UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE ARQUITECTURA E INGENIERIAS

Plan de Investigación de fin de carrera titulado:

"DISEÑO DE UNA METODOLOGÍA PARA EL ANÁLISIS FORENSE DE CONSOLAS DE VIDEOJUEGOS PLAY STATION 4 SLIM"

Realizado por:

ANGEL DANIEL UCHUARY JIMÉNEZ

Director del proyecto:

Ing. Luis Fabián Hurtado Vargas, MG

Como requisito para la obtención del título de:

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

DECLARATORIA

El presente trabajo de investigación titulado:

"DISEÑO DE UNA METODOLOGÍA PARA EL ANÁLISIS FORENSE DE CONSOLAS DE VIDEOJUEGOS PLAY STATION 4 SLIM"

Realizado por:

ING. ANGEL DANIEL UCHUARY JIMENEZ

Como requisito para la Obtención del Título de:

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

Ha sido dirigido por el profesor

Ing. Luis Fabián Hurtado Vargas, MG.

Quien considera que constituye un trabajo original de su autor

Ing. Luis Fabián Hurtado Vargas, MG.
DIRECTOR

PROFESORES INFORMANTES

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

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

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

Quito, 14 de septiembre del 2018

DEDICATORIA

Dedico este trabajo a mi amada madre María, quien con su ejemplo e incansable apoyo he podido cumplir todas las metas que me he propuesto; a mi amado padre Ángel, quien con sus palabras de aliento me ha impulsado a ser un gran profesional.

A mis cariñosas hermanas, Lenny que me motivó a salir y buscar nuevos rumbos sin tener miedo, María quien me ha dado la fortaleza necesaria para iniciar esta etapa que hoy estoy culminando, Diana quien con sus consejos me ha acompaño en cada decisión de mi vida, a mis queridos hermanos Manuel y Carlos, quienes han sido mis confidentes y sobre todo un ejemplo a seguir.

A mi cuñado Enrique, mi gran amigo; a mis cuñadas Cristina y Lizbeth, quienes nunca les falta una sonrisa; a mis lindos sobrinos Javier, Jorge, Martín, Sebastián, Yuri y mis tiernas sobrinas María, Mariángel, Isis, Lucía, Sofía; gracias por ser mi motivación y mi inspiración a ser cada día mejor.

A Daniela, gracias por tu cariño y amor incondicional, por tu comprensión, por tu paciencia, por tu apoyo, gracias por convertirte en mi paz y mi aliento en esta fuerte pero satisfactoria etapa de mi vida.

A mis grandes amigos, Miguel, Hernán y Jaime, gracias por su sincera amistad y su apoyo infalible; a mis compañeros, especialmente a Freddy y Eduardo con quienes iniciamos esta etapa que hoy culminamos y hemos formado un gran lazo de amistad.

AGRADECIMIENTOS

Son muchas las personas especiales a las que me gustaría agradecer su amistad, apoyo, ánimo y compañía en las diferentes etapas de mi vida. Algunas están aquí conmigo y otros en mis recuerdos y en el corazón. Sin importar en donde estén o si alguna vez llegan a leer esto quiero darles gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

El mayor agradecimiento a mis padres, por el esfuerzo que hicieron para darme una profesión y formar en mí, una persona de bien, gracias por todos los sacrificios y la paciencia que demostraron todos estos años de mi vida universitaria.

De manera especial al Ing. Diego Riofrio y al Ing. Fabian Hurtado por ser grandes mentores y guías durante el desarrollo de esta tesis. A la Universidad Internacional SEK, por su esfuerzo en formar profesionales con visión y enfoque empresarial.

A mi grupo de amigos por haber compartido conmigo estos últimos 2 años, de amistad y camaradería, gracias por las horas de compañía. Nombrar sería muy extenso y podría cometer algún olvido injusto, por ello, ¡Gracias amigos por estar ahí!

RESUMEN

Actualmente en el Ecuador es ya común escuchar sobre el término delitos informáticos; según la Fiscalía General del Estado éste se ha ido inmiscuyendo en la sociedad de manera espontánea, y ha tenido un crecimiento alarmante en los últimos años, ocasionando un elevado número de denuncias por un sinnúmero de casos; uno de los puntos débiles de nuestro Sistema Pericial del Ecuador es la poca o casi nula información que se tiene al momento de extraer la información digital contenida en los dispositivos especiales donde se realiza la pericia.

Uno de los casos particulares, son las consolas de videojuegos, ya que, el Sistema Pericial no cuenta con metodologías específicas para cada tipo de dispositivo a analizar. Las consolas de videojuegos y en especial la PS4 Slim, tiene una gran penetración en la sociedad y mayormente en el público de menor edad, según la empresa Statista han alcanzado ventas superiores a los 50 Millones de unidades (Moreno, 2016). Estas consolas no solo son usadas por hobby o simplemente por entretenimiento; sino por un sinnúmero de aplicaciones, como redes sociales o chats en vivo, lo que permite tener un nuevo vector de ataque para posibles delitos, que pueden ir desde la extorsión hasta la pornografía infantil.

En la presente investigación, se determina los tipos de delitos informáticos que pueden ser perpetrados usando una Play Station 4 Slim. Para esto primero se evaluó las vulnerabilidades de la consola en cada aplicación y servicio que brinda. Además, se realizó una comparativa con la consola Xbox One con el fin de validar la presente investigación en relación a trabajos similares. Se diseña una metodología de análisis forense específica para la consola PS4, considerando que los datos digitales y arquitectura de la consola es desconocida por peritos informáticos del Ecuador, por lo que para el diseño de la misma se usa un lenguaje claro, entendible y basado en las leyes y normativas del Ecuador.

Finalmente se presenta una guía de pasos para el análisis forense de los datos digitales contenidos en la consola de videojuegos Play Station 4 Slim, que pueda ser aplicada por peritos informáticos del Ecuador y llevada como una prueba valida en casos de juicio, sea civil o penal.

Palabras clave: Análisis Forense, Consola, Metodología, PlayStation 4, Videojuegos.

ABSTRACT

Currently in Ecuador it has become common to hear about the term cybercrime. According to Ecuador Attorney General, cybercrime has been getting spontaneously into society and grows exponentially in recent years, causing an increasing number of complaints for a number of cases. One of the weakest parts of the Ecuador Judiciary System is the little or lack of information available at the moment of extracting digital information stored in electronic devices where the analysis takes place.

One of the particular cases are videogame consoles, in which the Judiciary System does not have a methodology for every type of console existing for analysis. Videogame consoles are very popular in society, especially in minors. One of this consoles is the PS4 Slim which according to Statista have reached over 50 million units globally in sales (Moreno, 2016). These consoles are not used only for gaming and as a hobby, but now they implement a large number of applications for many purposes like social networks, live chats and streaming. This open a way for possible crimes such as child pornography.

In this research, it will be determined which cybercrime types are executed using a PS4 Slim. For this the vulnerabilities of each console's applications and services were evaluated. Furthermore, a comparative work with Xbox One console was made with the purpose of validating the present research according to the work already done in similar research. A forensic analysis methodology was designed for the gaming console PS4 Slim, considering that the digital data and architecture of the console are completely unknown to the cybercrime experts of Ecuador, so the research is written in plane and clear language, understandable and based on laws and standards of Ecuadorian regulations.

Finally, a step by step guide is presented for the forensic analysis of the digital information stored within the videogame console PS4 Slim, that can be used for Ecuador cybercrime experts and carried as a valid evidence for Civil or Criminal justice trials.

Keywords: Forensic Analysis, Console, Methodology, Videogame, Play Station 4.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS Y FIGURAS

CAPÍTULO I

INTRODUCCIÓN

1.1 PROBLEMA DE LA INVESTIGACIÓN

1.1.1. Planteamiento del problema

La poca o nula información que se tiene en el sistema pericial del Ecuador para poder extraer la información digital contenida en la consola de videojuegos Play Station 4 Slim, ocasiona que se creen nuevas ventanas por los cuales agentes externos puedan cometer delitos, esto está ligado a las nuevas funcionalidades de este dispositivo y al poco control por parte de los padres.

1.1.2. Diagnóstico del Problema

En los últimos años se ha tenido un elevado crecimiento del uso de consolas de videojuegos, principalmente en jóvenes y niños de edades escolares, lo que ha dado como resultado a un aumento en los delitos informáticos que son cometidos usando estos dispositivos (Aguinaga, 2016). Las consolas de videojuegos, en especial la consola Play Station 4 Slim, contiene nuevas herramientas y aplicaciones que brindan la posibilidad de una comunicación directa, redes sociales y compartición de información, que da como resultado un aumento en los delitos perpetrados por estos medios electrónicos.

En nuestro sistema pericial actual se procesa gran cantidad de información que esta almacenada de manera digital en computadores, teléfonos celulares y dispositivos comunes que contienen un disco duro o memorias del tipo Ram; para realizar estos procedimientos se cuentan con metodologías ya establecidas para la obtención de la evidencia digital en procesos judiciales. Pero, uno de los más grandes problemas que existen actualmente, es que no se cuenta con una metodología específica para extraer evidencia digital de dispositivos especiales como es el caso de las consolas de videojuegos y en específico el Play Station 4 Slim, ya que, en el departamento de Ciencias Forenses de la Policía Nacional no se cuenta con un conocimiento total de su arquitectura y de los datos digitales que en estas se almacenan.

Los delitos informáticos crecen a un ritmo acelerado, como lo describe Cuenca (2016) en su investigación sobre el delito informático en el Ecuador, donde las persona detrás de estos, buscan nuevos medios, métodos y acciones para poder llegar a su objetivo,

siempre buscando vacíos legales que les permitan cometer sus delitos sin ser detectados o mucho peor quedando impunes por la falta de pruebas o la omisión de las mismas.

Un delito informático se puede definir como aquel que en su concepción es perpetrado desde un dispositivo que tenga procesamiento y almacenamiento. Los delitos según la Organización de las Naciones Unidas en el documento de Iriarte (2008), van desde la pornografía infantil hasta el ciberterrorismo. En el Ecuador existen leyes para tratar de contrarrestar estos problemas, como por ejemplo el Código Orgánico Integral Penal, la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos, etc.

Sacando una pequeña muestra, en el Código Orgánico Integral Penal (COIP), existen artículos donde se habla sobre delitos informáticos, como por ejemplo en la SECCIÓN TERCERA: Delitos contra la seguridad de los activos de los sistemas de información y comunicación, estos son:

- Artículo 229.- Revelación ilegal de base de datos,
- Artículo 230.- Intercepción ilegal de datos,
- Artículo 231.- Transferencia electrónica de activo patrimonial,
- Artículo 232.- Ataque a la integridad de sistemas informáticos,
- Artículo 233.- Delitos contra la información pública reservada legalmente,
- Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Como estos artículos, también existen muchos más en otras leyes ecuatorianas, donde se determinan los delitos informáticos en muchos aspectos, formas y manera de cometerlos, así como las penas privativas de libertad de acuerdo al daño o agravio cometido; estos artículos no especifican los dispositivos por donde se puede cometer el delito, dejando un amplio espectro de posibilidades para que el atacante pueda realizar su objetivo.

En el Ecuador se cuenta con una completa tipificación de los delitos informáticos, pero no con los medios o dispositivos por donde se pueden cometer este tipo de delitos, dejando vacíos legales que son aprovechados por los atacantes. Cuando se llega a judicializar un caso, es necesario una extracción de los datos contenidos de manera digital, pero lastimosamente muchos de los delitos informáticos que son denunciados quedan en la impunidad o no se consideran las pruebas por la falta de conocimiento o una metodología que permita extraer la información contenida como lo señala el autor Córdova (2018), en su investigación determina que los peritos poseen títulos acordes al tipo de pericia a que se va a practicar, pero no se puede descartar que dichos peritos posean algún tipo de formación sobre el funcionamiento o la arquitectura de consolas de videojuegos y del tipo de información que se guardan en las mismas.

En el departamento de Ciencias Forenses de la Policía Nacional, se cuenta con muy pocas metodologías para la extracción de datos digitales, por ejemplo para la extracción de datos digitales de teléfonos celulares, computadores y algunos dispositivos que contengan una memoria Ram o un disco duro, procesos no estandarizados para el tipo de dispositivos al cual se pueden aplicar; determinando así que existen una carencia de metodologías y guías para el análisis forenses en consolas de videojuegos.

1.1.3. Pronóstico

Como se puede ver existe un desconocimiento y una falta de metodologías específicas para la extracción de imágenes forenses de dispositivos "especiales", como es el caso de la consola de videojuegos Play Station 4 Slim, el número de delitos, denuncias y casos en impunidad van a seguir en aumento, afectando de manera directa a las personas que cuentan con estas consolas para su diversión, confiando en que un sistema judicial los protegerá ante cualquier caso en el que esta consola sea usada como medio, herramienta o fin para cometer un delito.

1.1.4. Control de Pronóstico

Uno de los mayores problemas del sistema Judicial del Ecuador y específicamente en el departamento de Ciencias Forenses de la Policía Nacional, es que no existen una correcta estandarización de metodologías forenses aplicables a dispositivos específicos, donde, para resolver este problema, primero se lleva a cabo un análisis de los servicios y aplicaciones que brinda el dispositivo, permitiendo reconocer los tipos de delitos que pueden ser cometidos usando la consola de videojuegos Play Station 4 Slim.

Una vez determinados los delitos, se realizará una investigación sobre los tipos de metodologías de análisis forense existentes, para así poder seleccionar la que mejor que acople a nuestras necesidades, considerando la norma de manejo de la evidencia e integridad de datos. Finalmente se analizarán los datos obtenidos, para así elaborar una metodología específica para la consola de videojuegos Play Station 4 Slim, y la documentación de los pasos a realizados, para que puedan ser usados como una guía para futuros delitos.

1.1.5. Formulación del Problema

La falta de una metodología de análisis forense en consolas de videojuegos Play Station 4 Slim, influye en la resolución de un proceso judicial, cuando la evidencia fue omitida en casos de delitos informáticos perpetrados en estos dispositivos.

1.2 OBJETIVOS

1.2.1. Objetivo General

Diseñar una metodología específica para el análisis forense de consolas de videojuegos Play Station 4 Slim, mediante el uso de técnicas forenses existentes para la extracción de datos digitales.

1.2.2. Objetivos Específicos

- Reconocer los tipos de delitos informáticos que pueden darse usando la consola Play Station 4 Slim, para trazar una línea base como referencia de la información digital a extraer.
- Comparar las características de la consola Play Station 4 de su referente Xbox One, a fin de identificar rasgos únicos que definan a la consola, para determinar el procedimiento de análisis forense a utilizar.
- Analizar los datos extraídos de la Play Station 4, mediante la clasificación de la información analizada para la desmaterialización de la evidencia.
- Desarrollar una guía de pasos para el análisis forense de la consola de videojuegos Play Station 4, para ser utilizada en análisis periciales de futuros casos.

1.3 JUSTIFICACIÓN

1.3.1. Teórica

La investigación que se propone se realiza con el propósito de contribuir en gran medida a las metodologías ya existentes para el análisis forense de dispositivos electrónicos, cuyos resultados se podrán normalizar en una propuesta que puede incluirse como conocimiento a las ciencias forenses de Sistema Pericial Integral de la Función Judicial del Ecuador.

1.3.2. Metodológica

Para cumplir los requerimientos de la presente investigación, se hace empleo de técnicas, métodos científicos y pruebas piloto. Con estas técnicas se pretende lograr, mediante la exploración, como los datos e información digital contenida dentro de una consola Play Station 4 Slim pueden ser extraídos, se hará uso de metodologías de análisis forenses existentes que permitirán conservar y mantener la integridad de los datos, con el fin de obtener una metodología especifica que sirva como base para la resolución de procesos judiciales donde se tenga como evidencia una consola de videojuegos.

1.3.3. Práctica

Con relación a los objetivos, esta investigación se realiza porque existe la necesidad de mejorar el nivel de conocimiento y experticia de los peritos que pertenecen al Sistema Pericial Integral de la Función Judicial del Ecuador, con el uso de una metodología clara y sistemática aplicable a las consolas de videojuegos Play Station 4 Slim.

1.3.4. Relevancia Social

La presente investigación cuenta con un gran aporte social, se centra en las personas que sean víctimas de un delito informático, donde sea usado como medio, instrumento o fin una consola de videojuegos PS4 Slim, para que puedan obtener la mayor confiabilidad de un Sistema Judicial, cuando la evidencia obtenida tenga el tratamiento adecuado para ser resuelta en su brevedad.

Además, a las personas que están dentro del Sistema Pericial, como son los peritos Informáticos, los mismos que obtendrán el conocimiento tanto científico como teórico, que les permitirá resolver de mejor manera los casos donde se encuentren con este tipo de dispositivos, obteniendo la evidencia digital para su posterior redacción del informe pericial; a los Jueces y Fiscales para que puedan tener un conocimiento claro sobre los informes presentados por los Peritos informáticos, para que no exista la omisión de la prueba y poder tener una resolución que se ajuste a una real justicia social.

1.4 MARCO TEÓRICO

1.4.1. Delitos Informáticos

El delito informático se considera como toda acción fuera de la ley, que se realiza usando un dispositivo informático como método, medio o fin; y en un sentido más estricto, se puede definir como un acto ilícito penal que busca destruir, modificar, dañar o irrumpir la información contenida en dispositivos de almacenamiento, medios electrónicos o en redes de Internet.

La Organización de las Naciones Unidas (ONU), reconoce los delitos informáticos de acuerdo a una clasificación, esta se divide en secciones de acuerdo al acto cometido. (Estrada, 2008)

Tipos de Delitos informáticos de acuerdo a la ONU

a) Fraudes cometidos mediante manipulación de computadoras.
    - Manipulación de los datos de entrada

- La manipulación de programas
- Manipulación de los datos de salida
- Fraude efectuado por manipulación informática

b) Falsificaciones informáticas.
   - Como objeto
   - Como instrumento

c) Daños o modificaciones de programas o datos computarizados
   - Sabotaje informático
     i. Virus
     ii. Gusanos
     iii. Bomba lógica o cronológica
   - Acceso no autorizado a servicios y sistemas informáticos
     i. Piratas informáticos o hackers
   - Reproducción no autorizada de programas informáticos de protección legal

Además, existen otros tipos de delitos que los tipifica de acuerdo a acciones, como:

a) Directamente contra los propios sistemas
   - Acceso no autorizado.
   - Destrucción de datos.
   - Infracción al copyright de bases de datos.
   - Interceptación de correo electrónico.
   - Estafas electrónicas.
   - Transferencias de fondos.

b) A través de la red de Internet

   - Espionaje.
   - Terrorismo.
   - Narcotráfico.
   - Tráfico de armas.
   - Proselitismo de sectas.
   - Propaganda de grupos extremistas

1.4.2. Situación actual en el Ecuador

En el Ecuador, la Fiscalía General del Estado recepta denuncias por delitos informáticos de manera constante; solo en el periodo del 2016 al 2017 registro 530 delitos informáticos, donde la denuncia más común es la de apropiación fraudulenta por medios electrónicos. (Telégrafo, 2017)

El Ecucert (Centro de respuestas a incidentes informáticos del Ecuador), determinó que la mayoría de los ataques a los sistemas informáticos se deben a errores de los usuarios al acceder a sus redes sociales, brindar información personal o uso de credenciales en sus cuentas personales. Se reportó que los mayores casos se deben a (Ecucert, 2018):

- Personas que dejan sus teléfonos móviles con información laboral en sus vehículos o lugares de trabajo.
- Utiliza el mismo password en dispositivos laborales y personales.
- Descargas de archivos desconocidos vía correo.
- Respaldar información laboral en la nube
- Mal uso de las redes sociales

Uno de los mayores errores cometidos a través de las redes sociales, es brindar información personal en enlaces que ofrecen premios o promociones, donde se solicita al usuario información relevante para el atacante; un caso que tuvo mucho auge se dio en el segundo semestre del 2017 donde se solicitaba información de tarjetas de crédito por videos sexuales de celebridades, o por grabaciones de videochat.

Cabe destacar que la investigación de estos delitos informáticos se lleva a cabo con procedimientos técnicos, peritajes e intercepción de comunicaciones. Proveedores de redes sociales o buscadores tienen sus bancos de datos en los Estados Unidos, lo que dificulta en gran medida a las investigaciones, derivando muchas veces en la solicitud de asistencia internacional para obtener la información.

En el Ecuador se cuenta con leyes y normativas que tipifican este tipo de delitos informáticos, los mismos que en sus artículos tratan sobre el tipo de delito, la pena privativa de libertad y compensación económica. Estas normativas son:

- Código Orgánico Integral Penal (COIP).
- Código Orgánico General de Procesos (COGEP).
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Se cuenta con una Resolución que determina el funcionamiento y administración del Sistema Pericial Integral, como es la Resolución 040-2014.

1.4.3. Resolución 040 – 2014

La normativa legal en el Ecuador se rige por resoluciones especiales de acuerdo a la materia de análisis de las mismas, la resolución 040-2014 fue expedida por el Pleno del Consejo de la Judicatura con fecha 10 de marzo del 2014, donde se remitió el proyecto final para el Reglamento que regula el Sistema Pericial Integral de la Función judicial, el mismo que fue expedido e inscrito en el registro oficial. (Consejo de la Judicatura, 2014)

El reglamento, de acuerdo al Artículo 1 de la misma permite conocer el ámbito de aplicación, el cual señala que: "Este reglamento regulará el funcionamiento y administración del sistema pericial integral, en relación a la calificación, designación, obligaciones, evaluación, capacitación, régimen disciplinarlo y cualquier otro aspecto de los peritos que participen en los procesos judiciales, pre procesales, o de cualquier otra naturaleza que se lleven a cabo en la Función Judicial." (Consejo de la Judicatura, 2014)

Este reglamento consta de varios capítulos como son:

- Capítulo 1, Ámbito de aplicación y principios. – consta de 3 artículos numerados en temas de ámbito de aplicación, principios y calidad del perito. En principios, se habla sobre que el reglamento mantendrá la calificación de los peritos en términos de igualdad, no discriminación hasta llegar a la transparencia y libre acceso a la información.
- Capítulo 2, Calificación de Peritos. - consta de 8 artículos, donde principalmente se trata de los requisitos de acreditación de los peritos informáticos, específicamente en el Artículo 4; además de contar con artículos que tratan temas de las inhabilidades y prohibiciones para la calificación pericial, documentación procedimiento y otorgamiento de la calificación.
- Capítulo 3, Designación de Peritos. – permite conocer sobre la designación de los peritos siguiendo principios de profesionalismo, transparencia e igualdad; además de conocer los procedimientos para designación y posesión.
- Capítulo 4, Obligaciones de los Peritos. – permite conocer el ámbito de responsabilidad de los peritos, los mismos que son auxiliares de la justicia y deben mantener los principios de ética exceptuando juicios de valor.
- Capítulo 5, Informe Pericial. – este capítulo trata sobre la estructura, forma y contenido de un informe pericial.
- Capítulo 6, Honorarios de Peritos. – enmarcados principalmente en la designación y formas de pago con montos de acuerdo al caso y especialidad del perito y caso
- Capítulo 7, Evaluación de Peritos. – tiene como objetivo la evaluación y control del cumplimiento de las obligaciones de los peritos.
- Capítulo 8, Capacitación de los Peritos.

- Capítulo 9, Régimen Disciplinario de los Peritos.

Además, consta con disposiciones generales y transitorias las cuales son de aplicación obligatoria. Finalmente, con disposiciones derogativas y una final. (Consejo de la Judicatura, 2014)

1.4.4. Consola de videojuegos PS4 Slim

La consola de videojuegos PS4 Slim, es una de las consolas más vendidas en el mundo según la empresa Statista, llegan a tener 50 millones de unidades vendidas desde su lanzamiento (Moreno, 2016). La consola cuenta con características de alta gama y última generación, estas características se presentan a continuación:

Tabla 1. Características técnicas de una PS4
Fuente: https://www.playstation.com/es-es/explore/ps4/tech-specs/

Nombre del producto	**PlayStation®4**
Código del producto	Serie CUH-2000
Procesador principal	Procesador personalizado de un chip CPU: AMD 'Jaguar' x86-64, 8 núcleos GPU: motor gráfico AMD de 1,84 TFLOPS basado en Radeon™
Memoria	8 GB GDDR5
Capacidad de almacenamiento*	500 GB, 1 TB
Dimensiones externas	Aprox. 265 × 39 × 288 mm (ancho × alto × largo) (excluye la proyección de mayor tamaño)
Peso	Aprox. 2,1 kg
Unidad BD/DVD (solo lectura)	BD de 6 CAV DVD de 8 CAV
Entrada/Salida	2 puertos de altísima velocidad USB (USB 3.1 Gen1) 1 puerto AUX
Red	1 puerto Ethernet (10BASE-T, 100BASE-TX, 1000BASE-T) IEEE 802.11 a/b/g/n/ac Bluetooth® 4.0
Alimentación	AC de 100-240 V, 50/60 Hz
Consumo de energía	Máx. 165 W
Temperatura de funcionamiento	5 ºC - 35 ºC
Salida AV	Salida HDMI™ (compatible con salida HDR)

1.4.5. Informática Forense

Es una rama de la informática, y específicamente del área judicial que permite mediante el uso de técnicas y herramientas extraer la información valiosa de equipos informáticos, con el objetivo de no alterar el estado de los mismos.

De acuerdo al criterio de Porolli (2013), el cual es su investigación determina que la informática forense, "Permite buscar datos que son conocidos previamente, tratando de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta."

1.4.6. UNE 71506:2013 Sistema de Gestión de Evidencias Electrónicas (SGEE)

En el boletín oficial del Estado (BOE) de España, con fecha 1 de octubre del 2013 con número 235, se publica la resolución del 23 de septiembre del 2013, donde se publica las normas UNE que se aprueban con el AENOR. Estas normas son referentes a las Tecnologías de la Información de acuerdo al sistema de gestión de evidencias electrónicas (SGEE), donde se hace una contribución a la homogenización de las evidencias electrónicas y se establece el marco de referencias de las buenas prácticas para la recepción de estas pruebas en los procesos judiciales que sean utilizadas. (Jinza, 2013)

La norma tiene como objetivo principal establecer la metodología para (AENOR, 2013):

- **Preservación. –** Se trata de identificar todas las fuentes potenciales de evidencia digital, tomar fotografías, determinar topologías y configuraciones; una vez realizado esto, se preserva la información y equipos siguiendo las pautas de la cadena de custodia de la Policía Nacional, donde se evita la contaminación de la prueba, considerando su fragilidad y volatilidad.

- **Adquisición. –** Consiste en crear una copia o una imagen forense de la evidencia digital original, como norma, se lo hace para evitar causar daños o modificaciones de la información o dispositivos que se preservaron en el paso anterior, se considera la norma RFC 3227 para la adquisición de la información de acuerdo al estado en el que se encuentra el equipo o dispositivo.

- **Análisis. –** En esta etapa lo que se busca es realizar labores para localizar y extraer la evidencia digital, que sea relevante para la investigación; esto se lo realiza mediante la aplicación de diversas técnicas y herramientas forenses, buscando palabras claves, aplicaciones usadas, información borrada, historial web, correos electrónicos, etc. Tratando de dar respuesta al objetivo de la pericia.

- **Documentación. –** En esta fase, se documentarán todas evidencias que han sido encontradas en el apartado anterior, donde se considerara evidenciar todas las acciones con fotografías, esquemas, ubicaciones y demás información que respalden la información que ha sido encontrada.

- **Presentación. –** La normativa señala la presentación de los resultados una vez culminados los pasos anteriores, esto se lo hace en un informe describiendo claramente los pasos realizados e información encontrada. Deja explícitamente determinado que no se debe emitir juicios de valor, además de ser necesario, se expondrá explicaciones o aclaraciones de forma verbal y/o escrita.

Todo en lo referente a las evidencias electrónicas, donde se puede aplicar a cualquier tipo de organización, independiente de la actividad que se realice y del tamaño de la misma, con la condición de que sea manejada por profesionales con vastos conocimientos de la misma (AENOR, 2013).

1.4.7. RFC 3227 - Directrices Para la Recopilación de Evidencias

El análisis forense de datos digitales es un conjunto de técnicas y procedimientos para la recopilación y análisis de dispositivos electrónicos, comúnmente llamados evidencias, teniendo como objetivo la respuesta eficaz a un incidente relacionado con la seguridad de la información.

Aun con la existencia de un gran número de incidentes de seguridad que se relacionan a diferentes casos y dispositivos, los pasos a seguir en el proceso de adquisición en un análisis forense son habituales y recurrentes, estos según la RFC 3227 son:

- 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

De acuerdo a la investigación, los RFC «Request For Comments» son documentos donde se recoge todas las opiniones de expertos de un tema o materia en específico. El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento, y puede llegar a servir como estándar de facto para la recopilación de información en incidentes de seguridad (Martínez, 2014).

CAPÍTULO II

ESTADO DEL ARTE

El análisis forense es un tema que ha ido evolucionando a lo largo de los años, ha sido investigado, modificado y empleado en casos que requieran la pericia de expertos en temas informáticos, con el fin de extraer datos digitales de dispositivos que resguardan información esencial para casos donde la justicia lo requiera, sea en procesos civiles o penales.

Haciendo un buen uso de la Internet, se encuentra con investigaciones que hace unos años atrás hubiese sido imposible de revisar. La documentación encontrada relaciona el análisis forense con las consolas de videojuegos, utilizando en estas, casos y delitos en torno a la realidad de su país y a su propia justicia; se presentan los trabajos más relevantes con relación a la presente tesis.

2.1. Estudios Forenses de Consolas

Existe una investigación propuesta por los autores López et.al. (2002), en donde se presenta de manera general y especifica los aspectos técnicos de la informática forense, así como las herramientas necesarias para la extracción de datos contenidos en dispositivos electrónicos. Muestran la conceptualización de la evidencia digital, así como los detalles técnicos de su almacenamiento y eliminación de esta de manera segura.

En el trabajo se muestra el uso de herramientas y software forense, los mismos que de acuerdo al tipo de dispositivo a analizar serán utilizadas para un fin específico, además presentan muchas de las dificultades que actualmente son encontradas por los peritos informáticos al momento de realizar una investigación, y como de acuerdo a su realidad fueron resueltas de manera óptima y segura.

Los autores Conrad et al., (2009), realizaron una primera investigación sobre la extracción de datos digitales de un dispositivo de juegos portátil, como es el caso del PSP (Sony PlayStation Portable), este dispositivo fue uno de los primeros en contar con características de acceso inalámbrico a la Internet, además de contar con características de reproducción de multimedia.

Como la mayoría de los dispositivos que se basan en un procesador y una memoria de almacenamiento, la PSP se puede utilizar para fines muy distintos para los que originalmente fueron creadas, tanto legal como ilegalmente. Es por ello que la investigación se centró principalmente en el análisis de las características del navegador web de la PSP, donde sugiere las mejores prácticas para extraer evidencia digital.

De la misma manera los autores Conrad et al., (2010), realizaron la primera investigación sobre el análisis forense de consolas de videojuegos de la marca Sony, como es el caso de la Sony PlayStation 3 (PS3). Esta consola fue una de las más poderosas en salir en ese periodo de tiempo, ya que incluía características especiales que la competencia no tenia, como es el caso de actividades relacionadas a la conexión a la Internet, además de permitir a los usuarios particionar e instalar un sistema operativo secundario en el disco duro.

La nueva funcionalidad "de escritorio" que permite el sistema operativo secundario, junto con el cifrado del disco duro primario que contiene el software de juego plantea importantes problemas relacionados con el análisis forense de los sistemas de PS3. Por ello la investigación se centró en estudiar y analizar la arquitectura y el comportamiento de PS3, donde se proporciona recomendaciones para llevar a cabo investigaciones forenses de los sistemas de PS3 y concluyeron que no es posible evitar que la evidencia se altere durante el análisis de la Sony PlayStation 3, al usar un método nativo. Sin embargo, la metodología realizada sigue siendo válida, ya que el análisis realizado por los investigadores es repetible.

2.1.1. Estudios Forenses de Consola PS4

Los autores Davies et al. (2015), realizaron un primer acercamiento al análisis forense de la última versión de la consola de videojuegos de Sony, como es la PS4; la misma agrega nuevas funciones interactivas, que difieren en gran medida a su función principal, estas funciones son muy valiosas y de gran aporte al momento de realizar una investigación forense.

Las funciones van desde la navegación web hasta chat en vivo; es decir todas las funciones de comunicación que serán de interés para los investigadores forenses. La investigación de los autores es una primera visión forense de la consola PS4, donde se identifica posibles fuentes de información, además de proporcionar posibles métodos generales para adquirir los datos digitales, pero sin establecer cuál de los métodos sería el más recomendable, en cambió lo que hacen es sugerir acciones de acuerdo al modelo y caso a analizar; ya que muestra casos particulares centrándose específicamente en el proceso de investigación forense cuando la consola se encuentra en línea y fuera de línea.

2.1.2. Estudios Forenses de Consolas Similares

El autor Córdova (2018) realiza una investigación sobre la creación de una guía metodológica para el análisis forense de una consola Xbox One; donde plantea la obtención de la evidencia digital contenida en dicha consola y presentarla como una

evidencia en la resolución de un proceso judicial. Este trabajo guarda una gran relación con la presente investigación, considerando que ambas pretenden elaborar una guía metodológica para un tipo específico de consolas de videojuegos.

Se debe considerar que las consolas a analizar cuentan con una arquitectura completamente distinta, al ser de fabricantes que se encuentran en disputa por el liderato del mercado; se puede determinar que la arquitectura, distribución de elementos, tipos de memorias y sistema operativo difieren en gran medida la una de la otra, es por ello que la presente investigación partirá del trabajo realizado por Córdova (2018), para tomar en cuenta consideraciones realizadas, así como los errores aprendidos y posibles relaciones con elementos electrónicos que compartan ambas consolas.

2.2. Estudios Forenses de Componentes de Consolas

Nuestra investigación se centra principalmente en elaborar una metodología específica para consolas PS4 Slim, aplicando la normativa legal del Ecuador, donde se parte de la investigación realizada por los autores Loarte y Grijalva (2017), la misma que trata sobre la evidencia digital y como ésta ha sido de gran relevancia en la resolución de procedimientos civiles o penales; exponiendo como la mayor problemática actual, la falta de procedimientos que ayuden a guiar a los peritos informáticos del Ecuador.

Es por ello que el trabajo se tomará como referencia para la presente tesis, ya que cuenta con todas características necesarias para la extracción de datos digitales; Además, cuenta con un marco estandarizado para el análisis forense, considerando normas y estándares internacionales, haciendo una relación directa con la normativa legal del Ecuador para que de esta manera la evidencia sea aceptada legalmente en un tribunal.

2.2.1. Estudios sobre Des/Encriptación de datos

Al contener información preliminar de los documentos analizados, uno de los retos a presentarse es el disco cifrados de la PS4 Slim, para solventar esto Wismark (2009), presenta un artículo que habla sobre la Des/Encriptación en la Informática Forense, el articulo trata aspectos referentes a criptografía y como ayuda en el trabajo de los forenses informáticos con el fin de preservar la información más importante con el fin de ser usada como evidencias en juicios sean civiles o penales.

Además, Castañeda et al., (2009) en su investigación sobre Evaluación de herramientas para análisis forense orientado a discos duros, señala el uso de diferentes herramientas para obtener la imagen forense de discos, sean cifrados o no, realizando un análisis

exhaustivo para cada herramienta analizada, presentando resultados confiables, en donde se presentan los datos obtenidos de acuerdo al software utilizado, recomendando la herramienta más optima a utilizar de acuerdo a la finalidad u objetivo a lograr.

Manzano (2012), sobre cómo enfrentar el problema de la optimización de los procesos de descifrado de evidencias informáticas que se encuentran protegidas con contraseña. Analizar alternativas tecnológicas para la realización de una plataforma de tratamiento masivo de información cifrada utilizando la tecnología GPGPU para procesar datos. Determinando la manera de facilitar la unificación de distintas herramientas de descifrado en una misma plataforma, con la característica de una independencia del sistema operativo.

2.2.2. Visión General

Como se observa existe un gran número de investigaciones y trabajos sobre el análisis forense, así como su relación en consolas de videojuegos, pero, no existe ninguna metodología específica para la consola Sony PS4 Slim, donde se considere la normativa legal de Ecuador, así como metodologías de buenas prácticas forenses; haciendo que el sistema Pericial del Ecuador no cuente con el conocimiento ni la metodología para poder evidenciar estos delitos, llevando a una omisión de la evidencia y a su no judicialización y resolución un proceso civil o penal.

CAPÍTULO III

METODOLOGÍA DE ANÁLISIS FORENSE EN UNA PS4 SLIM

3.1. DELITOS PERPRETADOS EN CONSOLAS DE VIDEOJUEGOS

Las consolas de videojuegos que hoy en día salen al mercado, tienen cada vez más auge en la sociedad actual, ya que cuentan con servicios y aplicaciones que brindan una mejor comodidad al usuario al momento de interactuar con el medio exterior.

Las consolas de videojuegos cumplen la función para la que fueron diseñadas, como es el entretenimiento y la diversión; pero muchas veces estas consolas en manos equivocadas son usadas para otros fines, basados en la experiencia laboral y en el conocimiento colectivo de peritos informáticos del Ecuador, se ha podido determinar los usos que criminales informáticos hacen en estos dispositivos.

El discernimiento de la información recogida ha determinado que las consolas de videojuegos presentan puntos de vulnerabilidad de acuerdo a la aplicación o servicio que brinda. Los delitos que se pueden perpetrar en las consolas de videojuegos y específicamente en la consola PS4 Slim se pueden evidenciar en la tabla 2.

Tabla 2. Delitos perpetrados en consola de videojuegos
Fuente: Diseño del Autor

Aplicación / Servicio	Tipos de Delitos Informáticos				
	Extorsión	Robo de identidad	Fraude	Pornografía infantil	Manipulación de la información
Mensajería Instantánea	x	x	x	x	
Juegos en línea	x	x			x
Chat en vivo	x	x	x	x	
Ustream		x		x	
Descarga de APP		x	x		x
Navegador Web			x		x

Como se puede observar en la Tabla 2, existen delitos informáticos que se pueden perpetrar al usar una consola de videojuegos PS4, esto combinado con una falta de atención de los padres, crea una ventana donde el cibercriminal puede aprovecharse y sacar información o peor aún usar a los niños como medio para llegar a un fin delictivo.

El análisis se lo hizo de acuerdo a un manejo de los servicios y aplicaciones que brinda la Play Station 4 Slim, considerando las vulnerabilidades y poca seguridad que se brinda al usar este tipo de consolas.

3.2.ANÁLISIS DE LA PLAY STATION 4 SLIM

Las diferentes consolas de videojuegos, las mismas que constan de su propio sistema operativo de acuerdo a su fabricante, presentan un reto al momento de acceder e interpretar los datos. Como es de conocimiento ya ha existido análisis forense para dispositivos de juegos de ámbito similar a la PS4 Slim, donde se toma como referencia los desafíos y posibles problemas que enfrentaron al momento de acceder a los datos en las plataformas de juegos analizadas.

Un análisis más cercano es el realizado en la PlayStation 3 por Conrad et al., (2010) donde un desafío presentado es en el formato de encriptación AES 128, el mismo que es explotable a través de los diversos procesos de recuperación de las claves criptográficas que son utilizadas por la compañía Sony, identificadas por el grupo de pirateo fail0verflow.

En esta investigación también utilizaron diversas técnicas forenses de red y herramientas de software para evaluar las vulnerabilidades de seguridad de la consola Ps3, y observaron que las comunicaciones TCP/UDP de PlayStation 3 no están cifradas.

3.2.1. Desafíos forenses identificados

Uno de los primeros desafíos encontrados es con relación al sistema de archivos, el mismo que no es estándar (como en el caso de la Xbox One - NTFS), lo que presentaría inconvenientes al momento de la recuperación de metadatos.

Además, el disco duro aparece encriptado presentando una barrera importante al momento de acceder a los datos. Se puede crear la imagen forense del disco duro, a través de un bloqueador de escritura, pero la naturaleza de cifrado del disco no permitiría un análisis a profundidad de los datos contenidos en el dispositivo.

Otros inconvenientes encontrados, son la capacidad del usuario de modificar la información que contiene en la PlayStation Network (PSN) a través de otro dispositivo usando la APP de Ps4. Finalmente, al ser una consola de octava generación esta contiene un uso compartido a través de redes sociales del contenido que se genera, lo que requiere que la consola este siempre conectada a la red. Desde una perspectiva forense se puede determinar que la información generada por el usuario de la PS4 Slim, no se encuentre en la totalidad en el disco duro, sino en los servicios en línea que ofrece este tipo de dispositivos. (Davies et al., 2015).

3.2.2. Revisión Preliminar de la Consola PS4

Luego del análisis de la literatura disponible en la web, se realizó una investigación empírica de la Play Station 4 Slim, para poder identificar las posibles fuentes de información digital que pueden ser de gran importancia para la investigación forense.

Esto consistió en usar la PS4 Slim, donde una vez encendida, se navegó por los diferentes menús de la consola y de un juego en particular, identificando las posibles áreas que puedan proporcionar evidencia ya sea de uso y/o comunicación.

Las áreas de importancia son principalmente las que puedan brindar información sobre aspectos como: “de quién”, “qué”, “cuándo” y “dónde”. El "quién" en identificar qué usuario generó la evidencia (La consola PS4 Slim puede crear hasta 16) (Sony Computer Entertainment America, 2014), "qué" contenido se puede crear, tiempo para indicar "cuándo" se generó la información, "dónde" se puede almacenar la información (disco duro, medios externos, Internet / nube). (Davies et al., 2015)

3.2.3. Procedimiento analítico

La presente investigación tiene como fin la creación de una metodología de análisis forense, pero para que pueda ser usada como evidencia valida en el Consejo de la Judicatura y en cualquier tribunal del Ecuador, esta debe cumplir con estándares, normas y manuales de buenas prácticas forenses.

3.3.COMPARATIVA ENTRE CONSOLAS SIMILARES

Los dispositivos que están en la batalla por ser la mejor consola de videojuegos en la actualidad son la Play Station 4 Slim, la misma que es materia de análisis en la presente investigación y la Xbox One, que como se pudo ver en el estado del arte, ya fue analizada, en donde se generó un método de análisis forense.

Es por ello que es de gran importancia comparar ambas consolas de videojuegos, donde se analizará los puntos de relevancia para la presente investigación, como es su arquitectura, su estructura interna, su disposición de componentes y los servicios que prestan a la hora de generar el contenido que va a ser analizado por el software forense.

3.3.1. Interfaz

Una de las primeras comparaciones es el método en el que el usuario se relaciona con la consola, la interfaz es la conexión funcional que existe entre el dispositivo y el usuario al momento de encender y usar la consola.

La Xbox One al ser producida por Microsoft, su interfaz es muy parecida al sistema operativo Windows 8, en donde se tiene una opción similar a la multitarea, ya que desde su mando se puede navegar a través de las ventanas, la empresa lo reconoce como un "chasquido" de aplicaciones, donde se puede abrir aplicaciones mientas el usuario está jugando. (Microsoft, 2018)

La Play Station 4 Slim, cuenta como un sistema de menús dinámicos, donde se permite al usuario realizar una actividad especifica de acuerdo al menú seleccionado, es decir podrá seleccionar su juego, revisar sus redes sociales, ver el perfil del usuario, etc. La PS4 Slim cuenta con un método de "streaming" donde el usuario puede compartir su modo de juego en línea, la Xbox One cuenta con un servicio parecido, pero esta es solo bajo suscripción. (Sony Computer Entertainment America, 2014)

3.3.2. Arquitectura

Dentro de la arquitectura de las consolas de videojuegos, la misma que consiste en los bloques lógicos que constituyen el funcionamiento interno y como estos se comunican con el fin de lograr el máximo rendimiento permitido por el fabricante.

Ambas consolas cuentan con una arquitectura basada en una tecnología Jaguar AMD (Advanced Micro Device) de 64bits, donde cada fabricante realizó sus respectivas modificaciones. Cuentan con un procesador de 8 núcleos a una frecuencia de 1.6Ghz, con el cambio de que Microsoft modifico el reloj de su procesador a un 10% más, contando con un reloj de 1.75Ghz. Con la desventaja de que Jaguar diseño esta arquitectura para sistemas de bajo consumo y no para potencia en juegos o aplicaciones, lo que hace que los fabricantes opten por nuevas interfaces para mitigar este problema apostando por la relación potencia/consumo. (Méndez, 2013)

La GPU de ambas consolas están ciertamente distanciadas en números, pero si se considera que la GPU es la encargada de manejar el procesamiento especifico de gráficos y de operaciones de punto flotante, en donde la Play Station 4 Slim cuenta con 1.84 TFLOP AMD Radeon, mientras que la Xbox One con 1.4 TFLOP AMD. El procesador de 8 núcleos de ambas consolas, ayudan a mitigar ciertos problemas relacionados con la lentitud de procesamiento al momento de realizar varias tareas a la vez, donde la tecnología Jaguar AMD reserva núcleos para estas tareas y no comprometer la estabilidad del juego. (Méndez, 2013)

La memora Ram de las consolas permiten un acceso más rápido a los datos, ya que, al no ser secuencial, ayuda al procesador a mantener las instrucciones que necesita en tiempo relativamente cortos. La tecnología que manejan las consolas depende del fabricante ya que ambas cuentan con 8Gb de Ram, pero con tecnología muy diferente;

la consola PS4 Slim cuenta con la tecnología GDDR5 que ofrece una mejor interpretación con velocidades de datos de hasta 3.500 megatransfers por segundo, a diferencia de la GDDR3 de la Xbox One con velocidad de datos de 2.133 MT/s (Méndez, 2013). En las siguientes figuras, se diferencia la disposición de los elementos de las consolas de videojuegos.

Diagrama de Conexiones de las Consolas de Videojuegos

Play Station 4 Slim

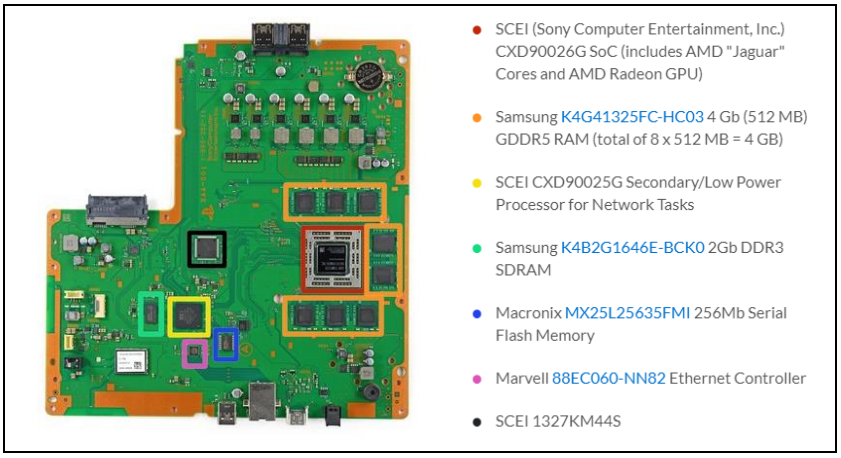

Figura 1. – Disposición interna de la Play Station 4 Slim

Fuente: Galan, W (2013). *PlayStation 4 Teardown*. Recuperado de: https://es.ifixit.com/Desmontaje/PlayStation+4+Teardown/19493

Xbox One

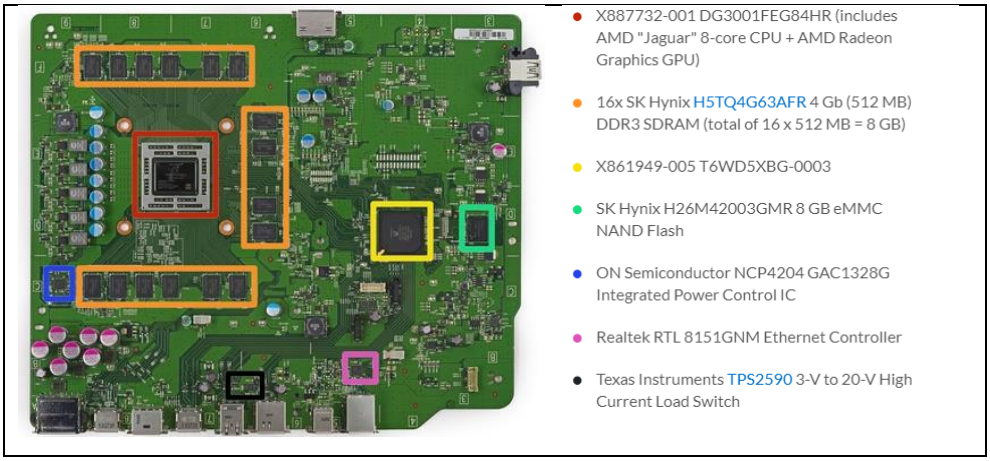

Figura 2. – Disposición interna de la Xbox One

Fuente: *Xbox One Teardown*. (2013). Recuperado de: https://www.ifixit.com/Teardown/Xbox+One+Teardown/19718

3.3.3. Gestión de Almacenamiento

El almacenamiento de las consolas es muy similar, ya que la Play Station 4 Slim viene en dos versiones con almacenamiento de 500GB y 1TB; por otro lado, la Xbox One cuenta con un almacenamiento de 500GB. La consola PS4 Slim es la única que ofrece un disco

duro extraíble, lo que significa que el usuario puede aumentar la capacidad de almacenamiento de fábrica. La Xbox también cuenta con puertos USB para aumentar la capacidad hasta 500Gb. (Microsoft, 2018; Sony Computer Entertainment America, 2014)

La característica principal que los diferencia es en el sistema de archivos, el mismo que es un componente del sistema operativo que permite una administración de las memorias, donde su función principal es la asignación de espacios a los archivos, es decir la manera como se guardan y organizan los datos generados por el usuario o sistema.

La Xbox One, maneja un sistema de archivos con NTFS (Preferido por Microsoft), el mismo que manejan los computadores; es usado ya que tiene una mejor interacción con las particiones del disco que presenta la consola para su mejor rendimiento. La Play Station 4 cuenta con un sistema de archivos no estándar, el mismo que cuenta con una estructura dividida en 15 particiones. (Microsoft, 2018; Sony Computer Entertainment America, 2014)

3.3.4. Tabla Comparativa

Luego de realizar el análisis de los diferentes componentes y elementos de las consolas, en la Tabla 3, se presenta un resumen de la comparativa realizada.

Tabla 3. Tabla Comparativa de consolas
Fuente: El Autor

Características	PS4 Slim	Xbox One
Procesador	AMD Jaguar 8 núcleos	AMD Jaguar 8 núcleos
Reloj	1.6Ghz	1.75GHz
GPU	1.84 TFLOP AMD Radeon	1.4 TFLOP AMD
RAM	8GB GDDR5	8GB GDDR3
Almacenamiento	500GB / 1TB	500GB
Sistema de archivos	Propia	NTFS
Dimensiones	288 mm x 265 mm	295 mm x 230 mm
Resolución de video	1080p	4K
Resolución de videojuego	720p-1080p	720p- 1080
USB	3.0	3.0
Conexión Web	Ethernet, IEEE 802.11 b/g/n Wifi	Giga - Ethernet, IEEE 802.11 b/g/n Wifi
Interfaz	Propia	Multitarea

Como se puede ver, ambas consolas cuentas con ciertas similitudes en comunicación y almacenamiento, además de su procesador; hay que considerar que para fines de la presente investigación, la consola Play Station 4 presenta puntos relevantes como es su sistema de archivos, el mismo que para fines forenses presenta un gran reto al no ser estándar, a diferencia de la Xbox One que usa NFTS el mismo que puede ser analizada como un computador común, además de contar con la complicación de que la consola tiene cifrado su disco.

3.4.HERRAMIENTAS DE ANÁLISIS FORENSE

Para realizar un análisis forense a la consola de Videojuegos PS4 Slim, se determina las herramientas que se utilizaran para el propósito. Ante todo, lo primero que debe conocerse son los procedimientos óptimos para poder realizar un buen análisis forense.

En la actualidad existen varias herramientas para cumplir con un buen análisis forense, en el presente apartado conocerá cual es la herramienta forense más óptima que se utilizará. Según Davies et al., (2015), la herramienta forense FTK Imager es la más óptima para cumplir con los requerimientos del sistema de la consola de videojuegos PS4.

3.4.1. FTK Imager

Conocida como Forensic Toolkit® (FTK®), es una herramienta poderosa para la obtención de imágenes forenses sin realizar ningún cambio en la evidencia original, ya que cuenta con un bloqueador de escritura que se maneja vía software. Cuenta con varias herramientas como (Access, 2018):

- Creación de imágenes forenses de dispositivos de almacenamiento masivo.
- Vista previa de archivos y carpetas y contenido de las imágenes forenses.
- Montaje de imágenes forense creadas previamente por otro usuario.
- Capacidad de exportar archivos y carpetas desde las imágenes forenses.
- Vista y recuperación de archivos eliminados que aún no se han sobrescrito.
- Creación de códigos HASH de archivos para verificación de integridad de datos.
- Generación de informes de imágenes forenses y archivos, donde se considere el código HASH para demostrar la integridad de los datos recopilados para ser usados como evidencia en un proceso judicial.

3.4.2. Autopsy

El software forense Autopsy®, es una plataforma que permite realizar un análisis forense de diferentes dispositivos de almacenamiento; funciona en diferentes plataformas como Linux, Windows, Mac OSx y Free BSD. Contiene una interfaz gráfica que fue desarrollada por The Sleuth Kit®. (Autopsy, 2018)

Esta creada bajo el lenguaje Perl (Practical Extracting and Reporting Language), este tipo de lenguaje se usa para la extracción de información de ficheros de textos y generación de informes. Actualmente cuenta con una versión en código JAVA y diseñada para ser una plataforma de visión extremo a extremo, algunos de sus módulos proporcionan (Autopsy, 2018):

- Visualización de eventos de manera avanzada, es decir maneja un análisis en línea de tiempo.
- Búsqueda de palabras clave indexadas en archivos
- Generación de código Hash
- Extracción de historial del navegador web, marcadores y cookies.
- Recuperación de archivos eliminados, extracción de metadatos de imágenes y videos.

3.5. ANÁLISIS FORENSE PRELIMINAR

Para poder realizar el análisis forense de la consola PS4, primero se consideró aspectos relevantes que serán considerados en los siguientes apartados, como es la creación de un escenario en condiciones controladas para poder determinar así la información que será extraída mediante métodos forenses.

3.5.1. Dispositivos y Herramientas a utilizar

En este apartado, se determinarán los dispositivos que se utilizarán en la creación del escenario, así como los que servirán para realizar el análisis forense, el estado inicial en el que se encuentran y la manera en cómo se configuraron.

Consola de Videojuegos PS4 Slim

Uno de los elementos primordiales de la investigación es la consola de videojuegos Play Station 4 Slim, la misma que para obtener un resultado fiable y con datos válidos, se consideró no adquirir una consola de segunda mano, por la dificultad de no poder asegurar que los datos adquiridos sean mediante un ambiente controlado; por lo que la mejor opción fue la adquisición de una consola de videojuegos PS4 Slim nueva, como se puede ver en la figura 3.

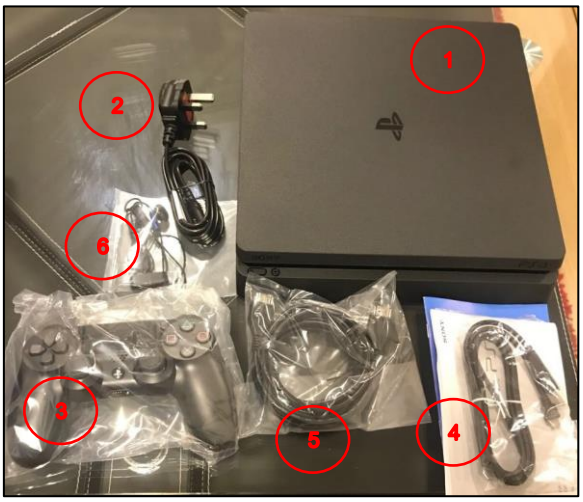

Figura 3. – Consola Play Station 4 Slim nueva

Fuente: *Autor*

De acuerdo a la figura 3, los elementos que forman parte de la caja son:

1) Consola de videojuegos PS4
2) Cable de alimentación AC
3) Control DualShock 4 Wireless
4) Cable USB
5) Cable HDMI
6) Audífonos

Una vez adquirida la consola, se configuró considerando que los datos que se ingresarán serán usados en la extracción de la información mediante métodos forenses. El primer paso para su configuración fue la conexión del control de juegos conocido como el Dualshock 4 Wireless a la consola mediante el cable USB, y luego pulsando el botón PS, que se encuentra entre los dos joysticks. Se selecciona el idioma y configura la conexión a Internet, en donde brinda la posibilidad de escoger entre una conexión LAN o Wifi, en nuestro caso se conecta la consola mediante Wifi, usando la red del hogar la misma que cuenta con un clave de 12 caracteres con encriptación WPA2.

Una vez realizadas las configuraciones generales, se crea el perfil de usuario, en donde previa a una actualización del firmware de la consola, se muestra la información del servicio de PlayStation Network. Este nuevo servicio brinda la posibilidad de: Descarga de juegos a través del PlayStation Store, posibilidad de hacer amigos de otros jugadores y chatear con ellos, y compartir información en cualquier momento. Para la creación del perfil de usuario de la PlayStation Network como se observa en las figuras 4 y 5, donde solicita los siguientes datos:

- País o región
- Idioma
- Fecha de nacimiento
- Ciudad
- Estado/Provincia
- Código postal
- Contraseña
- Condiciones y términos.
- Elección de un avatar
- Creación de un Id on-line
- Nombre y Apellido
- Id de inicio se sesión (correo electrónico)

Figura 4. – Servicio de PlayStation Network

Fuente: *Autor*

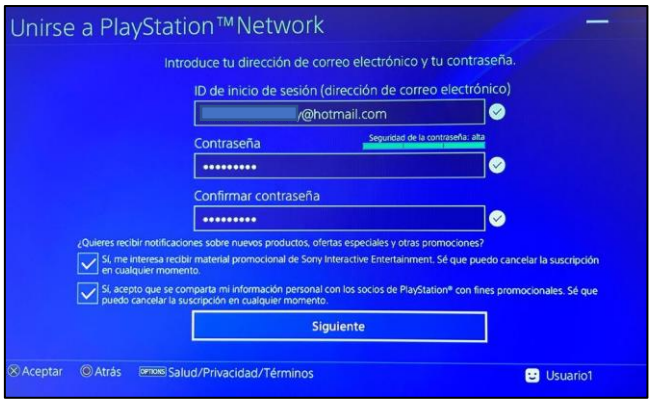

Figura 5. – Creación de Id de inicio de sesión y aceptación de términos y condiciones

Fuente: *Autor*

Solicita configurar las opciones de privacidad para todo lo que tiene que ver con juegos, música y películas, como se observa en la figura 6, todo se dejó por defecto de fábrica. En la figura 7, se observa la configuración de las conexiones, es decir permite controlar quienes pueden ser amigos, seguidores y demás conexiones, además de quien se da privilegios de verse mutuamente.

En la figura 8, existe la configuración de los mensajes, se configura quien puede ver tu nombre real al momento de hacer un chat general, además de quien puede comunicarse con el usuario.

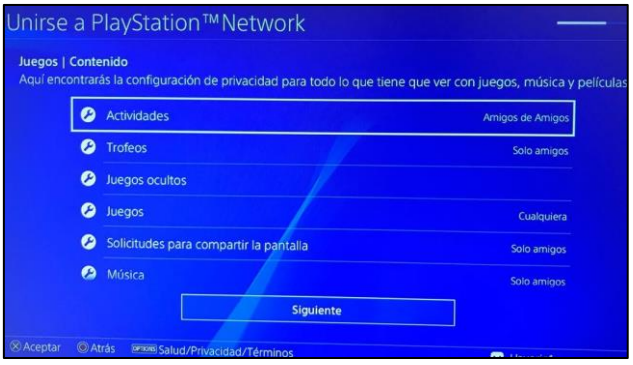

Figura 6. – Configuración de privacidad en contenido

Fuente: *Autor*

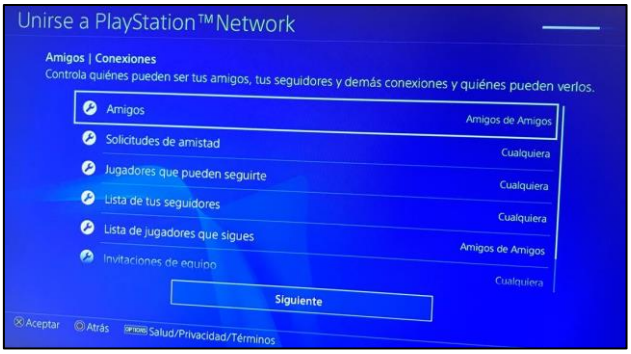

Figura 7. – Configuración de privacidad en conexiones

Fuente: *Autor*

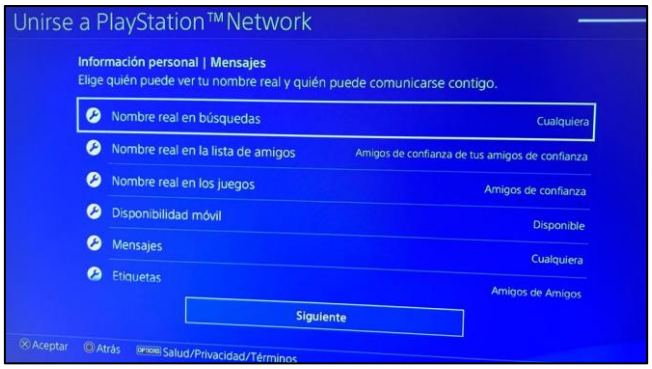

Figura 8. – Configuración de privacidad en mensajes

Fuente: *Autor*

Una de las configuraciones extras, es la opción de la verificación en dos pasos para inicio de sesión, donde se solicita el número de teléfono celular, y, la verificación de este mediante el envío de un código por mensaje de texto como se observa en la Figura 9.

Figura 9. – Configuración de verificación en dos pasos

Fuente: *Autor*

Una vez creado el perfil de usuario, se redirecciona a la opción de pantalla de mensajes, en donde se puede enviar solicitudes y buscar a gente que ya haya creado su perfil de usuario, en este caso se buscó dos personas para fines de la investigación, las mismas que eran conscientes del fin propuesto, como se observa en la figura 10 se envió mensajes a estos usuarios.

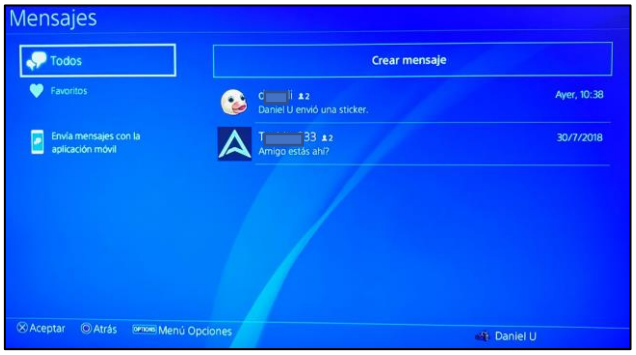

Figura 10. – Mensajes enviados a usuarios de PlayStation Network

Fuente: *Autor*

Finalmente, para fines de investigación se utilizó a la consola de videojuegos para el fin que fue desarrollada, en donde se realizó las 3 posibilidades al momento de adquirir un juego como es:

- Se compró un juego en físico: Call Of Duty: Infinity Warfare: Versión 1.25
- Se compró un juego de la PlayStation Store: Fifa 17
- Se descargó un juego gratuito de la PlayStation Store con posibilidad de juego en línea: Fortnite

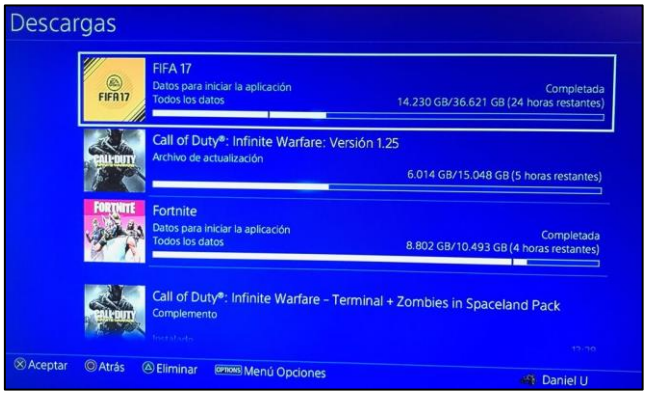

Figura 11. – Descarga de juegos de la PlayStation Store y actualización de juego físico
Fuente: *Autor*

Figura 12. – Juego On-line Fortnite
Fuente: *Autor*

Disco Duro externo USB

Disco Duro de 1Tb de marca SeaGate - Expansión, con capacidad igual o superior a la capacidad de almacenamiento de la consola PS4. Siguiendo la norma UNE 71506:2013 y RFC 3227, el Disco Duro tiene que ser nuevo para obtener una imagen forense con validez procesal.

Figura 13. – Disco Duro de 1Tb
Fuente: *Autor*

Kit de esclavizador de discos duros

Para poder tener acceso a los datos que están contenidos en el dispositivo de almacenamiento de la consola, se hace uso de un esclavizador de discos, el mismo sirve para conectar cualquier tipo de discos duros sean Sata o Ide a un computador mediante una conexión USB.

Figura 14. – R-Driver III, USB 2.0 To sata Ide cable
Fuente: *Autor*

Herramienta de Software para clonación de discos

Para la clonación de la unidad de almacenamiento de la consola, se usa el EaseUs Todo Backup, es una herramienta confiable y profesional (si se compra con licencia) para poder realizar copias de seguridad y recuperación de archivos, que permite a los

usuarios proteger archivos, particiones, discos y todo el sistema a través de copias de seguridad del sistema y copias de seguridad de archivos con facilidad.

Figura 15. – Software de clonación de discos

Fuente: EaseUS. *Free Data Backup Software Download - EaseUS Todo Backup Free*. Recuperado de: https://www.easeus.com/download/tbf-download.html

Herramientas varias

Para la manipulación de la consola y la extracción de los elementos de memoria, se usa varias herramientas que permiten el desmontaje de las piezas, se utilizará:

a) Desatornilladores de precisión

Figura 16. – Software de clonación de discos

Fuente: PcComponents. *Startech Kit Destornilladores Precisión*. Recuperado de: https://www.pccomponentes.com/startech-kit-destornilladores-precision

b) Kit de paletas de extracción

Figura 17. – Kit de extracción
Fuente: PcComponents. *Kit de reparación de celulares*. Recuperado de: https://www.pccomponentes.com/startech-kit-reparacion-celulares

3.5.2. Metodología a utilizar

Siguiendo las recomendaciones y lecciones aprendidas del autor Córdova (2018), ya que después de realizar una caracterización de diferentes metodologías y siguiendo el marco de la normativa legal del Ecuador, llego a la conclusión de que la metodología más optima de acuerdo al propósito de la investigación es la UNE 71506:2013

La norma tiene como objetivo principal establecer la metodología para (AENOR, 2013):

- Preservación
- Adquisición
- Documentación
- Análisis
- Presentación

3.6.METODOLOGÍA DE ANÁLISIS FORENSE

Para poder realizar una correcta metodología de análisis forense a la Play Station 4 Slim, se basó en estudios previos realizados los mismos que ayudarán a mantener una correcta serie de pasos a realizar con el fin de evitar el cometimiento de errores involuntarios que ocasionen la poca celeridad en la búsqueda de resultados.

Además, se realizó una investigación empírica, para poder identificar las posibles fuentes de información digital que pueden ser de gran importancia para la investigación forense. La misma consistió en identificar las posibles áreas que puedan proporcionar evidencia ya sea de uso y/o comunicación.

Existen dos tipos de análisis forense generales y estos dependen del estado en el que se encuentra la evidencia al momento de la preservación del mismo, siguiendo la norma RFC 3227, estos pueden ser análisis en frio y caliente.

El análisis forense en frio es aquel en el que se lo realiza cuando el dispositivo/elemento a analizar se encuentra en estado apagado tanto eléctrica como electrónicamente al momento de realizar el allanamiento. Este tipo de análisis requiere una mayor experticia del perito, ya que se debe seguir un mayor número de pasos para evitar la pérdida o modificación de la evidencia digital. Cabe recalcar que cuando se encuentra el dispositivo apagado, por norma no se lo debe encender ya que este proceso de encendido puede alterar la evidencia; además no se debe trabajar con el elemento original sino con una copia llamada imagen forense, usando medios estériles y herramientas de software especial.

El análisis forense en caliente es aquel que se lo realiza cuando el dispositivo a analizar se lo encuentra en estado encendido al momento de realizar el allanamiento. Se lo realiza en dispositivos como celulares o computadores, ya que se cuenta con herramientas de software específicos para análisis de memorias ram, además en este análisis se puede obtener con facilidad un mayor número de información ya que no se rompe contraseñas o se violenta sistemas de seguridad.

Córdova (2018) propone una serie de fases que ayudaran a determinar la validación de la metodología acorde a las normas RFC y UNE, y siguiendo la normativa legal del Ecuador. Estas fases son:

3.6.1. Fase de Requisitos

Según la Resolución 040-2014, específicamente en el Capítulo II, se especifica los requisitos para calificarse como perito, y en el artículo 511 del COIP se determina las reglas generales de las y los peritos.

Una vez cumplido con los requisitos, la autoridad competente designará al perito informático siguiendo el artículo 511 del COIP y los artículos 12, 13 ,14 y 15 de la Resolución 040-2014 (Consejo de la Judicatura, 2014). En este marco de determinan los siguientes pasos a seguir, como son:

- **Fase de designación. –** La realizan los jueces de acuerdo al SATJE y de acuerdo al Artículo 12 de la Resolución 040-2014.

- **Fase de posesión. –** Solo aplica en caso de ser un procedimiento civil, cabe recalcar que es responsabilidad del perito presentarse en la Unidad de

Evidencia de Criminalística de la Policía Nacional, en los límites de tiempo existentes.

- **Fase de investigación. –** Aquí es donde el perito pondrá en práctica toda su experticia con el fin de lograr el objetivo materia de la investigación.

- **Fase final. –** El perito presentará su informe pericial, el cual será defendido de manera oral de acuerdo al caso investigado, de acuerdo a los Artículos 18 y 19 de la Resolución 040-2014 y al artículo 222 del Código Orgánico General de Procesos.

3.6.2. Fase de Preservación

En esta fase la prioridad es preservar la información de la evidencia digital en la escena del delito, así como la integridad de la misma, para evitar daños, modificación o destrucción de la información. El perito deberá conocer todas las características de la escena del delito, para así poder tener todos los elementos listos tantos de hardware como de software previo al arribo del mismo.

La o el funcionario que llegue antes a la escena del delito será el responsable de la preservación de la escena hasta la llegada del personal especializado, en esta fase de seguirá 3 sub-fases como son:

- **Reconocimiento. -** Como lo establece el artículo 460 del COIP, que trata sobre el reconocimiento del lugar de los hechos.

- **Autorización. –** La autorización se la realiza para que el procedimiento cuente con una validez legal, y se la realiza de manera escrita a la autoridad competente o a las partes procesales; para así poder respaldarse al momento de alterar cualquier sistema de seguridad que este inmerso como objeto de la pericia, evitando cometer el delito tipificado en el Artículo 178 del COIP.

- **Identificación. –** Se identifica el tipo de evidencia, considerando las principales fuentes de información y el orden de volatilidad del mismo, se realiza de acuerdo a un orden específico, como es: 1) Perito fotográfico, 2) Perito de criminalística, 3) Perito dactiloscópico y para finalizar el 4) Perito informático; el mismo que identificará las fuentes de información que servirán para la resolución el objetivo de la pericia.

Siguiendo la norma UNE 71506:2013, en esta fase se realiza la preservación de la evidencia, es el caso de la PS4Slim. Considerando el estado en el que se la encuentra a la consola de videojuegos (apagado) como se puede ver en la figura 18:

Figura 18. – Estado inicial (apagado) en el que se encuentra a la consola PS4
Fuente: *Autor*

Procedimiento de preservación de la evidencia, siguiendo lo que estipula la norma, se la puede ver en la figura 19.

Figura 19. – Preservación de la evidencia
Fuente: *Autor*

Se considera mediante la orden de allanamiento de acuerdo a los Artículos 478, 480, 481 y 482 del COIP; los mismos que determinan las pautas del allanamiento, así

como la orden de esta y el procedimiento a seguir. Se considera la norma RFC 3227, que determina el uso de guantes de material aislante; además del embalaje y etiquetado de la evidencia de acuerdo a un número único determinado por el personal de criminalística de la Policía Nacional.

3.6.3. Fase de Adquisición

Una vez identificados los dispositivos a analizar, se realiza la extracción de la información contenida en dichos dispositivos; previamente considerando el estado en el que se encuentran los dispositivos, para así determinar los procedimientos que se seguirán para adquirir dicha información, como su transporte y cadena de custodia.

Se recopila toda la información, principalmente del estado actual de los dispositivos, ya que dependerá de si el dispositivo se encuentra encendido o apagado al momento de realizar el allanamiento, ya que en cada estado se cuenta con un procedimiento diferente.

Equipo Apagado

Para obtener la evidencia digital de un dispositivo que se encuentra apagado, se debe considerar las siguientes pautas, acorde a la norma RFC 3227:

- No encender el dispositivo, esto evitará que se modifique la información que contiene para su posterior análisis
- Desconectar toda conexión que tenga la consola, así como dispositivos alternos de memoria que constarán como una nueva fuente de evidencia.
- Sacar una imagen forense del dispositivo de memoria, para así trabajar en una copia del original y evitar cualquier modificación, daño, alteración o destrucción de la evidencia original.

Siguiendo estos preceptos, se realiza la extracción de la imagen forense del dispositivo de memoria de la consola de videojuegos PS4 Slim. Se desempaqueta la evidencia, para su posterior análisis, como se observa en la figura 20.

Figura 20. – Desempaquetado de la evidencia

Fuente: *Autor*

Una vez la evidencia se encuentra en manos del perito, se identifica donde se encuentra el dispositivo de memoria de la PS4 Slim, como se puede ver en la figura 21, esta se encuentra en la parte lateral de la consola.

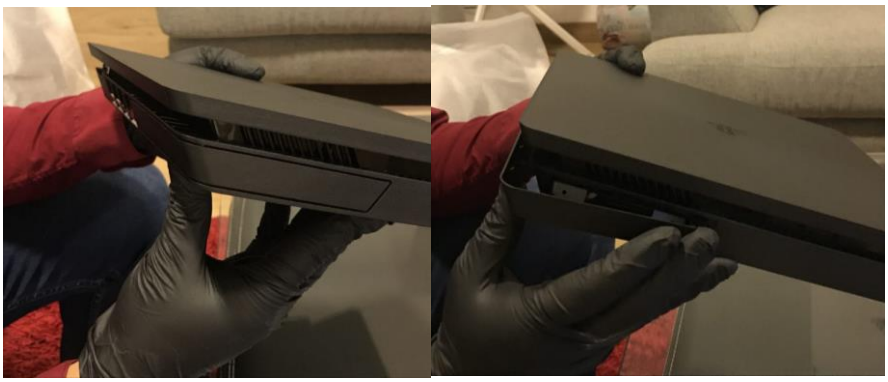

Figura 21. – Identificación del lugar donde se encuentra el dispositivo de memoria

Fuente: *Autor*

Una vez identificado, se extrae el dispositivo de memoria, como se puede observar en la figura 22, existe un tornillo y una lengüeta por donde se fija el disco duro de la PS4 Slim, y se extrae en dirección que indica la flecha como se observa en la figura 23.

Figura 22. – Dispositivo de memoria identificado

Fuente: *Autor*

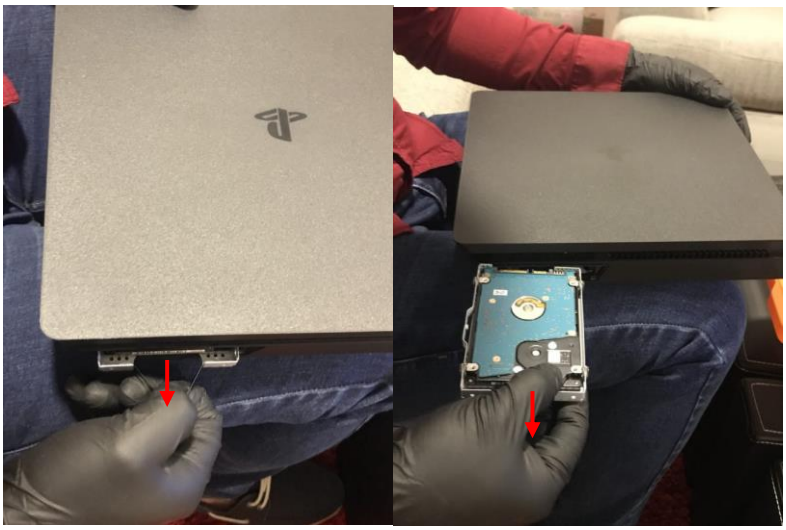

Figura 23. – Extracción del disco duro de la PS4 Slim.
Fuente: *Autor*

Para la extracción de la imagen forense siguiendo la norma RFC 3227, se hace uso del esclavizador de discos, para su posterior conexión al computador como se observa en la figura 24.

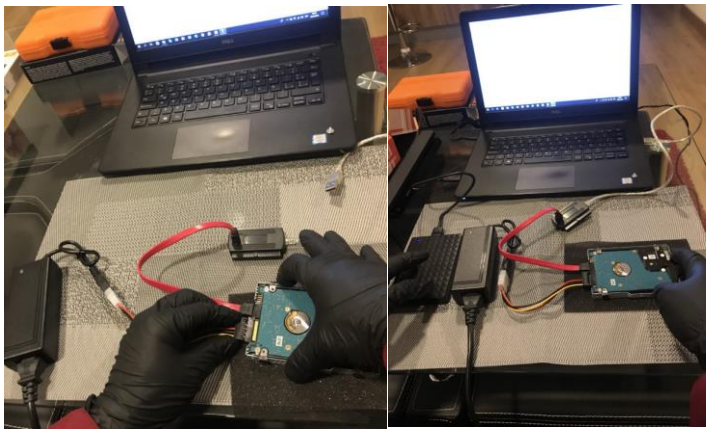

Figura 24. – Conexión del para extracción de imagen forense.
Fuente: *Autor*

Finalmente, se coloca en un puerto USB al esclavizador de discos, y en otro puerto USB al Disco Duro nuevo para su posterior formateo, como se observa en la figura 25.

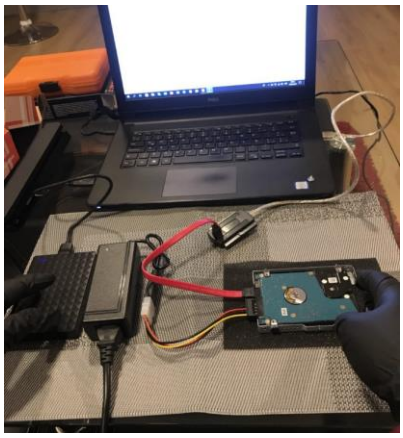

Figura 25. – Conexión total de los dispositivos para extracción de imagen forense.
Fuente: *Autor*

Una vez extraída la imagen forense haciendo uso del software FTK Imager 4.2, se observa el código HASH y MD5 de validación de la imagen forense, figura 26.

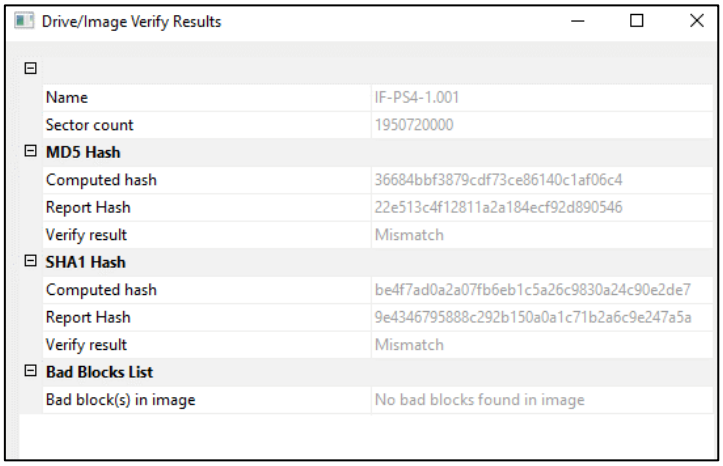

Figura 26. – Código Hash y MD5 de la imagen forense
Fuente: *Autor*

Equipo Encendido

Para obtener la evidencia digital de un dispositivo que se encuentra encendido, se debe considerar las siguientes pautas, acorde a la norma RFC 3227:

- Como primera pauta, no se deberá apagar el dispositivo, ya que existen procesos que son volátiles, como, por ejemplo: chats o transmisiones en vivo, juegos en línea, etc.
- Se debe considerar la volatilidad de la información, ya que, para recopilar los datos de la evidencia, primero se considera la información con mayor grado de volatilidad.
- Considerando la arquitectura que presentan las consolas de videojuegos y específicamente la consola PS4 Slim, no existe un procedimiento para

realizar un análisis de la memoria RAM, por lo que se considera a la Norma RFC 3227, que determina un proceso como:

  - Contenidos de logs y registros de la consola.
  - Estado de las diferentes conexiones de red.
  - Estado de los procesos encontrados en ejecución.
  - Contenido del disco duro.
  - Contenido de terceros dispositivos de almacenamiento.

- Conjuntamente de debe realizar una documentación de toda información que se encuentre en la consola PS4 al momento del allanamiento, 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 iniciados.
  - Videojuego en ejecución
  - Chats dentro del videojuego si fuere el caso.

- Los numerales 1 y 2 del Artículo 500 del COIP, determinan el procedimiento de recolección de la evidencia se obtuvo siguiendo la normativa legal del Ecuador.

Con estas recomendaciones, se realiza la adquisición de la información de la consola de videojuegos PS4 en estado encendido, considerando el orden de volatilidad determinado RFC 3227. Una vez que la información ha sido recopilada, se realiza al almacenamiento de la evidencia, siguiendo los preceptos de la Cadena de Custodia de la Policía Nacional.

La Cadena de Custodia está determinada por el Artículo 456 del COIP, donde se determina la autenticidad y legitimidad de los procesos de transporte y almacenamiento de la evidencia digital; así como el Artículo 457 del COIP que determina los criterios de valoración de la evidencia que fue o no llevada a través de la cadena de custodia. El proceso se lo lleva siguiendo las pautas del Artículo 482 del COIP donde determina la presencia de una autoridad al momento de realizar el allanamiento.

Para el análisis en caliente de la consola PS4 Slim, primero se hace uso de la herramienta de Software EaseUs Todo Backup; con la cual se clona el Disco Duro de

la PS4 Slim en un nuevo Disco Duro, respetando así la norma RFC 3227, que determina que no se debe trabajar con la evidencia original.

Una vez clonado el disco, se reinstala la unidad de memoria en la consola PS4 Slim, como se ve en la figura 27.

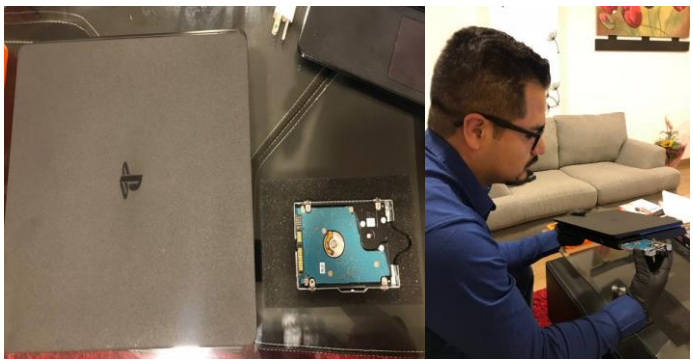

Figura 27. – Instalación del disco duro clonado a la PS4 Slim.
Fuente: *Autor*

Con esto, se coloca nuevamente todas las conexiones eléctricas de la PS4 y a se enciende la consola, como se observa en la figura 28.

Figura 28. – Reconexión y encendido de la consola PS4 Slim.
Fuente: *Autor*

Una vez puesta en marcha la consola, se realiza la pericia, siguiendo la norma RFC 3227, analizando las aplicaciones o servicios que generan información dentro de la consola PS4 Slim.

Los puntos se detallan a continuación:

Contenidos de logs y registros de la consola

Para poder visualizar el registro de actividades de la consola, se dirige al menú superior y seleccionar la pestaña notificaciones, donde se pude observar en la figura 29, todas las actividades que en la consola se han realizado desde el principio de su instalación.

Figura 29. – Registro de actividades de la PS4 Slim.
Fuente: *Autor*

Se puede observar que existe en registro con fecha, pero no con hora; a diferencia de los trofeos y premios que mantienen un formato de hora y fecha, como se observa en la figura 30.

Figura 30. – Registro de trofeos y logros.
Fuente: *Autor*

Estado de las diferentes conexiones de red

Al momento de realizar el allanamiento de la evidencia digital, lo que se procura determinar es que conexiones de red están siendo utilizadas en la consola, con el fin de establecer porque tipo de conexión la consola se comunicaba con la nube.

Para realizar este procedimiento, se dirige al menú superior, luego en la pestaña configuración, seguido de red y ver estado de conexión, donde se obtiene la información relevante como se observa en la figura 31.

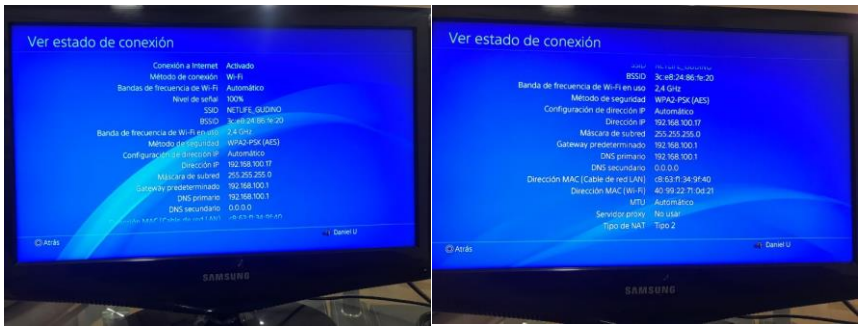

Figura 31. – Registro de conexión de red.

Fuente: *Autor*

Estado de los procesos encontrados en ejecución

Este paso no fue posible su determinación, ya que la interfaz de la PS4 Slim, no puede ser visualizada como multitarea.

Contenido del disco duro

Un componente importante es poder determinar que contenido esta guardado en el Disco Duro de la consola, ya que se puede establecer con qué tipo de contenido el perito puede encontrarse.

Para acceder a esta información, se coloca en el menú principal, luego configuración, almacenamiento y almacenamiento del sistema, donde se encuentra con la información que contiene la consola PS4 Slim, como se observa en la figura 32.

Figura 32. – Contenido del disco duro de la consola PS4 Slim.

Fuente: *Autor*

Una vez dentro de este menú, se presentan 4 pestañas de contenido donde están las aplicaciones, galería de capturas, datos guardados de los juegos y temas para la consola. En la figura 33 se observa el contenido de la pestaña aplicaciones y galería de capturas, las mismas que contienen información como hora y fecha de captura.

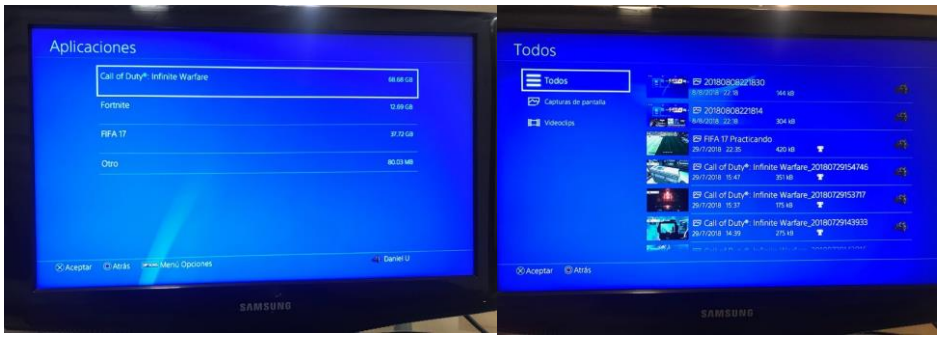

Figura 33. – Contenido del disco duro en las pestañas aplicaciones y capturas.
Fuente: *Autor*

Contenido de terceros dispositivos de almacenamiento

Actualmente no hay dispositivos de terceros conectados a la consola de videojuegos.

Hora y fecha actualmente configurada del sistema

Es de vital importancia determinar con qué fecha y hora la consola está configurada, ya que mediante esto se puede trazar una línea de tiempo de todos los eventos que pueden haber ocurrido con la consola.

Esto se consigue accediendo al menú superior, pestaña configuración y finalmente hora y fecha; se puede observar en la figura 34, además de esta información, la zona horaria y los formatos de las mismas.

Figura 34. – Fecha y hora de configuración de la consola PS4 Slim.
Fuente: *Autor*

Procesos que puedan estar en ejecución

Este paso no fue posible su determinación, ya que la interfaz de la PS4 Slim, no puede ser visualizada como multitarea.

Todas las conexiones de red que se puedan tener

Este apartado está relacionado con el estado de la red, ya que se puede determinar que interfaces de red están siendo utilizadas por la consola. La PS4 Slim, cuenta con conexión LAN y Wifi, como se pude observar en la figura 35, esta información la se obtiene al seguir el menú superior, configuración, red y configurar conexión a internet.

Figura 35. – Conexiones de red disponibles en la PS4 Slim.
Fuente: *Autor*

Absolutamente todos los usuarios que pueden estar conectados localmente, así como de manera remota

La consola Play Station 4 Slim no cuenta con visualización de multitarea en su interfaz, y los usuarios que se encuentran conectados de manera local solo se pueden establecer cuando se relaciona una palanca DualShock4 con un perfil específico creado en la consola. En este caso existió dos palancas y por lo tanto dos usuarios conectados de manera local a la consola PS4 Slim.

Aplicaciones abiertas y Videojuego en ejecución

Las aplicaciones que se encuentran corriendo al momento del allanamiento, permiten determinar las acciones que el usuario de la consola PS4 Slim estaba ejecutando en el instante previo a la preservación de la evidencia. Como se puede ver en la figura 36, en el menú principal pulsando el botón PS de la palanca permite obtener esta información.

Figura 36. – Aplicaciones y videojuegos abiertos.

Fuente: *Autor*

Chats iniciados

Los mensajes o chats que se encuentran iniciados y en proceso de ejecución es de vital importancia, porque se puede establecer las conexiones, los usuarios y la razón de comunicación con que el usuario principal tuvo con diferentes usuarios de Play Station a nivel mundial. Esto se puede visualizar accediendo al menú superior en la pestaña mensajes, como se ve en la figura 37.

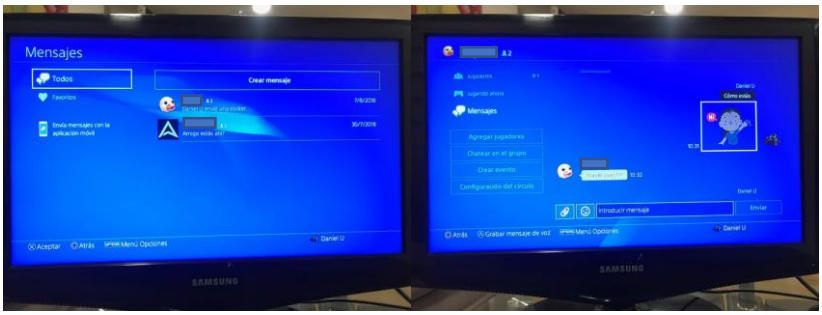

Figura 37. – Chats iniciados en la PS4 Slim.

Fuente: *Autor*

Chats dentro del videojuego si fuere el caso

Un videojuego que permite el chat dentro del videojuego es el FORTNITE, además del chat en vivo usando la palanca mediante los auriculares, esto se puede observar en la figura 38.

Figura 38. – Chats en vivo dentro del videojuego Fortnite.

Fuente: *Autor*

Información de la cuenta

La información que contiene la cuenta de usuario de la PS4, es de vital importancia porque contiene la información personal del usuario, tales como:

- Id de inicio de sesión
- Perfil
- Nombres reales
- Foto de perfil
- Descripción (acerca de mi)

Para acceder a esta información, se dirige al menú superior, configuración, administración de las cuentas y finalmente la pestaña información de la cuenta, como se observa en la figura 39 esta contiene este tipo de datos.

Figura 39. – Datos personales del usuario.
Fuente: *Autor*

Además, se puede ingresar y determinar con que ID de usuario se inicia la sesión, brindando un correo personal para su posterior proceso de repudio de correos, como se observa en la figura 40 esta contiene este tipo de datos.

Figura 40. – Id de inicio de sesión de la PS4 Slim.
Fuente: *Autor*

Play Station Store

La Play Station Store contiene información de relevancia, como datos personales e información bancaria, esto se accede en el menú principal mediante la pestaña Play Station Store, luego se selecciona un juego al azar, luego agregar al carrito y

continuar para finalizar la compra, como se observa en la figura 41, se cuenta con esta información.

Figura 41. – Datos bancarios del usuario de la PS4 Slim.
Fuente: *Autor*

Historial de Navegador

El historial de navegación determina las páginas web que fueron visitadas, la desventaja mostrada es que no se brinda información de hora o fecha de navegación, como se ve en la figura 42, esta información se obtiene en el menú principal, navegador, se pulsa en la palanca el botón “options” y seleccionados la pestaña historial de navegación.

Figura 42. – Historial de navegación de la consola PS4 Slim.
Fuente: *Autor*

3.6.4. Fase de Análisis

Es la fase fundamental del procedimiento de análisis forense, ya que es la fase en donde se determina que información fue recopilada luego de los procesos de preservación y adquisición. El perito hará muestra de todo su conocimiento el mismo que determinará donde, como, quien y en qué tiempo se recoleto la información haciendo uso de la evidencia recolectada.

No existe ningún proceso estandarizado para el análisis de la información y se determinará cada resultado de acuerdo al criterio del investigador.

Caso 1. – Equipo Apagado

Una prueba inicial del disco duro de la PS4 Slim, utilizando la herramienta forense Ftk Imager 4.2, determino que la estructura del disco consiste en un sistema de archivos desconocido, el mismo que se encuentra dividida en 15 particiones, como se puede ver en la Fig. 43; además la imagen forense que se realizó arrojó un solo archivo que no presentaba ningún archivo, como se observa en la figura 44. Nuestro análisis de la PlayStation 4 Slim se concentrará sobre el uso de la interfaz de usuario nativa para localizar información.

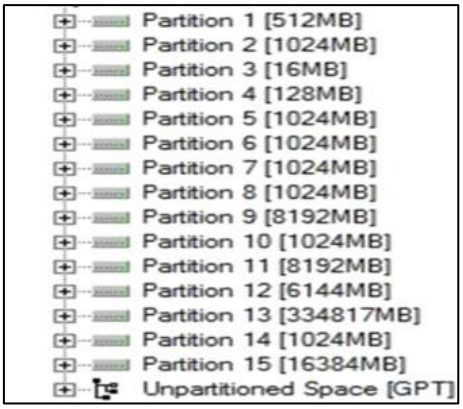

Figura 43. – Particiones del disco duro de la PS4 Slim.

Fuente: *Autor*

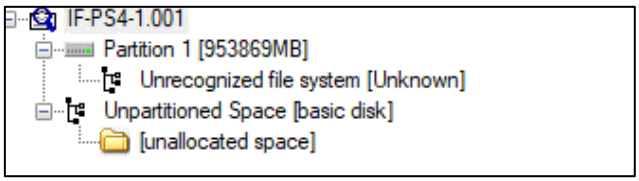

Figura 44. – Imagen forense del disco duro de la PS4.

Fuente: *Autor*

Se emplea la utilidad de tallado de datos de FTK Imager 4.2 en un intento de recuperar archivos adicionales de una imagen forense tomada de la PlayStation 4 Slim. Pero la herramienta forense FTK Imager v4.2 no pudo detectar la presencia de ningún archivo. Esto sugiere fuertemente el cifrado o un formato de contenedor a medida.

Caso 2. – Equipo Encendido

Datos encontrados en diferentes pestañas

Luego de la búsqueda de datos en la consola PS4 Slim, mediante su interfaz de usuario, se encuentra con datos de relevancia como nombres, o id de usuario; con el que al obtener un correo personal se puede realizar un repudio de correos y llegar

al dueño de la cuenta. Además de datos bancarios relevantes para obtener datos reales del usuario de la consola.

Se encontró con el contenido del disco duro, donde se observó el almacenamiento de los juegos y capturas de pantalla realizadas por el usuario las mismas que cuentan con un registro de hora y fecha. Se determina el estado de la conexión de red, y el uso de la interfaz de red en el momento del análisis.

Los mensajes y amigos del usuario se encontraron con registro de hora y fecha, además se pueden visualizar claramente imágenes enviadas o datos enviados a través de la interfaz de chat.

Prueba de tiempo y fecha

Se llevó a cabo un análisis de todo el sistema de la Sony PlayStation 4 Slim, centrándose principalmente en la recuperación de información de fecha y hora. Se descubrió que la mayoría de las funciones, como Trofeos, Novedades, etc., brindaban esta información. Por otro lado, las aplicaciones como el navegador web de Internet no presentaban ningún tipo de información de fecha y hora, mientras que como se habló anteriormente las funciones de mensajes presentaban las fechas y horas en que se enviaban y recibían los mensajes.

Navegador web, historial de marcadores y elementos recientes

Se determinó que el navegador web almacena cualquier tipo de web visitada, sin presentar alguna restricción por tener un navegador nativo de Play Station. Además, los términos de búsqueda de Google también aparecen en el historial del navegador web de PlayStation 4 Slim.

Además, un análisis del historial del navegador web, en donde los marcadores y las páginas más utilizadas que aparecen no presentaban la hora y la fecha en que ocurrieron los eventos, determinado que esta información no se puede obtener a través de la interfaz nativa.

Se trato de descargar fotos desde el navegador web hacia el disco duro, pero esta opción no fue culminada con éxito por bloqueo de la consola; donde se pudo determinar que solo existen dos opciones para hacer esta tarea como es guardarlas como marcadores y pulsando el botón “share” de la palanca permitiendo guardarla como captura de pantalla.

Prueba de carga y descarga de USB

Se copiaron varios formatos de archivo desde un computador portátil en una unidad flash (USB) que previamente fue formateada con FAT32. Los archivos se almacenaron en una carpeta etiquetada TESIS_PS4 y consistió en 4 imágenes con formato jpeg, 1 imagen en formato png, 2 archivos formato pdf y variedad de formatos de Microsoft Office. La unidad flash USB se insertó en la PlayStation 4 Slim y se realizaron varios intentos para cargar los archivos, con lo que se determinó que no era posible cargar dichos archivos en la PlayStation 4.

Se realizó una investigación previa del tipo de contenido que un usuario puede descargar en una memoria USB; existe una función llamada ShareFactory que permite la creación de videos de los juegos los mismos que se guardan en el disco duro de la consola. Finalmente, a través de la galería de capturas que se encuentran en el disco duro se pudo duplicar el contenido a una memoria USB.

Una vez obtenido la información de las capturas de los videos e imágenes de la consola PS4, se puede realizar un proceso de metadatos en estos archivos, lo que permite brindar una información detallada de los archivos a analizar.

3.6.5. Fase de Documentación

En esta fase, el perito informático deberá contar con toda la información necesaria para poder redactar su informe pericial, este es el documento que contendrá toda la información de relevancia que cumpla con el objetivo de la perica; se considera el Artículo 511 del COIP, el mismo que expresa en el numeral 5 sobre el plazo para presentar y defender el informe, así como en el numeral 6 dicta sobre el contenido mínimo que debe estar presente en el informe pericial.

En la Resolución 040-2014, también trata en su Artículo 21 sobre los contenidos mínimos obligatorios de un informe pericial; además de presentarse una aclaración o explicación extra se seguirá la norma que determina una defensa verbal o escrita de acuerdo al Artículo 19 y 20 de la misma resolución.

3.6.6. Fase de Presentación

Una vez terminadas las fases previas, la fase de presentación culmina la metodología propuesta. En esta fase el objetivo principal es la sustentación de la pericia, en donde el perito presentara sus resultados de manera oral, siendo esta su principal obligación, ya sea en procesos civiles como penales. El perito durante la defensa deberá contar la capacidad y el conocimiento suficiente para defender su informe

pericial, sin caer en ambigüedades, evitando dar juicios de valor, centrándose netamente en el objetivo de la pericia.

El Artículo 505 del COIP determina que *"Los peritos sustentarán oralmente los resultados de sus peritajes y responderán al interrogatorio y al contrainterrogatorio de los sujetos procesales."*

De igual manera en el Artículo 222 del COGEP, *"Declaración de peritos. 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".*

El perito deberá aclarar el informe las veces que sean necesarias, de acuerdo a solicitud de la o el Juez, así como lo dicta el Artículo 503 del COIP en su numeral 3, *"Las y los testigos o peritos volverán a declarar cuantas veces lo ordene la o el juzgador en la audiencia de juicio."*

Una vez finalizado toda la investigación, el perito tiene la obligación de devolver todos los elementos que fueron incautados en el allanamiento, con lo que se termina el caso para el que fue asignado el perito.

3.7.ELABORACIÓN DE LA GUÍA

Una vez culminada la metodología de análisis forense de la consola de videojuegos Play Station 4 Slim, se realiza una guía de pasos sencillos y en lenguaje entendible para que pueda ser aplicado por cualquier perito informático que se encuentre dentro de la Función Judicial del Ecuador.

3.7.1. Diagrama de la guía de pasos

Para tener una mejor visión de la guía de pasos a proponer, se presenta en la figura 45, un diagrama de bloques especificando los procesos y el camino más óptimo de acuerdo al estado inicial en el que se encuentra la consola de videojuegos PS4.

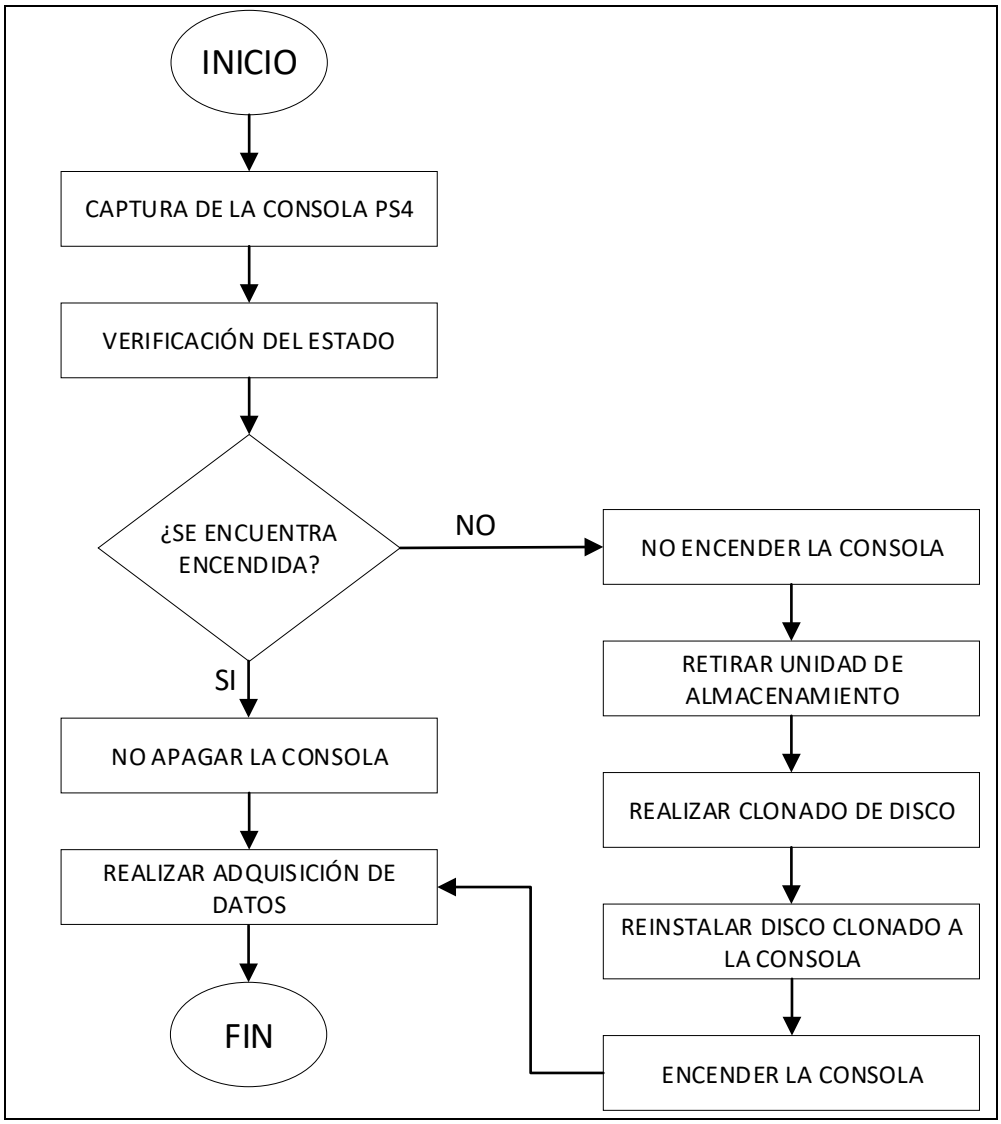

Figura 45. – Diagrama de bloques de la guía de pasos.

Fuente: *Autor*

3.7.2. Desarrollo de la Guía

La presente guía será una referencia de las buenas prácticas de análisis forense para la consola de videojuegos Play Station 4 Slim, que puede ser aplicada por los especialistas en Peritaje Informático que conforman parte de la Sistema Pericial Integral De La Función Judicial del Ecuador.

Para dar inicio a la guía, se sobreentiende que los pasos antes mencionados como son la Preservación, la tomarán en consideración los profesionales en Peritaje informático siguiendo la Normativa Legal del Ecuador, como fue expuesta en apartados anteriores.

Para la fase de adquisición y análisis se presentan los pasos a seguir a continuación:

Paso 1

El inicio de la guía es la preservación de la evidencia siguiendo la normativa legal del Ecuador, como el proceso lo determina es la “Captura de la Consola”.

Paso 2

Este paso está determinado en la verificación del estado en el que se encuentra la evidencia, se presentan dos casos:

a) Consola Apagada

1.- No encender la consola.

2.- Desconectar toda conexión eléctrica de la consola.

3.- Identificar la ubicación de la unidad de almacenamiento.

La misma se encuentra en la parte posterior de la consola, este paso requerirá de guantes antiestáticos.

Figura 46. – Identificación de la unidad de almacenamiento.
Fuente: *Autor*

4.- Retiro de la tapa de protección del disco duro

Figura 47. – Retiro de la protección del disco duro.
Fuente: *Autor*

En este paso se realiza una leve presión entre las esquinas y extraerla en dirección a la indicada en la figura 47.

5.- Retirar la tapa protectora, e identificar el tornillo de fijación del disco duro.

Figura 48. – Identificación del tornillo de fijación.
Fuente: *Autor*

Este tornillo es del tipo “estrella”, como se observa en la figura 48.

6.- Retirar el tornillo y extraer el disco duro desde la cejilla

Figura 49. – Extracción del tornillo de fijación.
Fuente: *Autor*

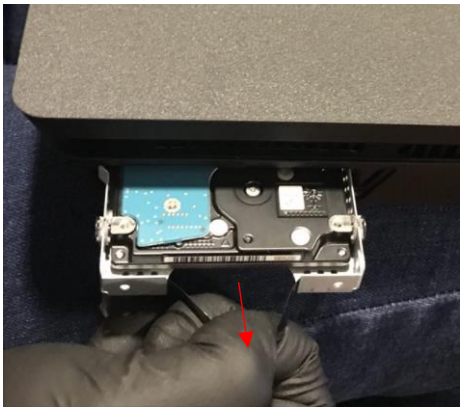

Figura 50. – Extracción del disco duro.
Fuente: *Autor*

7.- Una vez extraído el disco duro, se hace uso del esclavizador de discos para su posterior clonado en un disco duro nuevo y formateado.

Figura 51. – Kit de esclavizador de discos duros.
Fuente: *Autor*

8.- Se hace uso del software de clonación de discos EaseUS Todo Backup, donde se sigue los siguientes pasos:

- Se ejecuta el programa
- Se ubica la pestaña de copia de seguridad o creación de imagen, como recomendación se debe marcar todo el disco.
- Se selecciona la fuente de la creación de la imagen del disco.
- Solicita un nombre de etiqueta de la imagen
- Se coloca en guardar y se dé inicio al proceso.
- Una vez finalizado el proceso, se restaura la imagen creada en el disco en blanco, en la opción “recuperación” en los registros de backups.
- Se selecciona la totalidad del disco para recuperar (no escoger particiones), para obtener una copia idéntica del disco duro de la PS4.
- Se selecciona la unidad de destino, de igual manera se escoge la totalidad del disco
- Se da un clic en proceder y en ok siempre luego del mensaje de perdida de la totalidad de datos en el disco destino.
- Una vez finalizado el proceso se obtiene la imagen copia del disco duro de la PS4 Slim.

Figura 52. – Disco duro clonado.
Fuente: *Autor*

9.- Instalación del disco duro clonado en la consola PS4 Slim.

Figura 53. – Instalación del disco duro clonado.
Fuente: *Autor*

10.- Fijar las protecciones del disco duro

Figura 54. – Colocación de las protecciones del disco duro.
Fuente: *Autor*

11.- Una vez culminado el proceso de fijación de las protecciones coloca todas las conexiones eléctricas de la consola PS4

Figura 55. – Colocación de las conexiones eléctricas de la consola.
Fuente: *Autor*

12.- Se enciende la consola

Figura 56. – Encendido de la consola con disco duro clonado.
Fuente: *Autor*

13.- Una vez los pasos cumplidos se realiza la adquisición de la información siguiendo los preceptos como si en su estado inicial esta hubiese estado en encendida, como lo determina el literal b) consola encendida, a partir del punto 2.

b) Consola Encendida

1.- Cuando en el momento inicial de la investigación, la consola se encuentra en estado de encendida, no se debe apagar la consola bajo ninguna circunstancia. Se debe mantener encendida el tiempo que dure la adquisición de la información.

2.- Al tratar de analizar la memoria RAM de la consola, se imposibilita dada la arquitectura interna de la PS4 Slim, al no existir un procedimiento de extracción de datos de la memoria RAM en circuitos integrados que se encuentran soldados con tecnología de montaje superficial (SMD).

3.- Proceso de extracción de datos digitales usando la interfaz de usuario de la consola PS4 Slim, de acuerdo a la norma RFC 3227.

- Contenidos de logs y registros de la consola

Para poder visualizar el registro de actividades de la consola, se dirige al menú superior y seleccionar la pestaña notificaciones, donde se puede observar, todas las actividades que en la consola se han realizado desde el principio de su instalación, existe un registro con fecha, pero no con hora; a diferencia de los trofeos y premios que si contienen esta información.

- Estado de las diferentes conexiones de red

Para realizar este procedimiento, se ubica al menú superior, luego en la pestaña configuración, seguido de red y ver estado de conexión, donde se obtiene la información relevante acerca de las conexiones de red activas, así como la dirección IP, mascara de subred y método de conexión.

- Contenido del disco duro

Un componente importante es poder determinar que contenido esta guardado en el Disco Duro de la consola, ya que se puede establecer con qué tipo de contenido el perito puede encontrarse.

Para acceder a esta información, se ubica el menú principal, luego configuración, almacenamiento y almacenamiento del sistema, donde se presenta con la información que contiene la consola, como se observa en la figura 57.

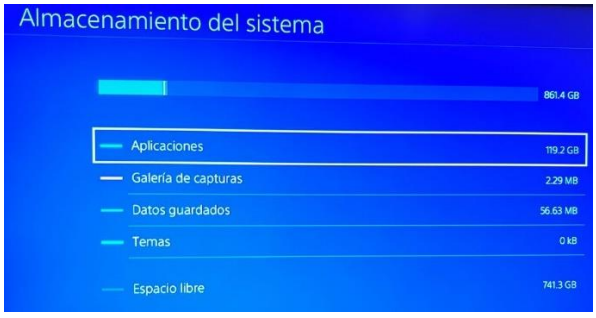

Figura 57. – Contenido del disco duro de la consola PS4 Slim.
Fuente: *Autor*

Una vez dentro de este menú, se presentan con 4 pestañas de contenido donde están las aplicaciones, galería de capturas, datos guardados de los juegos y temas para la consola. Dentro de este menú, se ubica el menú de capturas las cuales s encuentran con un registro de hora y fecha que fue realizada por el usuario.

- Contenido de terceros dispositivos de almacenamiento

Se determina que dispositivos de memoria externa se encuentran conectados a la consola, como una memoria flash del tipo USB o una expansión del disco duro de la consola.

Primero se determina, si están siendo usados en los procesos actuales de la consola, si es de esa manera primero se realiza todo el proceso de extracción de los datos desde la interfaz, para una vez terminado el proceso, desconectar dichos dispositivos de memoria externa, para su posterior análisis forense siguiendo las metodologías ya existentes.

- Hora y fecha actualmente configurada del sistema

Es de vital importancia determinar con qué fecha y hora la consola está configurada, ya que mediante esto se puede trazar una línea de tiempo de todos los eventos que pueden haber ocurrido con la consola.

Esto se consigue accediendo al menú superior, pestaña configuración y finalmente hora y fecha; donde se puede visualizar la hora y fecha de configuración de la consola, así como la zona horaria y los formatos de las mismas.

- Todas las conexiones de red que se puedan tener

Este apartado está relacionado con el estado de la red, ya que se puede determinar que interfaces de red están siendo utilizadas por la consola. La PS4 Slim, cuenta con conexión LAN y Wifi, esta información la se obtiene al seguir el menú superior, configuración, red y configurar conexión a internet.

- Absolutamente todos los usuarios que pueden estar conectados localmente, así como de manera remota

La consola Play Station 4 Slim no cuenta con visualización de multitarea en su interfaz, y los usuarios que se encuentran conectados de manera local solo se pueden establecer cuando se relaciona una palanca DualShock4 con un perfil específico creado en la consola. En este caso existió dos palancas y por lo tanto dos usuarios conectados de manera local a la consola PS4 Slim.

- Aplicaciones abiertas y Videojuego en ejecución

Las aplicaciones que se encuentran corriendo al momento del allanamiento, permiten determinar las acciones que el usuario de la consola PS4 Slim estaba ejecutando en el instante previo a la preservación de la evidencia. En el menú principal, se pulsa el botón PS de la palanca que permite obtener la información de las aplicaciones y juegos que actualmente están ejecutándose en la consola.

- Chats iniciados

Los mensajes o chats que se encuentran iniciados y en proceso de ejecución es de vital importancia, porque se puede establecer las conexiones, los usuarios y la razón de comunicación con que el usuario principal tuvo con diferentes usuarios de Play Station a nivel mundial. Esto se puede visualizar accediendo al menú superior en la pestaña mensajes.

- Chats dentro del videojuego si fuere el caso

Este apartado dependerá únicamente del juego que este ejecutándose al momento de analizar la información en caliente, ya que no todos los juegos cuentan con la opción de chat dentro del videojuego.

- Información de la cuenta

La información que contiene la cuenta de usuario de la PS4, es de vital importancia porque contiene la información personal del usuario, tales como:

- Id de inicio de sesión
- Perfil
- Nombres reales
- Foto de perfil
- Descripción (acerca de mi)

Para acceder a esta información, se ubica al menú superior, configuración, administración de las cuentas y finalmente la pestaña información de la cuenta.

Además, se puede ingresar y determinar con que ID de usuario se inicia la sesión, se lo hace siguiendo los pasos anterior mente mencionados con el único cambio de que luego de la pestaña cuentas, se ingresa a ID de inicio de sesión, brindando un correo personal para su posterior proceso de repudio de correos.

- Play Station Store

La Play Station Store contiene información de relevancia, como datos personales e información bancaria, esto se accede en el menú principal mediante la pestaña Play Station Store, luego se selecciona un juego al azar, luego agregar al carrito y continuar para finalizar la compra.

- Historial de Navegador

El historial de navegación determina las páginas web que fueron visitadas, la desventaja mostrada es que no se brinda información de hora o fecha de navegación, esta información se la obtiene en el menú principal, navegador, se pulsa en la palanca el botón “options” y seleccionados la pestaña historial de navegación.

Paso 3

Una vez obtenida la información, el perito cuenta con todos los datos para su análisis y documentación de los resultados.

Paso 4

El perito presentará sus resultados, plasmándolos en un informe pericial como se observa en el Anexo 1, para su posterior defensa siguiendo las normas presentes en el COIP, COGEP y la Resolución 040-2014.

Paso 5

Finalizado todo el proceso, se da por terminado la guía, en donde el perito por ley devolverá todos los dispositivos que en su momento fueron allanados para fines de investigación.

CAPÍTULO IV

CONCLUSIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

4.1. Conclusiones

Las consolas de videojuegos cumplen la función para la que fueron diseñadas, como es el entretenimiento y la diversión; pero muchas veces estas consolas en manos equivocadas son usadas para otros fines, se determinó que las consolas de videojuegos presentan puntos de vulnerabilidad de acuerdo a la aplicación o servicio que brinda. Los delitos que se pueden dar en las consolas de videojuegos y específicamente en la consola PS4 Slim, van desde un acoso, extorsión hasta delitos de gran impacto como es la pornografía infantil.

Al realizar una comparación entre las consolas que están en lucha por el liderato del mercado, como es la PlayStation 4 Slim y la Xbox One y con el fin de validar un bajo grado de concordancia con investigaciones similares, se puede concluir que, ambas consolas cuentan con ciertas similitudes en comunicación, almacenamiento, y procesador; pero, la consola Play Station 4 Slim muestra puntos relevantes en su sistema de archivos NO estándar, a diferencia de la Xbox One que usa NFTS. En términos Forenses se está hablando de dos dispositivos completamente distintos ya que la forma en que se guardan la información en los dispositivos es completamente diferente.

Cada dispositivo electrónico que tenga o funcione de manera similar a otro dispositivo del cual ya exista una metodología, no necesariamente deberá aplicarse las mismas técnicas forenses, ya que presenta un reto distinto en términos forenses al tener un tipo de información y un sistema de archivos propio para cada dispositivo con un distinto nivel de encriptación.

El análisis de los datos extraídos del disco duro de la PS4 Slim, utilizando herramientas forenses tradicionales, mostró una estructura del disco con un sistema de archivos desconocido, dividido en 15 particiones, en las cuales no se cuenta con archivos reconocibles, es decir no se pudo detectar la presencia de ningún archivo, esto demuestra un cifrado de disco robusto, por lo que la medida más recomendable fue utilizar nuevos métodos de extracción de datos digitales.

El análisis de la PlayStation 4 Slim se concentró sobre el uso de la interfaz de usuario nativa para localizar información relevante para el perito. Utilizando esta técnica, se encontraron datos de relevancia como nombres, o id de usuario; con el que al

obtener un correo personal se puede realizar un repudio de correos y llegar al dueño de la cuenta. Además de datos bancarios relevantes para obtener datos reales del usuario de la consola. Sin embargo, se cuenta con horas y fechas en capturas de pantalla realizados por el usuario, estados de conexión de red, los y registros de actividad; así como mensajes enviados, recibidos con registros de tiempo, historial del navegador web y la posibilidad de hacer análisis de metadatos a través de imágenes extraídas del disco a través de una memoria flash externa.

La metodología propuesta, permitirá a los Peritos que forman parte del Sistema Integral Pericial de la Función Judicial, realizar un análisis de la consola PlayStatión4 protegida contra lectura, previniendo la alteración de los datos, manteniendo la integridad probatoria de acuerdo a la Normativa Legal del Ecuador. También permite ofrecer conocimientos nuevos a los profesionales de la rama, con el fin de agilizar los procesos judiciales cuando se tenga con prueba del delito una consola de videojuegos PS4 Slim.

4.2. Recomendaciones

Se recomienda que las técnicas, procedimientos y herramientas que se utilizaron en la presente investigación sean usadas para futuras aplicaciones forenses, ya que están basadas en normas y guías de buenas prácticas, que se aplicaron conjuntamente con la Normativa Legal del Ecuador, garantizando que la información que se extraiga sea reconocida y validada por el Sistema Judicial, evitado una posible descalificación de la prueba.

Al momento de realizar la extracción de los datos en una consola encendida, se recomienda realizarlo en la brevedad posible, ya que una de las mayores desventajas de la Play Station Network, es que se puede ingresar a la cuenta desde cualquier dispositivo que tenga acceso a Internet, lo que permitiría un posible borrado de perfil y datos personales que se quisieran analizar.

Se debe tener un especial cuidado al momento de extraer el dispositivo de memoria de la consola PS4 Slim, ya que los componentes electrónicos son sensibles a cargas estáticas; por lo que se recomienda el uso de guantes aislantes y de una manilla antiestática, permitiendo así la preservación de la prueba para su posterior proceso de normalización del dispositivo.

La presente guía de análisis forense se recomienda ser difundida y aplicada por peritos informáticos de la Función Judicial del Ecuador, con el afán de lograr importancia al fortalecer conocimientos y resolver futuros casos donde exista una consola de videojuegos PS4 Slim.

4.3.Trabajos Futuros

A medida que la tecnología avanza, cada vez son más los accesorios y las opciones de interactividad que implementa la PlayStation 4 Slim, los mismos que pueden requerir investigación propia para cada actualización. Una de las nuevas opciones es la cámara de la PlayStation, esta permite a los usuarios utilizar características de seguridad mejoradas, como es el reconocimiento facial para inicio de sesión. Esta característica podría usarse para proteger la consola, pero también podría usarse para probar la identidad del usuario que es propietario de la cuenta en un sistema, ya sea en de usuario único o multiusuario. La investigación futura debería considerar la importancia de la capacidad de las conexiones de PlayStation 4 Slim con la aplicación de Sony Vita y la aplicación "PlayStation Companion" en *Smartphones* y en *Tablets*. Donde, cualquier tipo de información de transferencia de datos de propiedad y de comunicaciones será de interés para los investigadores. Además, deberá considerarse que para futuras consolas creadas por la compañía Sony como la Play Station 5, deberá considerarse si la metodología creada cumple con los requerimientos de extracción de datos digitales, en todo al tipo de información que guarda y al sistema de archivos que esta manejaría.

CAPÍTULO V

BIBLIOGRAFÍA

Access, D. (2018). FTK® Imager 3.4.2. Retrieved from http://marketing.accessdata.com/ftkimager3.4.2

AENOR. (2013). UNE 71506:2013. Retrieved from https://www.aenor.com/normas-y-libros/buscador-de-normas/UNE?c=N0051414

Aguinaga, C. (2016). Cibercrimen: modalidad delictiva que más puede crecer. Retrieved from https://losandes.com.ar/article/cibercrimen-modalidad-delictiva-que-mas-puede-crecer

Autopsy. (2018). Autopsy, Digital Forensics. Retrieved from https://www.autopsy.com/Castañeda, F., Rojas, V., Villanueva, N., & Prudente, M. (2009). *Evaluación de Herramientas para Análisis Forense Orientado a Discos Duros*. Retrieved from https://tesis.ipn.mx/handle/123456789/5250

Conrad, S., Rodriguez, C., Marberry, C., & Craiger, P. (2009). Forensic Analysis of the Sony Playstation Portable. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics V* (pp. 119–129). Berlin, Heidelberg: Springer Berlin Heidelberg.

Conrad, S., Dorn, G., & Craiger, P. (2010). Forensic Analysis of a PlayStation 3 Console. In K.-P. Chow & S. Shenoi (Eds.), *Advances in Digital Forensics VI* (pp. 65–76). Berlin, Heidelberg: Springer Berlin Heidelberg.

Consejo de la Judicatura. (2014). *Reglamento del sistema pericial integral de la función judicial.* Quito. Obtenido de http://www.funcionjudicial.gob.ec/

Córdova, B. (2018). *Metodología Para El Análisis Forense De La Información Digital Contenida En Consolas De Videojuegos En El Ecuador, Caso De Estudio Xbox One*. UISEK.

Cuenca, H. (2016). El Delito Informático: Su Evolución, Punibilidad y Proceso Penal en el Ecuador. Pontificia Universidad Católica del Ecuador. Retrieved from http://repositorio.puce.edu.ec/bitstream/handle/22000/6966/13.J01.001569.pdf?sequence=4&isAllowed=y

Davies, M., Read, H., Xynos, K., & Sutherland, I. (2015). Forensic analysis of a Sony PlayStation 4: A first look. *Digital Investigation*, *12*, S81–S89. https://doi.org/https://doi.org/10.1016/j.diin.2015.01.013

Ecucert. (2018). Incidentes en el Ecuador. Retrieved from https://www.ecucert.gob.ec/incidente.html

Estrada, M. (2008). DELITOS INFORMÁTICOS. Retrieved from https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

Iriarte, E. (2008). Meta 25 eLAC2007: Regulación en la Sociedad de la Información en America Latina y el Caribe. Retrieved from https://www.cepal.org/socinfo/noticias/noticias/2/32222/GdT_eLAC_meta_25.pdf

Jinza. (2013). UNE 71506:2013 Sistema de Gestión de Evidencias Electrónicas (SGEE). Retrieved from http://www.foroevidenciaselectronicas.org/2013/11/11/une-715062013-sistema-de-gestion-de-evidencias-electronicas-sgee/

Loarte B, Grijalva J. (2017). Elaboración de un marco de trabajo estandarizado para el análisis forense de la evidencia digital en procesos civiles y penales en el

Ecuador para ser utilizado por los Peritos acreditados en Informática por el Consejo de la Judicatura del Ecuador. *Revista Publicando*, 42-78.

Loarte, B., & Grijalva, J. (2017). *Modelo para el análisis forense y la legalización de evidencia digital atípica en procesos judiciales en Ecuador*. Retrieved from http://repositorio.uisek.edu.ec/handle/123456789/2952

López O, Amaya H, León R. (FEBRERO de 2002). *Informática Forense, Generalidades, Aspectos Técnicos Y Herramientas*. Obtenido de URRU: http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf

Manzano, J. (2012). *Análisis de Herramientas y Técnicas de Apoyo a la Recuperación de Información Cifrada*. UNIVERSIDAD DE ALCALÁ. Retrieved from http://hdl.handle.net/10017/30209

Martínez, A. (18 de Junio de 2014). *RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento*. Obtenido de https://www.certsi.es/blog/rfc3227

Méndez, M. (2013). PlayStation 4 vs Xbox One, comparadas punto por punto. ¿Cuál es mejor? Retrieved from https://es.gizmodo.com/la-playstation-4-por-dentro-pieza-a-pieza-1465063482

Microsoft, C. (2018). XBox One. Retrieved from https://www.xbox.com/es-ES/xbox-one-s

Moreno, G. (9 de 12 de 2016). *Statista*. Obtenido de https://es.statista.com/grafico/7159/la-playstation-4-alcanza-los-50-millones-de-ventas/

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

Sony Computer Entertainment America, L. (2014). *User profiles on PS4*. Obtenido de https://support.us.playstation.com/app/answers/detail/a_id/5065/~/ps4-remote-play-and-second-screen

Telégrafo. (2017). En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario. *El Telégrafo*. Retrieved from https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Wismark, P. (2009). Des/Encriptacion en la Informática Forense. *RITS*, 41–45. Retrieved from https://s3.amazonaws.com/academia.edu.documents/31755419/RITS_3_INFORMATICA_FORENSE.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1531588122&Signature=hGgLZ7avJS0LHcLu%2FZYJGWwWG%2BM%3D&response-content-disposition=inline%3B filename%3DRITS_3_INFORMATICA_FORENSE.pdf#page=42

ANEXO 1

FORMATO DE INFORME PERICIAL

Las y los peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCION JUDICIAL. Por lo tanto, el presente formato es de uso obligatorio para la presentación de los informes periciales, sin perjuicio de lo establecido en normas legales específicas.

"INFORME PERICIAL"

1. DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA

Nombre Judicatura o Fiscalía	
No. de Proceso	
Nombre y Apellido de la o el Perito	
Profesión y Especialidad acreditada	
No. de Calificación	
Fecha de caducidad de la acreditación	
Dirección de Contacto	
Teléfono fijo de contacto	
Teléfono celular de contacto	
Correo electrónico de contacto	

2. PARTE DE ANTECEDENTES, en donde se debe delimitar claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por el juez, el fiscal y/o lo solicitado por las partes procesales.

3. PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE, en donde se debe explicar claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. La o el perito deberá relacionar los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizará si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

4. PARTE DE CONCLUSIONES, luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. Se prohíbe todo tipo de juicios de valor sobre la actuación de las partes en el informe técnico. El informe solamente versará sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dirá sobre el accionar de las partes procesales en el caso en particular. Las conclusiones solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no será tomado en cuenta al momento de resolver, y será tomado en consideración para la evaluación de la o el perito.

5. PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO, deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, etc); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas de la o el perito para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos o con la explicación técnica y científica exigida en este numeral. La o el perito deberá razonar y motivar diáfanamente la razón de sus dichos, esto es, justificar desde todo punto de vista las conclusiones que incluya en el informe. En caso de que no fundamente sus conclusiones y esto sea informado por el juez, la jueza, o el/la fiscal, será considerado al momento de la evaluación de la o el perito.

6. OTROS REQUISITOS, si la ley procesal correspondiente determina la inclusión de requisitos adicionales a los establecidos por el reglamento, la o el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.

7. INFORMACIÓN ADICIONAL, la o el perito podrá incluir cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.

8. DECLARACIÓN JURAMENTADA, la o el perito deberá en la parte final del informe, declarar bajo juramento que su informe es independiente y corresponde a su real convicción profesional, así como también, que toda la información que ha proporcionado es verdadera.

9. FIRMA Y RÚBRICA, al final del informe se deberá hacer constar la firma y rúbrica de la o el perito, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."