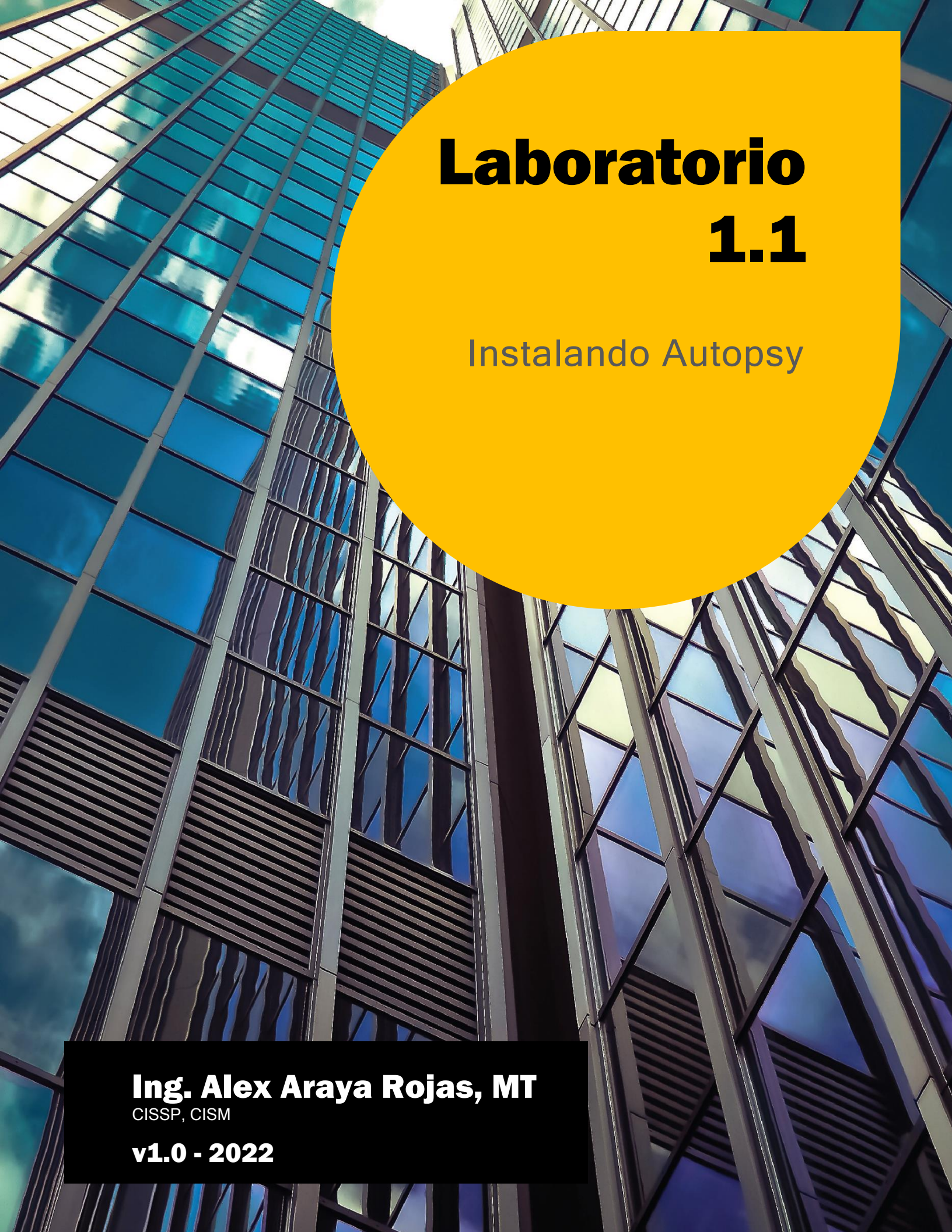


Laboratorio 1.1

Instalando Autopsy

Ing. Alex Araya Rojas, MT
CISSP, CISM

v1.0 - 2022

Lab 1.1

Instalando Autopsy

01 **Descargar el instalador**

02 **Proceso de instalación**

03 **Guía de inicio básica en autopsy**

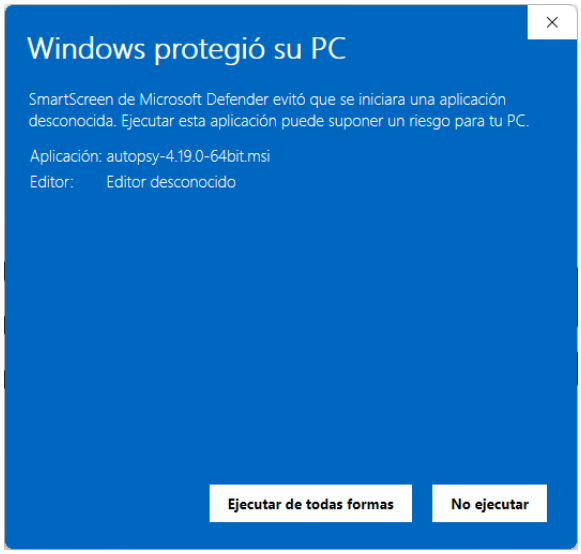
Procedimiento

Descargar el instalador

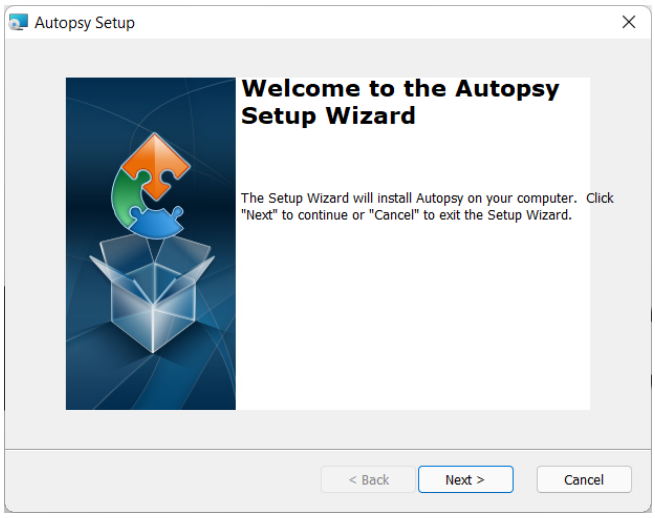
01. Autopsy Digital Forensics es un software open source que incluye los elementos core de las soluciones comerciales. Visite el sitio web https://www.autopsy.com/ e investigue un poco acerca de la plataforma.
02. Descargue la versión disponible del software, cuando se elaboró esta guía era la versión 4.19.0, esta guía se orienta a la instalación en Windows.

Proceso de instalación

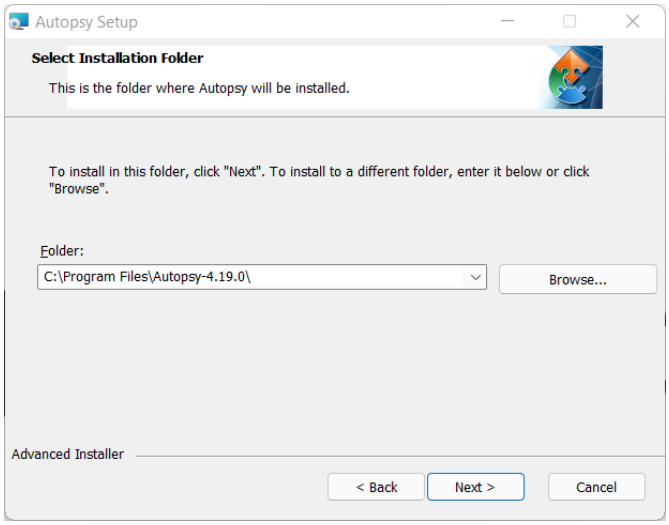
01. Una vez descargado el instalador, se procede con su instalación, haga doble click sobre el archivo descargado.
02. Es probable que su Windows indique que existe un riesgo al instalar el software, haga click en ejecutar de todas formas. Si tiene dudas al respecto o su organización limita las aplicaciones que ud puede instalar, se recomienda que haga la instalación en una máquina virtual o en otro equipo sin restricciones.



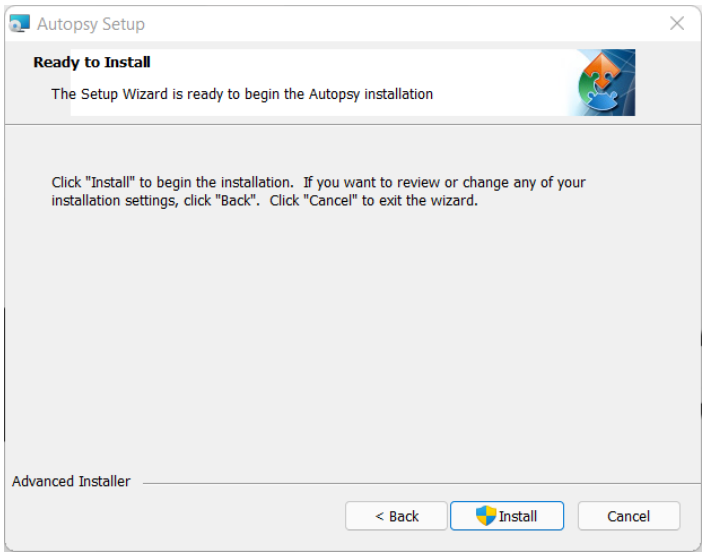
03. El proceso de instalación es muy simple, haga clic en el botón Next para iniciar con el proceso.



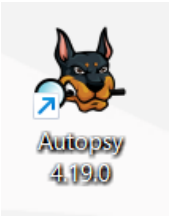
04. Seleccione la ruta de instalación de la herramienta, puede dejar la sugerida y presionar Next.



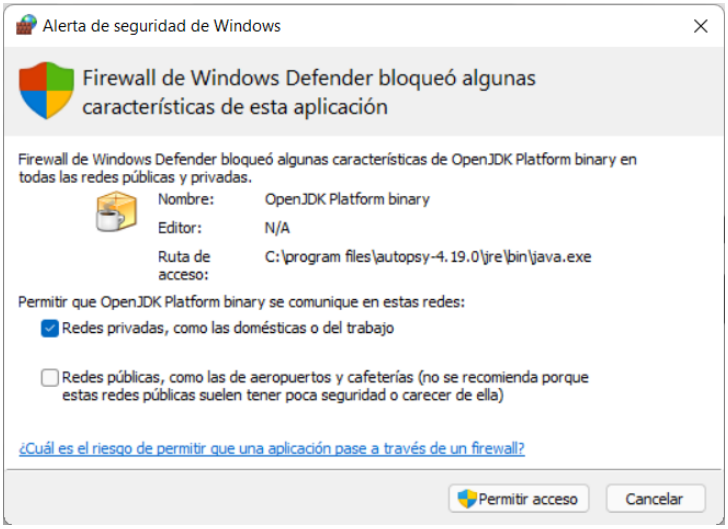
05. Una vez definidos los parámetros de la instalación, haga clic en Install para comenzar, esté atento a confirmaciones de Windows para poder continuar con el proceso.



06. Al finalizar el proceso de instalación, presione el botón Finish y verá un ícono en su escritorio.

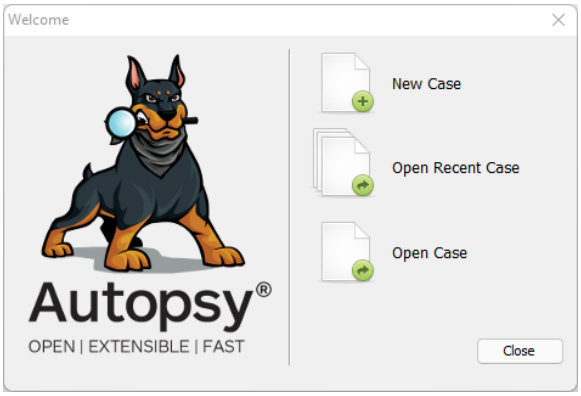


07. Haga doble clic sobre el ícono para abrir la herramienta.
08. Esté atento a posibles mensajes para liberar bloqueos del firewall de Windows sobre el aplicativo, haga clic en Permitir Acceso.

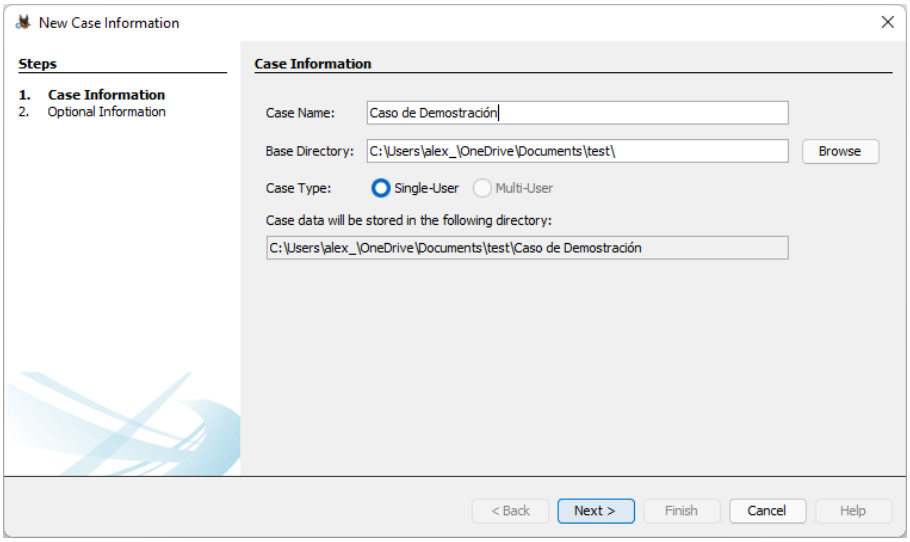


Guía de inicio básica en Autopsy

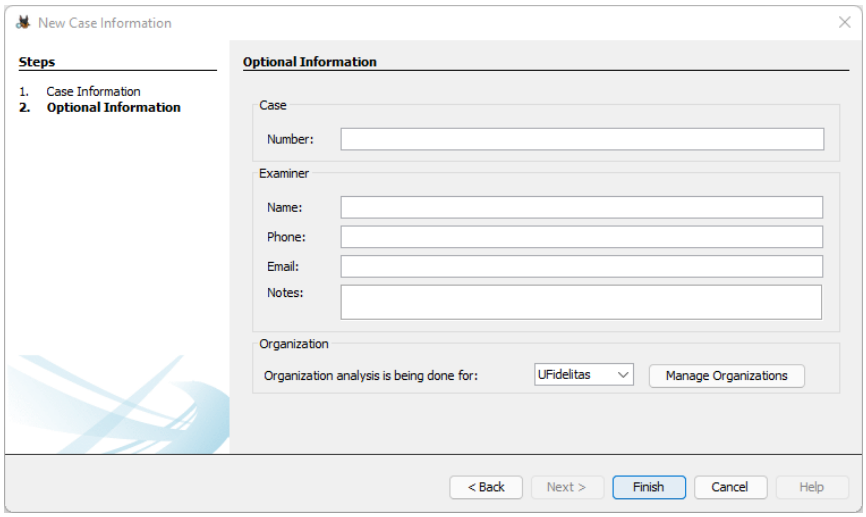
01. Una vez que el aplicativo está ejecutándose, tiene 3 opciones, abrir un caso en el que ya haya estado trabajando, abrir un caso reciente o crear un nuevo caso. Haga clic en New Case.



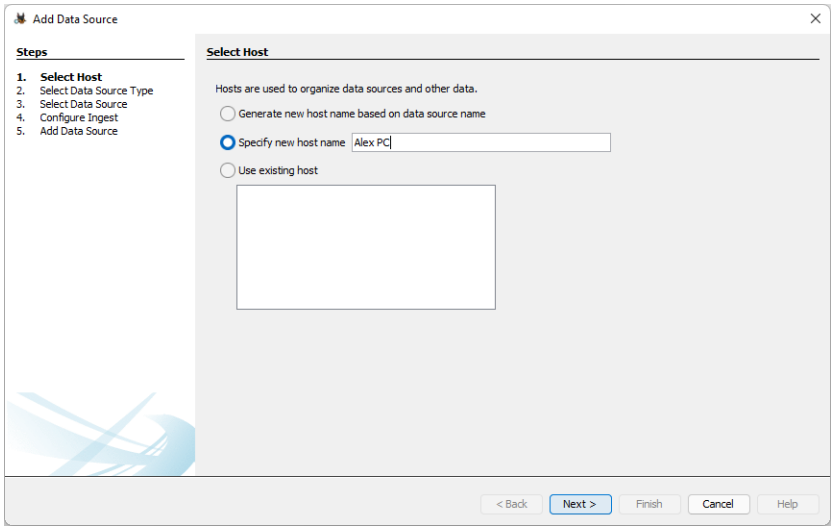
02. Asigne un nombre al caso y una ruta para almacenar la información del mismo, una vez realizado esto, haga clic en Next.



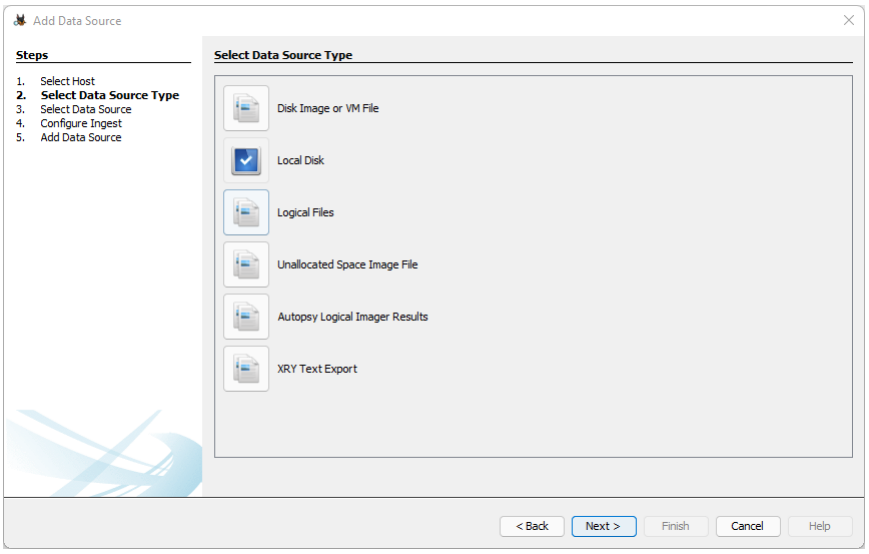
03. Para casos reales, se recomienda completar toda la información opcional del caso, ligar la organización con la cual estamos trabajando, nombre de los investigadores, etc. Una vez introducida toda esta información, haga clic en Finish.



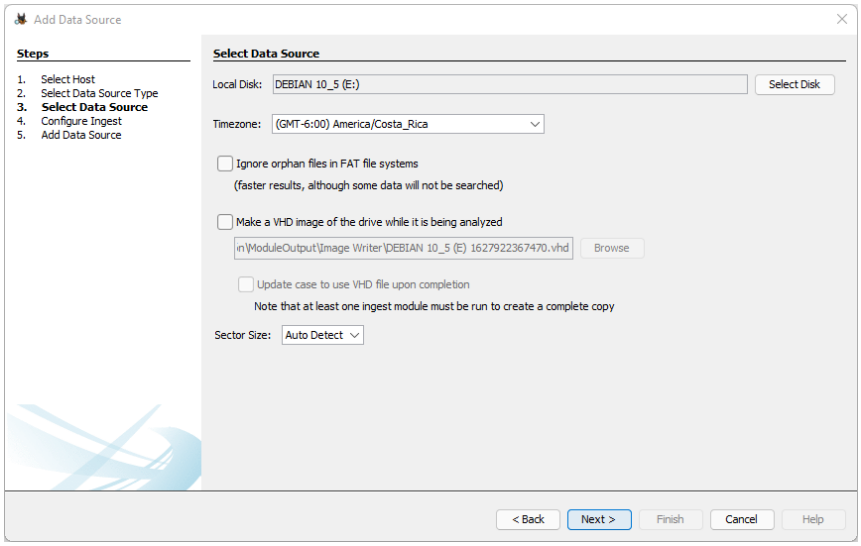
04. Los siguientes pasos le permitirán ir introduciendo las fuentes de datos que serán analizadas, agregue el nombre de su máquina y haga clic en Next.



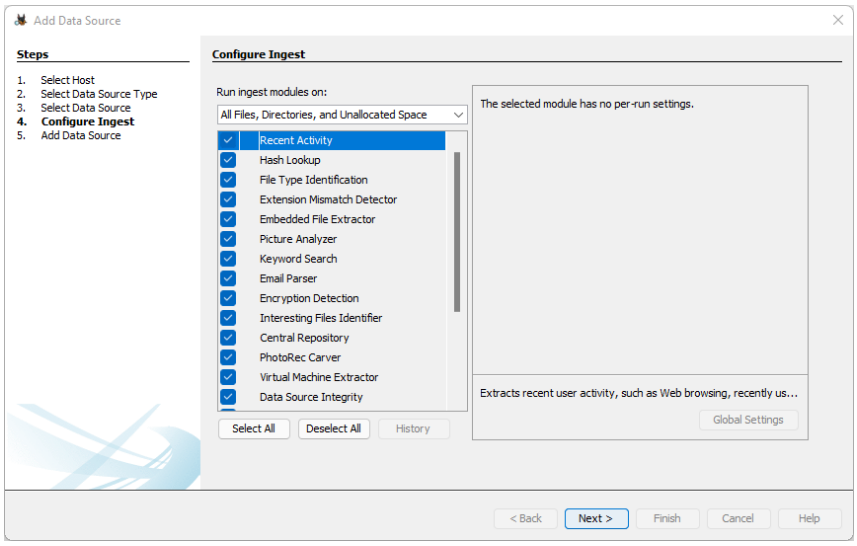
05. Tome una unidad USB y cree un archivo de texto en la raíz, escríbale su nombre como nombre del archivo. Dentro del archivo de texto, escriba su número de cédula, guarde el documento. Abra nuevamente el archivo para asegurarse de que el contenido está en la llave USB y cierre el archivo.
06. Borre el archivo de la llave USB.
07. Conecte el USB a su equipo, preferiblemente de baja capacidad para acelerar el proceso. Elija la opción Local Disk.



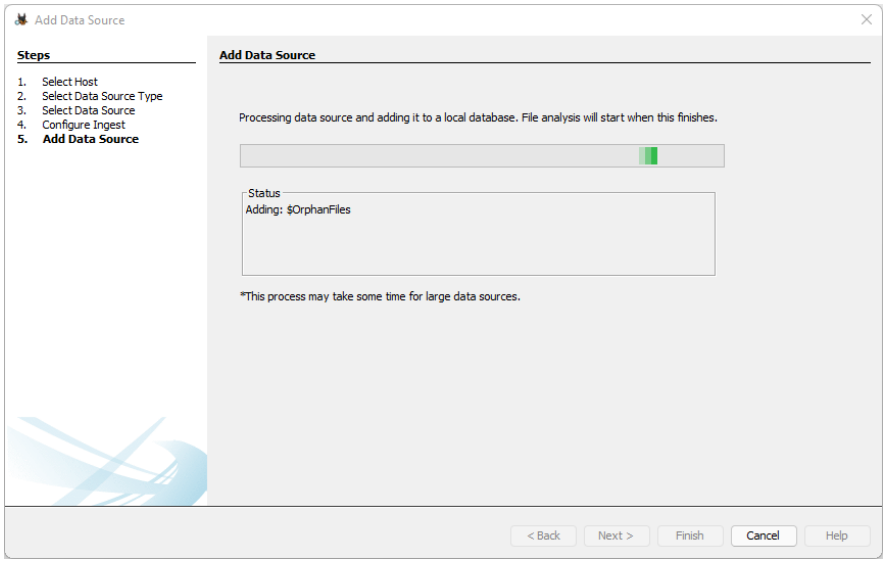
08. Seleccione el disco USB que acaba de ingresar en el Local Disk, configure el Timezone y presione Next.



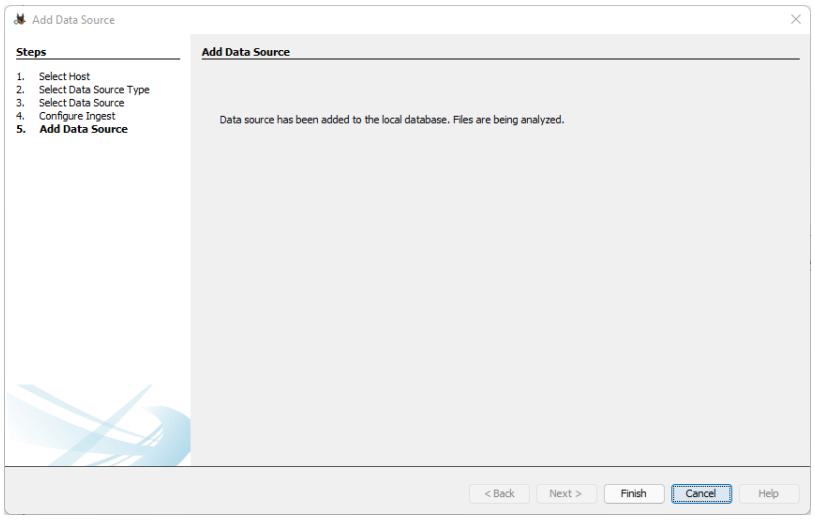
09. Presione Next nuevamente para configurar la ingesta de la data y luego Finish para procesar la muestra. El proceso tardará varios minutos dependiendo de la capacidad de su equipo de cómputo y del tamaño del disco USB (le recomiendo que utilice un Pendrive de 4 u 8 GB cómo máximo)



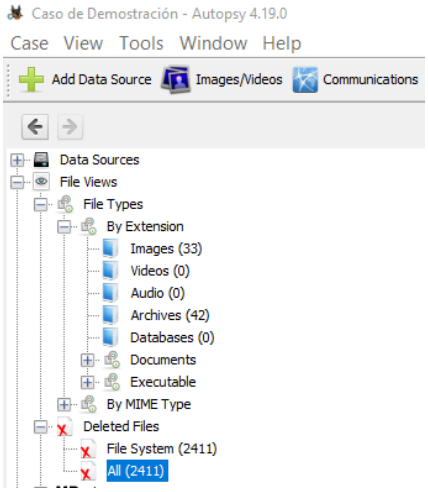
10. Sea paciente en esta parte del proceso…



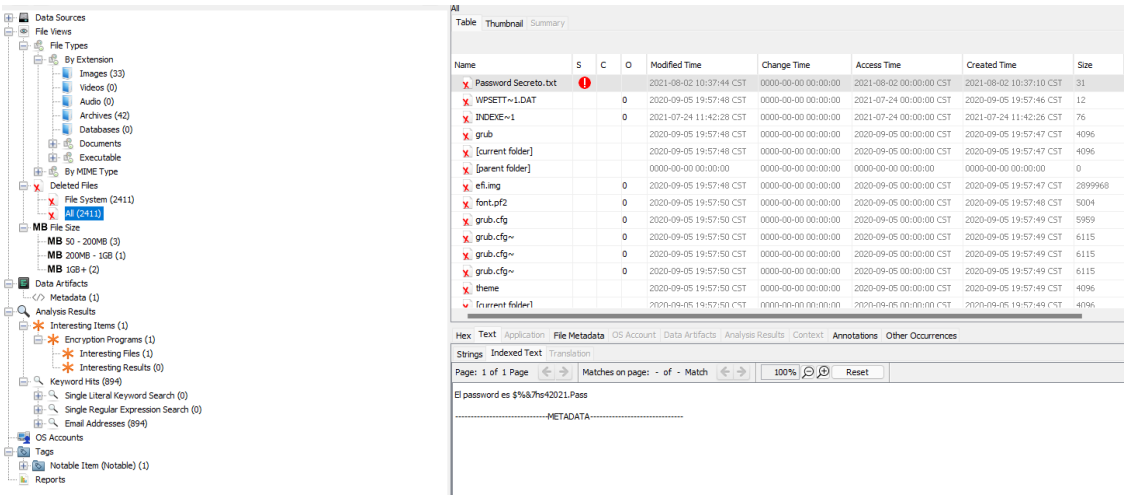
11. Una vez finalizado el proceso, debe hacer clic en Finish.



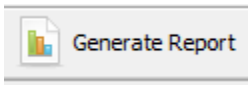
12. En el árbol de la izquierda, ubique la sección de archivos borrados y trate de visualizar el archivo que anteriormente borró de la USB. En mi caso particular, en la llave que utilicé se encontraron 2411 archivos eliminados



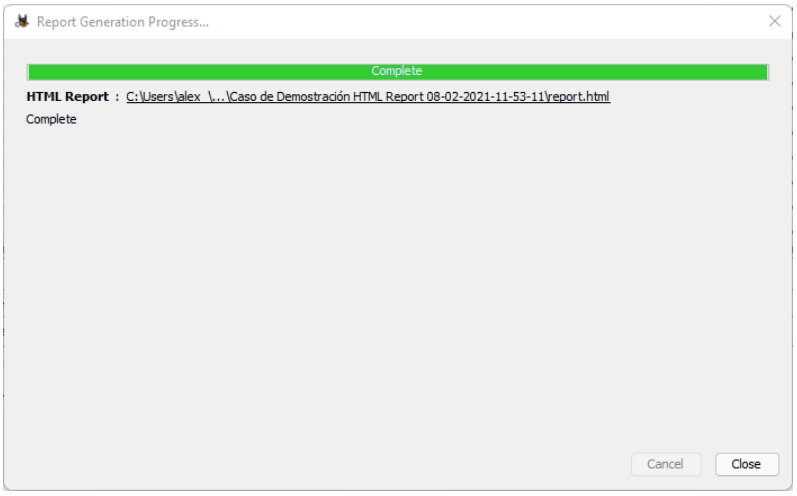
13. En la ventana de la derecha se muestran los archivos, haga clic sobre algún archivo de interés y márquelo como Notable (Clic derecho > Add File Tag > Notable Item)



14. Genere un reporte del caso en formato HTML. Agregue algún contenido para el Header y Footer si así lo desea. Presione Next en las siguientes ventanas.



15. Abra el informe generado.



16. Busque en los Tagged Files y encontrará el archivo que rescatamos.