# Internet of Things Forensics: Challenges and Approaches (Internet de las Cosas Forenses: Desafíos y Enfoques)

**Abstracto:**

El alcance de este documento es doble: en primer lugar, propone la aplicación de un enfoque de Zonas 1-2-3 a las investigaciones forenses digitales (DF) relacionadas con Internet de las cosas (IoT). En segundo lugar, presenta un modelo de triaje de la siguiente mejor opción (NBT) para usar junto con el enfoque de las zonas 1-2-3 cuando sea necesario y viceversa. Estos dos 'enfoques' son esenciales para el proceso de DF desde una perspectiva de IoT: la naturaleza atípica de las fuentes de evidencia de IoT (es decir, Objetos de interés forense - OOFI), la omnipresencia del entorno de IoT y sus otros atributos únicos, y la combinación de estos atributos dictan la necesidad de un enfoque sistemático del DF a los incidentes. Los dos enfoques propuestos están diseñados para servir como un faro para los respondedores de incidentes, aumentar la eficiencia y efectividad de sus investigaciones relacionadas con IoT maximizando el uso del tiempo disponible y asegurando la identificación y adquisición de evidencia relevante. Los enfoques también se pueden aplicar junto con los modelos, metodologías y marcos de trabajo existentes y reconocidos.

**Publicado en:**[IX Conferencia Internacional de IEEE sobre Computación Colaborativa: Redes, Aplicaciones y Compartir Trabajo](https://ieeexplore.ieee.org/xpl/conhome/6675896/proceeding)

**Fecha de la conferencia:** 20-23 de octubre de 2013

**Fecha de adición a IEEE *Xplore* :** 12 de diciembre de 2013

**ISBN electrónico:**978-1-936968-92-3

**Número de acceso de INSPEC:** 13970691

**DOI:**[10.4108 / icst.collaboratecom.2013.254159](https://doi.org/10.4108/icst.collaboratecom.2013.254159)

**Editorial:**IEEE

**Lugar de la conferencia:** Austin, TX, EE. UU.

**SECCIÓN I.**

## **Introducción**

En el dominio de Internet de las cosas (loT), los objetos como los monitores para bebés, los automóviles y las tabletas están equipados con la capacidad de comunicarse entre sí, lo que proporciona una mayor eficiencia para quienes los poseen o los usan. Los objetos que no son en sí mismos inteligentes se están integrando con capacidades de inteligencia y comunicación mediante el uso de tecnologías como la identificación por radiofrecuencia (RFID), sensores y otras formas de computación integrada [1]. La comunicación con dichos objetos se realizará i) directamente, ii) utilizando métodos remotos, por ejemplo a través de Internet o iii) a través del control 'aprendido' u otros dispositivos inteligentes. En el loT, las cosas (también conocidas como spimes o blogjects) están destinadas a ser inteligentes, autónomas y estarán en red en forma de redes de área 'X', por ejemplo, redes de área personal (PAN), redes de área doméstica (HAN) y metropolitana. Redes de área (MAN). Estas tecnologías dispares dentro de loT se están interconectando en redes que son híbridas y evolucionan (es decir, cambian su estructura). Por ejemplo, la X-box de un usuario que es parte de su HAN puede convertirse en parte de la HAN de un vecino cuando es prestada por un amigo. Esta interconexión entre tecnologías y dispositivos inteligentes y dispares ya ofrece varios beneficios y aplicaciones útiles para los usuarios finales, la industria,[2] , [3] . Los beneficios de ingresos estimados de Cisco que ofrecerá loT es de $ 14.4 billones entre 2013 y 2022 [4] .

Sin embargo, varios problemas de seguridad, amenazas y ataques en relación con loT ya se han identificado y estos incluyen vigilancia, virus y ataques de denegación de servicio (DoS) [5] , [6] . Incluso se ha debatido sobre la posibilidad de botnets disruptivas a gran escala [7] dentro de las redes basadas en 10T. La necesidad de una metodología forense para la investigación de delitos relacionados con loT es, por lo tanto, pertinente. LoT plantea algunos desafíos para los investigadores forenses, incluida la difusión ampliada de datos e información, el desenfoque de las líneas entre redes y la (expectativa de) privacidad por parte de los usuarios con redes personales que se desvanecen cada vez más en redes no personales y redes privadas en redes públicas. .

Actualmente, el enfoque en el dominio loT se centra en sus beneficios y aplicaciones, así como en los problemas de seguridad y privacidad que se aplican. Apenas existe una metodología de respuesta a incidentes dedicada para los respondedores forenses digitales (DF) dentro del dominio loT. Esta brecha es lo que este documento pretende llenar: proponer una estrategia de respuesta a incidentes de alto nivel para abordar escenarios de crímenes basados ​​en LD

El documento está estructurado de la siguiente manera: la Sección II revisa el trabajo previo en el área de DF; La Sección III presenta un escenario hipotético de delitos de IoT e intenta identificar fuentes de evidencia dentro de él; La Sección IV discute la unicidad de IoT con respecto a Digital Forensics (DF); La Sección V discute el análisis forense en el Internet de las Cosas e introduce las Zonas 1–2-3 y el requisito de un Modelo de Análisis Forense Digital Next Next Thing (NBT). Finalmente, la Sección VI discute la investigación futura y concluye el documento.

**SECCION II.**

## **Trabajo previo**

Varias áreas principales conforman el IoT. Estas áreas incluyen la nube, la virtualización, los dispositivos móviles, la informática fija, las tecnologías de sensores y RFID, y la inteligencia artificial. Por lo tanto, el análisis forense en IoT abarcará el análisis forense en todas estas áreas y más. Esta sección presenta la situación actual dentro del paisaje del DF.

### A. Forense digital: simple y llanamente

El análisis forense digital es un campo que se ocupa de la investigación de delitos relacionados con la tecnología. Estos crímenes cubren a los perpetrados contra, utilizando o perpetrados mediante la tecnología. Con el IoT, una adición clave serían los delitos perpetrados y originados únicamente por la tecnología.

Las investigaciones del DF son realizadas por investigadores capacitados, experimentados y calificados que utilizan herramientas de código abierto y / o patentadas (por ejemplo, el entorno de investigación asistido por computadora CAIN.E. Y Encase) para llevar a cabo tareas como la adquisición y el análisis de evidencia digital relevante. Emplean metodologías ampliamente aceptadas para garantizar que toda la evidencia obtenida durante estas investigaciones sea aceptable en un tribunal de justicia. Entre las metodologías existentes se encuentran el Proceso de Investigación Forense Informática de 4 etapas y el Modelo Extendido de Investigación de Cibercrimen (EMCI) de 13 etapas [8]. Todas las metodologías tienen la fórmula básica subyacente de preparación, investigación, análisis / examen, informes / presentación /, almacenamiento (y evidencia en algunos casos). Además de estas metodologías, las directrices, como las directrices de la Asociación de Oficiales de Policía (ACPO) [9] y los Estándares y Principios del Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE) / Organización Internacional de Evidencia Digital (lODE) [10]son ampliamente reconocidos y aplicados adecuadamente por los respondedores del DF durante las investigaciones. Estas metodologías y directrices seguirán siendo útiles en el dominio de IoT porque, aunque las escenas de crímenes de IoT pueden diferir de los crímenes digitales tradicionales en su mayor alcance, las investigaciones seguirán, en cierta medida, relacionadas con crímenes digitales y, por lo tanto, requerirán similares (y posiblemente incluso enfoques híbridos [11] ).

En escenarios típicos de DF, los dispositivos de hardware de enfoque incluyen computadoras personales (PC), impresoras y, más recientemente, dispositivos móviles como teléfonos celulares, tabletas y lectores electrónicos. Los puntos focales de computación flexible incluyen sitios web y aplicaciones de software. Todos estos seguirán siendo puntos de interés y fuentes de evidencia durante las investigaciones relacionadas con IoT. En el IoT, el panorama de la evidencia, en lugar de cambiar por completo, se ampliará en términos de la cantidad y el tipo de dispositivos de interés, su ubicación, la cantidad de información que llevarán y su interacción con otros dispositivos. Los investigadores del DF deberán tener en cuenta el movimiento de personas, con su IoTware entre redes (en este documento, las cosas, dispositivos y / u objetos que componen el IoT también se denominan con el término genérico 'IoTware', pronunciado yotware) . Estos factores contribuirán a la mayor complejidad de las situaciones a las que se enfrentarán los respondedores de incidentes a las investigaciones de IoT y, por lo tanto, requerirán enfoques de investigación altamente eficientes y efectivos que complementen los modelos, metodologías y marcos forenses ya probados y probados. Este documento reconoce que por razones destacadas enEn la sección III , el IoT introduce dimensiones únicas para el DF y que estas diferencias requerirán un enfoque único para el análisis forense en el IoT y los sistemas inteligentes relacionados.

### B. Forense en la nube

El análisis forense en la nube desempeñará un papel clave en la esfera del análisis forense de IoT, especialmente porque los datos generados por IoTware y las redes de IoT ya se encuentran, o se almacenarán cada vez más, en ubicaciones en la nube. Esto se debe a que las soluciones en la nube ofrecen varios beneficios que incluyen conveniencia, gran capacidad, escalabilidad y accesibilidad bajo demanda. Sin embargo, los ataques como la inyección de lenguaje de consulta estructurado (SQL), el canal lateral, la autenticación, los ataques de intermediarios y la eliminación insegura de máquinas virtuales, etc., que se descubren y explotan en varios delitos relacionados con la nube han llevado a una necesidad para forense digital en el entorno de la nube. El análisis forense de la nube se dificulta por la ausencia de acuerdos entre las partes en la nube que pueden permitir investigaciones dentro y entre los servicios basados ​​en la nube del cliente. Adicionalmente,[12] . Estas amenazas y desafíos para los entornos de nube inevitablemente también se aplicarán a las investigaciones forenses basadas en IoT.

La siguiente sección presenta el escenario hipotético del crimen que proporcionará el telón de fondo para la discusión sobre cómo se podrían abordar las investigaciones relacionadas con IoT.

**SECCION III.**

## **Escenario hipotético**

Para responder la pregunta planteada por el título de este documento y resaltar las preguntas que los investigadores del DF pueden tener que responder en situaciones de delitos relacionados con IoT, un delito hipotético llevado a cabo por un Sr. X que utilizó varios IoTware para cometer delitos es descrito.

### Escenario hipotético

El Sr. X trabaja para 'Smart Kids' en la escuela primaria local como técnico de TI. Su red de área personal (PAN) está compuesta por su teléfono móvil y una tableta. Utiliza servicios gratuitos de almacenamiento en la nube proporcionados por Microsoft Sky y Amazon Cloud para almacenar archivos que ha adquirido ilegalmente. Su trabajo principal es el espionaje corporativo y el chantaje. Trabaja fuera de casa y siempre está en movimiento, accediendo a Internet aprovechando las redes abiertas disponibles que puede encontrar. Sus dispositivos personales no están registrados con ningún proveedor de servicios móviles o de Internet. Los compró de segunda mano y pagó en efectivo por un señuelo. Él usa su teléfono para hacer y recibir llamadas y mensajes solamente.

La red de área doméstica (HAN) de la Sra. Smart está compuesta por su computadora portátil, la consola de juegos X-box de su hijo, su sistema inteligente de iluminación y calefacción doméstica, su automóvil y un dispensador de medicamentos inteligente. La Sra. Smart es la maestra principal de 'Smart Kids'.

El hospital local, 'Healing Hands' ha lanzado un sistema en el que todos los dispositivos electrónicos y sistemas relacionados con el paciente se han conectado en red. Esto se hizo para mejorar la eficiencia, reducir el error humano y ahorrar tiempo. Los gabinetes de dispensación de medicamentos 'inteligentes' del hospital y los registros de pacientes también están conectados a este sistema con diferentes niveles de derechos de acceso asignados a diferentes servicios y recursos en el hospital. Los médicos en el hospital interactúan con los pacientes de forma remota, aconsejando y recomendando cambios en las dosis sin el requisito de que los pacientes ingresen a los hospitales.

Por último, 'Smart Kids' también ha lanzado un sistema en el que todas las computadoras están conectadas en red. Todas las rutas de entrada y salida (puertas, portones y ventanas) están centralmente controladas por computadora. Además, la escuela tiene un sistema central en la nube donde los estudiantes pueden almacenar archivos y recuperarlos, y los resultados de los estudiantes están disponibles en línea y se puede acceder de forma local o remota para que los estudiantes puedan ver sus resultados desde la comodidad de su propio hogar.

El Sr. X fue despedido recientemente por 'Smart Kids' por reclamos de que manipuló sus servicios de seguridad informática. Siente que fue despedido injustamente por probar en el trabajo las habilidades que adquirió en un taller de seguridad. Como resultado, el Sr. X no está contento con su antiguo empleador.

### El ataque

El Sr. X usa sus dispositivos móviles para acceder a los registros del hospital y llevar a cabo los siguientes ataques:

* Comienza por manipular los medicamentos de la Sra. Smart, que debe recoger más tarde ese día. Él obtiene el control de la cuenta de correo electrónico del hospital de su médico de cabecera y, desde allí, le envía un correo electrónico informándole que la receta renovada se ha reducido porque su salud ha mejorado. Por lo tanto, su dispensador de medicina inteligente solo dispensará la dosis reducida. La Sra. Smart está desconcertada porque no ha notado ni reportado ninguna mejora en su salud a su médico de cabecera.
* Él accede al sistema de navegación automático en su automóvil y lo configura para que seleccione la ruta más larga a cualquier destino seleccionado.
* Usando un exploit de puerta trasera que instaló mientras trabajaba en 'Smart Kids', el Sr. X accede a los registros escolares de su hijo y baja sus calificaciones. Luego presenta una queja a la policía local sobre la discriminación contra su hijo debido a su propia reputación con la escuela.
* Él llena el espacio de almacenamiento de 64 Gb de su hijo en su Xbox con imágenes indecentes de personas que ni ella ni su hijo conocen.
* Al escalar sus privilegios en la red de su hogar, manipula el sistema de iluminación inteligente en la casa de la Sra. Smart. El sistema se programó originalmente para encender sus luces en función de los movimientos de una habitación a otra. El Sr. X modifica la configuración para que las luces se apaguen cada vez que la Sra. Smart y / o su hijo entren en una habitación y se enciendan cuando se vayan. La Sra. Smart está preocupada porque esto significa que las luces permanecen encendidas todo el tiempo que están lejos de la casa.

Como resultado de estos ataques, la escuela 'Smart Kids' solicita una investigación sobre el problema con sus sistemas informáticos. El hospital también ordena una investigación para determinar por qué ciertos registros del hospital parecen haber sido alterados. La Sra. Smart está preocupada por el aumento de sus facturas de electricidad en el hogar. Tampoco le agrada que su automóvil haya elegido constantemente las rutas más largas a varios destinos en los últimos días, lo que la hace llegar tarde. Extravió el manual del automóvil y no sabe cómo anular la configuración automática de su automóvil. La Sra. Smart llama a las compañías que proporcionaron e instalaron los diferentes servicios para investigar las situaciones. También invita a una compañía forense para asegurarse de que no haya sido atacada,

La siguiente sección propone algunas preguntas que serán pertinentes en los escenarios anteriores.

### A. Algunas preguntas que los investigadores que son llamados para investigar estos escenarios podrían elegir hacer

#### 1) Preguntas al hospital y a la escuela.

* ¿Quién tiene acceso a qué registros?
* ¿Cómo se suele acceder a estos registros de forma local y remota?
* ¿Cuáles son los niveles de permiso y se han violado en el pasado? ¿Qué tan fácil es violar estos, es decir, hay algún resultado de las pruebas de penetración que se han llevado a cabo?
* ¿Hay registros guardados por el hospital y la escuela sobre quién accedió a qué y cuándo?
* ¿Hay alguna cámara de seguridad alrededor de la escuela que pueda mostrar a las personas merodeando con computadoras portátiles u otros dispositivos móviles que se pueden usar para acceder a la red de la escuela?

#### 2) Preguntas al diseñador del sistema de iluminación inteligente

* Is there any recourse from the Smart lighting system designer for the issues she has been experiencing?
* Does the designer have any system in place that might assist with forensic investigations?

#### 3) Questions to the Smart lighting system vendor

* Is there any recourse for the issues your customer has been experiencing?
* Do you have any incident response system in place to investigate such issues?

#### 4) Questions to Mrs. Smart and her son

* How is the lighting system controlled-locally or remotely? Does she have a strong password setup? Has she shared the password with anyone else or used the same password for other services?
* Do you have a firewall, intrusion detection/intrusion protection system and other such perimeter security services set up?

It is clear from the above questions that DF in the IoT will have to work closely with law enforcement and end users especially in domestic (non-commercial) cases. For instance, in the scenario presented, access will be required to Mrs. Smart's son's X-box game online records which may reveal his gaming habits etc. and this might be a cause for concern for him. Also, giving investigators access to hospital records may be a cause for concern for patients of the ‘Healing Hands’ hospital. Therefore a clear definition of permissions, access rights and access methods must be agreed during the preparation stage (section V.C.1)) of any investigation.

#### B. One possible approach to the problem

Los investigadores del DF pueden optar por configurar el monitoreo y monitorear física y lógicamente la red de comunicación HAN de la Sra. Smart, aunque puede haber alguna dificultad para obtener evidencia si los dispositivos en su red se comunican usando un protocolo de comunicación patentado. En ese caso, las herramientas especializadas deben diseñarse para capturar y analizar la información capturada.

Evidencia de interés en este escenario.

* Registros: registros de acceso al hospital a los registros de la Sra. Smart y a los dispositivos y la cuenta de su médico.
* Acceda a los registros de la consola de juegos de su hijo
* Acceda a los registros de su automóvil y posiblemente a la caja negra del automóvil.
* Sistema de iluminación inteligente de registros.
* Registros de todos los dispositivos periféricos en su hogar, por ejemplo, firewall, sistema de detección de intrusiones de red y host (NIDS y HIDS), etc.

Si bien es importante prepararse adecuadamente para una investigación en el dominio de IoT, es importante evitar un enfoque de 'Gran Hermano' para el análisis forense proactivo. Por ejemplo, imagine una situación en la que los investigadores del DF logran rastrear una camisa a un usuario en función de la información transmitida por la etiqueta RFID en la camisa; se debe desalentar el seguimiento de esa persona en una localidad si no hay un respaldo legal previamente acordado para este tipo de actividad. Tener la facilidad para lograr el objetivo no debe interpretarse como el derecho a hacerlo; establecer estos límites desalentará el desarrollo de posibles situaciones de cazarrecompensas del Salvaje Oeste.

En este escenario, un humano era el perpetrador. En otros casos, un 'error' de software puede causar que algo inteligente desencadene involuntariamente una cadena de eventos, como dispensar la cantidad incorrecta de medicamentos en un sistema hospitalario que utiliza botiquines inteligentes. Esto también puede ser activado por un dispositivo inteligente mal entrenado. Por ejemplo, una enfermera robot mal entrenada que debe ir a los barrios limpiando los platos de los pacientes después de que hayan terminado sus comidas puede adoptar un estándar deficiente y, por ejemplo, retrasarse con el horario habitual. Estos ejemplos resaltan el requisito de supervisión humana en tales sistemas.

**SECCION IV.**

## **Singularidad del IOT desde una perspectiva forense digital**

Hay una serie de factores que deben considerarse cuando se aborda una escena del crimen relacionada con IoT. Uno de esos factores es el tipo de evidencia de hardware involucrada. El IoT está previsto como un sistema que implicará la comunicación entre una amplia variedad de objetos desde dispositivos que ya se comunican (PC en red, teléfonos móviles, etc.) a dispositivos que podrán comunicarse (electrodomésticos y órganos internos humanos). Esto introduce una dimensión a la discusión del DF en términos de los elementos que son incautados o acordonados para investigación; por ejemplo, se puede acordonar un hogar completo durante una investigación para que los dispositivos que se encuentran en ellos (por ejemplo, hervidores de agua) no se enciendan / apaguen, lo que garantiza que no se modifiquen los valores de entrada creada de acceso modificado (MACE).

### A. Forense digital tradicional versus IoT

El IoT está diseñado como una red de sistemas inteligentes, de toma de decisiones y de autogestión. El impacto de esto en el análisis forense es interesante porque, desde el punto de vista de la cantidad de dispositivos, la responsabilidad de los delitos cometidos por cosas inteligentes en el IoT, entre otros. Esta sección presenta las dimensiones que IoT presentará al DF. El IoT presenta una serie de dimensiones que afectarán las prácticas habituales del DF en la perspectiva del DF que hacen que esta discusión sea esencial. Estas áreas se discuten a continuación. Se podría esperar que los forenses en el IoT difieran de los forenses tradicionales en las siguientes formas.

La Tabla I destaca las áreas que serán de interés en el IoT además de las áreas bajo el DF tradicional. Ahora se presenta una discusión sobre estas diferencias.

**TABLA I.** Análisis forense de IoT y análisis forense tradicional comparados

|  | **IoT y forense tradicional comparados** | |
| --- | --- | --- |
| ***Forense tradicional*** | ***IoT forense*** |
| Fuentes de evidencia | PC, nube, virtualización, dispositivos de comunicación móvil, clientes web, redes sociales, servidores de autenticación y autorización (AAA), puertas de enlace, por ejemplo, servidores proxy. | Electrodomésticos, automóviles, etiquetas, lectores, nodos de sensores de sistemas integrados, redes de sensores, implantes médicos en humanos y animales, otros IoTware. |
| Jurisdicción | Individuo, redes sociales, sociedad, empresa, gobierno | Mismo |
| Número de dispositivos | Miles de millones de dispositivos | 50 mil millones para 2020 a billones de dispositivos |
| Tipos de evidencia | Documentos electrónicos, formatos de archivo estándar. JPEG, MP3, etc. | Cualquiera y todos los formatos posibles. |
| Tipos de redes | Alámbrico, Wi-Fi, redes inalámbricas bluetooth, internet, comunicaciones móviles, | RFID, redes de sensores, p. Ej. Sensor al lector y viceversa. |
| Cantidad y tipo de datos y evidencia | Hasta terabytes de datos. | Hasta exabytes de datos. |
| Protocolos | Ethernet, inalámbrico (802.11 a, b, g, n), bluetooth, IPv4 e IPv6 | RFID, Rime [14] . |
| Qué aprovechar | Aproveche los dispositivos según sea necesario | Identifique posibles siguientes mejores cosas para la fuente de evidencia (ver sección VC .3) a.) |
| Propiedad | Individuos, grupos, empresas, gobiernos, etc. | Mismo |
| Límites de la red | Límites y líneas de propiedad claramente definidos | Líneas de límite cada vez más borrosas |

#### 1) Fuentes de evidencia, es decir, tipos de dispositivos

Se puede esperar que la recopilación de evidencia en una escena del crimen basada en IoT se centre en varias fuentes de evidencia. Estos pueden incluir los sistemas informáticos típicos, es decir, computadoras personales de escritorio, teléfonos móviles. Con el IoT, cosas como los electrodomésticos pueden convertirse en temas de interés forense; lavavajillas, planchas y monitores para bebés. Esta disparidad de tipos de dispositivos presentará desafíos interesantes para las investigaciones a nivel de dispositivo.

#### 2) El número de dispositivos

The proliferation of interconnected and interconnection technologies is evident all around us e.g. Fleisch talks about trillions of interconnected “nerve endings” (or devices) in the IoT [13]. This is not the same scale in terms of number of devices that traditional DF has typically dealt with. With DF the focus started with a few devices, typically a desktop computer; then widened to devices on the desk and other items of interest such as USB drives, external hard drives and mobile computing devices e.g. tablets and e-book readers. This is because there might be information on the devices that may prove crucial in DF investigations.

#### 3) The quantity and type of data

Within the IoT we expect to see an explosion of data because of the increased number of interconnected devices that will be communicating and exchanging information across the loT information highway. This data explosion has been discussed in [15] in which the authors anticipate a “data deluge” within the IoT domain. Gantz and Reinsel point out in their IDC (International Data Corporation) report that the expected growth of data that will be experienced from 2005 to 2020 will be 40,000 exabytes (where an exabyte is a trillion gigabytes) [16]. Within the IoT landscape, data sources in the IoT may increasingly include IoTware such as baby monitors and milk bottles all transmitting data and information and all contributing to the increase in data generated on a regular basis. This data deluge has implications for DF investigations with respect to the amount of time to be spent sifting through the increased volume of data. In addition, the format of the data retrieved from some IoTware may be different from what is typically encountered during traditional DF investigations and this data would have to be unraveled by investigators and placed into an understandable and usable format. There is already a push towards triage and automated forensics as methods of solving DF crimes and these two methods will almost certainly find increased use within the IoT crime domain. Automated forensics for instance is being promoted because when correctly applied it can lead to overall savings in time and money compared to the situation with traditional manual forensics methods. Triage and automation would be even more pertinent for handling DF tasks within the IoT domain.

#### 4) The location of evidence

The storage of user data in multiple locations which may have multiple jurisdictions is already recognised issue for forensics examiners due to the locations and possible differences in laws that apply in these different locations. This issue will be mirrored in the IoT due to the use that the cloud will continue to see for the storage of IoT-generated data.

Increased juridical complexities as devices travel between networks and cross various barriers. With the IoT (in addition to the existing complexity of deciding which rules under which to prosecute cases where devices have been used between different countries) is the added dimension of devices being used between people's private, personal and public networks.

#### 5) (Increasingly) blurring lines between networks

Con el DF tradicional, por ejemplo, investigaciones basadas en computadoras y redes, las líneas de límite generalmente están claramente definidas: la cantidad de dispositivos que se incautarán, la cantidad de personas involucradas en las comunicaciones, etc. Sin embargo, con el IoT, las redes se mezclan entre sí con las Redes de área corporal (BAN) que se mueven entre las WAN a medida que las personas viajan desde, por ejemplo, sus hogares a sus lugares de trabajo. Una ramificación para DF será cómo manejar el desarrollo de métodos eficientes para recopilar toda la evidencia relevante de un Objeto de Interés Forense (OOFI) que ha viajado entre múltiples redes, dejando múltiples huellas digitales a su paso. Por el contrario, esta situación puede tener algún beneficio para el DF, ya que puede facilitar la trazabilidad del OOFI.

DF se enfrentará a problemas de privacidad, ya que OOFI se ubicará en áreas como hospitales donde se recopilan datos personales como los datos de los pacientes. Por lo tanto, obtener el tipo correcto de permiso para confiscar e investigar esto deberá ser un tema de discusión a medida que se desarrolla el IoT. Por ejemplo: si el OOFI está en una BAN interna, ¿cuál será el enfoque recomendado para los profesionales del DF? Este es un panorama complicado que requiere una mayor exploración y el enfoque NBT descrito en este documento es una contribución a esta discusión.

### B. Evidencia relevante: una discusión basada en escenarios

En el escenario de IoT (o Internet futuro), será importante discutir el significado de la evidencia relevante y posiblemente incluso clasificar la evidencia por grado de relevancia o importancia. Los que responden a un incidente tendrán que lidiar con preguntas como qué y dónde se encuentran las pruebas en una escena del crimen de IoT. Las áreas o posibles puntos de ataque dentro de un IoT en el hogar son numerosas y será útil para el DF como un campo para resaltar las áreas / grupos / categorías principales donde la evidencia relevante puede estar disponible en un hogar IoT. La Tabla II destaca las posibles fuentes de evidencia en una situación de delito de IoT. Es posible que los respondedores tengan que completar una tabla como esta durante cada respuesta a un incidente.

**CUADRO II.**Posibles fuentes de evidencia en un escenario de IoT

|  | ***Fuentes*** | ***Ejemplos*** | ***Evidencia esperada*** |
| --- | --- | --- | --- |
| Interna a la red | Nodos finales de hardware | IoTware, por ejemplo, consolas de juegos, refrigeradores, dispositivos móviles, medidores inteligentes, etiquetas, lectores, sistemas integrados, controlador de calor Nest | Datos del sensor, por ejemplo, dirección IP, número de tiempo, ID del sensor, etc. |
| Red | Alámbrico e inalámbrico, comunicaciones móviles, por ejemplo, GSM, redes de sensores, HIDS, NIDS, HMS | Red, Registros |
| Dispositivos perimetrales | Servidor AAA, firewall, servidor NAT, IDS, NIDS, HIDS. | Registros de redes y sistemas; datos de autenticación, etc. |
| Externo | Nube | Sistemas de nube pública, privada e híbrida. | Máquinas virtuales de cliente; registros |
| Web | Clientes web, servidores web, redes sociales. | Registros web; actividad del usuario |
| Nodos finales de hardware | Dispositivos móviles, nodos sensores y redes, | Datos del sensor, por ejemplo, dirección IP, número de tiempo, ID del sensor, etc. |
| X redes de área | Redes de área local (HAN) | Registros de red |

En el dominio de IoT, se revisarán las preguntas cardinales de las investigaciones forenses digitales. En las investigaciones del DF, las preguntas cardinales típicas son: ¿Qué pasó? ¿Cuando sucedió? ¿Como paso? y ¿Quién lo hizo? En IoT Forensics, las preguntas que los investigadores finalmente responderán serán revisadas para que la cuarta pregunta se convierta en ¿Quién y / o qué hizo? ( Fig. 1 ).

**SECCION V.**

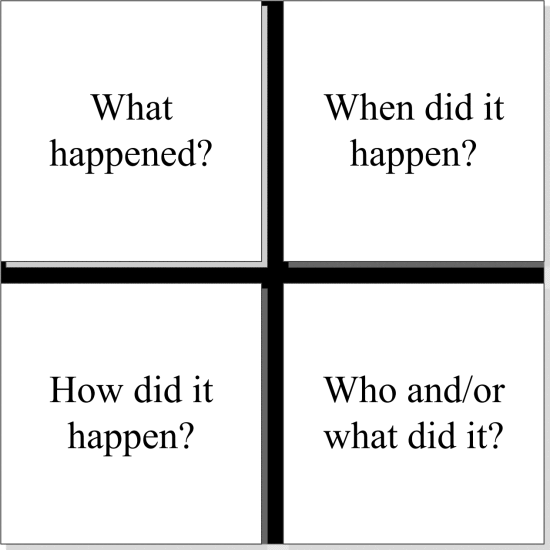
## **Forense en Internet de las cosas**

### A. Puntos de enfoque: las zonas 1–2-3 de forense digital

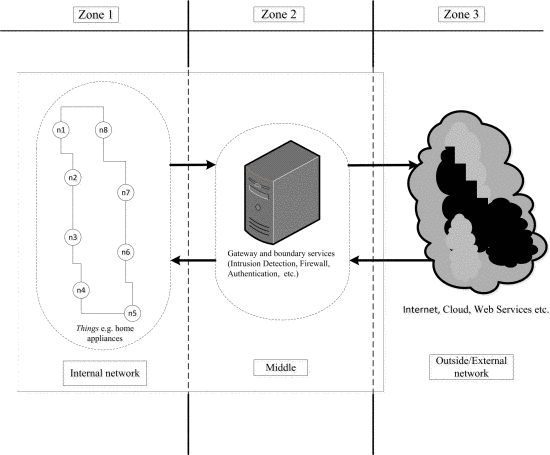
En el IoT DF implicará saber dónde mirar. Sin abordar el análisis forense de IoT de esta manera, se perderá un tiempo valioso buscando en los lugares equivocados pruebas irrelevantes. Este documento propone un método basado en zonas para abordar las investigaciones relacionadas con IoT.

#### Zona 1

Como se puede ver en la Fig. 2 , esta es la zona interna donde se cataloga todo el hardware, software y redes (por ejemplo, Bluetooth y Wi-Fi) que se relacionan con la escena del crimen y se toma una decisión sobre lo que es relevante para el caso y lo que puede contener evidencia que será útil para el caso. El IoTware en estas redes, como los controladores de temperatura inteligentes, puede ser útil incluso aunque solo sea para sus identificaciones de etiqueta (ID de etiqueta) y su estado, es decir, dormido, despierto y activo / transmitiendo, etc.

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6675896/6679958/6680032/6680032-fig-1-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6675896/6679958/6680032/6680032-fig-1-source-large.gif)

**Figura 1:**Las preguntas cardinales revisadas de las investigaciones forenses digitales

[[](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6675896/6679958/6680032/6680032-fig-2-source-large.gif)](https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/6675896/6679958/6680032/6680032-fig-2-source-large.gif)

**Figura 2:**1–2-3 Zonas de análisis forense digital

#### Zona 2

En esta zona residen todos los dispositivos y software que se encuentran en el límite de la red y que proporcionan un medio de comunicación entre las redes internas y externas. Esta zona contiene todos los dispositivos públicos de las redes en cuestión. Las investigaciones forenses generalmente involucrarán identificar estos elementos, catalogarlos y recuperar cualquier evidencia relevante disponible de ellos. Los dispositivos en esta zona pueden incluir sistemas de prevención y detección de intrusiones (IPS e IDS) y firewalls de red.

#### Zona 3

This zone covers all hardware and software that is outside of the network in question. This zone includes evidence from all cloud, social network, Internet Service Provider (ISP) and mobile network providers' data; Internet-and web-based services, object virtual online identities, edge network, internetwork evidence (e.g. 2 neighbour's HANs), device based evidence e.g. logs from RFID tags and readers; gateway or edge devices, etc.

The application of this approach will be at the discretion of DF investigators and can be done in parallel (all Zones investigated at the same time) or a Zone of greatest priority can be identified (this can be based on the description of the reported incidence and the possibly the area of greatest impact) and a decision may be made to focus on this first.

Responding to IoT-related digital attacks using the 1–2-3 Zones described provides DF investigators with a useful method to plan and systematically approach investigations and to effectively identify possible OOFI. This approach reduces the complexity that will be encountered in IoT environments and ensures that investigators can focus on clearly identified areas and objects in preparation for investigations.

### B. The Four (4) phase IoT forensics methodology

In this section, a proposed methodology for the loT is discussed as a way of introducing the Next Best Thing Model.

In the IoT, any forensics solution that fails to take into account the nature of the IoT to continually grow, adapt and mutate may eventually become too structured to be of any use. This is because in the IoT domain the boundaries between BAN, Personal Area Networks, Perimeter Area Networks and Premise Area Networks (PAN), Home Area Networks (HAN) and Hospital Area Networks (HAN), Local Area Networks (LAN), Neighbourhood Area Networks (NAN), Metropolitan Area Networks (MAN) and Wide Area Networks (WAN) will disappear and these networks will bleed into each other as users roam from one into another. Forensics solutions would have to recognise IoTware as they approach and join networks, and recognise when they leave. The identity and precise location of the subject of the investigation has to be established and ascertained over a period of time.

Movement of things from one network to another (Fig. 3) can have implications for forensics because of the challenge of obtaining permission at the perimeters of these disparate networks as well as within the networks.

#### 1) Preparation

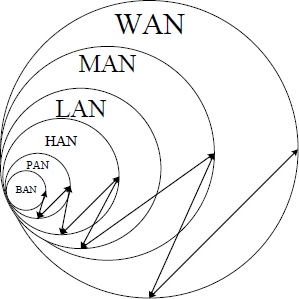
In this phase, the usual preparation steps of DF apply with additional steps. In the IoT preparation will include all security features that are put in place eve before an incident. Such systems may include installation of security tools and software, etc. this phase involves also identifying possible areas of attacks and locations of evidence in the IoT location. This phase also involves identifying the various possible locations of evidence in the crime scene and then making a decision about what is relevant evidence. During the preparations stage phase end users, law enforcement and designers will need to agree on a set of minimal requirements that should be applicable in all IoT domains such as PANs and HANs which will enable easier investigation of IoT-related crimes.

#### 2) Acauisition

Where typical computing devices are involved, the usual method of complete or selective imaging can be used. However, with unusual devices like baby monitors, bespoke methods may have to be developed for retrieving the data they hold especially if the interfaces available (if any at all), are not among the usual types e.g. Universal Serial Bus (USB) or Ethernet.

#### 3) Investigation

En esta fase, se produce la investigación del delito. Esta fase seguirá los pasos típicos recomendados en cualquier escenario forense, incluido el uso de herramientas reconocidas y probadas por la industria, excepto, por supuesto, en situaciones en las que la tecnología ante los investigadores es nueva y se requieren herramientas especializadas, por ejemplo, un refrigerador inteligente con un sensor conectado. En este caso, los métodos de captura y adquisición de datos pueden ser ligeramente diferentes. En esta etapa, y solo para ahorrar tiempo y espacio de almacenamiento (imagine tener que almacenar varios automóviles), se introduce el modelo forense NBT.



**Figura 3:**El movimiento de IoTware entre redes interconectadas presenta desafíos para el análisis forense digital.

#### a) Modelo de triaje Next Best Thing (NBT)

Un aspecto importante de la investigación forense de IoT es la cuestión de saber dónde buscar. Durante las investigaciones de IoT, algunas fuentes de evidencia pueden no estar disponibles después de que se comete un delito; por ejemplo, se puede eliminar un teléfono móvil o se pueden quitar los sensores de una HAN a la HAN de un vecino. El enfoque NBT se puede aplicar para determinar qué dispositivos se conectaron al OOFI y qué fragmentos de evidencia, si acaso, quedan tras su eliminación de la red. Se propone este método forense porque dentro del dominio de IoT no siempre es posible obtener evidencia directamente de fuentes que puedan considerarse pertinentes para una investigación. Con el modelo NBT, se pueden obtener datos probatorios de dispositivos que están directamente conectados o relacionados de alguna manera con el OOFI en caso de que el OOFI no esté disponible. Considere una situación en la que un chupete es el OOFI en una investigación; la mejor fuente de evidencia alternativa sería el enlace de comunicación del hospital con el chupete o el dispositivo de monitoreo móvil o fijo de un consultor, y no el chupete del paciente. En situaciones donde los sensores desplegados para capturar datos han sido alterados, lo que afecta su efectividad, el modelo NBT recomendaría que se capture y analice la evidencia del nodo principal o una estación base.

#### 4) Informes y almacenamiento

En esta etapa, cualquier evidencia recolectada habría sido investigada y analizada a fondo en busca de evidencia relevante. Luego, se prepara un informe y se envía a las partes relevantes. El informe se puede hacer manualmente o puede ser un proceso automatizado utilizando un sistema forense inteligente. En situaciones en las que los propietarios de viviendas se registran en los Centros Forenses Centrales, este informe se les puede enviar para tomar medidas adicionales si es necesario.

### C. Desafíos legales en relación con IoT Forensics

Dentro de la esfera de IoT, los sistemas legales actuales que están vigentes seguirán siendo ampliamente aplicables. Por ejemplo, la Ley de uso indebido de computadoras (CMA) de 1990 será relevante en casos que involucren el control remoto del sistema de iluminación del hogar de una persona. Sin embargo, desde el punto de vista del DF, el derecho de acceso a ciertas áreas puede ser mucho más difícil de obtener. Por ejemplo, si una botnet se hace cargo de dispositivos inteligentes en la cocina de una persona, se deberá establecer un marco legal que permita a los equipos de respuesta a incidentes del DF entrar y buscar dispositivos informáticos tradicionales y no tradicionales como posibles fuentes de evidencia. Sin embargo, si dicho propietario se niega a apagar su refrigerador porque no quiere que su comida se deteriore, y mientras el refrigerador permanezca encendido,

**SECCION VI.**

## **Conclusión**

La siguiente etapa de esta investigación es desarrollar y probar un Marco Forense Digital IoT (IDFF) para su uso en investigaciones relacionadas con IoT. Este marco se probará utilizando un Sistema Forense de Administración de Bordes (FEMS), un dispositivo diseñado para proporcionar servicios forenses automatizados dentro de la construcción de IoT con un enfoque especial en el entorno de IoT Home.

Este documento propuso dos enfoques para el análisis forense digital dentro del dominio de IoT considerando sus características únicas del número y tipos de dispositivos e interconexiones entre redes. Se propusieron las Zonas 1–2-3 de medicina forense para que los respondedores de incidentes puedan trazar su enfoque de las investigaciones y tomar decisiones sobre dónde exactamente deben centrar su atención durante las investigaciones. Se propuso el modelo Next Best Thing Triage (NBT) para abordar las investigaciones de IoT porque dentro del dominio de IoT el acceso directo a Objetos de interés forense (OOFI) puede no siempre ser posible (o apropiado, por ejemplo, chupetes). Por lo tanto, en tales situaciones, la opción de identificar y considerar la siguiente mejor fuente de evidencia relevante puede ser tomada.