Conciencia Digital
www.concienciadigital.org

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

Análisis informático forense a vehículos aéreos no tripulados (dron)

Computer forensic analysis of unmanned aerial vehicles (drones)

Carlos Alberto Guerrero Montero. [1] & Luis Alberto Pazmiño Gómez. [2]

Recibido: 05-08-2021 / Revisado: 17-08-2021 /Aceptado: 08-09-2021/ Publicado: 05-10-2021

Abstract.

DOI: https://doi.org/10.33262/concienciadigital.v4i4.1884

Introduction. The present research arises from the need-to-know what information an unmanned vehicle (drone) can store, since, many times they are used as a means of entertainment, to do competitions and stunts, but fundamentally, they are used to spy on people or organizations with the aim of exposing sensitive data that may affect them. **Objective**. Perform a forensic analysis for the management of information related to unmanned vehicles in the tracking of activities. **Methodology**. In this research, an experimental method was used from a descriptive-explanatory investigation. In this way, forensic information on unmanned vehicles is obtained for proactive decision making. **Results**. Recorded media files could be located. Photos and videos were exported for further analysis. EXIF (Exchangeable Image File) data is information embedded within JPEG images. The EXIF data obtained were: Date, Timestamp, File Source, GPS, Altitude, Altitude Reference, Latitude, Longitude. This information will help determine where and when the photos were taken. **Conclution**. The applied methodology is very useful as long as the drone has a removable storage memory, in addition, the application of this methodology can be complemented by having access to radio control devices,

[1] Pontificia Universidad Católica del Ecuador Sede Ambato, Escuela de Postgrado, Maestría en Ciberseguridad. Ambato, Ecuador, carlos.a.guerrero.m@pucesa.edu.ec, https://orcid.org/0000-0002-9283-5763

[2] Pontificia Universidad Católica del Ecuador Sede Ambato, Escuela de Postgrado, Maestría en Ciberseguridad. Ambato, Ecuador, lpazmino@pucesa.edu.ec, https://orcid.org/0000-0001-9913-0806

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

whether they are wireless controls, smart devices or computers, since in these devices logs are also stored, applying specific methodologies according to the device obtained.

Keywords: drone, UAV, forensic analysis, Autonomous vehicles.

Resumen.

Introducción. La presente investigación surge de la necesidad de saber qué información puede almacenar un vehículo no tripulado (dron), ya que, muchas veces se utilizan como medio de diversión, para hacer competencias y acrobacias, pero fundamentalmente, se emplean para espiar a personas u organizaciones con el objetivo de exponer datos sensibles que las pueden afectar. **Objetivo**. Realizar un análisis forense para la gestión de la información relacionada a los vehículos no tripulados en el rastreo de las actividades. **Metodología**. En esta investigación se utilizó un método experimental a partir de una investigación descriptiva-explicativa. De esta manera, se obtiene información forense sobre vehículos no tripulados para la toma de decisiones proactivas. **Resultados.** Se pudo localizar los archivos multimedia grabados. Las fotos y los vídeos se exportaron para su posterior análisis. Los datos EXIF (archivo de imagen intercambiable) son información incrustada dentro de imágenes JPEG. Los datos EXIF obtenidos fueron: Fecha, Marca de tiempo, Fuente de archivo, GPS, Altitud, Referencia de altitud, Latitud, Longitud. Esta información ayudara a determinar dónde y cuándo se tomaron las fotos. **Conclusión**. La metodología aplicada es de gran utilidad siempre y cuando el dron cuente con una memoria de almacenamiento extraíble además se puede complementar la aplicación de esta metodología teniendo acceso a los dispositivos de radio control ya sean mandos inalámbricos, dispositivos inteligentes o computadoras puesto que en estos dispositivos también se almacenan logs, aplicando metodologías específicas de acuerdo con el dispositivo obtenido.

Palabras claves: Dron, UAV, Análisis forense, Vehículos autónomos.

Introducción.

Los drones, también denominados UAV (vehículos aéreos no tripulados) en la literatura, están experimentando un aumento en popularidad en todo el mundo. Aunque inicialmente se describió como tecnología militar sofisticada, se están implementando cada vez más en los sectores comercial y recreativo. Hoy en día, los UAV se utilizan en un amplio espectro de aplicaciones que van desde la fotografía hasta la agricultura, la recuperación de desastres y el mantenimiento de la infraestructura. Sin embargo, la misma tecnología también se está utilizando para ataques y actividades poco éticas. Estos actos delictivos incluyen la invasión de la privacidad, el contrabando de drogas, las operaciones terroristas y la alteración de las infraestructuras críticas. La necesidad de investigación de los incidentes antes mencionados ha dado lugar a la creación de la disciplina Drone Forensics.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

Drone Forensics, un subdominio de la ciencia forense digital está especializado en extraer y procesar evidencia de drones y sus componentes asociados de tal manera que las entidades y acciones atacantes sean identificadas y rastreadas. El análisis forense de drones comprende análisis forense móvil e inalámbrico. La evidencia digital puede ser volátil, frágil y vulnerable si no se maneja y examina adecuadamente. Además, con la amplia variedad de drones que se utilizan hoy en día y la velocidad con la que se desarrollan y cambian, mantener el ritmo puede ser un gran desafío para las fuerzas del orden y otras empresas. El campo de Drone Forensics es todavía relativamente nuevo, y estos desafíos contribuyen a un escaso apoyo para las herramientas de investigación.

Este documento se centrará en extraer y analizar datos de diferentes modelos de drones, Dron DJI mini 2, Dron carreras" LHI racing drone 250" , Dron Intel aero ready to fly y DJI Phantom 3 Profesional, mientras se comparan herramientas forenses comerciales y de código abierto. El propósito de este estudio es desarrollar una guía que proporcione a los investigadores y examinadores forenses los conocimientos necesarios para diseñar los estándares y procedimientos adecuados con los que acercarse a los drones en el contexto de la investigación. La investigación tendrá como objetivo encontrar respuestas a las siguientes preguntas:

1. ¿Existen estudios teóricos adecuados relacionados con vehículos aéreos no tripulados?
2. ¿Existen metodologías precisas para obtener información de un dispositivo no tripulado dron?
3. ¿La información forense contribuye a la toma de decisiones de los datos pertenecientes a los vehículos no tripulados?
4. ¿Los resultados de la información forense garantizan la no vulnerabilidad de las personas y empresas?

Antecedentes

Un vehículo aéreo no tripulado es un avión sin piloto que se navega de forma remota. Los UAV se consideran parte de un sistema aéreo no tripulado (UAS), que incluye el UAV en sí, la estación de control de tierra (GCS) y el controlador. Cada una de estas partes es necesaria para operar y controlar con éxito y precisión el UAV. Los UAV actuales varían ampliamente en su capacidad, accesibilidad y asequibilidad, desde sistemas económicos y disponibles comercialmente hasta sistemas de grado militar que requieren una formación e infraestructura sustanciales para su funcionamiento. La clasificación de drones se realiza de varias formas. Según el Center for a New American Security, los drones se dividen en cuatro categorías:

1. Los drones aficionados se utilizan con fines recreativos o de pasatiempo. No requieren infraestructura formal o capacitación para operar y están disponibles por un precio de compra bajo.
2. Drones militares y comerciales de tamaño mediano, requieren infraestructura y entrenamiento formal. Los militares los utilizan principalmente para servicios de vigilancia, reconocimiento o entrega de carga útil.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

3. Grandes Drones específicos para militares, requieren una infraestructura y entrenamiento militar. Están limitados a aplicaciones militares.
4. Stealth Combat Drones, están integrados con tecnologías altamente sofisticadas y no son accesibles para fabricantes comerciales.

Esta investigación se centra en los drones aficionados, debido a su popularidad y disponibilidad en el mercado. Los drones aficionados se están volviendo más innovadores y avanzados en varios aspectos, incluidos hardware, software y redes. Por ejemplo, los drones disponibles en la actualidad están hechos de materiales compuestos ligeros para aumentar la maniobrabilidad y la eficiencia de vuelo. Son compatibles con sofisticados cardanes para estabilizar la cámara, baterías de litio y sensores. Contienen software mejorado con tecnologías de reconocimiento, lo que les permite fijarse en sujetos y seguirlos, detectar y evitar obstáculos y volver automáticamente a su punto de lanzamiento antes de quedarse sin batería. Equipados con capacidades tan avanzadas, estos drones recopilan y producen una gran cantidad de datos valiosos que indican patrones de uso y rendimiento.

Especificaciones	DJI Phantom 3 Profesional	Intel aero ready to fly drone	DJI mini 2	LHI racing drone 250
Costo (USD)	$900	$1200	$600	$450
Fecha de lanzamiento	2016	2018	2020	2016
Peso	1280 g	865 g	249 g	g
Almacenamiento interno	N/A	32GB eMMC	No	N/A
Almacenamiento externo	Sí	Sí	Sí	No
Tipo de transmisión	Wi-Fi	Intel Dual Band Wireless-AC 8260	Wi-Fi	Wi-Fi
Resolución de la cámara	UHD	8MP RGB RGB: 1920 x 1080 at 30 fps	4K	N/A
Tiempo de vuelo	Approx. 23 minutos	20 minutos	20 minutos	15 minutos
Velocidad máxima (Kph)	57.6 k/h (ATTI mode)	54 k/h	57,6 km/h	50
Volver a la ubicación de la casa	Sí	Sí	Sí	No
Sistema operativo		Linux	N/A	N/A
Batería (mAh)	4480 mAh	4500 mAh	5200 mAh	11.1 V 1500 mAh 35
Frecuencia de funcionamiento Ghz	2.400 - 2.483 GHz	2.4 GHz DSMX	2.400-2.4835 GHz, 5.725-5.850 GHz	2.4 y 5.8
Controlador de vuelo	Controlador inteligente	Aero Flight Controller with Dronecode PX4 Autopilot	Controlador inteligente	Sí (aplicación móvil)

Tabla 1. Especificaciones de drones para la investigación
Fuente. Autor.

Revisión de la literatura

La informática forense ha ganado un gran impacto en la información digital debido al aumento de la información, que puede utilizarse en el nuevo espacio informático de cualquier persona. Según un estudio realizado por (Paruma, s. f.) en la Universidad de Los Andes en Bogotá, mencionaron que cuando ocurren delitos informáticos, la

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

información se almacenará digitalmente. Sin embargo, el sistema informático no se puede operar directamente, por lo que es necesario obtener evidencia, extraerla, guardarla, analizarla y redactar informes.

Los drones tienen equipos de video integrados, como cámaras que se utilizan para capturar imágenes y videos, y se convertirán en posibles herramientas de videovigilancia independientemente del consentimiento del objetivo.

En la mayoría estos dispositivos cuentan con dos enlaces de datos, es decir tienen dos frecuencias para su comunicación, uno para el envío de comandos y el otro para recibir información de vuelo. No obstante, es viable descubrir enlaces extras que permiten la comunicación con elementos externos, como la comunicación GPS la cual se hace por satélite o la comunicación por radio control.

Al igual que los vehículos aéreos no tripulados, hay otros tipos de vehículos de tierra no tripulados en los cuales se realizaron averiguaciones para establecer su composición interna y permitir detectar la viabilidad del estudio forenses para la obtención de datos digitales almacenados en dichos sistemas.

Actualmente, existen trabajos y demostraciones relacionados con el análisis forense en equipos no tripulados y vehículos aéreos no tripulados. El contenido más relevante del proyecto de investigación se enumera a continuación.

El Análisis Forense a Dones es un campo emergente dentro de la ciencia forense digital y la aplicación de la ley. En particular, el análisis forense digital de drones aficionados es un desafío porque hay muchos tipos de drones con diferentes elementos técnicos, características y capacidades. No existe una forma estándar en que los UAV para aficionados almacenen datos.

(Toro-Alvarez et al., 2018) en su trabajo “Fundamentos de la investigación forense en ambientes informáticos” nos brinda conceptos básicos de la ciencia forense para dispositivos informáticos y los cuidados a tener en cuenta dada la volatilidad de la información y los desafíos tecnológicos acerca del almacenamiento de la información.

(Tacuri & Maribel, 2012) en su tesis “Investigación Forense: Estudio para determinar los métodos usados en la intrusión del banco JBR” explica cada concepto y las normas que se deben seguir para realizar una investigación forense de confianza, además se dan a conocer cuáles son las herramientas más apropiadas para realizar una investigación de este tipo, estas herramientas nos ayudarán a efectuar desde un simple proceso de recolección de evidencias hasta la presentación de un análisis.

(Rivas, s. f.) en su trabajo “Metodología para un análisis forense” nos brinda una perspectiva general sobre la metodología de estudio forense permitiendo que la prueba logre ser validada de manera correcta en la mayor cantidad de situaciones que se puedan presentar en el ámbito de la informática forense.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

(Bonetti et al., 2013) en su trabajo "A Comprehensive Black-box Methodology for Testing the Forensic Characteristics of Solid-state Drives", propone una metodología genérica, práctica y basada en pruebas que guía a los investigadores y analistas forenses a través de una serie de pasos que evalúan la "compatibilidad forense" de un SSD. La cual servirá en el análisis de información almacenada por un DJI matrice 600 ya que su medio de almacenamiento es un ssd

(Sánchez Herrera & Basantes Salazar, 2016) en su trabajo "Análisis forense a sistemas operativos mediante la utilización de herramientas Open Source, caso estudio Windows 8", nos presenta un enfoque de la implementación de herramientas forenses Open Source (fuente abierta) para la investigación del dispositivo con windows 8. Las cuales pueden ser aplicadas para la situación de análisis que se pretende examinar.

(Manzano & Fabricio, 2015) en su trabajo "DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR", nos presenta los puntos más relevantes que se tienen que considerar para mantener la cadena de protección en grupos tecnológicos, que acceden en indagaciones por ser pruebas en casos judiciales.

(Horsman, 2016) en su trabajo "Unmanned aerial vehicles: A preliminary analysis of forensic challenges", presenta una discusión introductoria sobre las aeronaves no tripuladas, análisis del vehículo y proporciona los resultados de una investigación forense digital de un Parrot de prueba Vehículo aéreo no tripulado Bebop. El cual proporcionara información para adquisición y extracción de datos de un dron

(Barton & Hannan Bin Azhar, 2017) en su trabajo "Forensic Analysis of Popular UAV Systems", cubre el uso de herramientas Open Source (código abierto) y el desarrollo de algunos scripts básicos para ayudaren el análisis forense de dos drones populares: el DJI Phantom 3 Professional y AR Drone 2 con el objetivo de reconstruir las acciones tomadas por estos drones, identificación de propietarios u operadores y extracción de datos de dispositivos móviles asociados.

(Clark et al., 2017) llevaron a cabo una investigación forense en 2017 del (DJI Phantom III) y presentaron una herramienta de código abierto forense (DROP) que permite analizar archivos DAT encriptados obtenidos del almacenamiento interno de un dron. Su trabajo también mostró hallazgos preliminares sobre archivos TXT encriptados que se encuentran en el dispositivo móvil que se utiliza para controlar el dron, que proporciona datos valiosos como la ubicación del GPS, el nivel / uso de la batería y el tiempo de vuelo.

(Bouafif et al., 2018) en su trabajo "Drone Forensics: Challenges and New Insights", presenta importantes resultados de una investigación forense, realizado en una prueba Parrot AR drone 2.0, se presentaron nuevos conocimientos sobre la ciencia forense de drones en términos de acceso a la tecnología digital contenedores de un dron interceptado y recuperando toda la información que puede ayudar a los investigadores forenses

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

(Barton & Azhar, 2018) en su trabajo "Open Source Forensics for a Multi-platform Drone System" , informa la extracción e interpretación de información importante que se encuentran en los registros de vuelo registrados en la memoria interna del UAV y la aplicación de control, así como el análisis de medios, registros y otros archivos importantes

(Chamba, s. f.) en su tema de tesis "DISEÑO DE UN MARCO METODOLÓGICO PARA ANÁLISIS FORENSE DE DRONES USADOS PARA ESPIONAJE APLICADO A LAS LEYES ECUATORIANAS: CASO DE ESTUDIO DJI PHANTOM III STANDARD", explica una metodología para sustracción de prueba digital forense de un dron DJI PHANTOM III STANDARD implementando leyes ecuatorianas, que dejará proteger la totalidad de la información. El cual aportara la metodología elemental para hacer la investigación forense.

(Kao et al., 2019) en su trabajo "Drone Forensic Investigation: DJI Spark Drone as A Case Study", presenta la reconstrucción del crimen en un ambiente de laboratorio para el análisis temporal y los artefactos necesarios para explorar y evaluar la asociación entre el dron, el teléfono móvil y la tarjeta SD.

(Yousef et al., 2020) en su trabajo "Drone Forensics: A Detailed Analysis of Emerging DJI Models", analizan los datos extraídos de cuatro modelos de drones para aficionados mientras comparan la aplicabilidad y capacidad de varias herramientas forenses comerciales y de código abierto. Las cuales servirán de sustento para realizar el análisis del presente trabajo

Herramientas

Se emplearon las siguientes herramientas forenses para analizar los datos de los drones (tanto internos como externos). Estos métodos se seleccionaron en función de su relevancia con los análisis de memoria física:

FTK Imager, una herramienta gratuita la cual permite crear de imágenes forenses y vista previa de datos realizada por AccessData. La herramienta es capaz de reconocer la estructura del sistema de archivos, archivos multimedia grabados, búsqueda de palabras clave permitidas, datos Exif / datos meta (en formato hexadecimal).

Autopsy, una plataforma forense digital de código abierto de extremo a extremo construida por Basis Technology, con la mayoría de las características disponibles en otras herramientas forenses comerciales . La herramienta es capaz de reconocer la estructura del sistema de archivos, archivos multimedia grabados, línea de tiempo, mostrar datos Exif, archivos del sistema, miniaturas (se muestran de una manera organizada visualmente).

Exif-tool, una herramienta para el análisis de metadatos de los distintos archivos encontrados, esta herramienta realiza el análisis individual de cada uno de los archivos y presenta los resultados más detallados a diferencia de autopsy que también permite ver metadatos, pero de una manera más simple.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

Datcon, una herramienta que permite desencriptar los archivos con extensión .DAT y permite exportar la información extraída en formato .txt .csv , las coordenadas gps en formato .klm

CsvView, una herramienta que permite visualizar los archivos con extensión .csv. txt o. Dat exportados con la herramienta antes mencionada y permite visualizar datos como la altitud inclinación velocidad de motores la fecha y hora del evento además de los mensajes de error que pudo generar el dron, adicional a esto posee un visualizador de las coordenadas gps en un mapa parecido al de google maps

Airdata.com: Es una página web en la cual podemos subir archivos logs para su análisis, Airdata ha tenido la suerte de ser la primera empresa en unirse al programa DJI FlightRecord SDK, lo que le permite decodificar los logs de los modelos más recientes de drones dji y soporta un gran número de marcas de drones para el análisis de logs entre las características que ofrece esta herramienta web tenemos la Gestión del libro de registro de vuelo, la que permite que Capture y registre detalles relevantes de su vuelo para informes y mantenimiento, Análisis del estado de la batería, la cual permite Identificar problemas en celdas de batería individuales, Mapas de sensores, la cual nos permite observar la conexión de la intensidad de la señal entre el control y la aeronave e identifique las áreas de interferencia

Herramientas de análisis forense	Descripción	Utilización
Estación de trabajo forense	MS Windows	Estación de trabajo forense
Estacion de trabajo virtualizada	CAIN forencics basado en Ubuntu 14.04	Estacion de trabajo forense basado en linux
Bloqueador de escritura de tarjeta Micro SD	Adaptador de Micro SD a SD con switch de bloqueo de escritura	Bloqueador de escritura de hardware
SAFE Block	Herramienta de bloqueo de escritura por software	Evitar la escritura de datos en dispositivos conectados al pc
FTK Imager 4.3.1.0	Visor de imágenes forenses/datos	Imágenes, hash, visualización de datos
Autopsy 4.17.0	Visor de imágenes forenses y analizador de datos forenses	análisis, visualización de datos
CsvView	Herramienta de archivo DAT/Texto	Análisis. ARCHIVOS DAT
Datcon 4.0.4	Herramienta de archivo DAT/Texto	Análisis. ARCHIVOS DAT
ExtractDJI	Herramienta de archivo DAT/Texto	Extraer/ descomprimir archivos DJI DAT
App.airdada.com	Herramienta web que permite subir logs para su análisis	Decodificar logs generados por drones

Tabla 2. Herramientas para la investigación
Fuente. Autor.

Metodologia.

El propósito primordial del trabajo presentado en este artículo es preservar, obtener, analizar y examinar los datos suministrados por las muestras de drones seleccionados los cuales fueron incautados simulando un ámbito real , para lo que hay reglas internacionalmente aceptadas y se encuentran en vigencia, las cuales se adaptan al sistema judicial de Ecuador y explican la mejor manera de hacer una adecuado análisis forense,

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

las normas más aceptadas por peritos informáticos son: UNE: 71505-3:2013, ISO 27037, RFC 3227, entre otras.

la metodología es experimental a partir de una investigación descriptiva-explicativa. De esta manera, se obtendrá información forense sobre vehículos no tripulados para la toma de decisiones proactivas, en la figura1 que se muestra a continuación podemos apreciar la metodología resumida basada en el trabajo de (Chamba, s. f.) a aplicarse en esta investigación.

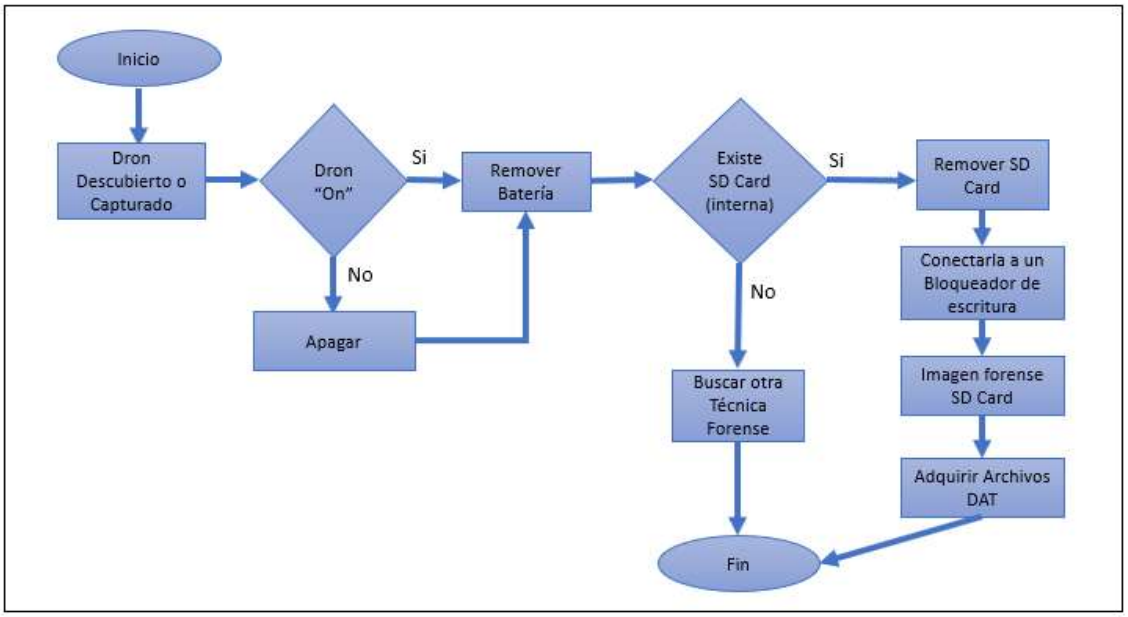

Figura 1. Metodología resumida
Fuente. Autor.

La Tabla2 anterior muestra la lista de hardware y software utilizados en el experimento, que comprende los siguientes pasos:

1) Entorno de prueba y equipo: El primer paso implica la incautación o captura de UAVs, sin los controladores remotos ni dispositivos de control externo. Para lo cual se procedió a solicitar los drones con el último vuelo realizado con el fin de simular un ambiente real de incautación sin alterar la configuración previa de vuelo seleccionada por el piloto y sin intervención del analista forense.
2) Creación de escenarios: Los vuelos se realizaron en diferentes lugares, en diferentes días y en diferentes momentos por cada uno de los pilotos de los drones, Se grabaron vídeos y se capturaron y almacenaron varias imágenes tanto en las memorias internas como externas.
3) Adquisición de datos: se centró en adquirir imágenes forenses digitales de cada uno de los UAV. Comenzamos esta fase usando FTK Imager para obtener una imagen física de las tarjetas micro SD externas ubicadas en todas las muestras de drones. Con los drones apagados, se procedió a la extracción de las tarjetas micro SD para luego colocarlas en el bloqueador de escritura de la tarjeta SD, con el objetivo de evitar escrituras de datos. Después de eso se obtuvo la

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

imagen usando FTK Imager y se comprobaron los hashes generados. Se extrajeron datos de los componentes restantes de los drones de la siguiente manera:

4) Memorias internas: El almacenamiento interno del **Dji mini2** se adquirió conectando el dron mientras se enciende a la estación de trabajo forense, y mediante imágenes como si se tratara de una unidad USB estándar. En este paso lanzamos SAFE Block, un bloqueador de escritura basado en software, y obtuvimos las imágenes del DJI mini 2 Pro usando FTK Imager.

Resultados.

Esta sección proporciona un análisis y comparación de las muestras de drones seleccionados en términos de su preparación para el análisis forense. El propósito es determinar la aplicabilidad y capacidad de las herramientas forenses actualmente disponibles para analizar los datos de estos drones, se recuperaron y analizaron los siguientes tipos de datos:

a) Medios grabados

Mientras se examinó las imágenes forenses obtenidas de las micro SD externas tanto del dji phantom 3 Pro como del drone dji mini 2, se pudo localizar los archivos multimedia grabados. Estos archivos se pueden encontrar en la carpeta "/DCIM/100MEDIA". El formato de los archivos es JPEG para imágenes y MP4 para vídeos. El nombre de los archivos consiste en de un prefijo DJI" seguido de un número de 4 dígitos que se mueve hacia arriba cada vez que se crea un nuevo archivo, por ejemplo (DJI0001. MP4).

Las fotos y los vídeos se exportaron para su posterior análisis.

b) Datos EXIF

Los datos EXIF (archivo de imagen intercambiable) son información incrustada dentro de imágenes JPEG. Las herramientas utilizadas fueron autopsy y exif tool, pudieron analizar y mostrar datos EXIF, la herramienta exif analizo los datos mejor que autopsy. Los datos EXIF obtenidos fueron:

Fecha, Marca de tiempo, Fuente de archivo, GPS, Altitud, Referencia de altitud, Latitud, Longitud. Esta información ayudara a determinar dónde y cuándo se tomaron las fotos.

También vale la pena mencionar que los drones al estar asociados o vinculados con un dispositivo inteligente tomo como referencia la configuración de hora y fecha del dispositivo, y al modificar el sistema de tiempo en el dispositivo inteligente, los archivos creados por los drones tendrían la marca de tiempo modificada.

c) Datos de registro de vuelo DJI Dron, archivos BlackBox

DATfiles: Los archivos internos del dron adquiridos con la herramienta FTK imager eran archivos de datos con un formato (.dat). Estos archivos guardan datos binarios que sólo pueden ser decodificados por la aplicación que los generó. Los archivos de registro tienen numerosos parámetros relacionados con la ubicación y la velocidad. Los archivos

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

DAT encontrados fueron nombrados utilizando una convención de nomenclatura estándar de: AAAA-MM- DD_[HH-MM- SS]-(Número de serie de los drones).dat.

Se utilizó una herramienta común, CsvView/Datcon, para realizar esta tarea además de la herramienta autopsy que en sus últimas versiones posee un módulo para decodificar estos archivos. La herramienta se descargó e instaló en la estación de trabajo, y los archivos DAT comprimidos se extrajeron utilizando EXTRACTDJI, una herramienta dentro de Datcon. A continuación, los archivos se cargaron en CsvView obteniendo el siguiente análisis.

- **DJI Phantom 3**:luego de aplicar la metodologia y analizar la imágenes forenses se observa lo siguiente: en la micro sd del gimbal solo se obtuvo imágenes y videos que contenían metadatos que brindan información muy útil como la posición de dron mediante los datos gps en cada una de las imágenes y de los videos, además de la altura y fecha en la que se tomaron las imágenes y los videos respectivamente, al analizar los videos se encontraron videos con dos formatos diferentes con extensión.mov y con extensión .mp4 lo inusual sucedió con los archivos .mov ya que no poseían metadatos de la posición gps ni de la altura solo posen metadatos de la fecha de creación, modificación y acceso , en el caso de los videos con formato .mp4 además de los metadatos de fechas de modificación, creación y acceso si se pudo encontrar metadatos de posición gps aunque no de altitud.

  En la microSD interna se encontraron varios archivos con extensión .DAT los mismos que contenían en su interior datos muy importantes como la velocidad ubicación y altura del dron así como registros de errores ademas de información como la velocidad de los motores, inclinación del dispositivo, para obtener esta información fue necesario analizar estos archivos con la herramienta DatCon y CsvView las cuales brindan mucha información de cada uno de los archivos .DAT encontrados, esta tarea se vuelve un tanto monótona ya que no todos estos archivos poseen datos gps que son los que resultan interesantes para esta investigacion, otros simplemente tienen registros de errores por lo que ayudarse de la herramienta autopsy es de mucha ayuda ya que la misma si pudo analizar estos archivos .DAT y muestra un resultado agrupado de cuales poseen datos de gps, estos archivos no poseen metadatos relevantes ya que la información útil se encuentra en el interior de estos archivos, la información de los metadatos se limita a la fecha de acceso modificación y creación del archivo y los permisos que posee el archivo en es te caso es rw.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

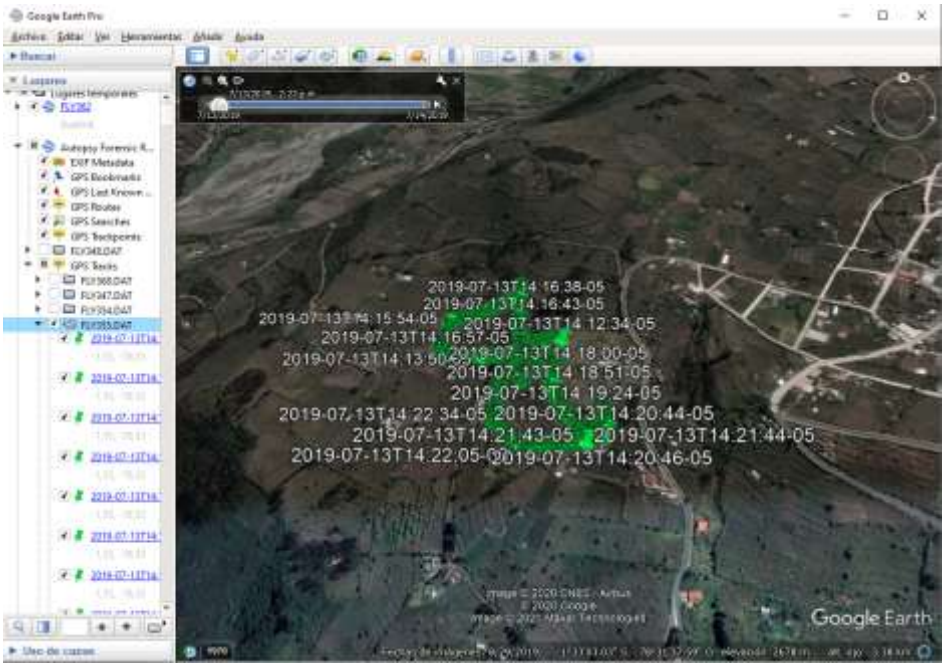

Figura 2. Rutas de vuelo obtenidas de archivos .DAT
Fuente. Autor.

- **LHI racing drone 250:** Este dispositivo no cuenta con almacenamiento externo de datos ni ranura para micro sd por lo cual no se puede aplicar la metodología propuesta debido a la falta de memorias de almacenamiento externo, sin embargo el dispositivo posee una memoria de 64kbits para alojar el firmware del dispositivo, el cual es el encargado de controlar el funcionamiento del mismo, este dispositivo posee un diseño muy ligero y compacto debido a su propósito el cual es alcanzar la mayor velocidad y poder realizar maniobras aéreas por lo que su diseño no incorpora gps ni Cámara para aligerar el peso y no sobrecargar el procesamiento del dispositivo, los componentes son los esenciales para realizar un vuelo y aligerar el peso de la aeronave, los motores y la batería son de gran tamaño permitiéndole alcanzar grandes velocidades y buena autonomía.

Figura 3. Componentes de Racing dron
Fuente. Autor.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

- **Dron Dji mini 2:** Este dispositivo solo posee una memoria externa de fácil acceso en la cual se almacenan los datos que registra el dron en una carpeta con el nombre log y en su interior se encuentran tres archivos que son logs del sistema logs de la cámara y log de vuelo los cuales encuentran encriptados , junto a esta carpeta se encuentran una carpeta con el nombre 100media la cual contiene los archivos multimedia creados por el dron. , los datos de vuelo se extraen con un software propio del dron llamado dji asistant el cual genera un archivo encriptado llamado "EXPORT_FILE_2021-02-24_19-31-55.DAT" a este archivo se lo proceso con las herramientas DATCON y CsvView sin lograr resultados ya que el método de encriptación es nuevo dando como consecuencia archivos de 0 KB, los datos de vuelo como altitud, posiciones gps se las obtuvieron a partir de los metadatos de las imágenes y videos con las herramientas autopsy y exif tool, esta última brindo mayor cantidad de metadatos y de una forma más ordenada para el análisis individual de los archivos multimedia, se logró obtener los datos de vuelo y las ubicaciones gps incluyendo número de serie y nombre del dispositivo mediante una página web https://app.airdata.com en la cual se creó una cuenta y luego se ingresó el usuario y la clave de acceso de la cuenta dji de la persona que opero la aeronave, luego de unos momentos se pudo observar cómo se sincronizaban los datos que están en la nube permitiendo observar los datos de vuelo, los logs y toda la actividad realizada por el dron, además esta página permite subir archivos logs manualmente para su análisis volviéndose muy útil para esta investigación.

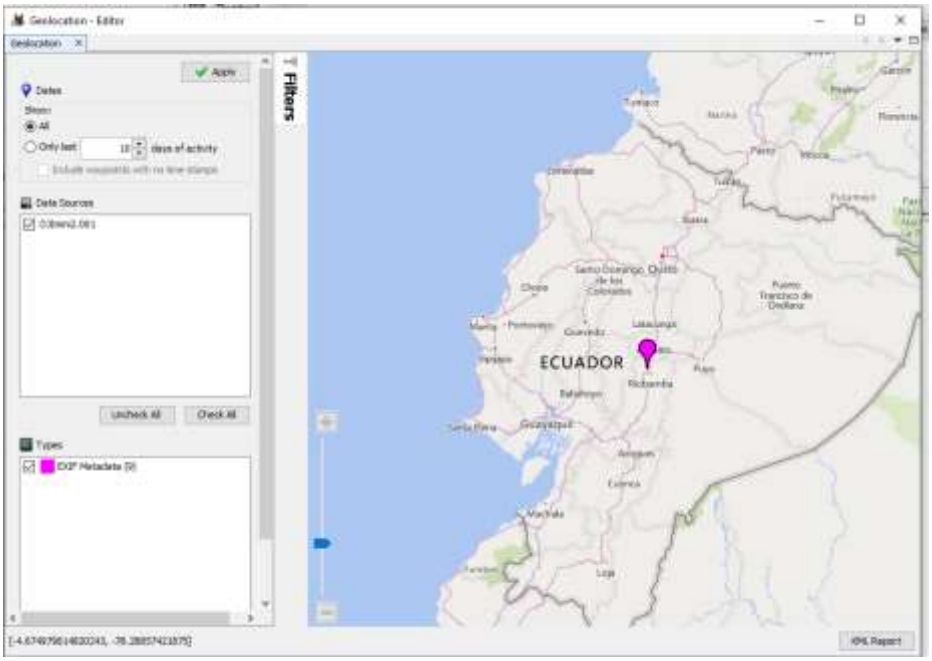

Figura 4. Posiciones Gps obtenidas de los metadatos con Autopsy
Fuente. Autor.

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

Figura 5. Información obtenida de la página web app.airdata.com
Fuente. Autor.

- **Intel aero Ready to fly:** este dispositivo posee una ranura para microSD además de una ranura pci expres para conectar un disco duro con formato M.2 ssd , ademas de una memoria interna de 32Gb en formato emmc como disco duro y 4 gb de memoria ram LDDR3 a 1600 Mhz las cuales estan soldadas a la placa cabe mencionar que este dron posee un microprocesador Intel atom y un puerto de comunicaciones micro usb 3.0 otg por esta razón posee una arquitectura muy parecida al de una computadora, al momento de realizar el análisis el dispositivo no contaba con ninguna unidad de almacenamiento externa ni microSD ni disco duro ssd solo funciono con el sistema operativo interno que se encuentra instalado en la memoria emmc interna por lo cual la metodología planteada para el análisis no es aplicable al no poseer un dispositivo de almacenamiento extraíble, se trató de buscar archivos multimedia en la memoria interna con el dispositivo encendido y por una conexión ssh sin lograr ningún resultado, lo que si se pudo observar es que la memoria interna posee tres particiones una partición de 28 Mb para el arranque en formato efi, la segunda partición de 27.7 gb para el sistema de archivos que está basado en Linux sin interface grafica por defecto aunque el fabricante indica que se lo puede instalar Ubuntu Desktop en la versión 16.04.X pero se recomienda la versión 16.04.3 en esta ya tendría interface gráfica, y la tercera partición de 1.5 Gb como memoria de intercambio swap, este análisis se lo hizo sin aplicar un procedimiento forense ya que la memoria se encuentra soldad a la placa y se necesitaría extraerá y un dispositivo especial para su lectura que no se encuentra en el país además que para volver a soldar esta memoria se volvería muy complicado por la necesidad de una estación de soldadura especial, por lo que se optó por sacar una imagen forense con el dispositivo encendido, insertando una memoria micro sd de 64 gb para posterior formatearla en formato ext4 y montarla en el sistema ya que no permitía montarla con el formato fat 32 que viene por defecto la micro sd, posterior a esto se creo la imagen forense con el comando dd para posterior analizar esta imagen con las herramientas antes mencionadas y concluyendo que no se encontraron archivos multimedia solo se pudo explorar los archivos del sistema que no brindaron información útil para esta investigaciones que los archivos de registro del sistema se encuentran encriptados por el sistema operativo y no se pudo extraer la información con las herramientas

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

planteadas .

Figura 6. Componentes de dron Intel Aero Ready to fly
Fuente. Autor.

Conclusiones.

- **LHI racing drone 250**: Este dispositivo no genera archivos de registro ya que no posee una memoria de almacenamiento y al no poseer Cámara ni gps tampoco guarda evidencia multimedia, por lo cual se puede concluir que la metodología no puede ser aplicada debido a la falta de las mismas, sin embargo el dispositivo posee una memoria de 64kbits para alojar el firmware del dispositivo en formato hexadecimal, el cual es el encargado de controlar el funcionamiento del mismo, y sería la única información que posee este dispositivo y no resulta relevante para esta investigación, además posee un diseño muy ligero y compacto debido a su propósito el cual es alcanzar la

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

mayor velocidad y poder realizar maniobras aéreas por lo que su diseño no incorpora gps ni Cámara para aligerar el peso y no sobrecargar el procesamiento del dispositivo.

En esta familia de dispositivos que están orientados a la velocidad se puede encontrar nuevas versiones como la controladora SP Racing F3 Evo la cual permite insertar una microSD como almacenamiento interno, para funcionar como caja negra (black box) el cual almacena los datos de vuelo(Flight Data Logs) y se lo podría analizar en una futura investigación.

- El dron Dji mini2 guarda los datos de vuelos y los archivos multimedia en una misma microsd por esta razón no es necesario desmantelar el dron para acceder a los mismos ya que se encuentran en la parte trasera y son de fácil acceso por lo cual de este dron solo se obtuvo una imagen forense para su análisis, para una posterior investigación se sugiere realizar un análisis de la encriptación de este modelo de dron para la obtención de los datos de vuelo.
- El dron Dji phantom 3 profesional posee una memoria para el almacenamiento multimedia de fácil acceso colocado en el gimbal de la cámara y además posee una tarjeta microSD adicional en el interior de la tarjeta madre de difícil acceso por lo cual se tuvo que desarmar el dron para acceder a la misma, por esta razón se generaron dos imágenes forenses para el análisis la una con datos multimedia y la otra solo con datos de vuelo , los archivos generados por este modelos fueron cifrados y se pudieron procesar utilizando CsvView/Datcon para una mejor visualización se exportaron la ubicaciones gps a Google Earth mediante la herramienta autopsy. Cabe mencionar que en este modelo de dron la información obtenida de la ubicación gps de los metadatos se pude contrastar con la información gps obtenida de los archivos .DAT de la segunda microsd
- Dron Intel Aero Ready to fly: Este dispositivo no tenía ninguna memoria de almacenamiento interno conectada al mismo al momento del análisis, sin embargo se tuvo que adaptar la metodología para investigar su memoria interna (no extraíble) , se procedió a insertar una microsd y crear una imagen forense del sistema raíz con el comando dd y con el dispositivo encendido para su posterior análisis concluyendo que con las herramientas planteadas no se pudo extraer información relevante para esta investigación ya que los datos de vuelo están encriptados por el sistema operativo, se sugiere crear una metodología especifica en una posterior trabajo para este tipo de dron ya que su arquitectura se asemeja más al de una computadora que a la mayoría de drones comerciales y en condiciones de laboratorio controladas ya que este dron posee muchas variables que lo diferencian como el sistema operativo basado en Linux que le permite ser más configurable ya que puede ser programado en Python para realizar

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

tareas específicas, la opción de añadirle un disco duro ssd además de la opción de almacenamiento por microSD y el control se lo realiza con un mando y una computadora lo que requeriría una investigación más profunda en este dron tan complejo.

La metodología aplicada es de gran utilidad siempre y cuando el dron cuente con una memoria de almacenamiento extraíble además se puede complementar la aplicación de esta metodología teniendo acceso a los dispositivos de radio control ya sean mandos inalámbricos, dispositivos inteligentes o computadoras puesto que en estos dispositivos también se almacenan logs, aplicando metodologías específicas de acuerdo con el dispositivo obtenido.

Referencias bibliográficas.

Barton, T. E. A., & Azhar, M. A. H. B. (2018). Open Source Forensics for a Multi-platform Drone System. En P. Matoušek & M. Schmiedecker (Eds.), *Digital Forensics and Cyber Crime* (pp. 83-96). Springer International Publishing. https://doi.org/10.1007/978-3-319-73697-6_6

Barton, T. E. A., & Hannan Bin Azhar, M. A. (2017). Forensic analysis of popular UAV systems. 2017 Seventh International Conference on Emerging Security Technologies (EST), 91-96. https://doi.org/10.1109/EST.2017.8090405

Bonetti, G., Viglione, M., Frossi, A., Maggi, F., & Zanero, S. (2013). A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives. Proceedings of the 29th Annual Computer Security Applications Conference, 269-278. https://doi.org/10.1145/2523649.2523660

Bouafif, H., Kamoun, F., Iqbal, F., & Marrington, A. (2018). Drone Forensics: Challenges and New Insights. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1-6. https://doi.org/10.1109/NTMS.2018.8328747

Chamba, J. R. J. (s. f.). DISEÑO DE UN MARCO METODOLÓGICO PARA ANÁLISIS FORENSE DE DRONES USADOS PARA ESPIONAJE APLICADO A LAS LEYES ECU. 72.

Clark, D. R., Meffert, C., Baggili, I., & Breitinger, F. (2017). DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III. Digital Investigation, 22, S3-S14. https://doi.org/10.1016/j.diin.2017.06.013

Horsman, G. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digital Investigation, 16, 1-11. https://doi.org/10.1016/j.diin.2015.11.002

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

Kao, D.-Y., Chen, M.-C., Wu, W.-Y., Lin, J.-S., Chen, C.-H., & Tsai, F. (2019). Drone Forensic Investigation: DJI Spark Drone as A Case Study. Procedia Computer Science, 159, 1890-1899. https://doi.org/10.1016/j.procs.2019.09.361

Manzano, A., & Fabricio, M. (2015). DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR [Thesis, Universidad Internacional SEK]. http://localhost:8080/xmlui/handle/123456789/1417

Paruma, Ó. A. L. (s. f.). INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS. 22.

Rivas, G. (s. f.). Metodología para un análisis forense. 55.

Sánchez Herrera, K. E., & Basantes Salazar, C. A. (2016). Análisis forense a sistemas operativos mediante la utilización de herramientas Open Source, caso estudio Windows 8. http://repositorio.espe.edu.ec/jspui/handle/21000/11954

Tacuri, J., & Maribel, A. (2012). Análisis del Crimen Cibernético en la Actualidad en la Ciudad de Cuenca. http://repositorio.uisrael.edu.ec/handle/47000/581

Toro-Alvarez, M., Jaimes, W., & Ortiz, E. (2018). Fundamentos de la investigación forense en ambientes informáticos. https://doi.org/10.13140/RG.2.2.20143.79523

Yousef, M., Iqbal, F., & Hussain, M. (2020). Drone Forensics: A Detailed Analysis of Emerging DJI Models. 2020 11th International Conference on Information and Communication Systems (ICICS), 066-071. https://doi.org/10.1109/ICICS49469.2020.239530

ISSN: 2600-5859
Vol. 4, N°4, p. 51-69, octubre-diciembre, 2021

PARA CITAR EL ARTÍCULO INDEXADO.

Guerrero Montero, C. A., & Pazmiño Gómez, L. A. (2021). Análisis informático forense a vehículos aéreos no tripulados (dron) . ConcienciaDigital, 4(4), 51-69. https://doi.org/10.33262/concienciadigital.v4i4.1884