1.- Realización de análisis forenses en Internet of Things (IoT).

Caso práctico

Pixabay (Dominio público)

María recibe una nueva llamada para trabajar en un caso dónde se investiga la actividad de un usuario.

Al llegar a la escena encuentra el portátil y teléfono móvil del sospechoso y sabe que durante el proceso de identificación encuentre nuevas evidencias que podrían no ser evidentes a simple vista pero que podrían aportar información al caso (piensa en el reloj inteligente del sospechoso, el sistema del coche eléctrico que hay en el garaje, o incluso pequeños electrodomésticos)

Sabe que estos dispositivos forman parte del Internet de las Cosas o IoT y que podrían aportar visibilidad sobre la localización del usuario, su actividad, relaciones con terceros, etc...

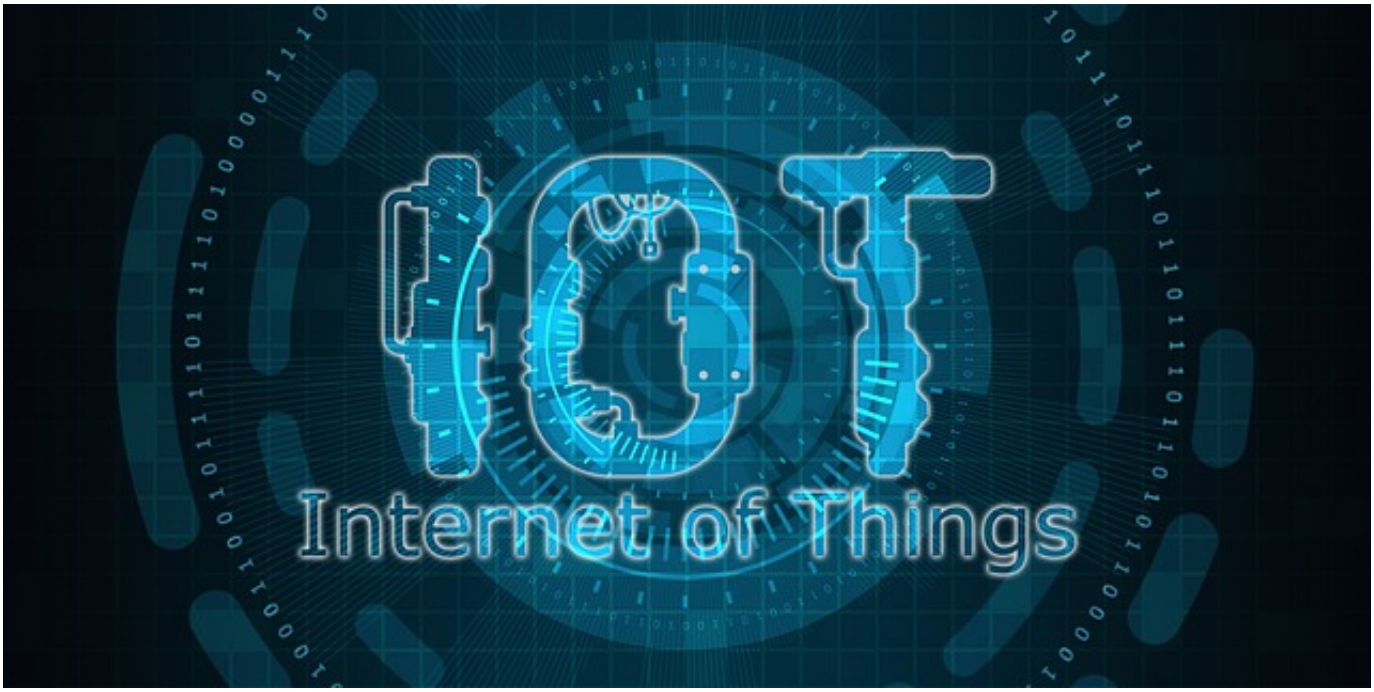
A nivel forense sabe que el escenario se complica desde la primera fase del análisis forense ya que la identificación ya no es tan sencilla y luego viene la adquisición de sistemas que ni si quiera conoce los detalles de como funcionan por dentro.. será un auténtico reto...

IoT trae muchas oportunidades y problemas para el análisis forense. La recopilación de datos forenses de dispositivos con interfaces y capacidades muy limitadas para el almacenamiento y procesamiento de datos es un desafío.

Por otro lado, la agregación de pequeñas piezas de datos de estos dispositivos puede proporcionar una visibilidad sin precedentes desde varias perspectivas. Eso abre un nuevo capítulo en el análisis forense digital.

El predominio futuro de dispositivos IoT proporcionará una gran cantidad de datos relevantes desde el punto de vista forense. Nuestras vidas conectadas digitalmente dejan rastros que podrían conducir a una era dorada de la ciencia forense.

1.1.- Identificar los dispositivos a analizar.



Pixabay (Dominio público)

A día de hoy no hay definida una metodología y un marco para el análisis forense de IoT. El análisis forense de IoT aún está en un estado muy inicial y se basa en metodologías y marcos de análisis forense digital estándar que pueden no ser completamente adecuados viendo la gran diversidad de dispositivos IoT existentes.

La primera fase de la metodología forense es la **Identificación** y es aquí donde encontramos más cambios. Saber si ese reloj inteligente, nevera, televisión ha recogido datos que puedan aportar a la investigación es importante.

Con el análisis forense de IoT, lo primero que debe hacer un analista es identificar las fuentes de evidencia disponibles en la escena del delito. El investigador debe establecer qué dispositivos registraron datos relevantes para la investigación.

La pregunta que debe responderse es:

- ¿Cómo interactúa ese IoT con su entorno?
- ¿Qué tipo de datos recoge?
- ¿Esos datos aportan algún tipo de información relevante para la investigación?

Una vez que el investigador ha podido plantearse o contestar a estas preguntas entonces puede saber si es una evidencia válida. Además, se considera una buen práctica anotar todas las posibles evidencias aunque luego se descarten. Nunca se sabe si podrían ser relevantes.

De todas maneras **el gran reto no es este sino ser capaces de reconocer la**

presentación de todos sistemas IoT y la identificación de los mismos.

Finalmente una amplia gama de dispositivos diferentes dificulta tener un enfoque estandarizado para la recopilación de evidencias.

1.2.- Adquirir, analizar y extraer las evidencias.

Pixabay (Dominio público)

Después de la identificación viene la adquisición y el escenario del forense de IoT vuelve a cambiar, en este caso una vez que tenemos la evidencia identificada el analista deberá plantearse las siguientes cuestiones:

- ¿Tengo alguna limitación para la recolección?
- ¿Qué tipo de sistema operativo y sistema de ficheros usa?
- ¿Qué formatos y dónde usa para almacenar los registros?
- ¿Tengo algún reto legal? (físicas, estándares de propiedad, legales).

Por ejemplo el dispositivo puede tener un sistema operativo cerrado, un sistema de ficheros no estandarizado o incluso el dispositivo puede contener datos sobre diferentes usuarios, no solo sobre los que son relevantes para la investigación. La identificación de los datos de un determinado usuario en un sistema cerrado no es una tarea sencilla. Si a esto añadimos que a nivel legal puede que accedamos sin quererlo a datos personales de usuarios no relacionados con la investigación hace que todo se complique.

De manera resumida tenemos los siguientes riesgos:

Técnicos

- Sistemas operativos cerrados o no documentados

- Sistemas de ficheros cerrado o no documentados
- Dificultad para acceder a los datos relevantes específicos
- Conectores o interfaces no estándar.
- Falta de mecanismos de seguridad que no permitan el borrado de eventos o evidencias

Organizativos

- Poca capacidad de estandarización del proceso
- Dificultad de formación nuevos miembros del equipo

Legales

- Acceso a información sensible (datos médicos, biométricos, personales) de usuarios no relacionados con la investigación
- Falta aún de base legal para admitir según que evidencias en proceso judicial

Autoevaluación

Identifica si las siguientes frases son verdaderas o falsas

Los entornos de IoT son todo ventajas.

○ Verdadero ○ Falso

Falso

Los sistemas en nube son una gran solución para las empresas pero a nivel forense pueden suponer varios problemas tanto de extracción de evidencias como de validez y legalidad de las mismas.

Los entornos de IoT suponen un gran avance a nivel forense pero implica muchos retos.

○ Verdadero ○ Falso

Verdadero

Mayor cantidad de datos aporta más visibilidad pero a cambio exige enfrentarse a nuevos dispositivos con sistemas operativos y de ficheros no estándard.

Los dispositivos IoT no están del todo documentados.

Verdadero Falso

Verdadero

Los fabricantes rara vez documentan cómo funciona el sistema y por tanto requiere de ingeniería inversa muchas veces.

Un forense en IoT implica un trabajo adicional de conocer el sistema operativo, ficheros...

Verdadero Falso

Verdadero

Los forenses en IoT supone enfrentarse a sistemas no documentados (sistema operativo, sistema de ficheros, etc) y por tanto un gran reto a nivel forense.

1.3.- Línea temporal y cadena de custodia.

Pixabay (Dominio público)

Una cadena de custodia fiable -de dónde proceden los datos, quién los ha manejado, quién los ha modificado (y qué ha cambiado), y cuándo ha ocurrido todo esto exactamente- es fundamental para garantizar la validez de la evidencia en un proceso judicial.

Pero en un entorno de IoT conseguir esto no es nada sencillo. A veces el origen de los datos es un concentrador o ***bridge*** que puede provocar eventos que no son confiables ya sea por un error en la fuente o por una línea de tiempo errónea.

Por tanto tenemos dos puntos claros de fallo en la cadena de custodia:

- **El seguimiento fiable de la fuente**
  - Quién envió, recibió y alteró los datos (y si estaba autorizado a hacerlo),
- **Línea temporal**
  - Cuándo sucedieron estos hechos mediante un sellado de tiempo o *timestamp* coherente

Los dispositivos de IoT que por diseño suelen tener más fallos que sistemas IT tradicionales y

que sufren mayores pérdidas de datos (porque no están configurados para ser robustos) generan múltiples eventos de los cuales muchos no son confiables. Al final el analista acaba trabajando con una mezcla de eventos considerados fiables con otros muchos corruptos o con información no confiable, produciéndose una mezcla que no deja discernir lo válido de lo descartable impactando en la línea temporal, en la validez de la fuente y por tanto condiciona la cadena de custodia y a la propia evidencia en si.

Para poder solucionar este problema deberemos de revisar de forma manual y mediante herramientas la validez de las fuentes de información, descartando las que generen eventos no confiables y tratando de tener una línea temporal coherente.

1.4.- Elaborar, Presentar y Exponer las conclusiones.

Pixabay (Dominio público)

Uno de los puntos mas importantes dentro del análisis forense es poder exponer los resultados de las investigaciones. Si tenemos un escenario donde:

- la evidencia no es confiable, produciendo información no veraz
- Puede ser alterada o borrada sin mecanismos de seguridad
- Cadena de custodia poco solida derivada de todo lo anterior

Hace que a nivel de reporting tengamos que tener hacer hincapié en muchos aspectos clave para que nuestro informe sea veraz y pueda aportar en un proceso judicial.

Las principales recomendaciones

- Describir la naturaleza de la fuente de información
  - Los tipos de eventos
  - Su línea de tiempo
  - La naturaleza de sus errores si hubiera
  - La confiabilidad

- Describir la cadena de custodia y su proceso de elaboración