UNIVERSIDAD INTERNACIONAL SEK

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Trabajo de fin de carrera titulado:

"METODOLOGÍA PARA EL ANÁLISIS FORENSE DE LA INFORMACIÓN DIGITAL CONTENIDA EN CONSOLAS DE VIDEOJUEGOS EN EL ECUADOR, CASO DE ESTUDIO XBOX ONE"

Realizado por:

BRYAN SEBASTIAN CÓRDOVA OJEDA

Director de Proyecto:

Ing. Luis Fabián Hurtado Vargas, MGS.

Como requisito para la obtención del título de:

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

Quito, 14 de junio de 2018

DECLARACION JURAMENTADA

Yo, BRYAN SEBASTIAN CÓRDOVA OJEDA, con cédula de identidad #171748494-1, 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.

Bryan Sebastián Córdova Ojeda

C.C.: 171748494-1

DECLARATORIA

El presente trabajo de investigación titulado:

“METODOLOGÍA PARA EL ANÁLISIS FORENSE DE LA INFORMACIÓN DIGITAL CONTENIDA EN CONSOLAS DE VIDEOJUEGOS EN EL ECUADOR, CASO DE ESTUDIO XBOX ONE”

Realizado por:

BRYAN SEBASTIAN CÓRDOVA OJEDA

Como requisito para la Obtención del Título de:

MAGÍSTER 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

_____

Ing. Luis Fabián Hurtado Vargas, MGS.

DIRECTOR

LOS PROFESORES INFORMANTES

Los Profesores Informantes:

CHRISTIAN DAVID PAZMIÑO FLORES

WALTER EDISON ESTRELLA MOGOLLON

Después de revisar el trabajo presentado,

lo han calificado como apto para su defensa oral ante

el tribunal examinador

_____ _____

Christian David Pazmiño Flores Walter Edison Estrella Mogollón

Quito, 14 de junio de 2018

DEDICATORIA

Dedico este trabajo a mi hijo Fabian Alfonso, a mi esposa Ana Gabriela y a mi madre Noemi Ojeda, así como a mi hermano y mi padre por estar siempre conmigo en cada decisión que tomo.

A la memoria de mis abuelos Luis Alfonso Ojeda y Fabian Córdova quienes siempre me inspiraron en ser una mejor persona y un mejor profesional.

Finalmente, todos mis compañeros en especial a David, Wilson, Diego y Marco ya que juntos logramos formar grandes lazos de amistad, así como profesional.

AGRADECIMIENTO

Al Ing. Sebastián Grijalva por haber aprobado el tema propuesto y al Ing. Fabián Hurtado por aceptar dirigir este proyecto de investigación con profesionalismo y dedicación además también por su apoyo y guía ya que han sido fundamentales para la realización del proyecto.

A la Ing. Verónica Rodríguez, al Ing. Edison Estrella, al Ing. Jose Luis Medina, quienes supieron impartir de manera adecuada sus conocimientos y desarrollar una visión diferente e integradora durante la formación y ahora se ven inmersos en torno a esta investigación.

A la Universidad Internacional SEK, por su esfuerzo en formar profesionales con visión y enfoque empresarial.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS Y FIGURAS

RESUMEN

Cada día la tecnología avanza más rápido, muestra de aquello se evidencia en las consolas de videojuegos, las cuales en la actualidad incorporan varios usos de las TIC (Tecnologías de la información y Comunicación), como son mensajería instantánea, video conferencia, chat por voz, redes sociales, navegación por internet, etc. en su cotidiano uso.

A medida que la tecnología se ha ido desarrollando con el objeto de satisfacer las necesidades de la sociedad mediante la simplificación para realizar actividades cotidianas de los usuarios, quienes consumen de manera masiva los productos y servicios tecnológicos, los cuales los exponen a nuevas y más graves amenazas de seguridad. Amenazas las cuales se comprenden en un sin número de delitos informáticos cometidos por diversos medios, entre los cuales se encuentran: robo de información, fraude a tarjetas de crédito, rapto, pornografía infantil, ya sea su producción o distribución, etc.

En el Ecuador, se requiere de un proceso formal y avalado en la judicialización de la evidencia, en este caso la evidencia proviene de equipos tecnológicos. Para lo cual se requiere de Peritos Informáticos o de personas capacitadas en el uso de tecnología especifica.

En esta investigación, se evidenciara que la información contenida en una consola de videojuegos de la actual generación de consolas no es considerablemente conocida por los Peritos Informáticos, además que existen metodologías para una variedad limitada de equipos tecnológicos sobre los cuales se puede extraer evidencia y generalmente se limita a computadores ya sean de escritorio o portátiles y a teléfonos celulares; por tal motivo se omite la información que se encuentra en otros equipos debido a la falta de conocimiento sobre el funcionamiento y los datos que se manejan a través de estos, en este caso, de las consolas de videojuegos. Se planteará la elaboración de una guía metodológica para la obtención de dicha información y presentarla como Evidencia Digital judicializable utilizando como medio una consola de videojuegos Xbox One.

Palabras clave: TIC, Delito informático, Análisis Forense, perito informático, Evidencia Digital, consola de videojuegos, Xbox One.

ABSTRACT

Every day the technology advances faster, shows that it is seen in the consoles of video games, which currently incorporate several uses of ICT (Information and Communication Technologies), such as instant messaging, video conferencing, voice chat, social networks, internet browsing, etc. in its daily use.

As technology has been developed to meet the needs of society through simplification to perform daily activities of users, who massively consume technology products and services, which expose them to new and more serious security threats. Threats which are understood in several computer crimes committed by various means, among which are: theft of information, credit card fraud, kidnapping, child pornography, whether its production or distribution, etc.

In Ecuador, a formal process is required and guaranteed in the judicialization of the evidence, in this case the evidence comes from technological equipment. For which it requires computer experts or people trained in the use of specific technology.

In this research, it will be evident that the information contained in a videogame console of the current generation of consoles is not known by the experts, in addition there are methodologies for a limited variety of technological equipment on which evidence can be extracted and generally limited to desktops or laptops and cell phones; for this reason the information found in other equipment is omitted due to the lack of knowledge about the operation and the information handled through them, this is the case of video game consoles. The elaboration of a methodological guide will be proposed to obtain this information and present it as judicializable evidence using as a medium an Xbox One videogame console.

Keywords: ICT, computer crime, forensic analysis, digital forensics analyst, digital evidence, video game console, Xbox One, forensic analysis methodology

CAPITULO I

INTRODUCCIÓN

1.1. EL PROBLEMA DE LA INVESTIGACIÓN

1.1.1. Planteamiento del Problema

En los últimos años hemos sido testigos de la evolución de la industria tecnológica, a tal punto que ahora contamos con una generación de consolas de videojuegos con características tan similares a las de un computador de escritorio, que nos permiten tener a parte del contenido de entretenimiento, así como también contenido social, lo que implica la capacidad de utilizar este medio para el cometimiento de actividades ilícitas y brinda un gigantesco campo lleno de potenciales víctimas de ataques.

La falta de conocimientos por parte de la población en general, de cómo evitar compartir ciertos contenidos aumenta la probabilidad para el cometimiento de delitos, esto sumado al crecimiento exponencial en ventas de las consolas merece ser tomado en cuenta al momento de realizar una investigación de carácter judicial.

Actualmente en nuestro país existen denuncias sobre delitos informáticos, lastimosamente la omisión de Evidencia Digital judicializable de consolas de videojuegos a limitado severamente el fallo adecuado en su juzgamiento, por tal motivo es de imperante necesidad brindar los conocimientos necesarios, así como un camino definitivo por el cual guiar a los Peritos Informáticos para la obtención de dicha evidencia.

Para que estos delitos informáticos sean juzgados ante una audiencia, se requiere presentar la denominada Evidencia Digital, siendo esta la información almacenada en cualquier dispositivo de almacenamiento electrónico digital o que hayan sido procesados electrónicamente en algún medio electrónico, como pueden ser correos electrónicos, archivos de audio, mensajes o datos en general transmitidos de manera digital.

Debido al hecho que la información se encuentre de manera digital, dejando de lado el almacenamiento en papel, se vuelve más relevante en un proceso de tipo civil o penal, debido a que esto deriva en pericias informáticas especifica en torno de obtener la evidencia, provocando una cierta cantidad de eventualidades:

- Falta de conocimientos específicos por parte de los Peritos Informáticos sobre el funcionamiento y la información contenida en consolas de videojuegos, ocasionando la omisión de Evidencia Digital en el proceso de búsqueda.

- Ante la falta de un método para el Análisis Forense de consolas de videojuegos, ocasiona que la Evidencia Digital obtenida de estos equipos sea repudiada legalmente ante un tribunal.

- El desconocimiento sobre la existencia de controles que pongan en evidencia cuando el equipo de cómputo o el de análisis donde se realiza la investigación no hayan sido manipulados y alterados por terceras personas con objeto de obstaculizar el resultado de la investigación forense, ocasionando que los informes periciales a partir de dicho análisis no sean concisos y por consiguiente pierdan credibilidad.

Lo mencionado anteriormente, ayuda a entender que el principal problema que se debe resolver es la falta de conocimientos por parte de los Peritos Informáticos sobre la obtención de la Evidencia Digital con carácter probatorio de consolas de videojuegos.

1.1.1.1.Diagnóstico

La constante evolución de las tecnologías de la información, han dado como resultado a un nuevo concepto, que la información debe estar disponible siempre y en todo lugar. Por tal motivo motivando al cometimiento de actos ilícitos con el objeto de apoderarse de dicha información que ya no solo la podemos encontrar en computadores o teléfonos celulares inteligentes sino también en las consolas de videojuegos.

Se puede definir al delito informático como la apropiación ilícita de la información, haciendo uso de la tecnología electrónica sea esta utilizada como método, medio o fin. El objetivo de estas prácticas puede ser entre otros: robo de información confidencial, destrucción de programas o datos y el acceso no autorizado a la información, fraudes, estafas, ciberterrorismo, pornografía infantil, falsificación de tarjetas de crédito, etc. todos estos tipos de delitos son reconocidos por la ONU[1].

Las consolas de videojuegos son equipos con tecnología electrónica, las cuales han avanzado de tal manera que en la generación actual ya contamos con servicios iguales a los de un computador, de tal manera que las empresas desarrolladoras están siempre intentando mejorar tanto la interfaz de usuario como el manejo de la información, dando lugar a aplicaciones tan sencillas de usar y que son pensadas para que hasta un niño pueda interactuar con los demás usuarios.

En el año 2016 se denunció un delito en la Provincia del Napo, indicando que un usuario solicito fotos que contenían desnudez explicita de un niño a cambio de un videojuego en

[1] Organización de las Naciones Unidas

formato físico, la denuncia fue presentada por parte de los padres del menor quienes luego de escuchar la declaración de su hijo concluyen que la información fue intercambiada utilizando una consola de videojuegos Xbox One como medio para el cometimiento de dicho delito, de manera penosa al entregar la consola para su análisis, no se logró obtener la evidencia requerida por parte del Perito Informático designado para el Análisis Forense de esta consola, con el objeto de determinar la verdad sobre el caso y como resultado el mismo término archivándose.

En el Ecuador de acuerdo al artículo 040-2014 del Consejo de la Judicatura, los requisitos para calificar como perito varían de acuerdo a su especialidad, por tal motivo y dado el caso que las consolas de videojuegos son equipos electrónicos con componentes informáticos, el perfil más idóneo para realizar el análisis de dichos equipos es el Perito Informático, pese a aquello los requisitos para calificar como tal se limitan a ser profesional de la carrera de informática y dos años de experiencia, de igual manera, cabe indicar que en ninguna malla curricular de la carrera de informática en universidades e institutos del país se imparte materia sobre la arquitectura, funcionamiento o la información que se encuentra en dichas consolas.

Actualmente, de acuerdo con la investigación realizada, los Peritos Informáticos carecen de la capacidad para llevar a cabo el Análisis Forense de consolas de videojuegos debido a que no cuentan con la preparación académica para ello, este resultado se pudo evidenciar al realizar un cotejamiento de datos de Peritos Informáticos que se encuentran acreditados en el Sistema Pericial de la página web de la Función Judicial del Ecuador y los datos investigados de la consulta de títulos registrados de la página web de la Senescyt.

- Para la investigación se obtuvo una muestra de 10 Peritos Informáticos que cumplan con los parámetros necesarios dentro de la provincia de Pichincha.

- De los peritos seleccionados se pudo determinar que 8 poseen título de tercer nivel, 5 de ellos poseen título de cuarto nivel y 2 cuentan con título de nivel Técnico o Tecnológico Superior.

Debido a que los peritos cuentan efectivamente con títulos acordes al tipo de pericia a realizar todavía no se puede descartar que dichos peritos posean formación sobre el funcionamiento de consolas de videojuegos además de la información contenida en las mismas. Por tal motivo se realizó un estudio sobre las mallas curriculares de las principales universidades de la provincia de Pichincha donde obtuvieron sus títulos de tercer y cuarto nivel.

En las universidades, Central, Escuela Politécnica Nacional, Escuela Politécnica del Ejercito, Universidad Particular Internacional Sek, Universidad de las Américas, se tomó como ejemplo la carrera de Ingeniería de Sistemas, donde se evidencio que en ninguna de sus mallas existe materia sobre la arquitectura o el funcionamiento ni cómo se maneja la información contenida en las consolas de videojuegos.

Además de la falta de capacitación en torno a las consolas de videojuegos, se puede demonstrar la existencia de metodologías preexistentes para el Análisis Forense tradicional,

siendo estas demasiado específicas. Dependerá mucho del entorno al cual se va a realizar el análisis, estos serán:

- Análisis forense de sistemas.
- Análisis forense de redes.
- Análisis forense de sistemas embebidos.

Esto sin embargo no significa que no existan trabajos sobre este tema, si bien en la publicación Preliminary forensic analysis of the Xbox One de acuerdo con (Moore, Baggili, Marrington, & Rodrigues, 2014) quienes utilizan una metodología de Análisis Forense dedicada a un videojuego especifico y en etapas inconclusas que no llegan a complementarse como una metodología como tal sino más como una investigación.

Además, se evidencio que, en el Departamento de Ciencias Forenses de la Policía Nacional, apenas cuentan con metodologías generales para el análisis de equipos de computación y teléfonos inteligentes, procesos los cuales no han sido estandarizados y por ende carecen del conocimiento científico sobre el cual se pueda aplicar a otro tipo de dispositivos electrónicos, siendo el caso no existen metodologías ni guías sobre Análisis Forense aplicable para consolas de videojuegos en el Ecuador.

1.1.1.2.Pronóstico

Por lo expuesto en el diagnóstico, se determina que el problema a resolver es, la falta de conocimientos sobre el funcionamiento y la arquitectura de las consolas de videojuegos Xbox One por parte de los Peritos Informáticos registrados en el sistema pericial de la función judicial, quienes son los encargados del procesamiento de dichos equipos.

Mientras no exista el conocimiento para realizar el Análisis Forense para las consolas de videojuegos Xbox One, aumentara la cantidad de estos equipos que permanecerán sin examinar, evitando de esta manera la obtención de evidencia con sustento legal probatorio de estos equipos.

1.1.1.3.Control del Pronóstico

El elaborar mecanismos que incluyan técnicas, herramientas con sustento legal vigente que permitan brindar el conocimiento necesario a todo Perito Informático que lo requiera, con el objeto de obtener evidencia con sustento legal probatorio de consolas de videojuegos Xbox One y que a su vez garantice el no repudio al ser presentada en un proceso judicial, esto servirá de ayuda para solucionar parte de la problemática y permitirá hacer campañas de prevención sobre delitos informáticos perpetrados con consolas de videojuegos y como esto afecta a la sociedad.

1.1.2. Formulación del problema

Cuando ocurra un delito en el cual se utilice una consola de videojuegos Xbox One ya sea como método, medio o fin, no se podrá judicializar la Evidencia Digital contenida en ella, debido a la falta de conocimientos técnicos por parte de los Peritos Informáticos sobre el funcionamiento y arquitectura de dichos equipos.

1.1.3. Sistematización del Problema

- ¿Cómo puede el investigador, adquirir el conocimiento para determinar qué información se puede procesar como Evidencia Digital?
- ¿Cuáles son las técnicas que permiten al investigador forense obtener el conocimiento sobre normas, métodos y estándares para el manejo adecuado de la Evidencia Digital que se adquiera de consolas de videojuegos Xbox One?
- ¿Con que método puede el investigador forense obtener el conocimiento sobre herramientas que permitan obtener Evidencia Digital de consolas de videojuegos Xbox One?
- ¿Cómo se podrá judicializar la Evidencia Digital obtenida de una consola de videojuegos Xbox One?

1.1.4. Objetivo General

Elaborar una metodología para el Análisis Forense de la consola Xbox One, mediante la aplicación y adaptación de las técnicas tradicionales, normativa legal vigente del Ecuador, el estudio de la arquitectura física y lógica de este tipo de consolas, que permita la obtención de Evidencia Digital judicializable de estos equipos.

1.1.5. Objetivos específicos

- Investigar sobre el funcionamiento, arquitectura y sistema de archivos del sistema operativo de la consola de videojuegos Xbox One, que permita obtener el conocimiento necesario para identificar fuentes de Evidencia Digital.
- Investigar normas, métodos y estándares, para el buen manejo de Evidencia Digital, obtenible mediante el Análisis Forense.
- Investigar que Herramientas Forenses son comúnmente utilizadas en investigaciones realizadas en el Ecuador con el objeto de determinar si dichas herramientas son capaces de interpretar la Evidencia Digital contenida en consolas de videojuegos Xbox One.

- Elaborar una metodología para el Análisis Forense de la consola que sirva de guía para los especialistas en procesos legales en los cuales se tenga como prueba una consola Xbox One.

1.1.6. Justificación

Según la revista Forbes, a partir de enero de 2014, Microsoft había vendido aproximadamente 3,4 millones de unidades Xbox One desde su lanzamiento el 22 de noviembre de 2013. En los últimos años, los sistemas de videojuegos de Microsoft han mantenido las mejores ventas de consolas entre sus competidores y no es diferente en nuestro país, con cerca de 5000 consolas vendidas.

Estos sistemas de videojuegos son ahora comparables a los computadores de escritorio con una capacidad de procesamiento similar, sistema operativo, funciones de red, procesadores gráficos de alta potencia y una gran cantidad de almacenamiento. A medida que aumentan las funcionalidades de estas consolas, también aumenta su potencial de uso en actividades ilícitas. Los investigadores criminales han buscado históricamente reunir pruebas de computadoras, teléfonos celulares y distintos dispositivos móviles; sin embargo, se pasa por alto las consolas de videojuegos, valorando sólo su carácter lúdico; ya que también poseen aplicaciones de carácter social como chat de texto, chat por voz, redes sociales, que son utilizadas para el cometimiento de delitos.

De acuerdo con (Moore et al., 2014) es imprescindible proporcionar el análisis de la Xbox One para proveer a los investigadores una comprensión del sistema propietario de la consola con el objetivo de recuperar las pruebas que puede contener.

El Código Orgánico Integral Penal del Ecuador vigente establece ciertos tipos de delitos que se pueden perpetrar mediante el uso de la tecnología, y en nuestro país existen varias metodologías para la obtención de elementos de juicio como es la guía metodológica propuesta por (Loarte & Grijalva, 2017); sin embargo, de acuerdo con dicho estudio indica que su marco metodológico será aplicado en computadores y teléfonos móviles, pero servirá de referencia para el desarrollo de esta investigación.

Adicionalmente con la realización de este proyecto de investigación se beneficiará a tres grupos importantes en la sociedad:

- A los Peritos Informáticos que se dediquen al Análisis Forense en el Ecuador, para que tengan un conocimiento técnico y científico que les permita descubrir en medios electrónicos no convencionales Evidencia Digital judicializable.

- A los fiscales y jueces, para que de esta manera puedan tener una base científica de los hechos que sucedieron con el delito cometido, mediante el trabajo realizado por parte de los Peritos Informáticos y que de esta manera evitar el no repudio de la información entregada como evidencia entregada.

- A la sociedad, para que, en el futuro, los delitos cometidos teniendo una consola de videojuegos como medio, víctima o instrumento del delito, se puedan judicializar y obtener la evidencia que permita esclarecer la verdad sobre un juicio ya sea civil o penal.

Cada usuario de consolas de videojuegos está expuesto a ser víctima de un delito informático, por lo cual para el caso de estudio se contará con una consola Xbox One, la cual pertenece a la actual generación de consolas de videojuegos y presenta todas las características para el desempeño del trabajo de investigación.

1.2. MARCO TEÓRICO

Delitos informáticos

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar información en computadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito.

Los delitos informáticos son aquellas actividades ilícitas que:

a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o

b) Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos)

Tipos de delitos informáticos

Los tipos de delitos informáticos presentes en la actualidad, entre los cuales tenemos:

Delitos en contra de la confidencialidad, la integridad y la disponibilidad de los datos y delitos informáticos, que, a su vez, se dividen en tres partes:

- Acceso ilícito a los sistemas informáticos.
- Interacción ilícita de los datos informáticos.
- Interferencia en el funcionamiento de los delitos informáticos.

Algunos ejemplos de estos delitos podrían ser: el robo de identidades, el ingreso a páginas web no autorizadas, y el uso de programas o virus malhechores que bloquean o intervienen en un sistema informático.

Delitos relacionados con los datos informáticos, los cuales se dividen en dos partes:

- Falsificación informática.
- Fraude informático.

Los cuales se caracterizan por la intervención de los sistemas informáticos, ya sea para lograr un borrado de los datos, un robo de información personal o una alteración de dichos sistemas. También es parte de este tipo de delitos, la obtención de bienes y servicios mediante el uso de tarjetas inteligentes.

Delitos relacionados con las infracciones de la propiedad intelectual, considerados como "Piratería Informática", la cual podríamos definir como la copia y distribución de programas informáticos.

Por último, tenemos los delitos relacionados con el contenido, el cual abarca la producción, oferta, difusión y adquisición de pornografía infantil, por medio de un sistema informático, o también, posesión de dichos contenidos en dichos sistemas.

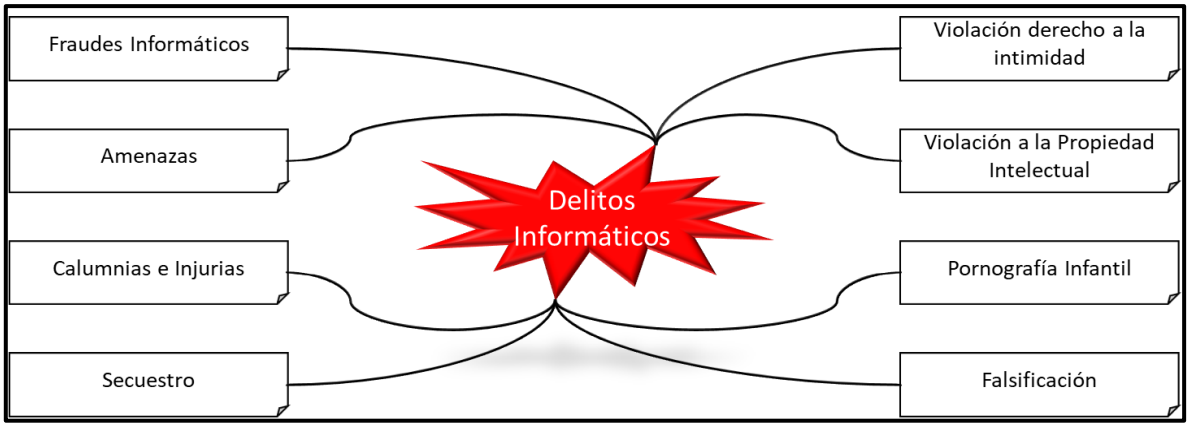


Figura 1. Delitos Informáticos
Fuente: Bryan Córdova

Normativa Legal en el Ecuador

- **Código Orgánico Integral Penal**

Publicado el 10 de febrero de 2014 mediante el Registro Oficial Nº180 El COIP[2] "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."(Asamblea Nacional, 2014)

- **Resolución 040-2014**

Esta resolución es el Reglamento del Sistema Pericial Integral de la Función Judicial, aprobado por el Pleno del Consejo de la Judicatura, el pasado 10 de marzo de 2014. Este

[2] Código integral penal (COIP) vigente de la República del Ecuador

reglamento ha sido modificado por el Consejo de la Judicatura el cual resolvió: "EXPEDIR EL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL". Permitiendo regular el funcionamiento y administración del Sistema Pericial, en relación con la calificación, designación, obligaciones, evaluación y cualquier otro aspecto que tenga relación con los peritos que participen en los procesos judiciales, pre procesales, o de cualquier otra naturaleza que se lleven a cabo en la Función Judicial.

- **Sistema Automático de Trámite Judicial Ecuatoriano "SATJE"**

Es un sistema donde se encuentran registrados todos los peritos acreditados por el Consejo de la Judicatura, ubicándolos en un catálogo de acuerdo con las Especialidades de estos. El proceso de selección del perito se lo realiza al azar con lo cual se garantiza una igual distribución o asignación de los Peritos que se encuentran registrados en la base de datos.

- **Requisitos de acreditación de Peritos Informáticos**

Según el reglamento del Consejo de la Judicatura (JUDICATURA, 2014) de peritaje, los requisitos que deben cumplir las personas para calificarse como Perito Informático están reglamentados en el Artículo 18 de la Resolución 040-2014 del Reglamento del Sistema Pericial Integral de la Función Judicial, según el cual estos son:

- Ser mayor de edad.
- Deben ser expertos en la profesión, arte, oficio, o actividad para cual soliciten calificarse.
- En caso de ser profesionales, deben tener al menos dos (2) años de graduadas o graduados. Para los demás expertos tener al menos dos (2) años de práctica y experiencia en el oficio arte o actividad.
- Finalmente, no encontrarse incursas o incursos en las inhabilidades o prohibiciones para ser calificada o calificado como Perito previstas en la ley y mencionadas en este reglamento.

- **Especialidades de Peritos Informáticos**

Un Perito Informático puede calificarse en las siguientes especialidades:

- Criminalística Informática: Siempre y cuando se otorgué una capacitación por afinidad que será avalado por la Policía Nacional.
- Ingeniería Informática o de Sistemas: Requiriendo su título de profesión debidamente aprobado por la SENECYT.

Informática Forense

Materia judicial que permite mediante el uso de un conjunto de técnicas para extraer información valiosa de equipos informáticos, sin alterar el estado de estos. "Esto permite buscar

datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta.” (Porolli, 2013)

Fases del Análisis Forense:

Según la norma UNE: 71505-3:2013 las fases para el Análisis Forense se dividen en cinco, Fase de Preservación, Fase de Adquisición, Fase de Documentación, Fase de Análisis y la Fase de Presentación las cuales a su vez cuentan con sub-fases las cuales ayudan al Perito Informático para que realice su informe pericial de la manera más completa y detallada posible, a continuación, se presenta un resumen de cada fase:

A. Fase de Preservación:

La prioridad es asegurar la integridad de la evidencia original en la escena del delito, es decir, en esta fase el Perito Informático se asegura y toma las medidas pertinentes para demostrar que no se realizaron modificaciones, alteraciones o destrucción sobre dicha información para que pase a ser definida como evidencia.

B. Fase de Adquisición:

Consiste en crear una imagen o clonado a bajo nivel de los datos originales del medio de almacenamiento, para lo cual se tomará de guía la RFC 3227 (Martínez, 2014), son directrices que contienen las mejores prácticas con relación a la recolección de información y su almacenamiento.

El primer paso será verificar el estado del equipo, si este se encuentra encendido o apagado, debido a que los procedimientos de recopilación serán diferentes para mantener la integridad de la evidencia original, como se detalla a continuación:

a) Equipo apagado

No prender el equipo, siempre debe estar apagado, ya que si se lo prende se puede alterar la evidencia. Por norma, no se debe trabajar con la evidencia original del soporte de almacenamiento de datos sino con una copia a bajo nivel llamada Imagen Forense; para realizar la copia se debe utilizar medios forenses estériles, empleando para ello herramientas de software especial que asegure que la evidencia no sea contaminada.

b) Equipo encendido

Es importante que la recopilación de la evidencia se realice siguiendo el orden de mayor a menor volatilidad de la información. El orden de volatilidad se enmarca al período de tiempo donde cierta información es accesible, es por eso por lo que se debe hacer la recopilación de la información que va a estar durante un tiempo menor, es decir cuya volatilidad sea mayor.

Una vez obtenida la Imagen Forense, es fundamental definir métodos adecuados para el almacenamiento y etiquetado de las evidencias. Este proceso es comúnmente llamado “Cadena de Custodia”.

C. 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[3], numeral 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.

D. Fase de Análisis:

Una vez que el proceso de almacenar la Imagen Forense fue documentado correctamente, comienza la fase de análisis, donde el Perito Informático utilizara todo su conocimiento con el objetivo de hallar huellas de la información que requiere encontrar.

El objetivo del análisis se enfoca principalmente en:

- Realizar la reconstrucción de la línea de tiempo, es decir, determinar la evolución de los hechos desde el instante anterior al inicio del ataque, hasta el momento de su descubrimiento.

- Llevar a cabo un examen detallado de los sistemas de archivos, detectar archivos sospechosos, realizar operaciones de búsqueda de caracteres, búsqueda de archivos específicos, recuperación de información y ejecutar otras tareas de investigación.

Esta fase exige mayores capacidades del Perito Informático, ya que por medio del análisis que se realice a la Evidencia Digital se llegará a responder las interrogantes de quién, cómo, cuándo, y donde sucedieron los hechos.

E. 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 informe pericial deberá ser redactado con lenguaje comprensible para el público no técnico explicando las razones por las cuales se ha llegado a tal conclusión.

El Perito Informático no puede emitir juicios de valor en su informe.

[3] Todos los artículos del COIP citados en esta investigación se encuentran en el Anexo E.

Consola Xbox One

Xbox One es la tercera videoconsola de sobremesa de la marca Xbox, producida por Microsoft. Forma parte de las videoconsolas de octava generación, fue presentada por Microsoft el 21 de mayo de 2013. Es la sucesora de la Xbox 360 y actualmente compite con PlayStation 4 de Sony y Wii U de Nintendo. Su salida a la venta fue el 22 de noviembre de 2013 a un precio de 499 dólares. La consola Xbox One se empezó a gestar tras la salida al mercado de su antecesora, la Xbox 360.

Figura 2. Recreación en modelo 3D de la Consola Xbox One
Fuente: Bryan Córdova

La intención de Microsoft desde el principio fue que la Xbox One fuera capaz de hacer más cosas aparte de hacer correr juegos. Desgraciadamente, la parte de aplicaciones acabaría interfiriendo tarde o temprano con la potencia dedicada a los juegos. Por esa razón, decidieron separar el sistema operativo en dos máquinas virtuales totalmente aisladas y en particiones de memoria distintas (una de 5GB para juegos y otra de 3GB para aplicaciones).

- **Sistema Xbox One**

El Sistema Xbox One (conocido también como Xbox OS) es el sistema operativo de la videoconsola de hogar de octava generación, Xbox One. Es un sistema operativo basado en Windows, aunque desde el lanzamiento de Windows 10. El sistema utiliza distintas máquinas virtuales integradas al sistema mediante Hyper-V y contiene sistemas distintos para los juegos y para las aplicaciones y se encuentra interno dentro del HDD para su uso día a día, aunque también se encuentra en el almacenamiento interno de NAND, para propósitos de recuperación y restablecimiento de fábrica. (Anthony, 2013)

1.3. ESTADO DEL ARTE

En la actualidad podemos afirmar que existen ciertos trabajos relacionados con el Análisis Forense aplicado a las consolas de videojuegos, los cuales han sido estudiados en diferentes países adaptados a su diferente realidad y tomando en cuenta las diferentes

experiencias sobre posibles delitos perpetrados, a continuación, se citan los estudios más relevantes acordes a esta investigación.

En el año 2011 se lleva a cabo una ponencia sobre el uso de consolas de videojuegos utilizadas en tribunales de los Estados Unidos, haciendo uso de estas para explicar o recrear la escena de un delito, tomando en cuenta que dicha recreación no podrá ser reproducida sino en un caso específico y que cada caso tendrá diferente enfoque con respecto a la reconstrucción de los hechos fue impartida por

Así mismo se puede revisar un estudio propuesto por los autores (Moore et al., 2014) en el cual presentan su versión de una metodología preliminar para el Análisis Forense de la información contenida en consolas Xbox One, aunque el enfoque de dicha ponencia se basa en el uso de un videojuego especifico como es Battlefield 4, evitando de esta manera ser aplicada fuera de las condiciones específicas de la consola junto con dicho título.

Por otra parte, existe una ponencia sobre la cual sus autores sugieren simplificar la enseñanza de prácticas forenses mediante el desarrollo de videojuegos, que permitan brindar una experiencia más inmersiva sobre los temas forenses y con el objetivo final que es brindar los conocimientos generales sobre el Análisis Forense Digital, propuesto por los autores (Yerby, Hollifield, Kwak, & Floyd, 2014).

Para poder aplicar una metodología de Análisis Forenses basada en normativa legal ecuatoriana partiremos de estudios realizados en nuestro país, por lo cual en el estudio propuesto por (Loarte & Grijalva, 2017) se encuentra una metodología aplicable al proyecto ya que cuenta con todos los parámetros que garantizan los resultados requeridos así como la normativa legal requerida para dar validez a la Evidencia Digital.

Aunque existan estudios y ponencias sobre el Análisis Forense, podemos evidenciar que no existe una metodología general aplicable a consolas de videojuegos Xbox One, lo que dificulta que en el país se cuente con el conocimiento necesario y tampoco herramientas para realizar esta clase de Análisis Forense.

1.4. ADOPCIÓN DE UNA PERSPECTIVA TEÓRICA

La elaboración de una metodología debe asegurar la comprensión de elementos que la sustentan, señalar cuales son las bases teórico-prácticas que sustentan la elaboración del marco metodológico y guiar de manera práctica y eficaz en la elaboración en este ámbito de un informe pericial sin omisión de datos relevantes que permitan judicializar la evidencia encontrada.

Para el desarrollo del proyecto de investigación, se decidió adaptar la metodología UNE 71506:2013. De acuerdo con (Loarte & Grijalva, 2017), esta abarca todas las fases del Análisis Forense y permite al investigador administrar de menor manera la Evidencia Digital obtenible, además, será complementada con la normativa legal vigente para evitar la desaprobación del informe final y no ser vulnerable a una desacreditación de este ante el tribunal.

Para finalizar se desarrollará una metodología que permita obtener Evidencia Digital de este tipo de equipos y sea aplicable para la mayoría de los casos en los que se tenga esta consola como método, medio o fin de un delito y socializar este método con el fin de tener una instancia de justicia que permita judicializar la evidencia obtenida. Dicho método será dirigido a organizaciones, profesionales y estudiantes que deseen involucrarse en el Análisis Forense.

1.5. MARCO CONCEPTUAL

- **Delito informático**

Se define como delito informático a la apropiación ilegal de la información haciendo uso de la tecnología ya sea como método, medio o fin con el objetivo de realizar manipulación fraudulenta de la información, robo de información, la destrucción de programas o datos y el acceso no autorizado a la información personal afectando principalmente a los usuarios pudiendo obtener beneficios económicos o causar importantes daños materiales o morales.

- **Análisis Forense**

Se define como, el estudio minucioso de un asunto, aplicado para todo tipo de asunto en el cual se intenta descifrar que ocurrió utilizando técnicas y procedimientos con la finalidad de reconstruir una línea temporal y de desarrollo de los hechos para llegar a una conclusión y exponer la verdad de lo ocurrido.

- **Perito Informático**

Es una persona capacitada y con manejo experto de varios temas en el ámbito de la informática, quien deberá ser capaz de emitir un resultado confiable en base a la investigación y la experiencia que posee aplicado en conjunto con técnicas y guías metodológicas con el objeto de optimizar y garantizar los resultados de su investigación. (JUDICATURA, 2014)

- **Consola de videojuegos**

Una consola de videojuegos es un equipo electrónico diseñado para suplir la necesidad de entretenimiento interactivo de sus usuarios. Posee una salida de video la cual puede ser enviada a un monitor, un televisor, etc. así como controles o demás periféricos, los cuales permiten al usuario disfrutar de una experiencia en la cual deberá interactuar con el equipo, más específicamente con su software sobre el cual se reproducirán los contenidos multimedia y demás pasatiempos.

1.6. Hipótesis

El desarrollo de una metodología para el Análisis Forense basada en técnicas y guías actuales, normativa legal vigente del Ecuador en consolas de videojuegos Xbox One, brindará

a los Peritos Informáticos el conocimiento necesario sobre cómo obtener la información de estos equipos para el posterior desarrollo de las pericias con el fin de judicializar la evidencia encontrada y presentarlas en procesos legales mediante un informe.

CAPÍTULO II

MÉTODO

2.1. TIPO DE ESTUDIO

Estudios exploratorios

Debido a que el resultado será la elaboración de una metodología para el Análisis Forense, se adoptará el tipo de estudio exploratorio, la información será procesada en un laboratorio forense de acuerdo con la metodología UNE 71506:2013 y se presentaran resultados de forma documental.

2.2. MODALIDAD DE INVESTIGACIÓN

Proyecto de desarrollo

El proyecto de investigación se desarrollará en base a una metodología de Análisis Forense existente. El objetivo es adaptar y documentar la metodología para su uso en consolas de videojuegos Xbox One y de esta manera garantizar la posibilidad de ejecutarla en posteriores análisis y extraer Evidencia Digital judicializable cuyo proceso de obtención será plasmado en un informe pericial.

Documental

Se ampliará y profundizará el conocimiento, debido a que las fases del Análisis Forense serán debidamente documentadas, además el producto del proyecto de investigación será la elaboración de un informe pericial, así como de la metodología que resulte para el Análisis Forense de consolas de videojuegos Xbox One.

2.3. MÉTODO

Método Hipotético-Deductivo

Se utilizará este método debido a que vamos a adaptar una metodología previamente probada y sobre la cual conocemos el marco de trabajo a aplicar. Luego de terminada la

investigación se podrá llegar a la conclusión sobre si es válida o no la adaptación de la metodología de acuerdo con lo descrito en la hipótesis de la investigación.

2.4. SELECCIÓN DE INSTRUMENTOS DE INVESTIGACIÓN

Análisis Documental

Esta investigación se realiza en base a diferentes fuentes bibliográficas tanto primarias como secundarias con base en otros estudios realizados, esta documentación se encuentra albergada en publicaciones, libros, páginas web, etc. referentes al proyecto de investigación.

Experimentación

Debido a que la investigación se basa en una metodología ya existente se utiliza el estudio experimental debido a que se evaluara el comportamiento de la aplicación de la metodología de Análisis Forense bajo las condiciones particulares de una consola Xbox One, debido a este particular, por lo general se usa un laboratorio para su aplicación.

Prueba Piloto

Se deberán realizar todas las pruebas necesarias para poder responder al objetivo principal de la investigación y ese es confirmar o negar la posibilidad de obtener evidencia judicializable mediante el análisis de la información en la consola.

2.5. VALIDEZ Y CONFIABILIDAD DE LOS INSTRUMENTOS

La validez se determina en base al juicio experto de un perito informático quien evaluará los resultados obtenidos y determina si la información presentada podrá ser utilizada como evidencia judicializable, ya que esta deberá contener ciertos requisitos para ser catalogada como tal.

Esta valoración se la realizará en base a los resultados de la prueba piloto, debido a que se desarrollará en base a la adaptación de una metodología para el análisis forense tradicional previamente comprobada, se deberá medir en base a la obtención de información resultante.

2.6. PROCESAMIENTO DE DATOS

Con el objetivo de procesar y generar resultados para evaluar el cumplimiento de los objetivos y la hipótesis planteada, se procederá a realizar una toma de datos obtenidos durante la investigación.

Uno de los primeros resultados es el de la fundamentación teórica, realizada en base a los síntomas mencionados en el diagnóstico del problema, así mismo otro de los resultados es la información del marco teórico de este documento. Para cerrar, tenemos los resultados obtenidos de publicaciones referentes a métodos de Análisis Forense en el Ecuador, que se pueden encontrar en la adopción de la perspectiva teórica.

CAPÍTULO III

RESULTADOS

3.1. LEVANTAMIENTO DE INFORMACIÓN

3.1.1. Introducción a la consola Xbox One

Xbox One es la tercera videoconsola de sobremesa de la marca Xbox, producida por Microsoft. Forma parte de la octava generación de consolas de videojuegos, fue presentada por Microsoft el 21 de mayo de 2013. Es la sucesora de la Xbox 360 y actualmente compite con PlayStation 4 de Sony y Wii U de Nintendo. Su salida a la venta fue el 22 de noviembre de 2013 a un precio de 499 dólares.

Las consolas tradicionales suelen confiar en una arquitectura ultra especializada en videojuegos. En otras palabras, el sistema operativo está específicamente diseñado para el hardware y ambos para jugar. Microsoft quería desde el principio que la Xbox One fuera capaz de hacer más cosas aparte de hacer correr juegos. Desgraciadamente, la parte de aplicaciones acabaría interfiriendo tarde o temprano con la potencia dedicada a los juegos. Por esa razón, decidieron separar el sistema operativo en dos máquinas virtuales totalmente aisladas y en particiones de memoria distintas (una de 5GB para juegos y otra de 3GB para aplicaciones).

3.1.2. Sistema operativo Xbox One

El Sistema Xbox One (conocido también como Xbox OS[4]) es el sistema operativo de la consola de videojuegos de octava generación, Xbox One. Es un sistema operativo basado en Windows, aunque desde el lanzamiento de Windows 10. El sistema utiliza distintas máquinas virtuales integradas al sistema mediante Hyper-V y contiene sistemas distintos para los juegos y para las aplicaciones y se encuentra interno dentro del HDD para su uso día a día, aunque también se encuentra en el almacenamiento interno de NAND, para propósitos de recuperación y restablecimiento de fábrica.

Se puede afirmar que el sistema Xbox One funciona con tres sistemas operativos diferentes, el primero denominado Xbox OS que es el encargado de la reproducción de videojuegos, la funcionalidad base de la consola, el siguiente sistema operativo es el core de Windows 10 utilizando la funcionalidad para ejecutar Apps, entre las cuales encontramos Apps de comunicación como son chat de texto, chat por voz y/o video (Skype) además de Apps desarrolladas por terceros como ejemplo tenemos Netflix, EA Access, etc., y el tercer sistema es el denominado como el Dashboard que mediante el uso de la tecnología de virtualización Hyper-V de Microsoft, sirve como puente entre los sistemas operativos mencionados

[4] SO Siglas de Sistema Operativo

anteriormente y los presenta mediante una interfaz de usuario fácil de utilizar y navegar a través de los distintos contenidos ofrecidos por la presente generación de consolas.

Estos tres sistemas operativos trabajan en conjunto y de manera simultánea, permitiendo que la capacidad SmartGlass de Microsoft funcione de manera que el usuario final tenga la capacidad de ver pantallas diferentes al mismo tiempo. Dicho de otra manera, estas características incluyen, pero no se limitan a jugar un videojuego mientras navegas con amigos y familiares, o ver una película y navegar por internet o descargar más juegos, todo al mismo tiempo. (Gravel & Hansen, 2015)

3.1.2.1.Versiones de Software

Desde su lanzamiento noviembre 22 del 2013, el sistema operativo de la Xbox One corría con bajo un core de Windows 8 pero a partir de la actualización del 12 de noviembre del 2015 la consola actualizo su firmware implementando el core de Windows 10 sobre el anterior, implementando nuevas características, sobre todo visuales, siendo la principal una nueva interfaz de usuario. Además de esta actualización visual, el sistema incorporo la capacidad de virtualizar los sistemas operativos encargados de ejecutar las aplicaciones y los videojuegos mediante Hyper-V, permitiendo un uso más optimizado de estas funciones que trabajan al mismo tiempo, permitiendo una experiencia más fluida y con características más sociales.

3.1.3. Sistema de archivos

Una parte primordial para el uso y compartición de información entre sistemas operativos es el sistema de archivos que operan, los cuales se encuentran constituidos por archivos, directorios y particiones, además existen opcionalmente, los archivos de enlace o conocidos comúnmente como los accesos directos de Windows.

Se puede definir al sistema de archivos como una estructura de datos dentro de una unidad lógica que permite al sistema operativo almacenar información de forma organizada e independiente de los procesos que la utilizan, esta información al ser independiente de los procesos se mantiene tras finalizarlos y puede ser utilizada por varios diferentes programas.

Un subsistema de archivos es el conjunto de módulos del sistema operativo que se encargan de la interacción entre el usuario y la información, de esta manera la interfaz con el usuario proporciona:

- Servicios de nombrado
    - Ubicación
    - Extensión
- Servicios de archivos

- Seguridad, protección y cifrado
- Compartición
- Acceso
- Soporte a distintos tipos de archivo

- Servicios de directorios
  - Organización de la información

3.1.3.1.Particionado

El sistema de archivos debe residir en una única unidad de disco, pero se pueden tener varios tipos de sistemas de archivos en un mismo equipo, o varios del mismo tipo, particionando el disco duro.

Particionar un disco duro es la manera de dividir el disco físico en varios discos lógicos, para delimitar los discos físicos, es necesario reservar una zona con la información de arranque llamada Master Booth Record (MBR), esta partición siempre ocupara el primer sector del disco, conteniendo la información de arranque y la tabla de particiones.

3.1.3.2.Tipos de sistemas de archivos

- **FAT. -** Por cada archivo, contiene una lista enlazada de los bloques que contienen la información, posee una tabla de asignación de archivos de ahí sus siglas del inglés File Assignation Table (FAT) la cual contiene una entrada por bloque de la partición, debido a la importancia de dicha tabla, se almacenan dos copias de esta, si no se actualiza frecuentemente la tabla FAT pueden aparecer datos inaccesibles ya que no están referenciados. Uno de los principales inconvenientes con este sistema de archivos es que al tener particiones muy grandes se desperdicia mucho espacio debido a que la tabla es demasiado grande y la fragmentación ya que los bloques de información se asignan sin ningún orden. Este sistema de archivos ya no es muy utilizado debido a que fue diseñado para sistemas con discos pequeños y equipos con poca memoria RAM.

- **FAT32. –** Es una evolución de FAT, más robusta y flexible, cuenta con algunas mejoras entre las cuales tenemos sistemas de archivos más grandes o nombres de archivos más largos, es el sistema utilizado por defecto en la mayoría de las memorias flash USB y tarjetas SD.

- **NTFS.** – El New Technology File System es el sistema de archivos preferido por Microsoft, desarrollado a partir del sistema HPFS de IBM usado en el sistema operativo OS/2 que también tiene ciertas influencias del sistema HFS de Apple. Su principal característica es que permite crear particiones de discos más grandes con el objetivo de utilizarlos en equipos de alto rendimiento y

servidores, al igual que el sistema FAT su principal inconveniente es que requiere una buena cantidad de espacio del disco duro por lo que no es recomendable su uso en discos con menor espacio de 400mb y entre sus mejores características encontramos que es un sistema transaccional, permite el cifrado de archivos y proporciona el control de acceso para archivos y directorios.

3.1.3.3.Sistema de archivos del Xbox One

Debido a que la consola Xbox One es también considerada como un computador de alto rendimiento por las características que presenta, además de brindar una gran capacidad de almacenamiento para los videojuegos, encontramos que el sistema de archivos utilizado para la funcionalidad de la consola es el NTFS.

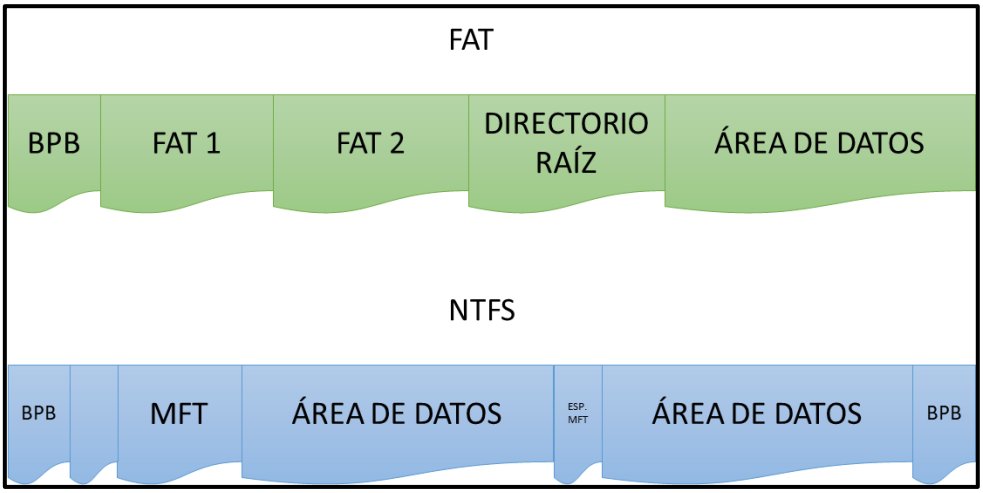


Figura 3. Alojamiento Sistemas de archivos FAT y NTFS
Fuente: Bryan Córdova

Se utiliza este sistema de archivos debido a que para su funcionamiento con los diferentes sistemas operativos de la consola el disco se encuentra particionado teniendo como resultado 5 particiones con capacidades que varían entre los 5gb y los 400gb, existen particiones para archivos temporales, para datos del usuario, recuperación del sistema operativo, actualización del firmware y la partición donde se almacenan los videojuegos.

3.1.4. Hardware de la consola

La consola Xbox One es una consola de videojuegos perteneciente a la octava generación de consolas presentada por primera vez en el año 2012 y lanzada al mercado un año más tarde. Desde su lanzamiento se ha actualizado el modelo de la consola en variantes como la Xbox One original, la Xbox One S y la Xbox One X.

Para este proyecto se utilizará la consola Xbox One original o Xbox One simplemente y se detallan sus características en la tabla 1.

Tabla 1. Características consola Xbox One

Componentes Xbox One	
CPU	CPU de 8 núcleos x86 fabricado por Microsoft
Procesador Grafico	Chip D3D 11.1 con 32 mb de memoria embebida
Memoria RAM	8GB DDR3
Memoria de almacenamiento	500 GB HDD
Unidad óptica	Combo Blu-Ray/DVD
Entrada y salida de información	USB 3.0
Comunicaciones	Ethernet, tres radiotransmisores 802.11n (Incluidos periféricos), Wi-Fi Direct
Audio y Video	Conexión HDMI de entrada y salida, 1080p.
Control	Nuevo mando Xbox One, opcional uso de teclado y mouse USB para comunicación y navegación por internet.
Cámara	Opcional, nuevo Kinect con sensor infrarrojo de 250,000 pixeles de profundidad y cámara 1080p.

Nota. Detalle de las características de la consola Xbox One original. **Elaborado por:** Bryan Córdova

A continuación, se presentan los componentes internos de la consola Xbox One tomado directamente de la experimentación al desmontar el equipo en la figura 4.

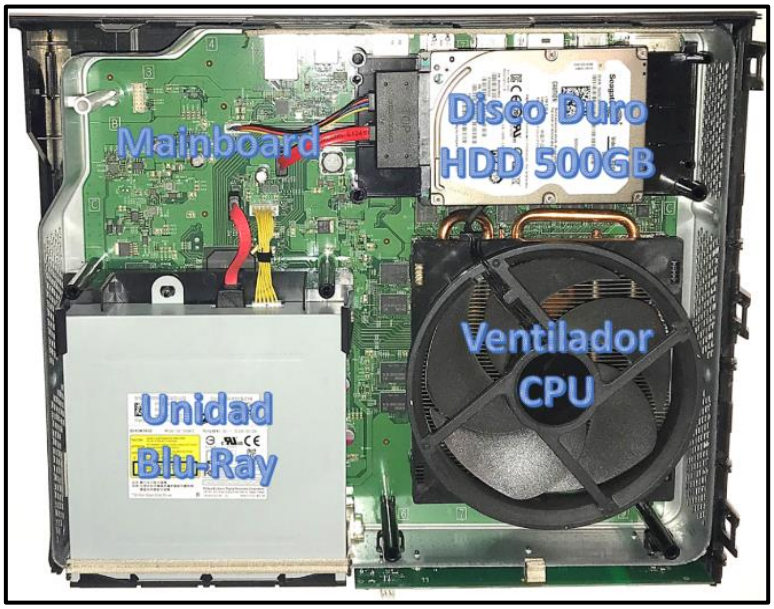


Figura 4. Distribución interna consola Xbox One
Fuente: Bryan Córdova

3.1.5. Normas, estándares y metodologías para el Análisis Forense

Para el Análisis Forense a nivel internacional ya se han desarrollado varias normas, estándares y guías de buenas prácticas para el manejo de Evidencia Digital con el objetivo de presentarlas en un proceso judicial mediante el análisis completamente científico.

Teniendo una metodología basada en normas, buenas prácticas y normativa legal, proporcionara a los investigadores de procedimientos, técnicas, bases y demás estrategias metodológicas para realizar un peritaje informático de manera adecuada, debido a que será esta metodología la que asegure la investigación desarrollada y pueda ser presentada como prueba relevante en un proceso judicial.

Durante el desarrollo de este capítulo se presentarán algunos estándares, metodologías y guías de buenas prácticas que servirán como referencia para el desarrollo de una metodología para el Análisis Forense de información digital en consolas de videojuegos Xbox One con el objeto de judicializar la Evidencia Digital y presentarla en procesos legales en el Ecuador.

3.1.6. Estándares, metodologías y guías de buenas prácticas existentes para el Análisis Forense

En la actualidad existen varias metodologías para el Análisis Forense propuestas por distintos autores y entidades, entre otras podremos encontrar las siguientes:

- Modelo según la Norma UNE 71506:2013, de AENOR1.
- ISO/IEC 27037
- RFC 3227
- Análisis preliminar forense del Xbox One (Preliminary forensic analysis of the Xbox one)
- Guía de buenas prácticas para evidencias basada en computadores (Good Practice Guide For Computer-Based Electronic Evidence)
- NIST

Las metodologías antes mencionadas tienen sus fases bien diferenciadas, por lo cual son válidas para cualquier Análisis Forense, sin embargo, se debe escoger entre una de ellas dependiendo de las necesidades, ya que algunas tienden a ser más específicas que otras y detallan más específicamente como tratar la evidencia.

3.1.6.1.UNE 71505:2013

Publicada por la AENOR[5], esta norma tiene por objetivo definir el proceso de Análisis Forense dentro del ciclo de gestión de las evidencias electrónicas, aplicable a cualquier organización con independencia de su actividad o tamaño.(AENOR, 2013)

De la misma manera dentro de esta norma, resalta la confiabilidad, es decir maximizar la veracidad de las evidencias electrónicas, fundamentando el cumplimiento de la siguiente manera:

A. **Autenticación e integridad. -** Garantizando que la información no ha sido modificada.

B. **Disponibilidad y completitud. -** La evidencia electrónica pueda ser localizada, recuperada, interpretada y presentada completamente.

C. **Cumplimiento y gestión. -** La evidencia electrónica se ha obtenido después de haberse gestionado y conforme a lo planificado previamente.

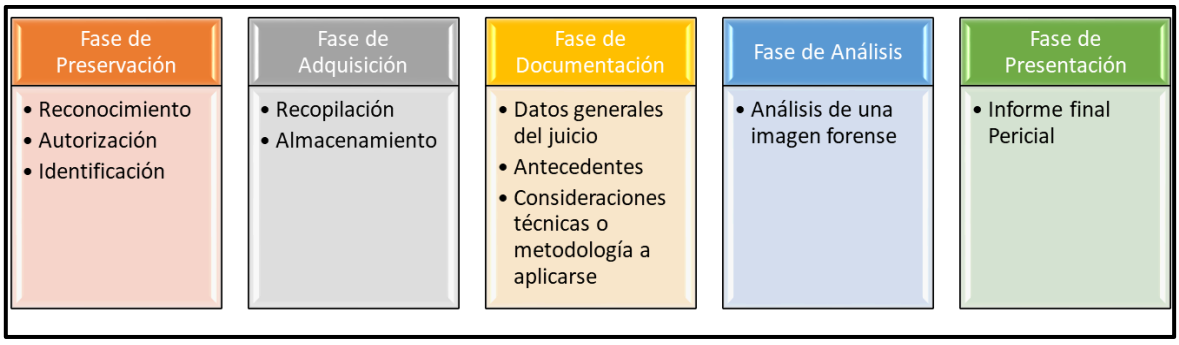


Figura 5. Fases del Análisis Forense según la norma UNE 71505:2013
Fuente: Bryan Córdova

3.1.6.2.ISO/IEC 27037

La norma ISO/IEC 27037 principalmente utilizada como la guía para la identificación, recolección, adquisición y preservación de la Evidencia Digital, teniendo en cuenta que no cuenta con el proceso de análisis de la evidencia.

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.)

El objetivo de la citada norma es siempre mantener la integridad de la evidencia y con una metodología aceptable contribuir a su admisibilidad en cualquier proceso legal.

[5] AENOR: Asociación Española de Normalización y Certificación.

3.1.6.3.RFC 3227

La RFC 3227 es un documento guía con pautas para la recolección y almacenamiento de la Evidencia Digital, publicado en el 2002 por Dominique Brezinski y Tom Killalea, documento cuya distribución es libre y gratuita.

En este documento se presentan una serie de pasos de alto nivel a seguir en actividades específicas para una correcta identificación y extracción de la Evidencia Digital en caso de existir un incidente de seguridad, precisando este último en el RFC-2828. (Shirey, 2007)

Es importante mencionar que es una guía que hace hincapié en el orden de volatilidad de los datos en un orden determinado, además que es totalmente flexible y la estructura que presenta esta guía toma temáticas de gran relevancia dentro de una investigación forense.

El esquema presentado dentro del RFC-3227 es la siguiente:

- Introducción
    - Convenciones utilizadas
- Guía de principios durante la recolección de la evidencia
    - Orden de volatilidad
    - Cosas que evitar
    - Consideraciones de privacidad
    - Consideraciones legales
- Procedimiento de recolección
    - Transparencia
    - Pasos para la recolección
- Procedimientos de almacenamiento
    - Cambio de custodio
    - Almacenamiento
- Herramientas

3.1.6.4.Análisis preliminar forense del Xbox One (Preliminary forensic analysis of the Xbox one)

Las consolas de videojuegos ya no se pueden ver como consolas de juegos, sino como máquinas multimedia completas, capaces de funcionar como un ordenador de escritorio. El

pasado ha demostrado que las consolas de juego se han utilizado en actividades delictivas como la extorsión, el robo de identidad y la pornografía infantil, pero con sus capacidades cada vez mayores, la probabilidad de la expansión de las actividades criminales realizadas en o sobre las consolas aumenta. Esta investigación tuvo como objetivo dar el primer paso para comprender la Xbox One, la más potente consola de Microsoft hasta la fecha. Informamos el resultado de la realización de un examen forense de la Xbox One, y proporcionamos nuestro conjunto de datos de Xbox One de imágenes de disco duro y archivos únicos para que la comunidad forense pueda ampliar nuestro trabajo. Se encontró que Xbox One había aumentado las medidas de seguridad sobre su predecesor (Xbox 360). El cifrado de los datos y los nuevos tipos de archivo introducidos dificultaban el discernimiento de la posible Evidencia Digital.

Si bien estas características adicionales de seguridad causaron gran dificultad en la adquisición forense de artefactos forenses digitales, se obtuvieron algunas pruebas digitales importantes e interesantes utilizando herramientas de código abierto. Hemos podido encontrar Evidencia Digital como las veces que el usuario inicialmente configuró la consola, y las veces en que el sistema fue restaurado o apagado. También pudimos determinar qué juegos y aplicaciones se habían descargado junto con cuando se jugaron los juegos. Finalmente, a través de nuestros experimentos forenses de red, pudimos determinar que varias aplicaciones tenían diferentes niveles de seguridad y que el tráfico del juego estaba cifrado. (Moore et al., 2014)

- **Metodología y herramientas**

Según (Moore et al., 2014), proponen que la metodología y las herramientas que fueron utilizadas siguieron las directrices para el examen forense de artefactos, según la metodología propuesta por el NIST.

Esta investigación se dividió en tres fases separadas:

- Fase I: Se restauró la consola Xbox One con los ajustes de fábrica. La unidad de disco duro se extrajo del equipo y se crearon imágenes forenses mientras se utilizaba un bloqueador de escritura de hardware. Se siguieron varios métodos de análisis del disco duro.

- Fase II: el disco duro se reinstaló en el sistema y se realizaron los eventos siguientes. Una vez que todos los eventos fueron completados, la imagen y el análisis se realizaron como en la Fase I:

    - Instalado Battlefield 4, jugado en modos multijugador y un solo jugador.

    - Instalado Dead Rising 3, jugado en modos multijugador y un solo jugador.

    - Instalado y utilizado varias aplicaciones, que consistía en: Skype, Twitch, YouTube, Xbox Video, Xbox Música y FXNow.

    - Una caja de cable se conectó a través de la Xbox One para permitir que la televisión se vea a través de la consola.

    - El usuario ha iniciado sesión utilizando la función de reconocimiento facial.

- El usuario ha iniciado sesión sin utilizar la función de reconocimiento facial.
- Visto los videos de juego de los amigos.

- Fase III: Ya que la Xbox One sin duda se utilizaría en un entorno en línea; algunos análisis de la interacción entre la Xbox One y la Internet era necesario. Los siguientes eventos controlados fueron utilizados para examinar esta comunicación:
  - Se utilizaron las aplicaciones de YouTube, Skype, Internet Explorer, Twitch y Game DVR.
  - Se jugó Battlefield 4 en modo un solo jugador y en la red de Xbox Live con otros usuarios.
  - Se jugó Dead Rising 3 en modo un solo jugador y en la red de Xbox Live con otros usuarios.
  - Registro dentro y fuera del perfil del usuario en la consola.

3.1.6.5.Guía de buenas prácticas para evidencias basada en computadores (Good Practice Guide For Computer-Based Electronic Evidence)

Esta guía fue desarrollada por la Asociación de Jefes de Policía del reino Unido (ACPO), publicando "Good Practice Guide For Computer-Based Electronic Evidence" (Haagman & Wilkinson, 2010)

La policía creó este documento con el objetivo de utilizarlo por sus miembros como una guía de buenas prácticas, basándose en computadores que puedan ser usados como evidencia.

El esquema que presenta dentro de esta norma es la siguiente:

A. Los principios de la evidencia basada en computadores.
B. Oficiales atendiendo a la escena.
C. Oficiales investigadores.
D. Personal para la recuperación de evidencia basada en computadores.
E. Testigos de consulta externos.
F. Anexos (legislación relevante)

3.1.6.6.NIST

El Instituto de Instituto Nacional de Estándares y Tecnología (NIST), en su publicación de agosto del 2006 "Guide to integrating forensic techniques into incident response" propone un modelo de fases para el proceso forense. Este modelo puede ser adaptado según a las

necesidades y en función a las políticas a seguir (Kent, Chevalier, Grance, & Dang, 2006), dividido en cuatro fases cronológicas:

A. **Recopilación:** identificación, etiquetado, registro y adquisición de datos de las posibles fuentes de datos relevantes, al tiempo que se siguen procedimientos que preservan la integridad de los datos.

B. **Examen:** el procesamiento forense de los datos recopilados mediante una combinación de métodos automáticos y manuales, y la evaluación y extracción de datos de interés particular, preservando al mismo tiempo la integridad de los datos.

C. **Análisis:** analizar los resultados del examen, utilizando métodos y técnicas legalmente justificables, para derivar información útil que aborde las preguntas que fueron el ímpetu para realizar la recolección y el examen.

D. **Informes:** informar los resultados del análisis, que puede incluir describir las acciones utilizadas, explicar cómo se seleccionaron las herramientas y procedimientos, determinar qué otras acciones deben realizarse (por ejemplo, examen forense de fuentes de datos adicionales, asegurar las vulnerabilidades identificadas, mejorar la seguridad existente controles) y proporcionar recomendaciones para mejorar.

3.1.7. Análisis previo a la sección de una metodología referencial

Para poder realizar un análisis de metodologías se deberán implementar parámetros para su medición, dichos parámetros se basan en la disponibilidad de documentos, aceptabilidad de normas y estándares relativos al Análisis Forense, adaptabilidad en la implementación experimental y cuente con las fases claramente detalladas.

Se evaluará utilizando los criterios del análisis forense que son preservación, adquisición, documentación, análisis y presentación repartidos en estas fases debido a que la metodología a desarrollar deberá cumplir con el mejor método de tratamiento de evidencia digital y de información relacionada con el caso de investigación.

Para esta medición se valorará con un criterio de estimación de 0 a 3, indicando que 0 no cumple con los criterios a perseguir y que 3 cumple con todos los parámetros y se ajusta a la normativa legal descrita en el Artículo 500 del COIP.

Tabla 2. Evaluación de metodologías de análisis forense

No	Metodología	Evaluación por fases del Análisis Forense					Resultados
		Preservación	Adquisición	Documentación	Análisis	Presentación	
1	UNE 71506:2013	3	3	3	3	3	15
2	ISO/IEC 27037	2	3	3	1	2	11
3	RFC 3227	1	2	2	2	1	8

No	Metodología	Evaluación por fases del Análisis Forense					Resultados
		Preservación	Adquisición	Documentación	Análisis	Presentación	
4	Análisis preliminar forense del Xbox One	0	2	1	1	0	4
5	Guía de buenas prácticas para evidencias basada en computadores	2	3	2	2	2	11
6	NIST	2	3	2	3	2	12

Nota. Para la evaluación de las metodologías, se calificó de acuerdo con cuantas subfases existían por cada fase del análisis forense, siendo el caso si existían 3 o más subfases la calificación máxima siempre seria de 3. **Elaborado por:** Bryan Córdova

3.1.8. Selección de la metodología para la investigación

Una vez que se ha realizado la evaluación respectiva, se llegó a la conclusión de que la metodología UNE71506:2013 es la más indicada para aplicar en este proyecto de investigación, además que será completada con el método de análisis de la consola Xbox One y contará con la actual normativa legal del Ecuador.

3.1.9. Tipos de Análisis Forenses

Según la teoría existen dos tipos de Análisis Forenses generales y dependen del estado en el que se encuentra el elemento de investigación, estos son el análisis en frio y caliente, como sus nombres lo indican el estado frio se debe a que el equipo se encuentra apagado tanto electrónica como eléctricamente, mientras que cuando el equipo o dispositivo se encuentra ya sea encendido o en reposo se lo denomina caliente.

3.1.9.1. Análisis Forense en caliente

Se conoce como análisis en caliente al tipo de análisis realizado cuando el equipo, dispositivo o elemento de investigación electrónico se encuentra encendido o en reposo al momento de realizar el levantamiento de pruebas por parte del elemento policial en la etapa de allanamiento.

Este procedimiento es generalmente realizado en computadores y teléfonos inteligentes debido a que se cuenta con software para dicho análisis y consiste generalmente en una revisión de información alojada en el equipo, dependiendo de la severidad del delito a investigar se puede obtener información sin necesidad de violentar contraseñas o sistemas de seguridad, para

lo cual existen varios métodos como por ejemplo el análisis de memoria volátil o memoria RAM.

Es importante que la recopilación de la evidencia se realice siguiendo el orden de mayor a menor volatilidad de la información. El orden de volatilidad se enmarca al período de tiempo donde cierta información es accesible, es por eso por lo que se debe hacer la recopilación de la información que va a estar durante un tiempo menor, es decir cuya volatilidad sea mayor.

3.1.9.2.Análisis Forense en frio

Se conoce como Análisis Forense en frio al tipo de análisis realizado cuando el equipo, dispositivo o el elemento de investigación se encuentra apagado al momento de realizar el levantamiento de pruebas por parte del elemento policial en la etapa de allanamiento.

Este procedimiento requiere de mayor experiencia en el campo forense ya que se debe seguir una serie de pasos para evitar la corrupción de la prueba original y evitar la manipulación de esta, a su vez se requiere de software especializado para tratar la prueba y extraer información relevante que pueda ser presentada como Evidencia Digital judicializable.

Previo a realizar el procedimiento de Análisis Forense en frio se debe asegurar la integridad de la prueba siguiendo pasos previos que debieron ser realizados por el personal de allanamiento y son el respetar y aplicar los procedimientos de la Cadena de Custodia ya que la prueba debe llegar tal cual fue encontrada en el sitio del delito.

No prender el equipo, siempre debe estar apagado, ya que si se lo prende se puede alterar la evidencia. Por norma, no se debe trabajar con la evidencia original del soporte de almacenamiento de datos sino con una copia a bajo nivel de este comúnmente llamado Imagen Forense; para realizar la copia se debe utilizar medios forenses estériles, empleando para ello herramientas de software especial que asegure que la evidencia no sea contaminada.

3.1.10. Herramientas para el Análisis Forense

Para todo Análisis Forense se debe contar con procedimientos, normas y guías, y para su desarrollo se deben contar con herramientas para el análisis, este es el caso del software que se utilizara para descubrir Evidencia Digital.

Durante el desarrollo de este capítulo se estudiarán ciertas herramientas y se evaluará su desempeño en cuanto al descubrimiento de información que posteriormente se podrá presentar como Evidencia Digital judicializable.

Entre las herramientas más comúnmente utilizadas encontramos las siguientes:

- **Forensic ToolKit FTK**

Este conjunto de herramientas permite obtener y analizar la información concentrando la información relevante en base a filtros de búsqueda más generales como son correos electrónicos, archivos eliminados, mensajes, entre otras. Está diseñada principalmente para el análisis de computadoras y dispositivos móviles todo basado en buenas prácticas forenses. (AccessData, 2018)

Es una herramienta potente que ha sido probada por varios investigadores forenses en el mundo y se ha podido verificar que procesa e indexa los datos por adelantado, eliminando de esta manera el tiempo invertido a la espera de la ejecución de búsquedas, no importan cuantas fuentes de datos diferentes tenga o la cantidad de datos que se tenga que extraer, es una de las soluciones más robustas del mercado.

- **Autopsy**

Es una herramienta fácil de usar, de interfaz netamente gráfica y que permite analizar eficientemente dispositivos de almacenamiento, así como teléfonos inteligentes se basa en una arquitectura de plugins y permite al usuario incluir más funcionalidades en formato de add-on desarrolladas en Java o Python. Es una herramienta utilizada mundialmente por investigadores forenses que incluso manejan una comunidad a través de correos electrónicos y foros en línea. (SleuthKit, 2003)

Sleuth Kit® es una colección de herramientas de línea de comandos y una biblioteca en C que le permite analizar imágenes de disco y recuperar archivos de ellas. Se usa detrás de escena en Autopsy y en muchas otras herramientas forenses de código abierto y comerciales, puede ser reconocido como la plataforma principal sobre la cual Autopsy ejecuta su conjunto de herramientas.

- **Kali Linux**

Kali es una plataforma de distribución Linux basada en Debian cuyo objetivo principal es la auditoria de seguridad informática en general, sin embargo, cuenta con una serie de herramientas preinstaladas las cuales pueden ser utilizadas para el Análisis Forense desde la obtención de la imagen forense hasta su análisis. (Offensive Security, 2018)

3.1.11. Estudio sobre el uso de herramientas forenses para el análisis de la información contenida en consolas Xbox One

Con el objeto de obtener Evidencia Digital de consolas Xbox One utilizando métodos o guías comúnmente utilizadas en el Análisis Forense de equipos de computación, se deberá realizar un estudio sobre y si es útil el uso de herramientas de Análisis Forense, para lo cual se obtendrá la Imagen Forense del disco de la consola y se realizará un análisis de la información contenida.

- **Extracción de Imagen Forense con el módulo FTK Imager**

Es el módulo del Forensic ToolKit diseñado específicamente para la extracción de la Imagen Forense de diferentes dispositivos o discos de almacenamiento incluidos discos duros, memorias USB, tarjetas SD entre otros.

Existen varias opciones para el formato de Imagen Forense y varían esencialmente por el tipo de compresión y el tamaño de división de las partes para su almacenamiento, también se puede crear una Imagen Forense en un solo archivo, pero esto va a demorar el análisis final de la imagen[6].

Para el estudio se valorará con porcentaje si la herramienta seleccionada cumple con los principales hitos para extracción de información que pueda ser presentada como Evidencia Digital.

Tabla 3. Evaluación de herramientas para el Análisis Forense

Nombre herramienta	Plataforma	Cantidad de archivos analizados	Información filtrada	Información de correos electrónicos	Información de mensajería instantánea	Total
Forensic ToolKit FTK	Windows	50000	558	0	0	1,12%
Autopsy	Windows	50000	56	36	0	0,18%
Kali Linux	Linux	50000	282	28	0	0,62%

Nota. Para esta evaluación se calificó de acuerdo con la cantidad de archivos fueron filtrados y desencriptados haciendo uso de las herramientas forenses descritas. **Elaborado por:** Bryan Córdova

Con base en el estudio de herramientas para el Análisis Forense, podemos encontrar que el uso de herramientas forenses para esta investigación queda descartado, por tal motivo se deberá adaptar la metodología utilizando el concepto base de preservación de la información, pero obteniendo de manera distinta la evidencia.

3.1.12. Elaboración de una metodología para el Análisis Forense de la información contenida de consolas de videojuegos en el Ecuador

Para realizar un Análisis Forense de equipos electrónicos distintos a computadores y teléfonos celulares inteligentes, podríamos seguir una secuencia de pasos basándonos en guías para el Análisis Forense de los equipos mencionados anteriormente. Pero para una correcta investigación forense se deberán seguir una serie de pasos detallados en un manual de procedimientos o una metodología cuyos antecedentes hayan sido probados y de esta manera evitar caer en inconvenientes y demorar o incluso sortear la obtención de la evidencia.

[6] El proceso de extracción de imagen forense se encuentra documentado en el Anexo No 5

Para el desarrollo de la presente metodología se implementarán los descubrimientos basados en los estudios realizados previamente y detallar todo el proceso desde la metodología para obtener el dispositivo de almacenamiento, así como el método para realizar el correcto análisis de la información contenida en la consola. Así mismo se plantea una estructura para la metodología a realizarse que seguirá el esquema demostrado en la figura 6, con el objeto de englobar todos los aspectos a considerar en un Análisis Forense.

Figura 6. Fases de la metodología propuesta
Fuente: Bryan Córdova

3.1.12.1. Fase de Requisitos

Para iniciar una investigación forense se deberán determinar los requisitos iniciales y el perfil que debe tener el investigador. Estos requisitos deben ser cumplidos para calificarse como Perito Informático y están reglamentados en el Artículo 18 de la Resolución 040-2014 del Consejo de la Judicatura. (JUDICATURA, 2014)

Para calificar como perito informático se deberá cumplir con el perfil especificado en el artículo No. 511 del COIP para poder realizar investigaciones forenses.

Luego que la autoridad competente haya designado a un perito calificado con la debida experiencia y conocimiento dentro de un proceso que requiera de investigación para esclarecer el fallo de un determinado delito informático, tomando en cuenta el tipo de delito cometido ya sea civil o penal y para lo cual se deberán seguir los siguientes procedimientos como se ilustra a continuación:

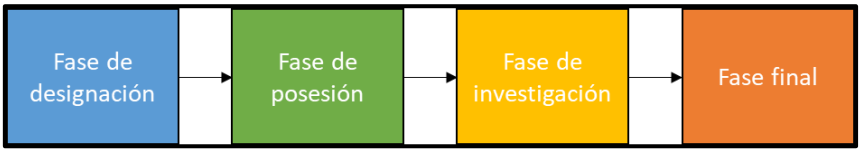


Figura 7. Fases para un Proceso Civil
Fuente: Bryan Córdova

En el proceso penal la fase de posesión se suprime debido a lo especificado en el artículo 12 de la resolución 067-2016 del Consejo de la Judicatura.

Figura 8. Fases para un Proceso Penal
Fuente: Bryan Córdova

- **Fase de designación**

La fase de designación se realiza por las y los jueces mediante el sistema SATJE el cual es un sistema donde se encuentran registrados todos los peritos acreditados por el Consejo de la Judicatura, ubicándolos en un catálogo de acuerdo con las Especialidades de estos. El proceso de selección del perito se lo realiza al azar con lo cual se garantiza una igual distribución o asignación de los Peritos que se encuentran registrados en la base de datos de acuerdo con lo especificado en el artículo No. 12 de la resolución 040-2014 del Consejo de la Judicatura.

En procesos civiles o no penales, las partes procesales podrán solicitar la designación de los peritos de forma directa, siempre y cuando el perito solicitado cumpla con los requisitos previamente descritos.

En cualquier caso, el perito designado recibirá una notificación vía correo electrónico, de su asignación a un caso y de la misma manera en la providencia se especifica el nombre del perito que ha sido asignado, mediante un sorteo e indica fecha y hora en la que el perito deberá posesionar el caso y tiempo para la presentación del informe pericial.

- **Fase de posesión**

Esta fase solo aplica en caso de ser un procedimiento civil y se deberá realizar la respectiva posesión del perito para que luego este pueda proceder a realizar su actividad, cabe destacar que será de entera y estricta responsabilidad del perito el acudir al departamento de evidencia de criminalística de la Policía Nacional debido a que existe un tiempo límite para la investigación.

- **Fase de investigación**

En esta fase el perito empleará todo su conocimiento al análisis a realizar y deberá de manera científica y comprobable encontrar y presentar información relacionada con el objeto del delito que se podrá catalogar como evidencia.

- **Fase Final**

Para poder presentar la información relevante hallada con relación al delito cometido, el perito deberá sustentar de manera oral los resultados de su investigación como una de sus obligaciones en procesos civiles y penales, siendo así presentándose al interrogatorio y contrainterrogatorio de los sujetos procesales.

La defensa oral tiene como objetivo ratificar, aclarar e incluso ampliar los resultados de la pericia ya que sin ellas los resultados del informa pericial carecerían de valor y no constaran como parte de la evidencia que deba ser valorada por el juez tal y como lo establece el Artículo 222 del COGEP[7] que dice: "La o el perito será notificado en su dirección electrónica con el señalamiento de día y hora para la audiencia de juicio, dentro de la cual sustentará su informe. Su comparecencia es obligatoria."(Asamblea Nacional, 2011)

La inasistencia injustificada del Perito a defender su informe será considerada como falta gravísima perdiendo su acreditación e incluso pudiendo ser llevado a la audiencia mediante el uso de la fuerza pública.

Previo a iniciar una investigación forense es menester del perito informático conozca toda la documentación necesaria que va a requerir en toda investigación, a continuación, se lista la documentación requerida:

Solicitud por escrito a una autoridad competente ya que ciertos casos se debe romper claves de seguridad, investigar sobre archivos personales en equipos informáticos o incluso para quebrantar los acuerdos de confidencialidad que tienen las empresas.

- **Formulario No. 1. -**contendrá información personal del Perito a cargo de la investigación, para corroborar que no se tenga ningún tipo de vínculo con las personas procesadas.

- **Formulario No. 2. -**contendrá información detallada acerca de la escena del delito.

- **Formulario No. 3. -** contendrá información referente a la recopilación de la evidencia original de los diferentes dispositivos de almacenamientos.

- **Formulario No. 4. -** contendrá información referente a los diferentes elementos físicos o contenido digital, principalmente los que formaran parte de la investigación y de la Cadena de Custodia para ser transportados al laboratorio forense.

Previo a comenzar con la fase de preservación el perito deberá llenar veraz y adecuadamente el Formulario No. 1.

[7] Código Orgánico General de Procesos

3.1.12.2. Fase de Preservación

La fase de preservación hace referencia al concepto del mismo nombre en la informática forense en el cual detalla que la prioridad es asegurar la integridad de la evidencia original en la escena del delito, es decir, no se debe realizar modificaciones, alteraciones o destrucción sobre dicha evidencia.

Previo al arribo a la escena del delito el perito deberá contar con información previa sobre los detalles de esta como el área, equipos, personal, sistemas, dispositivos, entre otros, con el objeto de estar preparado y acudir con herramientas tanto de hardware como de software que serán requeridas para la investigación. Cabe recalcar que el funcionario/a público que tome contacto inicial con la escena del incidente será el responsable de su preservación hasta contar con la presencia del personal especializado según se menciona en el artículo 178 del COIP.

Para asegurar los resultados en la fase de preservación se deberán seguir subprocesos enmarcados en la escena del delito como se ilustra en la fig.

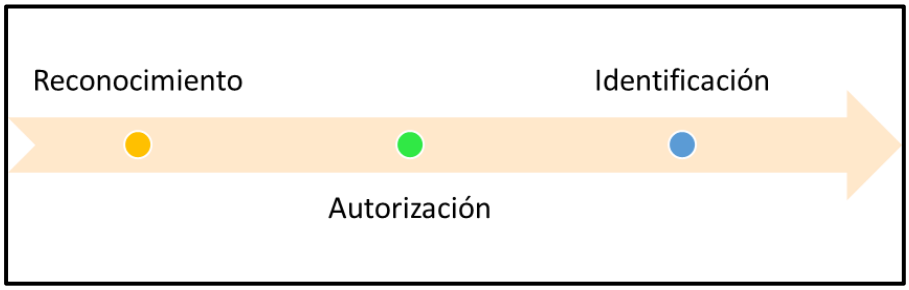


Figura 9. Sub fases de la fase de preservación
Fuente: Bryan Córdova

- **Reconocimiento**

El perito realizara el reconocimiento del lugar de los hechos tanto en territorio digital como en servicios digitales y medios o equipos tecnológicos preservando en todo momento la escena del delito evitando de esta manera que se realicen modificaciones o destrucciones de la Evidencia Digital existente, como lo establece el artículo 460 del COIP.

- **Autorización**

El perito deberá solicitar una autorización por escrito por parte de la autoridad competente o las partes procesales, debido a que en ciertos casos se deberá romper contraseñas, investigar sobre archivos personales o incluso quebrantar acuerdos de confidencialidad que se tienen con las empresas, todo esto previo a la realización de la pericia.

De no contar con dicha autorización el análisis no tendrá validez legal y se podría estar cometiendo un delito según lo mencionado en el artículo 178 del COIP sobre la violación a la intimidad, se menciona además que la alteración o destrucción de vestigios de evidencias materiales u otros elementos de prueba, serán sancionadas con pena privativa de libertad de uno a tres años.

- **Identificación**

Como dice su nombre, se procederá con la identificación según el tipo de evidencia, estableciendo entre otras cosas, el tipo de información que estará disponible y que formará parte de la evidencia a ser investigada. Existe un orden específico para que todo el personal especializado examine la escena del incidente y de esta manera garantizar una actuación optima y lograr siempre mejores resultados, el orden de actuación es el siguiente:

a) Perito fotográfico

b) Perito criminalista

c) Perito dactiloscópico

Una vez consumada la intervención de los expertos, debe proceder el perito informático, quien es el que determinará los procedimientos a realizar para identificar los elementos de estudio que requerirá para su caso.

Conocer con exactitud la clase de evidencia se requiere será de vital importancia para una investigación exitosa, sin embargo, uno de los errores comúnmente cometidos es levantar toda información e indicio que se encuentre en escena, debido cuestiones legales debe ser muy reservado en el ejercicio de sus funciones y en su investigación. Es por eso que en este punto se enumeran algunas consideraciones a tener en cuenta:

1) **Orden de allanamiento**

Existen incidentes en los cuales es necesario realizar una orden de allanamiento para lo cual los artículos 478, 480, 481 y 482 del COIP, determinan los parámetros, reglas y pautas que se deben tener en cuenta para el registro o incautación de los elementos a ser investigados.

2) **Verificar el estado de los equipos**

Es primordial verificar el estado del equipo, si este se encuentra encendido o apagado, debido a que los procedimientos de recopilación de información serán diferentes para mantener la integridad de la evidencia original. Por lo general es que si se encuentra el equipo apagado no encenderlo y caso contrario si se encuentra encendido no apagarlo.

Como recomendación si el equipo se encuentra encendido se debe realizar periódicamente movimientos del mouse, ya que algunos equipos cuentan con contraseñas a fin de evitar que el equipo se bloquee, permitiendo que el equipo se encuentre activo, así como programas ejecutados o archivos abiertos, en la fase de adquisición se detallara de manera clara el orden para la obtención de la información volátil.

3) **Etiquetado de dispositivos**

Es importante etiquetar con una numeración única cada uno de los dispositivos incautados de la misma manera acompañar con una fotografía, todos estos procedimientos los deberá realizar el personal de criminalística de la Policía Nacional pero el perito también debe estar capacitado en caso de observar algún comportamiento o acción indebida con la recolección de evidencia solicitada por el agente fiscal.

4) **Cambio de custodia**

Es importante documentar los procedimientos realizados en un cambio de custodia, los responsables que estarán a cargo, los dispositivos incautados, si existió o no algún escrito y la nueva ubicación donde serán transportados, el principal involucrado en el cambio de custodia es el custodio de la bodega de evidencias de la unidad de Criminalística de la Policía Judicial del Ecuador, debido a que es en este depósito a donde toda evidencia o indicio de evidencia recogido del lugar de los hechos, será almacenado.

5) **Manejo del lugar de los hechos**

El área debe ser aislada y acordonada, toda actividad debe ser claramente documentada. Se debe realizar una eficaz investigación en la búsqueda de elementos materia de prueba o evidencias físicas, por lo cual se deberá mirar todo meticulosamente. Establecer un perímetro de protección de los equipos afectados garantizará que la evidencia original no sea alterada por personas ajenas a esta.

6) **Fijación del lugar de los hechos**

Se debe realizar actividades que permitan la descripción detallada del lugar de los hechos y la localización de los elementos materia de prueba o evidencias utilizando técnicas establecidas que pueden ser fotografías, videos, imágenes, embalaje y rotulado entre otros. Todo lo mencionado puede ser aplicado según lo establece el Artículo 500, numeral cuatro del COIP.

Las actividades mencionadas se deben realizar con la utilización de guantes de látex, de esta manera estará en condiciones de tomar algún objeto con el fin de recabar algún dato relevante como el número de serie, conexiones de red, conexiones con los periféricos de entrada/salida, etc.

Es importante el uso de brazaletes antiestáticos con el fin de no alterar la evidencia producida por cargas electrostáticas en el momento de la manipulación de los equipos o dispositivos.

7) **Recreación de la escena del delito**

Una buena práctica es realizar dibujos o esquemas de conexiones, así como pequeñas descripciones de los dispositivos de almacenamiento, así como detallar el entorno del equipo ya que puede contener información que a futuro proporcionara más pistas sobre dónde buscar evidencias.

8) **Arquitectura de lo que se va a investigar**

Se deberán identificar el tipo de arquitectura de los equipos a investigar, sean estos servidores, router, switch, computadores personales, smartphones, consolas de videojuegos, entre otros, ya que de esto dependerá que procedimientos se seguirán para realizar la investigación.

9) **Componentes relacionados al incidente**

Los Peritos Informáticos evaluaran dos tipos de evidencia:

- Evidencia electrónica. - Todo elemento material de un sistema informático o hardware, este último refiriéndose a todos los componentes físicos que lo integra.

- Evidencia Digital. - Toda la información obtenida en un sistema informático como puede ser datos, programas almacenados y mensajes transmitidos para su posterior análisis y puedan ser presentadas como evidencias.

Siempre se deberá efectuar este tipo de análisis debido a que esta información influirá para que los procedimientos se realicen de manera adecuada para cada tipo de evidencia, con el fin de recabar la mayor cantidad de evidencia posible.

10) Identificar los posibles implicados

Se podrán realizar entrevistas a los implicados o a personas que tengan relación con el incidente, ya sean administradores o usuarios del o los sistemas, con el fin de recabar la mayor cantidad de información acerca de la investigación.

11) Fotografiar y rotular las evidencias

Siempre deberemos tener un registro fotográfico ya sea análogo (cámara réflex) lo cual es lo más aceptado, pero si es digital también será válido siempre y cuando aseguremos la validez de la imagen obteniendo el hash de los archivos de imagen. A esto también se puede acompañar con un registro de video y/o audio al cual se aplicarán las mismas condiciones que el registro fotográfico.

Siempre poner mayor énfasis en el estado del equipo, ya sea que este se encuentre encendido o apagado, así como los periféricos de entrada o de salida que se encuentren conectados, así como las conexiones físicas, esto servirá para demostrar el tipo de análisis realizado.

12) Reconocer el Sistema Operativo

Para poder utilizar la herramienta adecuada y el procedimiento sea lo más óptimo posible, deberemos siempre determinar el sistema de archivos ya que dependiendo del sistema operativo este varia.

13) Interrumpir las conexiones de red

Para desestimar un ataque remoto se deberán suspender las comunicaciones físicas del equipo, siendo desconectar el cable de red o de ser el caso encender el modo avión en el equipo y de esta manera cancelar las comunicaciones inalámbricas, además de esta manera garantizamos que no se altere la información original en el momento del allanamiento.

14) Corroborar con el diseño de la investigación

Verificar siempre si los procedimientos a utilizar son los correctos y si tienen concordancia justificada con la situación del incidente, ya que cada caso es diferente y requiere de un diferente acercamiento.

15) Documentar todas las acciones

En todo momento deberemos documentar toda acción y/o hallazgo que se haga sea o no relevante ya que muy posiblemente durante el continuo accionar de la investigación se puede encontrar información relevante que junto a los hallazgos anteriores vengan a materializar evidencia.

Esta documentación también podrá ser utilizada para desestimar información que no se requiera o no llegara a ser relevante, de esta manera se podrán determinar las acciones a seguir y es una buena práctica para no retrasar la fase de documentación, para esto se utilizara el Formulario No. 2.

3.1.12.3. Fase de adquisición

Ya identificados los equipos a ser investigados, se deberá realizar la extracción de la prueba original contenida de los dispositivos de almacenamiento, así como continuar con el proceso de almacenamiento y transporte sin olvidar el proceso de Cadena de Custodia.

Esta es la fase primordial de la investigación ya que en esta se determinarán los procedimientos a seguir y de esta manera seleccionar las herramientas forenses que permitirán asegurar que la evidencia sea legitima con respecto de la original, así como asegurar su integridad.

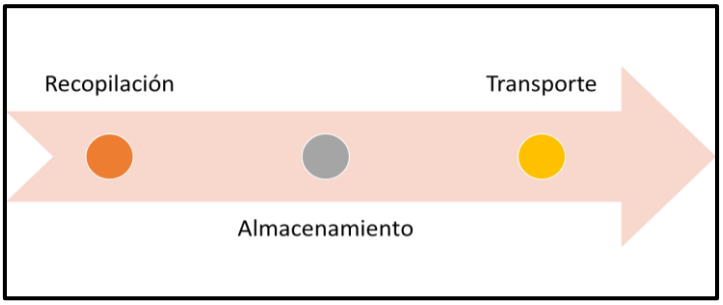


Figura 10. Sub-fases de la fase de adquisición
Fuente: Bryan Córdova

Recopilación

Se debe tener en cuenta que en esta sub-fase es que se puede contar con equipos que pueden ser trasladados al laboratorio forense y en otras ocasiones no.

Por eso es sumamente importante verificar el estado del equipo, si este se encuentra encendido o apagado, dependiendo de dicho estado los procedimientos de recopilación de información serán distintos con el objeto de conservar la integridad de la evidencia original.

Se deberá priorizar el orden de la volatilidad de la información contenida y por ende catalogar cal es la información más conveniente de obtener con respecto de las características del incidente, en cuyo caso se deberá seguir de acuerdo con los dos escenarios que son:

1) **Equipo apagado**

A continuación, se detalla una serie de procedimientos y técnicas para la obtención de la evidencia:

- No encender el equipo, la información que se encuentra en la consola deberá permanecer intacta para su posterior análisis en laboratorio.
- Desconectar todo cable y dispositivo de almacenamiento conectado a la consola, en el caso de encontrarse un dispositivo de almacenamiento conectado a la consola, proceder a etiquetarlo para procesarlo como posible fuente de evidencia.
- No se deberá trabajar con la evidencia original, se deberá proceder a clonar el dispositivo de almacenamiento masivo principal de la consola, haciendo uso de un software específico con el objeto de cumplir dicho objetivo. Para efectuar la clonación del disco se debe utilizar medios de almacenamiento estériles, evidenciando que la evidencia no sea contaminada.

2) **Equipo encendido**

A continuación, se detalla una serie de procedimientos y técnicas para la obtención de la evidencia:

- Antes que nada, no se deberá apagar el equipo, debido a que se podría perder información importante como es el caso de algún chat en vivo dentro de un videojuego especifico, información de conexiones remotas con la consola, aplicaciones en ejecución, etc. debido a que esto derivara en un proceso mucho más difícil para recopilar dicha información, con el riesgo de perderla.
- Es sumamente importante mencionar que la recopilación de evidencia se debe ejecutar en orden de mayor a menor volatilidad de la información. Dicho orden engloba la porción de tiempo donde la información es accesible, dando como resultado un análisis de la información que permanecerá el menor tiempo disponible, dicho de otra manera, información con mayor volatilidad.
- Debido a que no existe un método de análisis de memoria RAM[8] en consolas de videojuegos, se puede adaptar el orden de volatilidad de acuerdo con lo establecido en la RFC 3227, obteniendo un proceso como el siguiente:
    - Contenidos de logs y registros de la consola.
    - Estado de las diferentes conexiones de red.
    - Estado de los procesos encontrados en ejecución.

[8] Por el momento no se puede ejecutar un programa que permita el análisis de memoria RAM o todavía no ha sido desarrollada.

- Contenido del disco duro.
- Contenido de terceros dispositivos de almacenamiento.

- Documentar toda información que se encuentre en la consola en tiempo real, como:
  - Hora y fecha actualmente configurada del sistema.
  - Procesos que puedan estar en ejecución.
  - Todas las conexiones de red que se puedan tener.
  - Absolutamente todos los usuarios que pueden estar conectados localmente, así como de manera remota.
  - Aplicaciones abiertas.
  - Chats[9] iniciados.
  - Videojuego en ejecución[10].
  - Chats dentro del videojuego si fuere el caso.
- Una vez realizados los procedimientos anteriormente mencionados de forma correcta, se garantizará que la recolección de evidencia se la obtuvo de manera transparente y completa respetando el artículo 500, numerales 1 y 2 del COIP.

El perito informático deberá documentar detallando los procedimientos realizados y toda la información obtenida registrando sus hallazgos en el Formulario N.º 3.

Almacenamiento

Una vez que se haya terminado de recopilar la información requerida para la investigación, almacenándola cuidadosamente, se deben definir los métodos apropiados para el etiquetado y resguardo de la evidencia. Este proceso es conocido como “Cadena de Custodia”.

El perito deberá emplear el proceso de Cadena de Custodia para contenido digital, materia de prueba o elementos físicos, y de esta manera garantizando la legitimidad, estado original y acreditando su identidad, como dice el Artículo 456 del COIP. La demostración de autenticidad de los elementos probatorios y evidencia física no sometidos a la Cadena de Custodia, será llevada a cabo por parte de quienes las presenten, como lo indica el Artículo 457 del COIP.

[9] Chats por voz y/o texto.

[10] Se debe tomar en cuenta que la consola Xbox One solo permite un videojuego ejecutándose a la vez, pero si se pueden ejecutar aplicaciones a la par de los videojuegos.

Para poder dar inicio al proceso de Cadena de Custodia, siempre es preferible estar en presencia de la autoridad competente. Este proceso puede ser aplicado como se indica en el Artículo 482, numerales 2 y 3 del COIP.

La Cadena de Custodia deberá realizarse del siguiente modo:

1) **Fijación del lugar de los hechos**

Se deberá realizar una descripción detallada dl lugar donde sucedieron los hechos y la localización de evidencias o elementos de prueba, usando técnicas previamente indicadas, las cuales pueden ser videos, fotografías, dibujos, planos, etc. se puede aplicar la Cadena de Custodia, de acuerdo con lo que establece el Artículo 500, numeral 4 del COIP.

2) **Recolección de evidencia**

Luego de haber realizado el análisis respectivo sobre el estado del equipo y se haya aplicado las herramientas tanto de hardware como de software, y se ha obtenido la Imagen Forense, se deberá documentar las características de los equipos que serán transportados hacia el laboratorio forense para su respectivo análisis. Se puede aplicar la Cadena de Custodia, como lo indica el Artículo 500, numerales 2 y 3 del COIP.

3) **Embalaje y rotulado de la evidencia**

Se deberá realizar un registro fotográfico de los equipos y sus conexiones antes durante y después de su respectivo embalaje y se lo realizará en conjunto con el rotulado. Se deberán sellar todas las entradas y salidas del equipo frontales, posteriores y el puerto USB lateral. Así también se deberán sellar todos los tornillos, evitando de esta manera el reemplazo o retiro de piezas internas.

Para este proceso de sellado, se deberá emplear una cinta calificada previamente como adecuada para el proceso, que otorgue seguridad y una correcta preservación del equipo, de preferencia cinta de garantía[11]. Acompañar en cada sello con una rúbrica o firma y un indicador numérico de identificación y sobre cada una de estas adherir cinta transparente. De la misma manera se deberá rotular a todos los elementos que sean incautados y tengan relación con la evidencia.

4) **Documentación de la Cadena de Custodia**

Se deberá documentar a detalle todos los procedimientos realizados anteriormente junto con toda la información obtenida que será registrada en el Formulario N.º 4, garantizando la seguridad y preservación de los elementos que se almacene, procese o transmita contenido digital y de las evidencias obtenidas.

De esta manera se respeta lo que menciona el Artículo 457 del COIP sobre la valoración de la prueba, teniendo en cuenta su legalidad, autenticidad, sometimiento a Cadena de Custodia

[11] Cinta adhesiva que posea ya sea un logo a una advertencia y cada vez que es retirada deje un rastro que indique que ha sido violentado.

y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales.

Transporte

Se deberá transportar al laboratorio forense toda la evidencia encontrada y también todos los elementos que hayan sido incautados para lo cual todo este procedimiento deberá quedar registrado en el Formulario No. 4, se deberá hace uso de guantes antiestática con el fin de evitar alterar la evidencia electrónica producto de cargas electrostáticas al momento de la manipulación de dichos dispositivos o equipos, tal y como lo menciona el Artículo 500, numeral cuatro del COIP.

De acuerdo con lo mencionado en el Artículo 457 del COIP, durante el transporte de la evidencia se deberá mantener la Cadena de Custodia, tomando en cuenta las posibles alteraciones que pueda sufrir la evidencia durante dicho procedimiento. Toda vez realizada la documentación correcta de los procedimientos anteriormente descritos, se garantizará la integridad, preservación e inalterabilidad de la evidencia.

3.1.12.4. Fase de análisis

La fase fundamental de este tipo de investigación es la fase de análisis, tal y como su nombre lo indica, se deberá realizar un estudio detallado en donde el perito informático aplicará todo su conocimiento y técnicas conocidas para la recolección de la información con el objeto de determinar el dónde, como, quién y en qué periodo de tiempo sucedieron los hechos, todo esto utilizando la Evidencia Digital recolectada y si se cuenta con equipos incautados.

En esta fase se deberá obtener información relevante y bien estructurada con el propósito de documentar todos los hallazgos y desarrollar el informe pericial pertinente.

"Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuentas las diversas particularidades que nos podamos encontrar". (Rivas, 2014)

Debido a lo antes mencionado, se evidencian algunos procesos que se podrán adecuar en distintos casos y siempre tener en cuenta que el análisis se debe realizar exclusivamente en el Laboratorio Forense.

1) **Establecer un entorno de trabajo**

   - Cada caso es diferente, por dicho motivo se deberá adaptar el entorno de trabajo de acuerdo con las necesidades de los diferentes casos.

   - Se deberán retirar tanto el embalaje como los sellos de seguridad de la evidencia transportada al laboratorio forense, dicho proceso podrá ser realizado únicamente por el perito informático.

- Para garantizar la integridad de la evidencia, se deberá proteger fuertemente el material motivo del estudio, con el objeto de evitar que se encuentre expuesto a cambios de temperatura o campos electromagnéticos.

- Previamente el perito deberá definir las herramientas tanto de hardware como de software que le ayudaran a llevar a cabo la investigación y su posterior análisis.

- En el caso de poseer elementos digitales para el análisis, en ninguna circunstancia se podrá trabajar con la evidencia original, el procedimiento deberá ser llevado a cabo con una copia o respaldo de la original y de ser necesario se deberá utilizar una tercera copia, con el objeto de evitar utilizar la fuente original y exponerla a cualquier daño físico o lógico sobre ella.

2) Reconstrucción de la línea temporal

- Se deberá realizar un proceso de "ingeniería inversa[12]" para determinar y establecer la evolución de los hechos desde el momento anterior al inicio del incidente, hasta el momento en que se lo descubrió.

- Hay que registrar las fechas de modificación, cambio, borrado y acceso de archivos.

- También es de suma importancia registrar el huso horario del lugar del incidente, así como el del lugar de análisis.

- Evaluación y análisis de metadatos.

- Indagar en los logs del sistema, el cual brindara información relativa de aplicaciones instaladas, creación de usuarios, actualización del sistema operativo.

- Se podrá crear un bosquejo que permita visualizar la evolución de los hechos a partir de la información recolectada anteriormente.

3) Determinación del procedimiento utilizado por el atacante.

- Para determinar el procedimiento utilizado por el atacante se deberán analizar las fuentes principales por las cuales se podrían obtener información de la víctima.

- Se deberá realizar una exploración de información que tenga que ver con el caso como podrían ser fotografías, notas de voz, correos electrónicos, clips de video, etc.

[12] Proceso utilizado con el objeto de descubrir los antecedentes en la elaboración de un producto o sistema.

- Verificar el contenido de los canales de comunicación como chats de texto, logs de chats por voz, video llamadas, hasta chats dentro de algún videojuego especifico.

4) **Identificar a los autores de los hechos.**

- Se deberán revisar las cabeceras de los chats, así como la mensajería instantánea, ubicar la información de los contactos registrados, registro de conexiones remotas.

- Se pueden revisar también los historiales de navegación web, de ser posible revisar las cookies utilizadas, esto podría ser de gran ayuda para obtener más información e identificación del autor de los hechos que se están investigando.

5) **Aplicar la pericia específicamente a lo que esté autorizado.**

- Cuando el Perito Informático no realiza una adecuada investigación forense, se pueden aplicar penas severas, debido a que dependiendo del caso el perito tendrá acceso limitado a la información, debido a que en contados casos se cuenta con los permisos por parte del dueño de la información y de los procesos de seguridad utilizados para protegerla, el violar dichos procesos podría conllevar la perpetración de un delito si no se cuenta con dichos permisos, ya que en muchos casos los abogados presentan argumentos como por ejemplo: ¿Quién le dio la autorización para indagar en la información personal de mi cliente?, esto con el fin de anular los informes periciales. Esto podría llevar a una pena privativa de libertad por violación a la intimidad como lo establece el COIP en su Artículo 178.

6) **Documentación del/los proceso/s realizado/s.**

- Siempre se deberá documentar todo procedimiento por más pequeño y regular que este sea, con el objetivo de que los resultados obtenidos sean verificables y reproducibles en cualquier circunstancia por otro investigador forense, con la finalidad de reconstruir el proceso realizado durante la investigación y análisis dado el caso que se presente el recurso de revisión como lo detalla el Artículo 658 numeral 3 del COIP.

3.1.12.5. Fase de documentación

Para esta fase el perito informático deberá contar con la información mínima requerida para redactar el Informe Pericial, siendo de esta manera que las actividades realizadas a partir de la Fase de Requisitos hasta la Fase de Análisis queden plasmadas y claramente redactadas en el documento que deberá ser presentado dentro del plazo antes establecido, como lo menciona el Artículo 511 numeral 5 del COIP. Para efecto de lo anterior el informe deberá ser presentado y cargado al Sistema Informático Pericial en formato PDF, el mismo que podrá ser descargado y revisado por las partes e interesados. Si la hubiere, las aclaraciones o explicaciones podrán ser presentadas de manera verbal o escrita, de acuerdo a la normativa

procesal correspondiente, como se indica en el Artículo 19 y 20 de la resolución 040-2014 del consejo de la Judicatura.

El Informe Pericial tiene como objetivo el resolver y exponer el conocimiento experto del Perito Informático al proceso judicial. Este informe determinara el resultado del proceso legal para el cual fue requerida su elaboración y se justificara debido a la claridad con la que se presenten los resultados, evitando en mayor parte los tecnicismos en la redacción, siempre y cuando sea firme con los hechos y resultados obtenidos. Para ello se ha establecido un formato general y estandarizado de uso absolutamente obligatorio como lo indica los artículos 19 y 20 de la resolución 040-2014, siendo bastante claro y generalmente entendible para las autoridades competentes.

Este formato puede ser descargado desde la página web de la función judicial en la sección de Peritos, a continuación, se exponen los requisitos que son obligatorios en todo informe pericial:

- Datos generales del juicio, o proceso de indagación previa
- Parte de antecedentes
- Parte de consideraciones técnicas o metodología a aplicarse
- Parte de conclusiones
- Documentos de respaldo, anexos, o explicación de criterio técnico
- Otros Requisitos
- Información adicional
- Declaración juramentada
- Firma y rubrica

3.1.12.6. Fase de presentación

Esta es la fase final de la metodología propuesta, una vez terminado el informe pericial resultante del procedimiento llevado en todas las Fases anteriormente expuestas y luego de haber sido remitido al solicitante de la pericia. El perito deberá sustentar los resultados de su investigación uy análisis de manera oral, siendo esta una de sus principales obligaciones tanto en procesos Penales como Civiles, como lo establece el Artículo 505 del COIP, respondiendo al interrogatorio uy contrainterrogatorio de los sujetos procesales.

En esta defensa el perito deberá aclarar, ratificar e incluso ampliar la pericia realizada, debido a que sin dicha defensa las conclusiones del procedimiento pericial perderán su valor y no podrán ser utilizadas como prueba para que sea valorada por el juez, como se encuentra establecido en el Artículo 222 del COGEP.

Durante la defensa oral, el perito deberá tener la capacidad profesional y técnica para defender su informe, sin desviarse de la especialidad y del objeto para el cual fue nombrado perito, impidiendo caer en contradicciones, falsedades o juicios de valor. Siempre se deberá tener presenta que la inasistencia injustificada a defender el informe por parte del perito se considerará como falta muy grave, de esta manera perderá su acreditación como perito y debiendo ser obligado a presentarse en la audiencia por parte de la fuerza pública.

De ser requerido el perito deberá declarar las veces que lo ordene el/la juez/a en la audiencia de un juicio, como se establece en el Artículo 503 numeral 3 del COIP. Para dicho procedimiento se exponen algunas habilidades y destrezas que todo perito debería tener presentes durante la exposición ante la audiencia, como son:

- Vestimenta adecuada del contexto del caso, lo cual transmitirá el respeto hacia los sujetos procesales, así como el profesionalismo del expositor.

- Siempre mantener el respeto y la cordialidad hacia el otro profesional quien puede encontrar discrepancias en el informe pericial, esta será una señal de madurez psicológica y solvencia profesional.

- Expresarse de manera clara y comprensible durante el interrogatorio y contrainterrogatorio, siempre manteniendo la clama y expresando coherencia entre lo documento en el informe y lo expresado de manera verbal.

- Tener en cuenta que cada vez que se utilice la palabra “Objeción”, el juez será quien deberá indicar si da a lugar o lo niega para la posterior respuesta del perito.

- El interrogatorio directo es el que realiza la parte que introdujo al perito al proceso. Por lo cual el perito deberá acreditar su experiencia y exponer los fundamentos de los resultados de su pericia.

- Realizar preguntas y presentar pruebas no notificadas oportunamente orientadas a determinar su parcialidad y no idoneidad, a desvirtuar el rigor técnico de cada una de sus conclusiones, así como también impugnar su credibilidad, como lo establece el Artículo 511, numeral seis y siete del COIP.

- El Perito podrá estar en la capacidad de responder a cada una de las preguntas del interrogatorio de las partes, valiéndose con ilustraciones gráficas, como lo indica el Artículo 511, numeral seis y siete del COIP.

- De existir informes periciales divergentes, el juez tendrá la potestad de establecer en ese momento un debate entre los peritos, para posterior a ello iniciar un interrogatorio y contrainterrogatorio, con el objetivo de aclarar aquellos puntos de controversia, como lo indica el Artículo 222 del COGEP.

Se deberán devolver todos los elementos que fueron incautados para la realización de la investigación, finalizando de esta manera el caso asignado al Perito Informático.

3.2. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

Se demostrará el uso práctico de la metodología para el Análisis Forense previamente desarrollada en base a las características físicas de la consola Xbox One antes expuestas, se detalla una serie de pasos justificados de acuerdo con los estudios previamente realizados sobre metodologías, herramientas y tipo de información manejada en la consola.

El Artículo 161 del COIP señala que "La persona que prive de la libertad, retenga, oculte, arrebate o traslade a lugar distinto a una o más personas, en contra de su voluntad, será sancionada con pena privativa de libertad de cinco a siete años."

En Quito – Ecuador 2018 la Fiscalía provincial de Pichincha procede a realizar el allanamiento del lugar de los hechos, el domicilio donde reside la víctima, para lo cual la fiscalía solicita la presencia de personal capacitado de criminalística, así como la presencia de peritos calificados en el Consejo de la Judicatura.

Durante el proceso de levantamiento de la escena del crimen el Perito Informático realiza el triage[13] con respecto a los equipos electrónicos que se encuentren en la escena con el objeto de solicitar el levantamiento de estos, los cuales dispongan de unidad de almacenamiento, sobre los cuales se podría obtener Evidencia Digital que ayude a esclarecer los hechos sucedidos.

El perito procede a indicar que equipos requerirá para el análisis, entre los cuales se encuentran una computadora de escritorio, una laptop[14], una unidad externa de almacenamiento masivo[15] y una consola de videojuegos Xbox One primer modelo.

Una vez ordenado el levantamiento de los equipos antes mencionados el personal de Criminalística procederá a realizar el reconocimiento del estado de dichos equipos (verificar si se encuentran encendidos o no) y posterior a aquello procederán con el proceso de aseguramiento de evidencia y posterior Cadena de Custodia. El perito deberá proceder a retirar los elementos de investigación en el edificio de criminalística de la Policía Nacional, para lo cual este deberá poseer una orden del fiscal autorizando la salida de dichos equipos para realizar el Análisis Forense.

Cuando el Perito Informático haya obtenido todos los elementos de prueba solicitados con anterioridad al departamento de criminalística de la Policía Nacional, el perito procederá a realizar el Análisis Forense de los mismos en su laboratorio.

Luego de haber realizado el análisis de los equipos de computación, así como de la unidad externa de almacenamiento utilizando los métodos tradicionales de análisis junto con la normativa legal correspondiente, el perito se dispone a realizar el análisis de la información

[13] Es un protocolo o método de selección y clasificación de sujetos o elementos con el fin de evaluar la prioridad sobre lo que se requiere levantar teniendo en cuenta el tipo de elemento y su estado.

[14] Computadora personal portátil.

[15] Disco duro portátil de conexión USB

contenida en la consola Xbox One haciendo uso de la guía metodológica propuesta en esta investigación.

3.2.1. Extracción y clonación del dispositivo de almacenamiento principal de la consola Xbox One

Se deberá desmontar la consola con el objeto de obtener acceso al disco duro para luego realizar el proceso de adquisición de la Imagen de disco, este proceso deberá ser realizado utilizando los estándares de obtención de evidencia antes mencionados tanto en las fases de Preservación como de Adquisición y para lo cual se ha detallado el siguiente proceso para el desmonte y posterior obtención de la imagen sobre la cual se realizará el análisis de la información contenida.

3.2.1.1. Herramientas de hardware y software necesarios:

a) Palanca plástica gruesa y fina, generalmente se encuentran en los kits de reparación de teléfonos móviles

Figura 11. Juego de palancas plásticas para desmontaje de equipos electrónicos
Fuente: Bryan Córdova

b) Set de desarmadores Torx se utilizarán los de numeración: T9 y T10

Figura 12. Juego de desarmadores que incluyen juego Torx
Fuente: Bryan Córdova

c) Pinza para cejas

Figura 13. Pinza para cejas tipo tijera
Fuente: Bryan Córdova

d) Enclosure USB disco 2.5”

Figura 14. Enclosure para disco USB 3.0 duro de 2.5 pulgadas
Fuente: Bryan Córdova

e) Disco externo USB de al menos 1Tb (Terabyte)[16] de memoria o superior, es más recomendable siempre utilizar un medio de almacenamiento que sobrepase la capacidad del dispositivo de almacenamiento original

Figura 15. Disco duro externo USB 3.0 de 1 TB con número de serie
Fuente: Bryan Córdova

f) Disco duro 2.5” con igual capacidad al que se encuentre instalado en la consola

Figura 16. Disco duro de 500gb marca Samsung
Fuente: Bryan Córdova

[16] Dependiendo de la capacidad del disco de la consola, esta puede variar y superar los 500gb.

g) Software de clonación de discos duros, se utilizará EaseUS todo Backup[17]

Figura 17. Software para clonación de unidades de almacenamiento
Fuente: Bryan Córdova

h) Fuente de poder Xbox One

Figura 18. Fuente de poder Xbox One original
Fuente: Bryan Córdova

i) Cable Hdmi

Figura 19. Cable HDMI genérico
Fuente: Bryan Córdova

[17] El software de clonación puede variar.

j) Consola de origen[18]

Figura 20. Consola Xbox One del caso original
Fuente: Bryan Córdova

3.2.1.2.Desmontaje de la consola

a) Previo a iniciar el desmontaje, el investigador deberá colocarse los guantes[19] con la finalidad de evitar cualquier caso de contaminación de la evidencia original ya sea de huellas dactilares como elementos o reacciones químicas, así como la manilla antiestática cuya finalidad será evitar dañar los dispositivos de la evidencia original mediante una descarga de energía estática

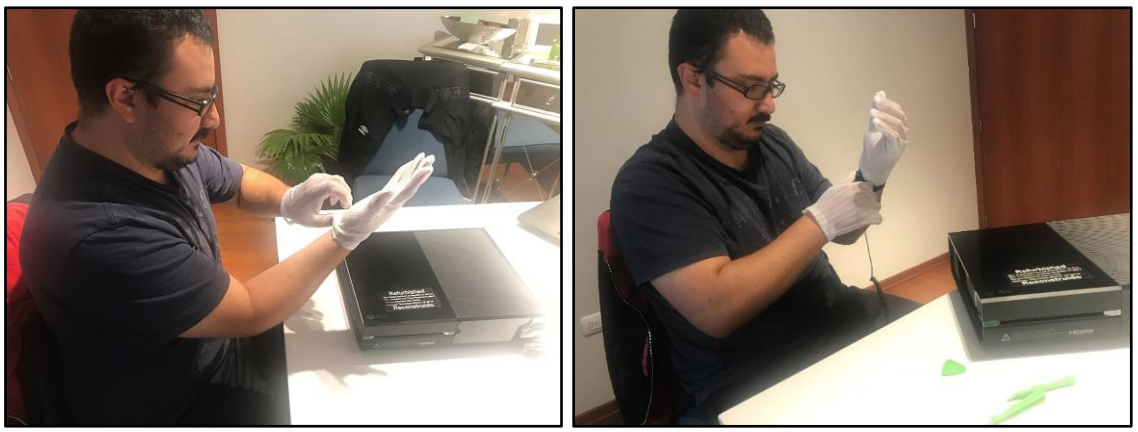


Figura 21. Colocación de los guantes y manilla antiestática
Fuente: Bryan Córdova

[18] Se requiere de la consola original, debido a que esta posee el software instalado correspondiente, cualquier variación podría causar el mal funcionamiento de la consola, alterando la integridad de la información contenida y por subsiguiente impidiendo el análisis de esta.

[19] El investigador forense siempre debe contar con guantes ya sean quirúrgicos o antiestática, así como la manilla antiestática para toda investigación forense que realice.

b) Se deberá retirar el sticker de garantía de Microsoft Xbox One ubicado en la parte posterior de la consola

Figura 22. Sticker de garantía de consola Xbox One original
Fuente: Bryan Córdova

c) Se procede a retirar la cubierta lateral separándola desde el conector USB en el costado izquierdo de la consola justo debajo del botón de sincronización de controles

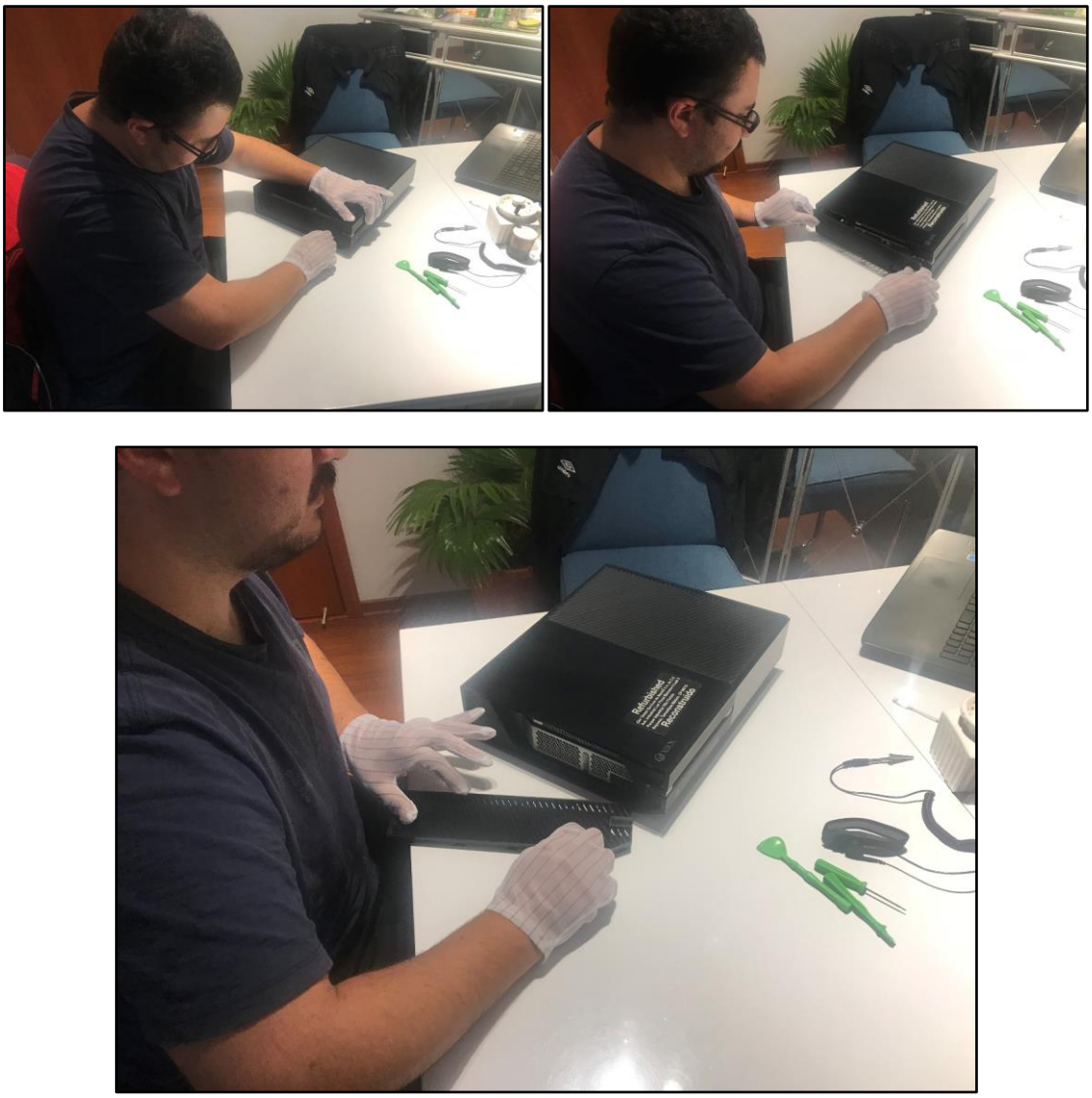


Figura 23. Proceso de retiro de cubierta lateral izquierda
Fuente: Bryan Córdova

d) Retiramos el seguro plástico que une las cubiertas superior e inferior

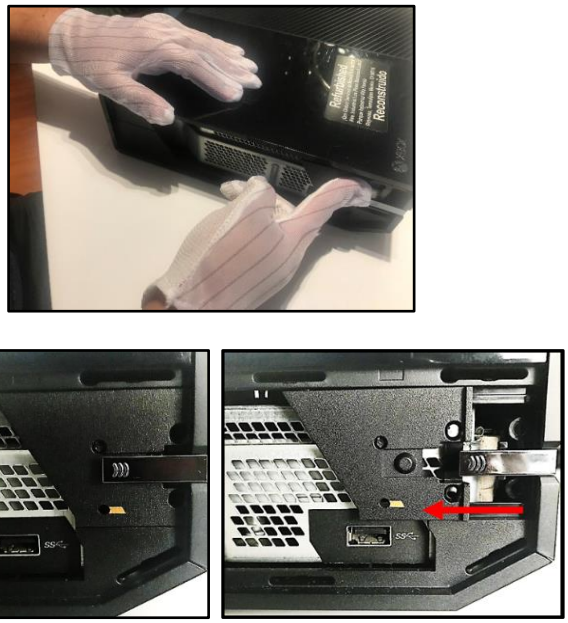


Figura 24. Retiro seguro plástico lateral izquierdo
Fuente: Bryan Córdova

e) Procedemos a separar los seguros plásticos de la cubierta superior alrededor de toda la consola con la ayuda de la palanca plástica gruesa

Figura 25. Proceso de retiro de cubierta superior
Fuente: Bryan Córdova

f) Luego se deberá retirar la cubierta, evitando romper el bus de datos que se encuentra en la parte posterior del panel frontal[20]

Figura 26. Proceso de retiro de panel frontal de la consola
Fuente: Bryan Córdova

g) Para retirar el bus frontal utilizaremos la pinza para cejas

Figura 27. Retiro de bus de datos del panel frontal
Fuente: Bryan Córdova

[20] El panel frontal de la consola cuenta con un bus de datos que controla las funciones táctiles del botón de encendido y el botón de expulsión de la unidad Blu-Ray de la consola.

h) Una vez retirado el bus de datos, retiramos la cubierta superior y frontal exponiendo la cubierta metálica interior de la consola

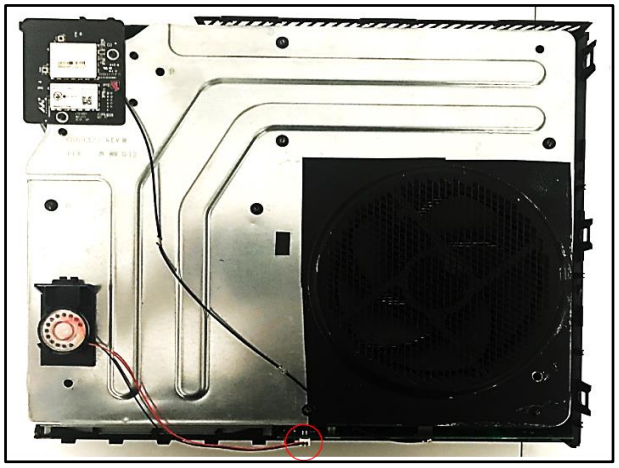


Figura 28. Ubicación del parlante del panel frontal
Fuente: Bryan Córdova

i) Para tener acceso al disco duro, todavía se deberá retirar la cubierta superior metálica, para lo cual se desconecta tanto el conector del parlante incorporado de la consola como el cable y la tarjeta Wifi

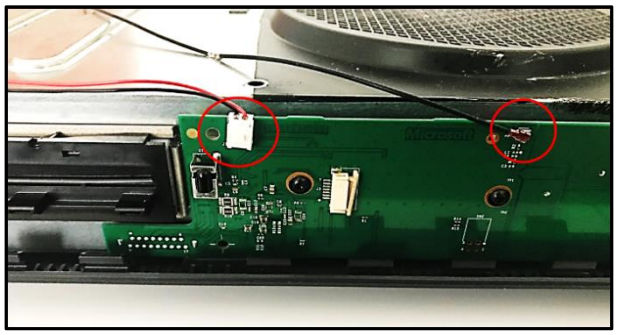


Figura 29. Ubicación de los conectores del parlante y el conector de la tarjeta WiFi
Fuente: Bryan Córdova

j) Se procede a retirar la tarjeta wifi con el uso del destornillador Torx, tomar en cuenta que la tarjeta está conectada con un bus de datos por lo que se deberá retirarla de manera vertical

Figura 30. Retiro de la tarjeta WiFi
Fuente: Bryan Córdova

k) Procedemos a retirar los tornillos Torx los cuales se encuentran sobre la placa metálica y cuentan con su propia nomenclatura "C"[21] Ej.: C3, C4, etc.

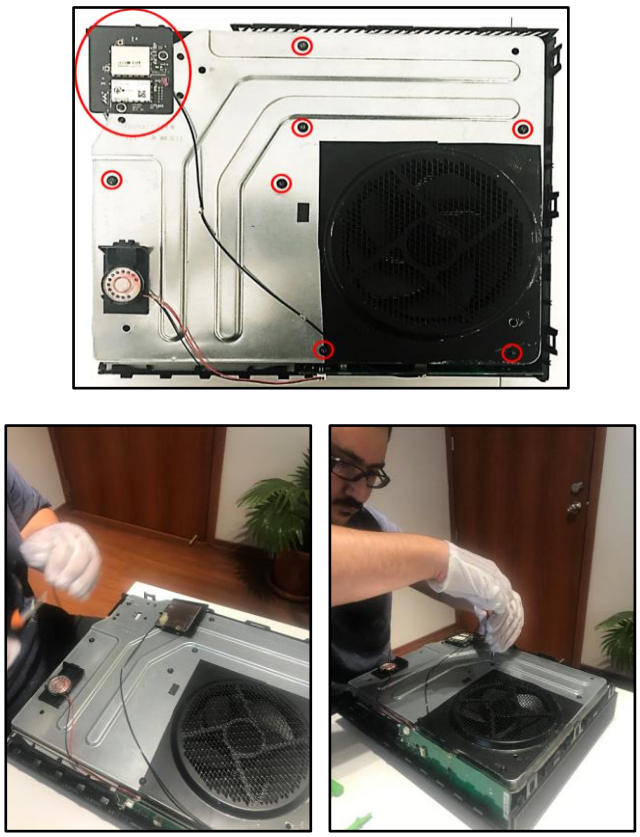


Figura 31. Ubicación y desmontaje de tornillos principales de la placa metálica
Fuente: Bryan Córdova

l) Se procede a semi levantar la tapa metálica para luego a desconectar el bus de datos de la tarjeta Wifi como se muestra en las figuras

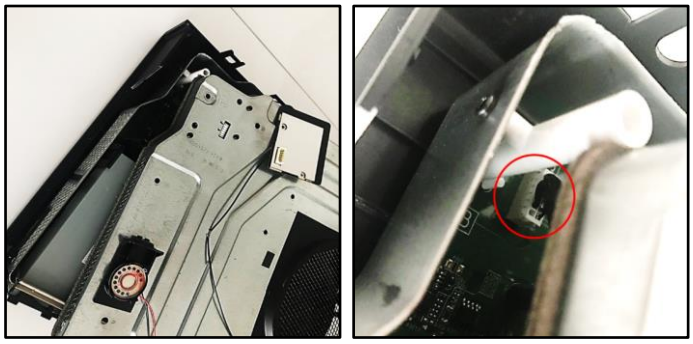


Figura 32. Desconexión bus de datos de tarjeta WiFi
Fuente: Bryan Córdova

[21] Tomar en cuenta debajo de la placa de wifi se encuentra un tornillo con nomenclatura "C" ubicado bajo la placa Wifi como se muestra en la figura anterior.

m) Una vez retirada la cubierta metálica ya se tiene acceso a la unidad de almacenamiento, para poder retirar el disco duro se deberá desconectar la alimentación eléctrica, así como el cable de datos SATA[22]

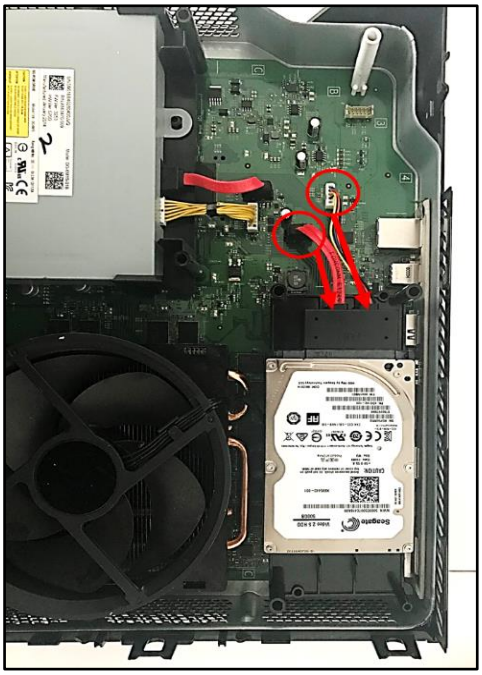


Figura 33. Ubicación de los conectores principales del disco duro de la consola
Fuente: Bryan Córdova

n) Para desmontar la base del disco duro se deberán remover los tornillos Torx que se encuentran hacia los bordes de la plataforma y no los que se encuentran por debajo que poseen una superficie más grande

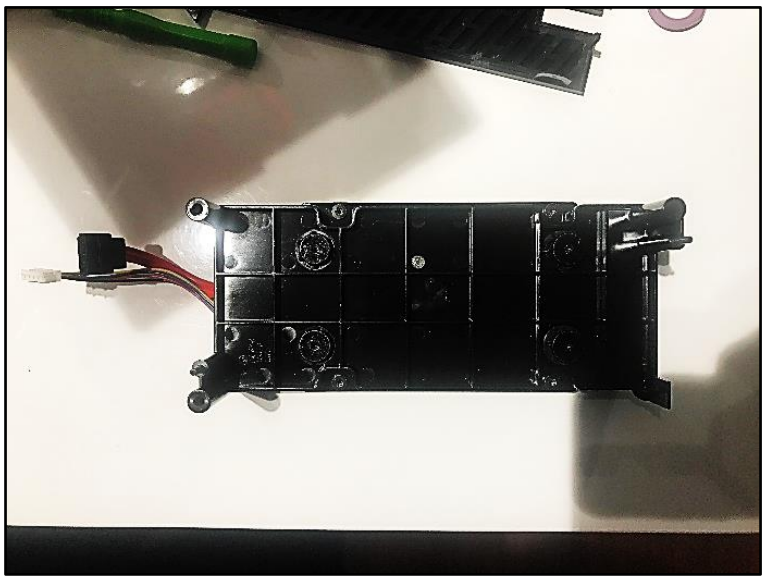


Figura 34. Ubicación tornillos de sujeción disco duro con plataforma
Fuente: Bryan Córdova

[22] Identificar y retirar los cables pertenecientes al disco duro únicamente.

o) Retirar el conector del disco duro para poder tener acceso a él desde un lector de disco duro vía USB

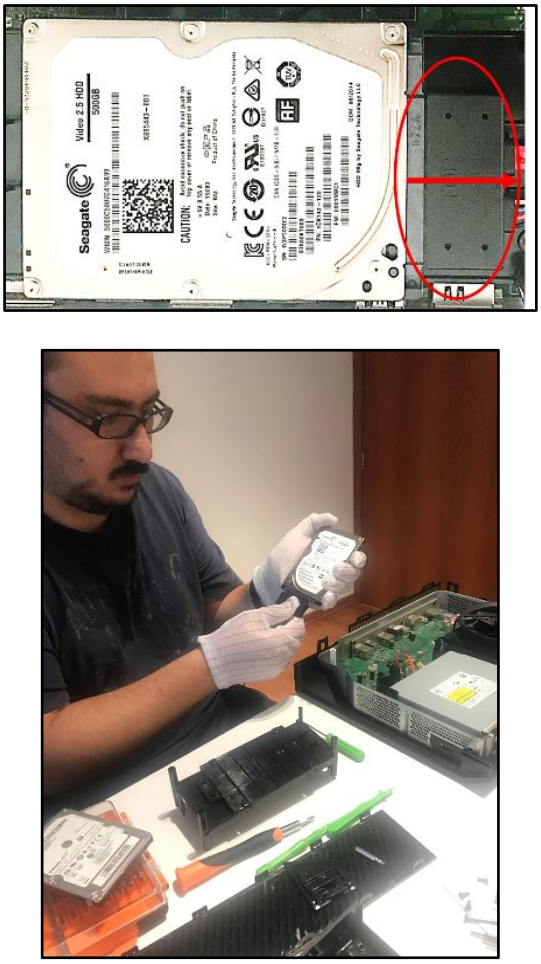


Figura 35. Retiro de módulo de conexión disco duro de la consola Xbox One
Fuente: Bryan Córdova

3.2.1.3.Extracción de imagen de disco de la consola

a) Para realizar la extracción de la imagen del disco deberemos conectar el disco duro obtenido de la consola en el enclosure para proceder con la conexión al computador

Figura 36. Conexión disco duro de consola con enclosure USB
Fuente: Bryan Córdova

b) Luego procederemos a conectar el disco externo USB y para evitar cualquier modificación no deseada de la información contenida en el disco se deberá formatear la unidad

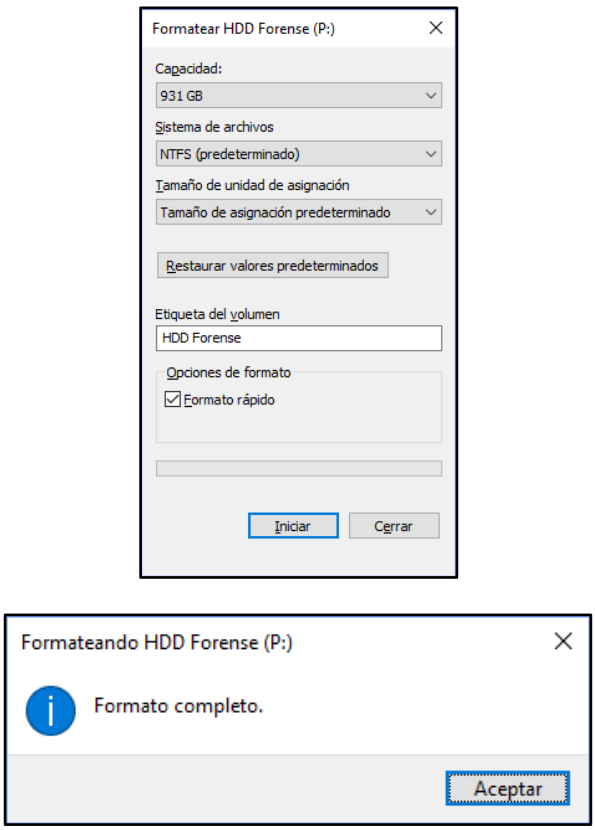


Figura 37. Proceso de formato de disco USB externo
Fuente: Bryan Córdova

c) Una vez formateado el disco externo USB procedemos con la clonación del disco de la consola Xbox One

- Procedemos a ejecutar el software para clonación de discos y creación de imágenes de respaldo

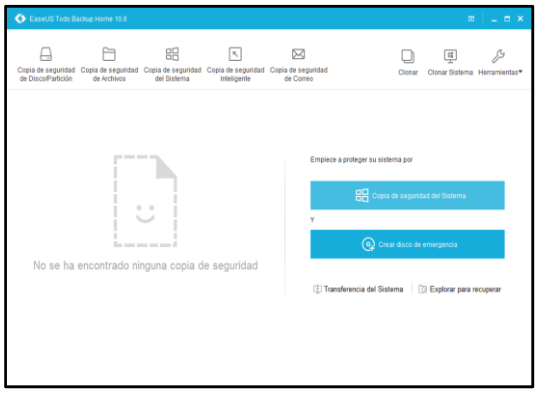


Figura 38. Pantalla principal software de clonación de discos
Fuente: Bryan Córdova

- Se procederá con la copia de seguridad o creación de imagen, se deberá marcar todo el disco para la creación de dicha imagen como se muestra en la figura

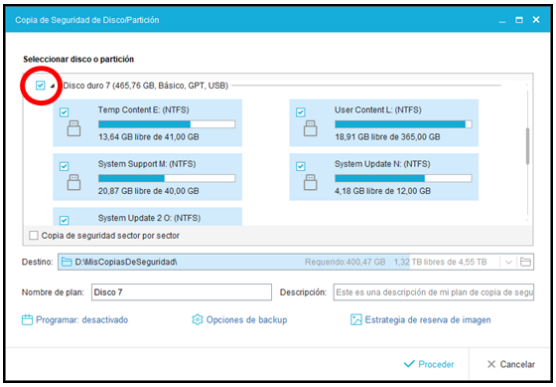


Figura 39. Selección de particiones de disco para clonación
Fuente: Bryan Córdova

- Luego seleccionaremos como destino de la creación de la imagen el disco externo USB

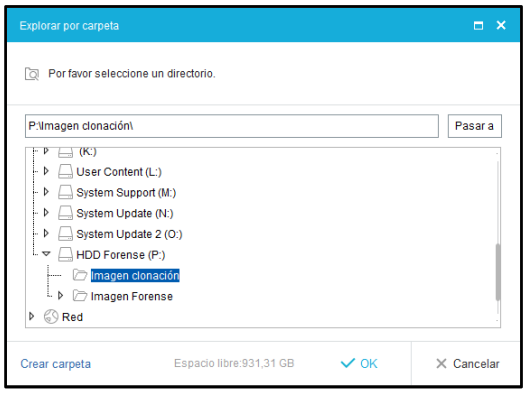


Figura 40. Selección de destino de imagen de clonación de disco
Fuente: Bryan Córdova

- Una vez escogida la ubicación donde se almacenará la imagen del disco, se procederá a etiquetar la imagen

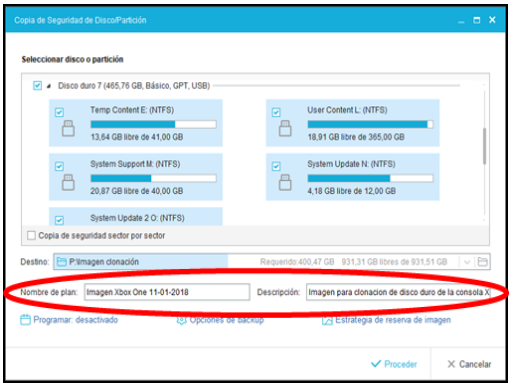


Figura 41. Nombramiento y descripción del archivo de imagen de disco
Fuente: Bryan Córdova

- Adicionalmente se podrán dar opciones adicionales y opcionales para la creación de la imagen de respaldo como son entre otras opciones de compresión de la imagen o encriptación de esta, esta última sería de gran importancia cuando se sospecha que se puede hallar evidencia de carácter reservado

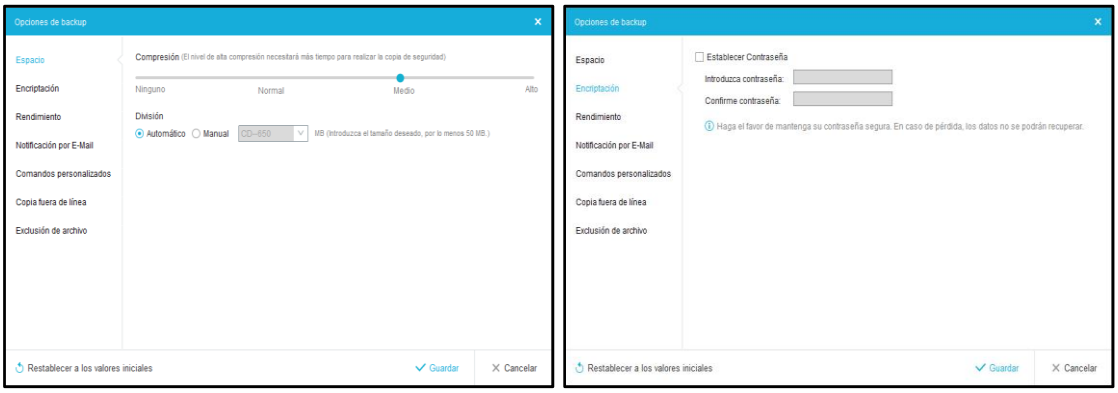


Figura 42. Menú con opciones adicionales para creación de imagen de disco
Fuente: Bryan Córdova

- Una vez completados los pasos anteriores, se hará click en guardar y luego en proceder para dar inicio al proceso de extracción de imagen del disco

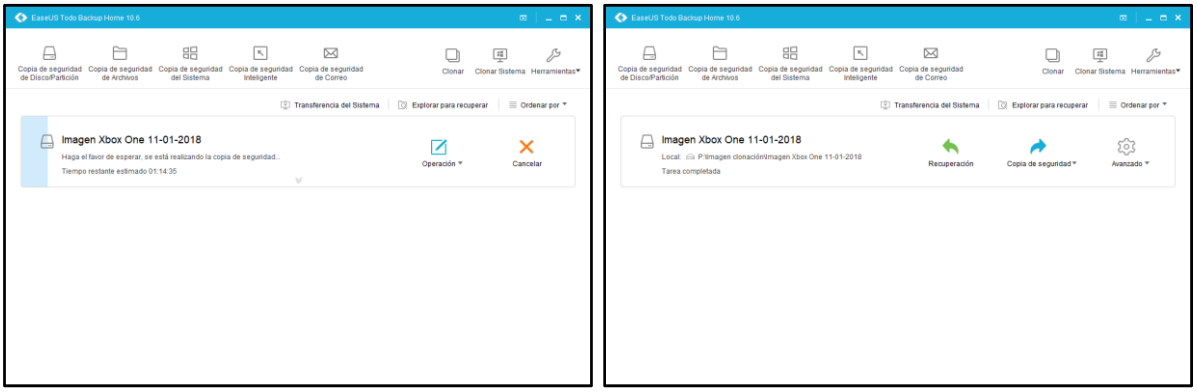


Figura 43. Proceso de creación de imagen de disco
Fuente: Bryan Córdova

- Una vez finalizado el proceso de obtención de la imagen del disco duro de la consola Xbox One, procederemos a restaurarla en el disco en blanco, con la opción Recuperación 

que nos aparecerá en nuestro registro de backups, por lo cual es recomendable guardar el nombre de la imagen junto con la fecha de creación

- El programa solicitará escoger que partición del disco deseamos recuperar, para este caso siempre deberemos rescatar la totalidad del disco, con el objeto de tener un clon idéntico al original, para lo cual se deberá hacer click el recuadro sobre las particiones

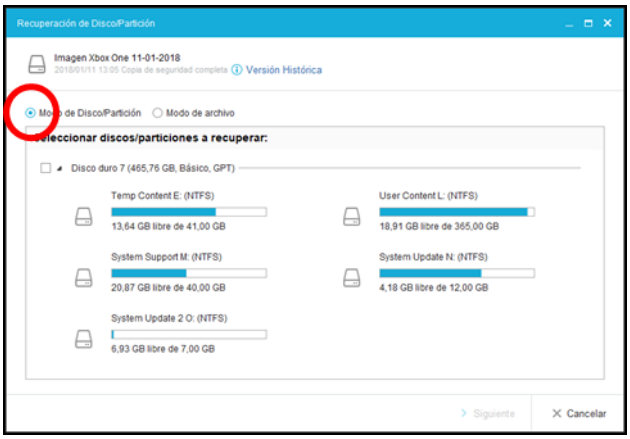


Figura 44. Proceso de recuperación de imagen de disco
Fuente: Bryan Córdova

- Una vez seleccionado damos click en siguiente y procederemos a escoger la unidad de destino, de igual manera procedemos a escoger la totalidad del disco de destino

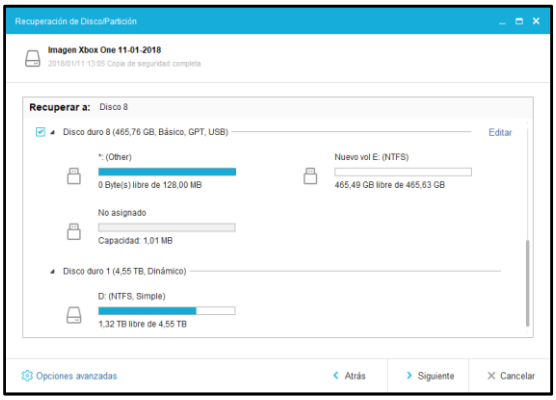


Figura 45. Selección de la unidad de destino para creación de imagen de disco
Fuente: Bryan Córdova

- Luego de haber verificado que el disco de destino escogido es el mismo que el disco físico de destino damos click en siguiente, lo cual nos indicara un breve resumen de cómo se encuentra distribuido el contenido de la imagen del disco de origen y de destino

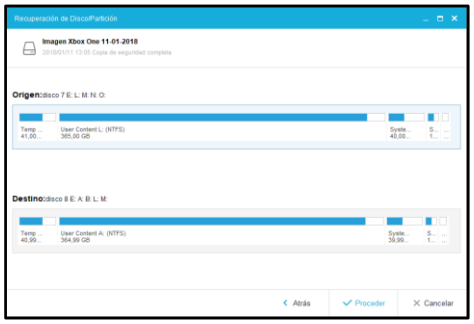


Figura 46. Resumen de distribución de particiones de imagen de disco y disco de destino
Fuente: Bryan Córdova

- Hacemos click en proceder y aparecerá un mensaje indicando que se perderán los datos en el disco de destino, para cual se deberá hacer click en ok siempre y cuando se haya verificado el disco de destino, luego empezará el proceso de recuperación de la imagen de disco en el dispositivo de almacenamiento de destino

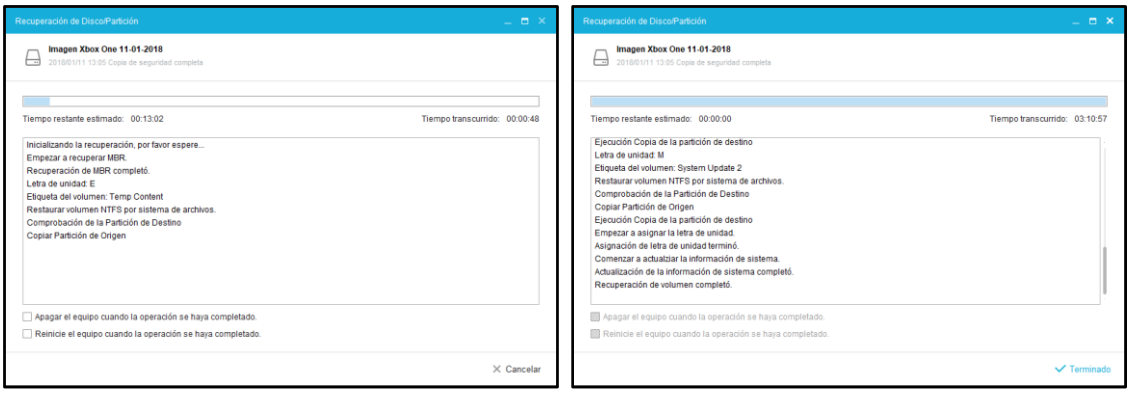


Figura 47. Proceso iniciado de recuperación de imagen de disco
Fuente: Bryan Córdova

3.2.2. Análisis de la información contenida en la consola Xbox One

Previo a la reconexión del disco clonado, no se deberá volver a ensamblar la consola, puesto que se deberá utilizar la misma consola para el procedimiento de análisis de la información.

Una vez clonado el disco duro de la consola, se procede a conectar el disco backup en la misma consola[23]

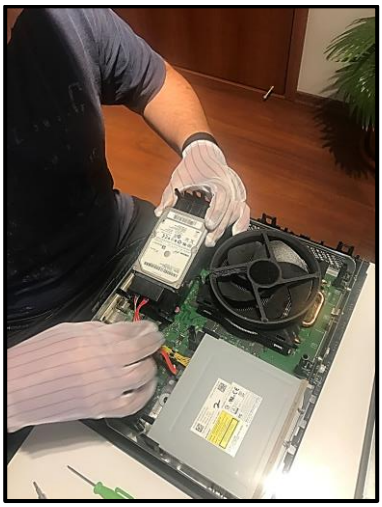


Figura 48. Instalación de disco backup en consola Xbox One
Fuente: Bryan Córdova

[23] Se deberá utilizar la misma consola puesto que la imagen del disco duro contiene una validación mediante código hash que impide que cada disco sea utilizado en diferentes consolas con el objeto de impedir la piratería.

Una vez conectado el disco backup se procede a reconectar el panel frontal junto con los conectores de la tarjeta Wifi y el parlante integrado

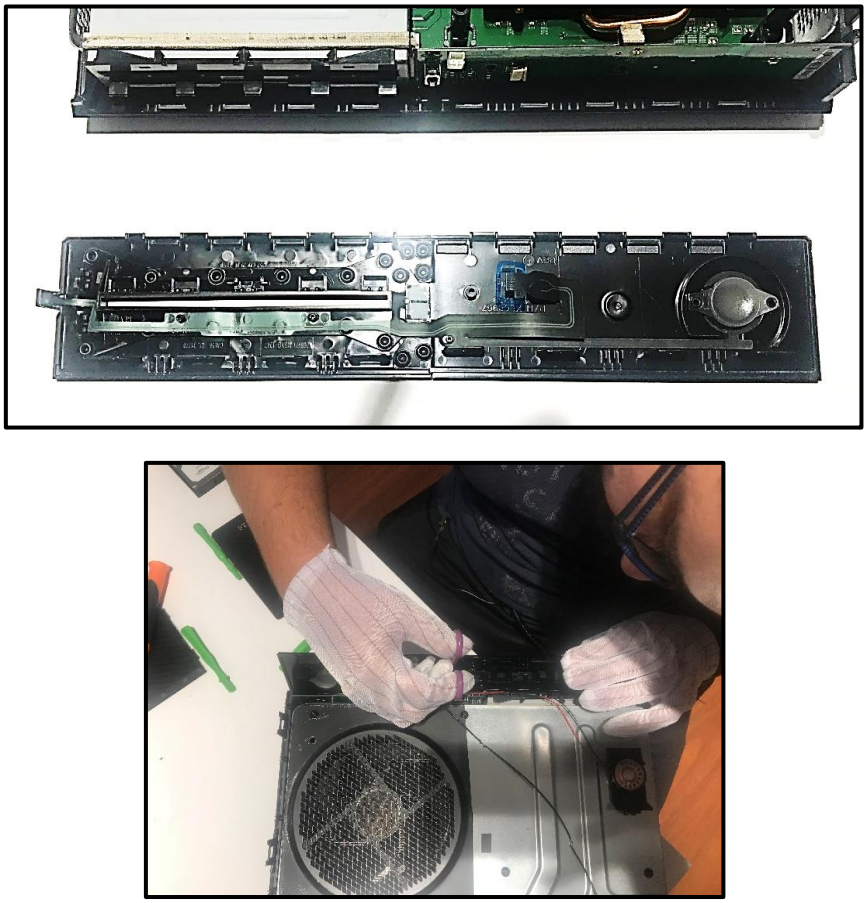


Figura 49. Reinstalación del panel frontal y cubierta metálica
Fuente: Bryan Córdova

Cuando se haya normalizado la conexión de los componentes principales, se procederá a conectar tanto la fuente de poder del Xbox One, así como el control inalámbrico y el cable Hdmi, este último conectado al televisor o monitor

Figura 50. Consola normalizada para puesta en funcionamiento
Fuente: Bryan Córdova

Siempre y cuando se pueda ingresar al sistema[24], se procederá con el análisis de la información contenida, haciendo uso del mando de la consola

- Una vez ingresado al sistema se puede acceder al log de chat por texto, se podrá acceder a las aplicaciones sociales, entre otros servicios

Se procede a verificar la integridad de la consola con respecto del disco backup instalado, procediendo a revisar la información de esta

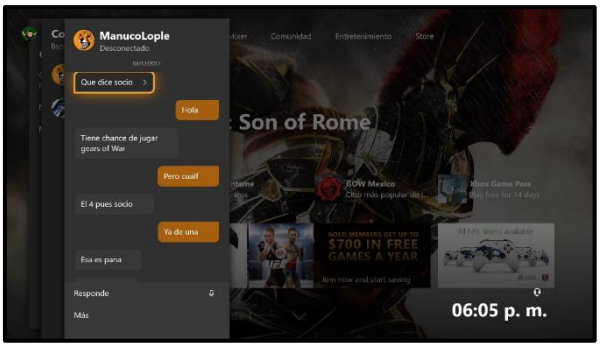
Figura 51. Información de la consola
Fuente: Bryan Córdova

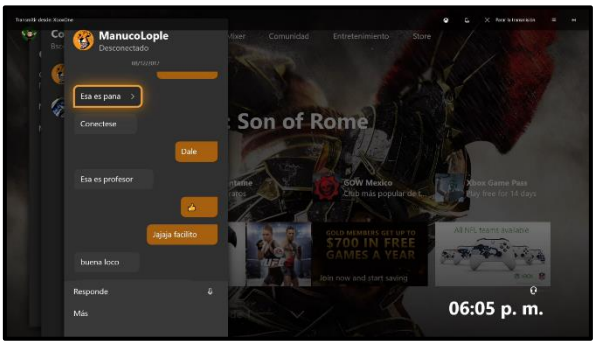
Una vez confirmada la integridad de la información con respecto de la consola, procedemos a revisar la actividad más reciente realizada por el usuario, una vez más realizando un procedimiento de triage determinando, los puntos más importantes de análisis como son, los de factor social, así como son el log de chat por texto y por último el uso de videojuegos.

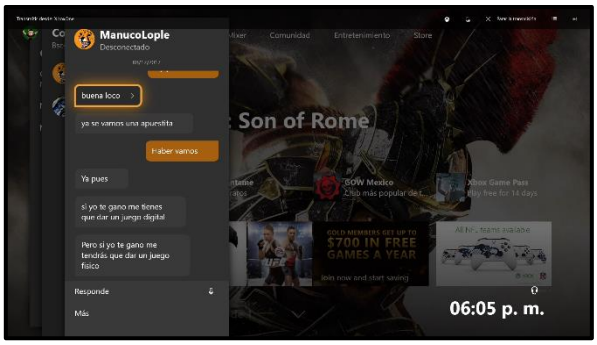
Para este procedimiento se deberá reconectar la consola a internet, debido a que a partir de la actualización de agosto del 2017 la consola debe permanecer actualizada para poder conectarla a la red y las aplicaciones sociales y de chat de la consola no se podrán acceder de manera offline por lo que se deberá proceder a actualizar la consola.

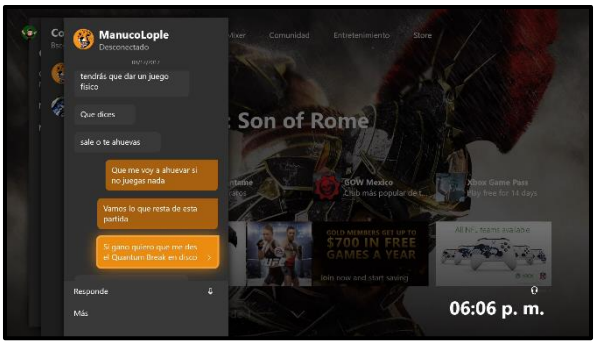
Durante la revisión de los chats se evidencia uno en particular, debido a que tiene que ver con un usuario que ha sido agregado recientemente y que de manera inmediata se pone en contacto con la víctima.

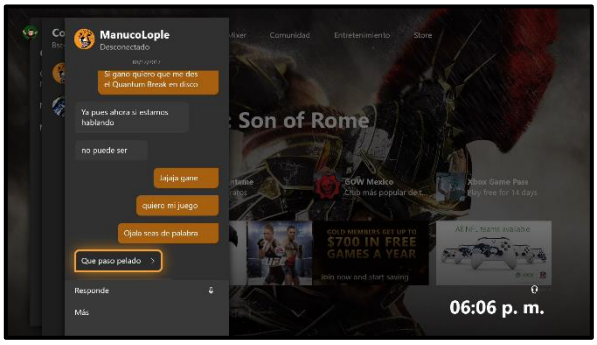
[24] La consola Xbox One cuenta con la característica de proteger el acceso indebido a la consola mediante el uso de contraseña, de ser el caso de poseer la contraseña se deberá primero investigar o de ser el caso romper la seguridad y desbloquear la consola.

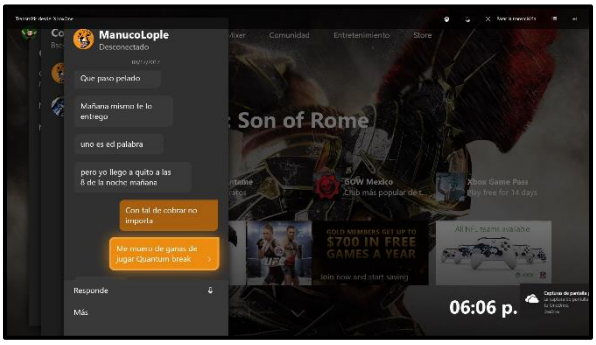

ManucoLople
Desconectado
Que dice socio
Hola
Tiene chance de jugar gears of War
Pero cuall
El 4 pues socio
Ya de una
Esa es pana
Responde
Más
Son of Rome
06:05 p. m.

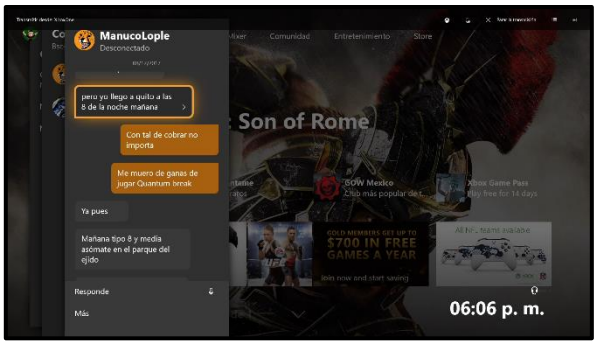

ManucoLople
Desconectado
Esa es pana
Conectese
Dale
Esa es profesor
Jajaja facilito
buena loco
Responde
Más
Son of Rome
06:05 p. m.

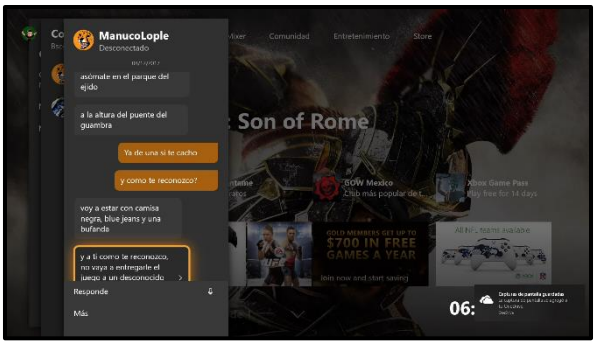

ManucoLople
Desconectado
buena loco
ya se vamos una apuestita
Haber vamos
Ya pues
si yo te gano me tienes que dar un juego digital
Pero si yo te gano me tendrás que dar un juego físico
Responde
Más
Son of Rome
06:05 p. m.

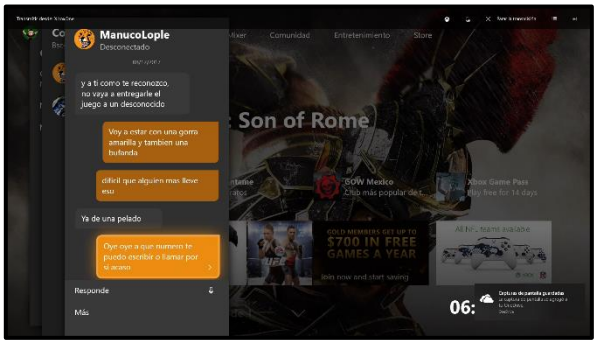

ManucoLople
Desconectado
tendrás que dar un juego físico
Que dices
sale o te ahuevas
Que me voy a ahuevar si no juegas nada
Vamos lo que resta de esta partida
Si gano quiero que me des el Quantum Break en disco
Responde
Más
Son of Rome
06:06 p. m.

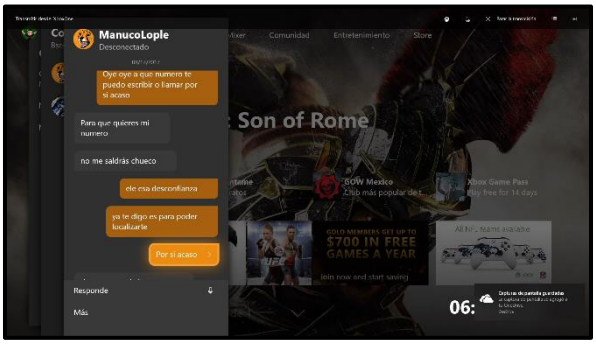

ManucoLople
Desconectado
Si gano quiero que me des el Quantum Break en disco
Ya pues ahora si estamos hablando
no puede ser
Jajaja game
quiero mi juego
Ojalá sean de palabra
Que paso pelado
Responde
Más
Son of Rome
06:06 p. m.


ManucoLople
Desconectado
Que paso pelado
Mañana mismo te lo entiego
uno es ed palabra
pero yo llego a quito a las 6 de la noche mañana
Con tal de cobrar no importa
Me muero de ganas de jugar Quantum break
Responde
Más
Son of Rome
06:06 p.


ManucoLople
Desconectado
pero yo llego a quito a las 6 de la noche mañana
Con tal de cobrar no importa
Me muero de ganas de jugar Quantum break
Ya pues
Mañana tipo 8 y media asómate en el parque del ejido
Responde
Más
Son of Rome
06:06 p. m.


ManucoLople
Desconectado
asómate en el parque del ejido
a la altura del puente del guambra
Ya de una si le cacho
y como te reconozco?
voy a estar con camisa negra, blue jeans y una bufanda
y a ti como te reconozco, no voya a entregarle el juego a un desconocido
Responde
Más
Son of Rome
06:


ManucoLople
Desconectado
y a ti como te reconozco, no voya a entregarle el juego a un desconocido
Voy a estar con una gorra amarilla y tambien una bufanda
difícil que alguien mas lleve eso
Ya de una pelado
Oye oye a que numero te puedo escribir o llamar por si acaso
Responde
Más
Son of Rome
06:


ManucoLople
Desconectado
Oye oye a que numero te puedo escribir o llamar por si acaso
Para que quieres mi numero
no me saldrás chueco
ete esa desconfianza
ya te digo es para poder localizarte
Por si acaso
Responde
Más
Son of Rome
06:

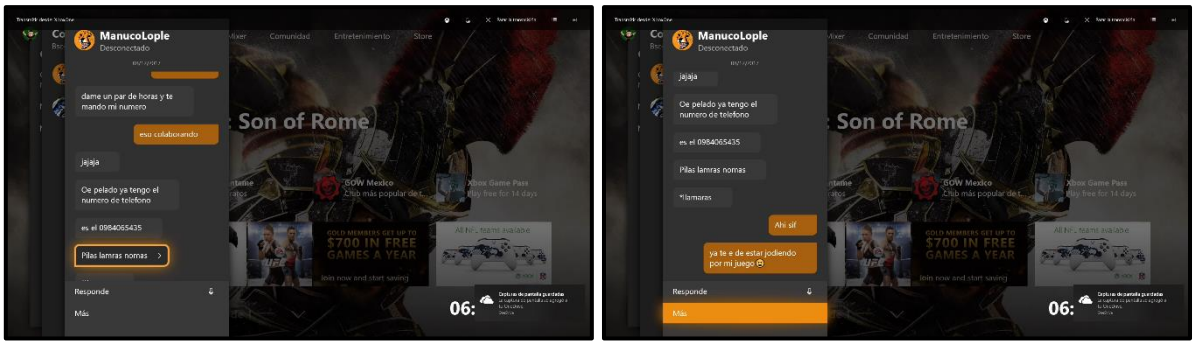


Figura 52. Chat de texto de la consola Xbox One
Fuente: Bryan Córdova

En dicha conversación el sujeto solicita a la víctima interactuar por medio de un videojuego especifico y de hecho muy popular entre los usuarios de dicha consola como es Gears of War 4.

La victima posee instalada la versión digital del videojuego por lo cual no fue necesario realizar otro proceso de allanamiento y se procede a verificar los logs dentro de dicho videojuego.

Figura 53. Menú Principal del videojuego Gears of War 4
Fuente: Bryan Córdova

Revisando los registros, se evidencia que efectivamente existió una partida uno contra uno con el usuario sospechoso. Una vez cotejado los hechos relatados en el chat de texto con los del videojuego se llega a la conclusión que la víctima gano la supuesta apuesta y el sujeto por medio de una charla aparentemente inocente, atrajo al usuario con el objeto de ganar su confianza y que creyera en el para el intercambio de la apuesta.

Por lo tanto, se obtiene el indicio donde la víctima pudo ser vista por última vez, debido a que en el chat el sujeto solicita encontrarse con la víctima en un horario y lugar en concreto. En el informe se evidenciará lo antes mencionado y se recomendara a la fiscalía solicitar los archivos de video de las cámaras que corresponden al sector en mención con el fin de continuar con la investigación y en el mejor de los casos que se pueda identificar al atacante.

CAPITULO IV

DISCUSIÓN

4.1. CONCLUSIONES

- Con la finalización del presente trabajo de investigación se concluye que una vez descartados ciertos métodos tradicionales se ha creado una metodología eficiente para el Análisis Forense de consolas de videojuegos Xbox One, la cual beneficiara a los Peritos Informáticos, fiscales, personal de criminalística, así como a los jueces para que posean mediante el informe pericial, un elemento con el cual se pueda dictar sentencia y se haga justicia.

- Se desarrolló esta metodología con la finalidad de brindar los conocimientos tanto a los Peritos Informáticos, así como a los fiscales y personal de criminalística que debido al desconocimiento pudieron dejar de lado las consolas de videojuegos durante el periodo de allanamiento, lo cual se demuestra que se pudo omitir evidencia de gran importancia al momento de realizar una investigación sobre algún delito.

- Tras la elaboración del presente trabajo investigativo también se llegó a concluir que cada equipo electrónico que tenga similares funciones a la de un computador tradicional no necesariamente será aplicable una metodología o técnicas tradicionales debido a que se depende del tipo de información y el sistema de archivos del equipo, estos pueden tener un nivel de encriptación no tradicional y por tanto no será posible aplicar las técnicas conocidas.

- Tanto en el transcurso de esta investigación como en el uso cotidiano de estas consolas se ha podido detectar que existen vulnerabilidades por parte de los desarrolladores, debido que al intentar brindar más servicios inicialmente se dan paso a ciertas omisiones en el aspecto de la seguridad y acuerdos de confianza entre la empresa y el cliente, solo cuando ya sucede algún percance se toman acciones por parte de la empresa que desarrolla e incluso por parte de los usuarios.

- Durante la experimentación con la extracción de información, se esperaba obtener la evidencia de manera más sencilla, debido a que al ser una consola de Microsoft, Xbox One cuenta con un core de Windows 10 para correr las

aplicaciones, pero al llegar al punto donde se obtuvo la imagen forense, esta no dio resultados por parte de las herramientas forenses, esto debido a que existe otro sistema operativo el cual maneja los dos sistemas de fondo de la consola y es el dashboard, para el cual todavía no se ha desarrollado una herramienta de análisis forense que permita ya sea, desencriptar la información o que permita obtener la evidencia directamente del core de Windows.

4.2. RECOMENDACIONES

- Los procedimientos redactados junto con las herramientas de hardware y software certifican que la integridad de la evidencia original no se altere, lo que garantiza que sea reconocida como evidencia en los tribunales y evitando la descalificación de esta.

- Esta metodología deberá ser difundida para que mediante su aplicación siga obteniendo más relevancia y a futuro sea expandida y fortaleciendo los conocimientos y sea posible utilizarla en nuevos casos a futuro en nuestro país.

- Se recomienda además siempre tener en cuenta las técnicas sugeridas para la investigación ya que han sido producto de una investigación y comprobación previa, por lo tanto, con el afán de lograr resultados más confiables y eficaces se ha desarrollado la metodología en cuestión.

- Al momento de realizar el desmontaje se deberá tener especial cuidado con los componentes electrónicos y en especial con el panel frontal debido que la consola deberá ser normalizada para su posterior investigación y el panel frontal es un componente esencial para ello.

- Se debe tener especial cuidado al momento de permitir el uso de estas consolas de videojuegos a los menores, por lo tanto, se pueden tomar las debidas precauciones como son el control parental, que es una herramienta que ha venido ayudando y ha aumentado su relevancia tanto por la interacción social de las consolas como por el contenido de las aplicaciones, además que es un factor de riesgo el permitir la libre comunicación entre usuarios, tal como se evidencio en este trabajo investigativo.

- Además de los cuidados que se deben tomar con respecto a los menores, también se debe tomar en cuenta que la mejor forma de combatir los delitos informáticos es fomentando la actualización y la investigación acerca de todo el

funcionamiento de una consola, debido a que por más que cueste aceptarlo, estos equipos cada vez son más complejos y que ya no se debería tomarlos en cuenta como una simple distracción para los jóvenes, sino como una herramienta de entretenimiento global que posee características de interacción social por lo cual se debe tener mayor atención y tomar en cuenta el factor de seguridad al momento de instalar estos equipos, así como los acuerdos que se aceptan si se desea hacer uso de estas consolas.

BIBLIOGRAFÍA

AccessData. (2018). Forensic Toolkit (FTK). Recuperado de https://accessdata.com/products-services/forensic-toolkit-ftk

AENOR. (2013). UNE 71506. Recuperado de http://www.aenor.es/aenor/inicio/home/home.asp

Anthony, S. (2013). Xbox One: Hardware and software specs detailed and analyzed. Recuperado de http://www.extremetech.com/gaming/156467-xbox-one-hardware-and-software-specs-detailed-and-analyzed

Asamblea Nacional. (2011). Código Órganico General de Procesos; Ecuador,. *Registro Oficial N° 506*, 1–79. Recuperado de http://www.funcionjudicial.gob.ec

Asamblea Nacional. (2014). Código Orgánico Integral Penal, COIP. *Registro Oficial Suplemento 180 de 10-Feb.-2014*. Recuperado de https://doi.org/10.1111/j.1559-1816.2000.tb02505.x

Gravel, C. E., & Hansen, R. (2015). *Xbox one file system data storage : A forensic analysis*. Recuperado de https://tinyurl.com/y97bhdbv

Haagman, D., & Wilkinson, S. (2010). Good Practice Guide for Computer-Based Electronic Evidence. *Association of Chief Police Officers*, *67*(5), 72. Recuperado de https://doi.org/10.1016/j.jad.2011.08.001

JUDICATURA, C. D. LA. (2014). Reglamento Del Sistema Pericial Integral De La Funcion Judicial. *Estatuto*, (125), 20. Recuperado de http://www.funcionjudicial.gob.ec/www/pdf/Reglamento del Sistema Pericial Integral de la Funcion Judicial.pdf

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. Recuperado de https://doi.org/10.6028/NIST.SP.800-86

Loarte, G., & Grijalva, J. (2017). Marco de trabajo estandarizado para el análisis forense de la evidencia digital, (11), 42–78. Recuperado de https://rmlconsultores.com/revista/index.php/crv/article/view/463

Martínez, A. (2014). RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento. Recuperado de https://www.certsi.es/blog/rfc3227

Moore, J., Baggili, I., Marrington, A., & Rodrigues, A. (2014). Preliminary forensic analysis of the Xbox one. *Digital Investigation*, *11*(SUPPL. 2). Recuperado de https://doi.org/10.1016/j.diin.2014.05.014

Offensive Security. (2018). Kali. Recuperado de https://www.kali.org/

Porolli, M. (2013). ¿En qué consiste el análisis forense de la información? Recuperado de https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

Rivas, G. (2014). Metodología para un análisis forense. Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf

Shirey, R. (2007). *Internet Security Glossary, Version 2*. Recuperado de https://doi.org/10.17487/rfc4949

SleuthKit. (2003). Autopsy. Recuperado de https://www.sleuthkit.org/index.php

Yerby, J., Hollifield, S., Kwak, M., & Floyd, K. (2014). Development of Serious Games for Teaching Digital Forensics. *Issues in Information Systems*, *15*(Ii), 335–343. Recuperado de http://iacis.org/iis/2014/135_iis_2014_335-343.pdf

ANEXOS

ANEXO A - FORMULARIO No 1

Se debe llenar con la información personal del perito a cargo de la investigación.

FORMULARIO N° 1 DATOS PERSONALES			
LUGAR Y FECHA			
NOMBRES COMPLETOS			
CEDULA DE CIUDADANÍA			
CORREO ELECTRÓNICO			
ESPECIALIZACIÓN			
CÓDIGO DE PERITO			
SERVIDOR/A PUBLICO		INSTITUCIÓN	
FIRMA PERITO INFORMÁTICO		_____	

ANEXO B -FORMULARIO No 2

Debe contener la información referente a la escena del delito.

FORMULARIO N° 2 DESCRIPCIÓN DE LA ESCENA DEL DELITO					
CASO					
LUGAR					
FECHA Y HORA					
NÚMERO DE PERSONAS EN EL LUGAR					
NOMBRES COMPLETOS DE LAS PERSONAS EN EL LUGAR					
PERSONAS QUE TIENE ACCESO AL EQUIPO A SER INVESTIGADO					
FOTOGRAFÍA DEL LUGAR			DESCRIPCIÓN		
TESTIMONIOS DE LAS PERSONAS QUE ESTABAN EN EL LUGAR	SI				
	NO				
DESCRIPCIÓN DE LOS EQUIPOS A SER INVESTIGADOS					
NÚMERO DE ETIQUETA					
TIPO DE DISPOSITIVO			CARACTERÍSTICA		
DESCRIPCIÓN FÍSICA					
ESTADO	ENCENDIDO		APAGADO		
UBICACIÓN					
PERIFÉRICOS CONECTADOS					
CONEXIÓN A INTERNET					
FOTOGRAFÍA					
OBSERVACIÓN					
OBSERVACIONES GENERALES					
---------- FIRMA PERITO INFORMÁTICO			---------- FIRMA NOTARIO / FISCAL		

ANEXO C -FORMULARIO No 3

Se debe llenar con la información que se haya recopilado referente a la evidencia original de los diferentes dispositivos de almacenamiento que serán utilizados para la investigación.

FORMULARIO N° 3 RECOPILACIÓN DE LA EVIDENCIA ORIGINAL						
CASO						
NOMBRE DEL PERITO INFORMÁTICO						
LUGAR						
FECHA Y HORA						
NÚMERO DE ETIQUETA						
TIPO DE EQUIPO IMPLICADO						
ESTADO			ENCENDIDO		APAGADO	
FECHA Y HORA DE APAGADO DEL EQUIPO						
OBSERVACIÓN						
MARCA	SERIE	MEMORIA RAM	SISTEMA OPERATIVO	PROCESADOR	DISCO DURO	
DESCRIPCIÓN DE LA RECOPILACIÓN DE LA EVIDENCIA						
NÚMERO DE ETIQUETA						
DISPOSITIVO DE ALMACENAMIENTO						
MÉTODO / APLICACIÓN UTILIZADO						
CREADO POR (NOMBRE Y CARGO)						
FECHA		HORA		CÓDIGO HASH		
---------- FIRMA PERITO INFORMÁTICO				---------- FIRMA NOTARIO / FISCAL		

ANEXO D -FORMULARIO No 4

Se debe llenar con la información referente a los elementos físicos o contenido digital, principalmente los que serán parte de la investigación y de la Cadena de Custodia para ser transportados al laboratorio forense.

FORMULARIO N° 3 ALMACENAMIENTO Y TRANSPORTE DE ELEMENTOS FÍSICOS O CONTENIDO DIGITAL						
CASO						
NOMBRE DEL PERITO INFORMÁTICO						
LUGAR						
DESCRIPCIÓN DEL ALMACENAMIENTO						
NÚMERO DE ETIQUETA						
TIPO DE EQUIPO IMPLICADO						
OBSERVACIÓN						
MARCA	SERIE	MEMORIA RAM	SISTEMA OPERATIVO	PROCESADOR	DISCO DURO	
REMITENTE				DESTINATARIO		
NOMBRE		FIRMA		NOMBRE		FIRMA
MOTIVO				LUGAR		
				CÓDIGO HASH		
FECHA		HORA				
FOTOGRAFÍA						
DESCRIPCIÓN DEL TRANSPORTE						
NOMBRE DE LA PERSONA A CARGO DEL TRANSPORTE						
MEDIO DE TRANSPORTE				PLACAS DEL TRANSPORTE		
---------- FIRMA PERITO INFORMÁTICO		---------- FIRMA NOTARIO / FISCAL			---------- - FIRMA DEL TRANSPORTISTA	

ANEXO E – ARTÍCULOS DEL COIP

sin que causen impedimento en el desempeño de sus actividades cotidianas, será sancionada con pena privativa de libertad de treinta a sesenta días.

2. Si se afecta de manera moderada en cualquiera de las áreas de funcionamiento personal, laboral, escolar, familiar o social que cause perjuicio en el cumplimiento de sus actividades cotidianas y que por tanto requiere de tratamiento especializado en salud mental, será sancionada con pena de seis meses a un año.

3. Si causa un daño psicológico severo que aún con la intervención especializada no se ha logrado revertir, será sancionada con pena privativa de libertad de uno a tres años.

Artículo 158.- Violencia sexual contra la mujer o miembros del núcleo familiar.- La persona que, como manifestación de violencia contra la mujer o un miembro del núcleo familiar, se imponga a otra y la obligue a tener relaciones sexuales u otras prácticas análogas, será sancionada con las penas previstas en los delitos contra la integridad sexual y reproductiva.

PARÁGRAFO SEGUNDO
Contravención de violencia contra la mujer o miembros del núcleo familiar

Artículo 159.- Violencia contra la mujer o miembros del núcleo familiar.- La persona que hiera, lesione o golpee a la mujer o miembros del núcleo familiar, causándole lesiones o incapacidad que no pase de tres días, será sancionada con pena privativa de libertad de siete a treinta días.

SECCIÓN TERCERA
Delitos contra la libertad personal

Artículo 160.- Privación ilegal de libertad.- La o el servidor público que prive ilegalmente de libertad a una persona, será sancionado con pena privativa de libertad de uno a tres años.

La o el servidor público que disponga la privación de libertad a una persona en lugares diferentes a los destinados para el efecto por la normativa vigente, será sancionado con pena privativa de libertad de tres a cinco años.

Artículo 161.- Secuestro.- La persona que prive de la libertad, retenga, oculte, arrebate o traslade a lugar distinto a una o más personas, en contra de su voluntad, será sancionada con pena privativa de libertad de cinco a siete años.

Artículo 162.- Secuestro extorsivo.- Si la persona que ejecuta la conducta sancionada en el artículo 161 de este Código tiene como propósito cometer otra infracción u obtener de la o las víctimas o de terceras

agravadas en un tercio. Si los actos de violencia producen la muerte de una persona, será sancionada con pena privativa de libertad de veintidós a veintiséis años.

SECCIÓN SEXTA
Delitos contra el derecho a la intimidad personal y familiar

Artículo 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Artículo 179.- Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Artículo 180.- Difusión de información de circulación restringida.- La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años.

Es información de circulación restringida:

1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.

2. La información producida por la Fiscalía en el marco de una investigación previa.

3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.

Artículo 181.- Violación de propiedad privada.- La persona que, con engaños o de manera clandestina, ingrese o se mantenga en morada, casa, negocio, dependencia o recinto habitado por otra, en contra de la voluntad expresa o presunta de quien tenga derecho a excluirla, será sancionada con pena privativa de libertad de seis meses a un año.

Si el hecho se ejecuta con violencia o intimidación, será sancionada con pena privativa de libertad de uno a tres años.

o el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones preacordadas.

Los partes informativos, noticias del delito, versiones de los testigos, informes periciales y cualquier otra declaración previa, se podrán utilizar en el juicio con la única finalidad de recordar y destacar contradicciones, siempre bajo la prevención de que no sustituyan al testimonio. En ningún caso serán admitidos como prueba.

7. Principio de igualdad de oportunidades para la prueba.- Se deberá garantizar la efectiva igualdad material y formal de los intervinientes en el desarrollo de la actuación procesal.

Artículo 455.- Nexo causal.- La prueba y los elementos de prueba deberán tener un nexo causal entre la infracción y la persona procesada, el fundamento tendrá que basarse en hechos reales introducidos o que puedan ser introducidos a través de un medio de prueba y nunca, en presunciones.

Artículo 456.- Cadena de custodia.- Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio.

La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación.

Artículo 457.- Criterios de valoración.- La valoración de la prueba se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales.

La demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente.

Artículo 458.- Preservación de la escena del hecho o indicios.- La o el servidor público que intervenga o tome contacto con la escena del hecho e indicios será la responsable de su

preservación, hasta contar con la presencia del personal especializado.

Igual obligación tienen los particulares que por razón de su trabajo o función entren en contacto con indicios relacionados con un hecho presuntamente delictivo.

CAPÍTULO SEGUNDO
ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN

Artículo 459.- Actuaciones.- Las actuaciones de investigación se sujetarán a las siguientes reglas:

1. Para la obtención de muestras, exámenes médicos o corporales, se precisa el consentimiento expreso de la persona o la autorización de la o el juzgador, sin que la persona pueda ser físicamente constreñida. Excepcionalmente por las circunstancias del caso, cuando la persona no pueda dar su consentimiento, lo podrá otorgar un familiar hasta el segundo grado de consanguinidad.

2. Las diligencias de reconocimiento constarán en actas e informes periciales.

3. Las diligencias de investigación deberán ser registradas en medios tecnológicos y documentales más adecuados para preservar la realización de la misma y formarán parte del expediente fiscal.

4. El registro que conste en el expediente fiscal deberá ser suficiente para determinar todos los elementos de convicción que puedan fundamentar la formulación de cargos o la acusación.

5. En caso de no existir una institución pública acreditada, las autopsias, exámenes médicos, de laboratorio o pruebas biológicas, podrán ser realizados en una institución de salud privada acreditada y los costos serán asumidos por el Consejo de la Judicatura. Los mismos tendrán valor pericial.

Artículo 460.- Reconocimiento del lugar de los hechos.- La o el fiscal con el apoyo del personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, o el personal competente en materia de tránsito, cuando sea relevante para la investigación, reconocerá el lugar de los hechos de conformidad con las siguientes disposiciones:

1. La o el fiscal o el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, podrá impedir a cualquier persona, incluso haciendo uso de la fuerza pública, que ingrese o se retire del lugar donde se cometió la infracción, por un máximo de ocho horas, hasta que se practiquen las actuaciones de investigación necesarias.

secreto profesional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones.

6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá solicitar la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa.

7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio.

8. El medio de almacenamiento de la información obtenida durante la interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio.

9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros.

Artículo 477.- Reconocimiento de grabaciones.- La o el juzgador autorizará a la o al fiscal el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de vídeos, datos informáticos, fotografías, discos u otros medios análogos o digitales. Para este efecto, con la intervención de dos peritos que juren guardar reserva, la o el fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento.

La o el fiscal podrá ordenar la identificación de voces grabadas, por parte de personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos.

SECCIÓN SEGUNDA
Registros y allanamiento

Artículo 478.- Registros.- Los registros se realizarán de acuerdo con las siguientes reglas:

1. Los registros de personas u objetos e incautación de los elementos relacionados con una infracción que se encuentren en viviendas u otros lugares, requerirán autorización de la persona afectada o de orden judicial. En este último caso deberá ser motivada y limitada únicamente a lo señalado de forma taxativa en la misma y realizado en el lugar autorizado.

2. El consentimiento libremente otorgado por la persona requerida para registrar un espacio determinado, permitirá realizar el registro e incautación de los elementos relacionados con una infracción. Únicamente podrán prestar el consentimiento personas capaces y mayores de edad. Se deberá informar a la persona investigada sobre su derecho a no permitir el registro sin autorización judicial.

3. Las y los servidores de la fuerza pública, sin que medie orden judicial, como una actividad de carácter preventivo o investigativo, podrán realizar el control de identidad y registro superficial de personas con estricta observancia en cuanto a género y respeto de las garantías constitucionales, cuando exista una razón fundamentada de que la persona oculta en sus vestimentas cualquier tipo de arma que pueda poner en riesgo la seguridad de las personas o exista la presunción de que se cometió o intentó cometer una infracción penal o suministre indicios o evidencias útiles para la investigación de una infracción.

Artículo 479.- Registro de vehículos.- Se podrá registrar un vehículo sin autorización judicial, en los siguientes casos:

1. En zonas de frontera o donde la aduana ejerza control. En ningún caso el registro deberá interferir en la intimidad de los pasajeros.

2. En controles de rutina policial y militar. En ningún caso el registro deberá interferir en la intimidad de los pasajeros.

3. En caso de existir razones fundamentadas o presunciones sobre la existencia de armas o de la existencia de elementos de convicción en infracciones penales.

4. Si el conductor no justifica documentada y legalmente los permisos de circulación, matriculación o de procedencia de la mercadería.

5. Por el hecho de haberse cometido una infracción flagrante. El funcionario que ha falseado la comisión de un delito flagrante para registrar un vehículo será destituido de su cargo, sin perjuicio de las acciones civiles o penales a que dé lugar.

Solo en los supuestos del segundo, tercero y cuarto numerales de este artículo se podrá realizar un registro superficial sobre las personas, con estricta observancia en cuanto a género, edad o grupos de atención prioritaria y respeto de las garantías constitucionales.

Artículo 480.- Allanamiento.- El domicilio o el lugar donde la persona desarrolle su actividad familiar, comercial o laboral, podrá ser allanado en los siguientes casos:

1. Cuando se trate de detener a una persona contra la que se ha dictado orden de detención con fines de investigación, prisión preventiva o se ha pronunciado sentencia condenatoria ejecutoriada con pena privativa de libertad.

2. Cuando la Policía Nacional esté en persecución ininterrumpida de una persona que ha cometido un delito flagrante.

3. Cuando se trate de impedir la consumación de una infracción que se está realizando o de socorrer a sus víctimas.

4. Cuando se trate de socorrer a las víctimas de un accidente del que pueda correr peligro la vida de las personas.

5. Cuando se trate de recaudar la cosa sustraída o reclamada o los objetos que constituyan elementos probatorios o estén vinculados al hecho que se investiga. En estos casos se procederá a la aprehensión de los bienes.

6. En los casos de violencia contra la mujer o miembros del núcleo familiar, cuando deba recuperarse a la agredida, agredido, o a sus familiares; cuando la agresora o el agresor se encuentre armado o bajo los efectos del alcohol, de sustancias catalogadas sujetas a fiscalización o esté agrediendo a su pareja o poniendo en riesgo la integridad física, psicológica o sexual de cualquier miembro de la familia de la víctima.

7. Cuando se trate de situaciones de emergencia, tales como: incendio, explosión, inundación u otra clase de estragos que pongan en peligro la vida o la propiedad.

En los casos de los numerales 1 y 5 se requerirá orden motivada de la o el juzgador y en los demás casos no requerirá formalidad alguna.

Para evitar la fuga de personas o la extracción de armas, instrumentos, objetos o documentos probatorios y mientras se ordena el allanamiento, la o el fiscal podrá disponer la vigilancia del lugar, la retención de las cosas y solicitar a la o al juzgador la orden de detención con fines investigativos para las personas que se encuentren en él.

Artículo 481.- Orden de allanamiento.- La orden de allanamiento deberá constar por escrito y señalar los motivos que determinan el registro, las diligencias por practicar, la dirección o ubicación concreta del lugar o lugares donde se ejecute el allanamiento y su fecha de expedición. En casos de urgencia, la o el fiscal podrá solicitar la orden verbalmente o por cualquier medio conveniente, dejando constancia de los motivos que determinen el allanamiento.

De no ser posible la descripción exacta del lugar o lugares por registrar, la o el fiscal indicará los

argumentos para que, a pesar de ello, se deberá proceder al operativo. En ninguna circunstancia podrá emitirse órdenes de registro y allanamiento arbitrarios.

La o el juzgador podrá autorizar el allanamiento por cualquier medio, dejando constancia de dicho acto.

Artículo 482.- Procedimiento del allanamiento.- El allanamiento deberá realizarse de conformidad con las siguientes reglas:

1. Con la presencia de la o el fiscal acompañado de la Policía Nacional, sin que puedan ingresar personas no autorizadas por la o el fiscal al lugar que deba allanarse.

2. Si presentada la orden de allanamiento, la o el propietario o habitante de la vivienda, lugar de trabajo o local, se resiste a la entrega de la persona o de las cosas o al ingreso o exhibición de lugares u objetos que se encuentren al interior de dichos lugares, el o la fiscal ordenará el quebrantamiento de las puertas o cerraduras.

3. Practicado el allanamiento, la o el fiscal reconocerá en presencia de los concurrentes las dependencias del local allanado, las armas, documentos u objetos concernientes a la infracción. El personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses, recogerá los elementos de convicción pertinentes, previo inventario, descripción detallada y embalaje para cadena de custodia.

4. Para allanar una misión diplomática o consular o la residencia de los miembros de las respectivas misiones, la o el juzgador se dirigirá con copia del proceso a la entidad encargada de las políticas de relaciones exteriores, solicitando la práctica de la diligencia. En caso de negativa del agente diplomático o consular, el allanamiento no podrá realizarse. En todo caso, se acogerá lo dispuesto en las convenciones internacionales vigentes en la República del Ecuador sobre la materia.

5. Para detener a las personas prófugas que se han refugiado en una nave o en una aeronave extranjera que se halle en territorio ecuatoriano, la reclamación de entrega se hará, según las disposiciones del numeral anterior, inclusive en los casos de negativa o silencio del comandante de la nave o aeronave.

SECCIÓN TERCERA
Técnicas especiales de investigación

Artículo 483.- Operaciones encubiertas.- En el curso de las investigaciones de manera excepcional, bajo la dirección de la unidad especializada de la Fiscalía, se podrá planificar y ejecutar con el

5. No se podrá hacer uso procesal o extraprocesal de ninguno de los datos que suministren los documentos si versan sobre asuntos que no tienen relación con el proceso.

6. Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código.

Artículo 500.- Contenido digital.- El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.

En la investigación se seguirán las siguientes reglas:

1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.

2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.

4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.

SECCIÓN SEGUNDA
El testimonio

Artículo 501.- Testimonio.- El testimonio es el medio a través del cual se conoce la declaración de la persona procesada, la víctima y de otras personas que han presenciado el hecho o conocen sobre las circunstancias del cometimiento de la infracción penal.

y comparecencia a la audiencia de juicio, en la que puedan rendir su testimonio a través de medios tecnológicos o de caracterización que aseguren su integridad.

10. El testimonio se practicará en la audiencia de juicio, ya sea en forma directa o a través de videoconferencia, con excepción de los testimonios anticipados.

11. Las o los servidores públicos que gozan de fuero de Corte Nacional, podrán rendir su testimonio mediante informe juramentado.

12. Quienes rindan testimonio deberán informar sobre sus nombres, apellidos, edad, nacionalidad, domicilio o residencia, estado civil, oficio o profesión, salvo el caso del testigo protegido, informante, agente encubierto o persona cuya integridad se encuentre en riesgo. Permanecerán en un lugar aislado, declaran individualmente y de forma separada de modo que no puedan oír mutuamente sus declaraciones.

13. Al momento de rendir testimonio, se prestará juramento en todo cuanto conoce y se es preguntada. Se le advertirá sobre las penas con las cuales será sancionado el perjurio.

14. Los sujetos procesales podrán realizar preguntas u objetarlas, y la o el juzgador deberán resolver la objeción para que la persona las conteste o se abstenga de hacerlo.

15. No se podrán formular preguntas autoincriminatorias, engañosas, capciosas o impertinentes.

16. No se podrán formular preguntas sugestivas en el interrogatorio, excepto cuando se trate de una pregunta introductoria o que recapitule información ya entregada por el mismo declarante.

17. Podrán hacerse preguntas sugestivas durante el contra examen.

Artículo 503.- Testimonio de terceros.- El testimonio de terceros se regirá por las siguientes reglas:

1. Los terceros que no sean sujetos ni partes del proceso, que conozcan de una infracción, serán obligados a comparecer personalmente a rendir su testimonio. Se podrá hacer uso de la fuerza pública para la comparecencia del testigo que no cumpla esta obligación.

2. No se recibirá las declaraciones de las personas depositarias de un secreto en razón de su profesión, oficio o función, si estas versan sobre la materia del secreto. En caso de haber sido convocadas, deberán comparecer para explicar el motivo del cual surge la obligación y abstenerse de declarar pero únicamente en lo que se refiere al secreto o reserva de fuente.

3. Las y los testigos o peritos volverán a declarar cuantas veces lo ordene la o el juzgador en la audiencia de juicio.

4. Cuando existan más de veinte testigos y peritos, la o el juzgador con los sujetos procesales determinarán cuántos y quiénes comparecerán por día.

5. Cuando existan varios testimonios o peritos en la misma causa, los testimonios se recibirán por separado, evitándose que se comuniquen entre sí, para lo cual permanecerán en un lugar aislado.

Artículo 504.- Versión o testimonio de niñas, niños o adolescentes, personas con discapacidad y adultos mayores.- Las niñas, niños o adolescentes, personas con discapacidad y adultos mayores, tendrán derecho a que su comparecencia ante la o el juzgador o fiscal, sea de forma adecuada a su situación y desarrollo evolutivo. Para el cumplimiento de este derecho se utilizarán elementos técnicos tales como circuitos cerrados de televisión, videoconferencia o similares, por una sola vez. Se incorporará como prueba la grabación de la declaración en la audiencia de juicio.

Artículo 505.- Testimonio de peritos.- Los peritos sustentarán oralmente los resultados de sus peritajes y responderán al interrogatorio y al contrainterrogatorio de los sujetos procesales.

Artículo 506.- Detención de testigos por falso testimonio y perjurio.- La o el juzgador ordenará la detención de un testigo por falso testimonio o perjurio y deberá remitir lo pertinente a la o al fiscal para su investigación.

PARÁGRAFO PRIMERO
Testimonio de la persona procesada

Artículo 507.- Reglas.- La persona procesada podrá rendir testimonio en la audiencia de juicio, de conformidad con las siguientes reglas:

1. El testimonio de la persona procesada es un medio de defensa.

2. La persona procesada no podrá ser obligada a rendir testimonio, ni se ejercerá en su contra coacción o amenaza, ni medio alguno para obligarlo o inducirlo a rendir su testimonio contra su voluntad.

3. Si decide dar el testimonio, en ningún caso se le requerirá juramento o promesa de decir la verdad, pudiendo los sujetos procesales interrogarlo.

4. La persona procesada tendrá derecho a contar con una o un defensor público o privado y a ser asesorada antes de rendir su testimonio.

5. La persona procesada deberá ser instruida por la o el juzgador sobre sus derechos.

6. La inobservancia de las reglas establecidas en los numerales 2 y 3 hará nulo el acto, sin perjuicio de la responsabilidad disciplinaria que corresponda.

el testimonio será receptado con el acompañamiento de personal capacitado en atención a víctimas en crisis, tales como psicólogos, trabajadores sociales, psiquiatras o terapeutas, entre otros. Esta norma se aplicará especialmente en los casos en que la víctima sea niña, niño, adolescente, adulto mayor o persona con discapacidad.

PARÁGRAFO TERCERO
La pericia

Artículo 511.- Reglas generales.- Las y los peritos deberán:

1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.

2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.

3. La persona designada deberá excusarse si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.

4. Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.

5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.

6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.

7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes y contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.

8. El Consejo de la Judicatura organizará el sistema pericial a nivel nacional, el monto que se cobre por estas diligencias judiciales o procesales, podrán ser canceladas por el Consejo de la Judicatura.

De no existir persona acreditada como perito en determinadas áreas, se deberá contar con quien tenga conocimiento, especialidad, experticia o título que acredite su capacidad para desarrollar el peritaje. Para los casos de mala práctica profesional la o el fiscal solicitará una terna de profesionales con la especialidad correspondiente al organismo rector de la materia.

Cuando en la investigación intervengan peritos internacionales, sus informes podrán ser incorporados como prueba, a través de testimonios anticipados o podrán ser receptados mediante video conferencias de acuerdo a las reglas del presente Código.

CAPÍTULO CUARTO
REGLAS PARA LA INVESTIGACIÓN DE DELITOS COMETIDOS MEDIANTE LOS MEDIOS DE COMUNICACIÓN SOCIAL

Artículo 512.- Reglas especiales.- Para la investigación de los delitos cometidos por medios de comunicación social, se aplicarán las normas generales de este Código y además las reglas especiales previstas en este Capítulo.

Artículo 513.- Responsabilidad.- Las o los directores, editores, propietarios o responsables de un medio de comunicación social responderán por la infracción que se juzga y contra él se deberá seguir la causa, si a pedido de la o el fiscal no manifiesta el nombre de la o el autor, reproductor o responsable de la publicación.

Igualmente serán responsables cuando la o el autor de la publicación resulte o sea persona supuesta o desconocida.

Artículo 514.- Remisión.- Las o los directores, administradores o propietarios de las estaciones de radio y televisión, estarán obligados a remitir, cuando la o el fiscal lo requiera, los filmes, las videocintas o las grabaciones de sonidos. De no hacerlo, el proceso se seguirá contra ellos.

La o el fiscal concederá el plazo de tres días para la remisión, previniéndole de su responsabilidad en caso de incumplimiento.

Artículo 515.- Exhibición previa.- Antes del ejercicio de la acción penal, la o el fiscal de oficio o a petición de la persona que se considere afectada deberá requerir al o el director, editor, propietario o responsable del medio de comunicación, para que informe el nombre de la o el autor o responsable del escrito, enviando una copia del mismo. En los demás casos deberá pedir además del nombre, la remisión de los filmes, videocintas y grabaciones mencionadas anteriormente.

Artículo 516.- Transcripción del original.- La presentación del original cuando el delito se cometa por medio de la radiodifusión o la televisión podrá suplirse con una transcripción judicial obtenida de la grabación.

Artículo 517.- Comienzo de la instrucción o del juicio.- Exhibido el original de la cinta o la grabación y realizado el peritaje correspondiente, si se trata de un delito de ejercicio público de la acción, la o el fiscal solicitará día y hora para formular cargos.

CAPÍTULO TERCERO
RECURSO DE CASACIÓN

Artículo 656.- Procedencia.- El recurso de casación es de competencia de la Corte Nacional de Justicia y procederá contra las sentencias, cuando se haya violado la ley, ya por contravenir expresamente a su texto, ya por haber hecho una indebida aplicación de ella, o por haberla interpretado erróneamente.

No son admisibles los recursos que contengan pedidos de revisión de los hechos del caso concreto, ni de nueva valoración de la prueba.

Artículo 657.- Trámite.- El recurso de casación podrá interponerse por los sujetos procesales, de acuerdo con las siguientes reglas:

1. Dentro de los cinco días hábiles contados a partir de la notificación de la sentencia. La o el juzgador remitirá el proceso a la Corte Nacional de Justicia, en el plazo máximo de tres días hábiles, una vez ejecutoriada la providencia que la conceda.

2. El tribunal designado por sorteo, dentro del plazo de tres días convocará a audiencia. De rechazar el recurso, ordenará su devolución a la o al juzgador de origen. De estas decisiones, no hay recurso alguno.

3. El recurso se sustanciará y resolverá en audiencia que se realizará dentro del plazo de cinco días contados desde la convocatoria. El recurrente deberá fundamentar su pretensión y los otros sujetos procesales se pronunciarán sobre la misma.

4. El recurso interpuesto por la o el fiscal, lo fundamentará en audiencia la o el Fiscal General del Estado o su delegada o delegado.

5. Si se estima procedente el recurso, se pronunciará sentencia enmendando la violación a la ley. De estimar improcedente, se declarará así en sentencia.

6. Si se observa que la sentencia ha violado la ley, aunque la fundamentación del recurrente sea equivocada, de oficio se la admitirá.

7. La sentencia se notifica dentro de los tres días de finalizada la audiencia.

8. El proceso se devolverá a la o al juzgador o tribunal respectivo para la ejecución de la sentencia.

CAPÍTULO CUARTO
RECURSO DE REVISIÓN

Artículo 658.- Procedencia.- El recurso de revisión podrá proponerse en cualquier tiempo, ante la Corte Nacional de Justicia, después de ejecutoriada la sentencia condenatoria por una de las siguientes causas:

1. Si se comprueba la existencia de la persona que se creía muerta.

2. Si existen, simultáneamente, dos sentencias condenatorias sobre una misma infracción contra diversas personas sentenciadas que, por ser contradictorias, revelen que una de ellas está errada.

3. Si la sentencia se ha dictado en virtud de documentos o testigos falsos o de informes periciales maliciosos o errados.

La revisión solo podrá declararse en virtud de nuevas pruebas que demuestren el error de hecho de la sentencia impugnada.

No serán admisibles los testimonios de las personas que declaren en la audiencia de juicio.

La interposición de este recurso no suspende la ejecución de la sentencia.

Artículo 659.- Recurrente.- El recurso de revisión podrá ser interpuesto por la persona condenada, por cualquier persona o por la o el mismo juzgador, si aparece la persona que se creía muerta o se presentan pruebas que justifiquen su existencia, con posterioridad a la fecha del cometimiento del supuesto delito.

En los demás casos, solo podrá interponer el recurso la persona condenada y si ha fallecido, podrán hacerlo su cónyuge, su pareja en unión de hecho, sus hijos, sus parientes o herederos.

El escrito de interposición del recurso será fundamentado y contendrá la petición o inclusión de nuevas pruebas, caso contrario se declarará inadmisible y se lo desechará sin lugar a uno nuevo por la misma causa.

Cuando se haya declarado el abandono del recurso, no se podrá admitir uno nuevo por las mismas causas.

Artículo 660.- Trámite.- El recurso de revisión deberá tramitarse de acuerdo con las siguientes reglas:

1. Recibido el expediente, en el plazo máximo de cinco días, se pondrá en conocimiento de las partes la recepción del proceso y en la misma providencia se señalará día y hora en que se celebrará la audiencia.

2. Si la revisión es de una sentencia dictada en un proceso de ejercicio público de la acción, se contará con la intervención de la o el Fiscal General del Estado, o su delegada o delegado.

3. En la audiencia, los sujetos procesales expondrán sus fundamentos y practican [sic] las pruebas solicitadas. La resolución se anunciará en la misma audiencia, debiendo notificarla dentro de los tres días siguientes.

4. El rechazo de la revisión, no impedirá que pueda proponerse una nueva, fundamentada en una causa diferente.