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.2023.33.4.633

오픈소스 기반 드론 라이브 포렌식 도구를 활용하는 드론 포렌식 방법론 연구

백 세 영,†‡ 이 상 욱
ETRI 부설연구소 (연구원)

A Study On Optimized Drone Forensic Methodology Applied with Open Source Based Drone Live Forensic Tool

Seyoung Baik,†‡ Sangwook Lee
The Attached Institute of ETRI (Researcher)

요 약

무인이동체 드론의 수요가 증가함에 따라 안전사고의 위험성뿐만 아니라 불법 드론에 대한 보안 위협도 증가하고 있다. 드론 포렌식의 필요성을 인식한 국내외 기관에서는 드론 포렌식 방법론을 수립하기 위해 노력 중이다. 실용적인 무인이동체 포렌식 방법론을 수립하기 위해서는 필수 아티팩트 정의와 포렌식 도구에 관한 검증이 선행되어야 하고, 드론 포렌식의 경우 기체 활성 상태에서 추출 가능한 데이터가 존재하기 때문에 라이브 포렌식도 고려되어야 한다. 본 연구에서는 다양한 드론 기종을 포괄하는 드론 포렌식 방법론의 필요성을 설명하고, 오픈소스 드론 대상 라이브 포렌식 도구(LiPFo, Live-PX4-Forensic)을 활용한 실용적인 포렌식 방법론을 제안한다.

ABSTRACT

The increases in UAVs(Unman Aerial Vehicle) such as drone result in safety issues and the threat of illegal drone as well. Recognizing the need for Drone forensics, domestic and foreign organizations and agencies are trying to establish drone forensic guidelines. The definition of Drone forensic artifacts and examination of forensic tools must be provided, in order to establish a practical drone forensic framework on security sites and also the concept of drone live forensic which provides meaningful data that can be extracted in a live state. In this study, the drone forensic methodology covering various types of drones is explained, and the practical forensic methodology with live forensic PoC(Proof Of Concept) tools; LiPFo(Live-PX4-Forenensic) is proposed.

Keywords: Drone Forensic, PX4, Open Source Drone Forensics, UAV

I. 서 론

드론은 국토조사, 영상촬영, 수송, 농/임업, 재난/방재, 국방 등 활용 분야가 확대되고 파급효과도 상당하다. 드론의 활용 분야와 역할이 커질수록 안전사고와 위협에 대한 불안감이 증가하고 있다. 드론 플랫폼은 기체, 조종기 그리고 지상관제 시스템으로 구성되며 관련 기술이 고도화되고 있지만, 기체, 조종기, GCS(Ground Control System)를 포괄하는 실용적인 드론 포렌식 방법론은 미비한 실정이다. 국가·공공기관에서 사용하는 드론이 사고로 인해 기체가 분실될 경우 데이터 유출 위험도 존재한다.

다양한 드론 플랫폼에 따른 드론 데이터가 상이하여 수집 가능한 데이터 종류와 수집방안이 다르다.

Received(06. 07. 2023), Modified(07. 25. 2023), Accepted(07. 25. 2023)
† 주저자, sybaik@nsr.re.kr
‡ 교신저자, sybaik@nsr.re.kr(Corresponding author)

오픈소스 기반 드론에서 상용 드론에 이르기까지 조종기 및 지상관제 시스템에서 수집할 수 있는 데이터가 방대하다[1]. 또한, 비행·임무 데이터를 기반으로 법적 근거로 활용되거나 사고조사 및 사고 예방에 적용 가능한 제도와 정책도 미비하다. 2015년 이후 국내 보험회사가 지급한 드론 사고 보험금 지급 건수는 704건인데 반해 국토교통부에서 발표한 드론 사고는 총 11건으로 큰 차이를 보이는데, 이는 사고라고 규명할 규정과 법적 증거자료로 채택될 수 있는 증거가 명확하지 않기 때문이다[2]. 또한, 사고 발생 시 단순한 기계적 결함으로 인한 사고인지 의도적인 사이버 해킹에 의한 분별이 어려워 책임소재에 관한 문제도 존재한다.

드론 플랫폼은 운용방법과 기체종류가 다양하여 일괄적인 포렌식 방법을 적용하기 어렵다. 이러한 문제를 해결하기 위해서 Fig. 1과 같이 드론 증거자료 수집과 데이터 분석 등 방법론에 관한 연구가 진행되었다. 특정 드론을 대상으로 추출 단계에서 시각화단계까지 다양한 연구결과를 제시하고 일반적인 방법론을 정립하였다. 주로 DJI 社 기체를 중심으로 연구가 이루어졌기 때문에, 오픈소스 기반 드론과 같이 확장성이 큰 플랫폼을 대상으로 한 연구는 부족하였다. 또한, 파손된 기체, 운용 상태 중인 기체, 특정 파일이 부분적으로 복구된 경우 그리고 기체를 모르는 상황 등 다양한 시나리오를 포괄하는 가이드라인이 필요하다.

본 연구에서는 기존 드론 포렌식을 위한 국내외 연구 동향을 요약하고 최적화된 드론 포렌식 방법론을 제안한다. 또한, Fig. 1의 방법론 중에서 드론 포렌식 수행을 위한 도구를 비교하고, 구체적인 방법론을 기술한다. 오픈소스 기반 드론을 대상으로 물리적 칩 제거(Chip-Off) 없이 대상 기체의 활성 상태에서 정보 수집을 위한 개념검증(PoC, Proof of Concept)을 수행하였다.

본 연구의 기여점은 다음과 같다.

- ○ 기존 드론 포렌식 연구 동향을 분석하여 포렌식 아티팩트와 데이터 추출 지점 등 정리
- ○ 상용 통합도구, 오픈소스 도구 그리고 라이브 포렌식 도구를 상호 활용하여 실용성 있는 드론 포렌식 방법론 제안
- ○ 오픈소스 기반 드론을 대상, 신속한 비행 로그 추출을 위한 라이브 포렌식 도구(LiPFo, Live-PX4-Forensic) 개념검증을 통한 드론 포렌식 도구의 개발 방향성 제안

II. 관련연구

2.1 연구 분류

드론 포렌식 관련 연구는 드론 데이터가 축적되는 지점 분석연구, 데이터 추출 연구를 포함한 방법론 연구 그리고 추출된 데이터 분석 등 Table. 1과 같이 크게 3가지 형태로 분류할 수 있다.

대부분의 드론 플랫폼은 SD카드에 미디어 데이터

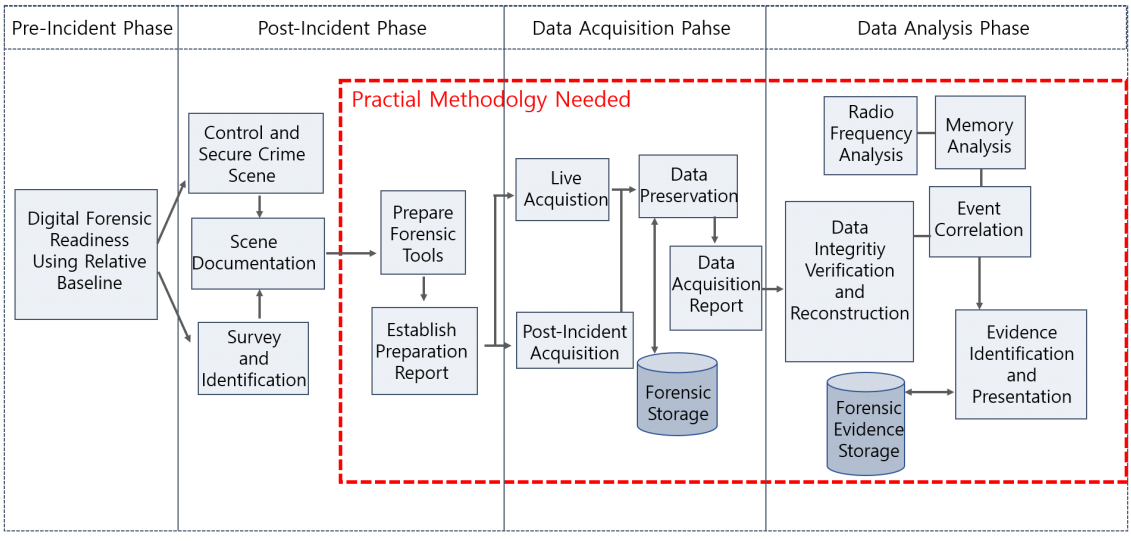

Fig. 1. Motivation of Drone Forensic Methodology based on Al-Dhaqm Research[6]

Table 1. Summary of Drone Forensics Studies

Research	Year	Focus	Forensic Target	Features and Contribution
[3]	2017	DJI Forensics	DJI Phantom 3	· DAT File system structure analysis · DAT tool development(DROP) · Proposal of acquisition for DJI data
[6][7]	2021	Drone Forensic Methodology	Mobile and Database analysis for forensic methodology	· Analysis of drone forensics and existing forensic technologies · Establishing drone forensic methodology including drone, mobile and network
[17]	2022	Classification of DJI Decryption	DJI	· Classification according to decoding method for DJI drones
[8][9][10] [11][12] [13][14] [15][16]	2022	DJI Forensics	DJI Mavic air 2 DJI Models	· Analysis of chip-off and research result · Drone Forensics tools
[18][19]	2022	PX4 Data Extraction Tool	Pixhawk	· Tool development using Mavlink
This Work (2023)		Drone Forensic Methodology	DJI Phantom4, Pixhawk	· Proposal of drone forensic methodology including various tools and drone live-forensics tools · Proposal for drone live-forensics concepts and development of proof-of-concept tool

와 비행 로그가 저장되는 방식으로 운용되어 외장메모리 복구 연구[3]가 주로 진행되었다. 외장메모리에서 유의미한 데이터 추출이 불가한 경우나, 암호화된 데이터 경우 플래시메모리를 칩 제거하여 데이터를 획득한 연구도 있다.

포렌식 방법론 연구는 주로 DJI 기종을 대상으로 사례기반 연구가 수행되었다[3][6][7]. DJI 비행로그 특성과 파일시스템을 분석, 비행 로그 복호화 방안을 적용한 방법론을 수립하였다. 드론 데이터의 경우에 추출 대상이 지상관제 시스템, 기체 그리고 조종 어플리케이션 등 데이터를 융합하여 증거 신뢰도를 높이는 방안이 연구되었다. 다만, DJI 기종을 대상으로 포렌식 편향되어, 오픈소스 기반 드론에 적용하기 위해서는 방법론의 보완이 필요하다.

임베디드 기기의 취약점 분석연구도 포렌식 방법론에 활용할 수 있다. 비행 로그뿐만 아니라 펌웨어 획득방안과 단계별 사용 가능한 도구 분류 연구가 수행되었다[5]. 메모리 칩 제거와 숨겨져 있는 시리얼 포트를 통한 데이터 획득 등 다양한 데이터 획득방안이 연구되었다.

이밖에도 추출된 데이터 기반의 사건 재연을 위한 시각화 도구개발도 활발하다. 다만, pix 4D 및 Flight Review와 같은 드론 미디어 데이터 시각화 플랫폼의 경우, 해당 서버에 비행 데이터를 업로드하여 분석하는 방식으로 운용되어 데이터 유출에 유의해야 한다.

2.2 국내·외 동향

2.2.1 국내현황

한국형사·법무정책연구원은 2022년 1월에 드론과 자율주행차량을 포함한 첨단 과학수사 정책 및 포렌식 기법 종합발전 방안연구 보고서를 발간하였다[1]. 드론산업 확대에 따른 포렌식 도구의 필요성을 기술하고, 이에 대응하기 위한 포렌식 기술과 절차, 개선방안 등 다양한 측면에서 연구를 수행하였다. 상용 DJI드론을 대상으로 드론 포렌식 방법론을 연구한 Al-Dhaqm의 방법론[6]을 기반으로 절차적 수사 가이드라인을 구체화하였다. 다만, 특정 상용 드론에 국한되어 미식별 기체를 포함한 다양한 드론에 적용하기에 다소 어려움이 있다.

Table 2. Classification of Drone Artifacts

Required Data List	Classification		Location	Feature	Main Tools
	Type	File Extension			
Flight log	DJI	*.TXT	Smart Phone(Controller), GCS	·Communication-based flight log ·Encrypted communication protocol	· FlightReader
		*.DAT	Drone, Smart Phone(Controller) GCS		· DatCon(Partial)
		*.Log	External MicroSD		· DatCon(Partial), · FlightReader · Commercial Integration Tools
	Yuneec	*.ulg	Drone	· Analysis with Opensource Tools · Lack of encryption function	· Pyulog · plotulog · MavGCL · Commercial Integration Tools
	Pixhawk	*.ulg *.tlog	Drone,GCS		
	Parrot	*.pud	Drone	· Real-time simulation and Flight log visualization analysis	· Sphinx
Media	Picture	*.jpg *.png *.mp4	External MicroSD	· Comparative analysis with flight log is required	· Commercial Integration and Opensource Tools
	Video				
Personal Identification Information	· Unique module for drone identification · Hardware information such as manufacturer model number and battery information · Data exchange history based on ASTM F3411[1] Remote ID standard				

2.2.2 국외현황

국제형사기구 인터폴(Interpol)은 2020년 초기 대응자 및 디지털 포렌식 실무자를 위한 드론사고 대응 프레임워크(Framework For Respondering To A Drone Incident)를 발행하였다. 드론 장치의 기본적인 구조, 드론사고 대응 초기지침, 증거획득방법, 조사방안 그리고 분석 후 제출에 관한 포괄적인 지침을 기술하였다.

미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)는 디지털 포렌식 도구 검증을 위한 CFReDS (Computer Forensic Reference Datasets) 프로젝트를 수행하였고, 2018년부터 드론 포렌식 분석 결과를 공유하였다. 적용된 기체는 총 20여종 상용 모델로 60여대 드론으로 진행되었고, 논리적, 물리적, 칩 오프 결과를 바탕으로 획득한 데이터를 제시하였다. 하지만 구체적으로 드론 포렌식에 적용된 도구와 검증방안에 대해서는 언급하지 않았고, 드론 포렌식을 수행한 구체적인 수행시점과 환경은 공개되지 않았다. 또한, 비행데이터와 미디어 데이터를 위주로 획득하였고, 파일시스템 분석 등의 구체적인 시스템 분석 정보는 공개하지 않았다.

III. 드론 포렌식 방법론 수립

실용적인 드론 포렌식 방법론 수립을 위해서 드론 포렌식 관점의 아티팩트를 정의하고, 이를 기반으로 다양한 드론 플랫폼에서 데이터 획득·분석·검증 단계를 구체화한 절차가 필요하다.

1) ASTM F3411 Specification for Remote ID and Tracking과 ASD-STAN prEN 4709-002 Direct Remote Identification, 원격 식별 장치 표준화 작업이 진행 중

3.1 드론 아티팩트 정의

Pixhawk 및 Ardupilot 등 확장성이 높은 오픈소스 플랫폼부터 시장 점유율이 가장 높은 DJI 社 드론까지 포괄할 수 있는 데이터 아티팩트(artifact)를 정의하고, 적용 가능한 상용 통합도구 및 오픈소스 도구를 Table. 2에 정리하였다. 비행 로그, 개인식별정보, 미디어 데이터 등 총 3가지를 주요 아티팩트로 정의하고, 분석 대상 플랫폼은 모바일 기기, 전용 조종기, GCS, 기체, 클라우드 서버, 시각화 서비스 서버 등으로 분류하였다.

비행 로그에는 비행궤적, 고도, 기체 자세값, 모터 출력 및 각종 실시간 센서값 등 비행 정보가 포함된다. 미디어 데이터는 드론 기체에서 촬영된 사진, 동영상으로, 미디어 데이터와 비행 로그를 하나의 아티팩트로 융합하여 비행 데이터로 정의된다. 비행 시점에 따른 경로와 미디어 데이터를 재구성하는 것이 사건 분석의 핵심이다. 이러한 비행 데이터는 주로 기체 자체 내·외부 SD카드에 저장되고, 모바일 기기 및 GCS(Ground Control System)에도 존재하기 때문에 추출 지점과 융합 방안을 고려해야 한다. 개인식별정보와 관련된 드론 아티팩트는 원격식별장치 탑재 여부와 데이터 교환 이력이 반영되어야 한다. 美 FAA의 원격식별장치(RemoteID) 장착 의무화에 따라, 개인식별정보에는 원격식별장치와 관련된 데이터가 식별정보 아티팩트 반영에 필수적이다. 따라서, 드론 포렌식 증거자료로 원격식별장치 여부 확인과 관련 데이터의 별도 저장 방안 및 검증도 선제적 대비가 필요하다.

3.2 드론 플랫폼에 따른 비행 로그 특성

DJI 社 계열 드론의 경우 비행 로그를 암호화하여 저장하는 추세이고, 기종에 따라 오픈소스 도구로 복호화하는 데 한계가 있다. 이때, 물리적 칩 제거를 통해 비행 데이터 획득이 가능할 수도 있지만, 이후 복구가 불가능하므로, 물리적 분해 이전에 최대한 다양한 추출기술을 적용하여야 한다.

DJI 계열 드론의 비행 로그 분석 연구 결과[17], Table. 3과 같이 기종에 따라 DAT 파일의 복호화 방안이 다르다. 또한, On-Board 메모리에서 비행 로그를 저장하는 개발 추세에 따라, 데이터 확장자와 암호화 방식도 기체별로 달라 매번 추가적인 복호화 연구와 분류가 필요하다. 모바일 기기가 조종기 역할을 하는 플랫폼의 경우에는 모바일 기기에서 비행 로그추출이 필요하여 모바일 포렌식도 수반된다.

Table 3. Classification of DJI Drone data

Type	DJI Drone	Year	Acquisition and analysis method
A	Phantom3,4 Phantom4 Pro Inspire1,2 Spark1,2 Mavic Pro	'15~ '19	· Drone/Mobile · DatCon
B	Mavic Air1,2 Mavic 2 Mavic 2 Pro Mavic Mini	'18~ '20	· Mobile · DatCon (Partially Chip-off)
C	Mavic Mini2	'19~	· DatCon Not Available · DJI SDK

Pixhawk나 Ardupilot과 같은 오픈소스 기반 드론은 *.ulg 와 *.tlog 형식으로 비행 로그 파일을 저장한다. 확장자가 *.ulg인 ulog는 기체 내부 센서 입·출력값과 시스템 상태 정보를 포함하며, 내부 메시지 통신을 통해 PX4 아키텍처 내 Logging 모듈에 저장된다. tlog는 텔레메트리를 통해 전달된 메시지로 미션 명령 값을 중점으로 저장된다. ulog의 데이터는 headers, Definition, Data로 구성되어 있고, header 영역의 매직넘버와 버전 정보로 ulg 식별이 가능하다. Definition과 Data 영역에 다양한 메시지 데이터를 포함하는 구조를 가지는데, Definition 영역에는 저장될 메시지 타입과 크기 정보 등 구조체를 정의하고, 이를 바탕으로 Data 영역에서 구체적인 데이터를 정의한다. Definition 영역에는 플래그 비트, 포맷 정의, 정보, 파라미터를 명시하며, Data 영역에는 구독 정보(Subscription), 저장데이터, 동기화 정보 등의 상세 정보를 정의할 수 있다. 기체 내 저장 경로는 일반적으로 ./build/(PX4빌드환경)/logs 와 같이 빌드 된 환경 내 logs 폴더에 저장된다.

3.3 기존 포렌식 도구 분석

드론 포렌식 도구는 통합 상용도구와 오픈소스 도구로 분류할 수 있다. 각 도구는 상호보완적이고 교차검증이 가능하여, 포렌식 도구에 대한 이해가 반드시 선행되어야만 최적화된 드론 포렌식 방안을 수립

할 수 있다. 사건 재연의 경우, 비행 로그를 기반으로 웹서비스와 연동한 분석이 쉬워진 만큼 데이터 유출방지나 비행 데이터의 무결성 검증 그리고 위변조 방지 등의 방안이 함께 고려되어야 한다.

3.3.1 오픈소스 도구

오픈소스 도구는 Table. 4과 같이 비행 데이터 추출, 분석, 시각화단계에서 활용될 수 있다. DJI 비행 로그 파일(.Dat) 복호화를 위해서 DatCon 활용이 필수적이며, DatCon으로 복호화가 가능한 기종은 DJI spark, Phantom계열이고, Mavic 계열을 포함한 최신 기종은 DatCon으로 복호화가 불가능하여 메모리 칩 제거 기술을 활용하거나 전용 SDK를 활용해야 한다.

오픈소스 기반 드론의 경우, MicroSD 카드와 QGC(QGroundControl)에서 PX4 로그 데이터(*.ulg)를 추출할 수 있고, pyulog, FlightPlot, ulogreader와 같은 도구를 활용하여 분석할 수 있다. 또한, ulg 파일을 csv 파일 형태로 변환하여 Flight Review 및 Flight Reader 등에서 재연할 수 있다.

Table 4. Open source tool for Drone Forensics

	Software Name	Function
Extraction and analysis	ExifTool	Media Forensic
	DatCon	DJI Flight log Extraction
	binwalk	Firmware file analysis
	ST2Dash, Dashware	Yuneec Flight log extraction and analysis
	HxD	Data Comparison
	pyulog, FlightPlot, pyFlightAnalysis, mavlinnk-router, ulogreader	PX4 Flight log analysis
Visualization	CsvView	Visualization (*.csv)
	ArcGIS Pro	3D Visualization
	Google Earth	3D Visualization
	Flight Log, Analysis, Flight Review	PX4 Visualization

3.3.2 상용 통합도구

드론 포렌식 상용 통합도구는 데이터 추출 및 분석, 최종 증거제출을 위한 무결성 검증단계를 수행하는 도구이다. 추출된 비행 로그와 미디어 데이터를 자체 이미징 파일로 융합하여 관리한다. 모바일 기기, 기체 등으로부터 추출된 미디어 데이터, 비행로그 데이터, 임무데이터를 통합하여 시간·사건 기반 분석을 지원한다. 대표적인 드론 포렌식 상용 통합도구는 Cellebrite 社의 UFED 4PC와 GMDSOFT 社의 MD-Drone 등이 있다.

통합도구는 지원하는 기종, 출력정보, 중점 기능에서 차이가 있다. Cellebrite UFED 4PC는 앞서 언급된 NIST CFTT[2] 인증 도구로 지정되어 있다. 기존 모바일 기기와 USIM 포렌식에 특화된 솔루션에 드론 포렌식 기능을 확장하였다. 추출된 비행데이터는 이미징 파일(*.ufd)에 기반한 사건 시각화 및 재구성 기능을 지원한다. 복호화가 어려운 경우에는 드론 기체 메모리를 디솔더링(Desolodering)하여 파일시스템을 추출하는 도구도 별도 제공한다. 드론 조종기 역할을 하는 모바일 기기에 저장된 로그 데이터를 추출하여 하나의 이미징 파일로 통합할 수 있고, UFED PA(Physical Analyzer)를 통해 통합 분석도 가능하다. 또한, Fig. 2와 같이 비행 로그와 미디어 데이터를 하나의 전용 이미징 파일로 융합하

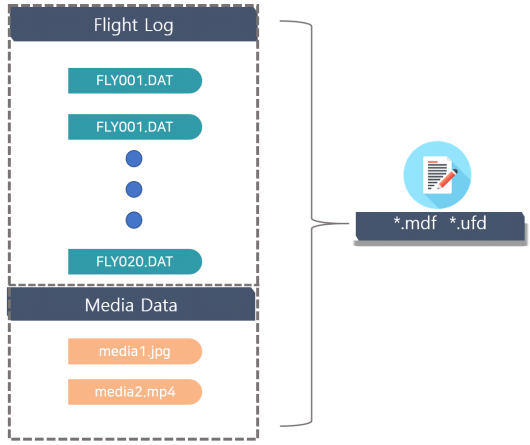

Fig. 2. Features of Commercial Drone Forensics tool

2) 美 국립표준기술연구소(NIST)에서 디지털 포렌식 도구 검증 체계 구축과 관련하여 수행 중인 프로젝트명

는 기능을 제공한다. 미디어 데이터와 비행 로그는 모바일기기(조종기) 혹은 기체 에 그 데이터가 분산되어 있으므로, 통합도구를 통해 이를 편리하게 융합하여 관리 할 수 있다

GMDSOFT 社에서 개발한 MD-Drone은 UFED 4PC와 유사한 기능을 제공한다. 자체 파일 확장자인 *.mdf 이미징 파일을 기반으로 비행데이터를 분석하고 재구성한다. 오픈소스 기반 드론을 포함한 다양한 기종에 대한 포렌식이 가능하며, 추출과 분석을 같은 플랫폼에서 수행할 수 있다. 다만, 모바일 기기(조종기) 포렌식의 경우 MD-RED, MD-NEXT 계열의 별도 솔루션을 적용하여, *.mdf 이미징 파일로 융합 후 분석해야 한다. 두 도구 모두 추출-분석-시각화의 포렌식 절차에 따라 독립적인 이미징 파일을 생성한다는 점이 유사하지만, 모바일 포렌식으로 추출한 데이터 융합 방법과 분석에 적용되는 솔루션에 차이가 있다.

3.3.3 도구 간 비교 분석

Table. 5에서는 DJI Phantom4 Pro와 Pixhawk CUAV V5 기체를 대상으로 두 상용 통합도구를 비교한다. MD-Drone은 DJI 드론 이외에도 오픈소스 기반 드론에 대한 포렌식이 가능하지만, UFED 4PC 경우에는 지원하는 기종이 DJI 계열에 집중하고 있다.

동일한 DJI 기체를 대상으로 추출 및 분석한 결과 MD-Drone이 더 많은 시간이 소요되었지만, 드론의 위치, 자세, 모터 출력 값 등 다양한 비행데이터 속성을 출력하였다. Cellebrite UFED는 추출 속도는 빠르지만, 출력되는 비행 데이터 속성이 간결하였다. 동일한 DAT파일을 오픈소스 도구 DatCon으로 비교해 본 결과 MD-Drone으로 추출한 Waypoint 개수와 DatCon에서 추출된 개수가 유사하게 출력하였다. UFED 4PC로 추출한 비행경로는 같았지만, 총 Waypoint 개수에서 차이가

Table 5. Comparison between Commercial Drone Forensics tools

<table>
<tr><th></th><th colspan="3">MD-Drone</th><th colspan="3">Cellebrite UFED</th></tr>
<tr><td>Support Drone Platform</td><td colspan="3">23 drones
(Including Opensource based drones)</td><td>9drones
(DJI mavic, phantom line)</td><td colspan="2">DJI-Inspire2
DJI-Mavic Air
DJI-Mavic Pro
DJI-Mavic Pro 2
DJI-Phantom 3
DJI-Phantom 4
DJI-Spark
Parrot - Bebop</td></tr>
<tr><td>Certification Case</td><td colspan="3">None</td><td colspan="3">NIST CFTT Certified Tool</td></tr>
<tr><td rowspan="3">Related Solution</td><td rowspan="2">Extraction</td><td>Drone</td><td>MD-Drone</td><td rowspan="2">Extraction</td><td>Drone</td><td rowspan="2">UFED 4PC</td></tr>
<tr><td>Mobile</td><td>MD-Next
MD-Red</td><td>Mobile</td></tr>
<tr><td>Analysis</td><td colspan="2">MD-Drone</td><td>Analysis</td><td colspan="2">Cellebrite PA</td></tr>
<tr><td>Imaging File Type</td><td colspan="3">*.mdf</td><td colspan="3">*.ufd</td></tr>
<tr><td>Time Consumption</td><td colspan="3">Approx. Three hours or more
(Equivalent File)</td><td colspan="3">Approx. 1 hour (Equivalent File)</td></tr>
<tr><td>Visulization</td><td colspan="6">Playback function including location and Drone information</td></tr>
<tr><td>Waypoint</td><td colspan="3">Approx. 3,000 points</td><td colspan="3">Approx. 300 points</td></tr>
<tr><td>Features</td><td colspan="3">· Specialized in event visualization(takeoff and landing analysis)
· Support reading tool after chip-off
· Various Flight data information
· Various extraction points</td><td colspan="3">· Specialized in file system and hexa data analysis
· Concise and refined flight data information
· Extraction rapidity and efficiency</td></tr>
</table>

발생하여, 포렌식 도구 별로 추출기준이 다른 것으로 판단된다. 데이터 획득 시점에서도 도구별로 차이가 있다. UFED 4PC는 모바일 기기와 드론 기체에서 자동화 추출 및 이미징 파일 생성으로 관리가 쉬운 반면, MD-Drone은 Fig. 3과 같이 획득 지점을 선택하여 추출할 수 있다. 다만, 모바일에 존재하는 데이터를 추출하기 위해서 별도의 도구를 사용해야 하는 번거로움이 존재하지만, 추출 시점과 지원 기종 등 상호보완적으로 사용하기에는 유용하다.

상용 통합도구는 오픈소스 기반 드론과 상용 드론을 대상으로 지속적인 지원이 필요하다. DJI 드론의 데이터 분석은 오픈소스 도구 DatCon에 의존적이어서, 상용 통합도구가 복호화할 수 있는 기체 범위도 DatCon의 지원 기체 범위를 크게 벗어나지 않아서 실효성에 한계가 존재한다. 즉, 통합도구에서 지원하지 않는 DJI 모델은 DatCon의 복호화 범위를 벗어났기 때문에 정식 SDK를 활용한 적용 방안 필요하지만, 아직 지원하지 않고 있다. 오픈소스 기반의 드론의 경우 교차검증이 가능한 별도의 도구가 부족하여 오픈소스 기반의 드론 포렌식 도구개발도 필요하다.

Fig. 3. Options for Data Extraction in MD-Drone Solution

3.4 드론 라이브 포렌식 도구 PoC(Proof of Concept)

신속한 비행 로그 획득과 RAM의 휘발성 데이터 보호를 위해 드론 라이브 포렌식(Live Forensics)도 고려해야 한다. 드론 라이브 포렌식을 위해서 DJI 社와 같은 상용 드론은 정식 SDK를 통해 저장된 비행 데이터에 접근할 수 있지만, 오픈소스 드론의 경우 Mavlink 및 Fast-RTPS(DDS)를 통한 uORB 메시지 통신을 통해 데이터 추출이 가능하다. 본 연구에서는 활성화된 오픈소스 기반 드론에서 데이터를 추출할 수 있는 도구를 제안하고 검증한다.

3.4.1 LiPFo(Live-PX4-Forensic) 연구배경

오픈소스 기반 드론에서 주로 사용하는 PX4는 비행 제어 관련 스택과 내·외부 인터페이스 접근 및 페이로드 장치를 관리하는 미들웨어 스택으로 분류할 수 있다. 비행제어 스택은 주로 조종 명령 값과 현재 자세 값을 활용한 PID(Proportional, Integral, Derivative) 제어, 모터 구동 등 비행 관련 임무를 수행한다.

미들웨어 스택은 오픈소스 로봇 운영체제(ROS2, Robot Operating System 2)와 유사하다. 명령 값에 따른 기체의 비행, 미션 수행과 같은 기능을 제공하기 위해서는 해당 하드웨어 설계부터 드라이버 작업까지 방대한 작업이 필요하다. 하지만 로봇 운용 체제는 하드웨어에 의존하지 않고, 공개된 다양한 센서와 하드웨어를 활용하여 최소 실행 단위로 나누어진 노드 간 통신을 통해 동작한다. 프로세스 단위로 실행되기 때문에 오류검출과 디버깅이 용이하다.

이러한 미들웨어 구조를 지니는 드론 플랫폼은 메시지 통신기반의 라이브 포렌식 방식을 적용할 수 있다. 드론 플랫폼의 활성 상태에서 내부정보를 추출하는 방법은 SD카드의 마운트 해제로 인한 증거 훼손 문제, 사고조사의 신속성, 재연성 그리고 신뢰성을 강화할 수 있다.

오픈소스 기반 비행 데이터는 Fig. 4와 같이 Database, Parameters, Logging 아래, 각각 dataman, param, logger 모듈에 저장한다. 각 모듈은 Mission 데이터, Geofence 데이터, 비행데

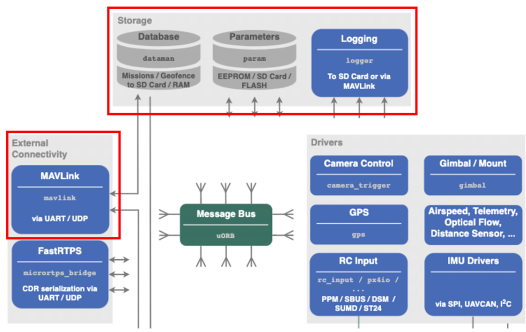

Fig. 4. Mavlink Path for Data Access

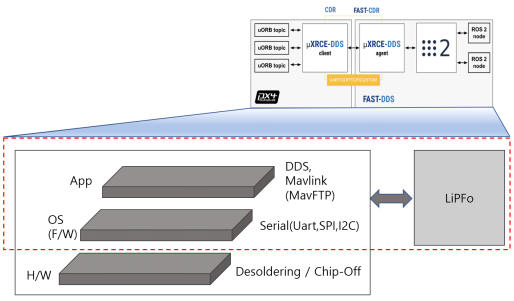

Fig. 5. Proof of Concept for LiPFo

이터 등은 uORB메시지 통신을 통해 SD카드, EEPROM 및 Flash에 저장되고 Mavlink를 통해 접근할 수 있다.

LiPFo 구조는 Fig. 5와 같이 운영체제에서 지원하는 시리얼 통신을 기반으로, Mavlink 프로토콜 Mavftp(File Transfer Protocol)을 활용하거나 PX4의 미들웨어 스택 Fast-RTPS(DDS) 기반의 데이터수집 노드를 활용하는 것이다. 만약 Mavftp 기능을 제한하도록 설정된 경우에는 별도 데이터 수집 노드를 이용해야 한다.

3.4.2 LiPFo 개발방안

PX4는 Nuttx 기반의 RTOS(Real-time Operating System)에서 동작하여 nsh(Nuttx shell)을 통해서 접근할 수 있다. 파일시스템에 접근한 결과 Nuttx 파일시스템 구조와 유사하다는 것을 확인하였다. 비행 데이터는 임무(Mission), 설정(Param), 로그(Logging) 등 총 세 가지로 분류되고 데이터셋이 저장되는 디렉터리 경로를 Mavftp를 통해 그대로 복제하는 방안을 모색하였다. 신속한 비행 데이터 획득을 위해서 로그 데이터(Logging module)를 중점으로 DFS(DepthFirstSearch) 기반의 신속 추출을 개념검증의 목표로 하였다. 이는 Mavftp의 Opcode 명령에 기반하여 비교적 신속하게 필요한 데이터만 추출할 수 있다.

Mavftp는 PX4 드론 기체 내 Mavlink 모듈 내에서 동작하며, Fig. 6과 같이 기존 FTP 프로토콜과 유사하게 데이터 읽기, 쓰기, 삭제, 생성, 수정 그리고 디렉터리 삭제도 가능하다.

Mavftp 메시지 페이로드 내 Opcode를 목적에 맞게 활용하여 추출 도구의 명령 값을 지정할 수 있다. 예를 들어, Fig. 7과 같이 OpenFile 명령을

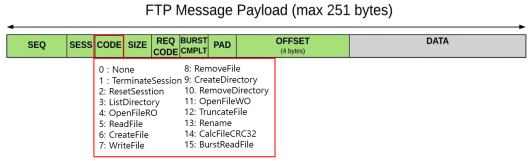

Fig. 6. Mavftp Message Payload

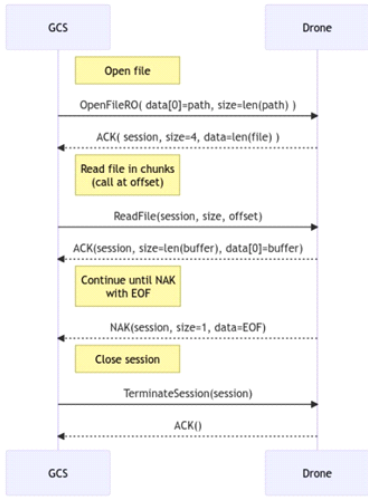

Fig. 7. Mavftp Operation Sequence

요청하면 클라이언트인 드론 기체는 Mavftp의 데이터 교환 규칙에 따라 데이터 통신이 가능하다.

Mavftp를 통한 내부 데이터 획득 기능을 검증하기 위해 Fig. 8과 같이 CLI(Command Line Interface) 기반의 자동화된 라이브 포렌식 도구 LiPFo(Live-PX4-Forensic)를 개발하였다. 포렌식 절차 가이드라인을 반영하기 위해 CLI 프레임워크인 Sploitkit를 적용하여 로그 데이터 획득을 수행한다.

LiPFo는 Use-Set-Run의 단계로 포렌식 수행 환경을 구성하고 추출 및 무결성 검증을 수행한다. Use 명령은 수행하고자 하는 포렌식 임무를 설정하는 단계로 기능선택, 무결성 검증 기능을 포함한다. 추후 완전 추출기능 및 비행 데이터 융합 등 목적에 따라 기능 확장이 가능하다. Set 명령은 Use 명령을 기반으로 하드웨어 인터페이스 호환성, 대상 기체 등 수행 환경을 재확인 후, 수행 직전 상황에 대한 정보와 수행 예정 내용을 표시한다. 최종적으로 Run 명령은 앞서 Use와 Set 환경 구성에 따라 데이터를 추출한다.

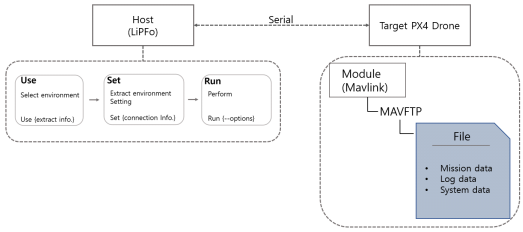

Fig. 8. Execution Process and Environment of LiPFo

3.4.3 LiPFo 추출 실험

LiPFo 검증을 위해 PX4 기반의 드론이 활성화된 상태에서 추출실험을 진행하였다.

- ○ 드론 H/W : Pixhawk CUAV V5 Nano, Pixhawk 6
- ○ SD 카드 : Sandisk Ultra 계열
- ○ Host PC: Ubuntu 22.04 LTS

Fig. 9는 LiPFo의 show 명령으로 지원하는 기능 모듈과 추출과정을 나타낸다. SD카드 제거 없이 활성 상태 드론의 로그 데이터만을 추출하는 실험을 진행하였다. Use 명령으로 신속 추출기능을 선택하고, Set 명령으로 외부 인터페이스(Serial)를 재확인한다. Run 명령 후 추출된 폴더 구조 및 데이터는 Fig. 10과 같이, 식별한 PX4 파일시스템 구조와 동일한 디렉터리 복제를 확인할 수 있다. 추출된 데이터 중에서 /log 폴더 내 추출된 ulg 로그 파일을 pyulog 도구로 주요 정보를 분석하였다. pyulog 도구를 이용하면 비행 컴퓨터의 하드웨어

Fig. 9. The example of extraction Process using LiPFo

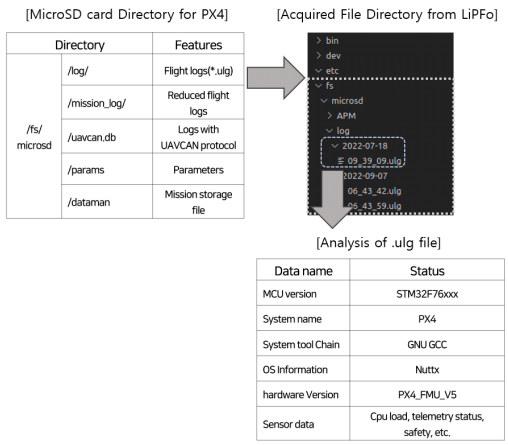

Fig. 10. The Result from LiPFo Extraction

정보, 운영체제 정보를 포함하여 각종 센서값, 사용 전력 값, 비행 위치 등 다양한 정보를 신속하게 확인할 수 있다. 증거제출을 위한 로그 파일의 무결성을 보장을 위해 일방향 암호화 방식을 적용할 수 있다. /dev, /obj, /bin 은 데이터 추출은 가능하지만 정확한 데이터 분석까지 자동화하기 위해서는 추가적인 연구가 필요하다.

3.5 제안하는 드론 포렌식 방법론

상용 통합도구와 오픈소스 도구 그리고 라이브 포렌식 도구를 적용한 드론 포렌식 방법을 Fig. 11에 도식화 하였다. 제안하는 방법론은 다양한 드론 플랫폼, 포렌식 도구 간 교차검증, 포렌식 수행 시점 등을 세분화하여 실용적인 드론 포렌식 가이드라인 수립을 목표로 한다. 오픈소스 기반 드론의 경우 LiPFo 적용을 통한 라이브 포렌식 방안을 포함하여, 기체 및 칩 분해 이전에 수행 가능한 신속한 데이터 획득 방안을 반영하였다.

3.5.1 가상 시나리오 기반 분석

제안하는 Fig. 11의 드론 포렌식 방법론을 가상의 시나리오 기반으로 검증하였다. DJI 계열의 드론 및 조종기를 획득한 경우, 오픈소스 기반 드론을 획득한 경우 그리고 비행 데이터만 획득한 경우를 분류하여 분석하였다.

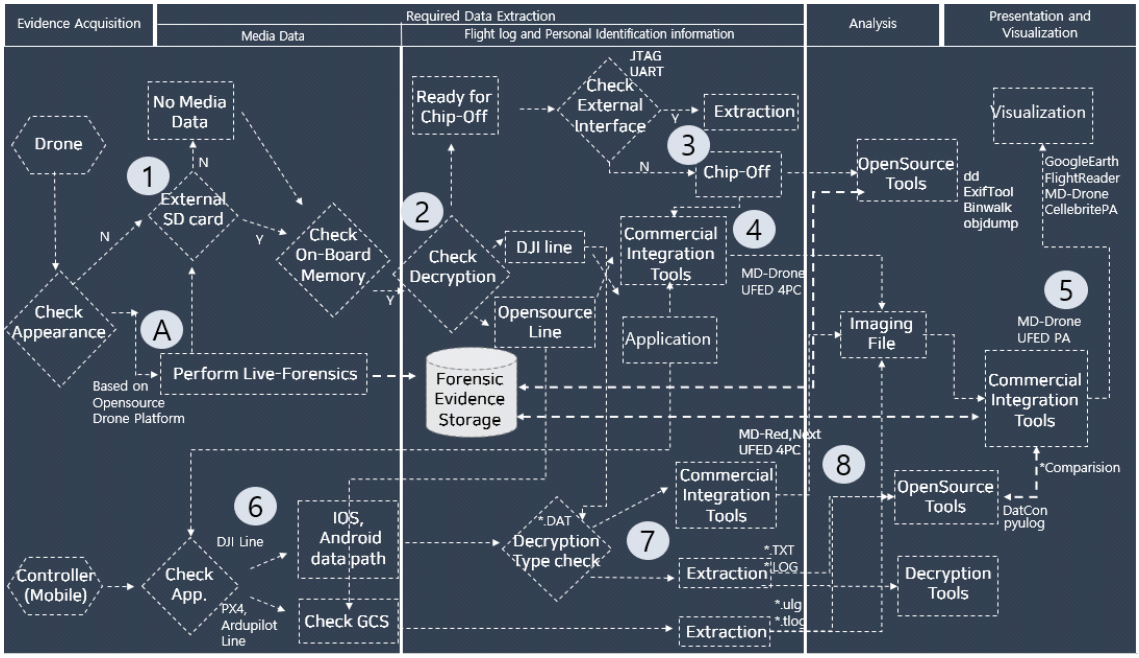

Fig. 11. The Proposed Drone Forensic Methodology

3.5.1.1 DJI 드론 기체 및 모바일(조종기) 대상

DJI 계열의 드론과 조종기 모두 획득한 경우를 가상으로 설정하였다. Fig. 11의 Evidence Acquisition 단계를 시작으로, 외부 상태 확인을 통해 DJI 계열 드론임을 확인하고, 비행 데이터 분석이 가능한 기종인지 파악한다. Fig. 11과 같이, ①번 지점에서 드론 기체 외장 SD카드 유무를 확인하고 SD카드가 없음을 확인하였다. 외장 SD카드가 없는 경우, 기체에서 획득할 수 있는 비행데이터(DAT)와 미디어 데이터를 모바일기기(조종기) 혹은 내장 메모리에서 획득해야 한다. ②번 지점은 기종 파악을 통해 복호화 가능 여부를 판단하는 단계로써, 내장형 메모리를 확인하여 내부 데이터가 존재하는지 확인한다. 상용 통합도구와 DatCon을 기반으로 복호화 가능 여부를 재확인하고, 복호화가 불가한 최신형의 DJI 기종으로 식별하였다. 복호화 가능 기종의 경우, 상용 통합도구를 활용하여 모바일 기기와 기체 내부메모리에서 추출한 이미징 데이터 획득이 가능하다. 복호화 불가 기종의 경우, 메모리 칩 제거후 eMMC 추출 도구를 사용하여 데이터를 획득해야 한다. 칩 제거를 한 이후에는 복구가 어려우므로 칩 제거 이전에 외부 통신 인터페이스(Uart, SPI 등)를 활용하여 데이터 복구 방안도 반드시 확인해야 한다[4]. ③번 지점에서는 메모리 칩 제거 이후 통합도구를 사용하여 추가 데이터를 획득한다. ④번 지점에서 획득한 데이터와 모바일 기기에서 얻은 데이터는 상용 통합도구를 활용하여 증거 스토리지에 저장한다. 이를 기반으로 ⑤번 지점에서 통합도구 내 사건 재연과 시각화 분석을 수행한다.

모바일 기기(조종기)의 경우에는 상용 통합도구를 활용하여 기체에서 획득한 비행 로그 데이터와 미디어 데이터를 융합한다. ⑥번 지점과 같이, 모바일 기기와 어플리케이션 정보를 통합도구와 연동시킨다. ⑦번 데이터 복호화 과정과 ⑧번 데이터 융합과정을 통해 하나의 융합된 이미징 파일을 생성하고 증거 스토리지에 최종 저장한다.

3.5.1.2 오픈소스 기반 드론 대상

오픈소스 기반의 드론 기체 획득을 가정하였다. 외부 SD카드가 있음을 확인, 데이터 손상 및 증거 훼손을 방지하기 위해, SD카드를 바로 제거하지 않고, Fig. 11의 A 지점과 같이 라이브 포렌식 도구(LiPFo)를 사용하여 열린 포트 및 Mavftp 지원 여부를 스캔하였다. 대상 드론이 Mavftp를 지원하여, LiPFo의 신속 비행 로그추출 기능을 통해 Ulog 파일을 추출하였다. 이후 기체 전원을 차단하

고 외부센서 및 페이로드를 식별한다. 상세 데이터 획득을 위해 SD카드를 제거하고 드론 포렌식 통합 도구와 오픈소스 도구를 활용하여 데이터 추출을 수행한다. 통합도구 활용 시 미디어 데이터와 비행 데이터를 통합한 이미징 데이터 획득이 가능하므로, 통합도구를 우선적으로 사용한다. 4번 지점의 통합도구로 획득한 이미징 데이터를 교차 검증하기 위해 오픈소스 기반 도구 pyulog, plotulog 분석결과를 비교한다. 사이버 공격 여부 및 사고 원인분석을 위해서 조종 값(명령 값) 대비 물리적 궤적 비교, GPS 등 외부 센서의 무선신호 특성 변화, 모터 변속 모듈(ESC, Electronic Speed Control) 피드백 기록 등의 구체적인 분석을 진행한다.

3.5.1.3 비행 데이터 관련 파일 획득

특정 통합도구의 이미징 파일 또는 비행 로그로 추측되는 파일만 수집한 경우, 파일 확장자를 식별하여 해당 포렌식 도구로 분석한다. 상용 통합도구는 기체나 모바일 기기에 물리적으로 연동한 경우에만 데이터 추출과 이미징 작업이 가능하고, 통합도구 간 상호 이미징 파일 교환은 불가능하다. 상용 통합도구의 경우 각 도구 내 추출 절차부터 진행이 되어야 자체 이미징 파일로 관리하기 때문에, 비행 데이터 관련 파일만 획득했을 때는 오픈소스 도구 적용이 적절하다.

IV. 결 론

드론 포렌식 방법론 연구는 특정 드론을 대상으로 비행 로그를 추출하는 방식의 방법론을 제시하였다. 본 연구에서는 드론 포렌식을 위한 상용 통합 도구, 오픈소스 도구, 라이브 포렌식 도구를 접목하여 다양한 드론 기종에 알맞게 적용할 수 있는 실용적인 포렌식 방법론을 제안하였다. 여러 드론 포렌식 연구를 기반으로 포렌식 도구를 활용한 구체화된 방법론을 수립하였고, 가상 시나리오를 기반으로 실용성을 확인하였다. 또한, 드론 라이브 포렌식의 필요성을 설명하고 개념검증을 위한 도구, LiPFo를 개발하였다. 드론 라이브 포렌식 검증을 위해 개발된 LiPFo는 로그 데이터 추출을 위해 Mavlink의 Mavftp를 이용하고, 향후 PX4-FastRTPS 기반의 uORB 메시지 교환 방식도 지원할 예정이다. 제안하는 방법론은 오픈소스 기반의 다양한 무인이동체를 대상으로 적용할 수 있으며, 라이브 포렌식 도구는 활성 상태 드론에서 신속한 비행 로그추출이 가능하여, 기존 상용 포렌식 통합도구들과 차별점이 있다.

References

[1] Comprehensive Policy for Developing Scientific Criminal Investigation and Forensic Science(Ⅳ)- Review of relevant laws and policies on national security and human safety, pp543, Jan. 2022.

[2] Yonhap news, "The number of drone accidents reported by insurance companies is 704, but the Ministry of Land, Infrastructure and Transport has only identified 11 cases." yna.co.kr/view/AKR20210916095400001, Aug. 2021.

[3] Devon R. Clark, Christopher Meffert, Ibrahim Baggili, Frank Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," DFRWS 2017 USA, Volume22, Aug. 2017

[4] Junho Jeong, Beomseok Kim, Jinsung Cho, "A Digital Forensic Process for Ext4 File System in the Flash Memory of IoT Devices," pp48(8),865-870, Journal of KIISE, Aug. 2021.

[5] Yejun Kim, Jeonghyeon Gim, Seungjoo,"A Study on Systematic Firmware Security Analysis Method for IoT Devices," Journal of the Korea Institute of Information Security & Cryptology, 31(1), pp 31-49. Feb. 2021

[6] A. Al-Dhaqm et al., "Digital Forensics Subdomains: The State of the Art and Future Directions," IEEE Access, vol. 9, pp. 152476-152502, Oct. 2021.

[7] T. E. A. Barton and M. A. Hannan Bin Azhar, "Forensic analysis of popular UAV systems," 2017 Seventh

International Conference on Emerging Security Technologies (EST), Canterbury, UK, Sep. 2017

[8] M. Yousef and F. Iqbal, "Drone Forensics: A Case Study on a DJI Mavic Air," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, pp. 1-3, Nov. 2019.

[9] J. K. W. Lan and F. K. W. Lee, "Drone Forensics: A Case Study on DJI Mavic Air 2," 2022 24th International Conference on Advanced Communication Technology (ICACT), PyeongChang Korea, Republic of, pp. 291-296, Feb. 2022.

[10] M. Yousef, F. Iqbal and M. Hussain, "Drone Forensics: A Detailed Analysis of Emerging DJI Models," 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, pp. 066-071, Apr. 2020.

[11] H. Bouafif, F. Kamoun, F. Iqbal and A. Marrington, "Drone Forensics: Challenges and New Insights," 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, pp. 1-6, Apr. 2018.

[12] Azhar, H., Barton, T. and Islam, T. "Drone forensic analysis using open source tools" Journal of Digital Forensics, Security and Law. 13 (1), pp. 7-30, May. 2018.

[13] Mantas,E., Patsakis,C. "GRYPHON: Drone Forensics in Dataflash and Telemetry Logs" Advances in Information and Computer Security. IWSEC, vol 11689, July. 2019.

[14] B. K. Sharma, G. Chandra and V. P. Mishra, "Comparitive Analysis and Implication of UAV and AI in Forensic Investigations," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, pp. 824-827, Apr. 2019.

[15] Chi-Cheng Yang, Hsuan Chuang, Da-Yu Kao, "Drone Forensic Analysis Using Relational Flight Data: A Case Study of DJI Spark and Mavic Air", Procedia Computer Science, Volume 192, pp 1359-1368, Oct. 2021.

[16] Stanković, M.; Mirza, M.M.; Karabiyik, U. "UAV Forensics: DJI Mini 2 Case Study", Drones 2021, 5, 49, June. 2021.

[17] Youngwoo Lee, Juhwan Kim, Jihyeon Yu, Joobeom Yun, "Classification of DJI Drones Based on Flight Log Decryption of DJI Drones Based on Flight Log Decryption Method," Journal of the Korea Institute of Information Security & Cryptology, 32(1),pp 77-88, Feb. 2022.

[18] Youngbeen Yoo, Jinsung Cho, "A data extraction and analysis tool for PX4 Autopilot," Proceedings of the Korean information Science Society Conference, pp. 1709-1711, Dec. 2022.

[19] Jeon Sohn, Jinsung Cho, "Access Control and Integrity Schemes in PX4 Autopilot," Proceedings of the Korean information Science Society Conference, pp. 1700-1702, Dec. 2022.

〈저자소개〉

백 세 영 (Seyoung Baik) 정회원
2021년 7월~현재: ETRI 부설연구소 연구원
〈관심분야〉 정보보호, 시스템 보안, 드론·UAM 보안

이 상 욱 (Sangwook Lee) 정회원
2004년 2월~현재: ETRI 부설연구소 책임연구원
〈관심분야〉 사이버보안, 취약점분석·평가, 드론·UAM 보안