MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

MARCO DE REFERENCIA PARA EL DESARROLLO DE UN ANÁLISIS FORENSE A FUENTES DE EVIDENCIAS DIGITALES EN SISTEMAS INFOTAINMENT DE VEHÍCULOS

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:

Javier Fernando LEON CABRERA

Bajo la dirección de:

Roberth Darío CHAVEZ JARA.

Universidad Espíritu Santo

Maestría en Auditoría de Tecnología de la Información

Samborondón - Ecuador

Abril del 2018

Marco de referencia para el desarrollo de un análisis forense a fuentes de evidencias digitales en sistemas infotainment de vehículos.

Framework for the development of a forensic analysis to sources of digital evidence in vehicle infotainment systems.

Javier Fernando LEON CABRERA [1]
Roberth Darío CHAVEZ JARA [2]

Resumen

Dentro del análisis forense informático existen varios marcos de referencia, unos tradicionales y otros específicos dirigidos a equipos de computación o algún otro equipo en especial, que permiten al investigador llevar adelante un análisis forense digital. Pero existen dispositivos que por sus características particulares, requieren un tratamiento diferente como los equipos infotainment de vehículos, para los cuales no existe un marco que permita cumplir un proceso forense que cubra las exigencias que se presentan estos dispositivos durante una investigación. Por esta razón, se presenta un trabajo que aborda el análisis forense desde una perspectiva de los dispositivos infotainment de vehículos, fundamentado en la revisión literaria sobre los equipos de información y entretenimiento para vehículos, sus características técnicas, así como de las recomendaciones y dificultades que se presentan dentro de un trabajo forense. De igual forma se fundamenta con la revisión literaria de otros marcos de referencia, cuyas fases pueden ser aplicables a este tipo de tecnología. Esto permitirá un mejor manejo en los procesos de adquisición de imágenes forense y análisis de las evidencias lo que evitará una afectación a la cadena de custodia. Esta investigación presenta un marco de referencia específico para llevar adelante un análisis forense sobre equipos infotainment de vehículos, en donde cada fase cubre los requerimientos que este tipo de tecnología exige, así mismo permite cumplir con el objetivo y principios del análisis forense. La validación de este marco se lo realizó mediante la técnica de grupo focal, que permitió la participación de profesionales con gran experiencia en el área, logrando obtener información de forma cualitativa, que mostró la perspectiva de cada uno de ellos sobre el marco de referencia presentado.

Palabras clave: | Forense 1, Evidencia 2, Infotainment 3, Vehículos 4, Digitales 5.

Abstract

Within the computer forensic analysis there are several frames of reference, some traditional and others specific to computer equipment or some other special equipment, that allow the researcher to carry out a digital forensic analysis. But there are devices that, due to their particular characteristics, require a different treatment, such as vehicle infotainment equipment, for which there is no framework that allows a forensic process to be fulfilled that covers the demands that these devices present during an investigation. For this reason, a paper is presented that addresses forensic analysis from a vehicle infotainment perspective, based on the literary review of information and entertainment equipment for vehicles, its technical characteristics, as well as recommendations and difficulties They are presented within a forensic work. Similarly, it is based on the literary review of other frames of reference, whose phases may be applicable to this type of technology. This will allow a better management in the processes of forensic image acquisition and analysis of the evidences which will avoid an affectation to the chain of custody. This research presents a specific frame of reference to carry out a forensic analysis on infotainment equipment of vehicles, where each phase covers the requirements that this type of technology demands, likewise allows to comply with the objective and principles of forensic analysis. The validation of this framework was carried out through the focus group technique, which allowed the participation of professionals with great experience in the area, obtaining qualitative information, which showed the perspective of each one of them on the reference framework presented.

Keywords | Forensic 1, Evidence 2, Infotainment 3, Vehicles 4, Digital 5.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail jleonc@hotmail.com.
[2] Máster en Diseño, Gestión y Dirección de proyectos, PMP, CISA, CISM, CRISC, y Certified Trainer at PECB – roberth.chavez@gmail.com

INTRODUCCIÓN

El aspecto más importante en un análisis forense informático es la búsqueda, extracción de datos digitales que puedan ser presentados como evidencia dentro de un proceso judicial o extrajudicial (Pino, 2016) .

Si bien, la metodología utilizada normalmente es la misma, se han generado varios marcos de referencia que permiten a los investigadores basarse en sus en sus procedimientos para poder sacar adelante una investigación que tenga características específicas ya sean por aspectos legales o por un escenario de investigación diferente.

Al ser una práctica utilizada comúnmente en la investigación de ambientes digitales, su campo de acción crece cada día con el desarrollo de nuevos productos que se fusionan con la tecnología, permitiendo así nuevas formas de interacción con los usuarios, lo que lleva a la generación de información, sea está procesada o almacenada, convirtiéndose de esta forma en un nuevo objeto en análisis en una investigación digital.

Una de las industrias que ha conseguido introducir nuevos dispositivos para sus clientes es la industria automotriz, que con la inclusión de equipos de entretenimiento y multimedia, denominados *Infotainment*, en sus vehículos permite la generación y almacenamiento de información proveniente de la sincronización con otros equipos tecnológicos o generada por la interacción con el propio usuario, así como por acciones propias el vehículo.

(LeMere & Bollo, 2017) dicen que esto ha llamado mucho la atención de las entidades de justicia y actualmente se considera a un vehículo como una fuente de información digital que necesariamente debe ser investigada si se encuentra involucrado en alguna actividad ilícita o simplemente que sean parte de algún proceso legal de cualquier índole donde se considere que la información que puedan brindar estos sistemas sirvan como evidencia en un caso.

Al convertirse un sistema infotainment de vehículos en una fuente potencial de evidencia, se generan requerimientos desde el campo judicial y privado para la búsqueda y extracción de algún tipo de Evidencia digital.

Aquí es donde los analistas forenses se encuentran con un nuevo ambiente poco convencional de trabajo, poniendo en práctica durante su investigación marcos de deferencia generales que pueden poner en riesgo el resultado de su trabajo al no cubrir los procesos necesarios que son requeridos para este tipo de equipos, pudiendo verse afectada la cadena de custodia[3], proceso fundamental para la valoración de una prueba.

Por esta razón, contar con un marco de referencia para sistemas infotainment, permitirá a investigadores forenses, peritos informáticos y auditores, asegurar que las tareas llevadas a cabo no sean calificadas como viciadas de nulidad al verse alterada la cadena de custodia.

MARCO TEÓRICO

Los Sistemas Infotainment de Vehículos

Infotainment es una palabra en inglés que nace de la unión de 2 términos, info que refiere a la palabra *information (información)* y tainment extraído de la palabra *entertaiment* (entretenimiento), encargado de definir a productos mediáticos que dentro de sus servicios manejan de forma hibrida estas 2 estas características. (Carrasco, 2014)

Esta nueva característica ha sido utilizada en varios campos de la industria para brindar mejores servicios o productos a sus usuarios, siendo el sector televisivo los primeros en incursionar en esta nueva tendencia (Berrocal, 2014).

(Scoltock, 2016) menciona que el área tecnológica no pudo quedarse atrás e introdujo

[3] Cadena de Custodia: Proceso que permite comprobar que una prueba no ha sido alterada y que se ha sido manejado acorde lo que dispone de la ley.

al mercado varios dispositivos que permite vivir la experiencia infotainment, siendo el sector automotriz uno de los más beneficiados, a tal punto que en la actualidad cada una de las unidades que salen al mercado cuenta con un dispositivo de este tipo.

(Simon , Bharath , & Matthias , 2015) consideran que el inicio de la era infotainment en vehículos inicia en el año 2007 provocado por el aumento exponencial en el uso de teléfonos móviles e inteligentes, lo que produjo la inclusión de aplicaciones de entretenimiento dentro de los automóviles. Además, resaltan que este cambio en la industria produjo que empresas como Blackberry's QNX, Google y Apple presenten productos con la finalidad de posesionarse en este mercado.

La principal característica de estos sistemas según (Aadarsh, Sneha , & Pooja, 2013) es la interacción que se produce entre el conductor o los ocupantes del vehículo con el equipo infotainment, cuando acceden a sus diferentes opciones como las aplicaciones de conectividad, de navegación (GPS) , recursos de audio y video o sincronización con el equipo celular, registrando así una gran cantidad de información en el equipo.

(Everett, 2013) nos dice que dentro de la arquitectura interna de estos sistemas existen varios componentes que permiten el envío y recepción de datos, entre los más importantes se tienen a las unidades de control electrónico (ECU), el cual es utilizado para realizar las tareas encomendadas por el usuario del vehículo así como el bus que maneja el área de control (CAN) que permite las comunicación entre los diferentes componentes para satisfacer las necesidades del usuario.
En la tabla 1 se detallan los componentes de un sistema infotainment de vehículos.

Tabla 1
Componentes sistema infotainment

Componente	Descripción
Bus CAN	(Control Área Network) Conecta los componentes de todos los buses.
Bus LIN	(Local Interconnect Network) Utilizada para trasmitir datos de redes de baja velocidad como del manejo de puertas y ventanas
FlexRay	Sub red utilizada para los mensajes de seguridad crítica, por ejemplo los sensores y el control de la estabilidad del vehículo.
Bus MOST	(Media Oriented System Transport) sub red utilizada para aplicaciones multimedia videos, streaming, cámaras retro entre otros.
OBD-II	Trasmite datos de diagnóstico del vehículo
Junction Box	Conecta el OBD-II con el bus CAN
Multimedia Head Unit	Sistema de info-entretenimiento, se comunica con las pantallas multimedia a través del Bus MOST y puede recibir datos también del bus CAN

Nota: Descripción de algunos componentes que intervienen dentro de la arquitectura de un sistema vehicular infotainment.

La informática forense

(Carrier B. , 2002) Nos dice que la metodología tradicional de la informática forense está basada en 4 pasos que son: la identificación, preservación, análisis, y la presentación de evidencias. Cada paso tiene sus características especiales que deben ser tomadas en cuenta por el analista forense para que su análisis sea óptimo y no recaiga en ilegalidad alguna. (Mouhtaropoulos, 2015). En la imagen 1 vemos los 4 pasos tradicionales de la metodología de la informática forense.

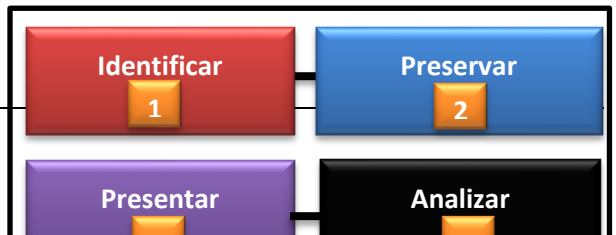

Imagen 1: Metodología tradicional del análisis forense informático.

Dentro del primer paso metodológico en la identificación de evidencia (Bulbul, 2013) señala que investigador forense levanta toda la información necesaria para llevar su análisis, es aquí donde se podrá tener las bases suficientes para saber lo que se va a investigar, en que dispositivos deberá enfocar su análisis, además podrá saber que recursos de hardware y software necesitara para realizar su trabajo.

La preservación de evidencia es el segundo paso dentro del análisis forense, (Casey, 2011) nos dice que es donde se genera procesos de resguardo que permite controlar la integridad de la información, menciona también que es muy común en este paso la generación de imágenes forenses de los dispositivos de almacenamiento y con estos sus respectivos códigos hash[4]

Posteriormente se encuentra la fase de análisis de datos donde (Carrier B. , 2006) nos dice que es el paso donde se aplican las técnicas y herramientas escogidas por el investigador para la búsqueda y extracción de las evidencias encontradas.

Así mismo hace referencia al último proceso metodológico que es la presentación del informe de hallazgos que maneja una particularidad y debe ser desarrollado para el entendimiento de personas poco conocedoras del tema informático.

Análisis forense a sistemas Infotainment

(Larry & Lars, 2012) dicen que un marco de referencial tradicional que está pensado para para computadores, o un ambiente digital específico, puede ser adaptado en investigaciones sobre sistemas infotainment de vehículos porque manejan procedimientos bien definidos, como el generar una copia de la evidencia digital, la de llevar a cabo un análisis de la información preservada o la presentación de un reporte final de investigación.

Pero (Park, Lee, & Kim, 2014) aclara que para efectuar un trabajo forense sobre una tecnología infotainment instalada en un vehículo es indispensable considerar el nivel de análisis requerido, los tipos de adquisición necesarias; porque un examen mientras más completo sea, puede requerir otro tipo procesos de los que nos ofrece un marco tradicional.

(Lacroix, 2017) dice que hay varios factores que diferencian un análisis forense de computadores a uno realizado a un sistema infotainment de vehículos, entre los más relevantes están: el ambiente donde se encuentran instalado, los diversos lugares de almacenamiento que maneja el dispositivo, los diferentes tipos de adquisición de evidencia que pueden realizarse, el uso frecuente de adquisiciones intrusivas y la diversidad de sistemas operativos existentes en el mercado. Esto muestra la necesidad de contar con nuevas propuestas dentro del campo forense informático, relacionadas a este tipo de dispositivos

La fase de adquisición o preservación es la más crítica, dentro de la cual (Edwards, 2014) nos recomienda que debemos tener claro la normativa legal sobre el tratamiento de evidencia digital que rige dentro de la jurisdicción de donde se realice este proceso, permitiendo llevar así un proceso limpio y sin ningún vicio de nulidad.

[4] Código Hash: Es una secuencia alfanumérica que identifica a un archivo de datos, es el resultado de aplicar un algoritmo matemático sobre un archivo digital. Esta secuencia permite controlar la integridad de una información, ya que si existiera una modificación dentro de sus contenidos la secuencia alfanumérica (código HASH) cambiaría.

Antes de iniciar con la adquisición forense de un sistema infotainment (SWGDE, 2016) recomienda identificar los diferentes medios de almacenamiento que pueda tener el dispositivo y su respectiva ubicación, resaltando la importancia de revisar las especificaciones del fabricante para localizarlos, acceder a ellos y proceder con la preservación de estos medios.
En la imagen 2 apreciamos un proceso de extracción física del dispositivo previa adquisición

Imagen 2: Extracción física de equipo infotainment. Fuente:,Carly McGee, What Exactly is Vehicle Forensics?, 2015.

Dentro de este tipo de sistemas se pueden llevar a cabo varios tipos de adquisiciones, lógicas, de archivos, física no intrusiva y física intrusiva, siendo esta ultima la que conlleva a realizar procesos adicionales por las necesidades técnicas y legales, así como por la necesidad de transportar el dispositivo a un laboratorio para generar este proceso, esto permite fortalecer la cadena de custodia dentro del proceso (Bortles, McDonough, & Smith, 2017).

En la tabla 2 de detallan los diferentes tipos de adquisición o preservación de evidencia de un sistema infotainment1.

Tabla 2
Tipos de adquisiciones de evidencia

Tipo de Adquisición	Descripción
Lógica	Adquisición de todo sistema el archivos o solo de una partición de la unidad de almacenamiento.
De archivos	Adquisición de parte de la información.
Física no intrusiva	Se puede acceder limpiamente a la unidades de almacenamiento
Física intrusiva	Se requiere desarmar el dispositivo para adquisición mediante el circuito (JTAG)[5]

Nota: Se muestra una breve descripción de las diferentes formas adquisiciones de evidencia que podemos llevar a cabo con un sistema infotainment.

(Bortles, McDonoug, & Smith, 2017) aclaran el proceso de una adquisición intrusiva, describiendo que se inicia con la extracción del tablero del vehículo, luego se traslada el equipo a un laboratorio previamente preparado para posteriormente desarmar la cubierta del módulo y extraer la placa de circuito en el cual mediante un proceso de pegado o con equipo especializado se añade una tarjeta de interfaz que permite realizar la adquisición respectiva.

En la imagen 3 se muestra parte del proceso de adquisición física intrusiva.

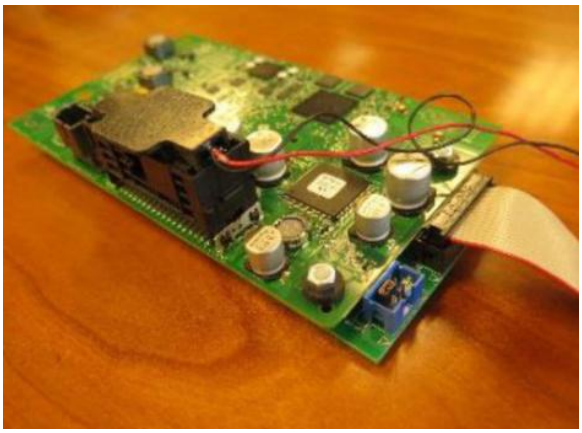

Imagen 3: Placa de circuito extraída de un sistema infotainment, para inicio de adquisición física intrusiva

También existen aspectos a considerar en esta fase (Lacroix, El-Khatib, & Akalu, 2013) nos

[5] JTAG: Proceso de adquisición de información de forma electrónica, mediante la utilización de medios no convencionales.

dicen que el análisis no está focalizado a un solo tipo de sistema operativo, al contrario, por la gran variedad que existen en el mercado, el investigador podrá toparse con sistemas operativos propios del fabricante de vehículos o sistemas infotainment generalizados como Android Automotive o de algún fabricante de este tipo de dispositivos como Pioneer, por esta razón recomiendan que se deberá tener más de una herramienta predispuesta a ser utilizada dentro de este proceso.

Es importante mencionar también que el análisis puede ser realizado en caliente es decir con el dispositivo encendido, navegando sobre la información, o en frio donde se trabaja con las imágenes forenses o con la información extraída (Moos, Gareth , & Nathan , 2016). De la misma forma el autor advierte que estas tareas deben ser documentadas y ejecutadas sin que ninguna acción efectuada altere el margen de la ley en la jurisdicción donde se llevara a cabo el proceso.

Evidencias digitales en sistemas Infotainment

(Cano, 2015) se refiere a la evidencia digital como cualquier dato que ha sido generado o almacenado en medio digitales, diferenciando que un dato generado es cualquier registro creado como resultado de la interacción del usuario y un equipo informático y que no necesariamente conoce de su existencia, añade como ejemplos a los logs y los cookies; en cambio dice que un dato almacenado es la información que el usuario conscientemente aloja en los dispositivos de almacenamiento como es la música, documentos ofimáticos o fotografías.

(Hook & Fraklaris, 2016) manifiesta también que la información que es considerada como evidencia puede estar situada en diversas ubicaciones dentro de un sistema de archivos o dentro de varios medios de almacenamiento del mismo dispositivo, es por esto que (Hannon, 2015) denomina a cada uno de estos sitios como fuentes de evidencia digital.

Dentro de los sistemas infotainment de vehículos (Henry, 2017) detalla los principales datos que podemos encontrar y que pueden ser considerados como una fuente de evidencia digital, agrupándolos en 6 categorías que son: información del sistema, información sincronizada, aplicaciones instaladas, dispositivos conectados, datos de navegación y eventos. Indicando que cada una de estas categorías puede tener uno o varios elementos que independientemente pueden considerarse como una fuente de información.

En la tabla 3 se muestran los diferentes tipos de evidencia digital que pueden ser recogidos de un sistema infotainment de vehículos.

Tabla 3

Fuentes de evidencia sistemas infotainment

Categoría	Elementos
Información del Sistema	• Número de serie • Número de parte • Número de compilación
Información Sincronizada	• ID de dispositivo • Llamadas • Contactos • SMS • Audio • Vídeo • Imágenes • Información del punto de acceso
Aplicaciones Instaladas	• Weather • Traffic • Facebook • Twitter
Dispositivos Conectados	• Teléfonos • Reproductores multimedia • Unidades USB • Tarjetas SD • Puntos de acceso inalámbricos
Datos de navegación	• Tracklogs y Trackpoints • Ubicaciones guardadas • Destinos anteriores • Rutas Activas e Inactivas
Eventos	• Apertura / cierre de puertas • Luces encendidas / apagadas • Conexiones Bluetooth • Conexiones Wifi • Conexiones USB • Reinicios del sistema • Sincronización de tiempo GPS • Lecturas del Kilometraje

Nota: Información que podemos recolectar y analizar de un sistema infotainment de vehículos.

Marcos de referencia para el análisis forense informático

Dentro de las ciencias forenses digitales existen varios marcos de referencia propuestos, enfocados en diversos aspectos de la investigación, los que enfatizan una etapa en particular o los que se centran en un entorno de análisis específico, lo que demuestra la complejidad del proceso forense digital. (Kohn, Eloff, & Olivier, 2006)

Durante los primeros años de desarrollo del cómputo forense, hubo la necesidad de definir marcos referenciales que permitan llevar un proceso consistente y organizado (Xiaoyu, Nhien-An, & Mark, 2015). Es así que (Lee, 2001) propuso un marco para la investigación forense digital basado en la escena delito el cual se compone de 4 pasos principales que son; reconocer, identificar, individualizar y reconstruir. Este marco es observado por (Ciardhuáin, 2004) quien piensa que sus procesos se inclinan más al trabajo con evidencias físicas. En la imagen 4 podemos ver los 4 procesos de este marco.

Imagen 4: Procesos y subprocesos del marco de Referencia de Henry Lee.

Otro marco de referencia importante es el que definió (Casey, 2004) el cual se enfoca en el procesamiento y análisis de pruebas digitales, este marco está compuesto de 7 pasos que son: Reconocimiento del incidente, Evaluación, e incautación, Preservación, Examinación y Análisis, Clasificación, Análisis y Reporte. En la imagen 5 podemos apreciar los 7 procesos de este marco.

Imagen 5: Procesos y subprocesos del marco de Referencia de Carrier & Spafford

Luego de tener un procedimiento general definido, los analistas forenses empezaron a generar marcos de referencia más específicos que establecen mejoras a un proceso de la investigación o para analizar un dispositivo específico dentro de un caso. (Kohn, Eloff, & Eloff, 2013).

(Martini & Choo, 2012) es un claro ejemplo**,** integrado para el análisis forense en la nube, el mismo está compuesto de 4 pasos esenciales que son: Origen de la evidencia identificación y preservación, recolección, examen y análisis y reporte y presentación. En las En la imagen 6 podemos apreciar los 4 procesos de este marco.

Imagen 6: Procesos y subprocesos del marco de Referencia de Martini & Choo.

De la misma manera en base a las necesidades encontradas durante el proceso de análisis forense a dispositivos LOT o Internet de las cosas (Perumal, Norwawi, & Raman, 2015) presentan un marco referencial para llevar adelante un análisis forense sobre esta tecnología, el mismo que está compuesto de 5 pasos que son: la planificación, identificación de dispositivos base, examinación y triage, análisis en laboratorio, archivo y almacenamiento. En la imagen 7 podemos apreciar los 5 procesos de este marco propuesto.

Imagen 7: Procesos y subprocesos del marco de Referencia de Perumal, Norwawi, & Raman.

Metodología

Para la construcción de este marco de referencia se escogió una metodología con enfoque cualitativo, que tiene como función principal el definir criterios y generar teorías que nos permitirá definir el marco de referencia propuesto.

Lo primero fue realizar una revisión literaria de aspectos relacionados a los sistemas infotainment y sus prácticas forenses, así como el análisis de las características de diferentes marcos de referencia tanto generales como específicos propuestos para la práctica de una investigación digital forense sobre estos sistemas.

Con el cumplimiento de la primera fase se analizará cada uno de los pasos de los marcos de referencia revisados, para clasificar cuál de estos pueden ser utilizados dentro de un análisis forense a sistemas infotainment de vehículos tomando como base las características técnicas y procedimientos requeridos para la preservación y análisis de estos dispositivos. Aquí se establecerá la necesidad de incluir una fase especifica que cubra algún paso necesario que deba ser manejado independientemente y que los otros marcos de referencia no lo cubren.

Para finalizar se propondrá un marco de referencia específico para el análisis forense a sistemas infotainment de vehículos el cual será validado con la proyección de un grupo focal de 5 expertos en el área, los cuales darán sus apreciaciones sobre la factibilidad de su uso en una investigación forense digital.

Es importante mencionar que el alcance establecido para esta investigación es exploratoria.

Hipótesis

La hipótesis tiene como base la recopilación de ideas y conceptos mediante el análisis bibliográfico relativo al análisis forense informático sobre sistemas infotainment de vehículos. Las particularidades técnicas y legales en los procesos de adquisición y análisis de evidencia en estos sistemas, así como el particular ambiente donde está instalado el dispositivo, nos hacer abordar la siguiente pregunta: ¿Que procedimientos son necesarios para realizar un análisis forense a sistemas infotainment de vehículos?

Marco de referencia propuesto

En esta sección, se propondrá un marco de referencia específico para el análisis forense a sistemas infotainment de vehículos, a partir de la comparación y análisis de los procesos de los marcos revisados, así como de las características de estos dispositivos, se presenta un marco compuesto de 4 fases:

Planificación, Preservación, Adquisición y Análisis en laboratorio y Reporte.

Cada una de las etapas respalda el mantenimiento de la cadena de custodia y cumplen con el objetivo de un análisis forense, lo que permitirá llevar a cabo una investigación ordenada con procesos adecuados para la investigación de equipos infotainment de vehículos.

En la imagen 8, se muestra el gráfico del marco de referencia propuesto para el análisis forense a sistemas infotainment.

Imagen 8: Procesos del marco de Referencia propuesto para análisis forense a sistemas infotainment de vehículos.

Con el desarrollo de la primera fase de Planificación, los subprocesos son orientados a responder preguntas como: ¿qué voy hacer?, ¿cómo lo voy hacer? ¿Qué consideraciones legales debo tomar?

Luego, en la segunda fase de Preservación, se toma en consideración 2 subprocesos mencionados en el marco de (Casey, 2004) , el de recolectar y documentar. De esta forma, la segunda fase permite recoger los elementos que serán objeto de un análisis y documentarlos de tal forma de iniciar un proceso de cadena de custodia.

La tercera fase propuesta se compone de 2 pasos: Adquisición donde se generan las imágenes forenses; y Análisis donde se buscan las evidencias necesarias para el caso. Basados en el proceso del marco analizado de (Perumal, Norwawi, & Raman, 2015) esta fase debe ser llevarse a cabo dentro de un laboratorio forense, lo cual permitirá tener un ambiente controlado ante cualquier acceso intrusivo a la información que por las particularidades de los medios de almacenamiento del dispositivo son necesarios.

De esta forma se podrá documentar y fundamentar que los procedimientos que se llevaron a cabo fueron técnicamente robustos, que la integridad de la información fue precautelada dentro del laboratorio, de la misma forma se podrá comprobar que la cadena de custodia no fue corrompida.

Finalmente, tenemos la cuarta fase encomendada a la generación y presentación del informe final de la investigación, en conjunto con las evidencias recolectadas que darán soporte al reporte.

Análisis de Resultados

El objetivo de realizar un grupo focal es validar el marco de referencia propuesto para el análisis forense a sistema Infotainment de vehículos, y conocer los criterios sobre la factibilidad de su uso dentro de una investigación digital. De la misma manera se evaluará si el marco propuesto cumple con los principios del análisis forense y permite la conservación de la cadena de custodia dentro del proceso.

El grupo focal se compuso de 5 profesionales con más de 12 años de experiencia en el análisis forense informático en países como Argentina, Colombia, República Dominicana, Guatemala y Bolivia, siendo referentes en el área en cada uno de sus países . Esta sesión se inició con el 100% de los participantes a los cuales se les planteó llevar a cabo un

conversatorio en donde los temas tratados se llevaron como preguntas, y respuestas logrando avanzar con la secuencia de una conversación estructurada.

El grupo focal fue llevado en 2 etapas, dentro de la primera se planteó la discusión sobre temas relacionados a su experiencia en el área, para conocer si dentro de las tareas de análisis forense encomendadas han tenido a cargo dispositivos que no necesariamente hayan sido equipos de computación o teléfonos celulares y si dentro de este segmento se han encontrado con equipos infotainment de vehículos.

El 70% de los profesionales referenciaron que la gran mayoría de las peticiones para un análisis forense se relacionan con computadoras y teléfonos celulares, y que fuera de ese segmento pueden nombrar a consolas de vídeos juegos, cámaras de vigilancia, y dispositivos de almacenamiento autónomos con los cuales han trabajado. El otro 30% está de acuerdo con las apreciaciones anteriores, pero mencionan que ellos si han tenido experiencia con sistemas infotainment de vehículos, destacando que para estos casos han aplicado una metodología tradicional.

De igual forma dentro de la primera parte de la discusión se consultó si conocen a los dispositivos infotainment de vehículos y que en base a sus características técnicas, conocen la manera de llevar a cabo un análisis forense sobre estos equipos. En la tabla 4 se presentan los resultados en referencia a las consultas planteadas.

Tabla 4

Conocimiento de los equipos infotainment, características técnicas y su análisis forense

Sistemas Infotainment	***Si conocen***	***No conocen***
Características técnicas	*100%*	*0%*
Consideraciones Para Análisis forense	*90%*	*10%*

Nota: Porcentaje de conocimiento en los temas planteados como preguntas a los participantes.

Así mismo los participantes se pronunciaron sobre las características técnicas del equipo así como dentro del análisis forense. En la tabla 5, se muestra algunas características mencionadas dentro del el grupo focal.

Tabla 5

Características mencionadas de los dispositivos infotainment

Participante	***Opinión***
1	*Maneja unidades de almacenamiento sólidas*
2	*El desmontaje del equipo podría resultar complejo*
3	*Manejan muchos sistemas operativos*
4	*En varias ocasiones será necesario afectar la integridad del hardware para acceder a la información*
5	*No hay mucha información que apoye las prácticas forenses sobre estos dispositivos*

Nota: opiniones del grupo focal sobre características de los dispositivos infotainment de vehículos.

Dentro de la segunda fase de la discusión se desarrollaron varios temas sobre el marco de referencia específico propuesto. En primer lugar, se evaluó si el mismo fue elaborado acorde a las necesidades técnicas que nos exige este tipo de dispositivos. El 90% concuerda que dentro de un análisis forense a estos equipos hay que tener una gran atención, en la extracción del dispositivo, en el acceso a los medios de almacenamiento y en la adquisición de la información. Mencionando que estos aspectos son cubiertos en las fases 2 y 3 del marco propuesto. Mientras que el 10% piensan que el marco debería tener un paso específico o adicional que cubra de forma independiente una adquisición intrusiva, que la consideran como la principal característica técnica al momento de un análisis forense.

Dentro de esta fase de discusión también se analizó si el marco de referencia propuesto permite cumplir con el objetivo de cadena de custodia. El 100% de los profesionales concuerdan que al ser un marco basado en otros marcos de referencia y con base en la estructura planteada para el desarrollo del análisis forense a los dispositivos infotainment de vehículos, el marco permite validar cada una de los procedimientos y técnicas llevadas a cabo por consiguiente permite iniciar y mantener la cadena de custodia durante todo el proceso.

Para finalizar la segunda fase de discusión se evalúo si cada una de las fases del marco propuesto están sustentadas en los objetivos del análisis forense, sobre todo el tercer paso en el cual es imprescindible llevarlo a cabo en un laboratorio forense.

Sobre este aspecto el 100% de participantes concuerdan que el marco propuesto si cumple con el objetico del análisis forense informático, manifestando que dadas las características y la complejidad que puede darse para lograr una adquisición forense y el análisis de datos, es necesario que el investigador realice directamente estos procesos dentro de un laboratorio forense donde pueda controlar técnicamente todo lo que realice, además agregan que este paso se encuentra bien acoplado con el resto fases planteadas.

Como parte del cierre del grupo focal se consultó si el marco de referencia propuesto para el desarrollo de un análisis forense a sistemas infotainment de vehículos, es aplicable en este tipo de investigaciones. Teniendo como resultado que el 100% de los profesionales validan como apropiado el marco propuesto. Mencionan lo importante de conjugar varios marcos existentes y generar uno que solvente las necesidades específicas de los equipos infotainment de vehículos. Además, se levantaron otras precisiones al respecto que la podremos observar en la tabla 6.

Tabla 6

Opiniones sobre la aplicabilidad del marco de referencia propuesto

Participante	***Opinión***
1	En muy viable su uso, se acopla a los requerimientos de este tipo de dispositivos, será importante conocer en lo posterior su aplicabilidad bajo procesos jurídicos en cada uno de nuestros países.
2	Considero que la etapa que se desarrolla en un laboratorio es muy necesaria y dará mucha transparencia al proceso. Es una las principales características por la cual considero viable su uso.
3	Como manifesté durante el conversatorio, hubiera considerado dividir en 2 procesos diferentes la fase 3, pero aun así el marco se encuentra sustentado de tal forma que su uso dentro de una tarea forense es recomendado.
4	De acuerdo a mi experiencia es muy viable el uso de este marco dentro de una investigación sobre estos equipos, porque se ha personalizado en cierta forma cada fase propuesta. Pero si recomendaría que se consideraría planificar revisiones y el mismo en base a las experticias que brinde el uso del mismo.
5	En mi opinión considero viable la aplicabilidad y uso del marco, me acojo a lo comentado por los profesionales, resaltando que además es el primer marco enfocado específicamente a este tipo de dispositivos

Nota: opiniones del grupo focal sobre la aplicabilidad del marco de referencia propuesto.

CONCLUSIONES

Los marcos de referencia tradicionales pueden ser una opción para llevar a cabo un análisis forense informático sobre dispositivos comunes, pero al existir equipos informáticos que requieren consideraciones especiales para su manejo o necesitan un tratamiento especial como los equipos infotainment de vehículos, se hace necesario aplicar un marco especifico que nos permita cumplir de mejor forma con el objetivo del análisis forense.

El marco de referencia especifico propuesto fue diseñado sobre la base de otros marcos

utilizados en el análisis forense, así como en las características técnicas y en los requerimientos especiales que se presentan cuando se investiga de manera forense un equipo infotainment de vehículos.

Este marco propuesto tiene 4 fases definidas: planificación, preservación, adquisición y análisis en laboratorio y reporte. Dentro del mismo, se plantea un tratamiento específico y técnico sobre el dispositivo principalmente en la fase 2 de preservación, donde se limita al investigador a desmontar el dispositivo y documentar lo necesario para dar soporte al proceso de cadena de custodia, y en la fase 3 donde se establece que los procesos de adquisición y análisis deben llevarse a cabo dentro de un laboratorio forense. El propósito de esta fase es evitar que al no tener un ambiente controlado como un laboratorio y dada la complejidad del proceso, la evidencia pueda verse afectada en su integridad.

Los resultados del estudio muestran la aceptación del marco de referencia propuesto como alternativa a los marcos tradicionales, para llevar a cabo un análisis forense a sistemas infotainment de vehículos. Además, se plantea que este marco puede ser considerado para otro tipo de dispositivos que requieran un tratamiento específico.

La validación del marco de referencia propuesto fue a través de un grupo focal conformado por profesionales de varios países mediante los cuales se pudo obtener información a través de datos cualitativos, instrumento que nos sirvió para analizar y validar el marco propuesto.

Uno de los limitantes encontrados durante la investigación son las escasas fuentes de información sobre trabajos previos relacionados al análisis forense a sistemas infotainment de vehículos, tanto desde un punto de vista técnico como del punto de vista legal, limitante que también fue resaltada dentro del grupo focal.

Para futuros trabajos se plantea aplicar el marco de referencia propuesto como un proceso experimental dentro del campo pericial y de esta forma poder evaluar la validez del modelo dentro del área judicial ecuatoriana.

Referencias Bibliográficas

Kohn, M., Eloff, J., & Olivier, M. (2006). Framework for a Digital Forensic Investigation. *Information and Computer Security Architectures Research Group*.

Aadarsh, K., Sneha , K., & Pooja, P. (2013). IN-VEHICLE INFOTAINMENT SYSTEMS. *International Journal of Advanced Computational Engineering and Networking*, 27-32.

Berrocal, S. (2014). La presencia del infoentretenimiento en los canales generalistas de la TDT española. . *Revista Latina de Comunicación Social*, 69, 85-103.

Bortles, W., McDonoug, S., & Smith, C. (2017). An Introduction to the Forensic Acquisition of Passenger Vehicle Infotainment. *SAE International*.

Bortles, W., McDonough, S., & Smith, C. (2017). An Introduction to the Forensic Acquisition of Passenger Vehicle Infotainment and Telematics Systems Data. *SAE Technical*, 1-28.

Bulbul, H. I. (2013). Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM. *Forensic Science International,*, 233(1-3), 244-256.

Cano, J. (2015). *Computación forense - Descubriendo los rastros informáticos.* bogota: Alfa&Omega.

Carrasco, M. C. (2014). Análisis de un producto de infoentretenimiento.

Carrier, B. (2002). Defining Digital Forensic Examination and Analisis Tools.

Carrier, B. (2006). Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation*, 121-130.

Casey, E. (2004). Digital Evidence and Computer Crime. En E. Casey, *Digital Evidence and Computer Crime* (pág. 169). Baltimore: ELSEVIER.

Casey, E. (2011). *Digital Evidence and Computer Crime.* Baltimore: Academic Press.

Ciardhuáin, S. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence* , 1-22.

Edwards, T. (2014). The Admissibility of Electronically Stored Information under the Federal Rules of Evidence. . *Computer & Internet Lawyer*, 6-11.

Everett, C. a. (2013). Open Car Testbed and Network Experiments): Bringing CyberPhysical Security . *CSET*.

Hannon, M. (2015). Evidence Authentication in a Digital World. *Computer & Internet Lawyer.*, 12-31.

Henry, P. (1 de Marzo de 2017). *https://digital-forensics.sans.org/*. Obtenido de https://digital-forensics.sans.org/blog/2017/05/01/digital-forensics-automotive-infotainment-and-telematics-systems-2

Hook, S., & Fraklaris, C. (2016). Oh, Snap! The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik, and Other Mobile Messaging Apps. *Computer & Internet Lawyer*, 1-17.

Kohn, M., Eloff, M., & Eloff, J. (2013). Integrated Digital Forensic Process Model. *Computers & Security*, 103–115.

Lacroix, J. (2017). Vehicular Infotainment Forensics. *University of Ontario Institute of Technology*.

Lacroix, J., El-Khatib, K., & Akalu, R. (2013). Vehicular Digital Forensics: What Does My Vehicle Know About Me? *Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications* , 59-66.

Lee, H. (2001). Henry Lee's Crime Scene Handbook, . *Academic Press*.

LeMere, B., & Bollo, J. (2017). Vehicle Solve Crime. *Digital Forensic Magazine*, 34-37.

Martini, B., & Choo, K.-K. (2012). An Integrated Conceptual Digital Forensic Framework for Cloud Computing. *Digital Investigation*, 71-80.

Moos, J., Gareth , D., & Nathan , W. (2016). Digital Forensics for Automobile Systems: The Challenges and a Call to Arms. *International Journal of Forensic Sciences*, 1-13.

Mouhtaropoulos, A. C. (2015). Digital Forensic Readiness: Are We There Yet? . *Journal of International Commercial Law & Technology,*, 173-179.

Park, Y., Lee, S., & Kim, J. (2014). Applyin Digital Forensics in Various. *Digital Forensics*.

Perumal, S., Norwawi, N., & Raman, V. (2015). Internet of Things (IoT) Digital Forensic Investigation Model. *Fifth International Conference on Digital Information* , 19-23.

Pino, S. A. (03 de 05 de 2016). *Delitos Informáticos: Generalidades.* Obtenido de OEA Derechos para la gente: http://www.oas.org

Scoltock, J. (2016). Focus: Infotainment and connectivity. *Automotive Engineer*, 41(3), 37-38.

Simon , N., Bharath , G., & Matthias , v. A. (10 de 08 de 2015). *Deloitte Insights.* Obtenido de The Internet of Things in automotive: https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-automotive-industry.html#endnote-sup-12

SWGDE. (2016). Best Practices for Vehicle Infotainment and Telematics Systems. *Scientific Working Group on Digital Evidence*, 1-9.

Xiaoyu, D., Nhien-An, L.-K., & Mark, S. (2015). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. *Computer Science and Network Security*, 34-38.