Laboratorio 1.2

Instalando FTK Imager

Ing. Alex Araya Rojas, MT
CISSP, CISM

Agosto 2021

Lab 1.2

Instalando FTK Imager

01 **Descargar el instalador**

02 **Proceso de instalación**

03 **Guía de inicio básica en FTK Imager**

Procedimiento

Descargar el instalador

01. Access Data es una compañía líder en temas forenses, existe un producto libre llamado FTK imager que podemos utilizar para hacer imágenes de discos o secciones de la memoria de Windows. Visite el sitio web https://accessdata.com/product-download, vaya al link de descarga del FTK Imager.
02. Descargue la versión disponible del software, cuando se elaboró esta guía era la versión 4.5 del 8 de octubre del 2020.
03. Debe registrarse para recibir el enlace de descarga.

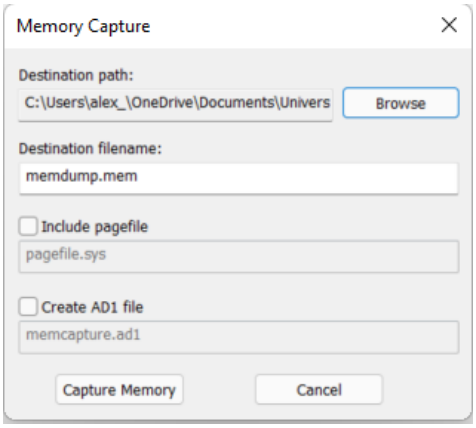
Proceso de instalación

01. Una vez descargado el instalador, se procede con su instalación, haga doble click sobre el archivo descargado.
02. Es probable que su Windows indique que existe un riesgo al instalar el software, haga click en ejecutar de todas formas. Si tiene dudas al respecto o su organización limita las aplicaciones que ud puede instalar, se recomienda que haga la instalación en una máquina virtual o en otro equipo sin restricciones.
03. El proceso de instalación es muy simple, haga clic en el botón Next para iniciar con el proceso.
04. Al finalizar el proceso de instalación, presione el botón Finish y verá un ícono en su escritorio.

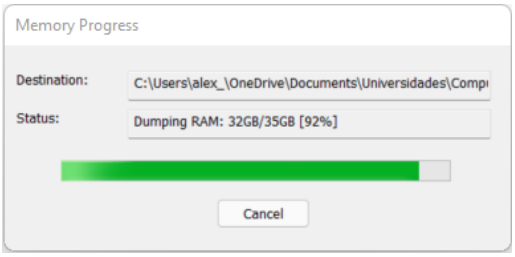
05. Haga clic derecho sobre el ícono y ejecútelo como administrador.
06. Esté atento a posibles mensajes para liberar bloqueos del firewall de Windows sobre el aplicativo, haga clic en Permitir Acceso.

Guía de inicio básica en FTK

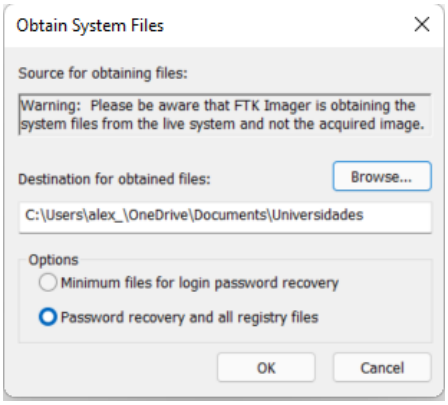
01. Una vez que el aplicativo está ejecutándose, presione File > Capture Memory.
02. Defina el Destination Path, es una ruta para guardar el archivo resultando del proceso.



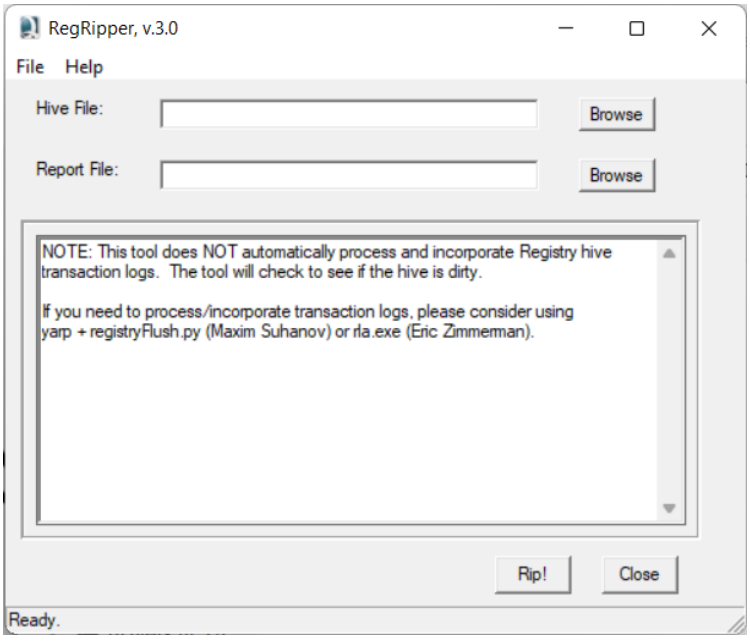
03. Estamos sacando una copia de su memoria RAM para dejarla en un archivo que luego analizaremos con varias herramientas.
04. La velocidad del proceso nuevamente dependerá de las características de su equipo de cómputo y de la cantidad de memoria RAM con que cuenta su equipo.
05. Tenga paciencia en el proceso…



06. La actividad anterior realizó un proceso conocido como volcado de memoria, más adelante en el curso trabajaremos con esos archivos resultantes.
07. Vaya a Files > Obtain Protected Files, defina una ruta para los archivos de salida de esta operación, marque las opciones como se muestran a continuación.



08. Puede cerrar el FTK y vaya a la carpeta donde ubicó los archivos de salida.
09. Solicite al profesor acceso a la carpeta llamada Registry Ripper.
10. Ejecute el programa llamado rr.exe
11. En el campo Hive File, seleccione uno de los archivos protegidos que se generaron con FTK, por ejemplo Software.
12. En el campo Report File, debe ponerle un nombre al archivo procesado que saldrá de la ejecución, por ejemplo Software.txt
13. Una vez cargado el archivo protegido y seleccionado el archivo de reporte de salida, solo necesita presionar el botón Rip It.



14. Repita esto para los archivos protegidos del sistema, no olvide hacerlo con el archivo NTUSER.DAT, que se encuentra dentro de la carpeta users/default

15. Analice los archivos de respuesta y genere un informe con los elementos más importantes que se pueden obtener de este proceso.
16. Este informe debe ser entregado en 8 días a partir de la asignación de este laboratorio. El informe debe contar con al menos 3 páginas y no debe contener datos confidenciales de su equipo, solo generalidades sobre la información que durante una pericia forense usted podría obtener.
17. Incluya como anexo 1 del informe los Laboratorios 1, pantallazos del proceso generado en el Lab1-1 que evidencien que se realizó el mismo.