Analisis Forensik Drone Menggunakan Metode Clark *et al.* dan Renduchintala *et al.* (Studi Kasus: DJI Phantom 3 Standard)

Rizki Kurniandi[1)], Desi Marlena[2)], Devi Clarisa[3)],
1) Badan Siber dan Sandi Negara, rizki.kurniadi@bssn.go.id
2) Politeknik Siber dan Sandi Negara, desi.marlena@bssn.go.id
3) Badan Siber dan Sandi Negara, devi.clarisa@bssn.go.id

Abstrak

Unmanned Aerial Vehicle (UAV) atau *drone* adalah pesawat yang dimaksudkan untuk beroperasi tanpa pilot di dalamnya. Pada awalnya, *drone* dimanfaatkan untuk berbagai aplikasi yang bermanfaat, misalnya dalam hal pertahanan, penanganan bencana, pengiriman barang, dan hiburan. Tetapi, seiring dengan berjalannya waktu, *drone* disalahgunakan untuk kegiatan yang melanggar hukum seperti pelanggaran privasi maupun penyelundupan barang-barang terlarang. *Drone forensics* merupakan ilmu terkait menemukan, melakukan ekstraksi, dan menganalisis data dari suatu perangkatan yang dapat dimanfaatkan untuk mendapatkan informasi berharga untuk mendukung investigasi pada tindak kejahatan kriminal dari segi fisik maupun lingkup siber (*cybercrime*). Pada penelitian ini, dilakukan *drone forensics* menggunakan metode Clark *et al*. dan Renduchintala *et al*. pada *drone* DJI Phantom 3 Standard. *Drone forensics* yang dilakukan bertujuan untuk mengambil data-data yang terdapat pada perangkat *drone* maupun perangkat *mobile*. Hasil yang didapatkan dari penelitian ini yaitu terdapat data dari memori internal *drone*, memori *gimbal rig*, dan penyimpanan perangkat *mobile* yang dapat dimanfaatkan untuk mendukung suatu investigasi.

Kata kunci: DJI Phantom 3 Standard, *Drone*, *Drone forensics*, Metode Clark *et al*., Metode Renduchintala *et al*., *Unmanned Aerial Vehicle* (UAV)

Abstract

An Unmanned Aerial Vehicle (UAV) or drone is an aircraft that is intended to operate without a pilot on board. Initially, drones were used for various useful applications, for example in defence, disaster management, freight forwarding, and entertainment. However, over time, drones are being misused for unlawful activities such as invasion of privacy or smuggling of prohibited goods. Drone forensics is a science related to finding, extracting, and analysing data from a device that can be used to obtain valuable information to support investigations of criminal acts in terms of physical and cybercrime. In this study, drone forensics was carried out using the Clark et al. and Renduchintala et al. on the DJI Phantom 3 Standard drone. Drone forensics is carried out to retrieve data contained on drones and mobile devices. The results obtained from this study are data from the drone's internal memory, gimbal rig memory, and mobile device storage that can be used to support an investigation.

Keywords: DJI Phantom 3 Standard, *Drone*, *Drone forensics*, Clark *et al. methodology*, Renduchintala *et al. methodology*, *Unmanned Aerial Vehicle* (UAV).

1. PENDAHULUAN

Unmanned Aerial Vehicle (UAV) atau *drone* merupakan pesawat yang dimaksudkan untuk beroperasi tanpa pilot di dalam pesawatnya [1]. *Drone* dapat digunakan untuk berbagai aplikasi, seperti penegakan hukum, penanganan bencana, pengiriman, dan hiburan [2]. Selain pemanfaatan dari fungsi *drone*, terdapat ancaman dalam penyalahgunaan *drone* dimana memungkinkan digunakan untuk kegiatan kriminal, ancaman terhadap privasi, dan penggunaan *drone* untuk pengangkutan barang- barang terlarang ke dalam tahanan [3].

Terdapat beberapa kasus penyalahgunaan *drone* di Indonesia. Tahun 2016, ditemukan *drone* di area Rumah Tahanan Kelas IA Tanjung Gusta, Medan yang diduga digunakan untuk penyelundupan narkoba ke dalam rutan. Namun, petugas masih belum dapat menelusuri pihak pemilik *drone* tersebut [4]. Pada tahun 2018, terdapat temuan *drone* yang terbang di atas kompleks Lembaga Pemasyarakatan Kelas IIA Kota Magelang, Jawa Tengah. Namun, tidak diketahui siapa pemilik *drone* tersebut dan pihak kepolisian pun menyatakan tidak menerbangkan *drone* tersebut [5]. Kejadian seperti ini mendorong perlunya investigasi lebih lanjut sehingga mendorong terciptanya disiplin ilmu dalam ruang lingkup siber untuk melakukan *drone forensics*.

Digital forensics merupakan ilmu terkait menemukan, melakukan ekstraksi dan menganalisis jenis data dari suatu perangkat yang dapat diinterpretasikan untuk digunakan sebagai bukti hukum [6]. *Drone forensics* dapat dilihat sebagai bagian dari *digital forensics*, yang memiliki spesifikasi dalam mengekstraksi dan memproses informasi berharga atau bukti dari *drone* dan komponen terkaitnya sedemikian rupa sehingga entitas dan tindakan yang berkaitan dengan *drone*

tersebut dapat diidentifikasi dan dilacak [7]. Dalam melakukan *drone forensics*, hasil reportase yang baik dapat menjelaskan kronologi yang dapat menjawab pertanyaan 5W1H (siapa, apa, kapan, dimana, mengapa, dan bagaimana) untuk mengidentifikasi masalah kunci yang berkaitan dengan suatu kejahatan ataupun insiden [2]. Dengan demikian, maka metode *drone forensics* dapat diterapkan untuk penggunaan praktis dalam investigasi kejahatan atau insiden yang melibatkan *drone*.

2. LANDASAN TEORI

Bagian Landasan Teori mencantumkan teori- teori yang terkait dengan pembahasan yang diperlukan. Judul bagian ini dapat diubah menyesuaikan dengan struktur teori-teori yang disajikan.

2.1 DJI Phantom 3 *Standard System*

Dalam dekade terakhir, DJI menjadi merek drone yang populer dan banyak digunakan di kalangan komersial. Berikut ini merupakan preview dari salah satu seri drone DJI Phantom Standard yang disajikan pada Gambar 1., dimana secara umum terbagi menjadi dua bagian perangkat keras utama *mobile aircraft device* yang berisi *intelligence camera* dengan dukungan stabilizer 3-axis Gimbal dan perangkat *controller*. Untuk mengoperasikan drone DJI Phantom 3 Standard dengan berbagai fitur yang dimiliki, maka digunakan aplikasi DJI GO yang terpasang pada perangkat mobile dengan sistem operasi berbasis Android maupun iOS.

Gambar 1. *DJI Phantom Standard system* [10]

2.2 *Digital Forensics*

Digital forensics adalah penerapan sains untuk mengidentifikasi, mengumpulkan, memeriksa, dan menganalisis data bukti digital dengan tetap mempertahankan integritas informasi yang ada [11]. Berdasarkan dokumen NIST SP 800-86 [12], terdapat empat tahapan dasar dari proses forensik. Tahapan-tahapan *digital forensics* adalah sebagai berikut :

1. *Collection*
   Tahapan *collection* adalah tahapan awal yang bertujuan untuk mengidentifikasi sumber- sumber data potensial dan memperoleh data tersebut. Langkah dilakukan yaitu mengidentifikasi sumber-sumber yang memungkinkan untuk mendapatkan data, contohnya dari lokasi fisik penyimpanan data. Selanjutnya, dilakukan pengambilan data, dengan cara membangun rencana pengambilan data, pengambilan data, dan verifikasi integritas dari data yang diperoleh.
2. *Examination*
   Setelah data diperoleh, tahapan selanjutnya yaitu untuk memeriksa data (*examination*). Tahapan ini melibatkan penilaian dan ekstraksi bagian informasi yang relevan dari data yang dikumpulkan.
3. *Analysis*
   Ketika informasi yang relevan telah diekstraksi, maka data dapat dipelajari dan dianalisis untuk mendapatkan kesimpulan. Analisis harus dapat mengidentifikasi data- data yang diperoleh sehingga kesimpulan dapat diperoleh.
4. *Reporting*
   Tahapan ini adalah tahapan terakhir, dimana merupakan proses untuk menyiapkan dan mempresentasikan hasil informasi dari tahap analisis. Sebagai bagian dari proses *reporting*, analis harus mengidentifikasi masalah yang mungkin perlu diperbaiki, seperti kekurangan kebijakan atau kesalahan prosedur.

2.3 *Drone Forensics*

Drone Forensics merupakan cabang dari *digital forensics* yang berhubungan dengan pemulihan bukti digital atau data dari suatu *drone*. Dalam *drone forensics*, informasi yang dikumpulkan dari pemeriksaan forensik meliputi foto, video dari penerbangan, dan pemetaan [13]. Kebutuhan akan *drone forensics* terhadap suatu investigasi semakin bertambah. Sebuah laporan investigasi kejahatan yang baik dapat menceritakan sebuah cerita yang dapat menjawab pertanyaan 5W1H [2]. Adapun pertanyaan yang dirumuskan adalah sebagai berikut:

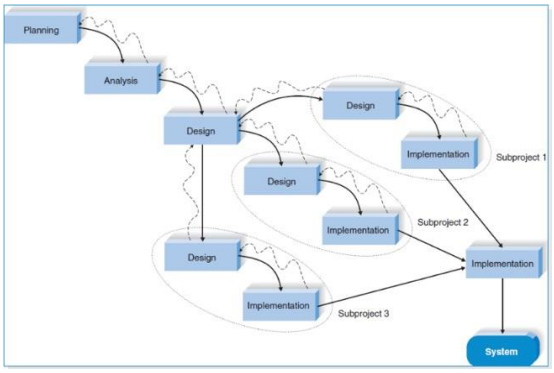
1. Siapa: Pihak terlibat dalam investigasi. Berdasarkan data penerbangan, penelitian ini bertujuan untuk mengidentifikasi pengguna *drone*.
2. Dimana: Lokasi kejadian atau lokasi terkait lainnya. Penelitian ini dapat dijawab dengan memetakan rute penerbangan.
3. Apa: Penjelasan mengenai fakta-fakta yang ada pada kejadian.
4. Kapan: Waktu kejadian dan peristiwa terkait.
5. Mengapa: Motivasi dari kejadian dan mengapa kejadian dapat terjadi pada waktu tersebut.
6. Bagaimana: Bagaimana kejadian dapat terjadi.

Enam pertanyaan ini dapat menjadi acuan bagi suatu metode *drone forensics* dapat diterapkan secara praktis dalam suatu investigasi.

3. METODE PENELITIAN

Metodologi yang digunakan pada penelitian ini yaitu *System Development Life Cycle* (SDLC) yang digambarkan pada Gambar 2. Adapun model pengembangan yang digunakan yaitu *parallel*

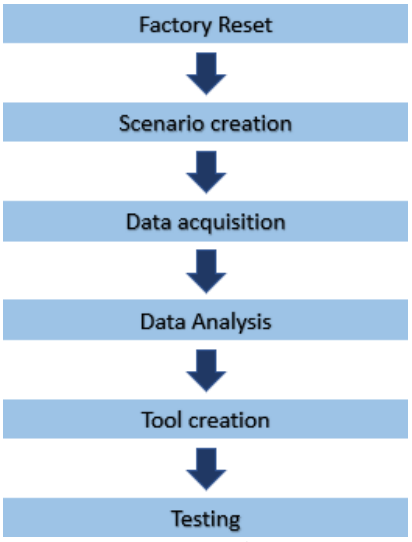
development. *Parallel development* membagi proyek menjadi serangkaian *subproject* [14]. Pada *parallel development*, penelitian dibagi menjadi tahap *Planning*, *Analysis*, *Design*, dan *Implementation*. Pada penelitian ini, penelitian dibagi menjadi dua *subproject*, yaitu *subproject* metode Clark *et al.* dan *subproject* metode Renduchintala *et al*.



Gambar 2. *Metode parallel development* [14]

3.1. *Subproject* Implementasi Metode *Drone Forensics* Clark et.al.

Pada metode yang diusulkan oleh Clark *et al*., terdapat enam tahapan yang dilakukan dalam melakukan *drone forensics* yaitu *factory reset*, *scenario creation*, *data acquisition*, *data analysis*, *tool creation*, dan *testing*. Enam tahapan pada Gambar 3. dijelaskan sebagai berikut :



Gambar 3. Diagram metodologi *drone* forensics yang diusulkan oleh Clark *et al.* [8]

1. *Factory reset*
   Tahapan ini dilakukan untuk memastikan tidak ada variabel eksternal yang memengaruhi hasil. *Factory reset* yang dilakukan meliputi *drone* dan perangkat *mobile* yang digunakan. Setelah itu, dilakukan instalasi aplikasi DJI GO pada perangkat *mobile*. Tujuan instalasi aplikasi DJI GO ini adalah untuk menyediakan *dashboard* perintah dan kendali pada *drone*.
2. *Scenario creation*
   Selanjutnya, *drone* diterbangkan pada titik tertentu. Ketika dilakukan pengujian penerbangan, maka *log* penerbangan *drone* akan tercatat.
3. *Data acquisition*
   Setelah penerbangan uji coba telah dilakukan, maka data *drone* dapat diakuisisi. *Data acquisition* dilakukan pada tiga bagian, yaitu penyimpanan SD *card* eksternal, perangkat *mobile*, dan penyimpanan *drone*.
4. *Data analysis*
   Dari data yang didapatkan, terdapat dua sumber utama data penerbangan dari *drone* DJI Phantom 3 Standard. Sumber utama ini adalah *file* TXT yang dibuat oleh aplikasi DJI GO pada perangkat *mobile* dan *file* DAT yang dibuat oleh *drone* dan terdapat pada penyimpanan internal *non-volatile drone*.
5. *Tool creation*
   Untuk penelitian yang dilakukan oleh Clark *et al*., setelah data dianalisis, maka dilakukan pembuatan *tool* yang digunakan untuk melakukan *parsing file* DAT. Tool ini bernama *Drone Open source Parser* (DROP). DROP bekerja dengan Python 3.4 dan berbasis pada *reverse engineering* DatCon. DROP dapat digunakan untuk memproses baik satu maupun banyak *file* DAT.
6. *Testing*
   Tahapan ini merupakan tahapan pengujian bagi data yang telah didapat dan diproses. Tahapan ini dilakukan untuk memvalidasi data yang telah dilakukan *parsing* dengan *tool* DROP. Konsep dari tahapan testing ini adalah untuk memeriksa apakah *file* DAT cocok dengan data TXT dari perangkat *mobile*.

3.2. *Subproject* implementasi metode *drone forensics* Renduchintala et. al.

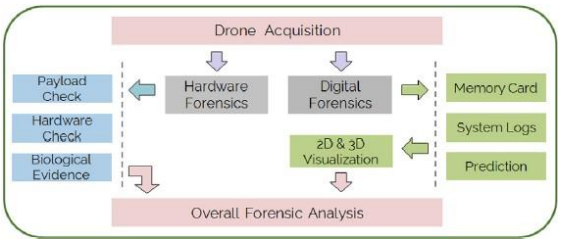
Metode yang diusulkan oleh Renduchintala *et al*., seperti pada Gambar 4., dijelaskan terdapat tiga fase yang dilakukan dalam melakukan drone forensics. Adapun tiga fase yang dilakukan adalah sebagai berikut:

1. *Drone acquisition*
   Untuk melakukan *drone forensics*, maka *drone* harus ada secara fisik. *Drone acquisition* dapat dilakukan dari tempat kejadian perkara atau ketika adanya kegiatan yang rentan terhadap pelanggaran privasi atau kegiatan ilegal.
2. *Hardware and Digital Forensics*
   Fase ini terbagi menjadi dua bagian, yaitu *hardware forensics* dan *digital forensics*. *Hardware forensics* tidak dilakukan dengan menggunakan log data yang tersimpan pada *drone*, melainkan dengan menganalisis secara langsung dan melakukan forensik fisik pada *drone* yang didapatkan.
   Hardware forensics dilakukan dengan *payload check*, *hardware check*, dan *biological evidence*. *Payload check* dilakukan dengan memeriksa muatan yang ada pada perangkat *drone*. *Hardware check* dilakukan dengan

memeriksa komponen yang ada pada *drone*. *Biological evidence* dilakukan dengan memeriksa bukti-bukti yang berhubungan dengan karakteristik fisik pengguna.

Digital drone forensics dapat dilakukan dengan mengolah data-data log yang tersimpan pada *drone* setelah *drone* berhasil didapatkan. Pada penelitian ini, hanya akan dilakukan *digital drone forensics* dengan alasan tidak tersedianya alat untuk mendapatkan *biological evidence*.

3. *Overall Forensic Analysis*
   Pada metode yang diusulkan, Renduchintala *et al*. membuat aplikasi DIGital drone Forensic (DIGON) untuk menganalisis data yang direkam oleh *drone*.



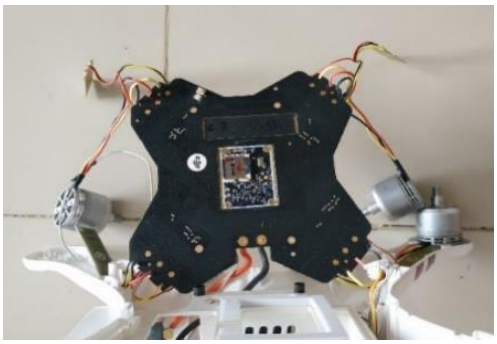
Gambar 4. *Diagram metodologi drone forensics yang diusulkan oleh Renduchintala et al.* [9]

4. HASIL DAN PEMBAHASAN

4.1. Implementasi Metode Clark et al.

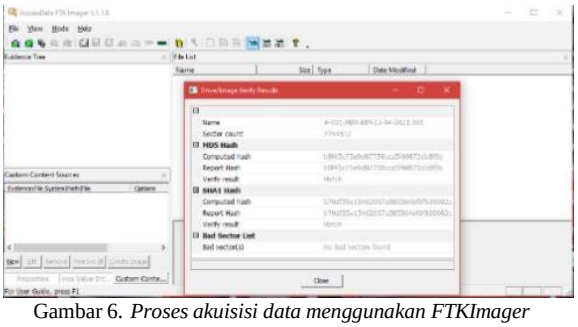
1. *Factory reset*
   Pada perangkat *mobile*, dilakukan instalasi aplikasi DJI GO. Aplikasi DJI GO berperan sebagai kendali fungsi-fungsi yang terdapat pada *drone*. Kemudian, dilakukan pengaturan pada *username* perangkat. Pada memori *gimbal rig*, dilakukan *formatting* dengan menggunakan aplikasi DJI GO. Memori gimbal rig diformat dengan sistem *file* FAT32.
2. *Scenario creation*
   Setelah perangkat disiapkan, *dilakukan test flight* untuk memperoleh data pada tanggal 21 Maret 2021 dan 11 April 2021. *Drone* diterbangkan pada lokasi kampus Poltek SSN. Pada test flight kedua, *drone* diterbangkan hingga daya baterai habis dan jatuh di titik akhir penerbangan. Selanjutnya, dilakukan pengambilan data secara manual yang selanjutnya akan dilakukan analisis terhadap data tersebut.
3. *Data acquisition*
   Dilakukan pengambilan data dari perangkat *drone* dan perangkat *mobile*. Terdapat dua memori yang dimanfaatkan sebagai penyimpanan, antara lain memori internal *drone* dan memori gimbal rig. Pada memori internal *drone*, terdapat log penerbangan yang tersimpan dalam format DAT. Pada memori gimbal rig, terdapat penyimpanan media video dan foto. Pada perangkat mobile, terdapat file log penerbangan yang tersimpan dalam format TXT.

   Untuk mengakses memori internal drone, perlu akses terhadap mainboard perangkat drone dengan membuka bagian body. Bentuk mainboard drone DJI Phantom 3 Standard disajikan pada Gambar 5. Memori internal drone terletak pada bagian bawah mainboard. Untuk mengaksesnya, perlu membuka lem permanen pada pengait SD card.



Gambar 5. *Mainboard drone DJI Phantom 3 Standard*

Pada memori internal *drone*, dilakukan akuisisi data dengan menghubungkan memori internal drone ke *workstation* dengan tangkapan layar seperti pada Gambar 6. Sebelum memori dihubungkan, USB WriteBlocker diaktifkan dengan tujuan data pada memori tidak mengalami perubahan. Setelah memori terhubung dengan *workstation*, dilakukan akuisisi data menggunakan FTK Imager Lite 3.1.1. Hasilnya yaitu file berekstensi DAT. Pada memori *gimbal rig*, dilakukan akuisisi data dengan metode yang sama dengan memori internal *drone*. Hasil yang didapatkan yaitu file media gambar dengan ekstensi JPG dan DNG.



Gambar 6. *Proses akuisisi data menggunakan FTKImager*

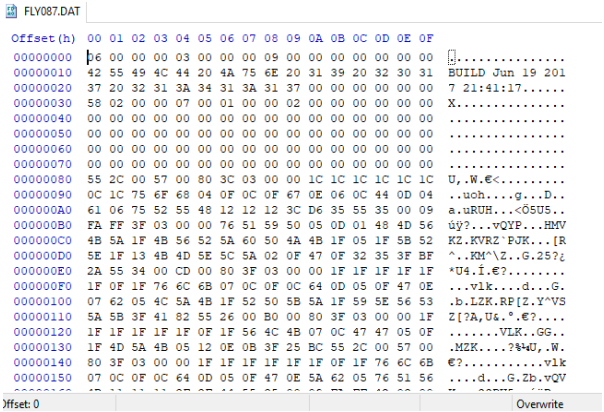
Aplikasi DJI GO menyimpan log penerbangan pada memori *non-volatile* perangkat *mobile*. Untuk mengakses data, perangkat mobile dihubungkan ke *workstation* dan *file* yang ada pada penyimpanan perangkat *mobile* disalin ke *workstation*. Data yang diperlukan pada metode ini yaitu data TXT yang didapat dari perangkat mobile. Data TXT didapatkan dari InternalStorage/DJI/dji.pilot/FlightRecord

4. *Data analysis*
   Memori internal *drone* memiliki kapasitas 4GB. Pada memori internal drone, terdapat data DAT dengan format nama DJIxxx.dat dimana xxx merupakan penomoran berdasarkan urutan *file*. Data DAT yang tersimpan pada memori *non-*

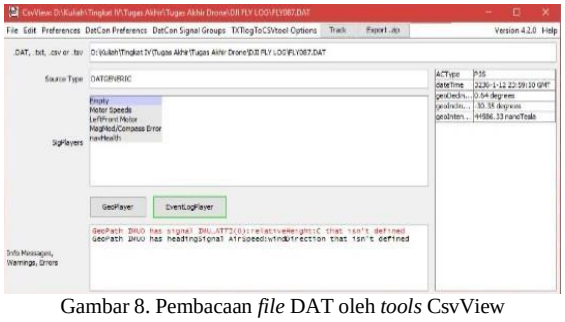
volatile ini, berisi data yang berhubungan dengan lokasi *drone*, status penerbangan, dan berbagai pembacaan sensor pada *drone*.

Pada penerbangan 21 Maret 2021 dapat dilihat pada Gambar 8., terbentuk tiga file log yang tersimpan, yaitu FLY087.dat, FLY088.dat, dan FLY089.dat.

Pada penerbangan 11 April 2021 dapat dilihat pada Gambar 9., data DAT baru dapat ditemukan ketika dilakukan *image mounting* pada FTK Imager karena *drone* mati tidak sesuai prosedur, data ini yaitu FLY096.DAT.FileSlack. File DAT pada Gambar 7. berisi karakter-karakter acak yang dienkripsi secara *proprientary* sehingga tidak dapat terbaca dengan mudah. Untuk membaca isi File DAT, maka digunakan DatCon dan CsvView untuk menerjemahkan isi *file* yang tangkapan layarnya ada pada Gambar 8.



Gambar 7. *Tampilan data DAT yang masih berupa karakter acak*



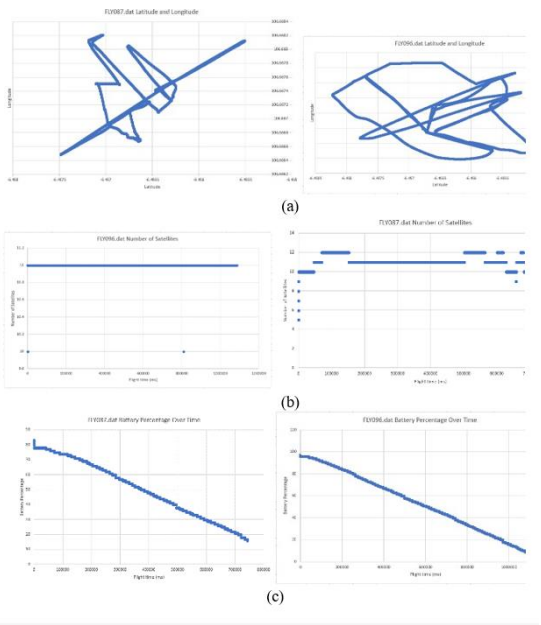
Gambar 8. Pembacaan *file* DAT oleh *tools* CsvView


Gambar 9 Visualisasi rute penerbangan *drone* pada 21 Maret 2021 oleh *tools* CsvView


Gambar 10. Visualisasi rute penerbangan *drone* pada 11 April 2021 oleh *tools* CsvView

5. *Tool creation*

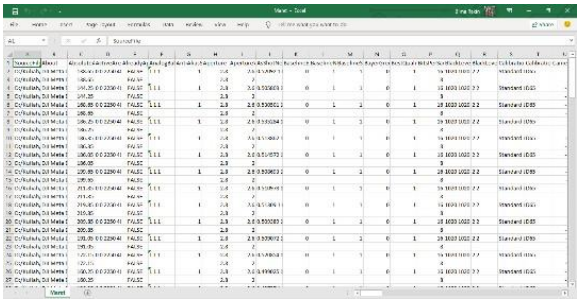
Untuk melakukan drone forensics pada data DAT drone DJI Phantom 3 Standard, digunakan tools Drone Open Source Parser, atau yang disebut dengan DROP. Tools ini berjalan dengan Python 3.4 untuk melakukan parsing data. Penelitian [8] melakukan percobaan tools DROP untuk file DAT dari DJI Phantom 3 Standard. Dari hasil parsing, akan dihasilkan output berupa file CSV yang berisi informasi-informasi mengenai penerbangan ataupun informasi mengenai drone ketika drone dinyalakan. Selain untuk melakukan parsing, DROP ini juga dapat dipakai untuk menguji integritas data, dengan membandingkan hash sebelum parsing dan hash setelah parsing. Algoritma hash yang digunakan oleh DROP adalah MD5, SHA1, dan SHA512. Output dari menggunakan DROP ada pada Gambar 11.



Gambar 11. *Output* data dari *tools DROP* berupa (a) data koordinat (b) jumlah satelit pada penerbangan (c) persentase baterai saat penerbangan pada 21 Maret 2021 (kiri) dan 11 April 2021 (kanan)

4.2. Implementasi Metode Renduchintala et al.

1. *Drone acquisition*
   Untuk melakukan *drone forensics*, perangkat drone harus ada secara fisik. Akuisisi *drone* dapat dilakukan dari suatu kasus kriminal atau ketika *drone* dicurigai melakukan pelanggaran privasi maupun aktivitas ilegal. Pada penelitian ini, *drone acquisition* dilakukan setelah *test flight*. Selanjutnya, pengambilan data pada *drone* DJI Phantom 3 Standard yang telah diakuisisi.
2. *Digital forensics*
   Untuk metode ini, *file* yang dimanfaatkan yaitu *file* media dari memori *gimbal rig* dan *file* log penerbangan berformat txt yang berasal dari perangkat *mobile*. Pada memori *gimbal rig*, terdapat data media dengan format .jpeg dan .dng. Data EXIF pada media ini dapat dimanfaatkan untuk melihat koordinat gambar yang diambil sebagai data pendukung rute penerbangan *drone*. Untuk membaca data EXIF pada media, digunakan *tools* exiftool. Hasil pembacaan data menggunakan exiftool disimpan dalam output *file* dengan format .csv. Dari hasil pembacaan exiftool Gambar 12, terdapat dua *file* csv untuk menyimpan data EXIF penerbangan pertama dan penerbangan kedua hal tersebut dapat dilihat pada Gambar 13.



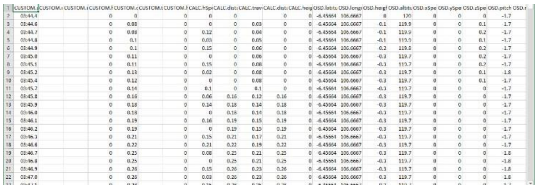
Gambar 12. Hasil pembacaan data EXIF oleh exiftool

Terdapat beberapa data yang didapatkan, contohnya *latitude* yang terdapat pada kolom GPSLatitude dan *longitude* yang terdapat pada GPSLongitude. Data ini kemudian di-input ke Google Earth Pro. Hasilnya yaitu titik-titik koordinat yang menunjukkan lokasi *drone* saat mengambil foto dari *gimbal rig*.

Gambar 13. Visualisasi koordinat data EXIF pada Google Earth Pro

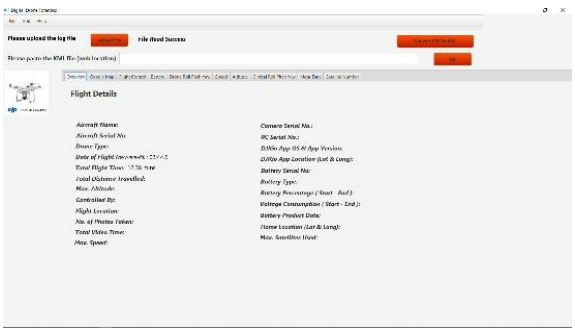
Selanjutnya, dilakukan pengolahan data untuk file pada perangkat *mobile*. File log yang tersimpan pada perangkat *mobile* dinamai dengan format DJIFlightRecord_YYYY-MM-DD_[HH- MM-SS].txt. Tanggal dan waktu pada *file* ini sesuai dengan waktu penerbangan *drone*. Seperti yang dapat dilihat pada Gambar 14., *file* TXT yang didapatkan masih berupa karakter yang tidak dapat dibaca. Untuk mendapatkan informasi dari file TXT ini, digunakan *tools* dari Phantomhelp untuk mengubah file TXT menjadi file CSV (Gambar 15.) dan KML dengan data yang dapat diinterpretasikan.

Gambar 14. Data TXT yang masih berupa karakter acak



Gambar 15. Data TXT yang telah dikonversi menjadi data CSV

Setelah data .CSV diperoleh, dilakukan pemrosesan data dengan menggunakan *tools* Digital Drone Forensics yang telah dibuat. Tools ini dapat digunakan untuk membaca data CSV seperti pada Gambar 16.



Gambar 16. Output data CSV pada *tools* Digital Drone Forensics (DIGON)

3. *Visualisation*
   Untuk melakukan visualisasi, digunakan Google Earth Pro. Agar Google Earth Pro dapat memvisualisasi rute penerbangan, maka diperlukan file KML sebagai input data. Untuk mendapatkan *file* KML dari log penerbangan DJI Phantom 3 Standard, maka digunakan *tools* dari Phantomhelp. Hasil dari visualisasi rute penerbangan dapat dilihat pada Gambar 17.

Gambar 17. Visualisasi data penerbangan dari *file* TXT oleh Google Earth Pro

4.3. Hasil Pengujian

Pada penelitian ini dilakukan pengujian dengan tujuan menjawab permasalahan terkait integritas data serta aspek-aspek yang berkaitan dengan laporan investigasi kejahatan.

1. Pengujian integritas data
   Pengujian integritas data dilakukan untuk menguji kebenaran data dengan memanfaatkan nilai hash yang dibangkitkan ketika dilakukan *imaging* data pada memori internal *drone*. Hash yang dihasilkan setelah proses *imaging* yaitu hash dengan algoritma MD5 dan SHA-1. Pengujian integritas data merupakan pengujian untuk memverifikasi apakah *file* yang diproses dilakukan perubahan. Pengujian ini dilakukan dengan melakukan *hashing file* yang digunakan pada *drone forensics*. Kemudian, nilai *hash* sebelum dan sesudah data diolah dibandingkan.

   Pengujian hash menggunakan FTKImager dan DROP. DROP dapat menguji hash dari setiap file DAT yang dilakukan forensik. FTKImager digunakan untuk menguji image file dari keseluruhan file penyimpanan pada memori

   BEFORE MD5 Hash Digest :
   f3dd1d115685fa261b6596de2cf388f5 AFTER MD5 Hash Digest :
   f3dd1d115685fa261b6596de2cf388f5

   BEFORE SHA1 Hash Digest :
   76b5e3d8df8109f499b22b38e0bc531cf4d22111
   AFTER SHA1 Hash Digest :
   76b5e3d8df8109f499b22b38e0bc531cf4d22111

   BEFORE SHA512 Hash Digest :
   ae8c2625a6cf74df4606071935340da6ab02a946 91dd
   b5fca6a07ef12dff2717fef9d11d871e7cc2a9abca 5860
   ad2c17281d2811f770466ff8a81c4ffa964e91

   AFTER SHA512 Hash Digest :
   ae8c2625a6cf74df4606071935340da6ab02a946 91dd
   b5fca6a07ef12dff2717fef9d11d871e7cc2a9abca 5860
   ad2c17281d2811f770466ff8a81c4ffa964e91

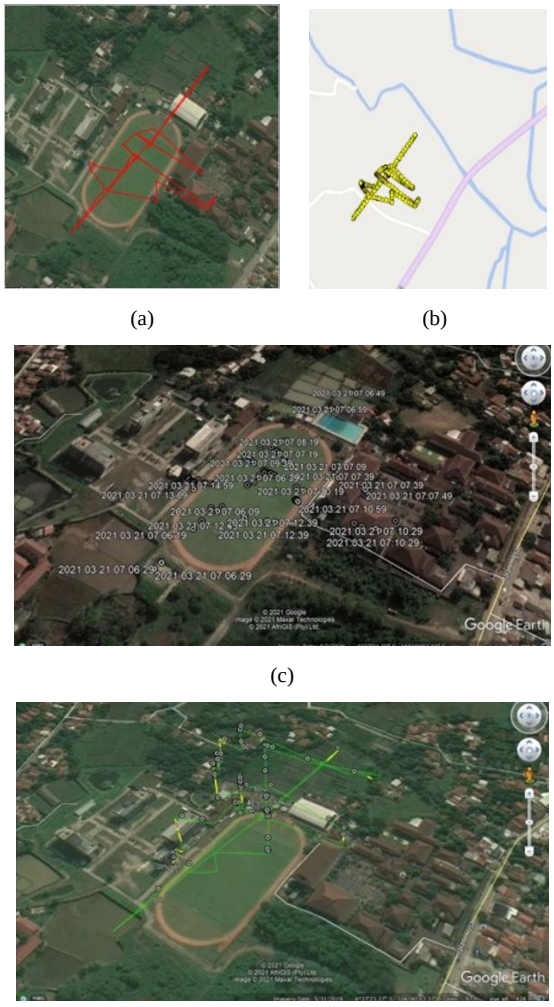
   Selain menggunakan *tools* DROP, pengujian hash juga dilakukan pada image file menggunakan tools FTKImager. Hasil dari perbandingan penghitungan hash ini terdapat pada file report yang ada setelah image file berhasil dibuat. Hasilnya yaitu sebagai berikut :

   [Computed Hashes]
   MD5 checksum:
   b8f45c75e9d07758cca5f40872db8f0b
   SHA1 checksum:
   b70df35e15462057a585364bf9f839902c200014
   Image Verification Results:
   Verification started: Mon Apr 12 22:46:10 2021
   Verification finished: Mon Apr 12 22:47:07 2021 MD5 checksum:
   b8f45c75e9d07758cca5f40872db8f0b :
   verified SHA1 checksum:
   b70df35e15462057a585364bf9f839902c200 014 :
   verified

2. Pengujian data akuisisi
   Hasil yang telah didapatkan dari *drone forensics* harus diuji kebenarannya. Pengujian ini dilakukan untuk membandingkan hasil yang didapatkan antara data penerbangan dari memori internal *drone*, memori gimbal *rig*, dan perangkat *mobile*. Kemudian, akan

dibandingkan hasil apa saja yang dapat menjawab pertanyaan 5W1H. Setelah itu, pada data yang dibandingkan, apakah data yang diperoleh memiliki korelasi.

a. Perbandingan data *test flight* 21 Maret 2021
Pada *test flight* yang dilakukanZ pada tanggal 21 Maret 2021, didapatkan data .dat, data exif, dan .txt. Pengujian dilakukan menggunakan tools CsvView, Autopsy, dan Google Earth Pro. Pengujian ini bertujuan untuk melihat apakah masing-masing data yang diolah memiliki korelasi, dengan kata lain data yang diolah menunjukkan titik lokasi yang berkaitan.



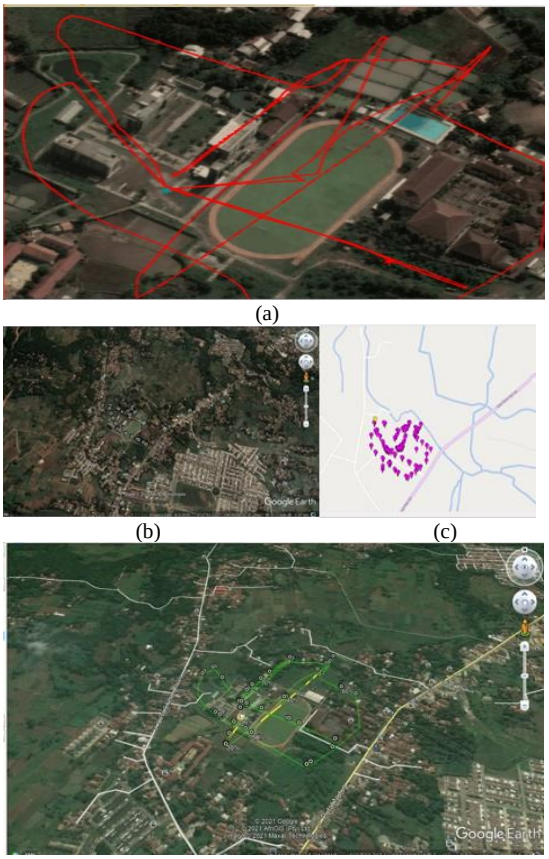
(a) (b)

(c)

(d)

Gambar 18. Hasil visualisasi rute penerbangan dari data (a), (b) memori internal *drone*, (c) data EXIF, dan (d) perangkat *mobile*

b. Perbandingan data test flight 11 April 2021
Pada test flight yang dilakukan pada tanggal 11 April 2021, didapatkan data exif, dan .txt. Pengujian dilakukan menggunakan tools CsvView, Autopsy, dan Google Earth Pro. Pengujian ini bertujuan untuk melihat apakah masing-masing data yang diolah memiliki korelasi, dengan kata lain data yang diolah menunjukkan titik lokasi yang berkaitan.



(a)

(b) (c)

(d)

Gambar 19. Hasil visualisasi rute penerbangan dari data (a)(b) data EXIF, dan (c) perangkat *mobile*

5. KESIMPULAN

Berdasarkan hasil proses implementasi, analisis, dan pengujian yang dilakukan, maka didapatkan beberapa simpulan sebagai berikut :

1. Berdasarkan implementasi *drone forensics* menggunakan metode Clark *et al*. dan Renduchintala *et al.*, dapat dimplementasikan pada *drone* DJI Phantom 3 Standard.
2. Adapun data-data yang didapatkan dari hasil *drone forensics* dapat digunakan untuk mendukung investigasi penyalahgunaan *drone*.
3. Untuk melakukan *drone forensics*, dilakukan beberapa tahapan pada masing-masing metode yang sesuai dengan tahapan *digital forensics* yaitu *collection*, *examination*, *analysis*, dan *reporting*. Setelah dilakukan *test flight* yang bertujuan agar terdapat data yang diteliti pada *drone*, dilakukan implementasi metode *drone forensics* Clark *et al*. dan Renduchintala *et al*. untuk mendapatkan hasil dari *drone forensics*.
4. Hasil *drone forensics* pada *drone* DJI Phantom 3 Standard dapat memenuhi aspek integritas data setelah dilakukan pengujian berupa korelasi data maupun *hash* data. Hasil pengujian korelasi data menunjukkan bahwa data DAT, EXIF, dan TXT saling berhubungan dan tidak terdapat perubahan sebelum data diakuisisi. Hasil

pengujian hash data menunjukkan bahwa tidak terdapat perubahan data sebelum dan sesudah data diproses pada *tools* yang digunakan.

5. *Drone forensics* yang dilakukan mampu menjawab beberapa pertanyaan berkaitan dengan investigasi mengenai insiden yang melibatkan *drone*. Beberapa pertanyaan yang dapat dijawab oleh *drone forensics* yang dilakukan meliputi pelaku insiden, waktu insiden, dan fakta yang terdapat pada insiden. Pelaku insiden dapat dijawab melalui visualisasi data penerbangan dan informasi mengenai nama perangkat dan nomor serial perangkat. Waktu insiden dapat dijawab dari waktu yang didapatkan dari waktu pembuatan data DAT, maupun informasi yang ditunjukkan dari data EXIF dan TXT. Fakta-fakta penerbangan yang ditemukan yaitu mengenai sumber data yang dapat dimanfaatkan, tipe *drone*, kondisi baterai dan sinyal GPS selama penerbangan, dan kapan dan dimana foto-foto diambil oleh *drone*.

Berdasarkan hasil penelitian yang dapat dilakukan dan kendala yang dihadapi ketika penelitian, terdapat saran yang diberikan untuk pengembangan penelitian selanjutnya. Saran yang diberikan dari penelitian ini adalah sebagai berikut:

1. Terdapat beberapa kendala dalam menjalankan *tools* yang dirujuk oleh referensi penelitian. Terdapat *tools* yang setelah digunakan, tidak bersifat universal. Untuk penelitian selanjutnya, diharapkan agar terdapat *tools* yang dapat digunakan untuk berbagai macam tipe *drone*.
2. Penelitian selanjutnya dapat menambahkan parameter *drone forensics* yang lebih komprehensif sehingga penelitian yang telah dilakukan dapat lebih bermanfaat.

REFERENSI

[1] International Civil Aviation Organization, *Unmanned Aircraft Systems (UAS)*, Montréal, Quebec: International Civil Aviation Organization, 2012.

[2] D.-Y. Kao, M.-C. Chen, W.-Y. Wu, J.-S. Lin, C.-H. Chen and F. Tsai, "Drone Forensic Investigation: DJI Spark Drone as A Case Study," *Procedia Computer Science Vol. 159*,pp. 1890-1899, 2019.

[3] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic," *Digital Investigation Vol. 16*, pp. 1-11, 2016.

[4] I. Harruma, "Pemilik Drone Pengirim Narkoba ke Rutan Belum Diketahui," 10 September 2016. [Online]. Available: https://republika.co.id/berita/odagnc/pemilik-emdroneem-pengirim-narkoba-ke-rutan-belum-diketahui.

[5] I. Fitriana, "Drone 3 Kali Terbang di Atas Lapas Magelang, Petugas Ancam Tembak Jatuh," 26 Juni 2018. [Online]. Available: https://regional.kompas.com/read/2018/06/26/19142261/drone-3-kali-terbang-di-atas-lapas-magelang-petugas-ancam-tembak-jatuh.

[6] G. Fenu and F. Solinas, "Computer Forensics Investigation An Approach to Evidence in Cyberspace," in *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec)*, Kuala Lumpur, 2013.

[7] H. Bouafif, F. Kamoun, F. Iqbal and A. Marrington, "Drone Forensics: Challenges and New Insights," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, 2018.

[8] D. R. Clark, C. Meffert and I. Baggili, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," in *DFRWS 2017 USA - Proceedings of the Seventeenth Annual DFRWS USA*, 2017.

[9] A. Renduchintala, F. Jahan, R. Khanna and A.Y. Javaid, "A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework," Digital Investigation Vol. 30, pp. 52-72, 2019.

[10] J. A. Saputro, "Implementasi Serangan GPS dan Reverse Engineering Firmware pada Drone DJI Phantom 3 Standard," Politeknik Siber dan Sandi Negara, Bogor, 2020.

[11] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology, Gaithersburg, 2006

[12] T. Grance, S. Chevalier and K. Scarfone, "NIST Special Publication 800-86," National Institute of Standards and Technology (U.S.), Gaithersburg, 2005.

[13] A. Iorliam, Fundamental Computing Forensics for Africa: A Case Study of the Science in Nigeria, Cham: Springer, 2018.

[14] A. Dennis, B. H. Wixom and R. M. Roth, System Analysis and Design, 5th Edition, Hoboken, New Jersey: John Wiley & Sons, Inc., 2012.