

*UNIVERSIDAD AUTONOMA DE CHIAPAS*

IINGENERIA EN DESARROLLO Y TECNOLOGIAS DEL SOFTWARE

FACULTAD DE CONTADURIA Y ADMINISTRACION, CAMPUS I

**COMPUTO FORENSE**

P. FINAL

PROYECTO FINAL DE LA ASIGNATURA DE COMPUTO FORENSE

ALUMNOS:  
  
ÁLVAREZ GÓMEZ TOMÁS – A200369  
ZEA HERNANDEZ NESTOR HORACIO -- A200727

CATEDRATICO

MTRO. ADÁN NAÑEZ COUTIÑO

OCTAVO SEMESTRE GRUPO “M”

TUXTLA GUTIÉRREZ, CHIAPAS

06/05/24

**Principios Básicos de la Computación Forense**

Los principios básicos de la computación forense son los fundamentos éticos y técnicos que guían la práctica de investigar y analizar evidencia digital para resolver crímenes cibernéticos o incidentes de seguridad. Estos principios aseguran la integridad, confiabilidad y legalidad del proceso. Por ejemplo, la integridad de la evidencia garantiza que la información no sea alterada o comprometida, mientras que la cadena de custodia establece un registro detallado de todas las interacciones con la evidencia para garantizar su admisión en un tribunal. Estos principios son los pilares sobre los que se construye la computación forense, asegurando que se realice de manera ética, legal y efectiva.

La computación forense es un campo especializado dentro de la seguridad informática que se enfoca en la adquisición, preservación, análisis y presentación de evidencia digital para su uso en procesos legales.

De los principios básicos tenemos como ejemplos los siguientes:

*1. Integridad de la evidencia:* Es fundamental preservar la integridad de la evidencia digital desde el momento en que se descubre hasta que se presenta en un tribunal. Cualquier alteración o modificación podría invalidar la evidencia.

*2. Cadena de custodia:* Se debe mantener un registro detallado de todas las personas que han tenido acceso a la evidencia digital y de todas las acciones realizadas sobre ella. Esto garantiza su validez y admisibilidad en un tribunal.

*3. Legalidad y autorización:* Todas las actividades de computación forense deben realizarse de acuerdo con la ley y con las debidas autorizaciones. Esto implica obtener permisos legales antes de realizar cualquier investigación forense.

*4. Confidencialidad:* La información obtenida durante una investigación forense debe manejarse con estricta confidencialidad para proteger la privacidad de las partes involucradas y garantizar la integridad del proceso legal.

*5. Métodos y herramientas apropiados:* Es crucial utilizar métodos y herramientas apropiados y reconocidos en la computación forense para garantizar la precisión y fiabilidad de los resultados obtenidos.

*6. Preservación de la evidencia original:* Se debe trabajar con copias forenses de la evidencia digital siempre que sea posible, para preservar la evidencia original intacta y evitar su contaminación o alteración accidental.

*7. Análisis exhaustivo:* El análisis de la evidencia digital debe ser exhaustivo y meticuloso, buscando no solo la información relevante para el caso en cuestión, sino también cualquier otra actividad o dato que pueda ser importante para la investigación.

*8. Documentación detallada:* Es necesario documentar de manera detallada todas las acciones realizadas durante el proceso de investigación forense, incluyendo los métodos utilizados, las herramientas empleadas, los hallazgos y las conclusiones.

**Tipos de Archivos**

En el análisis forense, los investigadores pueden encontrarse con una variedad de tipos de archivos que contienen información relevante para la investigación.

* *Archivos de sistema operativo:* Estos archivos incluyen registros de eventos, archivos de configuración y registros de actividad del sistema operativo, como el Registro de Windows en sistemas Windows o los archivos de registro del sistema en sistemas Unix/Linux.
* *Archivos de registro:* Los registros de aplicaciones, de seguridad y de sistemas pueden contener información sobre actividades del usuario, intentos de acceso no autorizado y eventos importantes del sistema que pueden ser críticos para la investigación forense.
* *Archivos de bases de datos:* Las bases de datos contienen una gran cantidad de información valiosa, como registros de transacciones, datos de usuarios y registros de acceso, que pueden ser analizados para reconstruir eventos y acciones específicas.
* *Archivos de correo electrónico:* Los correos electrónicos y los archivos de correo electrónico pueden proporcionar información sobre comunicaciones, interacciones y posibles evidencias de actividades ilegales o sospechosas.
* *Archivos de imágenes de disco:* Las imágenes de disco son copias exactas de dispositivos de almacenamiento como discos duros o dispositivos USB. Estos archivos se pueden analizar para recuperar datos eliminados, buscar archivos relevantes y examinar la estructura y el contenido del sistema de archivos.
* *Archivos de registro de red:* Estos archivos registran la actividad de la red, como conexiones entrantes y salientes, tráfico de datos y actividades de usuario en línea. Pueden ser cruciales para rastrear actividades maliciosas o identificar intrusiones en la red.
* *Archivos de aplicaciones:* Los archivos de aplicaciones pueden contener datos específicos de software, como archivos de configuración, registros de actividad del usuario, datos de sesión y otros registros que pueden ser relevantes para la investigación.
* *Archivos de medios multimedia:* Imágenes, videos y archivos de audio pueden contener metadatos útiles, como marcas de tiempo, ubicaciones geográficas y detalles de la cámara, que pueden ser utilizados como evidencia en una investigación forense.

Estos son solo algunos ejemplos de los tipos de archivos que los investigadores forenses pueden analizar para obtener información valiosa en una investigación. La naturaleza específica de los archivos analizados dependerá del contexto de la investigación y de los incidentes o delitos que se estén investigando.

**Herramientas Disponibles**

En la computación forense, existen diversas herramientas diseñadas para ayudar en la adquisición, análisis y presentación de evidencia digital. Estas herramientas se pueden clasificar en varias categorías según su función y uso.

*1. Herramientas de adquisición de datos:* Estas herramientas permiten realizar copias forenses de dispositivos de almacenamiento, como discos duros, dispositivos USB, tarjetas de memoria, etc. Algunas herramientas populares incluyen:

- FTK Imager, EnCase Forensic, dd (command-line tool), y Autopsy.

*2. Herramientas de análisis de sistema operativo:* Estas herramientas están diseñadas para examinar sistemas operativos en busca de datos relevantes, incluyendo archivos de registro, configuraciones del sistema, y otros artefactos. Ejemplos incluyen:

- Registry Viewer, Windows Forensic Toolkit (WFT), y Volatility Framework para análisis de memoria.

*3. Herramientas de análisis de red:* Estas herramientas se centran en el análisis del tráfico de red para identificar actividades maliciosas, intrusiones, o comunicaciones sospechosas. Algunos ejemplos son:

- Wireshark, NetworkMiner, y Security Onion.

*4. Herramientas de análisis de medios digitales:* Estas herramientas se utilizan para examinar y analizar archivos multimedia, como imágenes, videos y audio. Pueden ayudar a recuperar datos ocultos, extraer metadatos y realizar análisis de contenido. Ejemplos incluyen:

- Forensic Toolkit (FTK), Sleuth Kit, y ExifTool.

*5. Herramientas de análisis de bases de datos:* Estas herramientas están diseñadas para examinar y analizar bases de datos en busca de datos relevantes, registros de transacciones, registros de acceso, etc. Ejemplos son:

- SQLite Forensic Explorer, DB Browser for SQLite, y MySQL Workbench.

*6. Herramientas de análisis de malware:* Estas herramientas se utilizan para analizar y examinar software malicioso en busca de comportamientos sospechosos, características de virus, y otros indicadores de compromiso. Ejemplos son:

- VirusTotal, Malwarebytes, y Cuckoo Sandbox.

*7. Herramientas de análisis de archivos y documentos:* Estas herramientas se centran en examinar archivos y documentos en busca de metadatos, contenido oculto, y otras características relevantes. Ejemplos incluyen:

- olevba para análisis de macros de documentos de Office, y ExifTool para análisis de metadatos.

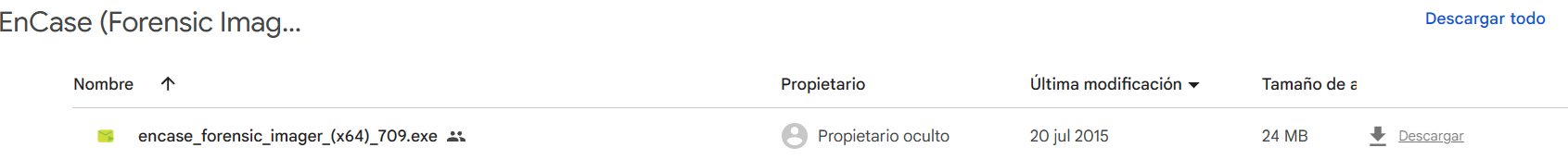
**Implementación de Herramientas Forenses**

Herramienta de Análisis Forense (EnCase Forensic)

Herramienta de Análisis Forense con características de seguridad ()

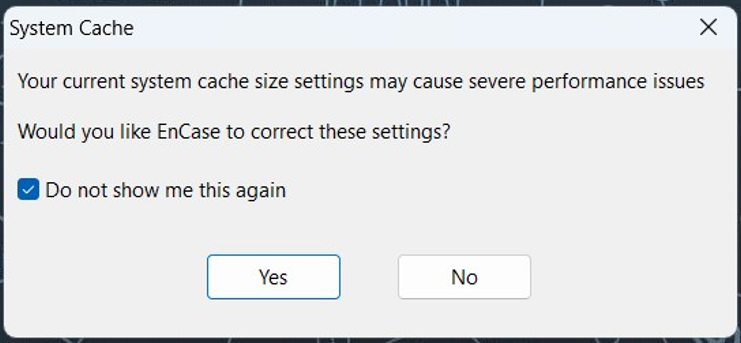
**EnCase Forensic**

Paso 1 – Descargar el software EnCase Forensic. <https://drive.google.com/drive/folders/1SCe46QvyKPXJnBbv4rQ7Js-GZbqlZlOa>

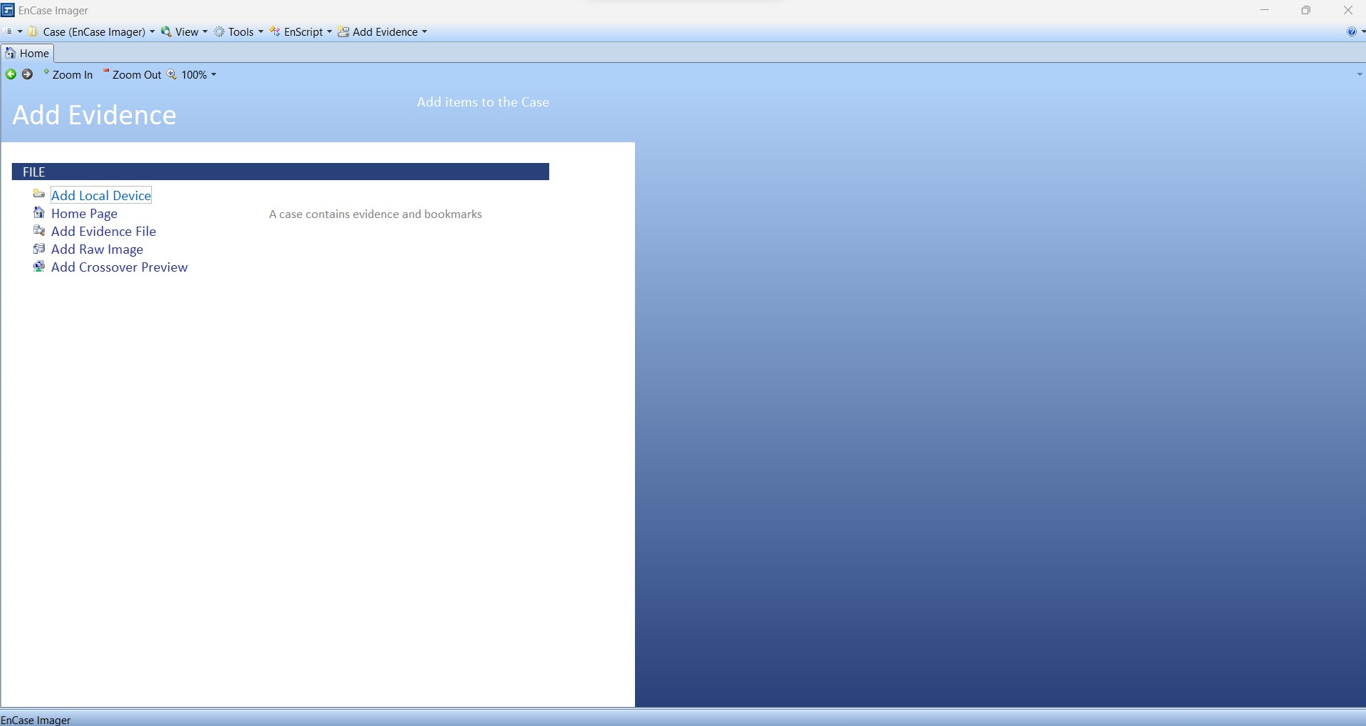


Paso 2 – Ya teniendo el archivo descargado, empezamos con su instalación.

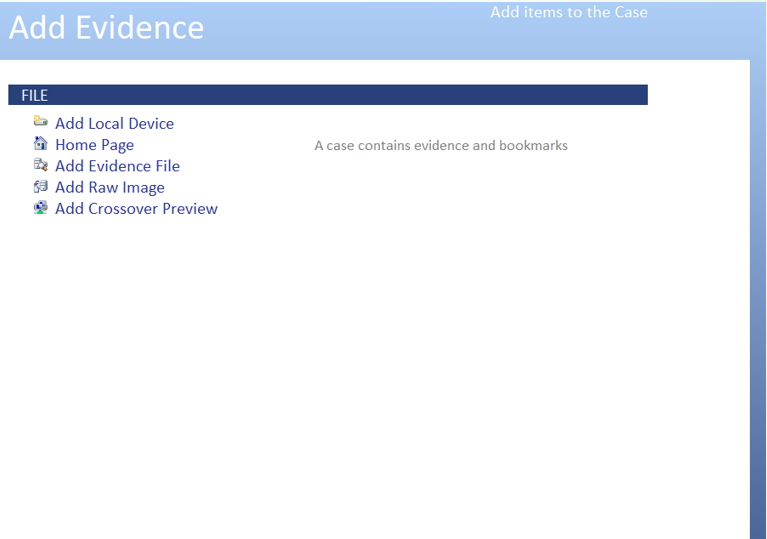
En este apartado le damos confirmación en Yes.



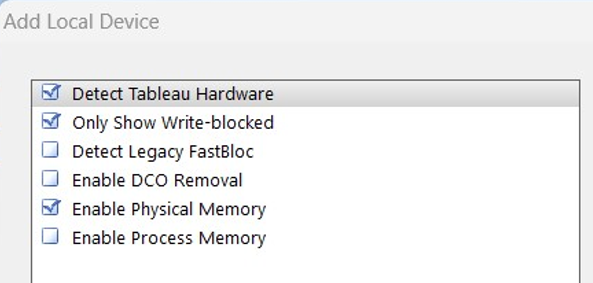
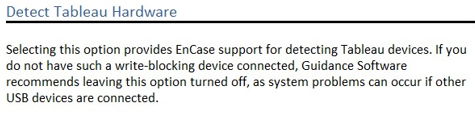
Paso 3 – Ejecutamos el software y nos saldrá la siguiente imagen.



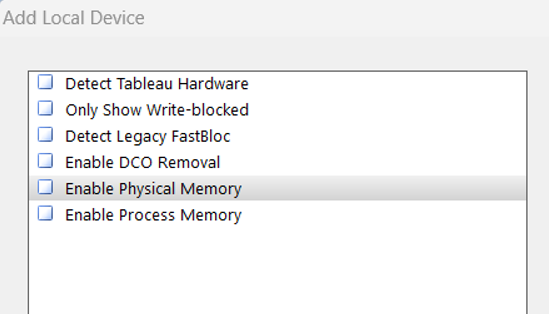
Paso 4 – Abrimos el panel de inicio o accesos rápidos



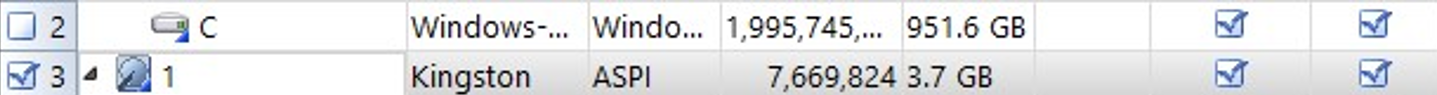
Paso 5 – En este paso vamos agregar nuestro dispositivo local.

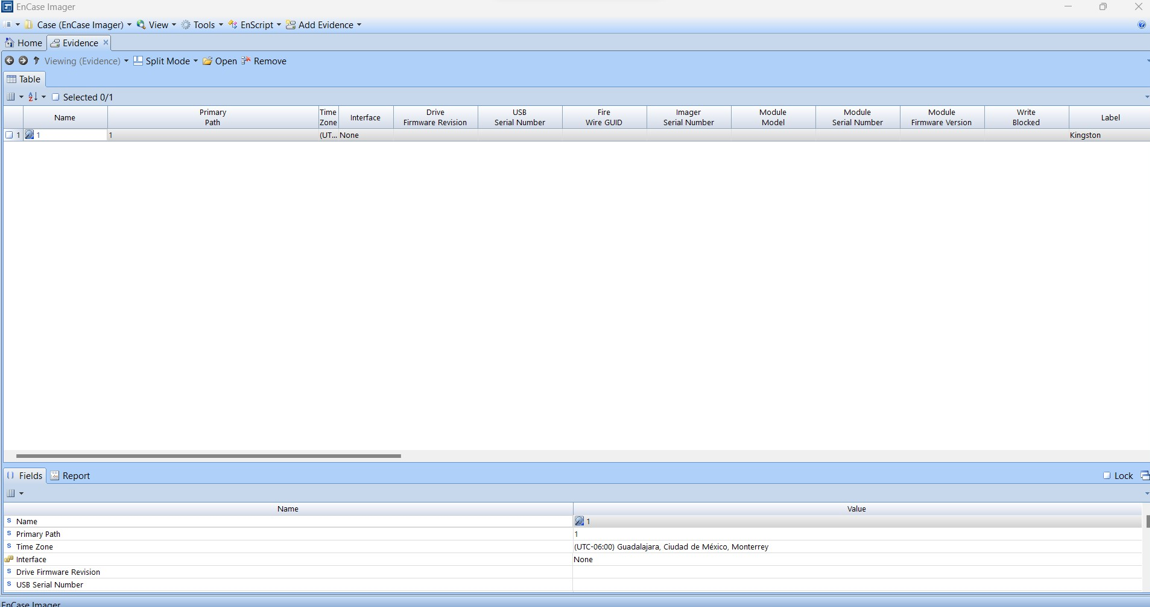
Paso 6 – Aquí vamos a desactivar las casillas como se muestra en la imagen



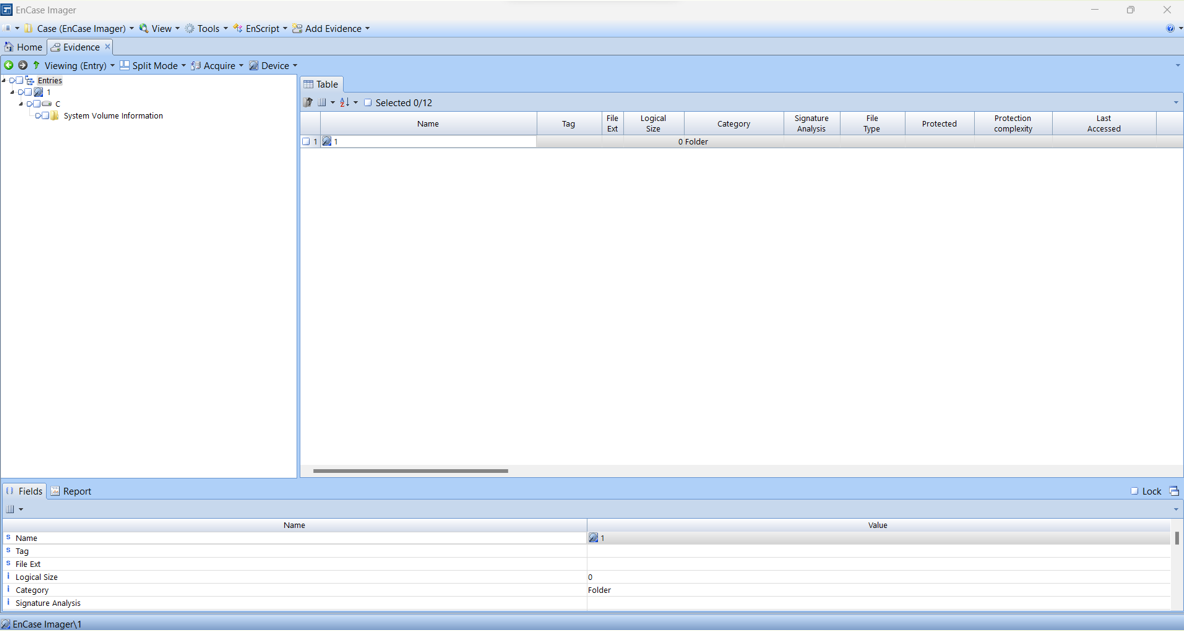
Paso 7 – Seleccionamos nuestro dispositivo local, en este caso es el 3



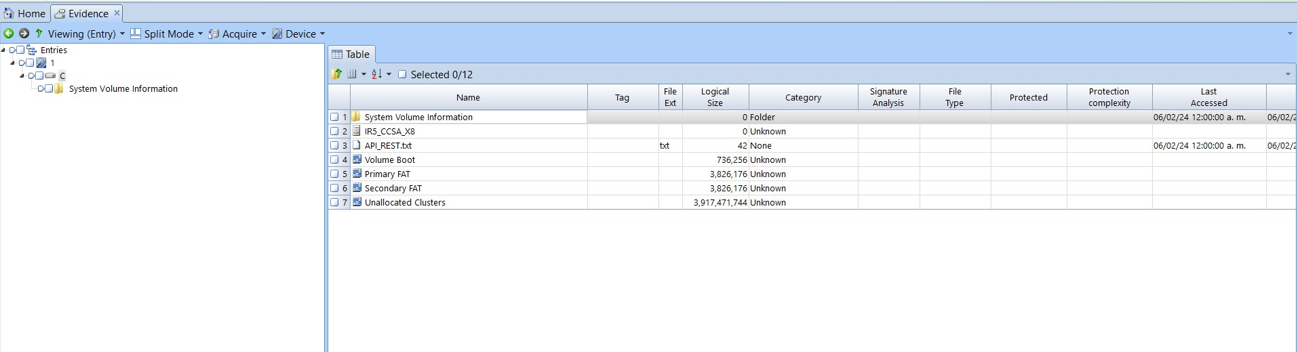
Paso 8 – Vamos a trabajar con la evidencia del dispositivo



Paso 8 – Exploramos la pestaña de evidence



Paso 9 – Tendremos la vista de la siguiente ventana



Paso 10 -