**Análisis Forense**

# Adquisición de Memoria con FTK Imager

### 

### 

**Portada**1

[**Indroducción**](#_1g4arwxepfc4) **3**

[1. Objetivo](#_2ftq7gp5tgoq) 3

[2. Resumen](#_wbx7njx56boa) 3

[**Instalación de FTK Imager en Windows**](#_82rtf668nkii) **3**

[**Interfaz de usuario de ftk imager**](#_5lci93scy62n) **3**

[Barras](#_rsr7c6jzcmo6) 4

[Barra de menú](#_rsr7c6jzcmo6) 4

[Barra de Herramientas](#_ba4ad8903dzt) 5

[Barra de estado](#_v20u5uodfta6) 5

[Paneles](#_jpkl324iyo) 6

[Arból de evidencia](#_cuiuggokmgw5) 6

[Lista de archivo](#_wom4ai19hhm4) 6

[Visor](#_ndugi52cl00x) 6

[Panel combinado](#_yoxdplv640ln) 6

[Propriedades](#_pajrsf82g65b) 6

[Intérprete de valores hexadecimales](#_bmunun8g4kyi) 6

[Fuente de contenido personalizado](#_w01xkqb0su8j) 7

[Modos de vista previa](#_wercsri2z9rz) 7

[Automático](#_rg297dswb7wx) 7

[Texto](#_nil49f4t9mrs) 7

[Hexadecimal](#_m0prdxtxbp1u) 7

[**Imágenes forenses**](#_u8bjrfswkjb6) **7**

[No volátil](#_2hrmb5v90ny2) 7

[Encriptación de la imagen](#_vtkgm8wwslek) 14

[Desencriptado de la imagen](#_5fl872s0y1cc) 15

[Volátil](#_sarxk97tl64k) 16

[**Agregar evidencias de la imagen**](#_8di53dgcqg1h) **18**

[**Verificar imagen**](#_osgomcug5bqp) **18**

[**Agregar evidencias de dispositivos desconectados**](#_8it48kx6k9u4) **19**

[**Montado de imagen**](#_n3baf3yh8pkf) **20**

[Desmontado de la imagen](#_roiev4o8cdae) 23

[**Eliminar evidencia**](#_a2871qwtnbdz) **23**

[**Copia de ficheros protegidos**](#_lj3sivcuv39u) **24**

| IndroducciónObjetivo Capturar memoria volátil como no volátil mediante software. Resumen Creación de la imagen forense de un disco y una memoria RAM. Además de verificar y encriptar imágenes creadas. |
| --- |
| Instalación de FTK Imager en Windows |
| Descargar .exe y ejecutar como administrador.  <https://www.exterro.com/ftk-imager> |
| Interfaz de usuario de ftk imager |
| La interfaz se encuentra dividida en múltiples paneles, cada uno de los cuales es ajustable. Los paneles incluyen el árbol de evidencia, la lista de archivos, las propiedades, el intérprete de valores hexadecimales, los paneles de fuentes de contenido personalizado, el menú y la barra de herramientas, todos los cuales pueden ser acoplados y redimensionados según las preferencias del usuario. Es posible acoplar o restablecer la vista completa de cada panel de manera individual. |
|  |
| Barras |
| Barra de menú |
| Permite acceder a todas las funciones de FTK Imager. |
| * **Archivo** → Acceso a todas las funciones que puede utilizar desde la barra de herramientas.      * **Ver** → Ajustes de apariencia, como revelar u ocultar. * **Modo** → elección del tipo de vista anticipada del visor. * **Ayuda** → Acceso al manual y detalles sobre la versión. |
| Barra de Herramientas |
| Incorpora herramientas, funciones o atributos a los que se puede entrar desde el menú de archivo, excluyendo la opción de salir. |
| Barra de estado |
| Muestra detalles pertinentes acerca del estado actual del sistema o la aplicación. |
| Paneles |
| Arból de evidencia |
| * Muestra elementos de evidencia organizados en una estructura jerárquica. * En la parte superior, se sitúan las fuentes de evidencia elegidas, y debajo de cada fuente se enlistan las carpetas y archivos que contiene. |
| Lista de archivo |
| Presenta los archivos y carpetas que conforman cualquier elemento actualmente señalado en el Árbol de evidencia. Se ajusta dinámicamente conforme cambia la selección. |
| Visor |
| Muestra el contenido del archivo seleccionado, de acuerdo con el modo de visualización escogido. Puede ser en formato **natural, texto o hexadecimal.** |
| Panel combinado |
| Propriedades |
| Información sobre el objeto seleccionado en el árbol de evidencia o en la lista de archivos. |
| Intérprete de valores hexadecimales |
| Convierte los valores hexadecimales seleccionados en el visor en números enteros decimales y posibles valores de fecha y hora. |
| Fuente de contenido personalizado |
| Facilita la generación de imágenes con contenido personalizado con el fin de disminuir su tamaño.  Despliega un registro de archivos incorporados que están siendo agregados a la imagen personalizada. |

| Modos de vista previa |
| --- |
| Automático |
| Se selecciona según el tipo de archivo para obtener una vista previa del contenido. |
| Texto |
| Genera una vista previa del contenido como caracteres ASCII o Unicode, incluso si el archivo no es de texto. |
| Hexadecimal |
| * Permite ver cada byte en hexadecimal. * Se usa para interpretar valores hexadecimales como enteros decimales y posibles valores de fecha y hora. |
| Imágenes forenses |
| No volátil |
| Haré uso de herramientas de virtualización de discos para hacer la prueba de concepto. |
| Seleccionar disco con administrador de disco |
|  |
| En este caso E: |
| En afk imager |
| File → create Disk image → physical drive → <elegir disco> → selección de imagen de destino |
|  |
| En una imagen forense se busca mantener la integridad de la imagen por lo que será una copia raw |
|  |
|  |
|  |
| Resultado: |
|  |
|  |
| Resultado con hash con los que comprobar la integridad |
|  |
| Resultado: |
|  |
|  |
| Encriptación de la imagen |
|  |
|  |
| Muy interesante la alternativa de encriptación con certificado digital |
| Desencriptado de la imagen |
|  |
| Resultado: |
|  |
| File → Image File → < Seleccionar el archivo > → |
| Volátil |
| File → capture memory → |
|  |
|  |
| Resultado |
|  |
| Agregar evidencias de la imagen |
| File → add evidence Item→ Image File → <seleccionar fuente (imagen)> |
| Resultado: |
|  |
| Verificar imagen |
| Evidencia → verify Drive/Image |
|  |
|  |
| Resultado |
|  |
| Podemos ver en las sub secciones “Verify result” el resultado **Match** |
| Agregar evidencias de dispositivos desconectados |
| Esto agrega tanto las unidades lógicas como físicas  File → Add All Attaches Devices |
| Resultado |
|  |
| Montado de imagen |
| File → Image mounting → <configurar el montado |
|  |
| →mount |
| Resultado: |
|  |
|  |
| Desmontado de la imagen |
| File → Image Mounting → <elegir el montado> |
|  |
| → unmount |
| Eliminar evidencia |
|  |
| Evidence tree → <seleccionar item> → Remove Evidence Item |
| Alternativa: |
| Files → Remove All Evidence Item |
|  |
| Copia de ficheros protegidos |
| File → obtain Protected Files |
|  |
|  |
| Resultado: |
|  |

Bibliografía:

* <https://youtu.be/6OUQcL_8XXA>
* <https://www.exterro.com/ftk-imager>
* <https://bardimin.com/en/windows-en/how-to-create-a-virtual-usb-flash-drive-in-windows-10/#1_Open_%E2%80%9CDisk_Management%E2%80%9D>