Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza
ISSN: 2525-1333
Vol.: 5 - Nro. 1 (AGOSTO-2020)

Comunicación en Congreso

PROYECTO DE CREACIÓN DE UN LABORATORIO DE FORENSIA DE IoT

PROJECT OF CREATION OF A IoT FORENSIC LABORATORY

Esteban RIVETTI[(1)], *Alvaro GAMARRA*[(2)], *H. Beatriz PARRA DE GALLO*[(3)]

[(1)]Instituto de Estudios Interdisciplinarios de Ingeniería (IEsIIng) – Facultad de Ingeniería – UCASAL
erivetti@ucasal.edu.ar

[(2)] Instituto de Estudios Interdisciplinarios de Ingeniería (IEsIIng) – Facultad de Ingeniería – UCASAL
agamarra@ucasal.edu.ar

[(3)] Instituto de Estudios Interdisciplinarios de Ingeniería (IEsIIng) – Facultad de Ingeniería – UCASAL
bgallo@ucasal.edu.ar

Resumen:

La tarea de un experto en informática forense es cada vez más necesaria y de suma importancia en los casos de investigación penal que involucran tecnologías informáticas. Está avanzando a un ritmo muy rápido y hay cada vez más dispositivos tecnológicos que se interconectan entre sí y pueden proporcionar información valiosa. Este es el caso de Internet de las cosas, conocido como IoT. El análisis forense de la evidencia digital en la que participan estos dispositivos requiere la implementación de un laboratorio específico, que tiene todos los componentes de software y hardware necesarios para el análisis forense. Este trabajo describe el proyecto para crear un laboratorio de estas características, que permitirá llevar a cabo

ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

pruebas de vulnerabilidad de la seguridad informática, así como la definición de guías de procedimiento para estos nuevos componentes que constituyen la evidencia digital.

Abstract:

The task of a forensic computer expert is increasingly necessary and of utmost importance in criminal investigation cases involving computer technologies. It is advancing at a very fast pace and there are more and more technological devices that interconnect with each other and can provide valuable information. This is the case of the Internet of Things, known as IoT. The forensic analysis of digital evidence in which these devices are involved requires the implementation of a specific laboratory, which has all the necessary software and hardware components for forensic analysis. This work describes the project to create a laboratory of these characteristics, which will allow vulnerability tests of computer security to be carried out, as well as the definition of procedure guides for these new components that constition the digital evidence.

Palabras Clave: *Forensia Digital, Internet de las Cosas, Laboratorio Forense*

Key Words: *Digital Forensics, Internet of Things, Forensic Laboratory*

Revista Digital del Departamento de
Ingeniería e Investigaciones
Tecnológicas de la Universidad
Nacional de la Matanza
ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

I. INTRODUCCIÓN

Internet de las Cosas, o Internet of Thing (IoT), es un concepto que comenzó a definirse desde el año 2010 [1], este autor ya indicaba la importancia de dos componentes esenciales en los sistemas informáticos: las personas y las "cosas" sobre las cuales se ingresaban innumerables datos en internet, incorporando los sensores como un nuevo componente de la arquitectura de procesamiento informático tradicional.

IoT sumó nuevas tecnologías como RFID (Radio Frequency IDentification), que permite la identificación automática de datos a través de una etiqueta electrónica o tags, mediante una comunicación inalámbrica entre un lector y un emisor. Como ésta, existen otras tecnologías vinculadas a la comunicación de datos que son requeridas por IoT.

Si bien existe abundante bibliografía sobre la arquitectura de procesamiento de IoT, a modo de orden se puede considerar el trabajo de [2] que sintetiza la arquitectura de IoT en siete capas: Dispositivos, Gateways, Red, Nube/Centro de Datos, Aplicaciones, Gestión y Seguridad, las cuales se muestran en la Fig. 1.

Fig. 1 Arquitectura propuesta para IoT por [2]

Desde el punto de vista del análisis forense, interesan dos componentes sustanciales vinculados a una evidencia digital: los procedimientos periciales y el laboratorio de forensia.

Respecto de los procedimientos o normas de trabajo para la realización de forensia de IoT, es mucho lo que se puede explicar, y todo relacionado a la forma en que se adaptan las metodologías existentes para el análisis forense de las distintas capas que integran la arquitectura de IoT. Y si se considera el laboratorio forense, IoT requiere de espacios propios en los que se puedan investigar cada componente vinculado a la evidencia digital.

El objetivo del presente trabajo es definir las características mínimas a las que debería responder un Laboratorio de Forensia de IoT.

Este trabajo se estructura de la siguiente manera: en la sección 1 se describe el marco teórico y estado del arte sobre laboratorios de forensia digital, en la sección 2 se propone y detalla cada uno de los componentes que integran dicho laboratorio, mientras que en la sección 3 se muestran las conclusiones correspondientes.

II. MARCO DE ESTUDIO Y ESTADO DEL ARTE

Actualmente existen trabajos que proporcionan elementos para tomar como base y seguir abordando desde ese punto el armado de un laboratorio pericial específico para IoT, el cual irá cambiando continuamente en todo sentido, tanto desde lo tecnológico como desde el perfil de las personas que integraran el equipo de trabajo de un laboratorio forense de IoT.

El primer documento "Lineamientos para la creación de laboratorios informáticos forenses" [3] en el Poder Judicial de la provincia de Rio Negro, brinda elementos a

ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

tener en cuenta y lineamientos para poder implementar esta propuesta.

Primeramente, los autores proponen un modelo de trabajo que permite definir lineamientos a todo el personal del área basándose en 6 factores: alineamientos a la especialidad, sistematización del proceso forense, separación de roles profesionales, desarrollo de competencias, distribución de la jornada laboral y gestión de conocimiento.

Resalta que la metodología de trabajo es muy importante en un laboratorio forense, la más conocida en esta rama de la informática es la publicada por Estados Unidos en el año 2001, la cual se la resume en 4 etapas para trabajar la evidencia digital: Identificación, Preservación, Análisis y Presentación de los resultados.

Existen otras metodologías de interés, como PURI propuesta por [4], y cada laboratorio podrá adaptarse a una u otra según el tipo de evidencia que deba analizarse.

Es importante que el laboratorio de forensia digital se base en normas, estándares y procedimientos de buenas prácticas desarrolladas por autores reconocidos, para poder aplicarlas en su trabajo como ser ISO/IEC 27037 la cual indica procesos específicos relacionados a tratamiento de evidencia digital. Otras normas a tener en cuenta son las ISO 27041, 27042, 27043 y 27050. Sus objetivos fundamentales son el aseguramiento de la calidad en las herramientas y procedimientos para el análisis forense de la evidencia digital.

En cuanto a las guías de buenas prácticas se pueden resaltar las desarrolladas por instituciones u organismo como las siguientes:

- Las guías de buenas prácticas del departamento de justicia de los Estados Unidos [5], NCJ 199408, la cual desarrolla procedimientos para la adquisición, preservación, análisis y presentación de la evidencia digital a tener en cuenta en el laboratorio pericial informático.
- Otra guía importante es NCJ 219941 la cual especifica todos los dispositivos informáticos que pueden contener evidencia digital.
- Las guías de buenas prácticas de las NIST (National Institute of Standars and Technology) [6], y entre ellas la NIST 7387 “Cell Phone Forensic Tools: An Overview and Analysis Update” que se utilizan para investigaciones en dispositivos móviles.
- Las guías de SWGDE[1] (Scientific Working Group on Digital Evidence) desarrolladas por un grupo de profesionales que hacen investigaciones científicas relacionadas a la evidencia digital, cuentan con una guía denominada “Best Practice for Mobiles Phone Forensics” para el análisis forense de teléfonos celulares.
- También la Guía de Buenas Prácticas de ACPO “ACPO Good Practice Guide for Digital Evidence” [7] la cual detalla procedimientos para el análisis de evidencia digital almacenada en dispositivos informáticos.

Un antecedente importante del equipo autor del presente trabajo, es el denominado “Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense” [8], formulado con el objetivo de estudiar y definir una metodología formal para el desarrollo del análisis forense acorde al proceso judicial propio del Poder Judicial de la Provincia de Salta.

Se identificaron las etapas principales de un proyecto de esta envergadura, en el cual había que armar un

[1] https://www.swgde.org/ [Consultado el 15/09/19]

ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

laboratorio de forensia digital desde cero, considerando el proceso completo, desde la planificación estratégica, la formulación del proyecto, su implementación y evaluación de funcionamiento.

Este plan propone las siguientes etapas:

a) Definición de la Misión y la Visión del Centro de Servicios de Informática Forense;
b) Análisis del Contexto Externo e Interno;
c) Formulación de Estrategias y
d) Plan de acción.

Estos 4 pasos son esenciales para poder iniciar y planificar la implementación de un centro de servicios de informática forense.

La primera etapa propone tener presente la misión que se busca y mantener una visión estratégica permitirá identificar el camino a recorrer para cumplir con la misión.

A esto debe colaborar también el Análisis del Contexto propuesto en la etapa dos, en el que se toman las variables internas y externas que impactan sobre el modelo de laboratorio que se requiere.

En la Formulación de Estrategias –etapa tres-, se requiere trabajar sobre 5 aspectos para conformar un centro de servicios de informática forense:

- Creación de la estructura organizativa que conformará el Centro de Servicios de Informática Forense.
- Generación de acciones de capacitación a fin de preparar al personal que integrará el centro.
- Definición y adquisición de la infraestructura tecnológica para el Laboratorio de Informática Forense
- Desarrollo de procedimientos técnico-legales para el análisis forense
- Plan de Crecimiento

Por último, dentro del Plan de Acción, se describen y proponen las especialidades de la informática forense que se desarrollarán para dar respuesta a necesidades periciales: Seguridad y Soporte Técnico de Servidores, Forensia de Video, Imagen y Voz, Forensia de componentes de hardware de la Tecnología de Información y Forensia de Telecomunicaciones.

Es necesario desarrollar procedimiento técnicos – legales para la recolección de la prueba, la cadena de custodia, el análisis y diagnóstico de la evidencia, y la elaboración del informe técnico de pericia. De esta forma se busca normalizar los procedimientos y guías de buenas prácticas.

Por último, el trabajo recalca que es importante que se tenga una visión multidisciplinar, con asistencia del derecho, las tecnologías y la criminalística para que todos aporten y enriquezcan el modelo que se propone.

El trabajo [9] tal propone una “Guía Técnica para la Implementación de un Laboratorio Judicial” que servirá de mucha ayuda al momento de poner en práctica el presente proyecto, con la opción de incorporar acciones para medir y evaluar la calidad de los procesos periciales, lo que posteriormente permitirá la definición de programas de calidad en este tipo de laboratorios.

Otro trabajo de interés es el denominado “Arquitectura y Organización de Laboratorios de Informática Forense” [10] realizado por investigadores de la Universidad FASTA, está enfocado en la arquitectura y organización del laboratorio.

Concluyen que todo laboratorio de informática forense debe contar con áreas de control, depósito, procesamiento, gestión y servicios y circulaciones.

ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

En el citado trabajo se describe el perfil de las personas que deberían conformar el laboratorio y las funciones que deberían cumplir. Además, propone un organigrama con la jerarquía interna que tendría que tener un laboratorio de este tipo (Fig. 2).

Las especificaciones generales propuestas por [11] para proyectar un laboratorio de características similares al propuesto resultan de interés.

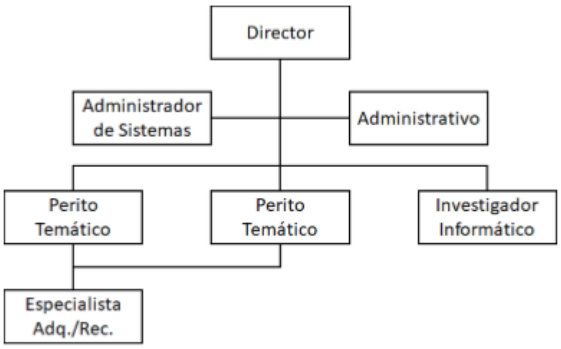

Fig. 2 Organigrama propuesto para un laboratorio de informática forense

Este autor aborda cuestiones relativas a la utilización que se le dará al laboratorio en una institución universitaria, considerando que además de servir a los proyectos de investigación, el laboratorio debería incluirse para la realización de prácticas de las carreras que se imparten en la institución, y en las que se puedan realizar experimentaciones o pruebas en temáticas afines (criminología, seguridad informática, procesos de comunicaciones, etc.). En este trabajo también se hace mención a la necesidad de contar con una infraestructura tecnológica de base, o piso tecnológico, que respete las normas de cableado estructura y de instalaciones eléctricas de rigor.

Los autores citados destacan que todo laboratorio que contenga los espacios aptos y una construcción acorde a sus necesidades, instrumentos, recursos técnicos y condiciones adecuadas el personal, permitirá trabajar de forma adecuada con mayor eficiencia y una mejor motivación, buscando facilitar la selección del personal del laboratorio brindando ciertas características para cada perfil dentro del organigrama propuesto anteriormente.

Se seleccionaron estos documentos por ser los más significativos dentro de nuestro contexto y por qué generaron experiencias concretas, con la implementación de laboratorios de informática forenses en Salta, Mar del Plata y Rio Negro. En otros casos, se consideraron trabajos relacionados a la instalación de laboratorios en instituciones universitarias, en donde además de la actividad forense, es conveniente la utilización del laboratorio en prácticas áulicas.

Creemos que estos documentos nos proporcionan el paso inicial para poder avanzar y enfocarnos en la tecnología que diariamente crece exponencialmente y son un desafío para los peritos informáticos por ser vulnerables y no contar con la seguridad adecuada, como es el caso de Internet de las cosas (IoT).

Considerando estos trabajos, se formula a continuación una propuesta para la creación de un Laboratorio de Forensia de IoT.

III. ESTRUCTURA GENERAL DEL LABORATORIO DE IOT

La misión propuesta para este laboratorio será la de servir de espacio de estudio para el desarrollo de la Forensia de IoT en el ámbito de la institución universitaria propuesta.

El análisis del contexto realizado permitió identificar el ámbito físico en el que se implementará el laboratorio, aprovechando las condiciones edilicias y de gestión

preexistentes para otros laboratorios de la universidad, al cual se integrará el Laboratorio de IoT.

Por otra parte, el personal técnico y de gestión que ya trabaja en los laboratorios existentes, será capacitado para el desarrollo de las tareas que implicarán la Forensia de IoT. El plan de trabajo inicial incluye cuatro actividades centrales:

a) Definición de un escenario delictivo de experimentación,
b) Estudio del funcionamiento, operatividad y vulnerabilidad de los componentes, tanto de manera individual como en su conjunto,
c) Definición de guías de análisis forenses con detalle para cada componente y todo el conjunto y
d) Estudio del contexto jurídico y legal correspondiente al escenario propuesto.

IV. ARQUITECTURA DE PROCESAMIENTO

Considerando las siete capas propuestas por [2], a continuación se describe una propuesta concreta para la infraestructura tecnológica que tendrá el Laboratorio de Forensia de IoT.

A. DISPOSITIVOS

La Capa de Dispositivos es la base de esta arquitectura y tiene a su cargo el nexo con el medio físico de los dispositivos de IoT. Para la arquitectura de nuestro laboratorio se proponen dos alternativas de dispositivos:

- Dispositivos Hogareños
- Dispositivos que se comunican mediante la especificación LoRaWAN[2].

Los primeros son dispositivos conectados entre sí mediante conexiones inalámbricas del tipo 802.11[3] a las que se las conoce normalmente como “WIFI”.

De este grupo, centraremos los estudios en dispositivos para encender y apagar luces y equipamiento eléctrico en general como, por ejemplo: SonOff Itead 4CH Pro R2[4], con el cual los usuarios pueden encender / apagar de forma remota las luces / electrodomésticos conectados mediante la aplicación iOS / Android eWeLink o el control remoto RF de 433MHz.

Respecto del segundo grupo de dispositivos, los que se comunican mediante LoRaWAN, la oferta es más amplia y proponemos el uso de un kit basado en Arduino con sensores de humo, fotoeléctricos, de movimiento, humedad, temperatura, televisores inteligentes, relay, celulares inteligentes y GPS.

Es importante destacar que esta enunciación no es taxativa, y será considerada en base a los dispositivos necesarios para estudiar el escenario de estudio.

B. GATEWAYS

Esta capa la conforman los equipos que realizan la comunicación de los dispositivos de IoT y la capa de Red, pueden ser componentes de hardware o software. Entre los que nos interesan están los siguientes:

- Software Itead provisto con sus dispositivos
- Amazon Echo DOT
- Altavoz inteligente Google Home
- LoRa Gateway LG01

[2] Especificación para redes de baja potencia y área amplia específicamente desarrollada para interconectar dispositivos IoT por LoRa Alliance https://lora-alliance.org/about-lorawan [Consultado el 15/09/19]

[3] Estándar Inalámbrico de la IEEE para el uso de transmisiones de datos en las frecuencias de 2.4 y 5GHZ http://www.ieee802.org/11/

[4] https://www.itead.cc/sonoff-4ch-pro.html [Consultado el 15/09/19]

ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

Es probable que se utilicen teléfonos inteligentes para establecer la comunicación entre los usuarios que actuarán en el escenario de análisis.

C. CAPA DE RED

Esta capa se emplea como interfaz entre los gateways e internet o una intranet. En nuestro caso emplearemos los distintos tipos de acceso a Internet con los que contamos en el espacio de los laboratorios ya existentes en la institución.

D. CAPA DE NUBE/CENTRO DE DATOS

Para el caso de los dispositivos que emplearan como Gateway a Amazon Echo DOT, al Altavoz Inteligente de Google y el software de Itead nos valdremos de la capa de valor agregado propuesta por el fabricante / desarrollador. En el caso de los dispositivos LoRa, la idea inicial es realizar las conexiones entre dispositivos bajo la modalidad punto a punto sin la necesidad de almacenar estos datos de manera centralizada.

F. APLICACIONES

En esta capa es donde ocurre la interpretación de la información. En el modelo de referencia de IoT no se encuentra definida de manera explícita ya que esta íntegramente vinculada al campo donde se realiza la implementación.

Por este motivo es que estos componentes son los últimos que se implementarán, y dependerán del plan de trabajo formulado para la realización de pruebas sobre este tipo de evidencia digital.

Pero es altamente probable que se desarrollen aplicaciones para celulares, siendo éste el contexto de comunicación más habitual en estos momentos.

G. GESTIÓN

El objetivo de esta capa consiste en acercar a los usuarios las herramientas de administración del entorno IoT mediante la interacción con las otras capas del modelo empleado en este trabajo.

Las principales funciones de esta capa son de permitir las actualizaciones de softwares de todos los componentes, gestionar las configuraciones de los mismos, reportar fallos y gestionar el desempeño de la implementación.

Los sensores y equipos propuestos para nuestro laboratorio cuentan con sus propios desarrollos que nos asistirán para resolver cuestiones relacionadas a esta capa por lo que se entiende no se requerirá de software o equipamiento adicional.

Se ha previsto también recurrir a los servicios de soporte técnicos de las marcas, cuando sea posible.

H. SEGURIDAD

En esta capa debemos garantizar confidencialidad, integridad, autenticidad e instantaneidad de los datos e información de la misma manera que lo hacemos en cualquier red de telecomunicaciones.

Se tomará en consideración las políticas de seguridad informática establecidas para los laboratorios de informática de la institución, a las que se agregarán aquellas que se consideren necesarias, en el marco de la realización de análisis forense de componentes de IoT.

Asimismo, la institución cuenta con lineamientos y políticas muy amplias, referidas a la seguridad física, que obviamente habrá que respetar al momento de implementarse el Laboratorio de Forensia de IoT.

En esta capa es donde se centrarán la mayoría de nuestras investigaciones y se partirá de las normas técnicas de rigor, establecidas ya para los distintos componentes.

ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

V. CONCLUSIONES

Hasta aquí hemos definido las principales características que deben considerarse al momento de definir un Laboratorio de Forensia de IoT.

El principal desafío será la discusión acerca del escenario de estudio, en el que sea posible considerar distintas variantes de interés, como para que se puedan estudiar en profundidad la vulnerabilidad de los componentes frente a la seguridad y formular las guías de actuación forense correspondiente.

Los investigadores que conforman el equipo de trabajo provienen sustancialmente des tres áreas: informática, comunicaciones y derecho. Los primeros se abocarán al estudio de los dispositivos, mientas que los segundos analizarán la infraestructura de transmisión de datos y de conectividad, y por su parte, los investigadores del área del derecho les corresponderán abordar el contexto legal y jurídico de la cuestión.

Contar con una infraestructura edilicia y una estructura organizativa en la cual implementar el laboratorio se considerar una fortaleza y una oportunidad, toda vez que hay costos de funcionamiento que ya están amortizados por otros laboratorios existentes en la institución.

VI. REFERENCIAS Y BIBLIOGRAFÍA

[1] K. Asthon, “That ’ Internet of Things ’ Thing,” RFID J., p. 4986, 2010.

[2] D. Benitez, C. Anias, and L. Plasencia, “Propuesta de arquitectura para Internet de las Cosas,” no. October, 2016.

[3] G. Semprini, P. Judicial, and D. R. Negro, “Lineamientos para la creación de laboratorios informáticos forenses,” pp. 7–19, 2016.

[4] A. H. Di Iorio et al., El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense. Mar del Plata: Esitorial UFASTA, 2017.

[5] S. Ó. Ciardhuáin, “An Extended Model of Cybercrime Investigations - A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf,” vol. 3, no. 1, pp. 1–22, 2004.

[6] B. Carrier and E. . Spafford, “Getting Physical with the Investigative Process,” Int. J. Digit. Evid., vol. 2, no. 2, pp. 1–20, 2003.

[7] U. S. D. of Justice, “Electronic crime scene investigation: A guid for first responders,” 2008.

[8] S. D. Appendino, F. Aprile, H. B. P. De Gallo, T. Para, L. A. Realizacion, and D. E. P. Informaticas, “Plan Estratégico para la implementación de un Centro de Servicios de Informática Forense,” in XXI Congreso Argentino de Ciencias de la Computación, IV Workshop de Seguridad Informática (WSI), 2015.

[9] A. H. Di Iorio et al., “Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense Considerations in desgning a Judicial Digital Forensics Laboratory,” REDI - Repos. Digit. la Univ. FASTA, pp. 1–6, 2016.

[10] B. Constanzo et al., “Arquitectura y Organización de Laboratorios de Informática Forense.” https://yardev.net/congreso/memorias/# de General Pueyrredon, M., del Plata, M., & Aires, B. Arquitectura y Organización de Laboratorios de Informática Forense.

[11] B. A. López Maxi and D. I. Varela Porro, Diseño, Especificaciones Técnicas y Seguridad para la Implementación de un Laboratorio de Informática Forense para la Carrera de Ingenieria en Networking y Telecomunicaciones. 2016.

Revista Digital del Departamento de
Ingeniería e Investigaciones
Tecnológicas de la Universidad
Nacional de la Matanza
ISSN: 2525-1333. Vol.: 5 - Nro. 1 (AGOSTO-2020)

Recibido: 2020-07-14

Aprobado: 2020-07-22

Hipervínculo Permanente: http://www.reddi.unlam.edu.ar

Datos de edición: Vol. 5-Nro. 1-Art. 2

Fecha de edición: 2020-08-15