



www.eysglobal.com



MÓDULO 3

PRACTICA 2:

Realización práctica del proceso de recopilación de evidencias y análisis de las mismas. Los asistentes se familiarizan con el proceso y con las herramientas más comúnmente utilizadas en el Análisis Informático Forense.

3.1 Recopilación de evidencias

- Metodología de trabajo
- Diferentes herramientas para clonado de discos duros y teléfonos móviles
- 3.2 Análisis de datos y reconstrucción de evidencias

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



RECUVA : Es un programa que puedes usar para recuperar imágenes, música, documentos, videos o cualquier otro tipo de archivos en tu disco duro, tarjetas de memoria, disquetes, iPod o reproductor de MP3 o USB. Normalmente, cuando usted o Windows eliminan un archivo, una gran parte del archivo se deja atrás, incluso si no puede verlo en el Explorador de Windows. Recuva recorre sus medios de comunicación (excepto CDs, DVDs y otros medios ópticos) y reúne las piezas para que pueda recuperar los archivos que necesita. Recuva también tiene la capacidad especial de borrar de forma segura los archivos recuperados.



DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



Las características de Recuva son:

- Recupera todos los archivos que han sido borrados en el ordenador.
- Recupera los datos que se han perdido en un disco duro dañado o que se ha formateado.
- Recupera los correos electrónicos que se han eliminado.
- Recupera la música perdida en dispositivos iPod.
- Restaura documentos de Word que no se han guardado.
- Incluye un sencillo y a la vez intuitivo asistente.
- Hace un análisis en profundidad de la unidad en la que tenemos que efectuar la recuperación.
- Elimina de forma segura todos los archivos que no deseamos, de los que no queremos que queden rastros.
- Existe una versión portátil o portable del programa.
- Soporta todas las versiones de Windows en una gran cantidad de idiomas.



DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



Iniciemos con esta práctica : Descarga, instalación y prueba con Recuva:

1 El programa se puede descargar de la página <https://www.piriform.com/recuva>.



Imagen :Captura de descarga Recuva

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



2. Dar clic donde indica la flecha para descargar la versión libre



DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



3. Se descarga del servidor de Piriform como lo muestra la imagen

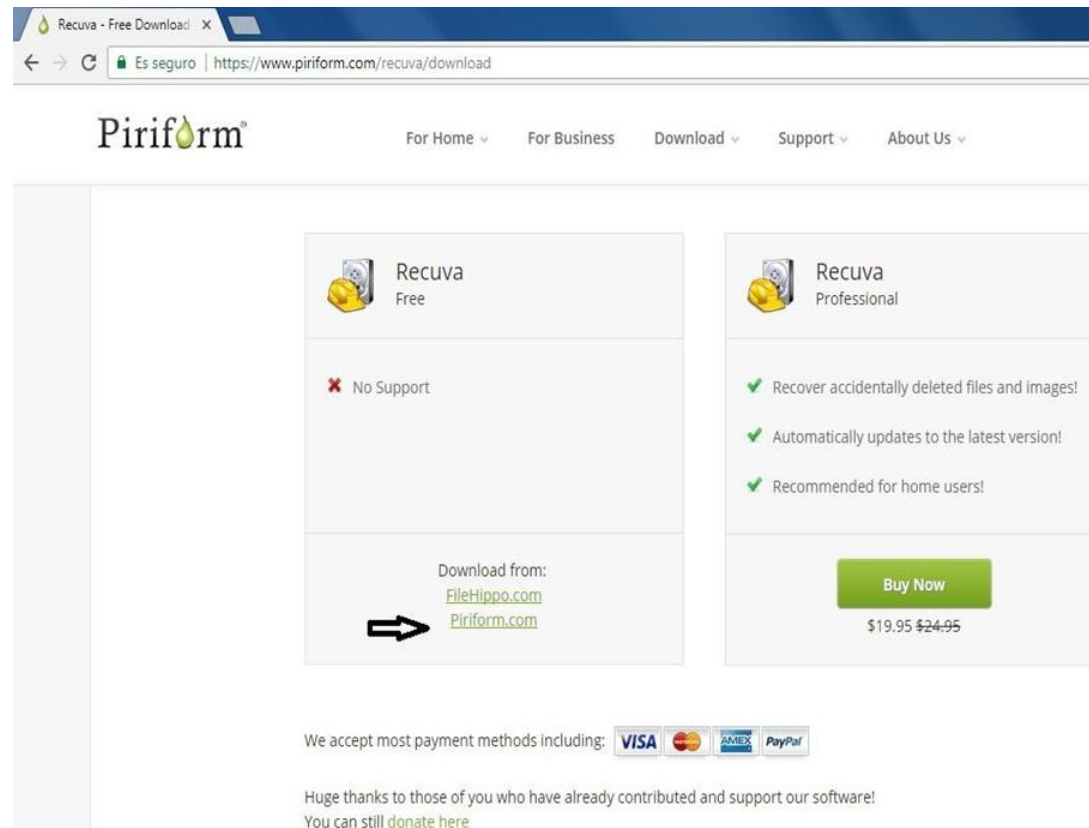


Imagen : Captura descarga versión free

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



4. Después de descargar el programa, lo ejecutamos y le damos en la opción “install” como muestra la imagen siguiente.



Imagen : Captura instalación Recuva

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA

5. Cuando haya terminado la instalación, se da clic en la opción “Run Recuva”.



Imagen : Captura abrir recuva

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



PRUEBA DE RECUVA

Para la prueba se va a utilizar un computador portátil HP, el cual tiene un sistema operativo Windows 7 con particiones C y D, se realizará un borrado de información contenida en una carpeta en la unidad D y se eliminará también de la papelera de reciclaje y se procederá a reiniciar el equipo. La carpeta que se va a borrar tiene un total de 37 elementos entre archivos e imágenes.



DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



La siguiente imagen muestra la información que se borrará

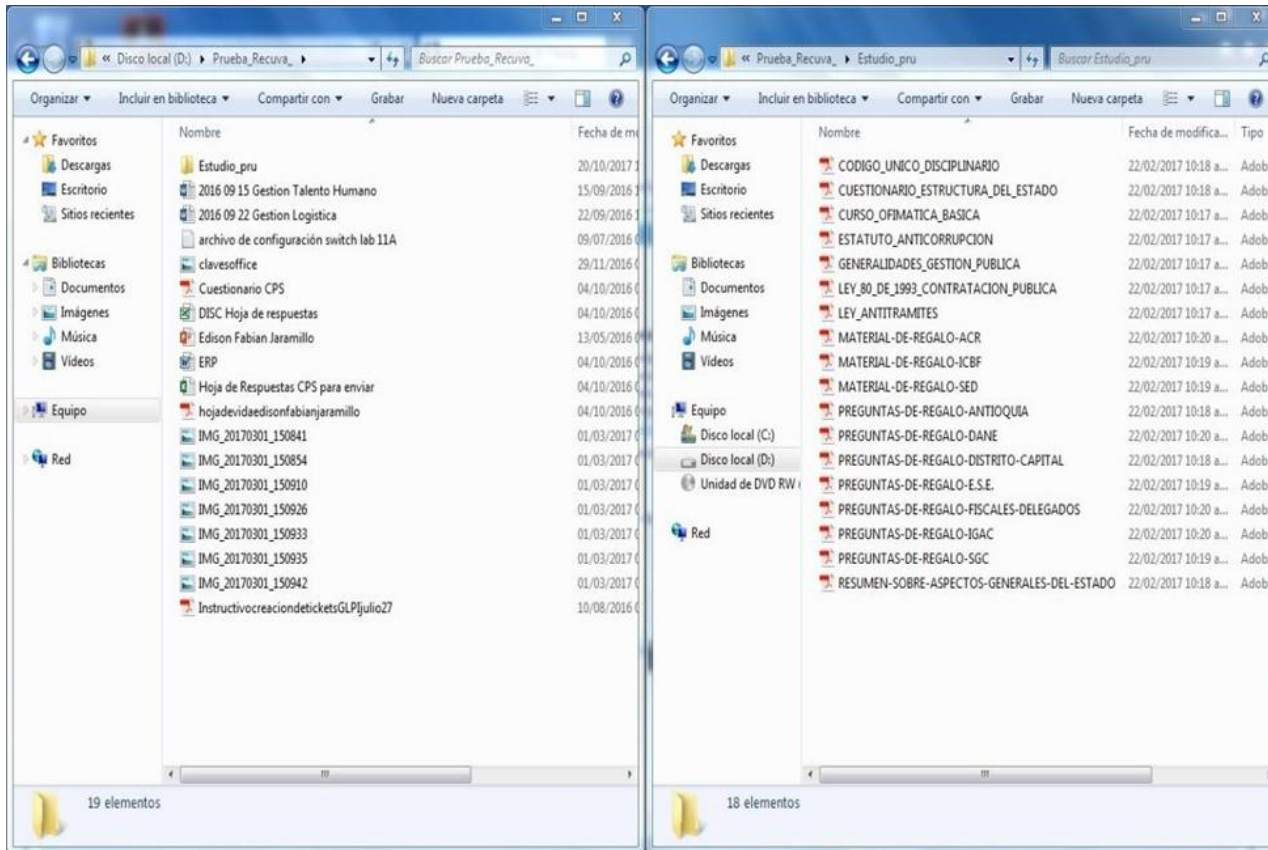


Imagen : Captura archivos a borrar

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



A continuación, la imagen muestra que la carpeta ya no está presente en la unidad D ni en la papelera.

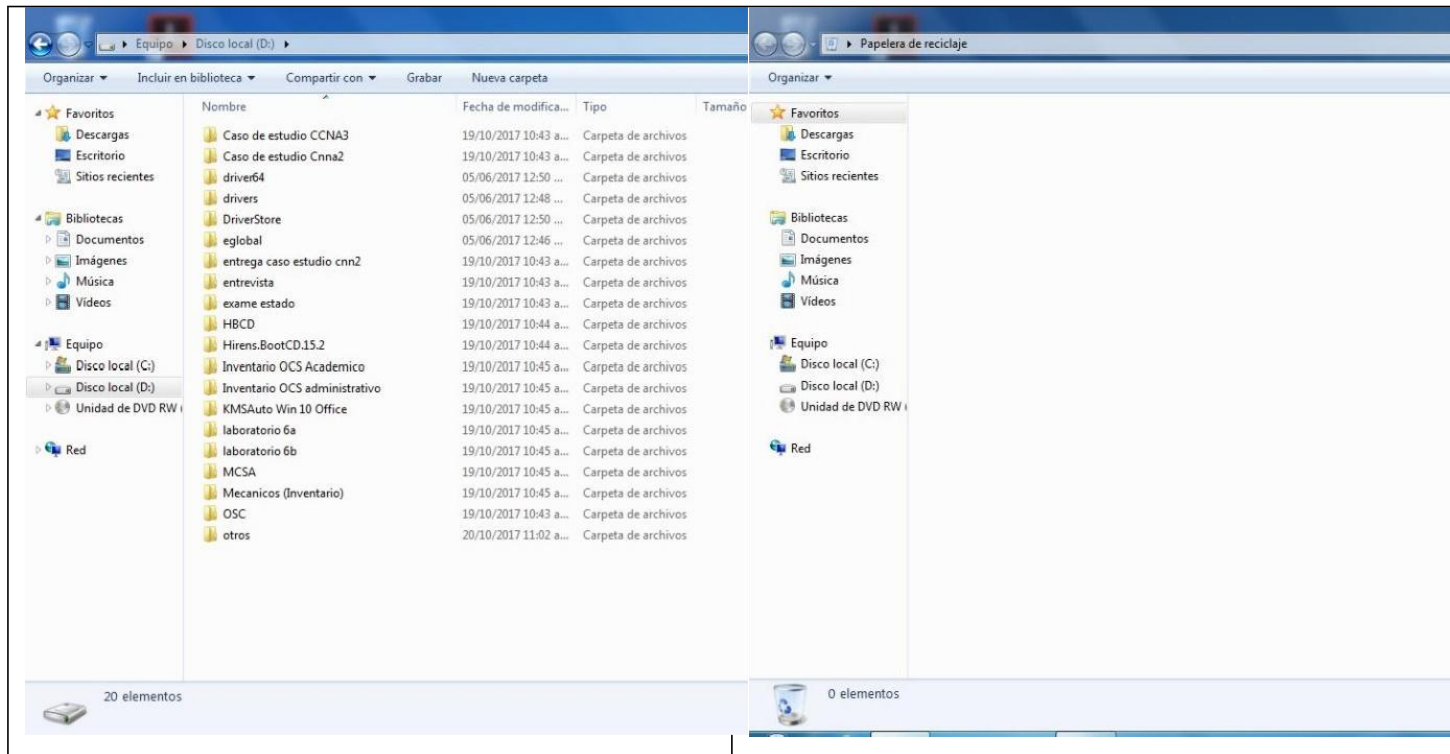


imagen : Captura archivos borrados

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



1. Se procede a abrir el programa Recuva y se le da en la opción siguiente.



Imagen : Captura asistente Recuva

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



Imagen : Captura tipos de archivos a recuperar

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



3. Seleccionamos la ubicación o la unidad donde se encontraban los archivos borrados, Clic en “Siguiente”.

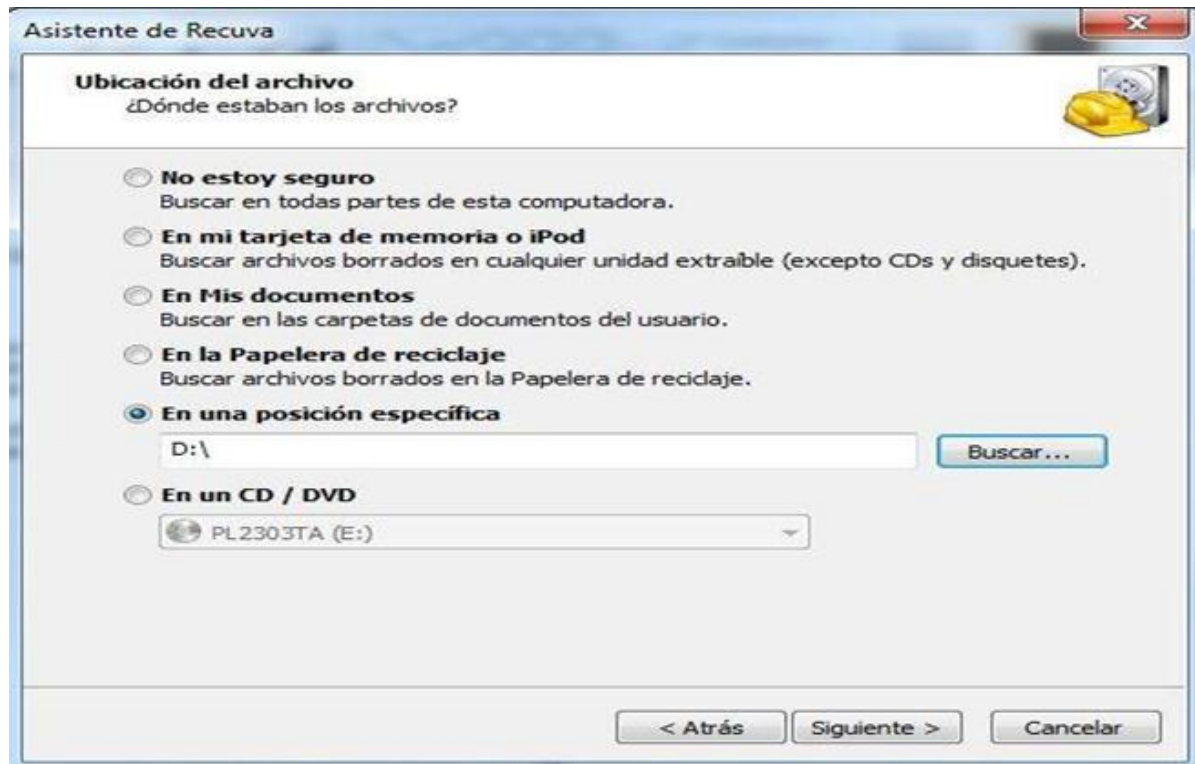


Imagen : Captura unidad que se escaneara

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



4. Se selecciona la opción “Activar escaneo profundo” para que el programa realice un escaneo más detallado y se le da clic “iniciar”.



Imagen : Captura Inicio proceso de recuperación

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA

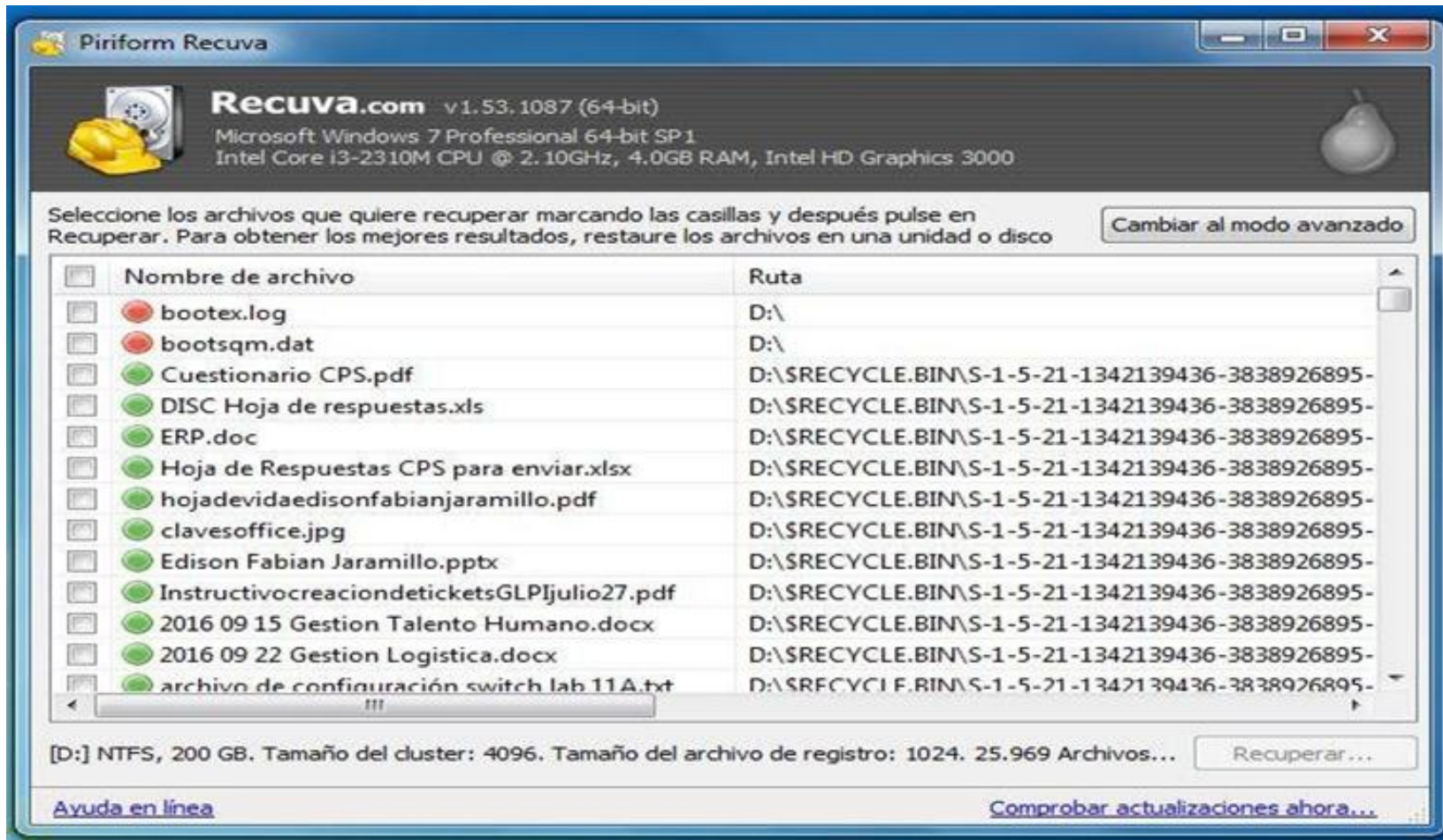


Imagen : Captura archivos a recuperar

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



6. Se seleccionan los archivos en verde los cuales vamos a proceder a recuperar y también la ruta donde se van a recuperar, se recomienda que no sea la misma de donde se realizó el escaneo.

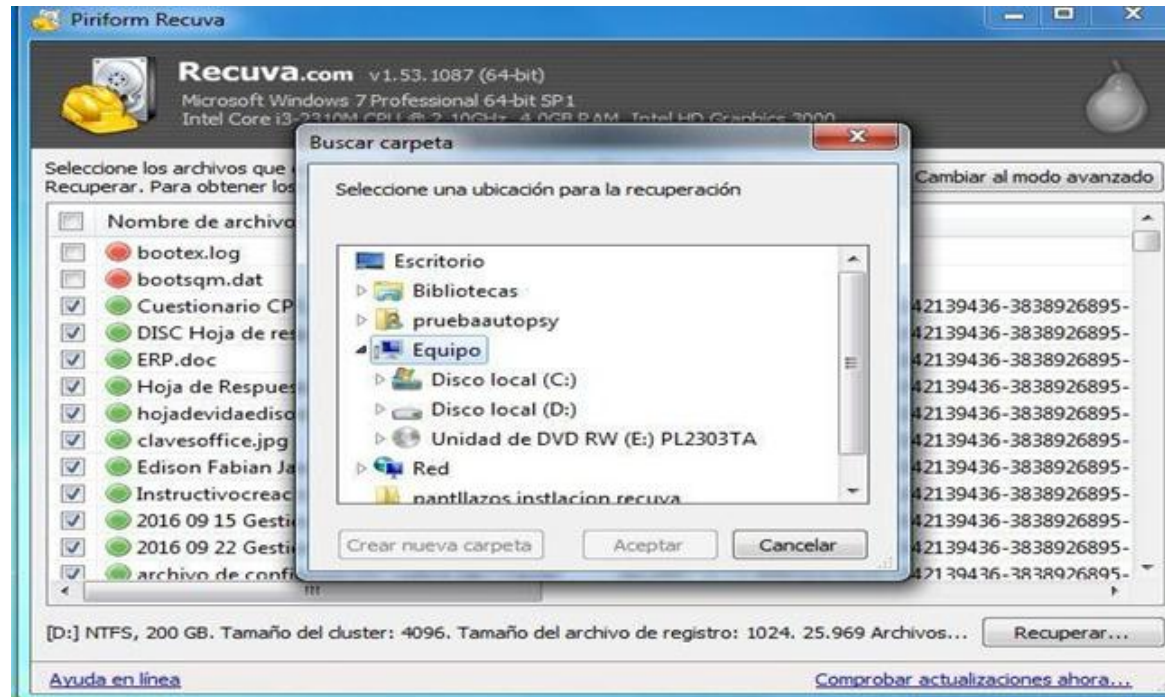


Imagen : Captura de selección de destino para los archivos recuperados

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA

7. Se comienza el proceso de recuperación a la nueva ruta, en esta prueba se recuperaron un total de 36 archivos, lo que quiere decir que la herramienta recuperó aproximadamente un 97.3% ya que el total de archivos eliminados fueron 37.

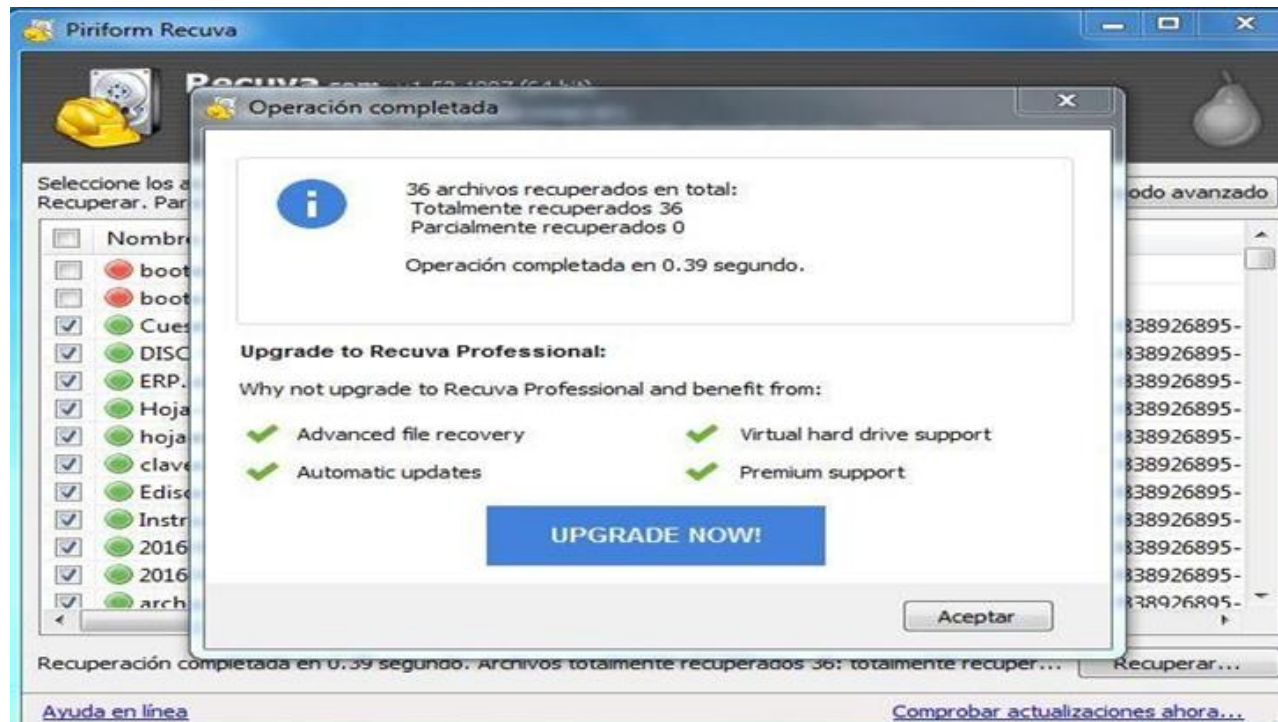


Imagen : Captura total archivos recuperados

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



8. La imagen siguiente muestra los archivos recuperados.

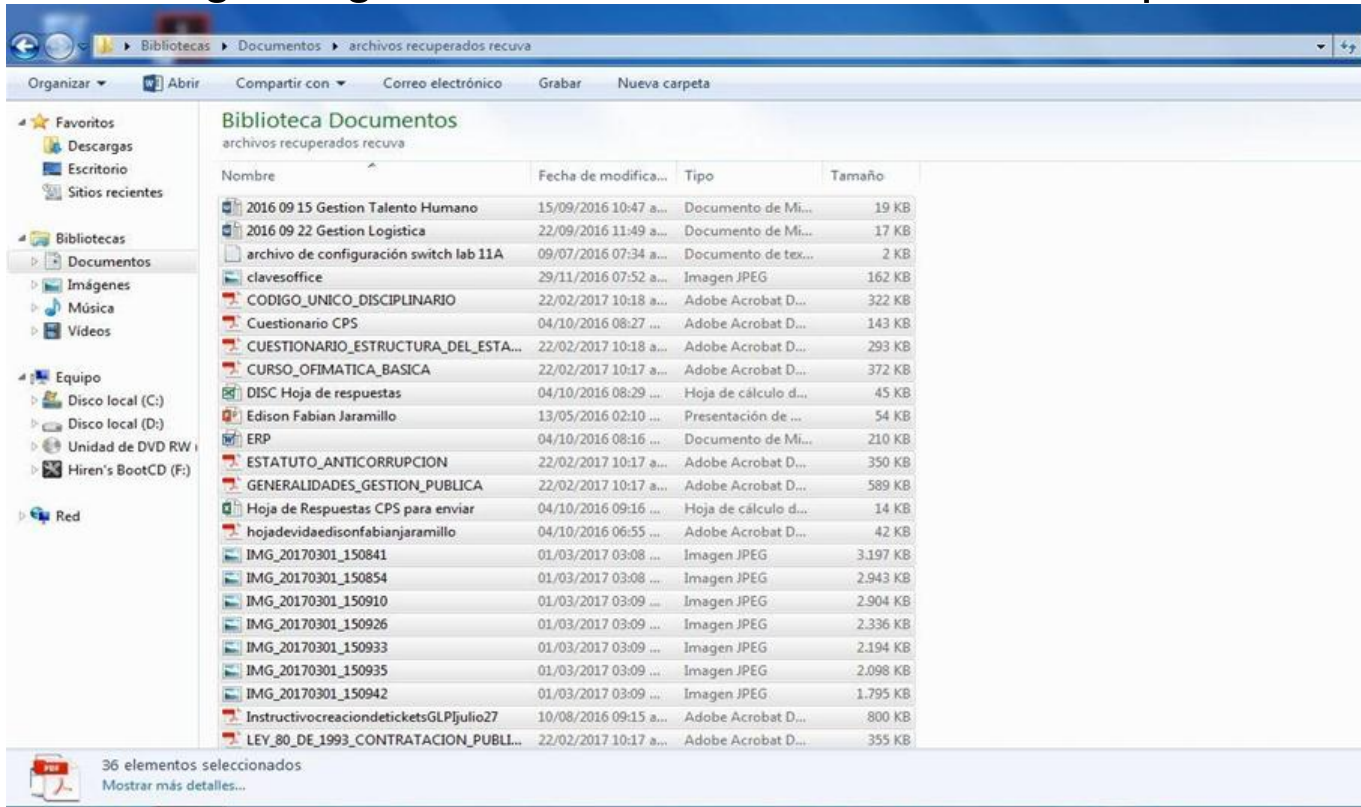


Imagen 45: Captura archivos recuperados

DESCARGA, INSTALACIÓN Y PRUEBA CON RECUVA



Conclusión de la herramienta Recuva:

Los resultados en eficacia y en tiempo de recuperación para esta prueba son muy buenos, recuperó 36 de 37 archivos borrados. Es importante resaltar que los resultados pueden variar de acuerdo con diversos factores como: la cantidad de archivos que se quieren recuperar, si los archivos han sido sobrescritos, el tiempo que estuvieron eliminados dichos archivos y que tipo de versión de la herramienta se utilice para la recuperación (libre o comercial), entre otros.

