methods. Therefore, when an unidentified drone is acquired from the perspective of a digital forensic investigator, a clear classification of a drone model to which analysis can be applied is required. This paper proposes a method of extracting and analyzing artifacts of DJI drones through forensics, and analyzes media data analysis and flight log analysis results and decryption methods for three drone models with different release years of DJI. Finally, drones in the DJI product line are classified according to whether the commercialized DJI drone flight log is decrypted.

Keywords: DJI Drone, Forensics Analysis, Flight Logs Decryption, Classification

I. 서 론

특히 지난 10년 동안 급속한 기술의 발전으로 무인 항공기(unmanned aerial vehicle)로 불리는 드론의 시장은 급격하게 성장해왔고, 드론은 물류 관리, 시설 관리, 촬영 감독, 농업 등에 이용될 수 있

Received(12. 14. 2021), Modified(1st: 01. 07. 2022, 2nd: 02. 04. 2022), Accepted(02. 04. 2022)
* 본 연구는 한국연구재단 연구과제(NRF-2021R1F1A1051251) 지원으로 수행됨
† 주저자, dbsgh013@gmail.com
‡ 교신저자, jbyun@sejong.ac.kr(Corresponding author)

도록 발전했다. 최근에는 산업 및 공업 용도의 드론을 넘어서 개인의 취미용 드론 사용자가 기하급수적으로 늘어났고, 동시에 드론을 통한 범죄행위 또한 증가했다. 미국 연방 항공청(Federal Aviation Administration)의 보고에 의하면, 2021년 7월부터 9월까지 미국에서만 691건의 불법 행위가 보고되었다[1]. 이는 전년도 대비 약 41% 증가했으며, 드론 포렌식(drone forensics)의 필요성을 강조한다. 따라서, 포렌식 관점에서 증거 제출에 필요한 비행 로그의 분석과 비행 로그의 암호화된 내용을 해석하는 것은 필수적이다.

본 논문은 세계 드론 시장을 주도하고 있는 DJI 드론 중 250g 미만의 경량화 드론인 DJI Mavic Mini, DJI Mini 2 드론과 초기 DJI 드론 모델인 DJI Phantom 3을 범죄 시나리오를 설정하여 비행시켰다. 이를 통해 우리는 드론에서 얻을 수 있는 아티팩트의 위치와 분석 방법을 제시하였고, 각 아티팩트가 가지는 의미를 분석하였다. 우리는 더 나아가 암호화된 비행 로그에 대한 복호화 방식이 드론 모델마다 다르게 적용되는 것을 파악하였고, 이에 따라 포렌식 분석이 가능한 DJI 드론을 분류하였다.

본 논문의 구성 체계는 다음과 같다. 제1장에서는 연구의 목적 및 방향을 제시하였고, 제2장에서는 이전까지의 DJI 드론을 분석하기 위한 배경 연구를 살펴본다. 제3장에서는 국내에서 구매할 수 있는 DJI 드론의 아티팩트를 추출 및 분석하는 방법을 보여주며, 제4장에서는 3가지 DJI 드론의 분석 결과에 따라서 DJI 드론을 분류하였다. 마지막으로 제5장에서는 본 연구의 결론 및 한계점을 서술하였다.

II. 배경 연구

2.1 드론 포렌식(Drone Forensics)

드론 포렌식은 드론의 디지털 증거나 데이터를 디지털 포렌식 분석을 통해 일반적인 상태로 복구하는 것을 말한다. 여기서 드론의 범위는 카메라, 와이파이, GPS, 셀룰러 통신 등을 포함한 무선 원격 조종 장치를 의미하며, 범죄 수사에 사용되는 자료로써 드론이 촬영한 사진, 조종자 ID, 메타데이터(metadata), 비행경로 등이 증거로 활용된다[15].

디지털 포렌식 관점에서 조사관은 드론 포렌식 증거물 제출을 위해 다음과 같은 질문에 답변할 수 있어야 한다[2][16].

- Who : 드론의 소유주 또는 조종자가 누구인가?
- When : 범죄 발생 시각 및 그 밖에 관련 사건이 발생한 시각은 언제인가?
- When : 범죄 장소 또는 관련 장소의 위치가 어디인가?
- What : 범죄 사실에 관해서 설명할 수 있는가?
- Why : 분석을 통해 범죄의 동기를 알 수 있는가?
- How : 어떻게 범죄가 성립되었는가?

위의 질문에 답변하기 위해서 드론 관련 장치의 아티팩트를 모두 분석해야 하고, 각 아티팩트가 가진 의미를 파악해야 한다.

2.2 드론 아티팩트(Drone Artifact)

드론에서 얻을 수 있는 아티팩트는 무수히 많지만, 그중에서 5W1H의 질문을 만족할 수 있는 아티팩트의 유형은 총 세 가지가 있다.

첫 번째는 미디어 데이터(media data)이다. 미디어 데이터는 드론이 비행하는 도중에 촬영하는 사진과 동영상 데이터를 일컫는 말로, 이미지 파일 메타데이터 포맷인 EXIF(Exchangeable Image File Format) 정보를 포함하고 있다. 해당 EXIF 정보를 분석하면 위도, 경도, 고도 등의 GPS 정보를 획득할 수 있다[3][12].

두 번째는 PII(Personally Identifiable Information)이다. PII는 개인과 특정하게 연관이 되어있는 정보를 의미한다. 실제로 DJI Mini 2에 대해서 안드로이드 스마트폰 Galaxy S7과 iOS 스마트폰인 iPhone 7을 세 가지의 포렌식 툴(Autopsy, Cellebrite, Magnet AXIOM)을 통해 분석했을 때, 스마트폰 내부에 논리적 백업 데이터로 컨트롤러 일련번호, 비행 앱 로그인 기록, DJI 제품 모델, 드론 카메라 일련번호 등이 발견됐다[3]. 이를 통해 누가 드론을 날렸는지, 언제 드론이 비행했는지에 대해 특정할 수 있지만, 스마트폰이 없는 탈취 드론의 경우에는 신원 특정이 불가하다. 본 논문에서는 연구 범위의 한계로 인해 PII 분석은 수행하지 않는다.

세 번째는 드론의 비행 로그(flight log)이다. 비행 로그는 드론의 내부 SD카드와 스마트폰 모두 가지고 있으며[13], 탈취된 드론의 경우 Chip-off 기술을 활용하여 비행 로그를 획득할 수 있다[4]. DJI 드론의 비행 로그는 TXT, DAT, LOG 형식의 로

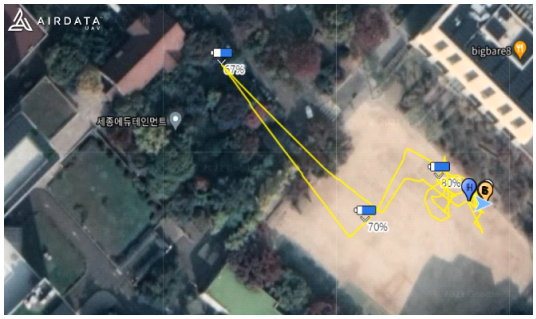


Fig. 1. The flight route of a drone using GPS in Airdata

그로 구별할 수 있으며, 각 로그의 특징은 Table 1과 같다. 세 가지 비행 로그 모두 비행시간에 대한 GPS 정보를 알 수 있으며, 연속적인 시간에 대한 GPS 좌표를 기록하면 드론의 목적지를 특정할 수 있고[14], 이는 Fig. 1.과 같이 시각화할 수 있다.

2.3 DJI 드론 포렌식 도구(DJI Drone Forensics Tools)

먼저, DJI는 드론 내부 데이터의 암호화 알고리즘을 현재까지 공개하지 않았으며, 비행 로그를 복호화하기 위해서는 DJI와 협약하여 복호화 API를 가진 Airdata[5], Phantomhelp와 같은 드론 비행 로그 관리 사이트에서 복호화가 가능하다. 하지만, 이러한 복호화 사이트에서 제공하는 정보는 오직 드론의 비행에 관한 정보만 포함하기 때문에 드론 조종사에게 충돌 방지 정보 및 드론 관리 프레임 제공의 목적이 크다. 따라서, 드론 포렌식 분석가로선 해당 정보의 범위는 다소 한정적이다. 이를 위해 복호화 API의 도움 없이 DJI 드론을 분석할 수 있는 DJI 전용 포렌식 도구는 필수적이다.

일반적으로 가장 많이 사용하는 DJI 전용 포렌식 도구는 DatCon[6]이다. 2016년 1월부터 배포된 DatCon은 DJI의 복호화 API 없이 독자적인 복호화 알고리즘을 구현하여 DAT 파일을 사람이 읽을 수 있는 CSV 파일로 변환시켜 준다. 또한, DatCon을 분석하여 만든 오픈소스 도구인 DROP (DRone Opensource Parser)의 제작자는 리버스 엔지니어링(reverse engineering)을 통해 DatCon을 분석하여 DAT 파일의 구조에 대한 포괄적인 개념을 정립하였고, DAT 파일의 암호화 알고리즘을 분석했다[7].

최근 연구에서는 DJI Phantom 4와 DJI Matrice 210 드론을 통해 가장 유명한 드론 포렌식 도구인 Datcon, Autopsy[8], Cellebrite[9]을 DJI 드론에 적용하며, 그 차이를 평가 및 강조하였다[10]. Autopsy와 Cellebrite 모두 비행 로그의 분석을 DatCon을 이용하여 진행하였고, 복호화된 Waypoint에 대해서 동일한 파일을 기준으로 동일한 결과를 도출하지 못했다. 이는 디지털 포렌식 관점에서 DatCon의 결과물이 증거 제출에 채택될 가능성이 높음을 보인다.

따라서, DJI 드론의 비행 로그 분석에 있어서 가장 중점이 되는 도구는 Datcon이며, 그 외의 도구들은 교차검증 용도로 사용하는 것이 바람직하다.

III. DJI 드론 아티팩트 분석 방법

본 논문에서는 DJI 드론의 아티팩트를 획득하는 방법부터 분석하는 과정을 제시한다. 드론의 아티팩트 획득할 수 있는 세 가지 장소와 각 장소에서 아티팩트를 얻기 위해 수행해야 하는 과정을 제시한다.

Table 1. The characteristics of DJI drone's flight log

	.TXT Log	.DAT Log	.LOG log
Location	Smartphone	Internal SD card, Smartphone	External SD card
Contents	Communication logs between drones and wireless controller	The flight log including the drone's own system log.	The latest DAT log.
Features	To include drone name, region, serial number, GPS data	Logs are recorded in more detailed time units than TXT log.	To be recorded in the case of drones without built-in SD cards.
Decryption Tool	Airdata.com	DatCon, Airdata.com,	DatCon, Airdata.com,

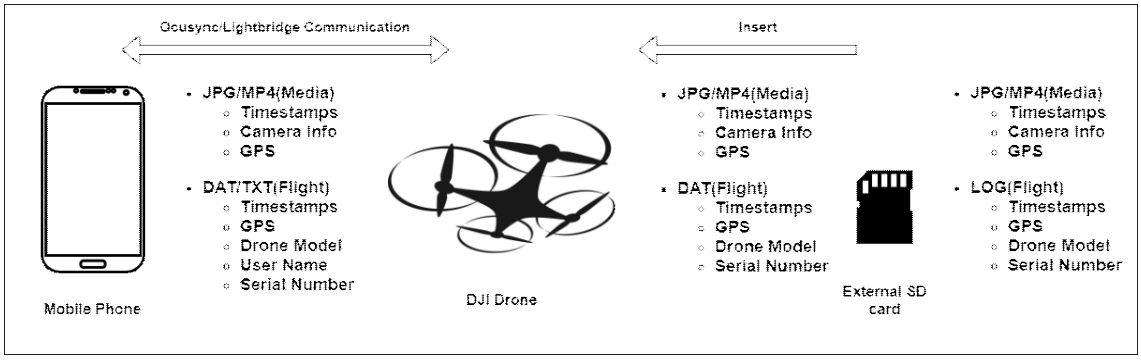


Fig. 2. Details of drone artifacts that can be obtained from mobile phone, drone, and external SD card

또한, 미디어 데이터 및 비행 로그를 분석하는 과정을 상세히 설명한다. 세 가지 장소와 얻을 수 있는 아티팩트의 전체적인 그림은 Fig. 2.와 같다.

3.1 드론 아티팩트 획득 방법

3.1.1 드론 내부 저장소(Drone Internal Storage)

본 논문은 드론 내부 저장소에서 아티팩트를 획득하는 방법은 크게 두 가지로 구분한다. 드론을 분해하지 않고 Chip-on 상태에서 데이터를 획득하는 방법과 드론의 메인 보드에서 메모리 칩을 획득하는 Chip-off 방법으로 구분된다. Chip-on 상태의 드론에서 아티팩트를 획득하기 위해선 DJI의 데스크톱 전용 애플리케이션 DJI Assistant를 사용한다. 해당 애플리케이션을 사용하면 비행 로그 및 미디어 데이터를 획득할 수 있지만 탈취된 드론을 분석하는 경우 비인증 소유자 상태에서 아티팩트를 획득하는 것은 제한된다. 이를 위해 드론을 분해하여 내부 메모리를 직접 분석하는 방법을 사용해야 하며, 이는 Fig. 3.과 같다.

DJI 드론을 분해했을 때, 탈착 가능한 SD 카드 형태의 내부 메모리를 사용하는 경우와 메인보드에 부착된 플래시 메모리를 사용하는 경우로 구분하고, 이는 Fig. 4.와 같다. SD 카드 형태의 메모리는 즉시 SD 카드 리더(e.g. Cellebrite UFED Memory Card Reader)를 통해 분석할 수 있지만 플래시 메모리의 경우 메인보드에서 제거한 후 데이터 시트에서 Read Pin의 위치를 확인해야 한다. 이는 하드웨어 분야에 전문적인 지식이 필요하며, 플래시 메모리의 이미지를 획득한 후 드론 내부 아티팩트를 획득할 수 있다.

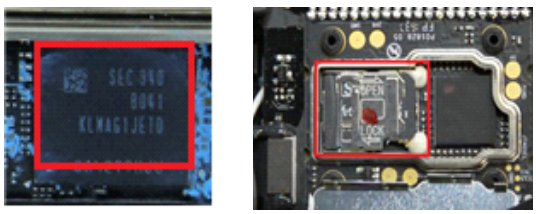


Fig. 3. On-board flash memory(left), on-board SD card(right)

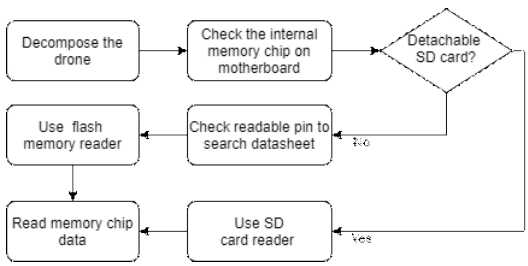


Fig. 4. Chip-off method

3.1.2 모바일 저장소(Mobile Storage)

모바일은 크게 안드로이드와 iOS로 나눌 수 있다. 일반적으로 안드로이드의 경우 ADB(Android Debug Bridge) 등의 도구를 사용해서 이미지를 획득하는 방법을 주로 사용하고 iOS의 경우 주로 아이튠즈(iTunes)를 이용하여 데이터를 획득한다.

DJI 드론의 모바일 앱의 종류에 따라서 모바일 저장소의 저장 유형은 다르다. 모바일 앱의 종류는 DJI GO, DJI GO4, DJI FLY 세 가지로 구분할 수 있다. 초기에 출시된 드론의 경우(e.g. Phantom 3) DJI GO 앱을 사용하고 최근에 출시

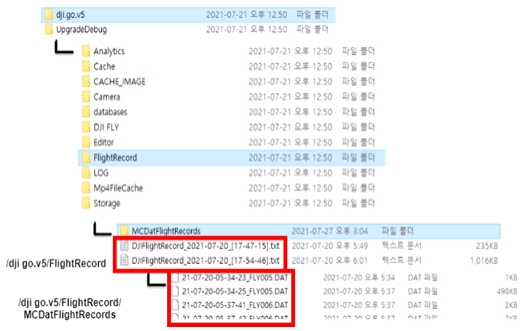


Fig. 5. The location of flight logs in DJI FLY

된 모델(e.g. DJI Mini 2)의 경우 DJI FLY 앱을 사용한다.

DJI GO의 경우 /dij.pilot/ 폴더를 루트로 사용하며 /dij.pilot/DJI_RECORD 폴더와 DJI Album 폴더에 동영상과 사진 파일을 저장한다. 또한, /dij.pilot/FlightRecord 폴더에 비행 로그를 저장한다.

DJI GO 4의 경우 /dji.go.v4/ 폴더를 루트로 사용한다. /dji.go.v4/DJI FLY/Photo와 /dji.go.v4/DJI FLY/Video 폴더에 사진과 동영상을 저장한다. 하지만 이는 축소된 이미지의 형태이며, /dji.go.v4/DJI FLY/PhotoOriginalFiles 폴더에 원본 형태의 미디어 파일이 저장되어 있다. 또한, /dji.go.v4/CACHE_IMAGE 폴더에 마찬가지로 축소된 형태의 이미지가 저장되어 있다. 한편, /dji.go.v4/FlightRecord 폴더에 TXT 형식의 비행 로그와 MCDatFlightRecord 폴더가 존재하며 해당 폴더에 DAT 형식의 비행 로그가 저장된다.

DJI FLY 앱의 경우 /dji.go.v5/ 폴더를 루트로 사용하고 각 아티팩트의 저장 위치는 DJI GO 4와 같다. 실제로 안드로이드 스마트폰의 DJI FLY 앱을 대상으로 포렌식 이미지를 획득한 후 비행 로그의 위치를 나타낸 그림은 Fig. 5.와 같다.

3.1.3 외장 SD 카드(External SD Card)

외장 SD 카드는 드론에서 촬영한 사진, 동영상, LOG 형식의 비행 로그를 저장한다. 미디어 파일은 /DCIM/100MEDIA/ 폴더에 저장되며, 비행 로그는 /MISC/LOG/flylog/ 폴더에 fc_log.log 와 같은 이름으로 저장된다. 다른 비행 로그는 비행 횟수에 맞춰서 여러 개의 로그가 저장되지만, LOG 형식의 파일의 경우 최신 DAT 파일만을 유지하며, 한

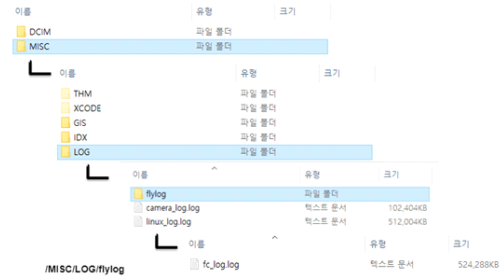


Fig. 6. Flight log in external SD card (DJI Mini)

개의 파일만 가진다. 외장 메모리에 비행 로그를 저장하는 이유는 드론이 내부 저장소가 존재하지 않을 때 외장 SD 카드가 그 역할을 대신하기 때문이다.

3.2 미디어 데이터 분석 방법

본 논문은 미디어 데이터를 분석하기 위해 EXIF 메타데이터를 분석하는 방법을 제안한다. 일반적으로 EXIF 메타데이터는 카메라 제조사, 카메라 일련번호, 회전 방향, 날짜 및 시간, 색 공간, 초점 거리, 플래시, ISO 속도, 조리개, 셔터 속도, GPS 등의 정보를 포함하고 있으며, 이 중 GPS 정보, 카메라 정보, 날짜 및 시간 정보를 획득하는 것을 목적으로 한다.

앞서 말했듯이 미디어 데이터는 모바일 저장소와 외장 SD 카드에 위치한다. 하지만 해당 저장소에 있는 모든 미디어 파일을 분석할 수 있는 것은 아니다. 일반적으로 DJI는 이미지와 비디오 파일을 축소된 형태의 캐시 파일로 추가로 저장하고, 이는 원본 파일의 약 1/10 정도의 크기를 가진다. 본 논문은 실험을 통해 확인한 결과 축소된 형태의 미디어 파일

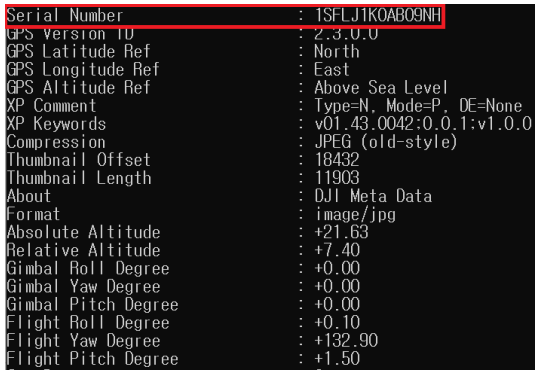


Fig. 7. Camera information to use ExifTool (v12.36)

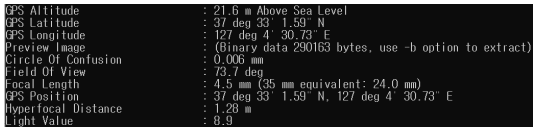


Fig. 8. GPS information to use ExifTool (v12.36)

은 EXIF 메타데이터를 가지고 있지 않은 것으로 판단한다. 따라서, 원본 파일만을 이용하여 미디어 데이터를 분석해야 한다.

EXIF 정보를 분석할 수 있는 도구는 다양하다. 메타데이터 정보는 어떤 도구를 사용하더라도 같은 정보를 구할 수 있다. 본 논문은 드론 포렌식에 사용되는 도구인 Autopsy와 가장 대중적으로 사용되는 오픈 소스 도구 ExifTool의 사용을 제안한다. 실제로 ExifTool을 이용해 카메라의 일련번호(Fig. 7.)를 획득할 수 있으며, GPS 정보(Fig. 8.) 또한 획득할 수 있다.

3.3 비행 로그 분석 방법

본 논문에서 비행 로그를 세 가지로 분류하지만, LOG 형식의 파일은 최신 DAT 형식의 비행 로그와 같다. 따라서 비행 로그를 분석하기 위해서는 TXT 형식의 로그와 DAT 형식의 두 가지 로그를 파악해야 한다. 앞서 논의한 바와 같이 비행 로그는 모두 암호화가 되어있으므로 일반적인 포렌식 도구로 인식되지 않는다. 따라서, 두 가지 형식의 비행 로그에 대한 분석 방법을 제안한다.

먼저, TXT 형식의 로그의 경우 모바일 저장소에만 존재하며, 현재까지 복호화하는 방법은 Airdata 또는 Phantomhelp와 같은 DJI와 계약한 드론 관리 사이트에서 수행할 수 있다. 하지만, TXT 형식의 로그가 가진 정보를 모두 제공하지 않으며, 드론을 취미로 사용하는 사용자 입장의 정보만을 제공한다. 해당 사이트에 TXT 형식의 비행 로그를 업로드하여 결과를 얻을 수 있으며, 획득한 정보는 CSV 또는 KML 파일로 다운로드할 수 있다. 본 논문에서 Airdata의 비행 로그 복호화 결과를 분석한 결과 얻을 수 있는 대표적인 특성은 Table 2.와 같다. 디지털 포렌식 조사관의 입장으로 봤을 때, 날짜 및 시간, GPS 정보, 드론의 속도, 진행 방향 등의 정보를 얻을 수 있으며, 이는 디지털 증거물로서 유의미하다.

Table 2. Representative features of TXT log (Airdata)

Feature	Unit	Feature	Unit
time	millisecond	max_distance	feet
datetime	UTC	pich	degrees
latitude	degrees	compass_heading	degrees
longitude	degrees	roll	degrees
speed	mph	gimbal_heading	degrees
distance	feet	gimbal_pitch	degrees
satelites	number	battery_percent	percent
voltage	V	battery_temparature	Fahrenheit
max_altitude	feet	isPhoto	bool
max_spped	mph	message	text

DAT 형식의 로그의 경우 마찬가지로 Airdata와 같은 드론 관리 사이트에서 복호화할 수 있다. 하지만, 본 논문은 DatCon을 이용해 DAT 형식의 로그를 분석하는 것을 제안한다. DatCon 도구는 프리웨어이며, 자체적으로 DJI와 협약을 맺지 않고 DAT 파일을 복호화하였다. 현재 논문이 쓰여진 시기를 기준으로 DJI 드론 중 Phantom 3, Phantom 4, Phantom 4 Pro, Inspire 1, Spark 및 Mavic Pro 드론을 지원하고 있다. Datcon을 사용하여 DAT 로그를 복호화한 그림은 Fig. 9.과 같다. 약 304개의 Feature를 얻었으며, TXT 로그가 가진 정보를 대부분 포함하면서, 더 세분화된 타임스탬프를 가진 것이 특징이다. 현재 지원하지 않는 모델에 관한 DatCon의 복호화 여부는 4장에서 설명한다.

두 가지 비행 로그는 복호화되면 CSV 형식의 파일로 변환된다. 하지만 CSV 형식의 파일을 그대로 분석하는 것은 시간 소모적이다. 이를 위해 CSV 파일을 시각화하여 분석하는 도구가 존재하고, 대표적

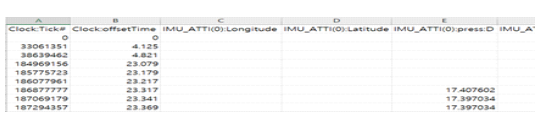


Fig. 9. Decrypted DAT log to use DatCon

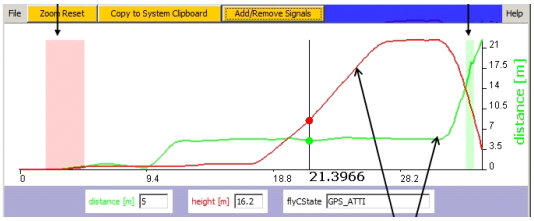


Fig. 10. Sigplayer in CsvView

으로 사용되는 도구는 CsvView 이다. CsvView는 두 가지 이상의 Feature를 시간 순서에 따라 그래프로 비교하여 나타내며(Fig. 10.), 특히 드론 관련 범죄에서 드론 조종자의 위치를 예측하는 데 유용하다.

IV. 실험 및 결과

본 장에서는 3장에서 제시한 DJI 드론의 아티팩트 분석 방법을 활용하여 출시 연월의 1년 이상의 차이가 있는 세 가지 드론을 대상으로 실험을 진행하였다. 먼저, 두 가지 범죄 시나리오를 작성하여 범죄를 저지른다고 가정하고 드론을 비행시켰다. 또한, 두 가지 시나리오를 미디어 데이터 분석과 비행 로그 분석에 적용하여 아티팩트 별 분석 결과를 도출하였고, 최종 결과로 드론의 복호화 여부에 따라서 분석 활용도가 높은 드론을 분류하였다.

4.1 실험 환경

본 논문의 실험을 진행한 환경은 다음과 같다. 먼저, DJI Phantom 3, DJI Mavic Mini, DJI Mini 2 세 가지 드론을 사용했다. 각 드론에 대해 모바일 저장소, 외장 SD 카드의 정보를 얻기 위해서, Samsung Galaxy S21+ 안드로이드 스마트폰을 이용하였고, 외장 SD 카드는 Sandisk 16GB Extreme을 사용하였다. 또한, 미디어 데이터 분석과 비행 로그 분석을 위해 ExifTool, Autopsy, Datcon, CsvView를 사용하였다.

4.2 드론 범죄 시나리오 설정

본 논문은 악의적인 사용자가 DJI 드론의 외형을 개조하여 범죄 행동을 하는 두 가지 시나리오를 묘사하였다. 두 가지 시나리오는 일반적인 드론 사용자도 실제로 저지를 수 있으며, 시나리오는 다음과 같다.

시나리오 1: 악의적인 사용자가 드론을 이용하여 불법 촬영을 통해 사진 및 동영상을 획득하고 복귀한다. (출발) - (목표물 도착) - (사진 및 동영상 촬영) - (복귀) 또는 (탈취) 순으로 진행된다.

시나리오 2: 악의적인 사용자가 드론으로 출입 불가능 지역에 진입하여 폭탄과 같은 유해성 물질을 운송하고 복귀한다. (출발) - (목표 지역 도착) - (복귀) 또는 (탈취) 순으로 진행된다.

만약 두 시나리오 모두 드론이 복귀하지 못하고 탈취된다면, 모바일 저장소의 미디어 데이터 및 비행 로그는 획득할 수 없다. 이는 디지털 조사관의 관점에서 범죄 현장에서 단순 드론 획득과 용의자 검거 시의 드론과 스마트폰 획득으로 구별된다.

4.3 DJI 드론 아티팩트 분석

3장에서 제시한 DJI 드론 분석 방법을 이용하여 세 가지 DJI 드론을 두 가지 범죄 시나리오에 따라서 비행한 후 아티팩트를 분석했다. 먼저, 드론 아티팩트 획득 장소와 획득 가능한 아티팩트를 정리한 표는 Table 3.과 Table 4.와 같다. 두 가지 표의 가장 큰 차이점은 내부 저장소의 유무이다. 내부 저장소가 존재하지 않는 DJI Mini 시리즈의 드론은 해당하는 아티팩트를 획득할 수 없었다. 하지만, 내부 저장소가 없는 대신에 외장 SD 카드에 fc_log.log 파일이 존재했고, 해당 파일을 분석하기 위해서 DAT 파일로 확장자를 변경해야 한다. 확장자를 변경할 경우 DAT 형식의 비행 로그 분석과 분석 결과와 이후 실험에는 LOG 형식의 비행 로그를 DAT 형식의 로그로 간주하고 실험을 진행하였다.

Table 3. Results of obtaining drone artifacts by location (Phantom 3)

Artifact / Location	Flight Logs			Media	
	dat	txt	log	jpg	mp4
Internal Storage	✓	n/a	n/a	✓	✓
Mobile Storage	✓	✓	n/a	✓	✓
External SD card	n/a	n/a	n/a	✓	✓

Table 4. Results of obtaining drone artifacts by location (Mavic Mini, Mini 2)

Artifact / Location	Flight Logs			Media	
	dat	txt	log	jpg	mp4
Internal Storage	n/a	n/a	n/a	n/a	n/a
Mobile Storage	✓	✓	n/a	✓	✓
External SD card	n/a	n/a	✓	✓	✓

4.3.1 드론 범죄 시나리오 분석 결과

Table 3.과 Table 4.을 통해 앞서 설정한 범죄 시나리오의 아티팩트 획득 여부를 분석하였다. 1번 시나리오의 경우 불법 촬영물에 대한 미디어 데이터 획득은 일반적으로 복귀 또는 탈취된 모든 DJI 드론에 대해서 가능하다. 하지만, DJI Mini 시리즈 모델의 경우 내부 저장소가 존재하지 않기 때문에 외장 SD 카드가 장착되지 않은 드론의 경우 한정으로 미디어 데이터를 획득할 수 없었다.

마찬가지로 2번 시나리오에서 드론이 출입 불가능 지역에 경유한 것을 판단하기 위해 비행 로그의 획득 여부가 중요하다. 탈취 또는 현장 검거로 획득한 드론은 Chip-off 방법과 모바일 저장소의 비행 로그를 획득할 수 있었지만, DJI Mini 시리즈는 내부 저장소의 부재로 인해 외장 SD 카드를 장착하지 않은 탈취된 드론의 경우 획득할 수 없었다. 따라서, 두 가지 시나리오에서 충분히 불법 범죄의 디지털 증거물을 획득할 수 있었지만, DJI Mini 시리즈 모델의 경우 외장 SD 카드를 장착하지 않고 범죄 이용되었을 때 증거 획득이 불가능하다.

4.3.2 미디어 데이터 분석 결과

세 가지 드론의 미디어 파일을 분석한 결과는 Table. 5.와 같다. 세 가지 드론에서 얻을 수 있는 정보의 차이는 없으므로 드론별로 분류하지 않는다. 획득한 미디어 데이터를 포렌식 관점에서의 의미를 파악하기 위해 5W1H를 통하여 판단하였다. 그 결과, 5W1H 중 5가지를 만족하였고, 이는 포렌식 관점에서 미디어 데이터 분석이 필요한 이유가 된다.

Table 5. Results of media data analysis

Information	Forensics Elements	5W1H
21.6 m Above Sea Level	GPS Altitude	Where
37 deg 33′ 1.59″ N, 127 deg 4′ 30.73″ E	GPS Position	Where
DJI Meta Data	Maker	How
1SFLJ1K0AB09NH	Camera serial umber	Who
2021:08:27 16:51:44	Timestamp	When
1.28 m	Hyperfocal Distance	What

4.3.3 비행 로그 분석 결과

세 가지 드론의 비행 로그를 분석한 결과는 Table 6.과 같다. Mavic Mini와 Mini 2의 온보드(onboard) DAT 로그의 경우 암호화 알고리즘의 미공개로 인해 분석할 수 없었다. 또한, 모바일 DAT 로그의 경우 Mini 2의 DAT 파일을 Airdata.com을 통해 복호화하였을 때의 결과를 확인하였을 때, 해수면 고도와 같이 시간 순서에 따라 연속적으로 변경되어야 하는 데이터가 무작위 또는 음수값을 가지는 것을 확인할 수 있었고, 이는 Fig. 12.와 같다. 따라서, Airdata.com의 복호화 API로 Mini 2의 DAT 파일을 복호화하지 못했다. 한편, TXT 로그의 경우 Airdata.com에서 복호화 API로 인하여 세 가지 드론에 대하여 복호화가 모두 성공하였다.

실제로 Mavic Mini의 모바일 DAT 파일에 대해서 CsvView로 분석한 결과는 Fig. 11.과 같다. 미디어 데이터와 다르게 배터리, 풍속, 비행시간, 컨트롤러의 일련번호, 펌웨어 정보 등 비행 기록과 드론 정보들이 포함되어 있으며, 이는 전체적으로

Table 6. Determining whether to decrypt the flight log of the three drones

Log type / Drone	DAT		TXT
	Onboard	Mobile	Mobile
Phantom 3	✓	✓	✓
Mavic Mini	X	✓	✓
Mini 2	X	broken	✓

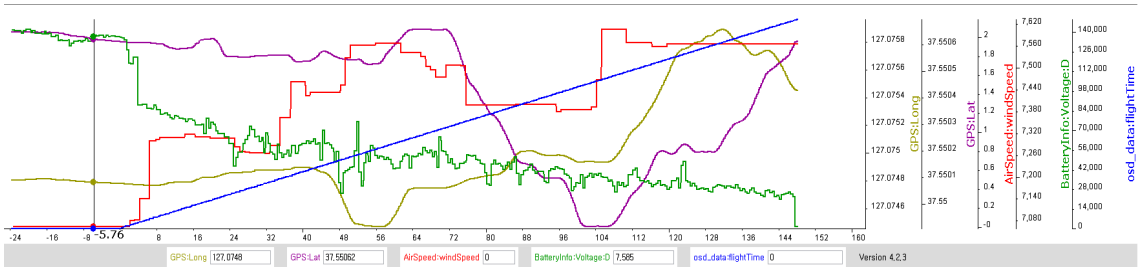


Fig. 11. GPS longitude, GPS latitude, wind speed, battery voltage, and flight time plotted using CsvView (Mavic Mini).

5W1H 중 Who, When, Where, How 총 4개를 만족할 수 있으므로 포렌식 관점에서 유의미하다.

드론 아티팩트 분석 결과를 통해 DAT 파일의 복호화가 세 가지 드론에 대해서 다르게 도출되었다는 사실을 바탕으로 각 드론의 모바일 DAT 파일에 대한 엔트로피 검사를 진행하였으며, 이는 Fig. 13.과 같다. 해당 그림에서 색깔이 연해질수록 엔트로피값이 높다.

암호학에서 엔트로피는 데이터 생성 기능의 무작위성 또는 다양성을 측정하는 것이다. 전체적으로 엔트로피가 높은 데이터는 복호화하기 위한 의미 있는 패턴을 찾기 힘들고, 낮은 엔트로피 데이터는 향후 생성될 값을 예측할 수 있게 한다[11]. 따라서, 세 가지 드론의 엔트로피 결과를 비교했을 때, DJI Mini 2 드론의 모바일 저장소 내부 DAT 파일이 복호화되지 않는 이유에 대해서 현재 복호화 도구가 감지하지 못하는 발전된 형태의 암호화 기술을 사용하고 있다고 예측할 수 있다.

실제로 본 연구에서 DAT 파일의 로그 버전의 변화를 확인하기 위해서 Hexeditor 도구를 이용하여 로그의 헤더 부분을 분석했고, 이는 Fig. 14.와 Fig. 15.와 같다. Fig. 14.은 DJI Phantom 3의 헤더이며, 약 256바이트의 크기를 가졌다. 하지만, Fig. 15.와 같이 최신 제품군의 DJI Mini 2의 경우 헤더 파일의 크기가 약 512바이트이며, 헤더에

altitude_above_seaLevel(feet)	altitude_above_seaLevel(feet)
123.2728849	-583.3333192
123.2728849	2005.249441
123.2728849	2596.128725
123.2728849	1877.296681
123.2728849	-1632.874035
123.2728849	1238.189049
123.2728849	2256.561785
123.2728849	7890.092149
123.2728849	-7500.000207
123.2728849	-7415.682619
123.2728849	1102.034189
123.2728849	-188.3201832
122.9448009	-5500.984395

Fig. 12. Results of the decrypted mobile DAT file

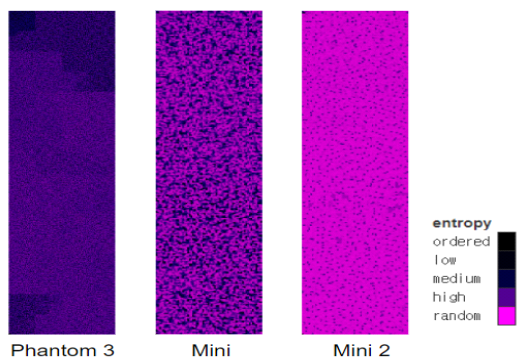


Fig. 13. Entropy of DJI Drones

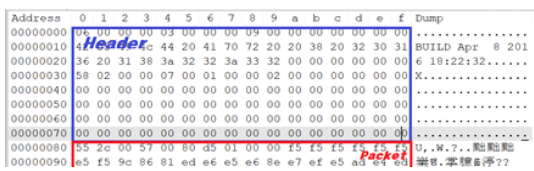


Fig. 14. DAT file header of DJI Phantom 3 in mobile storage

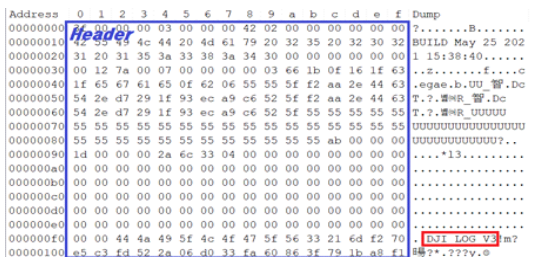


Fig. 15. DAT file header of DJI Mini 2 in mobile storage

포함된 문자열인 DJI LOG V3를 보면 알 수 있듯이 DJI Phantom 3보다 상위 버전의 로그 생성 알고리즘을 사용하고 있다. 한편, 본 논문은 LOG V3의 중요 암호화 알고리즘을 찾을 수 없었고, 현재까지도 해당 로그를 복호화할 수 있는 도구는 존재하지 않는다.

4.4 복호화 여부에 따른 DJI 드론의 분류

본 실험을 통해 DJI 드론의 비행 로그의 암호화 기술이 제품마다 다르게 적용되는 사실을 알 수 있었고, 실제로 DatCon의 제품별 복호화 지원 여부와 드론 포렌식 관련 논문을 참고하여 DAT 파일이 복호화 가능한 DJI 드론을 분류한다. 먼저, DJI 드론의 출시 연월을 나타낸 표는 Table 7.과 같다. 본 논문에서 실험한 Phantom 3의 경우 2015년 3월에 출시되었고, Mavic Mini와 Mini 2의 경우 각각 2019년 11월과 2020년 11월에 출시되었다. 출시 연월과 비행 로그의 복호화 여부를 연관 지었을 때 시간의 흐름과 관계되었다는 사실을 알 수 있다. 이 중 DatCon이 완벽하게 지원하는 모델인 Phantom 3, Phantom 4, Phantom 4 Pro, Inspire 1, Spark, and Mavic Pro는 약 2015년에서 2017년 사이의 모델임을 알 수 있다. 그 외의 모델 중 DJI Mavic Air, DJI Air 2, DJI Mavic 2의 경우 내부 저장소에서 획득하는 DAT 로그의 경우 복호화하지 못하였지만, 모바일 저장소에서 획득한 DAT 로그는 복호화할 수 있었다. 마지막으로, 본 논문에서 분석한 DJI Mini 2의 경우 모바일 저장소에서 획득한 DAT 로그를 복호화하지 못했으며, 외장 SD 카드에서 획득한 LOG 형식의 비행 로그도 복호화할 수 없었다. 이를 통해 DJI 드론을 세 가지로 분류하였으며, 이는 Table 8.과 같다.

Table 7. Release date of DJI drone

Classification	Drone name	Release
Phantom	Phantom 3	2015.03
	Phantom 4	2016.03
Inspire	Inspire 1	2015.11
	Inspire 2	2016.11
Mavic	Mavic Air	2018.01
	Mavic 2 Zoom/Pro	2018.08
	Mavic Mini	2019.11
	Mini 2	2020.11
	Mavic Air 2	2020.04
	Air 2s	2021.04
Spark	Spark	2017.05

V. 결 론

지난 몇 년 동안, 취미 용도 드론의 증가는 드론 범죄의 증가를 가져왔다. 이를 위해 본 논문은 악의적인 드론 사용에 맞서는 드론 포렌식 연구의 필요성을 강조하고, DJI 드론의 아티팩트 저장 위치와 분석 방법 및 분석에 용이한 드론 포렌식 도구를 제시하였다. 제안한 분석 방법은 모든 DJI 드론 제품군에 통용하여 사용할 수 있다. 먼저, 드론의 아티팩트 저장소는 내부 저장소, 모바일 저장소, 외장 SD 카드로 나눌 수 있고, 각 저장소에서 얻은 아티팩트를 분석 방법을 DJI Phantom 3, DJI Mavic

Table 8. Classification of DJI drones based on decryption

Type	Drone Name	Decryption
Type I (All Decrypted)	DJI Phantom 3, DJI Phantom 4, DJI Phantom 4 Pro, DJI Inspire 1, DJI Inspire 2 DJI Spark, DJI DJI Mavic Pro	Both the Onboard DAT file and the Mobile DAT file can obtain flight information, and the 2015-2017 launch model.
Type II (Mobile Decrypted)	DJI Mavic Air, DJI Air 2, DJI Mavic 2, DJI Mavic Mini	Only DAT files obtained from mobile devices can be read flight information. Models to be released in the first half of 2018~2020.
Type III (Not Decrypted)	DJI Mini 2	All DAT files cannot be decrypted. Drone models after the second half of 2020 release.

Mini, DJI Mini 2에 두 가지 범죄 시나리오를 적용하여 실험하였다. 범죄 시나리오 실험에서 탈취된 DJI Mini 시리즈의 드론은 외장 SD카드의 부재로 디지털 증거물 획득이 불가능했다.

또한, 미디어 데이터를 분석하는 경우 세 가지 드론에서 동일하게 GPS 정보와 타임스탬프, 카메라 일련번호 등을 얻을 수 있었으며, 이는 포렌식 관점에서 5W1H 중 5가지를 만족한다.

하지만, 비행 로그의 분석 결과는 DJI 드론의 종류마다 차이가 발생하였고, 이를 위해 본 연구에서는 세 가지 드론에 대한 DAT 로그의 복호화를 실험하였으며, 그 결과로 주로 사용되는 DJI 드론을 세 종류로 분류하였다. 본 논문에서 제시한 드론의 분류는 점진적으로 발전한 비행 로그의 암호화 방식을 나타내는 판단 근거가 되며, 불상의 DJI 드론을 획득 및 분석 시 드론 모델의 식별 이후 진행될 포렌식 분석의 기준점이 될 것으로 기대한다.

본 논문에서 제시한 세 가지 분류는 향후 DJI 드론이 더 발전된다면 새로운 유형의 드론에 대해서 적용되지 못할 수 있으며, 논문의 실험이 DatCon에 큰 비중을 두고 있어 더 완벽한 복호화 도구가 나온다면 결과가 달라질 수 있다는 한계가 있다. 향후 연구로 새로 출시된 DJI Mavic 3에 대해서 포렌식을 수행하여 기존 DJI 모델과 차이점을 파악하고 분석하여 본 논문에서 제시한 아티팩트 분석 방법을 개선할 계획이다.

References

[1] FAA. UAS Sightings Report. Available online: https://www.faa.gov/uas/resources/public_records/uas_sightings_report/.

[2] D. A. Hamdi, F. Iqbal, S. Alam, A. Kazim and A. MacDermott, "Drone Forensics: A Case Study on DJI Phantom 4," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), pp. 1-6, 2019.

[3] Stanković, Miloš, Mohammad Meraj Mirza, and Umit Karabiyik. "UAV Forensics: DJI Mini 2 Case Study," Drones 5, pp. 49-68, June 2021.

[4] Lan, James Kin Wah, Kin Wah Lee, "Drone Forensics: A Case Study on DJI Mavic Air 2," In: 2021 23rd International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 291-296, 2021.

[5] Airdata UAV. Available online: https://app.airdata.com/

[6] DatCon. CsvView/DatCon. Available online: https://datfile.net/

[7] Clark, Devon R., et al. "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," Digital Investigation, vol. 22, pp. S3-S14, August 2017.

[8] Technology, B. Autopsy. online: https://www.basistech.com/autopsy

[9] Cellebrite. Home-Cellebrite|Digital Intelligence for a Safer World. Available online: https://www.cellebrite.com/en/home/

[10] Salamh, Fahad E., Mohammad M. Mirza, and Umit Karabiyik. 2021. "UAV Forensic Analysis and Software Tools Assessment: DJI Phantom 4 and Matrice 210 as Case Studies," Electronics, vol 10, no. 6, pp. 733, 2021.

[11] Thomas W. Edgar, David O. Manz, in Research Methods for Cyber Security, 2017.

[12] Barton, T.E.A, Azhar, MA Hannan Bin Azhar, "Forensic analysis of popular UAV systems," In Proceedings of the 7th International Conference Emerging Security Technologies EST 2017, pp. 91 - 96, September 2017.

[13] Llewellyn, Mark, "DJI Phantom 3-Drone Forensic Data Exploration," Edith Cowan University: Perth, Australia, 2017.

[14] JAIN, Upasita, ROGERS, Marcus Rogers, and Eric T. Matson, "Drone forensic framework: Sensor and data identification and verification," In: 2017 IEEE Sensors Applications Symposium

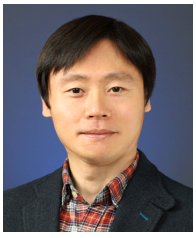
(SAS). IEEE, pp. 1-6, 2017.
[15] RENDUCHINTALA, Ankit LP S. ALBEHADILI, Abdulsahib; JAVAID, Ahmad Y. "Drone forensics: digital flight log examination framework for micro drones," In: 2017 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, pp. 91-96, 2017.
[16] Kao, Da-Yu, et al. "Drone Forensic Investigation: DJI Spark Drone as A Case Study," Procedia Computer Science, vol. 159, pp. 1890-1899, 2019.

〈저자소개〉

이 영 우 (Youngwoo Lee) 학생회원
2021년 2월: 세종대학교 정보보호학과 졸업
2021년 3월~현재: 세종대학교 일반대학원 정보보호학과, 지능형드론 융합전공 석사과정
〈관심분야〉 임베디드 장치 에뮬레이션 및 퍼징, 드론 포렌식

김 주 환 (Juhwan Kim) 학생회원
2016년 2월: 학점은행제 정보보호학 전공 학사
2019년 8월: 세종대학교 일반대학원 정보보호학과 석사
2019년 9월~현재: 세종대학교 일반대학원 정보보호학과, 지능형드론 융합전공 박사과정
〈관심분야〉 악성코드 분석, 시스템 보안, 소프트웨어 취약점

유 지 현 (Jihyeon Yu) 학생회원
2020년 2월: 세종대학교 정보보호학과 졸업
2020년 3월~현재: 세종대학교 일반대학원 정보보호학과, 지능형드론 융합전공 석박사통합과정
〈관심분야〉 악성코드 분석, 시스템 보안, 소프트웨어 취약점



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, 지능형드론 융합전공 부교수
〈관심분야〉 네트워크 보안, 시스템 보안, 인공지능 보안