Universidad Cenfotec

Maestría en Ciberseguridad

Tema:

El rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales

Elaborado por:

Elías Yoel Apú Murillo

Fecha: Julio, 2022

Universidad CENFOTEC
SOMOS LO QUE SABEMOS

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Apú Murillo Elías Yoel.**

DENNIS ALONSO DURAN CESPEDES (FIRMA)

Digitally signed by DENNIS ALONSO DURAN CESPEDES (FIRMA)
DN: SERIALNUMBER=CPF-01-1029-0075, SN=DURAN CESPEDES, G=DENNIS ALONSO, C=CR, O=PERSONA FISICA, OU=CIUDADANO, CN=DENNIS ALONSO DURAN CESPEDES (FIRMA)
Reason: I am the author of this document
Location:
Date: 2022.07.08 19:18:05-06'00'
Foxit PDF Reader Version: 12.0.0

M. Sc. Dennis Durán Céspedes
Tutor

MSEG. Aissen Contreras Castro
Lector 1

MSEG. César Solarte Castañeda
Lector 2

San José, Costa Rica, 07 de julio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de Contenido

Abstract

Esta investigación tiene como objetivo principal analizar el rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales, durante el periodo enero de 2018 a febrero de 2021, para el cual se utilizó la investigación evaluativa, por medio de la cual no se busca producir conocimiento nuevo, ni atender necesidades particulares de algún cliente, sino lo que se busca es emitir un criterio basado en los hallazgos. Se concluye que no se encontró evidencia de que el rol de la ciencia forense digital de dispositivos IoT haya sido determinante hasta ahora en las investigaciones criminales.

Palabras claves: investigaciones criminales, dispositivos IoT, ciencia forense digital.

Capítulo 1. Introducción

1.1 Generalidades

El presente proyecto tiene como objetivo principal analizar el rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales, durante el periodo enero de 2018 a febrero de 2021. IoT procede de las siglas en inglés de “Internet Of Things”, que se refiere a los diferentes dispositivos que se interconectan entre si por medio de una red, la cual puede ser privada o pública. El acelerado avance del internet ha permitido que estos dispositivos sean una realidad y que cada vez se involucren más en la cotidianidad de las personas.

Por otra parte, el uso de estas nuevas tecnologías genera grandes repositorios de información, que pueden ser blanco de ataques cibernéticos o que más bien puedan ser usados como evidencia en investigaciones criminales y facilitar la resolución de algún caso. De ahí la relevancia de considerar los dispositivos IoT en dichas indagaciones.

1.2 Antecedentes del problema

Debido al acelerado avance en el uso de dispositivos IoT y el involucramiento de estos en delitos digitales, la ciencia forense ha innovado y ha creado procesos, herramientas y metodologías para resolver estas necesidades. Estas nuevas tendencias en la ciencia forense digital se han creado en un corto tiempo, por lo que no se han realizado muchos análisis del estado actual, que permitan y señalen cuáles corrientes tienen el impacto esperado en las investigaciones y cuáles deben ser mejoradas.

Consecuentemente, existen bastantes estudios sobre metodologías, herramientas y procesos que utiliza la ciencia forense, pero no existen muchos análisis sobre el rol que ellos desempeñan en las investigaciones criminales.

1.3 Definición y descripción del problema

¿Cuál ha sido el rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales, durante el periodo enero de 2018 a febrero de 2021?

1.4 Justificación

En la actualidad, el uso de dispositivos IoT es cada vez más común y el rango de usos y tipo de industrias que lo utilizan es muy amplio. Esto agregado al aumento de crímenes digitales trae como consecuencia el uso de nuevas tecnologías, herramientas y metodologías que se adapten a los nuevos modelos de delincuencia. La ciencia forense ha innovado y se ha reinventado, con el fin de solventar estas necesidades. Por lo tanto, es importante realizar un análisis del rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales, con el fin de exponer su estado actual.

De la misma manera, un análisis del estado actual permite señalar áreas de mejora en las cuales es posible optimizar los procesos actuales y acrecentar el impacto que tiene esta ciencia en la resolución de delitos. De igual modo, el presente estudio permitirá indicar las partes del proceso que se están desarrollando de manera correcta y que servirán como base para futuras indagaciones a partir de cuyos resultados la ciencia forense pueda beneficiar la resolución de estos.

1.5 Viabilidad

1.5.1 Punto de vista técnico

Como base técnica, el autor del presente informe cuenta con un bachillerato en ingeniería en computación del Instituto Tecnológico de Costa Rica, además de 5 años de experiencia en el área de aseguramiento de calidad en el proceso de desarrollo de *software*, 1 año de experiencia como ingeniero en seguridad informática, sumado al conocimiento adquirido durante la maestría.

1.5.2 Punto de vista operativo

El diseño de esta investigación no involucra directamente a ninguna organización, por lo que no se afecta la parte operativa de ninguna empresa.

1.5.3 Punto de vista económico

El costo del desarrollo de este proyecto radica en las horas del investigador, incluidos los costos por servicios y herramientas tecnológicas, cuales fueron asumidos por este. Por lo tanto, no involucra gastos económicos extra.

1.6 Objetivos

Para la elaboración de estos objetivos se utilizó la taxonomía de Bloom.

1.6.1 Objetivo general

Analizar el rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales, durante el periodo enero de 2018 a febrero de 2021

1.6.2 Objetivos específicos

- Describir las principales etapas involucradas en el proceso del análisis forense de dispositivos IoT en investigaciones criminales.
- Explicar las herramientas utilizadas en las diferentes etapas del proceso del análisis forense de dispositivos IoT.

- Organizar los diferentes tipos de evidencias digitales que se obtienen según las herramientas utilizadas en las diferentes etapas del proceso del análisis forense digital.
- Reconocer la relevancia de las evidencias digitales que se obtienen del proceso del análisis forense digital en las investigaciones criminales.

1.7 Alcances y limitaciones

1.7.1 Alcances

Como resultado de este proyecto de investigación se generó este documento con un análisis del estado actual del rol de la ciencia forense digital de dispositivos IoT en investigaciones criminales.

1.7.2 Limitaciones

El hecho de que el informe final del presente estudio esté escrito en el idioma español, constituye la principal limitación, por cuanto solo puede difundirse entre los profesionales de habla hispana.

1.8 Estado de la cuestión

1.8.1 Planificación de la revisión

1.8.1.1 Pregunta de investigación

¿Qué trabajos e investigaciones se han hecho sobre el rol de la ciencia forense de dispositivos IoT en investigaciones criminales?

1.8.1.2 Palabras claves y sinónimos

IoT, “internet of things”, informática forense, “digital forensics”, “criminal investigations”.

1.8.1.3 Intervención

En el contexto de la revisión sistemática, se analizaron los estudios realizados sobre el rol de la ciencia forense digital en las investigaciones criminales.

1.8.1.4 Resultado

Los resultados esperados de esta revisión es el conocimiento sistemático de los análisis del rol que ha jugado la ciencia forense de dispositivos IoT en las investigaciones, además de identificar si es necesario profundizar en alguna metodología, proceso o herramienta utilizados en las indagaciones.

1.8.1.5 Aplicación

Los beneficiarios de la revisión sistemática serán todos los profesionales involucrados con el proceso de análisis forense de dispositivos IoT, además de todos los que deseen conocer el rol que esta ciencia está desempeñando en las investigaciones criminales.

1.8.1.6 Diseño experimental

El *metaanálisis* de la revisión está enfocado a analizar la información disponible sobre el rol de la ciencia forense de dispositivos IoT en las investigaciones criminales, así como los análisis que se hayan hecho sobre este rol.

1.8.2 Selección de fuentes

En este apartado se analizan las fuentes principalmente las que se usaron para realizar la revisión. Posteriormente, se utilizaron los elementos definidos en la

planificación para aplicar el procedimiento de obtención de estudios primarios en cada una de las fuentes seleccionadas.

1.8.2.1 Definición del criterio de selección de fuentes

El criterio para la selección de las fuentes de búsqueda está basado en una investigación previa del autor sobre ventajas y facilidades de ciertas fuentes sobre otras, con base en requisitos, como el acceso vía web, motores de búsqueda que permiten consultas avanzadas, la amplitud de repositorios consultados y, finalmente, una cuestión de limitaciones financieras pues muchos repositorios son pagados.

1.8.2.2 Fuente seleccionada

La fuente seleccionada para la revisión es Scholar Google, la cual maneja un motor de búsqueda completo, avanzado. Permite, además, el acceso a todo tipo de documentos, tales como artículos, tesis, trabajos finales, libros y de diferentes repositorios. Al incluir material de repositorios institucionales, se tiene acceso a las versiones web de texto completo de algunos artículos que las bases de datos no tienden a no enlazar. Además, se trata de una herramienta generalmente gratuita que si bien lo que hace es indexar resultados de diversas fuentes y muchas de estas pueden llevar a sitios pagados.

1.8.2.3 Cadenas de búsqueda

Con base en el operador “intitle” además de operadores AND sobre las palabras claves y conceptos relacionados identificados anteriormente, se establece la cadena de búsqueda utilizada en la presente revisión:

- “Intitle”:"Digital forensics" AND "criminal investigations" AND "internet of things”
- “Intitle”:"Digital forensics" AND "criminal investigations" AND "IoT"

1.8.3 Selección de los estudios

Una vez seleccionada la fuente, es necesario describir el proceso desarrollado y el criterio rector durante el proceso de revisión, así como para seleccionar y evaluar los estudios primarios. Para ello se define el proceso completo de selección, así como los criterios de inclusión y exclusión utilizados. En esta revisión se sigue un proceso iterativo e incremental. Se aplicó un proceso iterativo formado por las etapas de búsqueda, extracción y visualización de la información de la fuente seleccionada.

En primer lugar, se adapta la cadena a la fuente seleccionada y efectúa la consulta. Sobre el conjunto de resultados obtenidos se aplica el criterio de inclusión a modo de filtro, para obtener un conjunto de estudios relevantes. De seguido, se aplica el criterio de exclusión sobre este conjunto de estudios relevantes para identificar el conjunto de estudios primarios, los cuales se almacenan y se analizan con más profundidad para extraer su información bibliográfica y la información relevante de cada uno de ellos según un formulario previamente definido.

1.8.3.1 Definición del criterio de inclusión y exclusión de estudios

El criterio de inclusión actúa sobre los resultados obtenidos al ejecutar la búsqueda sobre la fuente, lo que permitió realizar una primera selección de documentos que fueron considerados en el contexto de la revisión como candidatos a convertirse en estudios primarios.

Como **criterio de inclusión** se utilizó principalmente un análisis sobre el título, las palabras claves y el resumen de cada documento. De esta forma fue posible, cómo están relacionadas estas palabras y por qué ha sido seleccionado dicho documento. Con este criterio se elimina la mayor parte de los resultados obtenidos ajenos a la pregunta de investigación planteada.

El **criterio de exclusión** actúa sobre el subconjunto de documentos obtenidos en la etapa anterior y permite obtener el conjunto de estudios primarios. Como criterio de exclusión el estudio se enfoca principalmente en la lectura y en el análisis del resumen del documento y sus conclusiones. En algunos casos fue necesario profundizar en el este. Con este criterio es posible ver en más detalle de qué trata cada documento, ver la relación real que presenta con los objetivos del presente estudio y si es verdaderamente relevante para la revisión, para seleccionarlo como estudio primario.

1.8.3.2 Definición de tipos de estudio

Los tipos de estudios primarios seleccionados durante la revisión sistemática son los artículos presentes en las fuentes seleccionadas, que cumplan con los criterios establecidos.

1.8.4 Ejecución de la revisión

En esta sección aplica la revisión por medio de Scholar Google para obtener nuevos estudios primarios.

1.8.4.1 Selección de estudios iniciales

Al utilizar la consulta inicial en el motor de búsqueda se obtuvieron resultados escuetos. Por lo tanto, se procedió a la búsqueda a partir de palabras claves. Al

introducir los términos: “intitle”: "Digital forensics" AND "criminal investigations" AND "IoT" se obtuvieron 30 resultados. Se procedió a hacer un filtrado por intervalo de fechas 2018-2021, con lo cual se obtuvieron 27 resultados, los cuales fueron analizados aplicando criterios de exclusión y se obtuvieron 9 estudios primarios.

01	Hou J, Li Y, Yu J, Shi W. A survey on digital forensics in internet of things. IEEE Internet Things J. 2020;7(1):1–15.
02	Al Qatawneh MQWAMKI. DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS. Journal of Theoretical and Applied Information Technology. 2019 Dec.19.
03	Collie J, Overill RE. DEEP: Extending the digital forensics process model for criminal investigations. Athens J Sci. 2020:7(4):225–40.
04	Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Commun Surv Tutor. 2020;22(2):1191–221.
05	Hernandez-Castro J, Avoine G, editors. Security of ubiquitous computing systems: Selected topics. 1st ed. Cham, Switzerland: Springer International Publishing; 2019.
06	Áine MacDermott, Thar Baker, Paul Buck, Farkhund Iqbal and Qi Shi. The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics. International Journal of Digital Crime and Forensics. 2020 Mar;13(1):13.
07	Arshad, Humaira & Jantan, Aman & Abiodun, Oludare. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems [Internet]. 2018 Apr; Available from: http://dx.doi.org/10.3745/JIPS.03.0095
08	MacDermott A, Baker T, Shi Q. Iot forensics: Challenges for the ioa era. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE; 2018.
09	Montasari R, Hill R. Next-generation digital forensics: Challenges and future paradigms. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). IEEE; 2019.

1.8.4.2 Evaluación de la calidad de los estudios

Todos los documentos identificados en la fuente Google Scholar tienen presunción de calidad porque para estar indexados en este buscador han debido pasar por una serie de filtros y evaluaciones.

1.8.4.3 Extracción de la información

En este apartado se analiza la información relevante de cada uno de los estudios primarios obtenidos en los pasos anteriores.

1.8.4.3.1 Formulario para la extracción de la información

El formulario consta de una primera parte de identificación del estudio en la que se muestra el título, datos de la publicación y de los autores del documento. La segunda parte se compone de la descripción general en la que se presenta un breve resumen y el área de interés, que aporta datos relevantes. Finalmente, se presentan los aspectos por destacar de cada documento, importantes para el desarrollo de la investigación.

1.8.4.3.2 Extracción de resultados objetivos y subjetivos

El formulario consta de una primera parte de identificación del estudio en la que se muestra el título, datos de la publicación y de los autores del documento. La segunda parte se compone de la descripción general en la que se presenta un breve resumen y el área de interés, que aporta datos relevantes. Finalmente, se presenta la sección “Aspectos por destacar” de cada documento, importantes para el desarrollo de este proyecto investigativo.

Título: IoT Forensics: Challenges For The IoA Era
Publicación: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)
Autores: Áine MacDermott, Thar Baker, Qi Shi
Área: Ciencias de la computación e Ingeniería
Resumen: Este artículo presenta los diferentes desafíos que han emergido en la era de IoT para la ciencia forense. Explica cómo el alcance de la ciencia forense ha cambiado y la forma como se maneja la evidencia forense en esta era. Expone diferentes metodologías sobre ese manejo.

Aspectos por destacar
• Menciona metodologías sobre el manejo de evidencia en la ciencia forense de dispositivos IoT. • Aporta ideas sobre el cambio en el alcance de la ciencia forense digital.

Título: Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence
Publicación: April 2018, Journal of Information Processing Systems 14(2):346 ~ 376
Autores: Humaira Arshad*, Aman Bin Jantan*, and Oludare Isaac Abiodun
Área: Ciencias de la computación e Ingeniería
Resumen: Este artículo explica que, aunque la ciencia forense digital ha evolucionado en gran medida en los últimos años, las evidencias digitales aún no tienen el papel que deberían tener. Menciona que las evidencias digitales usualmente tienen poco peso en las investigaciones criminales. El objetivo final del artículo es explorar el campo de la validación de la evidencia forense en las investigaciones criminales.
Aspectos por destacar
• Explora el campo de la validación de las evidencias digitales. • Muestra el peso que tiene la evidencia digital en la actualidad.

Título: Next-Generation Digital Forensics: Challenges and Future Paradigms
Publicación: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)
Autores: Reza Montasari, Richard Hill.

Área: Ciencias de la computación e Ingeniería

Resumen: Este artículo expone el hecho de que los últimos avances en la tecnología, tales como los dispositivos IoT, traen consigo nuevos retos para la ciencia forense digital. Expone cuáles pueden ser los nuevos paradigmas y retos que se pueden enfrentar.

Aspectos por destacar

- Explora los nuevos retos que impone los avances en tecnología como los en los dispositivos IoT.

Título: The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics

Publicación: June 2019, International Journal of Digital Crime and Forensics 12(1):1-13

Autores: Áine MacDermott y Paul Buck

Área: Ciencias de la computación e Ingeniería

Resumen: Este artículo explora los contribuyentes claves para el cambio de paradigma en las investigaciones criminales: pasar de evidencia física como predominante a evidencia digital e ilustra cómo las investigaciones sobre delitos cibernéticos y la ciencia forense digital se han adaptado a esta nueva ola de delitos informáticos.

Aspectos por destacar

- Ilustra cómo las investigaciones sobre delitos cibernéticos y la ciencia forense digital se han adaptado a esta nueva ola de delitos informáticos

Título: A Survey on Digital Forensics in Internet of Things
Publicación: IEEE Internet of Things Journal (Volume: 7, Issue: 1, Jan. 2020)
Autores: Jianwei Hou, Yuewei Li, Jingyang Yu y Wenchang Shi
Área: Ciencias de la computación e Ingeniería
Resumen: Este artículo describe de manera general el estado de la ciencia forense de IoT y busca proporcionar pautas para futuras investigaciones y prácticas al respecto. Intenta proporcionar un panorama completo y estructurado de la ciencia forense de IoT, en un marco tridimensional. El marco abarca una dimensión temporal, una dimensión espacial y una dimensión técnica.
Aspectos por destacar
• Describe el estado Actual de la ciencia forense digital de dispositivos IoT.

Título: DFIM: A new digital forensics investigation model for internet of things
Publicación: Journal of Theoretical and Applied Information Technology 31st December 2019. Vol.97. No 24
Autores: Áine MacDermott, Thar Baker, Paul Buck, Farkhund Iqbal y Qi Shi
Área: Ciencias de la computación e Ingeniería
Resumen: Este artículo propone un nuevo modelo de investigación forense digital para internet de las cosas (DFIM), que tiene dos componentes principales: el proveedor de zona de datos que se encarga de agrupar todos los datos recopilados por los nodos sensores en un conjunto de grupos, donde cada grupo contiene datos o documentos relacionados entre sí, y la autoridad investigadora, que recibe las solicitudes de investigación de los reclamantes, verifica la validación de la solicitud y finalmente selecciona a los investigadores apropiados.
Aspectos por destacar
• Propone un nuevo modelo para investigación forense de dispositivos IoT

Título: A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues
Publicación: IEEE Communications Surveys & Tutorials (Volume: 22, Issue: 2, Secondquarter 2020)
Autores: Maria Stoyanova , Yannis Nikoloudakis , Spyridon Panagiotakis , Evangelos Pallis, y Evangelos K. Markakis
Área: Ciencias de la computación e Ingeniería
Resumen: Este artículo examina de cerca los problemas de vulnerabilidad dentro de los sistemas de IoT desde un punto de vista forense y examina los enfoques forenses digitales de última generación.
Aspectos por destacar
• Examina los enfoques forenses de la actualidad, específicamente en el área de IoT.

Título: DEEP: Extending the Digital Forensics Process Model for Criminal Investigations.
Publicación: Athens Journal of Sciences- Volume 7, Issue 4, December 2020 – Pages 225-240.
Autores: Jan Collie y Richard E Overill
Área: Ciencias de la computación e Ingeniería
Resumen: Este documento presenta una extensión al modelo de análisis forense digital, el Proceso Mejorado de Evidencia Digital (DEEP), con el objetivo de ajustar

el mecanismo y asegurar que toda la evidencia digital sea examinada por un analista forense digital calificado. La consecuencia de adoptar DEEP en las investigaciones penales reales será garantizar que todas las pruebas digitales se analicen y evalúen con los más altos estándares de competencia profesional y técnica, lo que dará como resultado una mayor confiabilidad de las pruebas digitales presentadas en los tribunales, que servirán a la causa de la justicia en términos de casos reducidos de condenas inseguras asociadas y / o exculpaciones injustificadas.
Aspectos por destacar
• Muestra una extensión al modelo básico de análisis forense digital.

Título: Security of Ubiquitous Computing Systems
Publicación: 2021 by the registered company Springer Nature Switzerland AG.
Autores: Gildas Avoine y Julio Hernández-Castro
Área: Ciencias de la computación e Ingeniería
Resumen: Este libro presenta un compilado de capítulos relacionados con la seguridad de dispositivos IoT. Además, presenta metodologías de análisis para este tipo de dispositivos,
Aspectos por destacar
• Expone conceptos y metodologías de seguridad de dispositivos IoT, que pueden ser útiles para el desarrollo de la investigación.

Capítulo 2. Marco Teórico o Conceptual

El término de ciencia forense digital inicialmente se utilizaba como sinónimo del concepto de informática forense, pero se ha ampliado para incluir la investigación de todos los dispositivos capaces de almacenar, procesar y transmitir

datos digitales (1). También se puede hablar de ciencia forense digital cuando se trabaja con cualquier tipo de evidencia digital (2). Asimismo, las fuentes de evidencia forense usualmente suelen ser computadoras, dispositivos móviles, servidores o puertas de enlace, en lo que es definido como la ciencia forense digital convencional (3).

Por otra parte, internet de las cosas (IoT) puede verse como un sistema de información compuesto por cosas, redes, datos y servicios. Tales elementos (cosas) pueden ser sensores inalámbricos, computadoras tradicionales, teléfonos inteligentes, cámaras, tabletas, vehículos, electrodomésticos, etc., que están conectados a través de una red (3). Al respecto, Stoyanova et al. (4) mencionan que el internet de las cosas (IoT) es un paradigma muy conocido, que define un entorno dinámico de dispositivos informáticos interrelacionados con diversos componentes para la conectividad y transferencia de datos.

En la actualidad existen diferentes formas de definir el área de estudio relacionado al análisis forense de un dispositivo IoT. En primera instancia, se llama a esto ciencia forense digital de dispositivos IoT, pero algunos autores, como Jianwei et al. (1), prefieren llamar a esto “IoT Forensics”, por ser esta una rama específica de la ciencia forense para los dispositivos IoT.

Desde otro punto de vista, esta área de estudio relacionada con dispositivos IoT es también es llamada “Ubiquitous Computing”, con lo cual se hace referencia a dispositivos integrados, generalmente pequeños, con serias limitaciones en términos de memoria y potencia de procesamiento, por lo general sin baterías, pero con elevadas capacidades de conexión y con frecuencia con varios sensores (2).

Finalmente, para el desarrollo de esta investigación se utiliza el concepto de ciencia forense digital de dispositivos IoT, que permite delimitar mejor esta área de estudio.

Capítulo 3. Marco Metodológico

3.1 Tipo de investigación

El tipo de investigación utilizado en el presente estudio es la investigación evaluativa, la cual en lugar de producir conocimiento nuevo o atender necesidades particulares de algún cliente, lo que se busca es emitir un criterio basado en los hallazgos.

3.2 Alcance investigativo

El alcance investigativo es exploratorio, por cuanto lo que se busca es examinar un tema poco estudiado y el objetivo es familiarizarse con el proceso de análisis forense de dispositivos IoT y su rol en las investigaciones criminales. De la misma forma, permitirá identificar conceptos sobre los cuales se podrá profundizar en el futuro.

3.3 Enfoque

Para esta investigación se utiliza un enfoque cualitativo, un método de inferencia de resultados llamado “ideográfico”, en el cual no se comprueban leyes universales. Asimismo, se aplica el método inductivo (de lo específico a lo general).

Capítulo 4. Análisis del Diagnóstico

4.1 Descripción de las principales etapas

Durante el desarrollo de este capítulo se describen las principales etapas identificadas en el proceso del análisis forense de dispositivos IoT en investigaciones criminales. Se describen sus características más importantes que faciliten la comprensión de estas. Para la definición de las etapas, se analizaron diversas fuentes, con el fin de identificar las fases en común de cada enfoque y tratar de llegar a una definición uniforme.

En primer lugar, Stoyanova et al. (4) mencionan las siguientes etapas como parte de la investigación forense: identificación de la evidencia, adquisición de la evidencia, preservación y protección de la evidencia, análisis de la evidencia, interpretación y, como última, el reporte y presentación de la evidencia. De la misma forma, Stoyanova et al. (4) agrupan los retos de la ciencia forense digital de dispositivos IoT en 6 grupos, los cuales son: identificación de la evidencia, adquisición de la evidencia, preservación y protección de la evidencia, análisis y correlación de la evidencia, atribución del ataque y la presentación de la evidencia.

Por otra parte, Collie et al. (5) presentan las diferentes etapas encontradas en el modelo de la ciencia forense digital: la identificación de la evidencia, preservación de la evidencia, recuperación de la evidencia y la presentación de la evidencia. Qatawneh et al. (3) muestran las siguientes etapas, pre-investigación, recolección y evaluación, preservación, revisión y análisis, etapa de intercambio de información.

Sobre la base de estas 3 fuentes, las etapas que van a ser caracterizadas son: identificación, recolección, preservación, revisión y análisis, reporte o presentación de la evidencia.

4.1.1 Identificación

Stoyanova et al. (4) mencionan que la identificación es el paso más importante, por ser el punto de partida de los retos de la ciencia forense digital. Esto debido a que la complejidad y diversidad entre dispositivos de IoT hacen difícil el simple hecho de saber dónde está almacenada la información.

Durante esta fase, en primera instancia, se deben identificar las fuentes de evidencia disponible. El investigador debe definir cuáles dispositivos almacenan información relevante. Adicionalmente, se debe obtener el dónde y en qué formato está guardada información importante (2).

De la misma manera, Stoyanova et al. (4) mencionan que durante esta primera etapa puede presentar diferentes retos para los investigadores, como los pueden ser:

- Alcance del compromiso y reconstrucción de la escena del crimen: En la ciencia forense tradicional, los límites pueden definirse fácilmente. El contexto de IoT, sin embargo, implica una interacción autónoma y en tiempo real entre varios nodos, lo que hace casi imposible reconstruir la escena del crimen e identificar el alcance del daño, debido a la naturaleza altamente dinámica de la comunicación.
- Proliferación de dispositivos y datos: El creciente número de dispositivos interconectados y la cantidad de datos forenses digitales que requieren análisis, han generado que las herramientas forenses digitales tradicionales sean incapaces de manejar un aumento tan

colosal de volumen, variedad y velocidad, y que a la vez trae como consecuencia para los investigadores que no solo tengan que identificar lo que es útil para la investigación, sino también descartar los datos irrelevantes.

- Ubicación de datos: Mientras están en funcionamiento, los dispositivos de IoT pueden migrar con frecuencia entre diferentes ubicaciones físicas. Por lo tanto, incluso si se conoce la ubicación, adquirir el sistema no está exento de complicaciones, como lo pueden ser diferentes jurisdicciones o afectación que se puede dar a otros usuarios que estén utilizando la misma arquitectura.
- Tipo de dispositivo: A diferencia de la ciencia forense digital tradicional, donde los objetos de interés forense suelen limitarse a diferentes tipos de sistemas informáticos o teléfonos móviles, la fuente de evidencia en los casos centrados en IoT podría ser heterogénea: a partir de un vehículo autónomo que provocó un accidente fatal, a una tostadora inteligente que se encendió durante la noche e inició un incendio en el hogar. Algunos dispositivos de IoT pueden ser difíciles de encontrar para los profesionales forenses, debido a sus pequeñas dimensiones. Sensores médicos, por ejemplo, que podrían tener solo 8,1 x 10,5 mm de tamaño y pesar menos de 2 gramos.

4.1.2 Recolección

Después de que los dispositivos fueron identificados correctamente, sigue la etapa de recolección y extracción de la información, en la que los investigadores encuentran retos, como la no estandarización, que dificulta la utilización de un proceso estándar para este. Los mayores desafíos son creados por la capacidad

limitada de los dispositivos, sus diferentes interfaces y sus diferentes formatos de almacenamiento (2).

Como consecuencia de lo anterior, no existe un método estándar para extraer información de un dispositivo IoT, lo contrario a lo visto en la ciencia forense convencional, que tiene un proceso y métodos estándar que minimizan la tendencia a fallar o contaminar la evidencia durante este proceso (4).

Por otra parte, no solo los dispositivos presentan estos retos. También los investigadores enfrentan otra clase de desafíos, como los expuestos por Stoyanova et al. (4), detallados a continuación:

- Falta de capacitación y gestión del conocimiento deficiente: Se identificó la necesidad de capacitación en la nube para los primeros respondedores e investigadores y también se indica que los organismos encargados de hacer cumplir la ley deberían organizar programas de capacitación para sus primeros respondedores con el fin de instruirlos sobre cómo adquirir evidencia digital de una manera forense. Por último, también se mostró que muchos de los investigadores eran descuidados con la gestión de la evidencia.
    - Cifrado de datos: En la actualidad, para mejorar la confianza del consumidor, muchos sistemas operativos y plataformas brindan soporte integrado para el cifrado. La existencia de herramientas criptográficas tan fáciles de usar, ha hecho que sea conveniente para los usuarios preservar la seguridad de sus datos. Sin embargo, al tener un control total sobre la infraestructura de la nube, los usuarios podrían ocultar o manipular información, irrecuperable para el proveedor.

- Especificaciones heterogéneas de *software* y / o *hardware*: Otro desafío técnico relacionado con la extracción de pruebas de los dispositivos IoT es que cada fabricante adopta un *hardware* y sistemas operativos diferentes. Además de esta complejidad, los protocolos de comunicación de los dispositivos IoT pueden ser igualmente diversos.
- Privacidad y consideraciones éticas al acceder a datos personales: Más allá de los desafíos técnicos, la privacidad es un tema importante por considerar al recopilar datos. Los dispositivos de IoT, como los rastreadores de actividad física o los sistemas remotos de control de la salud, tratan información personal confidencial, incluidos los registros médicos, las recetas o el estado de salud actual de los usuarios. Para respetar los acuerdos de confidencialidad con sus clientes, los proveedores de servicios en la nube se niegan a dar acceso a la memoria compartida, por parte de las autoridades, porque también esta puede contener datos de clientes ajenos a la investigación. En especial, un contexto de tenencia múltiple, existen métodos muy limitados para crear una imagen forense sin violar ninguna consideración ética.
- Valor forense de la evidencia: Algunos proveedores de servicios de IoT dejan de respaldar sus marcos y aprovechan para entregar actualizaciones de seguridad. Esto se aplica en particular a las empresas. Es parte de la escena emergente en expansión, que decide concentrarse en nuevos productos y dejar de apoyar los antiguos. Los datos recopilados de dichos dispositivos de IoT son menos valiosos, porque podrían ser manipulados fácilmente por un

pirata informático que se aprovechó de las vulnerabilidades de seguridad. Aparte de eso, los datos de IoT suelen ser intermitentes. Los nodos que funcionan con energía solar, por ejemplo, podrían contener solo información fragmentaria, debido a un suministro de energía insuficiente.

- Falta de un modelo forense común en IoT: La teoría y la práctica carecen de un enfoque de adquisición válido y comúnmente aceptado para los sistemas de IoT Según el caso, el organismo de investigación responsable elige diferentes métodos. Sin embargo, un escogimiento de la metodología desafortunada podría tener muchas complicaciones posibles. Por una parte, las pruebas reunidas pueden impugnarse fácilmente en los tribunales debido a omisiones en la forma de recopilación. Por otra parte, los delitos transfronterizos requieren la cooperación entre organismos de investigación de dos o más países. Se encuentran problemas por la ausencia de acuerdos supranacionales. Por lo tanto, es necesario unificar los enfoques de recopilación de pruebas, porque, de lo contrario, existe el riesgo de violar una ley local y, en consecuencia, hacer que las pruebas importantes no sean confiables.

4.1.3 Preservación

Durante el desarrollo de esta fase se tiene como objetivo el preservar la información obtenida y el garantizar su integridad. El término "cadena de custodia" podría definirse como el control de auditoría, vigilantes de la originalidad e integridad de las evidencias. La ciencia forense convencional comienza cuando los investigadores reúnen una pieza de evidencia en la escena del crimen y termina con

la presentación del material probatorio en el tribunal. Como uno de los temas fundamentales en toda investigación forense, el propósito de la cadena de custodia es brindar información clara sobre cuándo y cómo se recopilaron, preservaron, analizaron y presentaron las pruebas. Además, este procedimiento demuestra que el material probatorio no ha sido alterado o cambiado durante todas las etapas de la investigación forense (4).

De la misma manera, esta etapa también presenta sus propios retos que Stoyanova et al. (4), describen de la siguiente forma:

- Asegurar la cadena de custodia: En el caso de los dispositivos IoT, los datos de las pruebas deben recopilarse de varios servidores remotos, lo que complica significativamente la misión de mantener una cadena de custodia adecuada. Además, el formato de los datos recopilados de un determinado dispositivo de IoT puede ser diferente del formato de los datos almacenados en la nube. Esto se debe a que antes de ser guardado, fue procesado por algoritmos analíticos. Por último, se debe devolver a su formato original antes de realizar el análisis. De lo contrario, no será admitido en los tribunales.
- Limitación de la vida útil: Otro desafío en la preservación de datos está relacionado con el espacio de memoria limitado en los dispositivos de IoT. Debido al hecho de que los sistemas de IoT se ejecutan continuamente, los datos se pueden sobrescribir fácilmente, lo que da lugar a la posibilidad de que falten pruebas. Transferir los datos a un dispositivo de almacenamiento local podría parecer una solución fácil en este caso. Sin embargo, este enfoque no puede asegurar la cadena de evidencia antes mencionada, porque los datos podrían modificarse

durante la transferencia. Además, algunos dispositivos IoT emplean sistemas operativos en tiempo real (RTOS) y no almacenan datos de forma predeterminada.

- Los problemas de la ciencia forense en la nube: La sinergia entre la nube y la IoT ha surgido porque la nube posee atributos que permiten y benefician la expansión de la IoT. Sin embargo, la nube se compone de una gran cantidad de problemas de seguridad. Esto no es sorprendente porque la computación en la nube abarca muchas tecnologías, incluidas las redes, la virtualización, las bases de datos, los sistemas operativos, la programación de recursos, el equilibrio de carga, la memoria y la gestión de transacciones. Las vulnerabilidades de todos los sistemas antes mencionados se reflejan en la seguridad de los marcos arquitectónicos de la nube. Por lo tanto, los datos conservados en la nube tienen un valor forense limitado, ya que podrían haber sido alterados por un usuario malintencionado que se aprovechó de las vulnerabilidades.
- Asegurar la evidencia según la implementación y/o el modelo de servicio de la nube (PaaS, SaaS, IaaS): Un aspecto importante en IoT Forense es la disponibilidad de diferentes paradigmas para brindar servicios en la nube. Según el modelo de implementación, la nube podría ser pública, privada, comunitaria o híbrida.

4.1.4 Revisión y análisis

Durante el desarrollo de esta etapa se desarrollan diferentes procesos que permiten analizar y correlacionar la información. Algunos de estos se

caracterizan en este apartado: la reducción de la información, análisis de correlación, reconstrucción de una línea de tiempo y procesos relacionados con la privacidad de la información (1). J. Hou et al (1) las describen de la siguiente manera:

- Reducción de datos: el creciente número de dispositivos IoT aumenta el volumen de datos forenses. Los investigadores deben revisar cientos o miles de documentos estructurados o no estructurados, recopilados de fuentes de datos para extraer y evaluar piezas de información relevantes. Algunas investigaciones exploraron el método de obtención de imágenes selectivas para reducir el volumen de datos forenses y extraer automáticamente los datos relevantes, conservando la información en el formato de archivo de origen nativo con *metadatos* originales. También se está trabajando en el uso de métodos de minería de datos y aprendizaje automático para identificar de manera eficiente los hechos, a partir de gran cantidad de datos forenses digitales. Sin embargo, los resultados obtenidos por medio de estas técnicas suelen ser difíciles de interpretar, lo que lleva a la duda de si los resultados son fiables y legalmente aceptables.
- Análisis de correlación: La combinación de datos de una variedad de fuentes de datos puede ayudar a proporcionar una mayor comprensión de un corpus de datos. Aunque analizar una variedad de dispositivos dispares no es nuevo en el análisis forense digital, cada vez es más difícil identificar por completo todas las fuentes de evidencia cuando el límite de un caso basado en IoT es borroso. También existe el desafío de mantener el equilibrio entre el creciente volumen de datos y el costo

de tiempo en el paradigma forense de IoT. Quick y Choo exploraron el método de análisis entre dispositivos y casos cruzados y las técnicas de análisis rápido. Propusieron un método de escaneo semiautomático para subconjuntos de datos forenses dispares, incluidos datos de una variedad de dispositivos portátiles, computadoras, teléfonos móviles y la nube.

- Reconstrucción de la línea de tiempo: El parámetro de tiempo es de gran valor para la asociación de evidencia de diferentes fuentes y ayuda a secuenciar los incidentes relevantes de interés. Sin embargo, muchos dispositivos no están sincronizados en el tiempo porque utilizan diferentes granularidades de tiempo y los usuarios están distribuidos en diferentes zonas horarias, lo que aumentaría la complejidad de la reconstrucción de la línea de tiempo para la ciencia forense de IoT.
- Preocupación por la privacidad: Los datos almacenados y procesados en dispositivos de IoT pueden ser confidenciales. Para recopilar y analizar datos en algunos dispositivos de IoT, los investigadores pueden acceder a los datos confidenciales, lo que genera preocupación por la privacidad. El trabajo existente ya ha comenzado a centrarse en la preservación de la privacidad en el proceso de investigación.

4.1.5 Reporte y presentación de la información

Presentar hallazgos forenses en un caso que involucra IoT puede ser un desafío. Es un nuevo campo legal y forense. Los tribunales recién están

aprendiendo a aceptar pruebas virtuales y esta combinación física / virtual que trae IoT puede resultar confusa (2). También hay una pregunta adicional en esta fase, así como en las otras, de si un tribunal aceptará la metodología y las herramientas utilizadas, porque aún no están estandarizadas (2).

Hay varios temas que son más relevantes para los forenses que para los investigadores, pero deben mencionarse. ¿Cuánto conocimiento judicial y comprensión de las operaciones de IoT se debe asumir? ¿Deben llevarse los dispositivos de IoT a los tribunales y proporcionar una explicación sobre cómo funcionan antes de presentar pruebas de ellos? ¿Debería un experto en TI o IoT presentar pruebas? (2). Hay sistemas legales que requieren la presentación de la evidencia frente a un panel de jurados en la sala del tribunal. Antes de ser interrogados y elegidos por el juez y/o los abogados, los posibles miembros del jurado fueron elegidos entre la comunidad utilizando un método razonablemente aleatorio. Esto significa que lo más probable es que el jurado solo tenga conocimientos básicos de informática en la nube y análisis forense, según los medios de comunicación o en su experiencia personal con la tecnología de IoT. Sería una tarea desafiante explicarles los tecnicismos detrás de una arquitectura tan compleja en el tiempo muy limitado del juicio (4).

4.2 Explicación de las herramientas utilizadas en las diferentes etapas

4.2.1 Metodologías

En un campo donde la poca estandarización de procesos y de los dispositivos analizados, las metodologías y los marcos de trabajo cumplen un rol fundamental en este proceso de obtener evidencias que sean veraces y que puedan ser relevantes en investigaciones criminales. En este apartado se muestran metodologías y

marcos de trabajo utilizados para este tipo de procesos, en los que se proponen diferentes enfoques para enfrentar los retos presentados.

Uno de los enfoques para la identificación de la evidencia es definida por Bouchaud et al. (6) Estos autores indican que cuando un investigador llega a la escena del crimen, lleva a cabo varias operaciones metódicas conserva toda la escena contra la contaminación externa, registra todos los elementos presentes para poder identificarlos y recogerlos posteriormente. El proceso de identificación se divide en 4 pasos: la detección, la localización, el reconocimiento y el *check-in*.

En la fase de detección, los investigadores estudian el comportamiento de un entorno, buscan señales emitidas. Esta información es visible con o sin acción externa. Por lo tanto, hay dos enfoques en la detección de acuerdo con los presentes elementos. Después de capturar la señal, los investigadores buscan determinar su origen triangulando el entorno y cruzando la información. Este enfoque de seguimiento de la red permite localizar la fuente de la emisión.

El proceso de reconocimiento se realiza a partir de la información visible en el dispositivo objetivo y la información de frecuencia capturada. Las tablas de correspondencia le permiten realizar conciliaciones. Se realiza el *check-in* en una lista de posibles pruebas. El investigador estudia los dispositivos de interconexión. Él determina el rol de cada elemento: actuadores, captores, nodos de red local, pasarelas, GUI, API. Se realiza un enfoque de gráfico de dependencia.

De la misma forma, Bouchaud et al. (6) proponen un procedimiento de selección de evidencias con la que buscan proporcionar el mejor indicio en la escena del crimen. Esta tarea se realiza después de la identificación de todos los dispositivos e infraestructura con el enfoque de identificación de IoT. En esta fase del proceso, se debe ser lo más objetivo y metódico posible.

En la propuesta se busca evaluar para posteriormente pesar la evidencia basada en 4 propiedades, como lo son relevancia de la información, que está compuesta por 3 ejes: la relación con el evento, la relación temporal y espacial. Cuanto mayor sea la proximidad espacial, temporal y relacional, más relevantes y precisos serán los datos recopilados para el evento. Esta información contextualiza los datos recopilados.

De la misma manera, otra característica de relevancia es la accesibilidad de la información presente en los dispositivos, que es también un criterio para tener en cuenta en la elección de la prueba. Para cada dispositivo seleccionado, es más o menos difícil acceder a los datos. La localización de la información es otro factor digno de ser considerado. Se centra en el posicionamiento de los datos capturados y la capacidad de almacenamiento de las diferentes infraestructuras de IoT.

Finalmente, el tipo de datos se divide en tres características: directo, transformado mecánicamente o interpretado por humanos. Los datos directos son datos brutos medidos por un sensor. Los datos son modificados y contextualizados por el dispositivo de acuerdo con los parámetros definidos, como una noción de umbral. Estos datos pueden llevar a una interpretación humana.

Por otra parte, otro modelo propuesto es el de combinar DFINT con el modelo OSINT. Presenta un marco para la identificación de entidades y la cohesión de la información de fuente abierta para agregar valor a las existencias de datos de subconjuntos de datos forenses digitales. La aplicación del marco para probar los datos dio como resultado la ubicación de información adicional relacionada con las entidades contenidas dentro de los subconjuntos de datos forenses digitales, lo que llevó a agregar valor de inteligencia relacionado con las entidades. El análisis de datos del mundo real confirmó el potencial de agregar valor a gran cantidad de

datos forenses digitales para descubrir información dispar e información de fuente abierta. Los resultados demuestran los beneficios de aplicar el proceso para lograr una mayor comprensión de los datos forenses digitales de manera oportuna. (7)

De la misma manera, Qatawneh et al. (3) proponen un nuevo modelo de investigación forense digital para IoT (DFIM). El DFIM tiene dos componentes principales: la zona de proveedor de datos (DPZ), que es responsable de agrupar todos los datos recopilados por los nodos sensores en un conjunto de grupos, donde cada grupo contiene datos o documentos relacionados entre sí, y la autoridad de investigación que recibe la información, solicitudes de los reclamantes para investigación, verifique la validación de la solicitud y finalmente seleccione los investigadores apropiados. Para mejorar el proceso de investigación forense de IoT, el DFIM propuesto consta de siete etapas y toma en consideración un conjunto de principios como seguridad, precisión de privacidad, rendimiento, reducción de datos, apertura y transparencia.

Por otra parte Jan Collie & Richard E Overill (5) presentan una extensión al modelo de proceso forense digital (DFPM), el proceso mejorado de evidencia digital (DEEP), con el objetivo de afinar el mecanismo y asegurar que toda la evidencia digital sea examinada por un analista forense digital calificado. La consecuencia de adoptar DEEP en las investigaciones penales reales será garantizar que todas las pruebas digitales se analicen y evalúen con los más altos estándares de competencia profesional y técnica, lo que dará como resultado una mayor confiabilidad de las pruebas digitales presentadas en los tribunales que servirán a la causa de la justicia en términos de casos reducidos de condenas inseguras asociadas y/o exculpaciones injustificadas.

Finalmente, Stoyanova et al. (4) muestran un resumen general de los marcos teóricos forenses de IoT recientes (2016-2019).

- DFIF-IoT: El marco de investigación forense digital para IoT (DFIF-IoT) es un marco genérico propuesto por Kebande y Ray en 2016. Una de las principales ventajas de este enfoque es que cumple con ISO / IEC 27043: 2015, una norma todavía válida y reconocida internacionalmente sobre principios de investigación de incidentes. Este modelo es capaz de analizar la evidencia digital potencial (PDE) generada por un ecosistema basado en IoT. Otra ventaja del modelo es que se pueden aplicar fácilmente a varios entornos de IoT. Al mismo tiempo, carecen de detalles de bajo nivel que permiten su adaptación a diferentes escenarios sin cambiar ningún componente o proceso principal.
- El algoritmo Last-on-Scene (LoS) de Harbawi y Varol: en 2017, Harbawi y Varol [94] proporcionaron un marco teórico mejorado para la ciencia forense de IoT que hace frente a los problemas de adquisición de pruebas. Su algoritmo LoS establece que el dispositivo que representa el último nodo en la cadena de comunicación debe ser el primero en ser investigado. El beneficio de este concepto teórico es que limita el alcance de la investigación.
- FSAIoT: Modelo de adquisición de estado forense para dispositivos IoT, otro modelo que se centra en el proceso de adquisición de pruebas consiste en un controlador de adquisición de estado forense centralizado (FSAC), empleado en tres modos de recopilación de

estados: controlador a dispositivo IoT, controlador a nube y controlador a controlador.

- Análisis forense digital de aplicaciones específicas: Ofreció un nuevo modelo forense que consta de tres componentes independientes: análisis forense específico de la aplicación, análisis forense digital y proceso forense.
- IoTDots (un marco de trabajo forense digital para entornos inteligentes): analiza y modifica automáticamente las aplicaciones inteligentes para detectar y almacenar información de relevancia forense dentro de las aplicaciones. El marco consta de dos componentes principales: modificador (ITM) y analizador (ITA). Una vez que el ITM detecta los datos relevantes, se envía a una base de datos segura (ITD). En un segundo paso, IoTDots aplica el procesamiento de datos y el aprendizaje automático para detectar evidencia digital valiosa, de dispositivos inteligentes, aplicaciones o actividades de los usuarios.
- Análisis forense de IoT consciente de la privacidad: extraer datos de pruebas, sin violar el derecho a la privacidad de los usuarios podría resultar especialmente complicado en el contexto de IoT. Por tanto, este modelo toma en consideración las regulaciones de privacidad al incorporar la regulación ISO / IEC 29100: 2011 a lo largo de todo el proceso de investigación forense. El marco propuesto enfatiza la importancia de colaborar con dispositivos cercanos para recopilar información y reconstruir el contexto de la escena del crimen.

- Un modelo forense holístico: En 2019 es presentado un modelo forense integrado para IoT que se basa en la norma internacional actual ISO / IEC 27043. El marco propuesto tiene como objetivo cubrir todo el proceso forense y, por lo tanto, consta de tres fases principales: preparación forense (proactiva), inicialización forense (incidente) e investigación forense (reactiva).
- Marcos de investigación basados en *blockchain*: este sugiere que mover el internet de las cosas por el camino descentralizado puede ser la clave para gestionar la gran cantidad de *ciberataques*. Además, la naturaleza inmutable y distribuida de la tecnología *blockchain* también puede adaptarse a las demandas de IoT Forensics. La evidencia digital podría recopilarse y actualizarse en el libro mayor donde la inmutabilidad de la cadena de bloques asegure su validez y su carácter, sin cambios. La unidad investigadora podría acceder de manera confiable a la información de relevancia forense desde cualquiera de los nodos, en cualquier momento. Por lo tanto, *blockchain* podría usarse para marcar la hora y mantener la integridad de la evidencia digital.
- Análisis de evidencia basado en video: En 2019, Ericsson predijo que el tráfico de video crecerá alrededor de un 34 por ciento anual, y para 2024 representará casi las tres cuartas partes del tráfico de datos móviles. Además, según el mismo informe de movilidad de Ericsson, se espera que la realidad aumentada y la transmisión de video de 360 grados sean otro factor significativo en el crecimiento del tráfico móvil. Debido a la mayor cantidad de datos de video de teléfonos

inteligentes, así como a la popularidad de los sistemas de vigilancia de bajo costo, el material visual se está utilizando progresivamente en la disciplina forense digital.

- Marcos de análisis forense de movilidad: el análisis forense de movilidad integra redes *ad hoc* de vehículos (VANET), internet de las cosas y computación en la nube móvil. Es un campo complejo que tiene como objetivo hacer frente a los desafíos de las infraestructuras distribuidas, altamente dinámicas. El ensamblaje de dispositivos interconectados incluye vehículos autónomos inteligentes y vehículos aéreos no tripulados (por ejemplo, drones), varios dispositivos móviles e incluso equipo militar.

4.2.2 Herramientas

Por otra parte, las herramientas que se enumeran en este apartado no son específicamente utilizadas para el análisis forense de dispositivos IoT, pero facilitan el proceso de análisis forense digital en general y se adaptan a diferentes enfoques de análisis. Desde el mismo punto de vista, Yaqoob et al. (8) muestra algunas de estas herramientas más comunes:

- El entorno de investigación asistido por computadora (CAINE) es una herramienta forense interactiva y de código abierto que admite múltiples fases forenses.
- EnCase se utiliza para realizar análisis de imágenes, datos y archivos forenses.

- Wireshark se utiliza principalmente para análisis forense de redes. La principal limitación de Wireshark es que presente deficiencias con grandes cantidades de datos de red.
- Bulk Extractor ayuda a escanear y extraer información, por ejemplo, números de tarjetas, direcciones de correo electrónico, direcciones web y números de teléfono de las imágenes de disco y archivos de directorio.
- NUIX se utiliza para escanear una gran cantidad de datos y procesos que conducen a extraer la información útil que luego se utiliza para el análisis.
- RegRipper se utiliza principalmente para escanear los archivos de registro de Windows.
- IEF se utiliza para escanear las imágenes forenses y una amplia gama de datos extraídos del historial de Internet, historial de chat y sistemas operativos.
- NetAnalysis ayuda a escanear las imágenes forenses y los datos asociados con el historial de internet.
- Pajek64 ayuda a analizar una gran cantidad de datos relacionados con la red.

4.3 Organización de los diferentes tipos de evidencias digitales

En esta sección se busca presentar la organización de los diferentes tipos de evidencias, que facilite la comprensión del valor de la evidencia en las investigaciones criminales. Desde este punto de vista, Bouchaud et al. (6) proponen un modelo de clasificación de la evidencia basado en el peso del dispositivo,

utilizando las propiedades de los datos descritas en la sección anterior (relevancia de la información, accesibilidad de la información, localización y el tipo de información), las cuales definen la relevancia de la recopilación de información en diferentes partes de la infraestructura de IoT. Esta clasificación se desarrolla respecto del principio técnico: el costo de desempeño de las operaciones y el impacto en la calidad de los resultados. La idea es proponer formas de seleccionar la mejor evidencia en la escena del crimen.

Entonces, la tabla está formada por las columnas de los cuatro criterios de datos: la relevancia, la accesibilidad, la localización y el tipo. La fila está integrada por las cuatro partes de la infraestructura de IoT: sensores, la puerta de enlace, la plataforma de IoT y el “Human-computer interaction” (HCI) por sus siglas en inglés y que envuelve todo lo relacionado con la interfaz de usuario y sus API’s. Los sensores son los puntos de recogida de información. Sensores de interfaz de pasarelas en Internet. La plataforma almacena datos y los procesa en espacios similares a la nube. El HCI proporciona a los usuarios un punto de acceso a la información de la infraestructura. Estas partes se desglosan según las nociones de productividad, el costo de las operaciones y el impacto de las operaciones en los datos.

La productividad es el resultado del esfuerzo realizado para obtener los datos, el costo humano es el tiempo de ejecución de la operación, el costo de ingeniería es el aspecto financiero de la operación, la alteración es el impacto de las operaciones realizadas en los dispositivos. En la tabla 1, el criterio 1 corresponde al peso más fuerte y el 4 al más débil.

A partir de los pesos definidos, elaboraron una clasificación de dispositivos de la infraestructura de IoT (tabla 2). El resultado principal, que no es sorprendente, es

que la recopilación de pruebas es fácil desde los dispositivos que administran los dispositivos de IoT o desde el operador de la nube que recopila los datos. Es más difícil obtener los mismos resultados cuando se trata directamente con los sensores.

La interfaz gráfica (API y GUI) representa el dispositivo con el mejor rendimiento. Debido a su posición de interfaz con los usuarios, se centra en los datos directos de todos los dispositivos IoT conectados a la red. Los datos devueltos a esta interfaz se interpretan y se ubican en perspectiva. Por lo tanto, los investigadores pueden aprovecharlos fácilmente durante el análisis. Sin embargo, el acceso a los datos depende del tipo de interfaz. Consecuentemente, las operaciones de recopilación pueden ser técnicamente complejas y requerir mucho tiempo, lo que genera un riesgo de corrupción de datos y costos significativos en investigación y desarrollo, especialmente en la capa de aplicación. Además, esta interfaz contiene solo los datos que el diseñador quiere que se muestren.

La plataforma también tiene un rendimiento interesante por su *hub* y función de almacenamiento de datos. En comparación con el HCI, la mayoría de las veces, la nube contiene datos transformados, sin filtros ni cálculos. Sin embargo, los datos son deportados a la escena del crimen y requieren la intervención de un tercero en la investigación: el operador de la plataforma IoT. Por lo tanto, el investigador no controla la forma de recopilar la información. Además, de antemano, es necesario un conocimiento preciso de los elementos por extraer para localizar la información correcta a recuperar. Este conocimiento depende de los elementos recopilados localmente. Por lo tanto, los factores de tiempo y distancia son los elementos de bloqueo de este enfoque.

La puerta de enlace, interfaz entre la red local e internet, contiene principalmente información indirecta en forma de archivos de registro. La

explotación de estos elementos requiere un conocimiento profundo de la red local y del dispositivo presente. Las puertas de enlace contienen información técnica sobre la red local, como dispositivos o configuraciones definidas por el usuario.

Los sensores son la interfaz entre la escena del crimen y la infraestructura de IoT. Son los testigos directos de los hechos. Este dispositivo de adquisición contiene datos de la escena del crimen, sin procesar. Esta información no siempre es legible ni accesible. Sus colecciones deben pasar por un enfoque electrónico. La red local consta de un conjunto de objetos interconectados. Por lo tanto, el objeto solo tiene la información que le es específica.

		Data relevance	Data accessibility	Data localization	Data type	Total	Classification
Productivity	Sensor	1	4	4	3	12	2
	Gateway - Node	4	1	3	4	12	2
	IoT platform	3	2	1	2	8	1
	HCI (API - GUI)	2	3	2	1	8	1
Human cost	Sensor	4	4	3	4	15	3
	Gateway - Node	3	1	1	3	8	1
	IoT platform	1	2	4	1	8	1
	HCI (API - GUI)	2	3	2	2	9	2
Engineering cost	Sensor	4	4	3	1	12	3
	Gateway - Node	3	2	1	4	10	2
	IoT platform	1	1	4	3	9	1
	HCI (API - GUI)	2	3	2	2	9	1
Alteration	Sensor	4	4	3	1	12	3
	Gateway - Node	3	3	2	4	12	3
	IoT platform	1	1	4	3	9	2
	HCI (API - GUI)	2	2	1	2	7	1

Tabla 1 – Categorización de dispositivos basada en propiedades de datos y principios técnicos (6)

	Total by data	Classification
Sensor	51 *(12+15+12+12)*	4
Gateway - Node	42 *(12+8+10+12)*	3
IoT platform	34 *(8+8+9+9)*	2
HCI (API - GUI)	33 *(8+9+9+7)*	1

Tabla 2 - Clasificación de dispositivos de la infraestructura de IoT (6)

Desde el mismo punto de vista, como se ha mencionado anteriormente, los dispositivos varían bastante en cuanto a forma, componentes, información que procesan, capaz de infraestructura, etc. por lo que esta clasificación debe entenderse de manera general y, según el dispositivo que esté en análisis, debe ser adaptada.

Además, sobre la base de lo mencionado por Bouchaud et al. (6), muestran que la clasificación de la información y la evidencia siguen siendo un camino incierto y donde depende completamente del dispositivo por analizar y que, como se ha mencionado, está en constante cambio y crecimiento.

4.4 Relevancia de las evidencias digitales

En esta sección se busca reconocer la relevancia que tienen o no las evidencias digitales que se obtienen del proceso del análisis forense digital en las investigaciones criminales. Para valorar la relevancia de las evidencias forenses digitales obtenidas de dispositivos IoT, es primordial entender el proceso de validación que esta sufre para ser considerada como válida en proceso de investigación criminal.

Desde ese punto de vista, según Arshad et al. (9), las técnicas forenses digitales deben verificar su precisión y validación utilizando metodologías probadas sistemáticamente. Para ello, es fundamental establecer la disciplina sobre principios científicos sólidos para ganar la credibilidad deseable y evitar conceptos erróneos y desacuerdos en los tribunales.

Además, menciona que lo que se considera como “buena ciencia” forense en tribunal es caracterizado por la presencia de hipótesis comprobables, resultados reproducibles, proceso verificable, revisión por pares o publicación, aceptación

general, estandarización, experimentación, practicidad, imparcialidad, explicación realista y uso de métodos precisos. La “buena ciencia" se convierte en "mala ciencia" si no se formula, entrega o se comporta de manera apropiada reflejando al menos una de las características mencionadas anteriormente como ciencia válida, ya sea accidentalmente o sin saberlo.

De la misma forma, es importante conocer los principales problemas de aceptación que presenta la evidencia digital como evidencia científica y que también son mencionados por Arshad et al. (9).

4.4.1 Conjuntos de datos estándar

Los investigadores deben utilizar conjuntos de datos idénticos para evaluar y probar nuevas técnicas o volver a implementar otros métodos para evaluar y verificar sus propios conjuntos de datos. Los investigadores del campo de la ciencia forense digital todavía se enfrentan al problema de no disponer de conjuntos de datos estándar con fines de experimentación comparativa, además: la disponibilidad, cantidad, integridad y calidad de los conjuntos de datos existentes son cuestiones importantes. Esto porque parecen ser insuficientes tanto en tamaño como en alcance. En ausencia de conjuntos de datos estándar, es casi imposible comparar los resultados de los diferentes métodos de investigación y evaluarlos en su uso práctico.

Al mismo tiempo, las pruebas sistemáticas no se pueden lograr sin los mismos conjuntos de datos y es posible que no sea posible compartir datos de casos criminales reales con la comunidad científica, debido a restricciones de privacidad y soberanía de datos.

En ausencia de conjuntos de datos estándar, los académicos, para probar su trabajo, han estado utilizando varios métodos para obtener datos adecuados. En consecuencia, generalmente se basan en conjuntos más pequeños de datos disponibles públicamente y, en la mayoría de los casos, crean sus propios conjuntos de datos, por lo que el proceso de recopilación, pre procesamiento y organización de datos suele crear un sesgo no intencionado en los conjuntos de datos.

La tasa de error es la medida de la frecuencia de errores en un método dado. Se utiliza para establecer la precisión y confiabilidad de ese enfoque y se presenta como falsos positivos y falsos negativos. Sin embargo, estas tasas de error se utilizan para referirse a errores aleatorios; estos errores surgen de cambios desconocidos e impredecibles durante el experimento. En las técnicas forenses digitales, la mayoría de los errores son sistemáticos en lugar de aleatorios y surgen a causa del uso de herramientas y de métodos imperfectos o inapropiados. Por lo tanto, calcular y asociar tasas de error arbitrarias para cualquier método o herramienta no confirma la confiabilidad ni la precisión de esa técnica o herramienta de *software*.

Además, Arshad et al. (9) mencionan que las técnicas y herramientas forenses para las redes sociales o la plataforma en la nube todavía se consideran en su infancia. Encontrar fuentes potenciales de errores y modelos de prueba formales sigue siendo un tema abierto en este campo.

4.4.3 Problemas de estandarización

Arshad et al. (9) explican que la ciencia forense digital se ocupa de una amplia variedad de dispositivos electrónicos y formatos de información que son propiedades adicionales de un grupo diverso de desarrolladores de *software* y fabricantes de dispositivos. De hecho, la creación de estándares, para un grupo tan

grande y variado de partes interesadas, es una tarea desafiante. Además, para complicar aún más la situación, los participantes se muestran reacios a aceptar determinadas normas y reglas y, a menudo, dan lugar a posibles conflictos de intereses entre ellos.

La comunidad académica y los profesionales siempre se han quejado de la falta de procedimientos operativos estándar en la ciencia forense digital y han expresado enérgicamente la necesidad de contar con métodos sistemáticos y sólidos para las investigaciones forenses. Aún así, muy pocos estándares y procedimientos parcialmente productivos están disponibles dentro del dominio.

4.4.4 Otros problemas

Arshad et al. (9) agregan, además, los siguientes problemas que enfrente en general la ciencia forense en la validación de sus pruebas:

- Falta de pruebas formales: que esto comúnmente se da por el rápido evolución de los dispositivos, costo de las pruebas, el *time* que estas consumen, falta de verificables y recursivos protocolos de pruebas en este campo.
- Problemas de aceptación general: estos normalmente se dan porque existe un grupo muy diverso de desarrolladores de software y fabricantes de dispositivos, conflicto de intereses y resistencia a unirse al estándar.
- Métodos *anti-forenses*: cualquier intento o metodología utilizada para modificar, alterar, refutar o restringir una investigación científica forense válida se considera anti-forense.
- Rápida evolución y diversidad.

Finalmente, Arshad et al. (9) considera que la ciencia forense digital no es una disciplina basura o inválida, sin embargo, necesita tiempo para madurar y establecerse como todas las demás ciencias. No se justifica referirse a la ciencia forense digital como ciencia inválida sin comprender las limitaciones fundamentales de la validez científica y los aspectos opuestos del dominio. El tiempo necesario para que prospere la ciencia forense digital se acorta gracias al rápido desarrollo de la tecnología de la informática y las comunicaciones digitales y que sería injusto culpar a los investigadores por la falta de esfuerzo en el desarrollo de métodos científicos.

Capítulo 5. Conclusiones y Recomendaciones

5.1 Conclusiones

- Se obtiene como primera conclusión que, a pesar de existir diferentes enfoques en cuanto al proceso de análisis forense digital de dispositivos IoT, las etapas de identificación, adquisición, preservación y protección, análisis y correlación de la evidencia, atribución del ataque y la presentación de la evidencia, son comunes a través de todos los enfoques, aunque en sí mismas cada una de estas etapas no posee un proceso estándar sino que, más bien, varía según la necesidad.
- Se concluye que cada una de estas etapas antes presentadas, exteriorizan diferentes retos que los investigadores deben enfrentar.
- Frente a la evidencia recopilada, se puede concluir que una de las principales actividades dentro del análisis forense es definir las herramientas por utilizar, aspecto fundamental para definir si la

metodología seleccionada es de relevancia en un campo tan poco estandarizado y tan cambiante.

- Como consecuencia de la investigación, se encontró que la organización de la información obtenida durante un proceso forense es un proceso aún en desarrollo, sobre el cual aún no se encuentran marcos específicos que apliquen para cada dispositivo IoT. Porque más bien existen marcos generales que deben ser adaptados a la necesidad de la investigación. Esto principalmente a consecuencia de la diversidad que existen en modelos y dispositivos IoT.
- En esta investigación, unos de los objetivos era reconocer la relevancia de las evidencias digitales que se obtienen del proceso del análisis forense digital en las investigaciones criminales, en las cuales no se encontraron casos donde las evidencias forenses extraídas de dispositivos IoT fueran concluyentes en un juicio, sino que más bien se encontraron problemas y retos a los que se enfrentan los investigadores al validar la información y que, finalmente, los procesos actuales no son compatibles en su mayoría con lo que se llama “ciencia buena” o “bien ciencia” aceptada por un tribunal.
- Finalmente, y sobre la base de las conclusiones anteriores, la respuesta a la pregunta de investigación es que no se encontró evidencia de que el rol de la ciencia forense digital de dispositivos IoT haya sido determinante, hasta ahora, en las investigaciones criminales.

5.2 Recomendaciones

- Se recomienda investigar más sobre formas de estandarizar el proceso de ciencia forense digital de dispositivos IoT para aumentar su relevancia y determinación en investigaciones criminales porque, como se mencionó en apartados anteriores, es un campo que presenta un crecimiento exponencial.
- Se recomienda a los investigadores elegir las metodologías y herramientas que mejor se adapten a las necesidades de cada proceso, de modo que les permitan fundamentar mejor sus procesos ante un tribunal.

Referencias

1. Áine MacDermott, Thar Baker, Paul Buck, Farkhund Iqbal and Qi Shi. The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics. International Journal of Digital Crime and Forensics. 2020 Mar;13(1):13.

2. Hernández-Castro J, Avoine G, editors. Security of ubiquitous computing systems: Selected topics. 1st ed. Cham, Switzerland: Springer International Publishing; 2019.

3. Qatawneh, Mohammad & Almobaideen, Wesam & Alkhanafseh, Mohammed & al Qatawneh, Ibrahim & Al,. (2019). DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS. 24.

4. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Commun Surv Tutor. 2020;22(2):1191–221.

5. Collie, Jan and Overill, Richard E. (2020). DEEP: Extending the Digital Forensics Process Model for Criminal Investigations. Athens Journal of Sciences, 7(4) pp. 225–240

6. Bouchaud, François & Grimaud, Gilles & Vantroys, Thomas. (2018). IoT Forensic: identification and classification of evidence in criminal investigations. ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security. 1-9. 10.1145/3230833.3233257.

7. Quick, D., & Choo, K.-K. R. (2018). Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. Future Generation Computer Systems, 78, 558–567. doi:10.1016/j.future.2016.12.0

8. Yaqoob, Ibrar & Hashem, Ibrahim & Ahmed, Arif & Kazmi, S.M. & Hong, Choong Seon. (2018). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems. 10.1016/j.future.2018.09.058.

9. Arshad, Humaira & Jantan, Aman & Abiodun, Oludare. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems. 14. 346 ~ 376. 10.3745/JIPS.03.0095.