|  |  |
| --- | --- |
| **Informe Final Pericial – MCS520 Informática Forense** | |
| **Investigador/a**: Ángel Peña | **ID Investigador/a**: 1094214 |
| **ID caso**: DO-IF-A000 | **Fecha, hora**: 23/04/2021 19:28 AST |
| **Descripción:**  Este documento describe paso a paso la realización de las prácticas de la asignatura “**MCS520 – informática Forense”** basado en el contexto de un informe pericial de cómputo forense.  El levantamiento de información indica que el 17 de marzo del año 2021 el Sr. Ángel Peña (Ing. En Sistemas de Computación) realizó el procedimiento de captura de los datos pertinentes al activo de información listado en la siguiente tabla:   |  |  | | --- | --- | | Nombre PC: | RESISTANCEB | | Usuario PC: | VPN\_user | | Dirección IPv4 | 169.254.11.13 | | Dirección MAC: | 08-00-27-9E-3F-E2 | | Sistema Operativo, versión, arquitectura: | MS Windows 10 LTSC, 1809, 64-bits | | Memoria RAM | 3048 MB | | Cantidad y capacidad disco duro: | 1 disco, 50 GB SATA III 5400 rpm | | Procesador, generación, velocidad Hz | Intel Core i7, 8750H, 2.20GHz |   **Detalle del evento:**  Para la realización de la practica 1: Se realizó búsqueda de un aplicativo web el cual genere tarjetas de crédito ficticias. En las siguientes capturas se muestra el paso a paso de esta actividad.   |  | | --- | | **Título**: Practica #1 | | **Objetivo**: Identificar el origen de un BIN |  |  | | --- | | Ingreso de datos ficticios requeridos por el aplicativo: | |  | | Datos ficticios generados: | |  | | *Fuente: https://www.vccgenerator.com/result/* |  |  | | --- | | **Ingreso de datos requeridos en aplicativo web:** | |  | |  | | **Resultados de busqueda en aplicativo web:** | |  | | *Fuente: http://exactbins.com/bin-lookup/* |   Posteriormente para la práctica #2, estos fueron los pasos y resultados:   |  | | --- | | **Título**: Practica #2 | | **Objetivo**: Formatear (Sanear) un Periférico de Almacenamientos |   Nota: Sanear un dispositivo o periférico de almacenamiento conlleva dos métodos.   1. Inicializar el proceso de análisis, búsqueda, identificación y remoción de artefactos maliciosos identificados por la solución Anti-Malware de su preferencia. 2. Inicializar un borrado de todos los archivos localizados dentro del periférico de almacenamiento, haciendo uso de la opción “formatear”.  |  | | --- | | **Seleccionar la solucion Anti-Malware de su preferencia** | |  | |  | | **Resultados del proceso de saneamiento finalizado por solucion Anti-Malware** | |  | | *Fuente: Mecanismo de control Anti-Malware Malwarebytes* | | **Proceso de saneamiento, mediante opcion “Formatear”** | |  | |  | | *Fuente: Opción de saneamiento “Formatear”* |  |  | | --- | | **Título**: Practica #3 | | **Objetivo**: Capturar volcado de memoria RAM – FTK Imager |  |  | | --- | | Seleccionar opcion “Capture memory…” | |  | | **Luego de seleccionar la ruta de destino proceder a hacer clic en el boton “Capture Memory”** | |  | |  | | **Proceso de creacion de volcado de memoria ram del activo de información** | |  | | **Archivo de volcado de memoria creado “memdump 25-04-2021.mem”** | |  | | **Hacer clic en la opcion “Find…” y colocar el nombre del usuario del activo para validar que el volcado se haya realizado de manera correcta.** | |  | |  | | *Fuente: FTK Imager* |  |  | | --- | | **Título**: Practica #4 | | **Objetivo**: Montar una memoria USB – FTK Imager |   Durante el proceso investigativo se identificó que el 17 de marzo del 2021 fue realizado un volcado de memoria de un dispositivo extraíble localizado en la ruta de disco (E:\) el cual posee una capacidad de almacenamiento total de 32 GB.   |  | | --- | |  | | **Seleccionar el disco extraible o USB objetivo (32GB)** | |  | |  | | **Posteriormente hacer clic derecho en la carpeta que desee recuperar y luego hacer clic en “Export Files” y la ruta destino.** | |  | |  | | *Fuente: FTK Imager* |  |  | | --- | | **Título**: Practica #5 | | **Objetivo**: Crear una imagen forense de una memoria USB – FTK Imager |  |  | | --- | |  | |  | |  | | **En este apartado se ingresan los detalles de la evidencia a analizar, responsable y datos de identificación de la evidencia (Cadena de Custodia).** | |  | | **Se procede a ingresar el nombre o titulo de la imagen de la USB “IMG\_USB\_U000”** | |  | | **Al hacer clic en “Finish”, mostrará una ventana indicando el destino de la imagen. Se debe hacer clic en “Start” para inicializar la construcción de la imagen.** | |  | | **Proceso de construccion de imagen inicializado.** | |  | | **Imagen creada con formato “.0001”** | |  | | **En la siguiente imagen, se pueden ver los detalles arrojados por el aplicativo FTK Imager acerca de la construccion de la imagen de la USB.** | |  | | *Fuente: FTK Imager* |  |  | | --- | | **Título**: Practica #6 | | **Objetivo**: Virtualizar o Montar imagen forense de memoria USB – FTK Imager |  |  | | --- | |  | | **Se debe hacer clic en la opción “Block Device/Read Only” para solo habilitar el uso de lectura de la imagen virtualizada.** | |  | |  | | **En la imagen anterior se puede observar el listado de la particion virtual y la imagen montada como un disco.** | | **En la siguiente imagen se ve el listado de los perifericos de almacenamiento del activo, siendo el “Disco local (F:\) la imagen virtualizada con bloqueo de escritura.** | |  | |  | | *Fuente: FTK Imager* |  |  | | --- | | **Título**: Practica #7 | | **Objetivo**: Calcular el valor HASH (HashMyFiles y FTK Imager) |  |  | | --- | | **Para generar el hash de integridad de la imagen de la USB creada, se utilizó el software “HashMyFiles”** | |  | | *Fuente: HashMyFiles* | | **Generar hash con FTK Imager** | |  | |  | |  | |  | |  | |  | | *Fuente: FTK Imager* |  |  | | --- | | **Título**: Practica #8 | | **Objetivo**: Obtener los Metadatos de un archivo |  |  | | --- | | **La imagen virtualizada “IMG\_USB\_U000” fue analizada con la herramienta “ExifTools”** | |  | | *Fuente: ExifTools* |  |  | | --- | | **Título**: Practica #9 | | **Objetivo**: ¿Porque debe de ir un experto al levantamiento? |  |  | | --- | | Debido a que los peritos informáticos forenses conocen las normas y reglamentos para el cuidado de las evidencias. Poseen un conocimiento especializado en las herramientas a utilizar, composición de los sistemas y como salvaguardar las evidencias. Tienen la habilidad y responsabilidad de evidenciar que los datos recolectados son íntegros e irrefutables ante cualquier juicio que se encuentre en ejecución. | | El perito informatico forense se encarga de extraer informacion tanto de activos de informacion encendidos, como los apagados, dispositivos móviles o cualquier otro dispositivo informatico que se encuentre asociado a una investigación. | | El Profesional del computo forense debe asistir a las escenas donde se identifique que fue utilizado un medio informatico para dar origen a un atentado criminalístico. |  |  | | --- | | **Título**: Practica #10 | | **Objetivo**: Análisis estático – OSForensics (Free Trial) |  |  | | --- | |  | |  | |  | | **Progreso de la captura de informacion y/o triaje:** | |  | | **Historial de comandos en consola o terminal de MS Windows** | |  | | **Datos activo de informacion: ResistanceB** | |  | | **Historial de navegación** | |  | | **Listado softwares instalados** | |  | | *Fuente: OSForensics* | | |