Drone Forensics: A Case Study on DJI Mavic Air 2

James Kin Wah Lan*, Frankie Kin Wah Lee*

*Digital & Information Forensics Centre of Expertise, HTX (Home Team Science & Technology Agency), Singapore

James_Lan@htx.gov.sg, Frankie_Lee@htx.gov.sg

Abstract— **With the inundation of more cost effective and improved flight performance Unmanned Aerial Vehicles (UAVs) into the consumer market, we have seen more uses of these for both leisure and business purposes. As such, demand for digital forensic examination on these devices has seen an increase as well. This research will explore and discuss the forensic examination process on one of the more popular brands of UAV in Singapore, namely DJI. The findings are from the examination of the exposed File Transfer Protocol (FTP) channel and the extraction of the Data-at-Rest on the memory chip of the drone. The extraction was done using the Chip-Off and Chip-On technique.**

Keywords— **DJI, Mavic Air 2, FTP, Drone Forensics, Unmanned Aerial Vehicle**

I. INTRODUCTION

With the reduction in cost and enhanced flight performance of the newer Unmanned Aerial Vehicles (UAVs), there is a growing interest for individuals and companies to explore the use of this device for leisure and business purposes. Individuals could use this to explore and capture aerial views of places they could never reach and new business opportunities opened up for business owners. A popular UAV maker, DJI, has produced a range of UAV models over the years for this consumer segment. The most popular drone models are the Mavic and Phantom series.

With the improved capabilities and performance, these drones have been exploited by people with ill intent to commit offensive acts like trespassing the No-Flight Zone and trafficking of forbidden goods or items. The advanced features of the drone help to conceal their notorious acts and make identification of the flight operator challenging [1] [2].

A digital forensic examination on a drone is normally done on the aircraft, the remote control device and the application on the mobile phone as well as the computer for any data related to an incident. The related data can be obtained from the File Transfer Protocol (FTP) channel through the USB port of the aircraft and the data stored on the mobile phone by the DJI flight application. Another common location of data is in the on-board SD Card [3]. The wealth of flight-related information is primarily stored in the aircraft on-board flash memory. These data are normally extracted through rooting the aircraft or exploiting the vulnerability of the FTP service in the older firmware. However, for the FTP service of the newer DJI drone models, namely the Mavic Mini and Mavic Air 2, we found that the FTP service is leveraging on the Trusted Zone for encryption/decryption keys generation. This presents a challenge for forensic examiners, as they need to clear an additional layer of hardware-enabled security before they could proceed with the examination on and analysis of the data.

The purpose of this study is to present the findings on an incident that involved a DJI Mavic Air 2 with a newer firmware that has utilized the trusted zone. The study documented the process, which included locating and accessing prominent artifacts from the drone. The objective of this paper, therefore, is to provide new insights and knowledge for the digital forensic community on the UAVs. The paper is presented in the following order: Section 2, a literature review on the current drone forensic methodologies. Section 3, discussion on problem statement and contributions. Section 4, proposed forensic methodology on examination of Mavic Air 2. Section 5, discussion on the experimental forensic examination results of Mavic Air 2 and Section 6, conclusion with a summary of key findings and recommendations for future follow-up/enhancement.

II. LITERATURE REVIEW

There has been an increase in the number of studies into drone forensics as the offering of hobbyist drones is on the rise. Hamdi et al. [4] and Yousef et al. [5] shared their technical study on conducting forensic examination on DJI drones, namely DJI Phantom 4 and DJI Mavic Air respectively. Both studies shared results and learning points relating to the on-board SD card, DJI Go Application, mobile phone that housed the DJI Go Applications, and DJI Assistance software.

For the general drone forensics that caters for a wider segment of UAV, Jain et al. [6] proposed a drone forensic framework that includes identification, examination and analysis of general drones. In addition, the INTERPOL has also published a framework for responding to a drone incident for the first responders and digital forensic practitioners. The framework provides details on the identification and the handling and some common forensic tools that are available for a more reliable examination.

Fadilah et al. [7] proposed a drone attack tool for a vulnerability assessment of the wireless channels, Global Positioning System (GPS) and Radio in the drone. Despite primarily targeting the DJI Mavic 2 Pro, the vulnerability assessment can be extended to other generic drones. It showed the vulnerability through side channel attacks, mainly with the relay attack and the hijacking commands. This vulnerability is crucial as individuals with ill intent could exploit it. In a drone network, there are connections between the aircraft, remote control device and the mobile phone that hosts the drone

application. Temporal relationships between different data sources from the drone network were analyzed and presented by Kao et al. [8]. They explored the impact of the timing in the transmitting and receiving of data between these sources in a forensic examination of DJI Spark drone.

These studies on the drone flight data relied fundamentally on obtaining the root (administrator) access to the operating system. The common path of attack vector is to exploit the vulnerability of FTP service exposed on aircraft USB port. The primary role of FTP is to upload and download data files. In order to manipulate the operating system services, the next path of exploitation is to enable command channel through Android Debug Bridge (ADB). The operating system inside the DJI drone is commonly a variant of Android. The flight data, the DAT files, were encrypted by the system when retrieved from the FTP channel. To our best knowledge, currently there is no public avenue available to decrypt the flight data of the newer DJI drone models.

III. Problem Statement And Research Contributions

The artifacts of the DJI Mavic Air 2 available for the forensic examination of this study are:

1. A damaged DJI Mavic Air 2 drone, with an unidentified operator, was found and brought to the regional digital forensic laboratory for digital forensic examination.
2. Encrypted Drone flight data DAT logs found in an external storage.

The key contributions of this study are:

1. The process/methodology to obtain flight data from the drone internal storage.
2. An analysis of the encryption format of the flight data to identify the original drone that generated the flight data and establishment of a relationship between encrypted flight data DAT logs found in an external storage and the Drone.
3. A detailed discussion on the evaluation and results of the forensic examination on the FTP service exposed on the aircraft USB port.

IV. Methodology And Implementation

To perform a forensic examination on the damaged DJI Mavic Air 2, firmware V01.00.0250, a wide spectrum of engineering equipment and software tools were used. The hardware tools used were:

1. 2-D and 3-D X-Ray machine
2. In-System Programming toolkit
3. Flash memory programmer

The software tools used were:

1. DatCon and CsvView
2. EnCase Forensic / FTK Imager
3. Compact Forensic Imaging Device (CFID)

A. Scenario Description

The DJI Mavic Air 2 drone was flown with the DJI Fly app using control targeted flight route. There were two sets of flight routes being created: the first set was the successful flight route. The flight data DAT file of this flight route was downloaded using DJI Assistance 2 for Mavic, version 2.0.12. The second set was flown with DJI Fly app and a crash landing was simulated due to some physical obstacles. As a result, the drone suffered physical damages, rendering it inoperative.

B. Acquisition of Done Data from the On-Board Storage

The damaged drone was unable to connect though the USB port to the computer installed with DJ Assistance 2 software. The drone was dismantled and the core motherboard was located. The flash memory chip was located and identified. This was a crucial step as it enabled the forensic examiners to source the corresponding technical data sheet of the memory chip and read relevant data points of the chip.

The data sheet revealed that the memory chip was a 16GB embedded Multi-Media Card (eMMC) with the 153 Ball Pin Configuration. The subsequent step was to trace the circuit schematic of the core motherboard linked to the connection points of the memory chip. To ease the tracing of circuit tracks, a 2-D and 3-D X-Ray was taken over the region covering the memory chip as shown in Figure 1. With the connection points identified, the data could be read off the memory chip directly or by using the In-System Programming. The data acquisition on the damaged drone was done with the chip-off and chip-on techniques. The details are shown in Figure 2.

Table I below lists the connection points to the eMMC memory storage chip. These connection points were used in the chip-off or chip-on technique to obtain data from the storage.

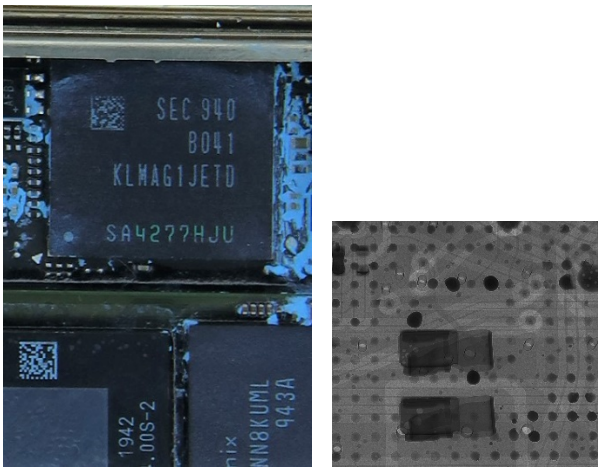

Figure 1. KLMAG1JETD-B041 model eMMC storage and 2D X-Ray image of core motherboard

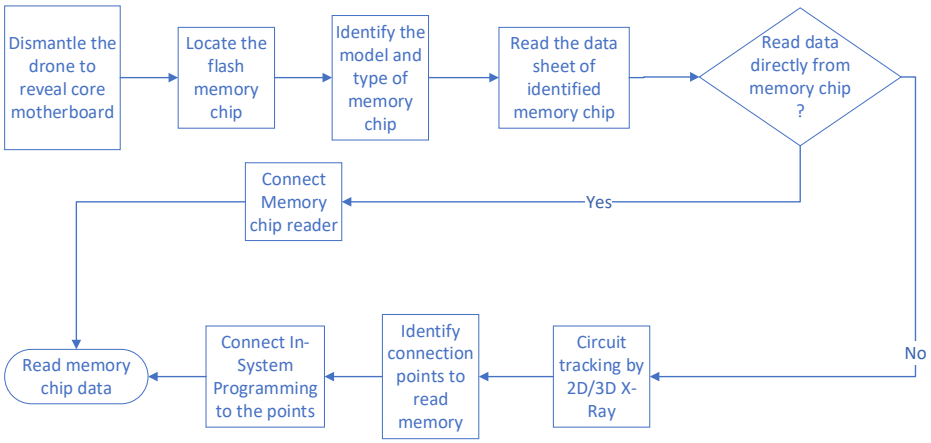

Figure 2. Our data acquisition methodology based on the Chip-Off and Chip-On technique

TABLE 1. CONNECTION POINTS FOR EMBEDDED MULTI-MEDIA CONTROLLER (EMMC) MEMORY STORAGE CHIP

Points	Type	Description
D0 – D7	Data 0 to Data 7	Data In/Out
CLK	Clock	Clock Signal
CMD	Command	Command instructions and device initialization
Vcc	Voltage	Voltage supply for flash memory
Vccq	Voltage	Voltage supply for memory controller
Vss	Ground	Grounding for connection points

C. Acquisition of Data from the external Micro SD Card storage

The external micro SD card found on the drone was connected to the SD Card reader through a write-blocker. The data of SD card were obtained using the EnCase acquisition software. This software enabled a physical acquisition of both logical and deleted data (complete data).

V. EXAMINATION RESULTS

The importance of the artifacts from the drone was to locate and determine the flight paths taken before the landing on the place of the event. This information could assist with the identification of the possible flight route, which could include that of a trespassing on a sensitive zone. Another purpose of this information was to provide some clues into the original place of which the drone took off. The file names of flight data were FLYxxx.DAT where xxx were the sequential incremental numbers and the DAT files were binary encoded using DJI LOG V3. The encoded DAT files were decoded and translated into human-readable format using DatCon and Compact Forensic Imaging Device (CFID).

A. On-Board Storage

The acquired data were processed by the standard computer forensic software, EnCase. We discovered the media files, such as photographs, taken during the simulated flight, could provide leads for identification of the owners and the whereabouts of the take-off site. They could also serve as a complement finding to the flight data DAT files. The standard forensic examination methodology on image forensic was conducted on these media for Exchange Image File Format (EXIF) metadata to extract data related to the event. Table 2 summarizes the important data after analyzing the storage for forensic values.

TABLE 2. IMPORTANT FORENSIC VALUES AFTER ANALYZING THE STORAGE

Name	Type	Forensics Elements
Blackbox	Folder	Base folder that stores drone flight information
System	Folder	Stores operating system information such as running and startup processes
Upgrade	Folder	Information on firmware upgrading
Logs	File	Stores system, process and disk details
FTP	File	Start time, commands and logon information of FTP transfer
Board Serial Number	File	Identification of drone core board. This is different from the drone serial number.
Camera senor serial number	File	Identification of drone camera.

One of the crucial purposes for the forensic examination was to address the question on the time of the event. For this purpose, the acquired data were processed by timeline analysis. Figure 3 shows that majority of the activities were congregated around June to July 2020. A further examination was done and it was discovered that the activities were carried out between 26 June and 1 July 2020 specifically as shown in Figure 4. The activities timeline artifacts have assisted to narrow the scope of the examination resulted in a faster response for the triage and the reduction of time in searching for any digital forensic leads.

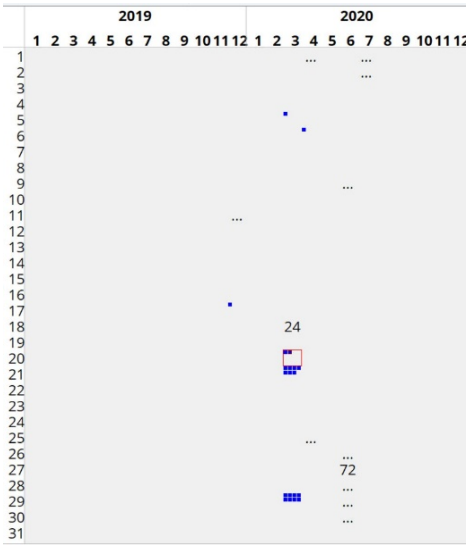

Figure 3. Drone activities for June and July 2020

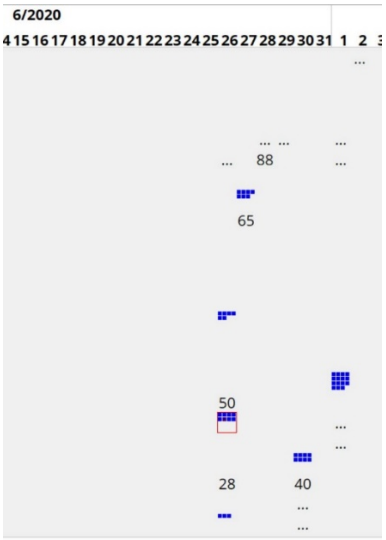

Figure 4. Drone activities between 26 June and 1 July 2020

B. External Micro SD-Card

The data acquired from the external micro SD card were processed with the EnCase forensic software. The analysis of the processed data for the photographs and video was identical to those of the standard computer forensics. Some EXIF information such as the camera model, FC3170, which is the camera for the DJI, the DJI build version 10.00.13.23 and other useful information such as the GPS of the flight coordinates were discovered. The most crucial piece of forensic information from the media storage was the camera sensor serial number, which was instrumental in establishing the relationship of the media to the drone when they were obtained from a different location.

C. FTP Service

Another possible way to locate and identify the link between the drone and the drone's owner is through the flight data DAT files downloaded by the DJI Assistance application or the manual FTP commands. The flight data DAT files were encrypted when they were extracted from the FTP or the DJI Assistance application. This finding was different from the older DJI drone models. The difference was due to the encryption process for the FTP service performed on the two different firmware. The older firmware that leveraged on the Busybox FTP service was susceptible to the FTP transverse vulnerability whereas the newer FTP service is leveraging on the Trusted Zone for encryption process. The newer FTP service on the DJI Mavic Air 2 firmware V01.00.0250 was examined by conducting reverse engineering with both the dynamic and static analysis. The reversing software used in the static analysis were IDA Pro and Ghidra software. For dynamic analysis, the FTP service was executed on the Android ARM emulator and on the Raspberry Pi board. To ensure a better control of the flow and the examination process of the data, we hooked the FTP service to IDA Pro and closely monitored the execution behaviour and the memory environment of the DJI drone services.

D. Encryption Process on the Drone

On the DJI Mavic Air 2 drone, the file data encryption function is not pre-set but is determined by the data and the folder when there is a request for FTP downloading. The temporary folder and the file that store the total number of files in the folder are unencrypted thus it will not be subjected to file data encryption in the Trusted Zone. The rest of the files will be encrypted. For any downloading of files to occur, the FTP RETR command must be issued by the FTP client or the DJI Assistance software from the computer to the drone over a USB transfer.

The file data encryption is performed through Advanced Encryption Standard (AES) using a random seed encryption key (RSEK). A random seed is used to generate the RSEK. The RSEK is the "password" used as the input to the AES encryption. The Trusted Application (TA) in the Trusted Zone generates both random seed and RSEK. The random seed is a string of 16 bytes randomly generated to encrypt each file data. Therefore, the random seed is unique to each individual downloaded file. There is no requirement for the user to enter a password for the AES encryption on the DJI Assistance or the FTP commands. After the file data is encrypted, the board serial number of the drone and the 16 bytes random seeds are appended to the encrypted file. There is no change in the file name and file extension. Figure 5 shows the flowchart of the file data encryption for the FTP service between the drone and the DJI Assistance.

E. Encrypted Flight Data File

The study also examined the encrypted flight data file in an attempt to establish a link between the file found in an external storage and the drone. From the static code analysis and dynamic testing of the FTP service, it was discovered that the board serial number and the model of the drone were recorded in the header of the encrypted file as shown in Figure 6. The decoded formats of the file header are shown in Table 3.

TABLE 3. DECODED FORMATS OF THE FILE HEADER

Name	Type	Forensics Elements
Size of header: 160 bytes	-	-
LOGH	File header "magic number"	DJI log file signature
WM231	Drone model	Identification of drone mode that flight data was taken out.
1TGCH123456789	Board serial number	Identification of drone core board. This is different from the drone serial number.
AB D6 54 E8 5D D7 7B E9 C6 BB EC 92 F9 D5 72 36	Random seed	For AES encryption and decryption

The knowledge of the drone model will help to narrow the scope to identify the owner of the flight data. This is done by matching the drone model to the database of owners who have possession of that model of the drone. This, in return, could provide new examination leads to the drone of interest. As mentioned before, the board serial number of the drone can be identified. This could potentially help to identify the owner of the drone. The board serial number has provided this crucial information to establish the link.

VI. CONCLUSION AND FUTURE WORKS

This paper has provided a forensic examination methodology and an in-depth discussion on the DJI Mavic Air 2 drone and the FTP service. It has also presented the discovery of the forensic values on the drone's artifacts as well as the encrypted flight data DAT file. The novel contribution of this study is the discovery of the board serial number that is critical in identifying the owner of the drone. This was done by establishing the connection between the encrypted flight data file and the drone. It is our hope that these findings would provide more clarity in and help to streamline the process of the drone digital forensic examination. Our study has focused on the drone aircraft of DJI Mavic Air 2, any future work could have more in-depth forensic examinations conducted on the remote control device, and the application on the mobile phone. Furthermore, the current encrypted flight data DAT file poses a technical challenge to the forensic examination. Therefore, additional studies into the encryption and decryption of encrypted flight data DAT file using Trusted Zone is required to provide more insights in this aspect. While our study was on DJI Mavic Air 2, the Chip-Off and Chip-On data acquisition technique, this methodology is also applicable to other DJI Mavic drone models such as DJI Mavic Mini and Mavic 2 Pro. Therefore, future forensic examinations could also focus on these DJI Mavic drone models.

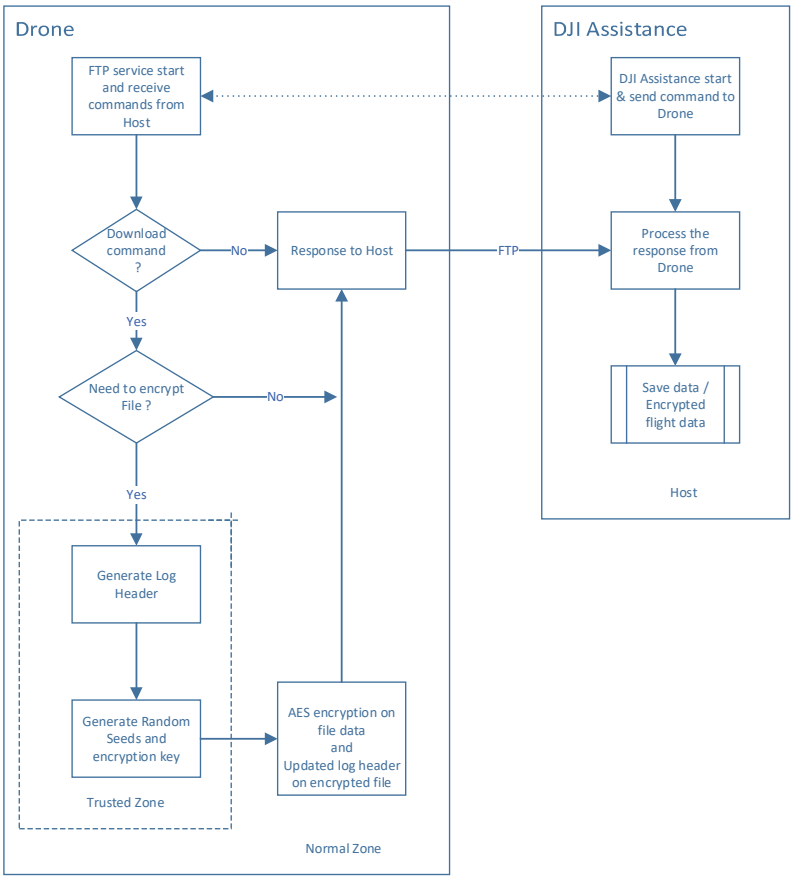

Figure 5. Flowchart of the file data encryption for FTP service

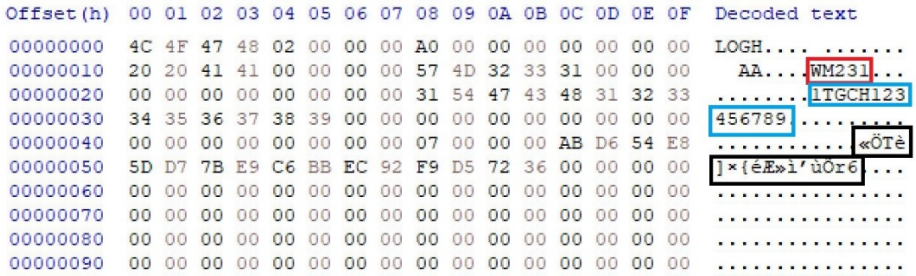

Figure 6. Header of encrypted flight file data

REFERENCES

[1] 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, 2018, pp. 1-6, doi: 10.1109/NTMS.2018.8328747.

[2] 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, 2020, pp. 066-071, doi: 10.1109/ICICS49469.2020.239530.

[3] *"VTO Inc - Drone Data Set", Computer Forensic Reference Data Sets*, 2018. [Online]. Available: https://www.cfreds.nist.gov/drone-images.html [Accessed: 01 October 2020].

[4] D. A. Hamdi, F. Iqbal, S. Alam, A. Kazim and Á. MacDermott, "Drone Forensics: A Case Study on DJI Phantom 4," *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, Abu Dhabi, United Arab Emirates, 2019, pp. 1-6, doi: 10.1109/AICCSA47632.2019.9035302.

[5] 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, 2019, pp. 1-3, doi: 10.1109/AICCSA47632.2019.9035365.

[6] U. Jain, M. Rogers and E. T. Matson, "Drone forensic framework: Sensor and data identification and verification," *2017 IEEE Sensors Applications Symposium (SAS)*, Glassboro, NJ, 2017, pp. 1-6, doi: 10.1109/SAS.2017.7894059.

[7] M.S. Fadilah, V. Balachandran, P. Loh and M. Chua. "DRAT: A Drone Attack Tool for Vulnerability Assessment," *2020 In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (CODASPY '20)*, New York, USA, 2020, pp. 153–155. doi: 10.1145/3374664.3379529.

[8] D. Kao, M. Chen, W. Wu, J. Lin, C. Chen and F. Tsai, "Drone Forensic Investigation: DJI Spark Drone as A Case Study," *Procedia Computer Science, Volume 159*, 2019, pp. 1890-1899, doi: 10.1016/j.procs.2019.09.361.

James received the Master of Computing (Security) from the National University of Singapore in 2009. From 2014 to 2019, he was the Officers-in-Charge / Principal Forensic Examiner with the Technology Crime Forensic Branch, Singapore, focusing on the digital forensic examination and investigation. Since 2019, he has been with the HTX (Home Team Science & Technology Agency), Singapore. He is currently the Acting Deputy Director of Digital & Information Forensics Centre of Expertise. His research interests are in the area of mobile/IoT security, vulnerability hunting and software reverse engineering. He has contributed widely to the forensic and security community through sharing, teaching and implementation of domain skills and knowledge.

Frankie received the Bachelor degree in Internet Science and Technology from University of Wollongong, Singapore in 2003. He is currently a Digital Forensics Research Engineer with HTX (Home Team Science and Technology Agency). His research interests include drone forensic, IoT devices, vehicular infotainment system and data recovery.