UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERIAS

Plan de Investigación de fin de carrera titulado:

"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"

Realizado por:

JAIME RAFAEL JARAMILLO CHAMBA

Director del proyecto:

Ing. Luis Fabián Hurtado Vargas, MGS.

Como requisito para la obtención del título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

DECLARACION JURAMENTADA

Yo, JAIME RAFAEL JARAMILLO CHAMBA, con cédula de identidad #1104217797, declaro bajo juramento que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y, que ha consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Jaime Rafael Jaramillo Chamba
C.C.: 1104217797

DECLARATORIA

El presente trabajo de investigación titulado:

“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”

Realizado por:

JAIME RAFAEL JARAMILLO CHAMBA

como requisito para la obtención del Título de:

MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN EN SEGURIDAD DE REDES Y COMUNICACIÓN

ha sido dirigido por el profesor

ING. LUIS FABIÁN HURTADO VARGAS, MGS.

quien considera que constituye un trabajo original de su autor

Luis Hurtado
DIRECTOR

PROFESORES INFORMANTES

ING. DIEGO RIOFRIO, PhD.
ING. CHRISTIAN PAZMIÑO, MsC.

Después de revisar el trabajo presentado,
lo ha calificado como apto para su defensa oral ante
el tribunal examinador

ING. DIEGO RIOFRIO, PhD.

ING. CHRISTIAN PAZMIÑO, MsC.

Quito, 17 de octubre del 2018

DEDICATORIA

El presente trabajo realizado para culminar el logro de mi sueño profesional se lo dedico:

A Dios, por darme sus bendiciones en el transcurso de mi carrera estudiantil dentro de la Universidad, iluminándome día a día para conseguir mis objetivos propuestos.

A mi madre, por ser el pilar fundamental en toda mi vida, por brindarme amor y apoyo incondicional, e inculcarme siempre el estudio como la mayor herencia dada por los padres.

A mis hermanos, por estar conmigo en cada una de las metas que he conseguido y por apoyarme siempre en cada uno de mis proyectos propuestos a nivel profesional.

A mi padre, por darme su apoyo incondicional en cada uno de los objetivos que me he propuesto.

Jaime.

AGRADECIMIENTOS

Al Ing. Fabián Hurtado por su acertada dirección de la tesis. Su profesionalismo y entrega fueron determinantes a la hora de conformar este documento.

Al Ing. Diego Riofrio quien con su lectura aportó una visión diferente e integradora de mi investigación.

A la Universidad Internacional SEK, por su esfuerzo de formar profesionales legítimos.

Finalmente, a todos mis compañeros de la carrera ya que juntos logramos formar una amistad tanto personal como profesional.

RESUMEN

La tecnología que utilizan los drones ha avanzado notablemente en el desarrollo de modelos aerodinámicos sofisticados. En la actualidad los drones son utilizados para: control de tráfico, coberturas de eventos, captura de imágenes en lugares de difícil acceso, envío de correspondencia de bajo volumen en cortas distancias, sistemas de video vigilancia, entre otros.

Sin embargo, la utilización de drones ha suscitado algunos riesgos, ya que pueden ser aprovechados para cometer actos ilícitos como carga de sustancias no permitidas o como medios de espionaje. Además, presentan bajos costos monetarios que permiten al usuario adquirirlo fácilmente y utilizarlo para actividades maliciosas como vigilancia remota no autorizada.

El espionaje realizado con un dron se está convirtiendo en un arma potente, puesto que las imágenes captadas por estos dispositivos pueden revelar información que compromete la seguridad de la persona que es víctima de este delito.

Éste trabajo presenta el diseño de un marco metodológico de análisis forense para drones usados en el espionaje, aplicándolo a las leyes ecuatorianas, tomando como caso de estudio el dron DJI PHANTOM III STANDARD. Para esto, este trabajo proporciona una guía que describa el procedimiento de extracción de la evidencia digital encontrada en la memoria interna del Vehículo Aéreo no Tripulado, que permitirá cuidar la integridad de la información.

Palabras Claves: Análisis Forense, DatCon, DJI Phantom III Standard, Informática Forense, Perito Informático.

ABSTRACT

Technology used by drones has advanced remarkably regarding the development of sophisticated aerodynamic models. Nowadays, drones are used in applications like traffic control, events coverage, image capturing in hard access locations, low-weight package delivery for short distance and video surveillance among others.

However, the use of drones has come along with some risk since they may be used for illegal activities such as transport of prohibited substances or espionage means. Furthermore, a drone is low-priced and that allows the user to easily get it. And once its obtained, use it for malicious activities like remote unauthorized surveillance.

Espionage done with drones is becoming a powerful weapon, since the images captured by these devices can reveal compromising information regarding security of the people victims of this felony.

This work presents the methodology design of forensic analysis for drones used in Espionage, applying Ecuadorian laws and taking as a case of study the drone model DJI PHANTOM III STANDARD. Providing the steps to follow to extract the digital evidence found in the Unmanned Aerial Vehicle intern memory which will allow to protect the information integrity.

Key Words: Forensic Analysis, DatCon, DJI Phantom III Standard, Forensic Informatics, Informatics Expert.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

CAPITULO I

INTRODUCCIÓN

Los drones son dispositivos con gran impacto tecnológico en la sociedad, se pueden convertir en medios de almacenamiento de información con diferentes finalidades. Si se tiene en cuenta que estos vehículos aéreos no tripulados tienen la habilidad de llegar a grandes distancias para obtener capturas fotográficas, así como videos en tiempo real que revelen datos comprometedores de determinados objetivos, se puede iniciar una causa de litigio legal y ser declarado el dron como una fuente de información que puede establecerse como evidencia digital y ser determinante en un proceso legal.

Es importante mencionar que la empresa China DJI, produce dos modelos de aviones no tripulados y controlados de forma remota, el modelo Phantom y el modelo Inspirare en sus diferentes series. Sin embargo, la investigación se enfoca en el análisis forense de la Phantom III Standard, considerando el análisis estadístico proporcionado por la empresa estadunidense Statista GmbH [1] que determina que el 75 % del mercado está copado por la marca DJI.

Además, con el aumento en popularidad y la utilización de este dispositivo por parte de la población civil, es necesario la aprobación de leyes en el sistema judicial de Ecuador con respecto al uso de drones en espacios públicos. ´

Los aviones no tripulados también han tenido un impacto en las actividades terroristas. por ejemplo, el Estado Islámico ha llegado a utilizar drones con fines de vigilancia. Además, en esta investigación menciona que los grupos terroristas no está usando aviones de grado militar, sino que están recurriendo a drones disponibles comercialmente en la cual se incluye la serie DJI Phantom en diferentes versiones.(Marín, 2018)

No obstante Ecuador dispone de leyes estipuladas en el Código Orgánico General de Procesos (COGEP) y el Código Orgánico Integral Penal (COIP), que pueden ser interpretadas para sancionar actividades ilícitas como: la invasión de la privacidad de un individuo, la manipulación de información digital estipulada en la Ley de Comercio Electrónico, por otra parte, no existen leyes que sancionen directamente delitos relacionados con el espionaje utilizando drones.

Asimismo, debido al crecimiento en popularidad de drones junto con el pico en la actividad criminal, existe la necesidad de la creación de una metodología de análisis forense de drones entregando como producto una guía que permita extraer la información y el perito la pueda utilizar como evidencia en proceso judicial.

Sin embargo, uno de los grandes problemas al hablar de evidencia digital, es la falta de información de la estructura interna y funcionamiento de un dron en general, dificultad

[1] https://es.statista.com/estudio/40579/la-industria-mundial-de-drones/

que no le permite a los peritos acreditados por el Consejo de la Judicatura realizar un procedimiento adecuado para ejecutar un análisis forense exitoso, por lo cual, es necesaria la creación de este marco metodológico de análisis forense diseñando una guía que indique la forma correcta de extracción y análisis de información.

Inicialmente la investigación presenta la sección en la que se crea el escenario de un caso de espionaje, ahí se establecen las coordenadas de geoposicionamiento por parte del investigador con el fin de comparar ésta con la información extraída de la memoria interna del dron, y finalmente establecer en base a los hallazgos, que el dron capturado tuvo como objetivo realizar la actividad de espionaje en el lugar determinado por el escenario.

De acuerdo con el razonamiento que se ha venido realizando, el análisis forense que se propone, se lo realiza a un dron DJI Phantom III Standard, del mismo modo, la guía proporciona 36 pasos para realizar el análisis forense de este tipo de dron, los mismos que indican el procedimiento para extraer el dispositivo de almacenamiento interno del dron y analizar la información del vuelo del caso de estudio que se generó.

Luego se tomó como referencia normas vigentes para la realización de buenas prácticas forenses, en este caso se realizó el producto de esta investigación basándose en las normas UNE: 71505-3:2013 y RFC-3227, que dentro del sistema pericial son las utilizadas con más frecuencia. En consecuencia, de las normas ya mencionadas, la metodología se fundamenta en cinco fases: Preservación, Adquisición, Documentación, Análisis y Presentación. Al realizar la ejecución de cada una de estas fases, se obtiene como resultado una guía que garantiza la ejecución de un correcto análisis forense cuidando la integridad de la información.

Más adelante se encuentra la sección que describe la Fase de Análisis de datos, en donde se estudian los archivos adquiridos de la memoria interna del dron a partir de la metodología creada. Los archivos llevan la estructura de nombre del archivo generado por defecto: FLY01.DAT, el mismo que contiene información del estado del vuelo del dron. En esta sección la información se encuentra codificada, para lo cual se debe utilizar una herramienta que permita la conversión a un formato que pueda ser legible para el perito que analiza la evidencia.

Entonces, para la decodificación de la información contenida en este archivo se hace uso de la herramienta DatCon que es un código abierto especializado en la conversión de archivos codificados generados por Drones de la marca DJI (las características de este software se las detalla en el marco teórico de esta investigación).

Posteriormente, se obtiene un archivo con extensión CSV con la información decodificada por el software antes mencionado, entre la cual se encuentran datos del GPS que indican las coordenadas de geoposicionamiento del dron al momento de realizar el despegue.

Luego, se discuten los resultados que se obtienen analizando las coordenadas del GPS en el momento que se creó el escenario y los datos obtenidos en base a la altitud y longitud del archivo decodificado, en los que se encontró una coincidencia aproximada

de un 90 %, tomando en cuenta que la aplicación de control que toma esta información para que el dron regrese a su punto de origen, presenta un error de un 10%.

Finalmente, el trabajo presenta como producto final una guía que determina paso a paso la correcta forma de extracción de la memoria interna del dron sin causar daños externos e internos en la estructura del dron, luego se presentan los pasos para la creación de una imagen forense del cual se extrae y comprueba el código MD5 Hash que permite comprobar la legitimidad e integridad de la información.

1.1 PROBLEMA DE LA INVESTIGACIÓN

1.1.1 Planteamiento del problema

La tecnología de los vehículos aéreos no tripulados no es reciente, según Cuerno, García, Sánchez, Carrio, Sanchez, Campoy (2016), en 1918 se realizó el primer vuelo controlado de manera remota, después de 14 años del invento de los hermanos Wright. Sin embargo, durante la primera guerra mundial no tuvo un gran desarrollo este tipo de tecnología por problemas internos de funcionamiento (giroscopio, sistemas de radiofrecuencia), dando paso al desarrollo de la aviación comercial.

En el mismo artículo menciona que, ya a finales de la primera guerra mundial se da inicio a una nueva era tecnológica de los Vehículo Aéreo no Tripulado (VANT), en 1927 el ejército británico realizó el primer dispositivo capaz de desplazarse 480 Km controlada de manera remota y cargado de armamento bélico, dando el inicio a la fabricación de estos dispositivos con fines militares. Como era de esperarse potencias mundiales como Estados Unidos, Rusia y Alemania, empezaron a incursionar en esta nueva tecnología ya en la segunda Guerra Mundial, utilizándolos también como herramientas de reconocimiento de territorio. (Cuerno et al., 2016)

Luego de la segunda guerra mundial se empieza la fabricación de estos dispositivos con para aplicaciones civiles, que en un principio solo eran utilizados para reconocimiento de terreno y video vigilancia. Sin embargo, las grandes empresas confiaron en el desarrollo tecnológico de los VANT de tal manera que la utilidad y los servicios que brindan han tenido una gran acogida. Los sistemas de control son cada vez más interactivos con el usuario, empresas como DJI que acaparan el 75% (ver figura 1) del mercado de drones presenta un importante número de modelos con versiones mejoradas.

Por otra parte, se está presentando un problema social en base a los avances de la tecnología de un VANT, todo inicia con la fácil accesibilidad que tienen cualquier persona civil para adquirir uno de estos dispositivos, el único requisito es tener los recursos económicos para comprarlo, como se mencionaba anteriormente los sistemas de control remoto de los drones son fáciles de manipular y entender, basta con leer el manual y realizar uno o dos vuelos de prueba para dominar sus funciones.

Entonces, el problema radica en que no todas las personas que adquieren un dron tiene la intención de darle una buena utilidad, existen personas que tienen fines delictivos

para aplicaciones con estos dispositivos, la video vigilancia con drones tiene otra connotación cuando los delincuentes realizan capturas de imágenes o graban videos a determinados objetivos sin el consentimiento de ellos.

Ante el delito de espionaje cometido por el usuario del dron, es necesario que este dispositivo sea involucrado dentro del proceso legal. Se debe considerar que el dron es un dispositivo de almacenamiento de información digital, entonces, se pueden realizar procedimientos forenses por parte de un perito informático para encontrar evidencia digital y ser analizada.

Sin embargo, no existe información disponible de la estructura interna de un dron y su funcionamiento. Los fabricantes de estos dispositivos, tomando como referencia la empresa DJI, revelan información de la existencia de concretamente dos dispositivos de almacenamiento los cuales albergan algún tipo de información que con la ayuda de este trabajo se podrá descubrir de que tipo es y si puede ser determinante como evidencia digital dentro de un litigio legal.

Finalmente, con este trabajo al no existir una un procedimiento forense de extracción de evidencia digital de un dron, se realizará una metodología de análisis forense para un dron DJI Phamton III Standard como caso de estudio con el fin de establecer una guía para extracción de la memoria interna y análisis de la información que contiene, proporcionando al perito informático una herramienta válida que permita el correcto proceso forense.

1.1.2 Diagnóstico del Problema

Debido a la falta de información técnica disponible que ayude a entender el funcionamiento y la composición interna de la estructura de un dron, se presentan casos en los que la evidencia no puede ser procesada, se ha tomado como ejemplo un caso del Laboratorio de Criminalística y Ciencias Forenses de la ciudad de Quito, donde reposa como evidencia de un delito un Dron DJI Phantom del cual no se supo especificar que versión de la marca corresponde.

Dadas las condiciones que anteceden, se le realizó una entrevista al capitán Diego Vicente Guerra Santana, jefe del departamento de Audio y Video del Laboratorio de Criminalística y Ciencias Forenses de la ciudad de Quito que comentó: “las personas encargadas de procesar la evidencia albergada en este artefacto no pueden extraerla al no contar con un procedimiento estándar que garantice la integridad de la información al lograr ser obtenida”. Es evidente entonces, que el equipo se encuentra almacenado en la bodega de dicho laboratorio. Por lo tanto, se entiende que el período de instrucción fiscal ha vencido y la evidencia no pudo ser judicializada.

Como puede observarse, en el Ecuador no se contemplan leyes específicas que tipifiquen los delitos realizados con la utilización de drones, sin embargo, algunas medidas se las puede encontrar dentro del Código Orgánico Integral Penal (COIP), en la SECCIÓN TERCERA en donde se estipulan artículos que sancionan este tipo de delitos. (ver anexo 1)

1.1.3 Pronóstico

Los antecedentes citados en el diagnóstico permiten deducir que el mundo se va digitalizado cada vez más y esto ha provocado que se genere un incremento de la tecnología disponible para realizar actividades delictivas informáticas involucradas con drones, que combinado con la poca información que expliquen la ubicación de los dispositivos de almacenamiento del dron y la falta de procedimientos forenses que garanticen la correcta extracción y análisis de la información, permitirá que las víctimas queden expuestas a casos de espionajes y no puedan establecer una prueba en base a la evidencia digital generada.

1.1.4 Control de Pronóstico

El dotar a los peritos informáticos con una metodología de análisis forense que incluya técnicas y herramientas que permitan brindar el conocimiento necesario a través de una guía con 36 pasos para la extracción y análisis de la información generada por el dron y almacenada en la memoria interna del mismo, podría convertirse en una solución donde los peritos informáticos contarán con los elementos necesarios que les ayude a realizar las pericias adecuadas en búsqueda de la evidencia digital, lo que ayudaría a solucionar parte de la problemática, así como motivar a futuros investigadores realizar este tipo de investigaciones para diferentes marcas y versiones de drones.

1.1.5 Formulación del Problema

De acuerdo con los razonamientos que se han venido realizando, si ocurre un delio de espionaje en el cual participe un dron de la marca DJI Phantom III Standard, la judicialización de la evidencia digital proveniente de este dispositivo, no se podrá procesar debido a la falta de información técnica de la estructura interna y funcionamiento por parte de los fabricantes, que permitan a los peritos informáticos realizar procedimientos forenses adecuados para la extracción y análisis de la información obtenida.

1.1.6 Objetivo General

Diseñar un marco metodológico para el análisis forense de drones DJI Phantom III Standard usados para el espionaje en el Ecuador, que permitan la búsqueda de datos digitales que puedan constituirse en una prueba y sirvan como un indicio útil y legal para un proceso judicial.

1.1.7 Objetivos Específicos

- Analizar la estructura interna y los datos generados por el sistema GPS del DJI Phantom III Standard, mediante el análisis forense de la memoria interna SD, para obtener los valores de geoposicionamiento del dron dentro del caso de estudio creado.

- Desarrollar un caso de delito de espionaje con un dron DJI Phantom III Standard, mediante la creación de un escenario controlado, para comparar los datos obtenidos con los valores del caso de estudio.

- Realizar el análisis forense con las herramientas expuestas a lo largo de esta investigación y descritas en la creación del marco metodológico de análisis forense, para sacar conclusiones de validez de la herramienta proporcionada para los peritos informáticos.

- Realizar una guía que indique el procedimiento de extracción y análisis de datos de la memoria interna del dron DJI PHAMTON III, basado en las normas vigentes de correctas prácticas forenses, para proporcionar una herramienta para los peritos informáticos.

1.2 JUSTIFICACIÓN

El crear un marco metodológico para el análisis forense de drones usados en el delito de espionaje, provee una solución a la falta de información técnica de drones que permita la judicialización de la evidencia digital almacenada en estos dispositivos, por lo cual, en la actualidad no existen procedimientos forenses para extraer evidencia digital almacenada en un dron.

Analizando la poca información disponible de investigaciones realizadas al funcionamiento de drones, específicamente a la marca expuesta en esta investigación (DJI), se considera que existen los elementos necesarios para recolectar evidencia digital del vehículo aéreo no tripulado DJI Phantom III Standard, en el momento en el que sea detenido y puesto en custodia por peritos legalmente acreditados por El Consejo de la Judicatura.

Es importante mencionar que la selección de esta marca de dron se hizo en base a un análisis que realiza la reconocida empresa de estadísticas Statista GmbH [2] que cuenta con un equipo de más de 450 estadísticos expertos en bases de datos, analistas y editores. Statista menciona que el mercado actual de drones se encuentra monopolizado por DJI con 75 puntos sobre 100, como se muestra en el siguiente gráfico.

[2] https://es.statista.com/estadisticas/674761/drones-desglose-porcentual-por-segmento-de-las-empresas-de-drones-del-mundo/

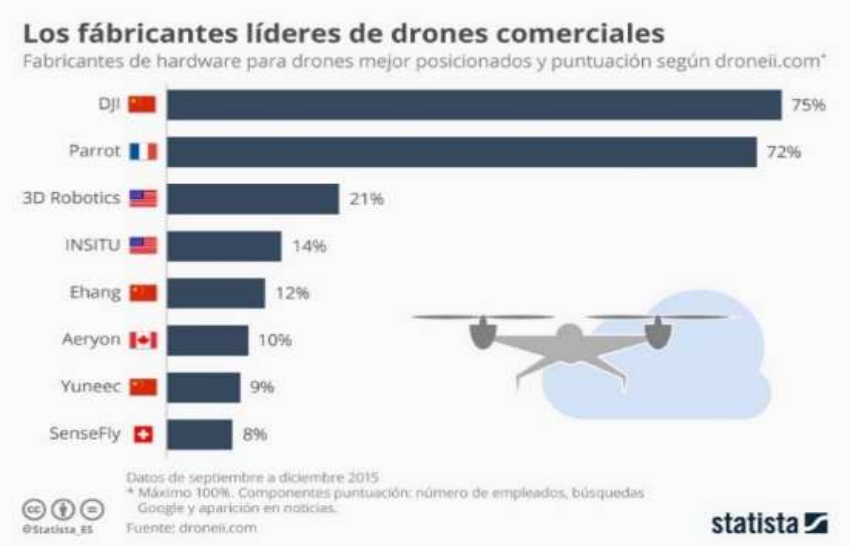

Figura 1. **Mercado de Drones.**
Tomada de Statista GmbH, 2015

Este trabajo además de proporcionar una herramienta válida para realizar una correcta práctica forense para un dron, ayudará a incentivar a otros investigadores que realicen futuras investigaciones de otros tipos de drones ya sea de la misma marca o de otras, especificando los tipos de metodologías correspondientes a cada una de ellos o a la vez en un futuro lograr tener un formato de análisis forense estándar a estos dispositivos.

1.3 MARCO TEÓRICO

1.3.1 Delitos Informáticos

En el Ecuador con el COIP existe la tipificación de algunos delitos informáticos, con penas de entre tres y cinco años, una de las limitaciones para el cumplimiento de la normativa y que se sigan tipificando más delitos en esta temática es la falta de conocimiento que existe no solo a nivel personal sino a nivel empresarial, la falta de denuncias, y en algunos casos la falta de evidencias encontradas al momento de realizar las respectivas pericias. (Loarte, 2018)

Ante el complicado panorama que actualmente existe por la lucha contra la falta de tipificación de los diferentes delitos realizados con artefactos tecnológicos proporcionará un razonamiento adecuado tanto para jueces y fiscales con el fin de propiciar una reforma en el Código Penal en donde se incluya a todos los delitos informáticos en todas sus modalidades que en años atrás no tenían sentencia o procedimiento a seguir, para que de esta manera todos los incidentes que se presenten se puedan judicializar de una forma adecuada. (Loarte, 2018)

1.3.2 Código Orgánico Integral Penal

El código integral penal fue publicado el lunes 10 de febrero de 2014 Registro Oficial Nº 180 El Código Integral Penal (COIP) “Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover

la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas."(Ministerio de Justicia, 2014)

1.3.3 Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos

Esta ley publicada en el Registro oficial N°557 de l 17 de abril del 2002, estipula "Art. 1.- Objeto de la Ley. - Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas".(Congreso-Nacional, 2012)

1.3.4 Resolución 040 – 2014

La Resolución 040 – 2014, es el Reglamento del Sistema Pericial Integral de la Función Judicial, que fue aprobado por el Pleno del Consejo de la Judicatura, el 10 de marzo de 2014; Donde, el Consejo de la Judicatura resolvió: "EXPEDIR EL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL". En el que en su artículo.1 muestra su ámbito de aplicación, que dice "Este reglamento regulará el funcionamiento y administración del sistema, pericial integral, en relación a la calificación, designación, obligaciones, evaluación, capacitación, régimen disciplinarlo y cualquier otro aspecto de los peritos que participen en los procesos judiciales, pre procesales, o de cualquier otra naturaleza que se lleven a cabo en la Función Judicial."(Consejo de la Judicatura, 2014). Ver el anexo 2.

1.3.5 Informática Forense

El desarrollo continuo de la tecnología ha permitido la creación de sistemas digitales avanzados, en el cual se realizan procesamientos de señales digitales y se guardan en diferentes sistemas de almacenamiento. La informática forense es la ciencia que presenta procedimientos que permiten extraer y analizar estos datos.

La informática forense forma parte de una de las ramas de las ciencias forenses, su aplicación se basa específicamente a la evidencia digital, permitiendo que un especialista pueda descubrir y tratar información digital encontrada en diferentes medios magnéticos, y pueda plantear hipótesis a partir de la interpretación de los datos.(Cano, 2015)

Es importante mencionar, que la informática forense presenta una estructura técnica por lo que se convierte en una importante herramienta para la informática forense moderna. La estructura que presentan las mayorías de normas de buenas prácticas forenses son las siguientes etapas: identificación, preservación, extracción, análisis, interpretación, análisis, interpretación, documentación y presentación. La aplicación organizada de cada una de estas etapas, ayudarán al especialista en temas informáticos redactar un informe pericial correcto.

Si se menciona de un especialista en temas de informática se está hablando de un perito informático que, además, debe tener conocimientos legales y técnicos para llevar a cabo

una investigación, en la cual se extraen y reúnen pruebas necesarias con la integridad de la información que sean válidas y sustentables frente a un juez o en un litigio legal.

1.3.6 Metodologías de Análisis Forense

Como se mencionaba en el apartado anterior, existen normas internacionales vigentes que se adaptan al sistema de justicia de Ecuador y describe la forma de realizar una correcta práctica forense, las normas más acogidas por adaptadas por peritos informáticos son: ISO 27037, RFC 3227, UNE: 71505-3:2013, entre otras.

Para el desarrollo de este trabajo se va a tomar como referencia las normas RFC 3227 y la UNE: 71505-3:2013, con la cual se puede interpretar cada una de las fases en la elaboración de la metodología de análisis forense para el dron.

De acuerdo a la norma UNE: 71505-3:2013 las fases para el análisis forense se dividen en cinco, como:

1. Fase de Preservación:

En esta fase el perito informático debe asegurarse que la información conserve la integridad de su contenido. Se debe realizar los procedimientos adecuados para que la información en el dispositivo de almacenamiento no se produzcan modificaciones o contaminación de la evidencia.

Es indispensable que el especialista, utilice guantes en el proceso de extracción de los dispositivos de almacenamiento para evitar que las huellas dactilares de la persona que realiza el análisis forense. Además, el perito debe sellar cada parte de la superficie que permita la desarticulación de la estructura, con la finalidad de que personas ajenas a la investigación puedan tener acceso a la evidencia.(Zúñiga, 2014)

2. Fase de Adquisición:

Lázaro (2013) menciona que en esta fase se va a realizar el procedimiento que permita obtener los archivos digitales para que el especialista pueda someterlos a un análisis. Además, para la extracción de los archivos digitales se debe realizar una copia a bajo nivel de todo el dispositivo en un medio físico que supere la capacidad de almacenamiento del objeto. El duplicado del dispositivo de almacenamiento no debe ser un simple backup de la información sino una imagen completa del medio de almacenamiento en donde consten: el espacio no asignado del sistema de archivos, documentos que hayan sido eliminados, entre otros.

Es importante mencionar que el equipo que contiene los sistemas de almacenamiento se lo puede encontrar en estado encendido como en estado apagado:

a) Equipo apagado

Como regla general no se debe encender el equipo, este, siempre debe mantenerse apagado, ya que si este es encendido se modificará la evidencia alterando los datos

originales. Loarte y Grijalva (2017) mencionan que, no se debe realizar análisis en la información general sino que se debe trabajar en la imagen del dispositivo a bajo nivel, utilizando las herramientas que mantengan la integridad de la información.

Además, es necesario que otra persona se encuentre presente en el momento que el perito esté en el proceso de recopilación de la información, esta persona se convertirá en testigo de las acciones que realice el perito.

> Sin embargo, “una regla importante es documentar toda la información sobre el soporte de almacenamiento de datos o si este se encuentra alojado en un equipo, números de serie, hora de inicio y de fin de cada uno de los procedimientos que se realicen, etc., de preferencia siempre es recomendable tomar una fotografía de lo mencionado anteriormente.”(Loarte y Grijalva, 2017, p.55)

b) Equipo encendido

En este estado del equipo se debe realizar la copia a bajo nivel de los sistemas de almacenamiento utilizando programas que no modifiquen la información cuidando su integridad. De la misma manera los programas que se utilizan para el análisis deben permitir solo lectura de los datos.

De cada uno de los soportes deberá realizarse la verificación de autenticidad por medio de la función hash, aplicando algoritmos que permitan la lectura de estos archivos cifrados asimétricos.

Es importante mencionar que no siempre es recomendable realizar el análisis en caliente (equipo encendido), ya que algunos dispositivos electrónicos necesitan de la suspensión de alimentación eléctrica para retirar sus partes internas y evitar algún daño en la desarticulación de sus partes (cortocircuito).

3. Fase de Documentación:

En esta fase el perito informático debe contar con los elementos mínimos para redactar el informe pericial, de tal manera que todas las fases del análisis forense queden plasmadas en el documento, tal y como lo establece el Artículo 511, inciso seis del COIP.

El informe pericial debe ser presentado y cargado al Sistema Informático Pericial en formato PDF; para que pueda ser descargado, conocido, estudiado por las y los interesados. Sus explicaciones o aclaraciones se presentarán de forma verbal y/o escrita, de conformidad con la normativa procesal correspondiente. Como lo establece el Artículo 19 y 20 de la Resolución 040- 2014.(Consejo de la Judicatura, 2014)

4. Fase de Análisis:

En esta fase se realiza la identificación, estudio y la interpretación de la información obtenida en la etapa de adquisición con el objetivo de encontrar algún elemento que

pueda constituirse como evidencia. El investigador en esta etapa debe realizar un examen detallado de la información proporcionada por el sistema de archivos, buscando archivos sospechosos para analizarlos detenidamente. En el proceso de búsqueda el perito informático debe realizar búsqueda de caracteres, establecer líneas de tiempo, entre otros. Además, el profesional debe en esta etapa poder contestarse las interrogantes de quién, cómo, cuándo y dónde sucedieron los hechos.(Lázaro, 2013)

5. Fase de Presentación:

Con esta fase se culmina el análisis forense propuesto en la norma UNE: 71505-3:2013, y como resultado se obtendrá el informe final pericial con los resultados de todas las fases antes descritas.

El perito informático debe preparar la presentación de sus resultados para que las partes pertinentes en el proceso legal y hacerlos valer frente un tribunal. Finalmente, el perito debe documentar todos sus hallazgos en un informe pericial que deberá ser redactado con lenguaje comprensible para el público no técnico explicando las razones por las cuales se ha llegado a tal conclusión.

1.3.7 Seguridad Informática ISO 27000

Una de las normas reconocidas internacionalmente es la ISO/IEC 27037, que presenta una guía de referencia para la identificación, recolección, adquisición y preservación de la evidencia digital, teniendo en cuenta que no entra en el proceso de análisis de la evidencia.(Loarte, 2018)

Según Loarte (2018), “otro punto a favor de esta norma es que es de alcance global proveniente de la normativa de Seguridad Informática ISO 27000, definiendo los dispositivos y las funcionalidades usados en la misma por ejemplo (dispositivos de almacenamiento masivo, Smartphone, GPS, ordenadores conectadas en red, sistemas de video vigilancia, etc.)”

1.3.8 Herramientas de Análisis Forense

1.3.8.1 AccessData FTK Imager

FTK es una herramienta de análisis forense que permite al perito informático realizar una imagen de un dispositivo de almacenamiento digital. Entonces, el programa lleva a cabo una exploración sistemática de la imagen creada para organizar los elementos almacenados en el dispositivo. El objetivo de esto es clasificar la información para facilitar la búsqueda mediante cadenas de caracteres y de esta forma el perito tendrá facilidad de encontrar información determinante para su informe, por ejemplo archivos generados por correos.(Lázaro, 2013)

Una de las desventajas de FTK es la utilización de muchos recursos del sistema en el momento de crear particiones del dispositivo de almacenamiento en el proceso de creación de la imagen forense. Por ejemplo, en esta investigación se creó la imagen

forense de un dispositivo de almacenamiento de una capacidad de 4 GB y el tiempo estimado de creación de la imagen fue de 15 minutos.

Una de las principales funciones claves que permiten dar veracidad del procedimiento forense del perito es que este software permite la extracción de los hashes MD5 o SHA de todos los archivos que permitirán la validación de evidencia. También se presentan dentro de las particiones los espacios no asignados como File Slack, ayudando al perito a despreciar información que no debe ser motivo de análisis por no ser determinante para generar su reporte.

1.3.8.2 DatCon

DatCon es un software de decodificación especializado en la transformación de archivos DAT generados por los drones al realizar vuelos y los convierte en formato CSV.

DatCon es una aplicación que lee un archivo DAT y luego crea archivos de salida que contienen datos extraídos de DAT en un formato CSV que se visualizan en un libro de Excel entre otros programas, este software funciona para la marca DJI en sus series Phantom 3 (Professional, Advanced y Standard), este programa está disponible gratuitamente en la web y se instala simplemente con un ejecutable.

1.3.9 Dron

Los vehículos aéreos no tripulados son conocidos, también como drones, estos dispositivos han logrado alcanzar una gran popularidad en el mercado en pocos años tomar gran popularidad. Estos vehículos están caracterizados por poseer varios rotores, por lo que adquieren la capacidad de realizar despegues y aterrizajes de manera vertical. Las características de los VANT que los posiciona en el mercado, son las capacidades superiores de maniobrabilidad y estabilidad que poseen frente a los aviones y helicópteros.(Pérez, Benítez y Díaz, 2017)

Los vehículos aéreos no tripulados de ala rotatoria, tienen la característica de tener una fuerza de sustentación mediante el giro de las hélices en el aire. (Díaz, 2015)

Díaz (2015) menciona en su trabajo de grado que los VANT de ala rotatoria presenta las siguientes características:

1. “Despegue y aterrizaje vertical, reduciendo las necesidades de espacio para las maniobras de aterrizaje y despegue.
2. Posibilidad de volar a puntos fijos.
3. Vuelo estacionario, muy útil para aplicaciones de video-vigilancia.
4. Mayor maniobrabilidad y precisión de vuelo, ya que los sistemas de ala fija siguen trayectorias curvilíneas, con radios de giro relativamente grandes y velocidades de ascenso y descenso bastantes estrictas, sin embargo, los multirrotores pueden volar siguiendo cualquier trayectoria en las tres dimensiones.
5. El diseño de los multirrotores permite embarcar cargas de pago más voluminosas.”(Díaz, 2015)

Una de las características relevantes de los vehículos aéreos no tripulados es la función de control remota.(Pardo, 2016). La conexión se realiza mediante un enlace creado entre la estación de control y el dron. En el momento que se enciende el dispositivo de control y el dron se crea una señal Wifi en la que el usuario puede enlazarse mediante una contraseña.

Estos avances tecnológicos han facilitado el acceso público a esta tecnología en los últimos años. Gracias al desarrollo de la ingeniería geoespacial se ha logrado el ingreso de tecnologías emergentes al mercado con un numeroso campo de aplicaciones en distintas ramas de las ciencias experimentales como la física, geología, entre otros.(Thomson, Fountain y Watts, 2007)

1.3.10 Dron DJI PHANMTON III STANDARD

El dron DJI PHAMTON tiene características y componentes que se detallan en la tabla 1, teniendo en cuenta que se escogieron las más importantes para el desarrollo de la investigación:

COMPONENTE	CARACTERÍSTICAS
Velocidad de ascenso máx.	5 m/s
Velocidad de descenso máx.	3 m/s
Velocidad máx.	16 m/s (modo A, sin viento)
Sistema GPS	GPS incorporado
Modos de grabación de vídeo	2,7 K: 2704x1520p30 FHD: 1920x1080p 24/25/30 HD: 1280x720p 24/25/30/48/50/60
Formatos de archivo admitidos	FAT32/exFAT Fotografía: JPEG, DNG Vídeo: MP4/MOV (MPEG-4 AVC/H.264)
Tipos de tarjetas SD admitidas	MicroSD, Capacidad máxima: 64 GB Clase 6 o superior
WIFI: Frecuencia de funcionamiento	De 2400 GHz a 2483 GHz
Distancia máxima de transmisión	FCC: 1000 M ; CE: 500 m (al aire libre y sin obstáculos, altitud de la aeronave a 120 m/400 pies)
CONTROL REMOTO: Frecuencia de funcionamiento	5,725 GHz - 5,825 GHz, 922,7 MHz - 927,7 MHz
Batería de vuelo inteligente	(PH3 - 4480 mAh - 15,2 V)
Tipo de batería	LiPo 4S

Tabla 1. **Características del DJI PHANTOM III STANDARD**.
Fuente: DJI PHANTOM 3 STANDARD Manual de usuario V1. 0 [3]

[3] https://dl.djicdn.com/downloads/phantom_3_standard/es/ES-Phantom%203%20Standard%20User%20Manual(1).pdf

1.3.11 Sistemas de Archivos

Según González (2013), “un sistema de archivos es la estructura subyacente que un equipo usa para organizar los datos de un sistema de almacenamiento, por ejemplo, si se está instalando un disco duro nuevo, se tiene que realizar las particiones y formatearlo empleando un sistema de archivos para comenzar a almacenar datos o programas. Para los sistemas operativos contemporáneos se distinguen tres sistemas de archivos los cuales son NTFS, el FAT32 y la más obsoleta que ya es poco usada FAT que se la conoce también como sistema de archivos FAT16.”

A continuación, se explicará cada uno de los sistemas de archivos anteriormente mencionados con la finalidad de poder distinguir las características principales de cada uno de ellos y entender el porqué de la implementación de FAT32 en la memoria interna del dron estudiado en esta investigación.

1.3.11.1 Sistema de archivos NFTS

Este sistema de archivos tiene muchos beneficios respecto al FAT32, de los que se ponen a consideración los siguientes:

1. La capacidad de recuperarse a partir de algunos errores relacionados con el dispositivo de almacenamiento, lo que FAT32 no puede hacer.
2. Compatibilidad mejorada para discos duros más grandes.
3. Mejor seguridad porque puede utilizar permisos y cifrado para restringir el acceso a archivos específicos para usuarios aprobados. (González, 2013)

El sistema de archivos NTFS lo desarrolló Microsoft para los primeros sistemas operativos NT, además, este sistema de archivos dispone características avanzadas de seguridad como: encriptación, permisos, registro de transacciones, entre otros.

1.3.11.2 Sistema de archivos FAT (FAT16)

Este sistema de archivos es el más obsoleto y ya no es usado por sistemas electrónicos actuales, si se retrocede un poco en la historia y echamos un vistazo a sistemas de almacenamiento digital antiguos era común encontrarlo en sistemas operativos de Windows tales como: Windows 95, Windows 98 y Windows Millennium Edition.

1.3.11.3 Sistema de archivos FAT32

FAT es el primer sistema de archivos de uso generalizado, la historia menciona que se empezó a utilizar en los primeros ordenadores de escritorio.

> FAT localiza los archivos a través de entradas de directorio que hacen referencia tanto a directorios como a archivos. Estas entradas incluyen el nombre del archivo o del directorio junto con extensiones adicionales para nombres de 8 caracteres más 3 caracteres correspondientes a la extensión.(Lázaro, 2013)

El sistema de archivos FAT32 no tiene la seguridad que NTFS proporciona, entonces cualquier usuario que tenga acceso a estos archivos podrán leerlo independientemente si éste se encuentra encriptado o no. Lázaro (2013) en su artículo de análisis forense de una plataforma Windows, afirman que no se puede crear una partición FAT32 mayor de 32 GB en la versión de sistema operativo que analiza y no se puede almacenar un archivo mayor que 4 GB en una partición FAT32.

1.3.12 Sistema de Archivos del DRON DJI PHANTOM III STANDARD

Realizando las investigaciones pertinentes de la funcionalidad y de la estructura del dron del caso de estudio de la investigación se determina que el sistema de archivos que utiliza el DJI Phantom III Estándar es el FAT32 el mismo que es compatible con todos los Sistemas Operativos, además, es utilizado para dispositivos de almacenamiento extraíbles. Al inicio de la investigación se habló de la existencia de una memoria interna que según las características del dron es de 4 Gb la misma que alberga archivos DAT y File Slack correspondientes a información producida por el dron proporcionando datos de los vuelos que realizó el dispositivo.

1.3.13 Archivos DAT

Un archivo DAT tiene la característica de almacenar información específica que se asocia con determinado programa con el cual se creó el archivo, además, por lo general se encuentran asociados con archivos de configuración DLL. Por lo general las aplicaciones utilizan este tipo de archivos como referencia de ciertas operaciones en sus programas.(ReviverSoft, 2014)

Otra de las grandes utilidades de este formato de archivos es que se utilizan para poder almacenar datos de cualquier índole, por ejemplo, gráficos o texto, se puede decir que los archivos de extensión DAT no tiene una estructura clara y precisa de un editor para relacionarlo con la aplicación correcta. (ReviverSoft, 2014)

Los archivos DAT tienen el carácter de universal y pueden contener datos con formato de texto o binario, teniendo la particularidad de distinguirse por la aplicación que creó el archivo.

1.3.14 File Slack

Este tipo de archivos tienen la principal característica el tamaño con el que es creado y que depende exclusivamente de lo que contengan y por el sistema que lo origina, por ejemplo: sistemas basados en DOS, Windows 95/98/ME/XP y Windows NT/2000 almacenan los archivos en bloques de tamaño fijo llamados clusters. Además, es importante mencionar que se entiende por File Slack, el espacio de almacenamiento de datos existentes desde el final del archivo hasta el final del cluster, de la misma manera estos cluster van variando de longitud según los sistemas operativos involucrados en la creación de los mismos.(López, Amaya y León, 2001)

CAPITULO II

ESTADO DEL ARTE

La informática forense está adquiriendo un gran impacto dentro de la información digital, esto se ha dado debido al aumento de información, que se dispone en nuevos espacios informáticos para cualquier persona. Según un estudio realizado en la Universidad de los Andes de Bogotá por López, Amaya y León (2001) mencionan que en el momento que se ha realiza un delito informático la información queda almacenada de forma digital. Sin embargo, no se pueden manipular los sistemas informáticos directamente por lo tanto se debe realizar técnicas forenses para la extracción, preservación, análisis y redacción de reportes.

La mayor parte de drones, está formado por su respectivo cargamento, como pueden ser cámaras para capturar imágenes y filmar videos, convirtiéndose en potenciales herramientas para realizar vigilancia con consentimiento o no del objetivo.

La mayoría de este tipo de vehículos presentan dos enlaces de datos para cada lado de la comunicación, uno para el control y envío de comandos y otro para la recepción de la información de vuelo. Sin embargo, también es posible encontrar enlaces de comunicación para elementos externos como sería la comunicación satelital mediante GPS o la comunicación con un mando radio control.

Al igual que los drones existen otros tipos de vehículos no tripulados en los cuales se han realizado investigaciones para determinar su estructura interna y que permiten saber la factibilidad de la realización de un análisis forense para obtener datos digitales almacenados en su sistema.

Actualmente existen trabajos relacionados y ponencias sobre análisis forense tanto en dispositivos no tripulados y de vehículos aéreos no tripulados. A continuación, se citan los más relevantes acordes al proyecto de investigación.

2.1 Sistemas Robóticos Teleoperados

Al hablar de vehículos no tripulados aéreos tenemos de diferentes clases, una de ellas son los vehículos con sistemas robóticos teleoperados, que se relaciona directamente con la investigación al poseer la característica de no ser tripulado. Según Ceron (2005) en su investigación “Sistemas Robóticos Teleoperados”. Los robots teleoperados son aquellos controlados por un usuario a distancia desde una estación remota, los drones poseen una estación remota móvil gracias a su mando o control, aunque tienen su limitante al radio de alcance de transmisión en relación con los robots teleoperados que abarcan mayores distancias. Otro aspecto importante en esta investigación habla sobre la incorporación de sistemas de procesamiento de imágenes o video que al igual que los drones puede estar montado en el vehículo o procesarse en una estación remota.

Los datos se almacenan en una memoria interna dedicada para esto, que según la programación en la fabricación de estos vehículos puede ser extraíble o montado dentro

de la placa madre. La investigación menciona un sistema dedicado para albergar datos generados por el sistema GPS en el dispositivo, con el fin de que quede registrado en el vehículo las coordenadas que le permitan su retorno a su lugar de origen gracias a la interacción del mando remoto con él usuario.

2.2 Análisis Forense Dron DJI PHAMTON II

Maarse, Sangers, Van-Ginkel y Pouw (2016) desarrollan otra propuesta para realizar el análisis forense de Drones, en su artículo Denominado “Análisis Forense Digital en UAV DJI Phantom Vision +2” en el cuan proponen una serie de pasos que ellos llevaron a cabo para realizar dicho procedimiento forense. La investigación se llevó a cabo en un UAV versión DJI Phantom 2 Vision Plus 2.0 en su configuración por defecto. Ellos mencionan en su estudio todo el procedimiento que llevan a cabo desde la ejecución de la aplicación el cual lo nombran como software asistente, que conjuntamente con el sistema remoto, controlan el correcto funcionamiento del UAV.

Los datos proporcionados en este artículo tienen un gran realce para el desarrollo de esta investigación al relacionarse con la estructura y funcionamiento del dron DJI Phantom III en su versión Estándar. En la fase de adquisición de los datos digitales en esta investigación se habla de creación de un ingreso fantasma como lo mencionan en la investigación, mediante líneas de comandos para extraer datos en la transición del UAV al mando remoto.

2.3 Análisis Forense Dron DJI PHAMTON III ESTÁNDAR

En la actualidad no se encuentra definida una metodología establecida y estandarizada para realizar el análisis de drones. Pero Clarck, Meffert, Baggili y Breitinger (2017), pertenecientes al grupo de investigación de la Cibernética Forense de la Universidad de New Haven en Boston, mencionan en su investigación denominada “Forensic analysis of the DJI Phantom III”, en el cual suponen la existencia de un delito con estos UAV y realizar el análisis forense del dron DJI Phantom III.

Los autores con esta investigación proporcionan características importantes de la estructura interna del Dron DJI Phantom III dejando al descubierto la existencia de una memoria interna tipo SD (Storage Digital). Además, menciona la existencia de dos tipos de datos que se pueden alojar en esta memoria (datos con extensiones “dat” y “txt”) proporcionados por el sistema GPS y datos informativos al realizar la creación de la imagen forense, que le permiten al dron realizar la acción de aterrizaje en su punto de origen o despegue como lo mencionan en el artículo. Finalmente, los investigadores realizaron varias pruebas para validar la herramienta construida y sus hallazgos. También se realizaron pruebas con respecto a la tarjeta SD interna en el dron (Prueba de sección y hallazgos). (Clarck et al., 2017)

2.4 Metodologías de Análisis Forense

Gervilla (2014) menciona en su trabajo “Metodología para un análisis forense” da a conocer una visión global sobre la metodología de análisis forense para que la evidencia pueda ser validada correctamente con dispositivos en este campo.

Basantes y Sanchez (2016) en su “Análisis forense a sistemas operativos mediante la utilización de herramientas Open Source, caso estudio Windows 8”, da un enfoque de la utilización de herramientas de fuente abierta para el análisis de la información obtenida del artefacto electrónico.

Azas (2015) en su tema de tesis “DISEÑO DE UN MODELO PARA LA CADENA DE CUSTODIA Y HERRAMIENTAS PARA EL ANÁLISIS FORENSE DE EQUIPOS TECNOLÓGICOS EN PROCESOS JUDICIALES EN EL ECUADOR”, menciona los aspectos más importantes que se deben tener en cuenta para la cadena de custodia en equipos tecnológicos, que entran en investigaciones por ser pruebas en casos judiciales.

CAPITULO III

DISEÑO DEL MARCO METODOLÓGICO PARA ANÁLISIS FORENSE DE UN DRON DJI PHANTOM III STANDARD

Realizar el diseño de un marco metodológico consiste en realizar una guía que indique una secuencia de pasos con fundamento lógico y estructurado dentro de una referencia de análisis forense que permita primeramente extraer la información cuidando su integridad para finalmente analizar los archivos digitales almacenados en este dispositivo.

El diseño del marco metodológico se centra en la extracción de información que se encuentra alojada en la memoria interna del dron, al extraer la información de este dispositivo de almacenamiento se conseguirá datos de los vuelos que ha realizado el dron, encontrando información importante como es el geoposicionamiento del dron al momento de realizar el despegue.

La funcionalidad de esta memoria interna no volátil consiste en albergar datos del GPS para ser aplicados en una de las funciones implementadas en de dron de la línea DJI Phantom (Retorno a la ubicación de partida). Se puede ver en la figura 2 la pantalla de control del dron, en el cual se resalta la opción de retorno al punto de despegue. El manual de funcionamiento dispuesto por el fabricante en sus plataformas de la marca, esta opción presenta un margen de error del 10 % que aproximadamente son 5 metros a la redonda distanciado del punto de despegue.

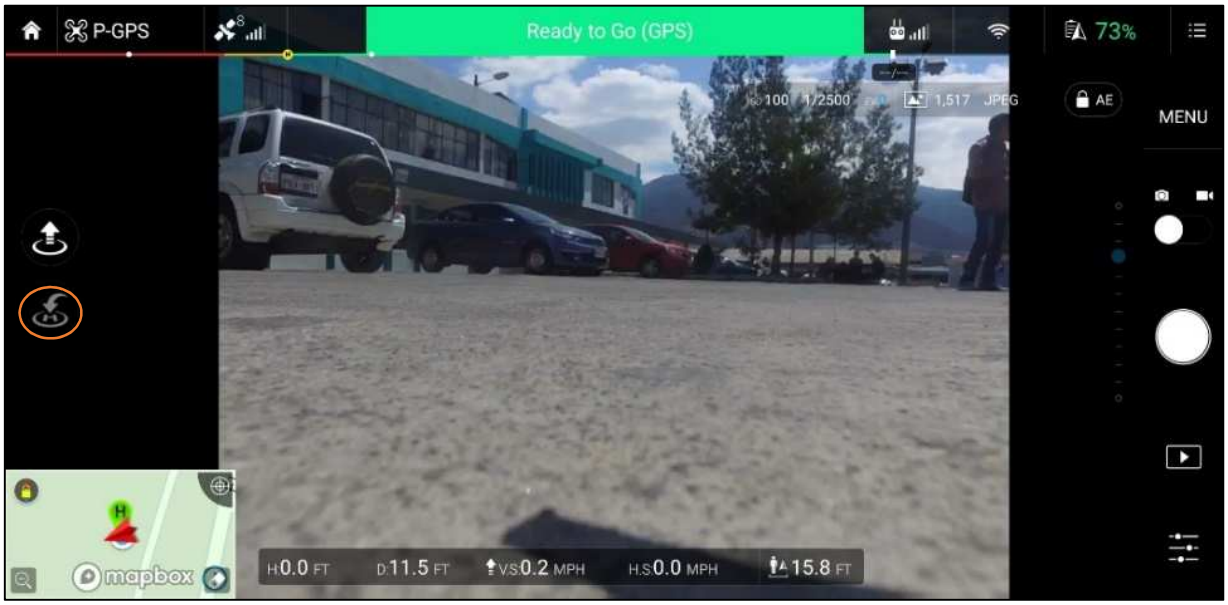

Figura 2. **Aplicación DJI GO, opción de retorno al punto de despegue.**
Fuente: autor

La figura 3 presenta un diagrama de flujo, explicando el procedimiento que se realizó para la elaboración del marco metodológico de análisis forense del dron desde su

captura en el momento de ser sorprendido realizando el acto ilícito de espionaje hasta la extracción de los archivos almacenados en la memoria, obteniendo una imagen forense al realizar procedimientos establecidos en normas internacionales.

Según las investigaciones realizadas el tipo de memoria que se encuentra alojada en este dispositivo es una memoria Micro SD el cual se comunica con el dron por medio del sistema de archivos FAT32, es importante resaltar que esta memoria interna no es indispensable para el funcionamiento del dron, ya que se realizó pruebas de vuelo sin la incorporación de esta memoria y el dispositivo pudo realizar el despegue y operó normalmente excepto que se inhabilita una de sus características principales que es el regreso y aterrizaje en su punto de despegue, generando un error en la aplicación instalada en el dispositivo que controla al dron, al darse el caso mencionado se deben buscar alternativas de análisis forense diferentes a la planteada en esta investigación.

Al extraer la memoria interna del dron se saca una imagen forense de la Micro SD HC 1 con las herramientas forenses adecuadas e indicadas posteriormente en la metodología de análisis forense, para finalmente extraer los archivos DAT que contienen información comprometedora de los vuelos realizados del dron.

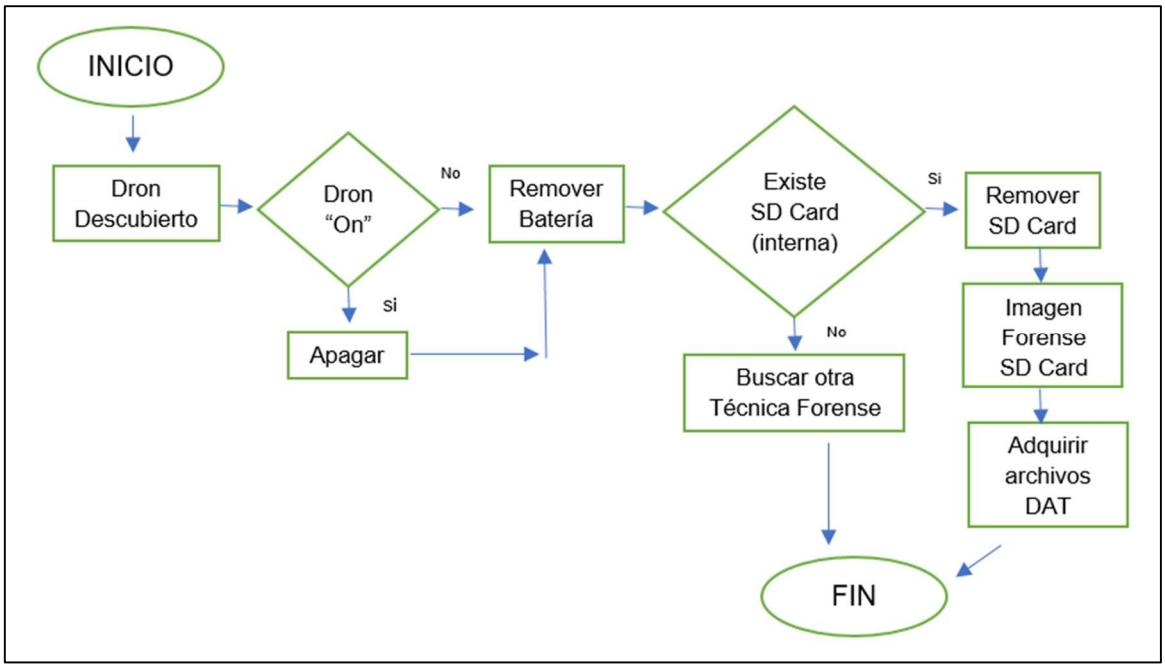

Figura 3. **Procedimiento para realizar el análisis forense del Dron.**
Fuente: autor.

Para la creación del caso de espionaje se toma como referencia la norma UNE 71505-3:2013 y la norma española RFC 3227, de las cuales se plantea seguir el siguiente procedimiento para la creación del caso de investigación. La metodología de análisis forense que se presenta ahora es una visión general, que posteriormente se desarrollará detenidamente paso a paso:

1. Restablecimiento de Fábrica: con esto se garantiza que ninguna variable externa pueda generar cambios en los resultados del caso de estudio.

2. Creación de Escenario: se establece un lugar específico del cual se puede obtener datos de geoposicionamiento otorgados por dispositivos de GPS, además, se realiza un vuelo con el dron simulando un caso de espionaje luego de obtener los permisos correspondientes.
3. Adquisición de Datos: según el diagrama de flujo de la figura 3 se deben considerar los dos diferentes de estados en los cuales se puede capturar el dron (encendido o apagado), luego realizar los procedimientos establecidos en la RFC 3227 para extracción integra de la información.
4. Análisis de Datos: los archivos DAT obtenidos del dispositivo de almacenamiento se encuentran encriptados, para lo cual se utiliza software (DatCon) para decodificar y obtener información comprometedora del vuelo realizado por el dron.

3.1 Caso de espionaje utilizando un dron DJI Phantom III Standard

En este apartado se va a detallar los pasos que se realizan para el caso de espionaje hasta la extracción de la información, finalmente se presentará una guía que permita a los peritos obtener información del dron sin perder la integridad de la misma y a la vez con esto poder presentar un correcto informe forense.

3.1.1 Creación de Escenario

Para la creación del escenario en primer lugar, se creó una cuenta en la aplicación DJI GO, que se encuentra disponible por parte del fabricante en la Play Store la misma que se instala en el dispositivo para controlar el dron.

Luego se seleccionó el Taller de Electrónica del Instituto Tecnológico Superior Central Técnico de la ciudad de Quito. El objetivo del caso de espionaje se encuentra en el segundo piso sobre el Área de Electrónica de la institución antes mencionada y que se encuentra ubicado en las calles Isaac Albeniz y el Morlán, teniendo las siguientes coordenadas de geoposicionamiento: 0°09’07.6’’S, 78°28’42.0’’W; latitud = -0.152110, longitud = -78.478326

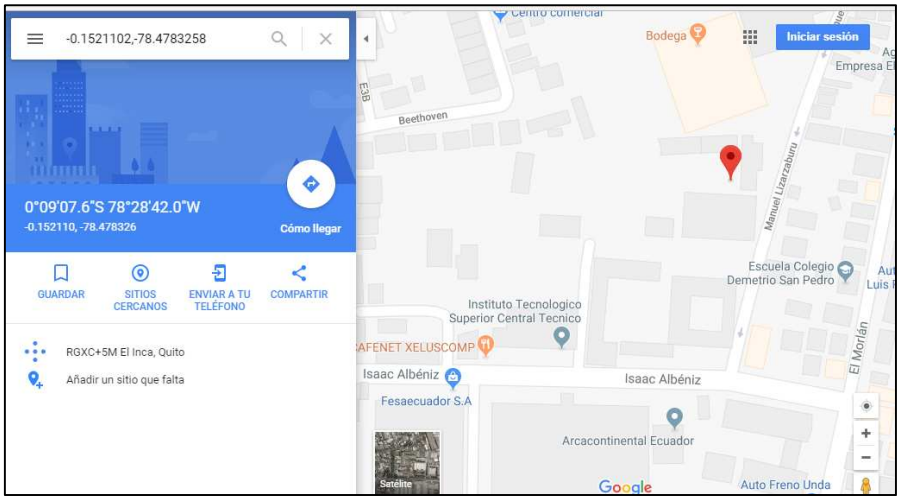

Figura 4. **Coordenadas geográficas del Taller de Electrónica del Instituto Tecnológico Superior Central Técnico.**
Tomado de Google Maps, 2018

Como se había mencionado anteriormente el dron lo vamos a restaurar de fábrica para no contaminar la evidencia y analizar específicamente en los archivos generados en el vuelo del caso de estudio. Para realizar esta acción se debe encender el dispositivo y mantener presionado un pulsador alojado en un costado del armazón del dron por un lapso de 30 segundos, la ubicación de este pulsador la puede observar en la figura 5.

Figura 5. **Punto para restauración de fábrica del Dron.**
Fuente: autor.

El dron fue encendido en el patio frontal al Taller de Electrónica de la Unidad Educativa antes mencionada para luego realizar el despegue para cumplir con el espionaje del objetivo. En la figura 6 y figura 7, se puede observar el momento en el que se pone en marcha el dron y las imágenes captadas del interior del Taller que se obtuvo al sobrevolar el dron por la ventana del objetivo respectivamente.

Figura 6. **Puesta en marcha del dron, simulación del caso de espionaje.**
Fuente: autor.

Figura 7. **Dron realizando espionaje del Taller de Electrónica, Imágenes capturadas por la cámara del dron.**
Fuente: autor.

Luego de crear el escenario del caso de espionaje se toma como referencia la norma UNE 71505-3:2013, que establece cinco fases para un correcto análisis forense, por lo cual esta investigación se regirá en cada una de estas fases que se detallarán a continuación:

3.1.2 Fase de Preservación

Una vez descubierto el dispositivo realizando el acto ilícito (espionaje al Taller de Electrónica ubicado en un edificio de la entidad educativa antes expuesto en las coordenadas establecidas en la creación del escenario), el dron es capturado y se toma un conjunto de procedimientos para cuidar la integridad de la información, para lo cual se realiza una cadena de custodia. Para iniciar, se verifica el estado de dron al analizar si está en estado encendido o apagado al momento de forzar su aterrizaje.

Figura 8. **Captura y aterrizaje forzoso del Dron.**
Fuente: autor.

Cuando encontremos el VANT en estado encendido se debe apagarlo y luego retirar la batería para conservar los últimos datos de coordenadas del GPS que proporcionan la ubicación de despegue, con el objetivo de establecer la dirección de la cual se empezó a manipular este caso de espionaje.

Figura 9. **Estados en los que se encuentra el Dron en el momento de la captura.**
Fuente: autor.

De la misma manera cuando se verifica el estado del dron y si lo encontramos en estado apagado, se desmonta la batería del dispositivo para evitar posibles errores de inicio del sistema involuntariamente y perder los datos de coordenadas de despegue del dron.

Figura 10. **Desmontaje de la batería del dron luego de ser capturado.**
Fuente: autor.

Finalmente, en esta fase para conservar la integridad de la información del dron cuando lo capturamos y para cumplir con una correcta cadena de custodia, colocamos tanto el dron como la batería que se desalojó del mismo en fundas anti estática y con la respectiva etiquetación de las mismas.

3.1.3 Fase de Adquisición

Una vez que se completó el vuelo de prueba del caso de estudio de espionaje se debe realizar el levantamiento de los datos.

En esta fase de adquisición se detallan los métodos que se realizan para desmontar la estructura del dron y obtener la placa mainboard. Una vez que se desaloja la mainboard de la estructura del dron, se extrae la memoria micro SD que se encuentra alojada en un sócalo ubicado en la parte posterior de la misma.

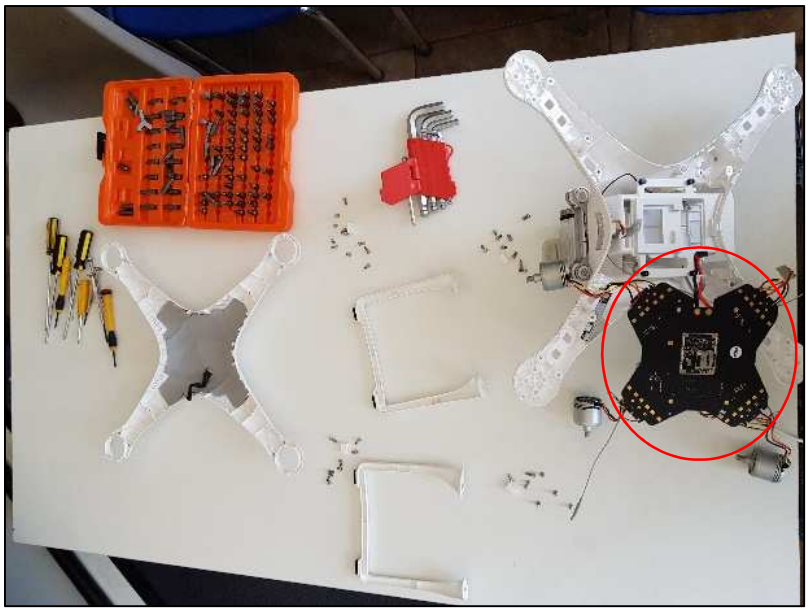

Figura 11. **Mainboard del dron DJI, vista posterior.**
Fuente: autor.

En capítulos anteriores se habían estudiado las características del Dron DJI Phantom III Standard, en las cuales se resaltó la existencia de dos memorias de almacenamiento del dispositivo, una interna para información comprometedora de los vuelos, de la cual sacaremos el análisis forense, pero también tiene una memoria externa de 8 GB para guardar las imágenes capturadas durante el vuelo por el dron, suponiendo que una persona que utiliza un dron para realizar un acto ilícito tratará de no dejar evidencia de sus acciones, por lo cual quitará la memoria externa que va alojada en el sócalo ubicado en la parte superior de la cámara.

Para la recopilación de la evidencia y almacenamiento de la información obtenida del dron, se utiliza la norma RFC 3227, la misma que se aplica en este caso de la siguiente forma:

4. Luego de desmontar la estructura del dron y extraer la memoria interna se debe crear una imagen forense (clonado de la micro SD a bajo nivel) con la herramienta adecuada y que cuide la integridad de la información, la norma recomienda que se haga en lugares adecuados para una buena práctica forense, por lo cual se determinó que se realizará este procedimiento en un lugar aislado de elementos que generen interferencias con la extracción de la información o

que alteren la estructura de la misma, además, es indispensable que tenga las herramientas adecuadas y necesarias.

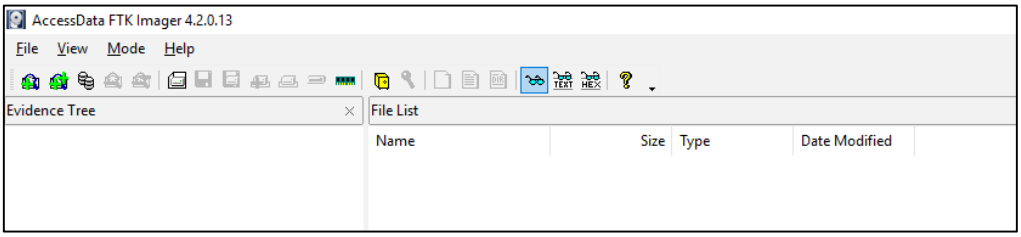

Figura 12. **Pantalla principal del programa AccessData FTK Imager versión 4.2.0.13.**
Fuente: autor.

La extracción de la evidencia digital se la va a detallar paso a paso en la elaboración de una guía que indique el proceso adecuado para obtener la información del dispositivo. Previamente se explica que para la obtención de la imagen forense del dispositivo de memoria interna del dron se utiliza el programa de análisis forense con denominación AccessData FTK Imager versión 4.2.0.13. Con esta herramienta se realizará un clonado a bajo nivel de la memoria micro SD.

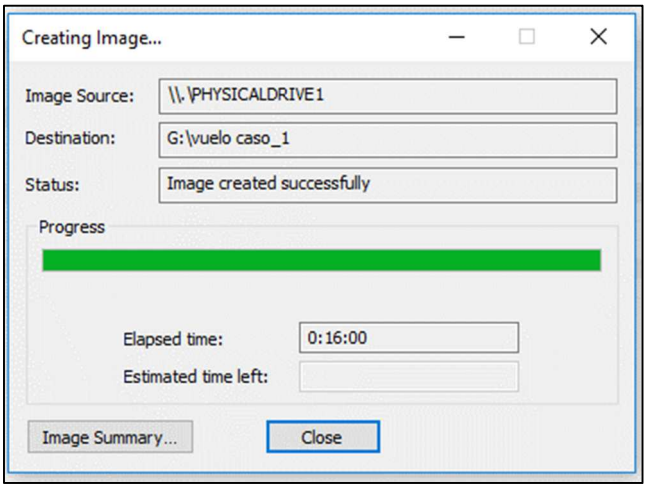

Figura 13. **Creación de la imagen forense de la memoria interna del dron.**
Fuente: autor.

Al extraer la imagen forense del dispositivo se genera el Hash MD5, la misma que podemos observar en la figura 14.

Figura 14. **Código Hash MD5.**
Fuente: autor.

Figura 15. **Dispositivos de almacenamiento nuevos de fábrica.**
Fuente: autor.

Para realizar el procedimiento de clonado es necesario adquirir elementos de almacenamiento con las siguientes características:

5. Dispositivo lector de tarjetas micro SD, que sea totalmente nuevo de fábrica, con esto se garantiza la integridad de la información. Para esta investigación se adquirió un dispositivo Card Reader USB 2.0, con una velocidad de lectura de 480 Mbps, el dispositivo mencionado se lo puede observar en la figura 16.
6. Además, se adquirió una memoria USB con una capacidad de almacenamiento mayor que la capacidad de la memoria externa extraída del dron. Las características de esta memoria son: capacidad de 8 GB de la marca Kingston DataTraveler G4, de la misma manera este dispositivo de almacenamiento es nuevo de fábrica.

Figura 16. **Card Reader USB 2.0.**
Fuente: autor.

El clonado a bajo nivel se lo va a realizar con el software AccessData FTK Imager versión 4.2.0.13 instalado en el ordenador de la marca DELL con las siguientes características: procesador Intel Core i3, con sistema operativo Windows 10 Pro de 64 bits, 4 Gb de memoria RAM.

Se inserta la memoria Micro SD extraída del dron en el Card Reader USB 2.0 y ésta la introducimos en uno de los puertos USB del ordenador de las características antes mencionada, de la misma manera ubicamos en el otro puerto del ordenador la memoria USB Kingston nueva, para que sea guardada la imagen forense que se crea de la memoria Micro SD que se introdujo con su lector en el otro puerto.

Este procedimiento se lo puede observar en la figura 17.

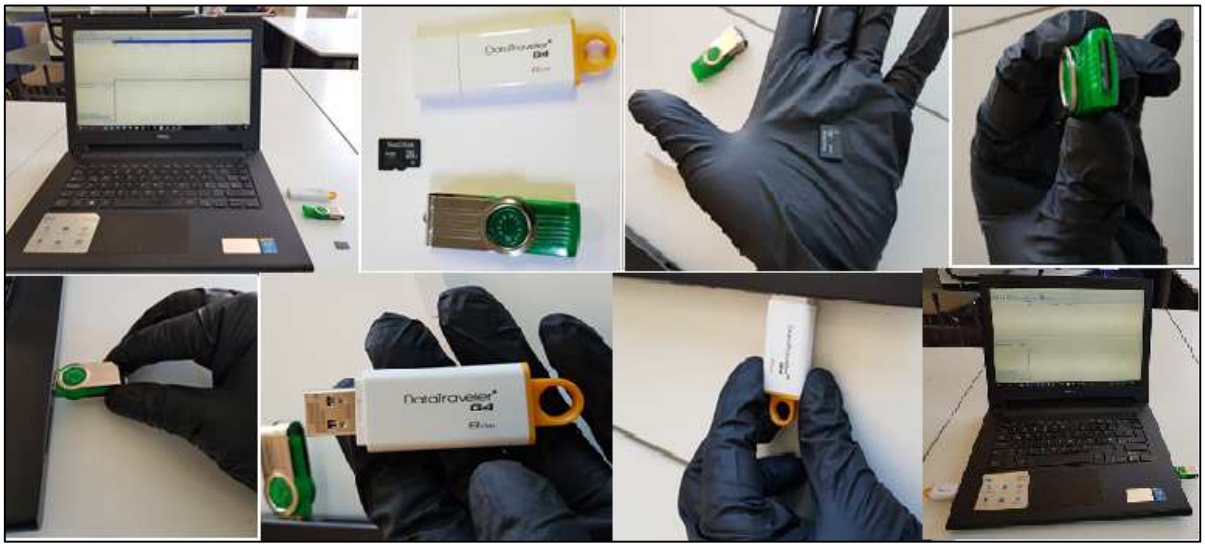

Figura 17. **Ubicación de los dispositivos de almacenamiento para la clonación a bajo nivel de la memoria interna.**
Fuente: autor.

Luego de haber sido creada la imagen forense como se observa en la figura 13 y revisar el código hash MD5, podemos ingresar al dispositivo de almacenamiento que contiene la imagen forense de la memoria Micro SD y vamos a encontrar cuatro archivos con las características que se pueden observar en la figura 18, esto se deba a que el programa hace particiones para el almacenamiento en la creación de la imagen forense.

El nombre de la imagen forense fue designado por el autor de esta investigación “vuelo caso_1” y las particiones en el almacenamiento toman los nombres, vuelo caso_1.001, vuelo caso_1.001. txt, vuelo caso_1.002 y vuelo caso_1.003, que son nombradas por el mismo programa.

El análisis del contenido de cada uno de los archivos se los va a realizar en la fase de análisis, ya que necesitan un software que permitan desencriptar los datos para ser analizador por el perito que vaya a realizar el informe.

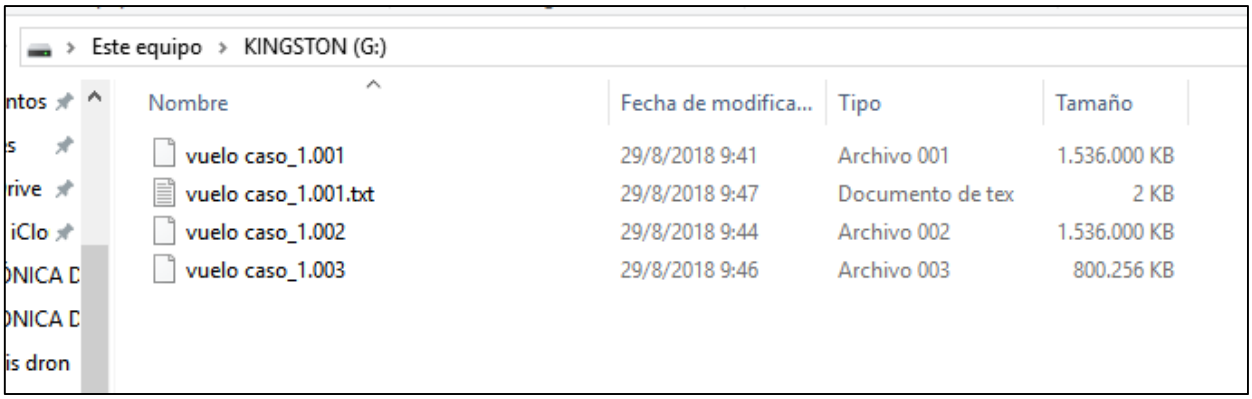

Figura 18. **Imagen forense almacenada en la memoria USB Kingston.**
Fuente: autor.

3.1.4 Fase de Documentación

En esta fase el especialista que lleve a cabo el análisis forense debe recopilar toda la información que se obtuvo en la fase de adquisición, realizando capturas fotográficas, grabaciones de audio o video, que vayan describiendo todos los hallazgos que se hacen al momento de analizar la información.

3.1.5 Fase de Análisis

En la fase de análisis vamos a llevar a cabo un examen minucioso de cada uno de los archivos con el fin de encontrar información relevante del caso de estudio.

El programa FTK Imager tiene la herramienta para cargar la imagen forense que se generó. Esto permite examinar los archivos almacenados en la imagen forense. En la figura 19 podemos observar el momento que se carga la imagen forense denominada vuelo caso_1.001 en el programa FTK Imager.

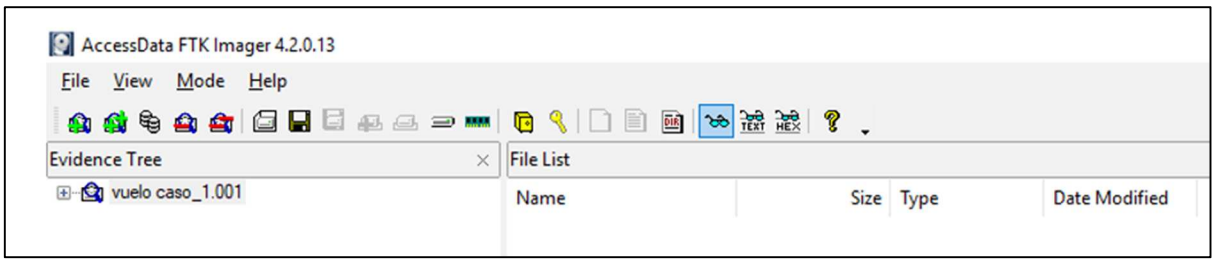

Figura 19. **Open File de la imagen forense del vuelo caso_1.001.**
Fuente: autor.

Una vez cargadas las tres particiones que se crearon en la imagen forense, se empieza a analizar la información que estos proporcionan. Es importante mencionar que dentro de la imagen forense existe un archivo con un formato diferente a los otros tres. Este archivo tiene una extensión TXT, que al analizarlo podemos encontrar información importante de la creación de la imagen forense tal como un sumario de datos del analizador de la evidencia, el código Hash MD5, el número de segmentos en el que se dividió la imagen, etc. Estos datos podemos revisar en la figura 20.

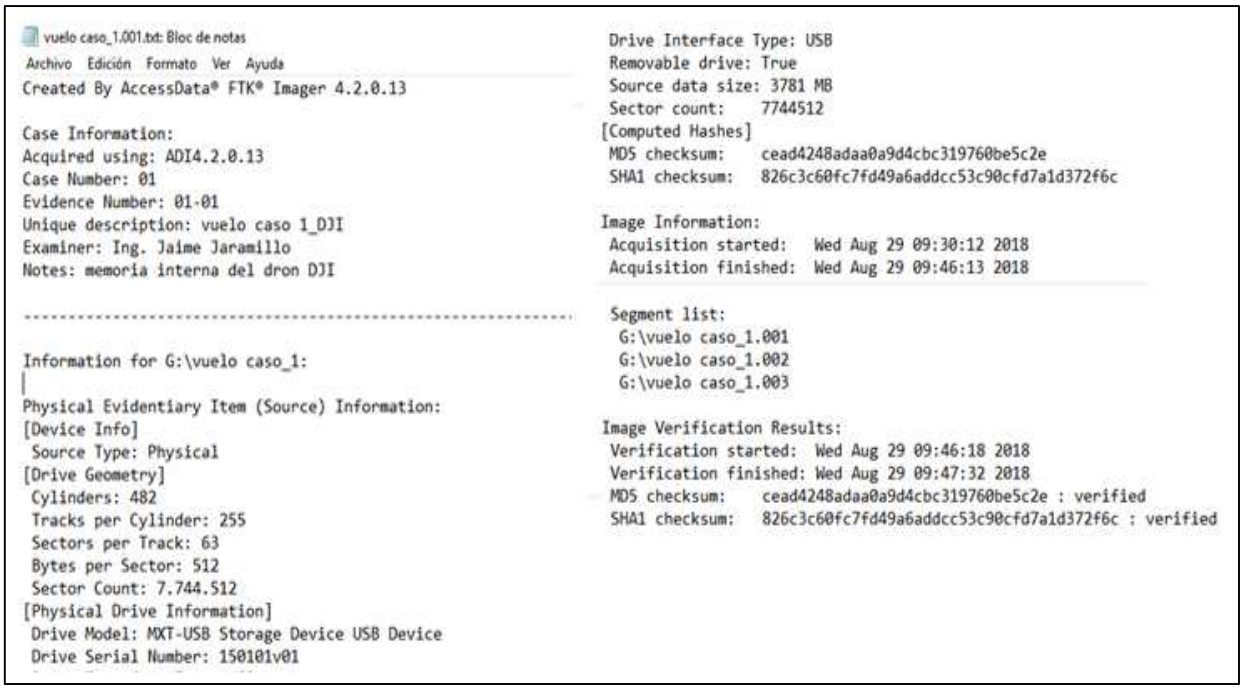

Figura 20. **Archivo TXT generado al realizar el clonado a bajo nivel.**
Fuente: autor.

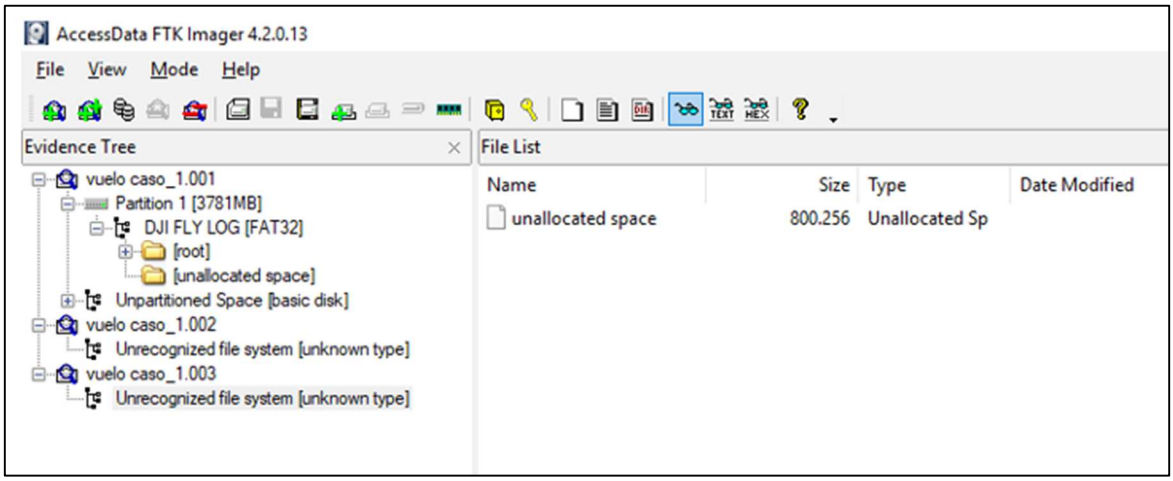

Figura 21. **Open File de las 3 particiones de la imagen forense.**
Fuente: autor.

Como se puede observar en la figura 21 en las particiones de los casos: vuelo caso_1.002 y vuelo caso_1.003, aparece una extensión denominada “Unrecognized file system” y al ingresar a estos no encontraremos información relevante para el estudio del caso que podemos observar en la figura 22 y figura 23.

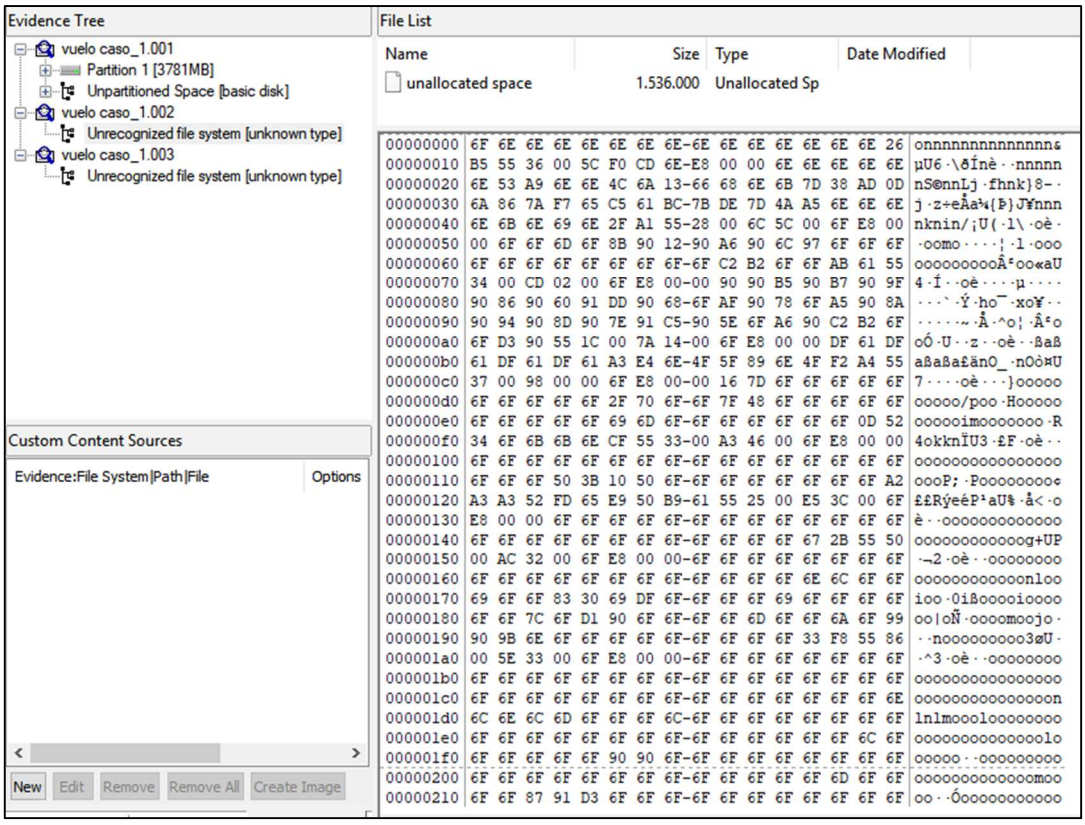

Figura 22. **Análisis del archivo de la partición vuelo caso_1.002.**
Fuente: autor.

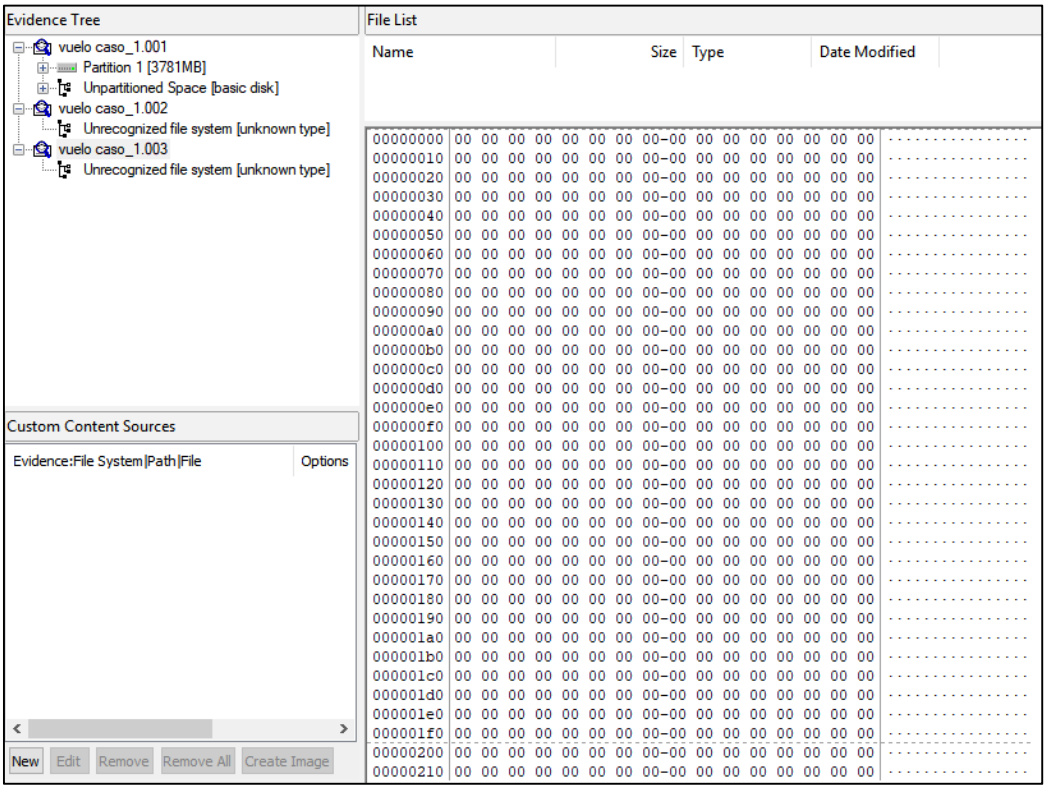

Figura 23. **Análisis del archivo de la partición vuelo caso_1.003.**
Fuente: autor.

Las particiones: vuelo caso_1.002 y vuelo caso_1.003, si bien no muestran mucha información al analizarla, se debe a que al crear el escenario se restauró de fábrica el dron, por lo cual los únicos datos que se generan son los que registraron el vuelo que simula el caso de estudio de espionaje, por lo tanto, las particiones mencionadas no albergan información.

Por otra parte, si analizamos la partición “vuelo caso_1.001”, se puede observar que la información que se aloja en este archivo es la del vuelo del caso de estudio como lo podemos ver en la figura 24. La primera partición abarca casi toda casi toda la capacidad de memoria de la que se sacó la imagen forense, la capacidad de esta partición de memoria es de 3781 MB.

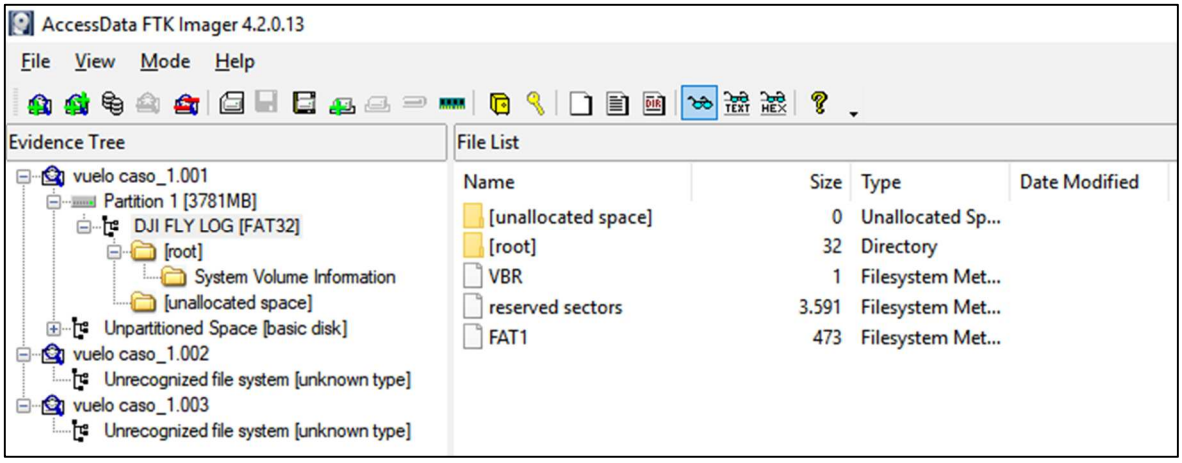

Figura 24. **Análisis del archivo de la partición vuelo caso_1.001.**
Fuente: autor.

Si entramos en la carpeta “root” se puede observar los archivos DAT que se generaron y que albergan la información del vuelo del caso de estudio. Como podemos ver en la figura 25, encontramos archivos DAT con la nomenclatura FLY01.DAT, donde la parte numérica se establece en un orden sucesivo, este tipo de archivo contiene una gran cantidad de datos de vuelo relacionados con la ubicación del dron, estados del vuelo y varias lecturas del sensor.

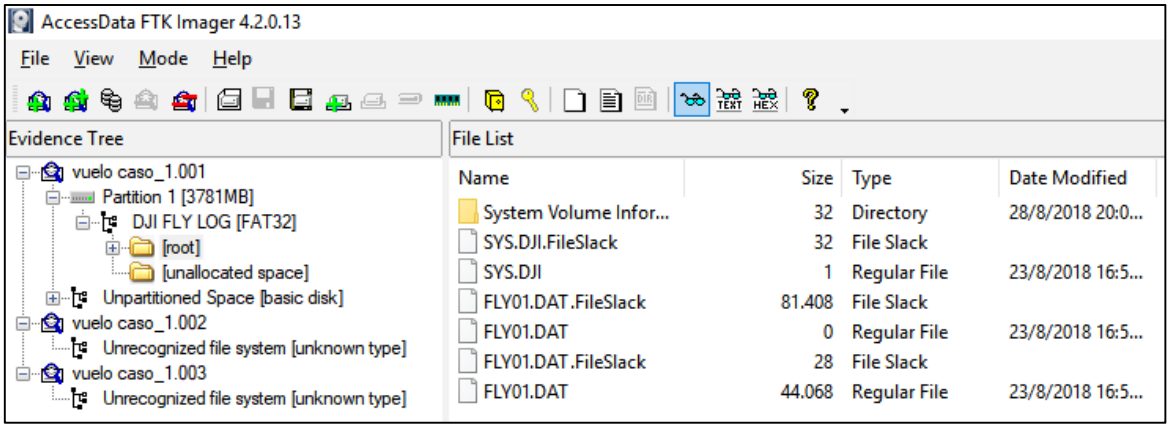

Figura 25. **Archivos de la carpeta root.**
Fuente: autor.

La fecha de modificación de los archivos como se puede apreciar es el 23 de agosto del 2018 a las 16:53 minutos, es importante reconocer estos datos ya que corroboran que los archivos fueron creados en base a la realización del vuelo del caso de espionaje ya que se realizó en esa fecha y hora en el patio de la Unidad Educativa. De la misma manera se observa una carpeta de denominación System Volume Information que agrupa cuatro archivos como se aprecia en la figura 25, y, que son datos que no aportan información relevante para la investigación al ser archivos de ajuste del programa para generar el clonado a bajo nivel de la memoria.

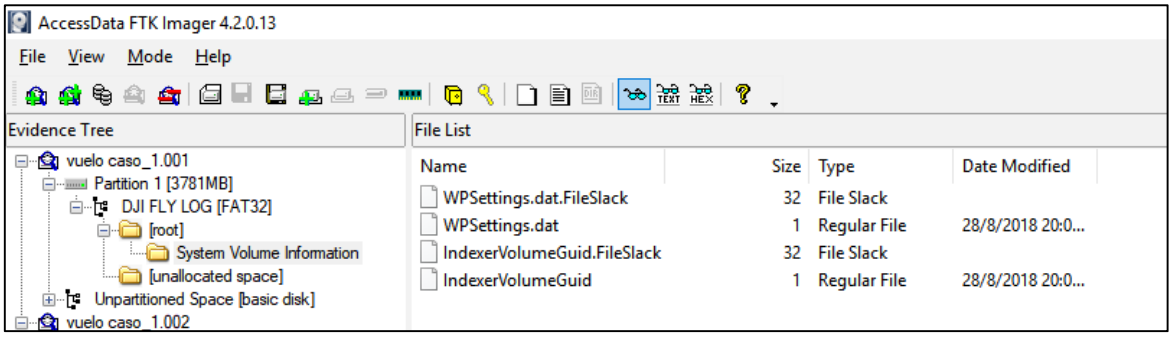

Figura 26. **Archivos de la carpeta System Volume Information.**
Fuente: autor.

Luego de haber analizado todos los archivos que contienen las particiones de la imagen forense, nos vamos a centrar en la partición en la siguiente dirección: vuelo caso_1.001/Parttion 1 [3781MB]/root/FLY01.DAT.FileSlack

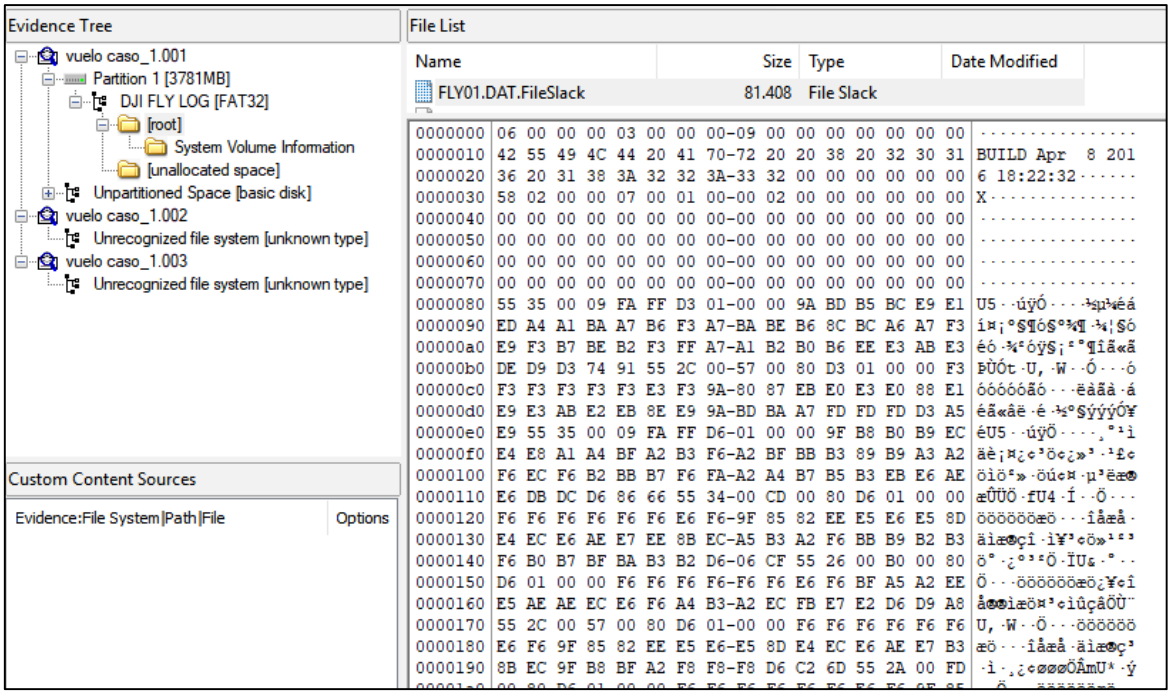

Figura 27. **Archivo generado del vuelo FLY01.DAT.**
Fuente: autor.

Como se había investigado anteriormente la información que se encuentra en este archivo DAT se encuentra codificada, por lo que se necesita decodificarla para poder

entenderla. Para lograr analizar la información de este archivo se hará uso de un software que permite leer los archivos DAT producidos por el dron y convertirlos a un formato CSV.

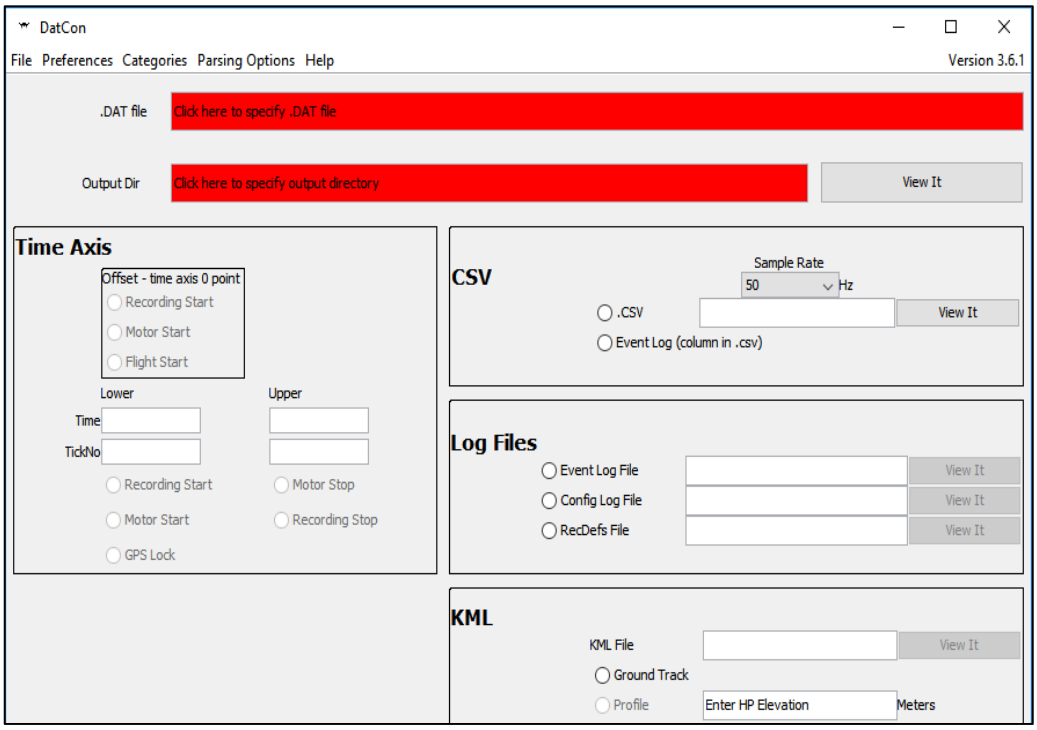

Figura 28. **Software DatCon.**
Fuente: autor.

DatCon es un software especializado en decodificar archivos DAT generados por el dron y transformarlos en CSV, éste se encuentra disponible en la red y podemos descargar el ejecutable (EXE) para cargar el archivo FLY01.DAT y generar su conversión a CSV.

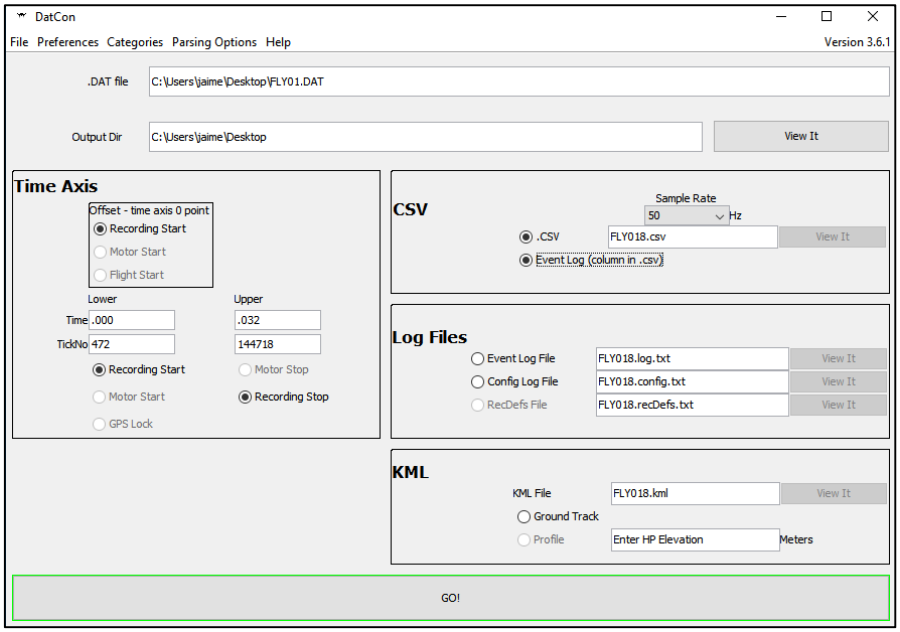

Figura 29. **Carga de archivo DAT al software DatCon.**
Fuente: autor.

Se debe mencionar que para poder cargar el archivo DAT al software de decodificación es necesario hacer la exportación del archivo desde el programa FTK Imager al escritorio del ordenador.

El archivo decodificado se encuentra en el formato CSV y se guardó en este caso en el escritorio del ordenador, el archivo generado conserva la misma nomenclatura del archivo importado del FTK Imager (FLY01.csv) cambiando solamente la extensión.

El archivo DAT después de ser decodificado y descifrado proporciona información comprometedora del vuelo del caso de estudio de espionaje, proporciona datos del dispositivo del GPS, IMU (Unidad de Medición Inercial), motores, control remoto, estado del vuelo, etc.

Como uno de los objetivos de esta investigación es encontrar la información generada por el módulo GPS dron, para obtener las coordenadas de geoposicionamiento del dron al realizar el despegue para el caso de espionaje, se ingresó al archivo decodificado FLY01.csv, y, se pudo encontrar la información requerida.

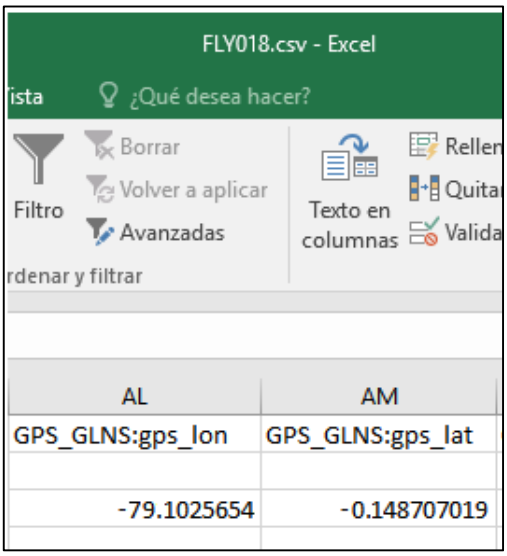

Figura 30. **Información del GPS del archivo FLY01.DAT decodificado.**
Fuente: autor.

Los datos del GPS entre otros, muestran tanto la latitud (-0.148707019) y longitud (-79.1025654). si comparamos esta información con la obtenida por un sistema de GPS: latitud (-0.152110), longitud (-78,478326), podemos deducir que las coordenadas tienen una proximidad de 90% por lo cual se puede establecer que se ha encontrados las coordenadas en las que el dron realizó el caso de espionaje.

3.1.6 Fase de Presentación

En la fase de presentación según el artículo 511 de COIP, el perito debe redactar un informe pericial donde explique todos los métodos y herramientas que utilizó para la extracción y análisis de la información, además, debe referirse a todos los hallazgos relevantes que se encontró al analizar los archivos del dron.

De la misma manera el especialista que lleve a cabo la investigación de un caso como el expuesto en esta investigación debe redactar un informe pericial que describa cada uno de los hallazgos, siguiendo los formatos disponibles en el Sistema Judicial, de tal manera que quede plasmado en el documento todos y cada uno de los procedimientos realizados, tal como lo describe el COIP.

El sistema pericial establece que el perito que lleva a cabo el caso de estudio, debe presentar el informe pericial en formato PDF y este debe estar disponible en las plataformas para ser descargado y leído por las partes participantes en el litigio legal.

3.2 Guía de análisis Forense para el Dron DJI PHANTOM III STANDARD

3.2.1 Captura del Dron

1. Forzar o esperar que el dron aterrice. Esperar que el dispositivo llegue al nivel bajo de su batería; recordemos que una de las características de este dispositivo DJI es su sistema inteligente, que obliga a aterrizar al dron en su punto de despegue si los niveles de batería llegan a su nivel mínimo (esta herramienta presenta un error del 10%).

Figura 31. **Captura y aterrizaje forzoso del Dron.**
Fuente: autor.

2. Una vez capturado el dron, se debe verificar el estado en el que se encuentra (encendido/apagado), si está encendido de debe apagarlo. Con esto se pretende que el dron no realice un nuevo despegue y los datos geoposicionamiento originales se pierdan.

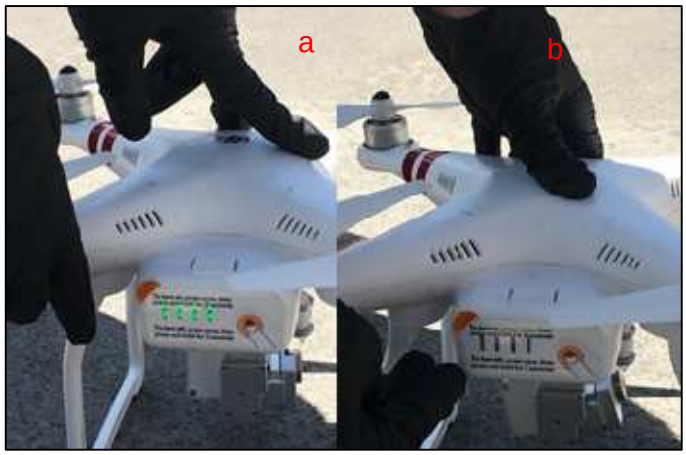

Figura 32. **Verificación del estado del dron: a) encendido, b) apagado.**
Fuente: autor.

3. Luego de apagar el dron se debe retirar la batería, para evitar un encendido no intencionado del dispositivo y perder los datos de las coordenadas de despegue originarias del caso de espionaje.

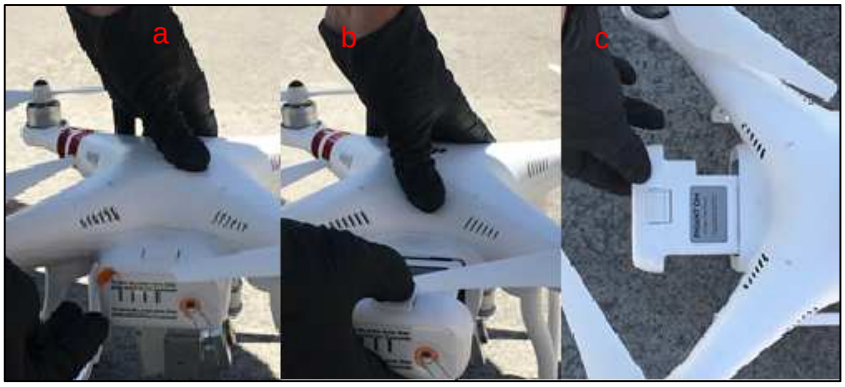

Figura 33. **Proceso de extracción de la batería del dron.**
Fuente: autor.

3.2.2 Extracción de la memoria Interna del Dron

4. Retiramos las 4 hélices de los rotores del dron.

Figura 34. **Extracción de las 4 hélices de los rotores.**
Fuente: autor.

5. Retiramos la protección para la antena del giroscopio que se encuentra en uno de los trenes de aterrizaje.

Figura 35. **Extracción de la antena del giroscopio, quitar los tornillos de la protección de esta antena.**
Fuente: autor.

6. Removemos las dos antenas wifi de los trenes de aterrizaje con sus respectivos seguros.

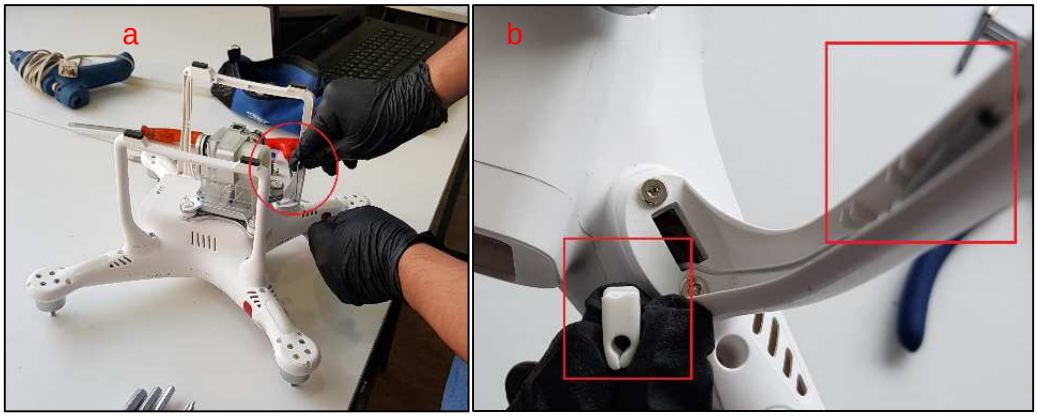

Figura 36. **Extracción de la antena wifi de los seguros del tren de aterrizaje.**
Fuente: autor.

7. A continuación, le quitamos los dos trenes de aterrizaje del dron que se encuentran sujetos a la estructura con dos tornillos cada uno.

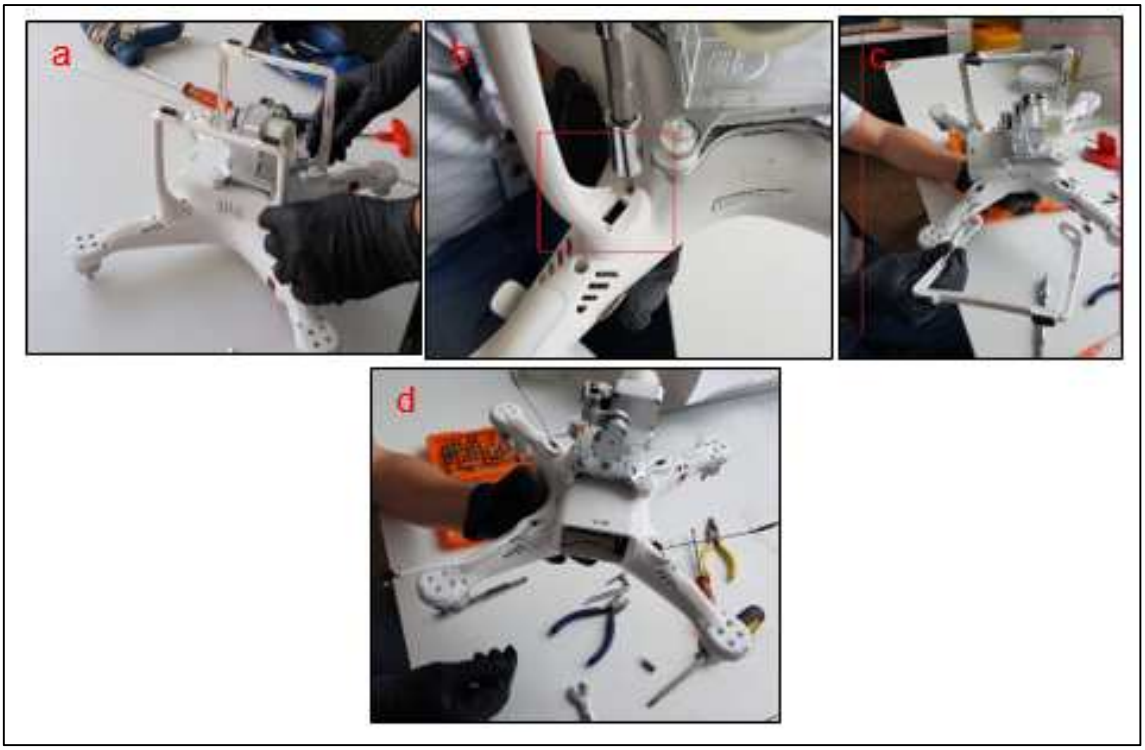

Figura 37. **Extracción de los trenes de aterrizaje del dron.**
Fuente: autor.

En la figura 38 d se puede observar las dos antenas WiFi y la antena del giroscopio antes mencionadas.

8. Remover los cuatro motores del dron, para poder desarticular cada uno de ellos se debe desatornillar 7 tornillos por cada motor.

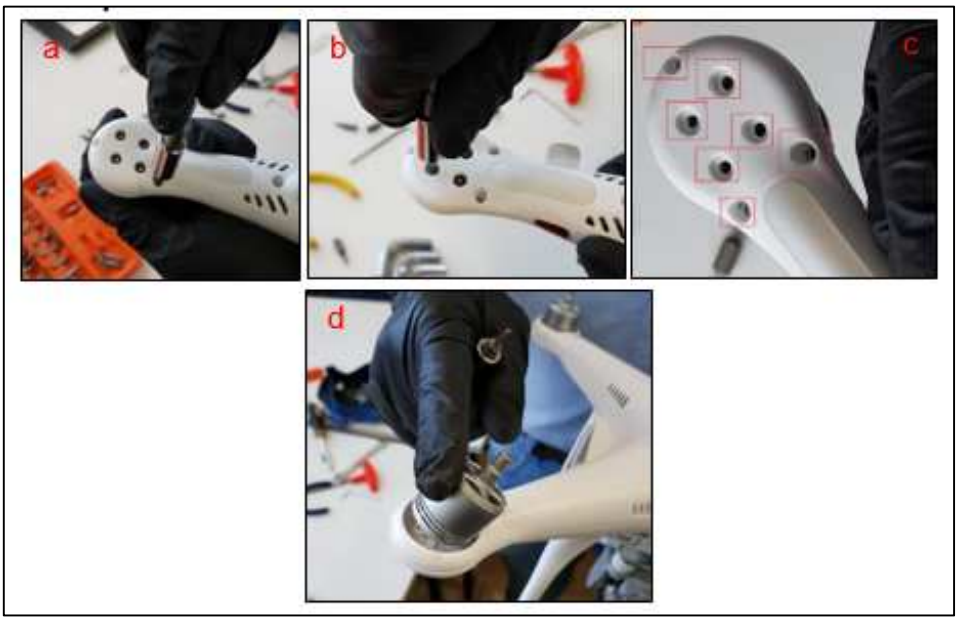

Figura 38. **Remoción de los motores del dron.**
Fuente: autor.

9. Luego sacamos los tornillos que sujetan la parte superior e inferior de la estructura y que permitirán separar las dos partes.

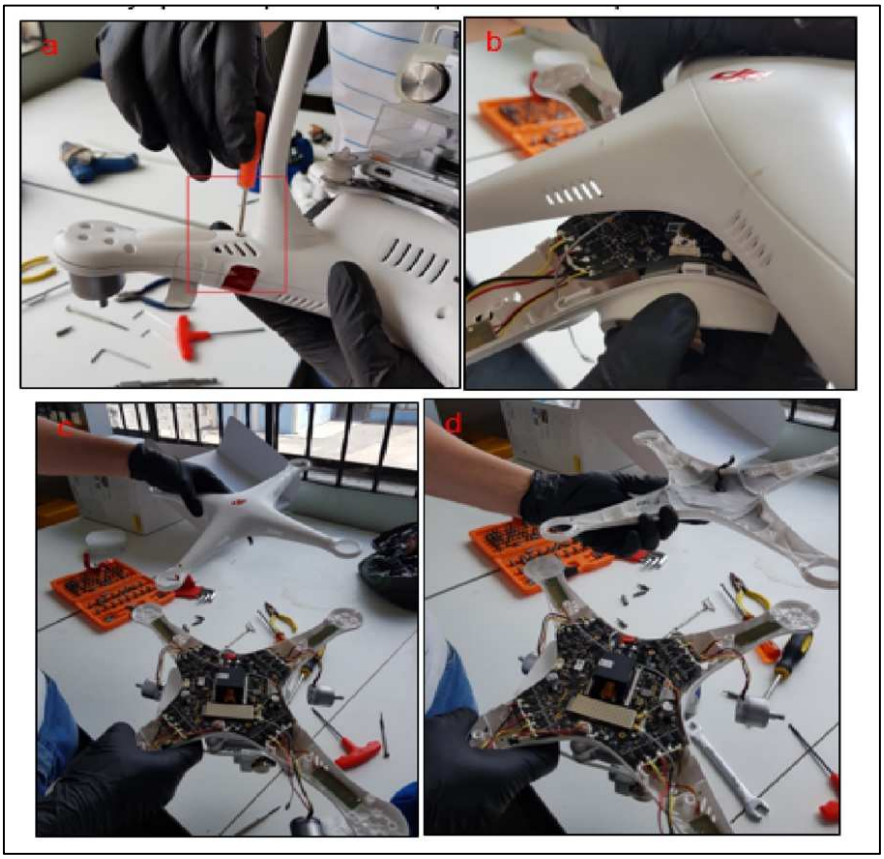

Figura 39. **Proceso de separación de la parte superior e inferior de la estructura.**
Fuente: autor.

10. Una vez que tenemos la placa mainboard expuesta, le quitamos los cuatro tornillos que la sujetan con la parte inferior de la estructura.

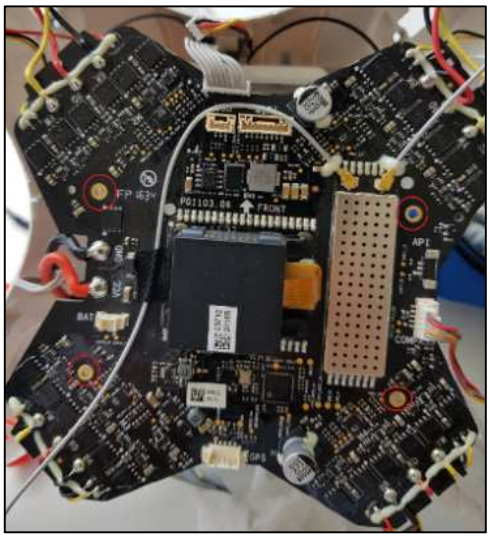

Figura 40. **Proceso para desalojar la placa mainboard.**
Fuente: autor.

11. Como se podrá apreciar hasta ese momento no se visualizará fácilmente la memoria Micro SD en la placa mainboard, luego de que quitemos los 4 tornillos en el paso anterior, se puede ver que, en la parte inferior de la placa se encuentra la memoria interna alojada en un sócalo, con una protección de silicón para evitar que el sócalo se abra fácilmente.

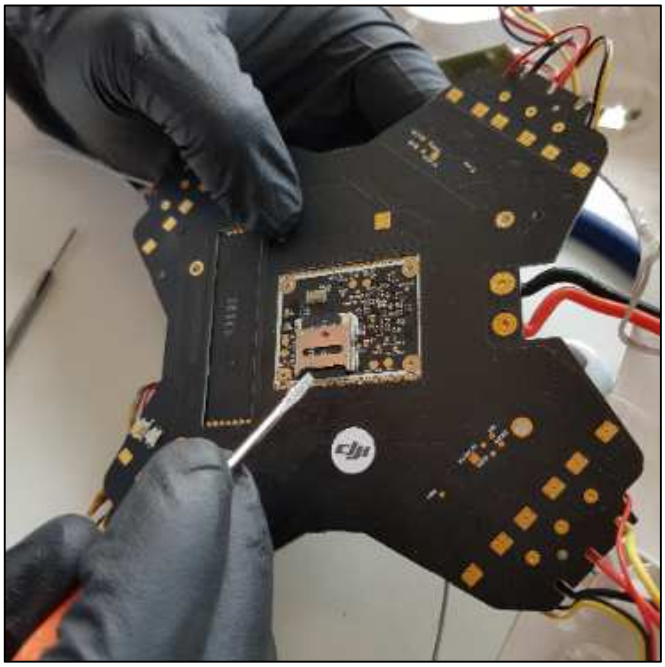

Figura 41. **Vista posterior de la mainboard, ubicación de la Micro SD.**
Fuente: autor

12. Una vez que se ha ubicado la memoria interna del dron, se debe realizar el siguiente procedimiento: a) retirar el silicón de protección del sócalo, b) levantar el seguro del sócalo y c) extraer la micro SD.

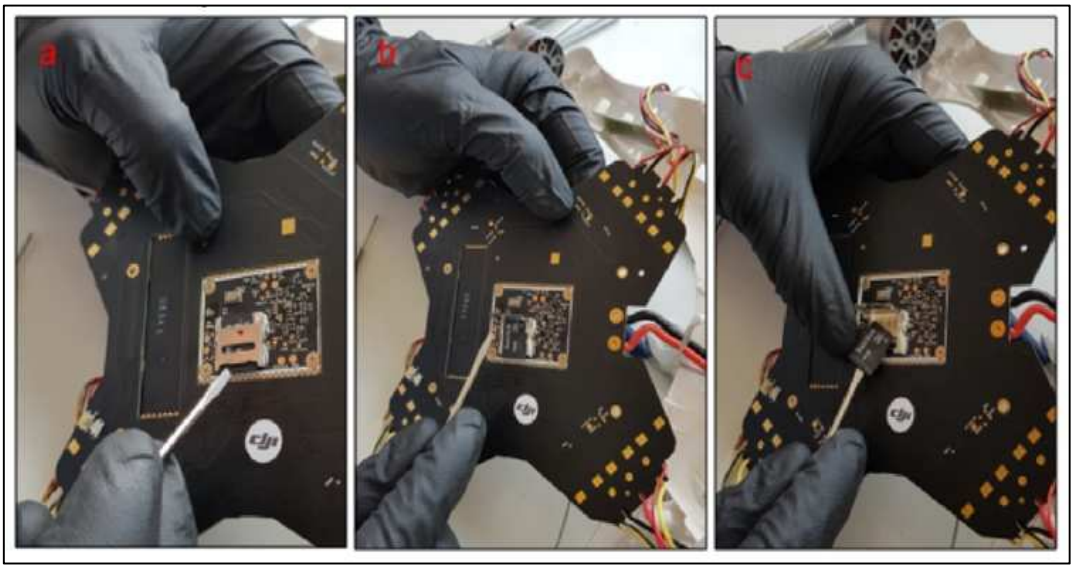

Figura 42. **Proceso de extracción de la memoria interna.**
Fuente: autor.

13. Finalmente obtenemos la memoria interna del dron para extraer la imagen forense y aplicar las técnicas forense pertinentes.

Figura 43. **Memoria interna del dron, memoria Micro SD.**
Fuente: autor.

3.2.3 Clonado a bajo nivel de la memoria Interna

14. Ubicamos la memoria micro SD en el Card Reader USB 2.0 de las características mencionada en la fase de adquisición.

Figura 44. **Acoplamiento de la Micro SD con Card Reader USB 2.0.**
Fuente: autor.

15. Una vez que colocamos la Micro SD en la Card Reader, la ubicamos en uno de los puertos del ordenador. De la misma manera en otro de los puertos USB colocamos la memoria de almacenamiento de características ya mencionadas en la fase de adquisición en don se alojará el clonado a bajo nivel de la memoria interna del dron.

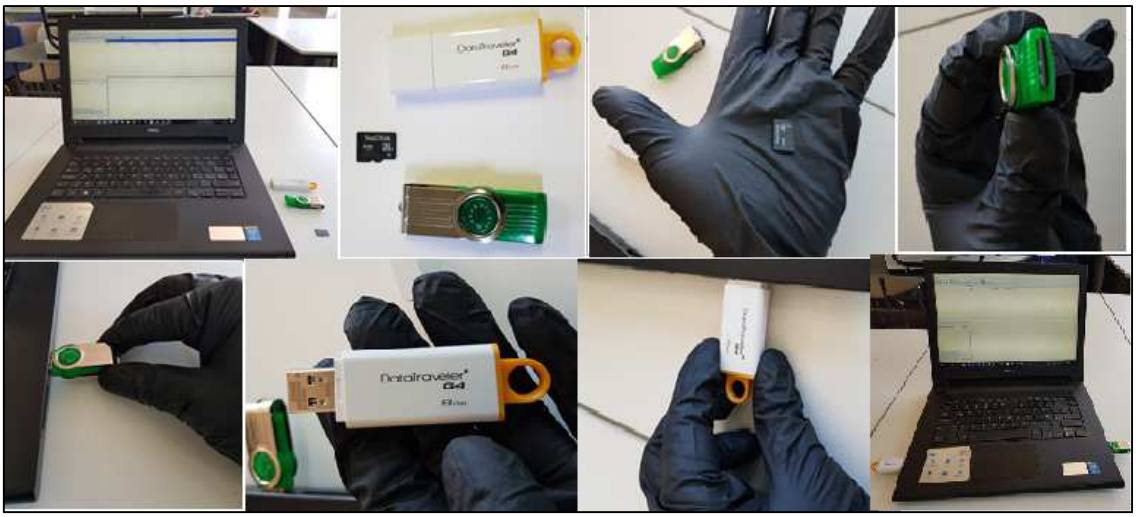

Figura 45. **Preparación de los dispositivos para la extracción de la imagen forense de la memoria interna del dron.**
Fuente: autor.

16. Abrimos el programa AccessData FTK Imager y ubicamos la opción Create Disk Image.

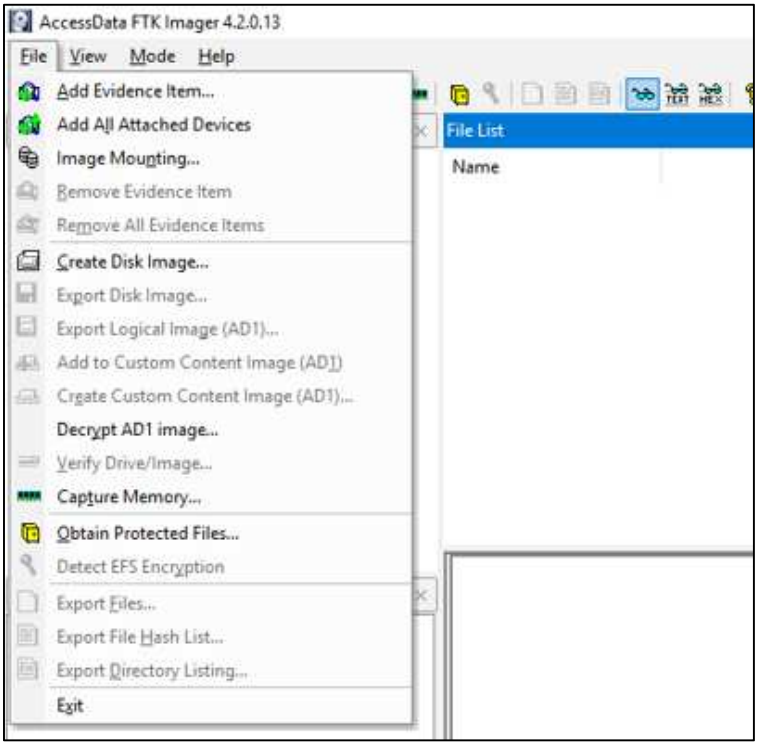

Figura 46. **Preparación de los dispositivos para la extracción de la imagen forense de la memoria interna del dron.**
Fuente: autor.

17. Luego de ingresar en la herramienta “Create Disk Image”, se debe seleccionar el tipo de fuente al que le vamos a sacar la imagen forense. Al ser una Micro SD la que alberga la información se debe seleccionar la opción “Physical Drive”.

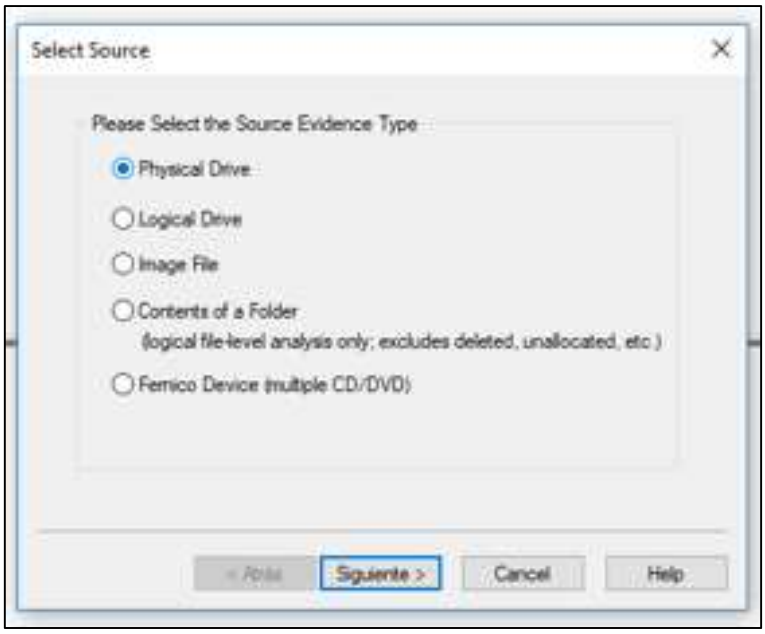

Figura 47. **Selección del tipo de fuente de la que se extraerá la imagen forense.**
Fuente: autor.

18. El programa FTK Imager no va a pedir que seleccionemos la ubicación del puerto en donde se encuentra la fuente de la cual se va a estraer la imagen forense, al desplegar las opciones, se selecciona el driver que realiza la conexión con la Micro SD Card, en el caso de esta investigación se selecciona el driver “PHYSICALDRIVE1 – MXT – USB Storage Device USB Device”.

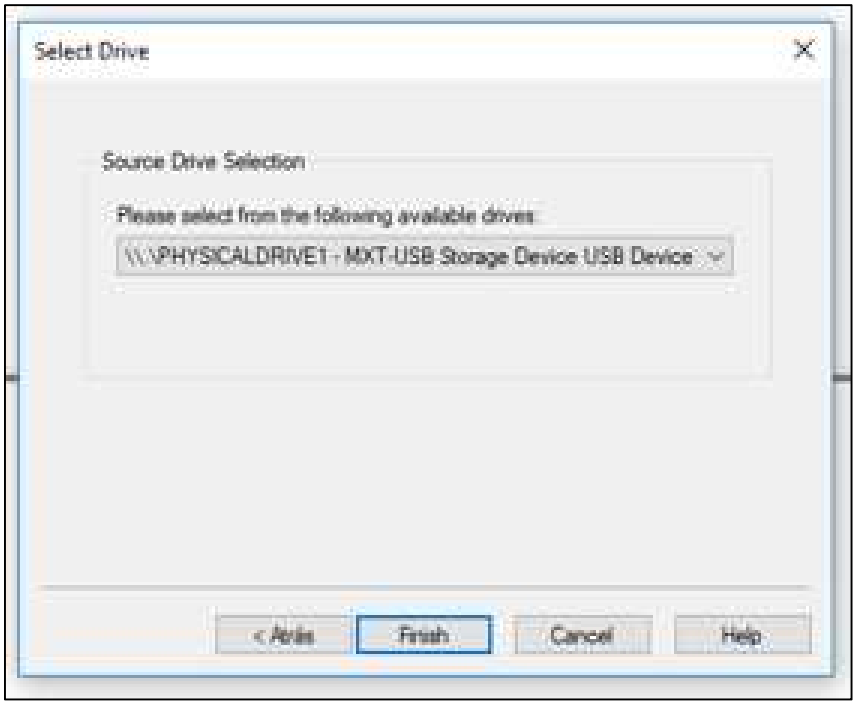

Figura 48. **Selección de la ubicación de la fuente.**
Fuente: autor.

19. Una vez seleccionada la ubicación de la Micro SD Card seleccionamos la opción “Add”.

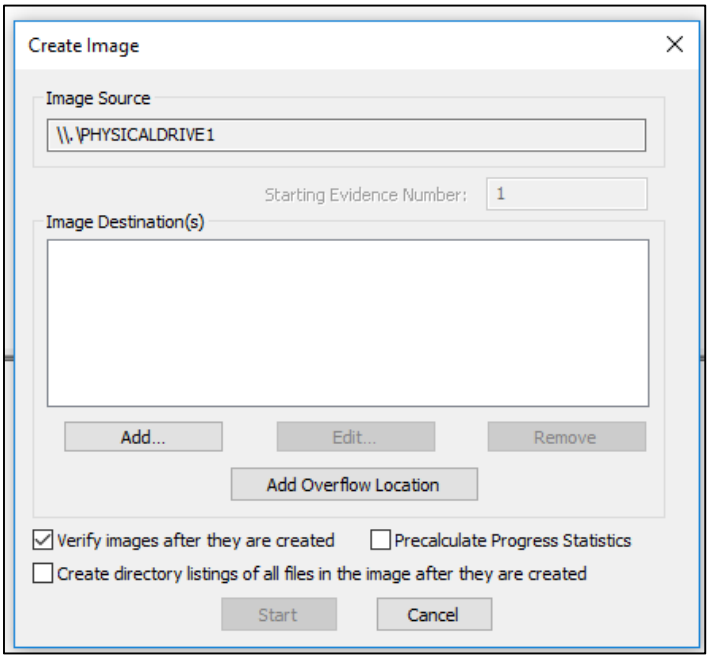

Figura 49. **Selección de configuraciones para la creación de la imagen forense.**
Fuente: autor.

20. Luego aparecen unas opciones de configuración para seleccionar el tipo de imagen que vamos a crear. Seleccionamos la opción “Raw (dd)” y luego hacemos clic en siguiente.

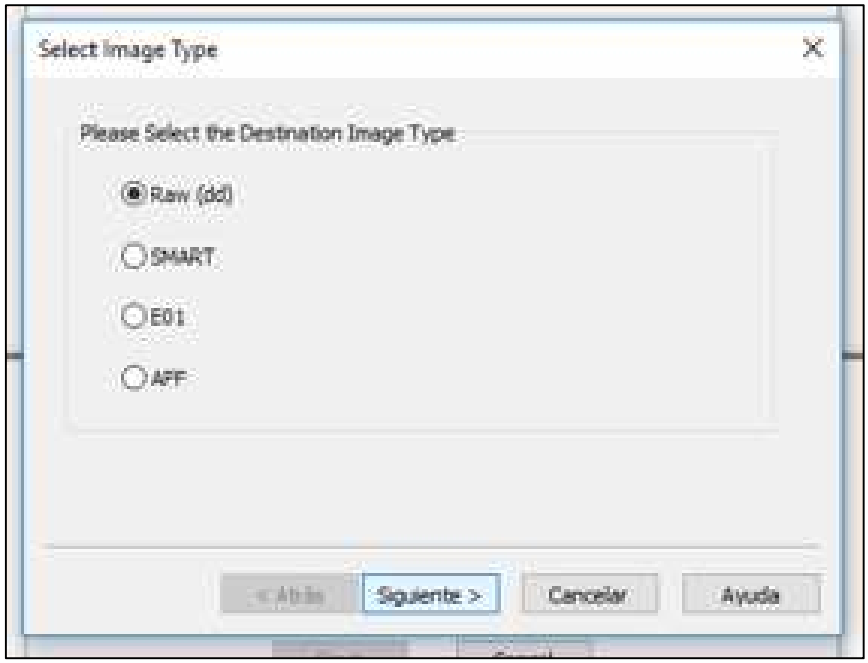

Figura 50. **Configuración para el Select Image Type.**
Fuente: autor.

21. Despues de habilitará una nueva ventana “Evidence Item Information”, en la cual setearemos datos informativos tanto de la evidencia como del investigador.

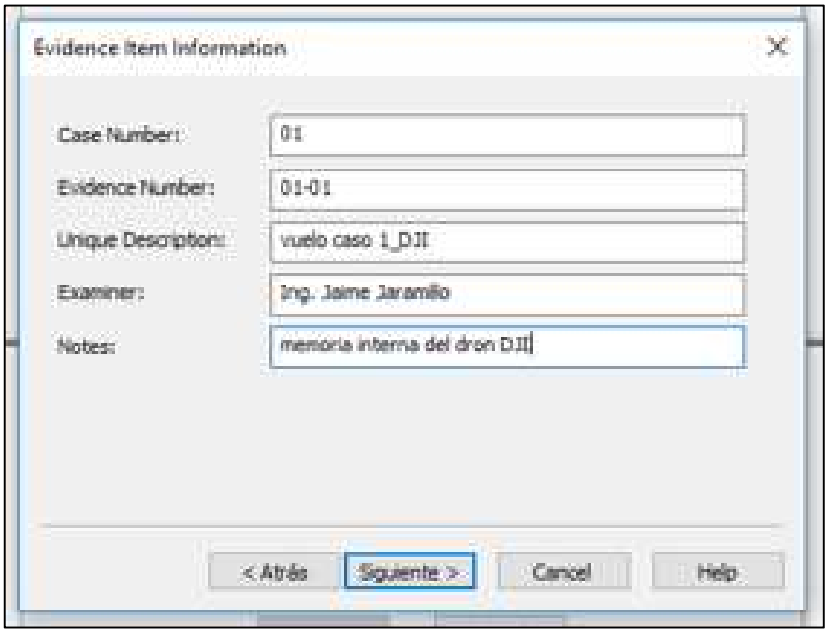

Figura 51. **Datos informativos de la evidencia y del investigador.**
Fuente: autor.

22. Luego de ubicar los datos informativos de la evidencia aparecerá una nueva ventana “Select Image Destination” en la dejaremos los valores por defecto del programa y haremos clic en la opción “Browse”.

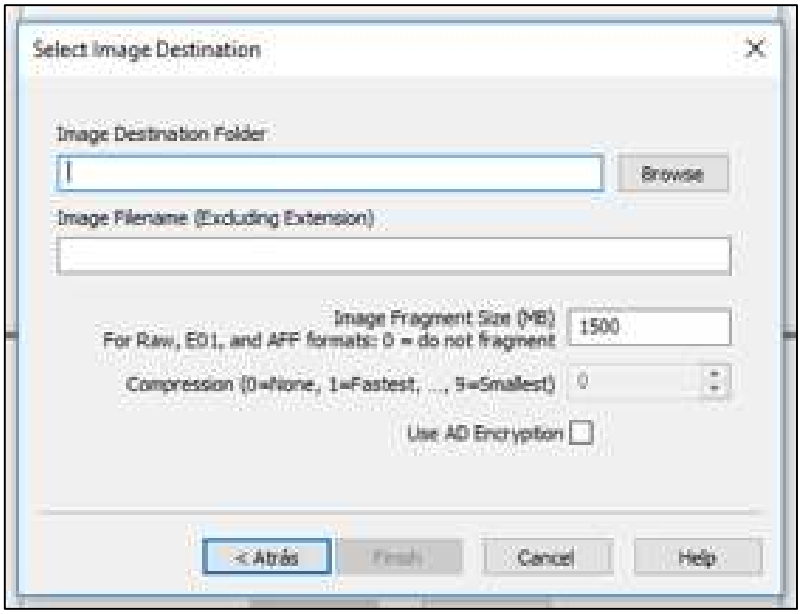

Figura 52. **Ubicación donde se guardará la imagen forense.**
Fuente: autor.

23. Inmediatamente se desplega una nueva ventana: “Buscar carpeta”. En esta ventana se debe seleccionar el destino en donde se creará la imagen forense de la Micro SD Card. A continuacion, se selecciona la fuente de la unidad (G) ya

que en esta se encuentra el dispositivo de almacenamiento USB Kingston de las características antes descritas.

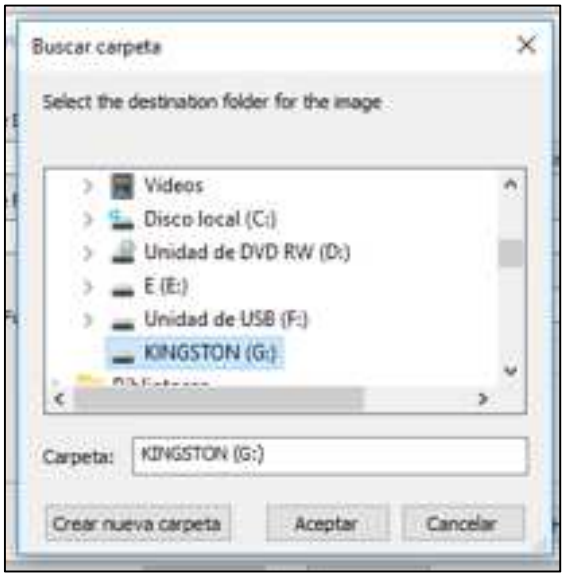

Figura 53. **Selección de ubicación de destino para la creación de la imagen forense.**
Fuente: autor.

24. Para finalizar el proceso de creación de imagen forense se debe colocar el nombre de la imagen forense en la opción “Image Filename”, aquí además se incluirá las extensiones para cada una de las particiones que se crearán en la extracción de la imagen forense.

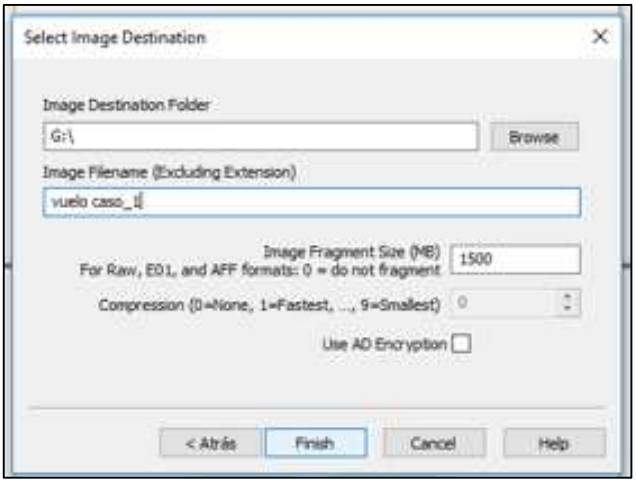

Figura 54. **Nombramiento de la imagen forense.**
Fuente: El autor.

25. Luego de establecer la información necesaria para la ubicación y extracción de la imagen forense, se hace clic en la opción “Start”.

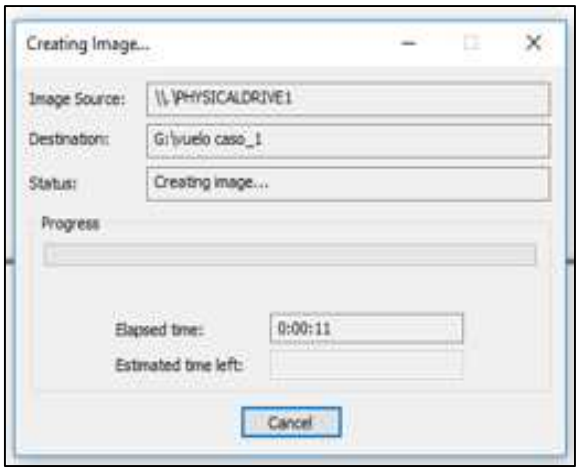

Figura 55. **Inicio de la extracción de la imagen forense.**
Fuente: autor.

26. Para finalizar este proceso seleccionamos la opción “close”, luego del tiempo transcurrido en la extracción “0:16:00”.

Figura 56. **Imagen forense extraída.**
Fuente: autor.

27. El programa FTK Imager automáticamente muestra una nueva ventana con un sumario en donde se revelan datos importantes como el código de autenticidad de la imagen MD5 Hash.

Figura 57. **Código MD5 Hash.**
Fuente: autor.

3.2.4 Decodificación del archivo DAT

28. Para realizar el análisis de la imagen forense de la memoria interna Micro SD Card, el mismo programa FTK Imager tiene una herramienta que permite leer la imagen forense. Para lo cual utilizamos la herramienta “Add Evidence Item”.

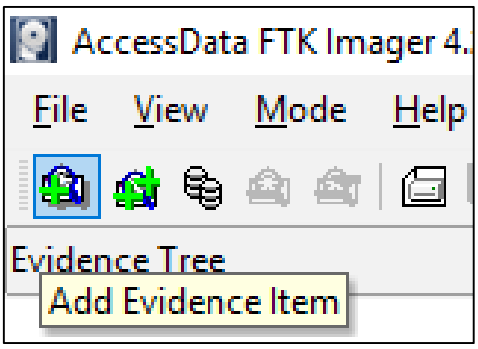

Figura 58. **Herramienta para Analizar Evidencia de la imagen forense.**
Fuente: autor.

29. Cuando ingresamos a esta herramienta se abre una nueva ventana que pide que seleccionemos el tipo de fuente del que se va analizar la evidencia, en esta opción se debe seleccionar la opción “Image File” y hacemos clic en siguiente.

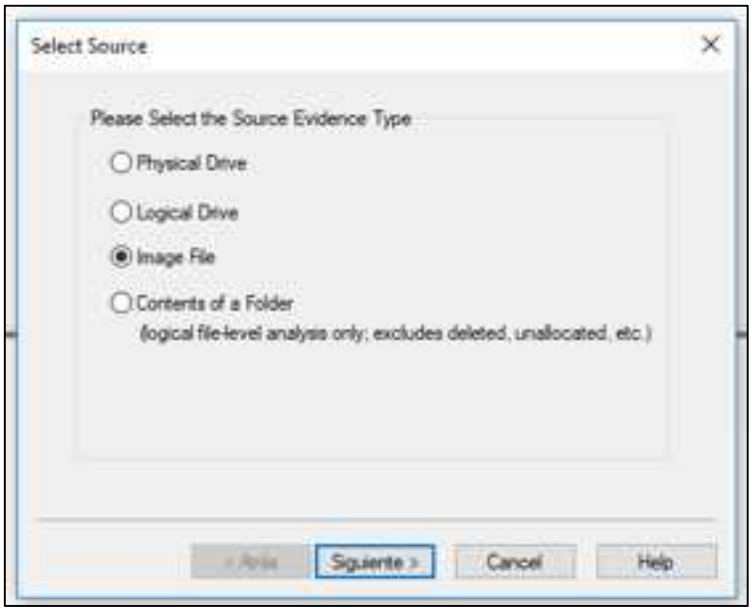

Figura 59. **Selección del tipo de fuente de la evidencia que se va analizar.**
Fuente: autor.

30. Luego se debe seleccionar el archivo que se va a leer que se ubica en este caso en la unidad “Kinston (G:)”, y, se desplegaran las tres particiones que se crearon para la imagen forense: “vuelo caso_1.001”, “vuelo caso_1.002” y “vuelo caso_1.003”. además, se observa un archivo: “vuelo caso_1.001.txt” el mismo que contiene datos informativos tipo sumario de la creación de la imagen forense como se muestra en la fase de análisis. Solo se deben agregar al análisis de

evidencia las tres partituras del disco que están con formato DAT y descartar el archivo con extensión TXT.

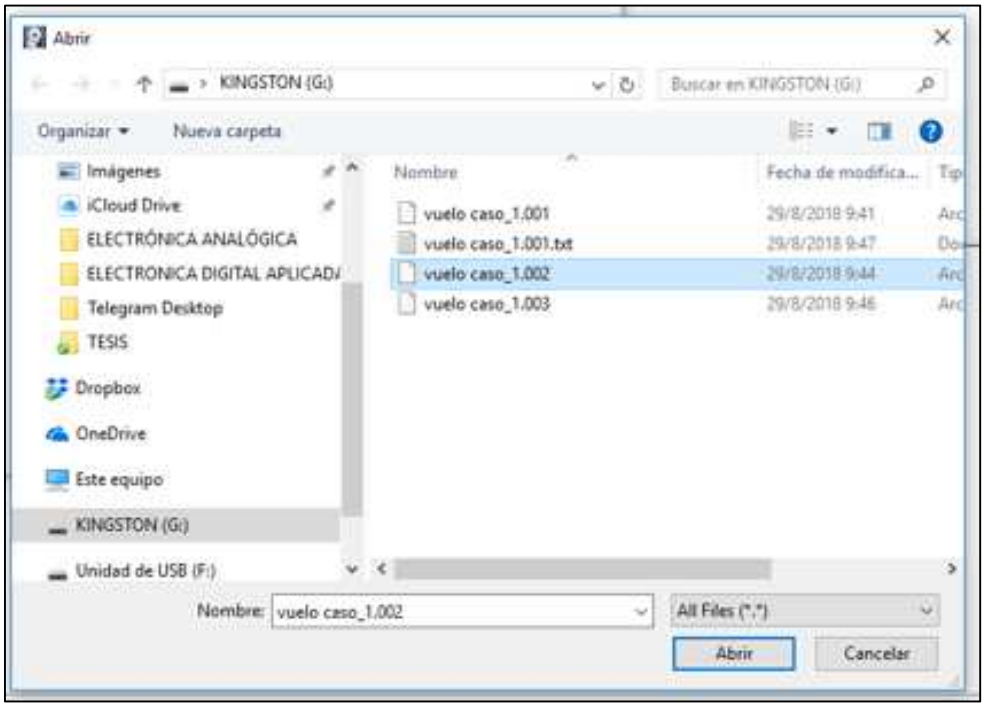

Figura 60. **Selección de particiones de la imagen forense.**
Fuente: autor.

31. Una vez agregadas las tres particiones de la imagen forense, se deberá centrar en la partición 1 ya que como se explicó en la fase de análisis, ésta contiene los datos del vuelo del caso de espionaje.

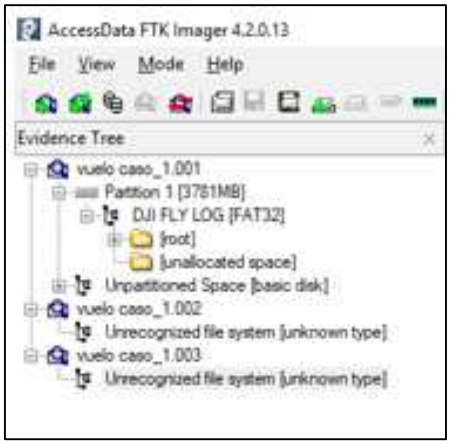

Figura 61. **Evidencia Completa (tres particiones agregadas).**
Fuente: autor.

32. Desplegamos la opción “vuelo caso_1.001” y encontramos la carpeta “DJI FLY LOG [FAT32]”, en esta carpeta se encuentran los registros de datos del vuelo del caso de espionaje preparado en la creación del escenario.

Figura 62. **Análisis de la evidencia del vuelo caso_1.001.**
Fuente: autor.

33. Ingresamos a la carpeta “root” y encontramos los archivos DAT con los registros del caso de espionaje. La información de estos archivos DAT no es legible para analizar directamente el investigador.

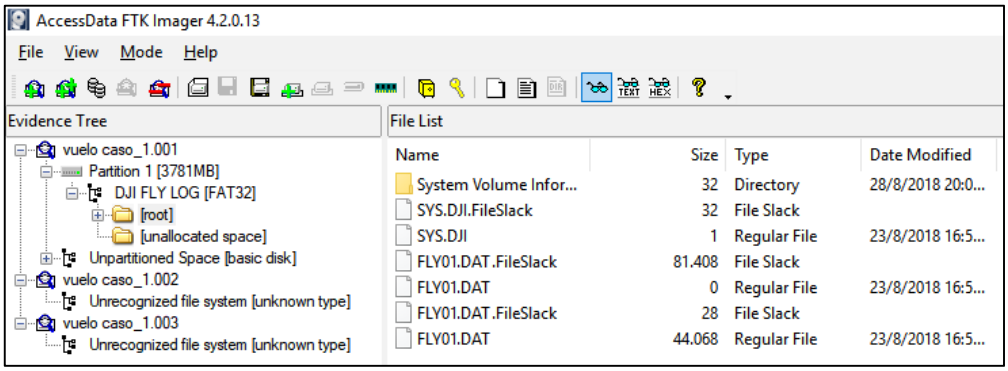

Figura 63. **Archivos DAT.**
Fuente: autor.

34. Al tener información no legible para el investigador, se utiliza una herramienta DatCon que es una herramienta de características descritas en el marco teórico de la investigación, que permitirá transformar de un formato DAT a un formato CSV. Abrimos la aplicación DatCon.

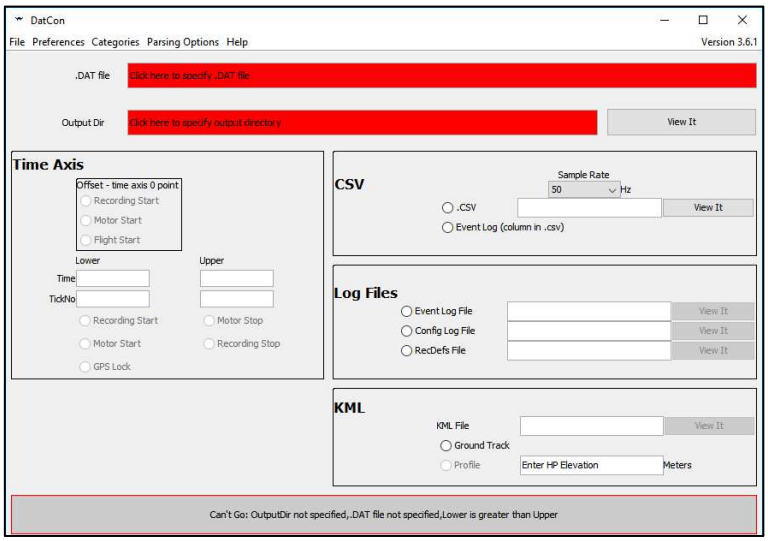

Figura 64. **Software decodificador DatCon.**
Fuente: autor.

35. Cargamos el archivo FLY01.DAT que fue extraído de la imagen forense y este caso había sido puesto como destino en el escritorio. La segunda opción “Output Dir”, se debe colocar la dirección donde se va a generar el archivo CSV, en este caso será en el “Desktop”. Luego marcamos la opción “CSV” y la opción “Event Log” y dejamos por defecto la opción “Sample Rate” en 50 Hz. Finalmente, hacemos clic en la opción “GO!”.

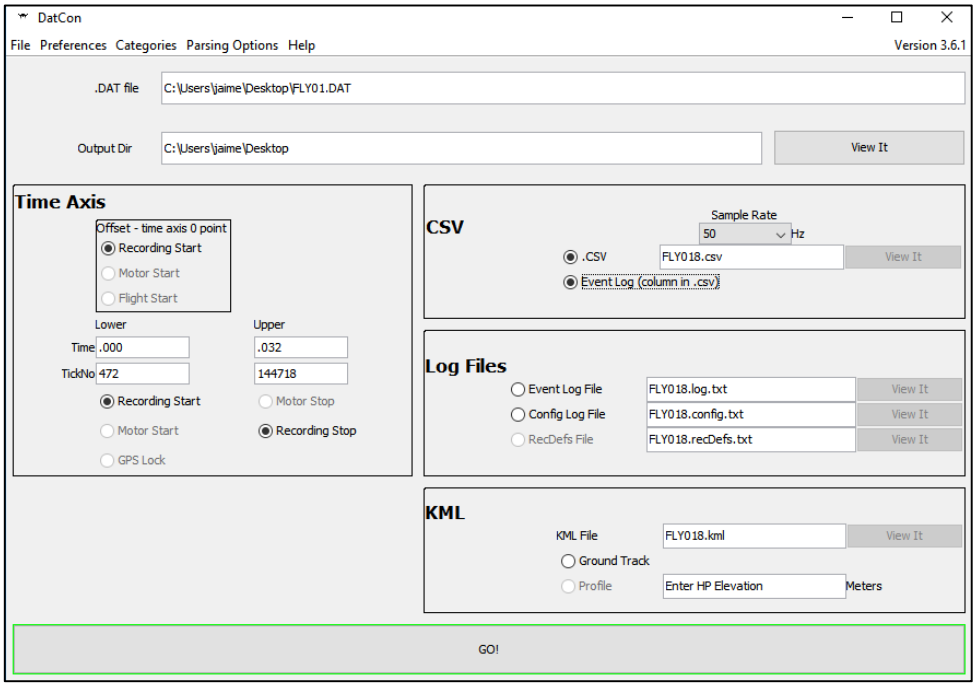

Figura 65. **Opciones de configuración para la conversión de formatos del programa DatCon.**
Fuente: autor.

36. El archivo CSV se generó en el escritorio, luego podemos ingresar y encontrar información del vuelo del caso de espionaje simulado en la creación del escenario, entre la información se encuentran datos del GPS como: latitud y longitud del despegue del dron.

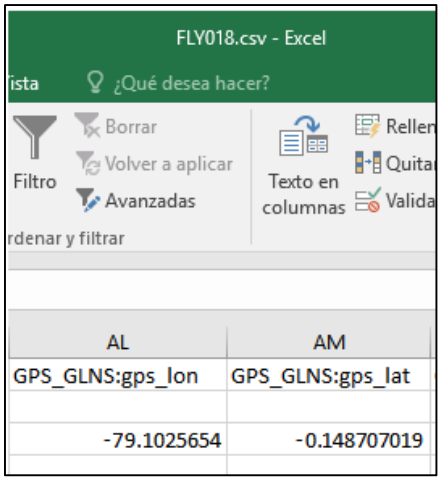

Figura 66. **Datos de latitud y longitud del archivo CSV.**
Fuente: autor.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

- Al realizar este trabajo se pudo evidenciar que hay investigaciones con respecto a la seguridad en los drones, pero existen pocos estudios realizados sobre el análisis forense de drones. A medida que los drones desarrollan nueva tecnología será necesario tener un estándar y aprobación de leyes que limiten sus capacidades tanto para el dispositivo como para el que lo opera.
- Se analizó detenidamente la estructura interna y funcionamiento de un DJI Phantom III Standard, centrándose en el análisis del almacenamiento, generación y proceso de archivos del GPS por parte del dron y a la vez de la aplicación que controla el dron. Al poseer la aplicación la opción de que el dron retorne al lugar del que despegó, es necesario guardar el registro en el dron de los datos de geoposicionamiento del cual realizó su despegue, los mismo que son leídos para aterrizar en una ubicación cercana ya que se comprobó que esta aplicación tiene un error del 10% que representan aproximadamente 3.5 metros a la redonda del punto de origen.
- Se comprobó que este 10% de error de la aplicación genera un problema para el aterrizaje del dron, ya que este dispositivo no presenta la opción de esquivar obstáculos por lo cual realizará el aterrizaje según sus coordenadas sin analizar el lugar donde aterrizará. Lo cual originará que el dron reciba golpes con algún objeto antes de llegar o no al objetivo.
- No existe ninguna información por parte de la empresa fabricante en sus plataformas hasta la fecha de esta investigación que indique los métodos de almacenamiento del dron lo cual demandó al investigador realizar pruebas sin guía al desmontar la estructura del dron y buscar la existencia de dispositivos de almacenamiento en la placa mainboard.
- Cuando se armó la estructura del dron se lo hizo sin colocar la memoria interna Micro SD Card en el sócalo del cual se la había retirado, luego se realizó pruebas de vuelo y el dron realizó todas las maniobras que normalmente el usuario demanda excepto la función de retornar al lugar de origen, cuando se seleccionó esta herramienta, el dispositivo ya que no pudo leer los datos de la memoria interna para realizar esta acción. De la misma manera una de las herramientas del DJI es que al mostrar un nivel bajo de batería (menor al 30%) el dron debe retornar a su lugar de despegue, en ese momento el dron colapsa y pierde el control al no detectar los datos de geoposicionamiento y realiza un descenso vertical automáticamente en la posición que detecta el nivel de batería.
- Se realizó un caso de delito de espionaje con un dron DJI Phantom III Standard y se realizó el análisis forense con las herramientas de análisis forense como AccessData Imager y la aplicación de conversión de formato DatCon, al ser herramientas sólidas en características de seguridad y del cuidado de la integridad de la información, permitiendo crear una guía que describe el paso a paso desde la captura del dron hasta la extracción de la imagen forense de la memoria interna donde se encuentran los datos del vuelo del caso simulado que

le servirán al perito para realizar sus informes forenses dándole veracidad en los mismos.

- La creación de la guía en este trabajo de investigación, proporciona al perito información técnica de la estructura interna del dron que no hay disponible por parte de los fabricantes de la marca China DJI. En esta guía el perito podrá encontrar rápidamente el procedimiento que debe seguir para extraer la memoria interna y también como extraer la información de este dispositivo de almacenamiento.
- Para crear la guía dentro del marco metodológico se determinó que su creación será en base a normas internacionales vigentes como la UNE 71505-3:2013 y la RFC 3227, que indican el correcto manejo de la evidencia digital para cuidar su integridad.
- En la fase de preservación de la norma UNE 71505-3:2013, recomienda que se debe obtener la imagen forense en el estado que se encuentra el dispositivo cuando es capturado (encendido), procedimiento que en este caso no se lo pudo llevar a cabo ya que para poder extraer la memoria interna del dron es necesario realizar el desmontaje de la estructura por lo cual es necesario no solo apagar el dispositivo sino también extraer su batería.
- El archivo CSV generado por el software DatCon necesita de una configuración dentro del programa Excel para ordenar los datos por filas y columnas para que el investigador pueda entenderlos rápidamente.

RECOMENDACIONES

La comunicación entre el dron y el dispositivo de control se realiza mediante una conexión Wifi por lo que presenta una vulnerabilidad por lo que se deben realizar investigaciones de metodologías de análisis de la seguridad en este tipo de conexión al existir un tráfico de paquetes en la red creada entre los dos dispositivos. Se debe crear como trabajo futuro una metodología que permita una vez que sea descubierto el dron, capturar los paquetes que se generan en el enlace entre los dos y a la vez puedan ser almacenados en un dispositivo de almacenamiento con un debido procedimiento forense que permita mantener la integridad de la información y que permita al perito realizar las pruebas necesarias para redactar un correcto informe forense, al realizarse esta metodología se obtendrían datos comprometedores de la aplicación que controla el dron, obteniendo información del dueño de la cuenta DJI GO que pide códigos propios del dron para su creación. Además, al obtener estos paquetes podemos obtener imágenes capturadas por el dron e incluso la transmisión de video que realiza el dron y se visualiza en el dispositivo de control.

CAPITULO V

BIBLIOGRAFÍA

Azas, 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*.

Basantes, C., & Sanchez, K. (2016). *ANÁLISIS FORENSE A SISTEMAS OPERATIVOS MEDIANTE LA UTILIZACIÓN DE HERRAMIENTAS OPEN SOURCE, CASO DE ESTUDIO WINDOWS 8*.

Cano, J. (2015). *Computación Forense*.

Ceron, A. (2005). SISTEMAS ROBÓTICOS TELEOPERADOS. *Ciencia e Ingeniería Neogranadina*, *15*, 62–69.

Clarck, D., Meffert, C., Baggili, I., & Breitinger, F. (2017). DROP (DRone Open source Parser) Your Drone: Forensic Analysis of the DJI Phantom III. *The International Journal of Digital Forensics & Incident Response*, *22*, 3–14.

Congreso-Nacional. (2012). Ley de Comercio Electrónico, firmas y mensajes. *Registro Oficial Suplemento 557*, *1*. Retrieved from http://www.justicia.gob.ec/

Consejo de la Judicatura. Reglamento del Sistema Pericial Integral de la Función Judicial, 1 § (2014). Retrieved from http://www.funcionjudicial.gob.ec/www/pdf/Reglamento del Sistema Pericial Integral de la Funcion Judicial.pdf

Cuerno, C., Garcia, L., Sánchez, A., Carrio, A., Sanchez, J., & Campoy, P. (2016). Evolución histórica de los vehículos aéreos no tripulados hasta la actualidad. *DYNA*, *91*(3), 282–288.

Díaz, J. (2015). *Estudio de Índices de vegetación a partir de imágenes aéreas tomadas desde UAS/RPAS y aplicaciones de estos a la agricultura de precisión.*

Gervilla, C. (2014). *METODOLOGÍA PARA UN ANÁLISIS FORENSE*.

González, J. (2013). Modelo para el Análisis Forense de una Plataforma Windows. *Universidad Piloto De Colombia*, 6.

Lázaro, F. (2013). *Introducción a la Informática Forense* (Ediciones).

Loarte, B. (2018). *DESARROLLO DE UNA GUÍA METODOLÓGICA PARA EL ANÁLISIS FORENSE DIGITAL EN EQUIPOS DE CÓMPUTO CON SISTEMA OPERATIVO Mac OS X EN EL ECUADOR*.

Loarte, B., & Grijalva, J. (2017). Marco de trabajo estandarizado para el análisis forense de la evidencia digital. *Revista Publicando*, *11*, 42–78.

López, Ó., Amaya, H., & León, R. (2001). INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS. *Universidad de Los Andes*, 22.

Maarse, M., Sangers, L., Van-Ginkel, J., & Pouw, M. (2016). Digital forensics on a DJI Phantom 2 Vision+ UAV. *University of Amsterdam*, *1.1*, 22.

Marín, J. (2018). Uso de drones comerciales como vectores terroristas. *Instituto Español de Estudios Estratégicos*, 35.

Ministerio de Justicia, D. H. Código Orgánico Integral Penal (2014). Retrieved from http://www.justicia.gob.ec/

Pardo, J. (2016). *IMPLEMENTACIÓN DE UN SISTEMA DE COMUNICACIÓN INALÁMBRICO ENTRE UN UAV/RPA CON SU ESTACIÓN TERRENA PARA LA TRANSMISIÓN DE IMÁGENES TÉRMICAS EN TIEMPO REAL Y SU UTILIZACIÓN EN EL CONTROL DE INCENDIOS.*

Pérez, H., Benítez, E., & Díaz, M. (2017). SISTEMA DE GEOREFERENCIADO DE IMÁGENES CON DRONES. *RA Ximhai*, *13*, 65–77.

ReviverSoft. (2014). Archivo DAT. Retrieved from https://www.reviversoft.com/es/file-extensions/dat

Thomson, S., Fountain, D., & Watts, T. (2007). Airborne Geophysics – Evolution and Revolution. *Decennial International Conference on Mineral*, *7*, 19–37.

Zúñiga, L. (2014). Código Orgánico Integral Penal. *Ministerio de Justicia, Derechos Humanos y Cultos*, *1*, 329.

ANEXOS

Anexo 1

SECCIÓN TERCERA
Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o

apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin

pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Anexo 2

En el capítulo II, artículo 4, de la Resolución 040-2014 del Reglamento del Sistema Pericial Integral de la Función Judicial, dice que “Las personas que deseen calificarse como peritos de la Función Judicial, deben cumplir con los siguientes requisitos:

1. Ser mayores de edad, ser capaces y estar en ejercicio de sus derechos de participación.
2. Ser conocedoras o conocedores y/o expertas o expertos en la profesión, arte; oficio, o actividad para la cual soliciten calificarse;
3. En el caso de profesionales, tener al menos dos (2) años de graduadas o graduados a la fecha de solicitud de calificación, y cumplir con los requisitos de experiencia establecidos en este reglamento. Para las y los demás expertos tener al menos dos (2) años de práctica y experiencia a la fecha de la solicitud de calificación, en el oficio, arte o actividad en la cual tengan interés de calificarse;
4. También se podrán, presentar, para justificar la experticia y conocimiento de la o el solicitante, hasta diez (10) informes periciales realizados en los últimos dos (2) años, los cuales serán analizados por el Consejo de la Judicatura para determinar si acreditan experticia; y,
5. 5. No hallarse incursas o incursos en las inhabilidades o prohibiciones para ser calificada o calificado como perito previstas en la ley y este reglamento.”

Una vez que el profesional ha cumplido con todos los pasos y requisitos establecidos en el Reglamento del Sistema Pericial Integral de la Función Judicial, la Dirección Provincial del Consejo de la Judicatura correspondiente procederá:

1. Entregar el certificado o identificación de calificación de Perito del Consejo de la Judicatura con una validez de dos (2) años, con la siguiente información:

    - Nombres y Apellidos completos;
    - Número de cédula de ciudadanía;
    - Número de código de calificación;
    - Tiempo de vigencia; y,
    - Área y especialidad a las que corresponde la calificación.

2. Asignar un código al Perito calificado, y abrir un expediente personal en el sistema informático pericial, para su evaluación y seguimientos de sus actuaciones posteriores en el ejercicio de actividad pericial.

El Artículo 18 de la Resolución 040 - 2014 menciona como obligaciones generales que un perito debidamente calificado debe cumplir: desempeñar su función de auxiliar de la justicia con objetividad, imparcialidad, responsabilidad, oportunidad, puntualidad, rectitud, corrección, honestidad y que su trabajo deberá enmarcarse en todo momento

en la ética, junto con la presentación de su criterio técnico y especializado, exento de juicios de valor de ningún tipo.

De igual manera el Artículo 19 de esta Resolución 040 - 2014, establece las obligaciones específicas que el perito de cumplir, dentro de las que se mencionan:

1. El perito debe asistir obligatoriamente cuando es convocado dentro de un proceso judicial.
2. Posesionarse obligatoriamente una vez que han sido designados.
3. Presentar el informe pericial correspondiente en la forma, plazos y términos previstos por la normativa o por la autoridad judicial correspondiente.
4. Explicar y defender el informe presentado con sus respectivas conclusiones.
5. Presentar en conjunto a su informe en todos los procesos judiciales, una copia de la factura de honorarios.
6. Aprobar todos los cursos de capacitación y cualquier otra obligación.
7. El Perito está en la obligación de realizar y terminar las pericias a su cargo, en caso de que haya sido excluido en su calidad de tal.
8. El perito debe exponer su informe en la audiencia convocada y contestar las preguntas realizadas por el juez, las partes o el fiscal, dependiendo de cada caso. Tanto la exposición como las preguntas deben referirse a aspectos técnicos contenidos en el informe.