Realización de análisis forenses en IoT (Análisis forense informático)

Identificar los dispositivos a analizar

Todos los dispositivos que puedan aportar información sobre lo ocurrido deben ser analizados, los routers, proxys, firewalls, móviles, ordenadores, etc.

Adquirir y extraer las evidencias

Cada dispositivo que interviene en el caso presenta pruebas que hay que recabar para analizar.

Ejemplos

- https://www.jesusninoc.com/05/01/listar-archivos-abiertos-recientemente/
- https://www.jesusninoc.com/02/06/adquisicion-de-datos-volatiles/
- https://www.jesusninoc.com/02/11/artefactos/
- https://www.jesusninoc.com/04/30/listar-cookies/
- https://www.jesusninoc.com/06/24/fecha-del-ultimo-arranque-del-sistema/

Analizar las evidencias de manera manual y automática

Todos los elementos de los que se puede obtener información hay que analizarlos, algunas veces se hará de forma automática y otras de forma manual.

Ejemplos

Comprobar integridad

- https://www.jesusninoc.com/02/04/integridad/

Analizar DLL

- https://www.jesusninoc.com/11/29/mostrar-los-procesos-que-estan-ejecutando-una-dll-de-un-listado-de-dlls-con-powershell/
- https://www.jesusninoc.com/02/01/explicacion-sobre-el-uso-de-funciones-que-estan-en-dll-del-sistema-operativo-en-powershell/

Volcado de memoria

- https://www.jesusninoc.com/10/14/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-de-forma-grafica/
- https://www.jesusninoc.com/03/04/crear-un-fichero-de-volcado-de-memoria-de-un-proceso/
- https://www.jesusninoc.com/03/13/buscar-una-cadena-dentro-de-un-fichero-de-volcado-de-memoria/
- https://www.jesusninoc.com/09/12/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-y-buscar-una-cadena/
- https://www.jesusninoc.com/09/14/realizar-un-volcado-de-memoria-de-un-proceso-cuando-se-empieza-a-ejecutar/
- https://www.jesusninoc.com/10/22/crear-un-fichero-de-volcado-de-memoria-de-un-proceso-y-detectar-dll/

Extraer imágenes de volcado de memoria

- https://www.jesusninoc.com/10/01/jpegextractor/
- https://www.jesusninoc.com/10/15/extract-all-the-jpgs-found-in-chrome-dmp-dump-file/

Coordenadas GPS en imágenes

- https://www.jesusninoc.com/01/01/extraer-coordenadas-gps-de-imagenes-con-powershell/

Más información

- https://www.jesusninoc.com/03/18/pestudio/
- https://www.jesusninoc.com/10/01/jpegextractor/
- https://www.jesusninoc.com/08/04/lnkanalyser/
- https://www.jesusninoc.com/11/29/dependency-walker/

Documentar el proceso realizado

Todas las acciones que se van realizando para comprender lo ocurrido en el caso se van documentando.

Establecer la línea temporal

A medida que se va realizando el análisis de los elementos que han intervenido en el caso se van colocando en una línea temporal.

Mantener la cadena de custodia

La cadena de custodia se trata de un concepto legal que cubre la validez e integridad de las evidencias recogidas para sustentar un proceso judicial. Cubre todos los pasos desde la

recogida hasta su utilización final.

Elaborar las conclusiones

Una vez analizada y relacionada toda la información se plantean conclusiones de lo que ha ocurrido.

Presentar y exponer las conclusiones

El último paso del análisis forense consiste en presentar las conclusiones obtenidas de todo el proceso.