MANUAL PARA AMISTADES VERDES: HERRAMIENTAS UTILES PARA WINDOWS

Y UN PEQUEÑO EXTRA

BY: Alpra_tdm

Temas

Aclaraciones

Este documento se hizo como celebración de 200 seguidores en la cuenta, :) gracias por eso. Lo que se prometió en la storie de amistades verdes fue “Un paquete de Herramientas útiles para Windows”, la pequeña introducción que he puesto es mas un extra para los interesados en el tema de la seguridad informática.

Realmente no encontraras nada referente a herramientas de hacking, ya que no fue lo que prometí. (por ahora)

Trate de que:

- No haya tantos tecnicismos.
- No haya un lenguaje tan formal.
- Pequeños retos.

En resumen, trate de hacerlo digerible para cualquiera.

Como fue prometido, en esta ocasión te daré un par de herramientas útiles para situaciones comunes.

Si te gustan las herramientas házmelo saber, así sabre si escribir un poco acerca de cómo funcionan por dentro.

Pd si me envías que realmente hiciste los retos, me asegurare que seas de las primeras personas que reciban las siguientes ediciones de los manuales de amistades verdes.

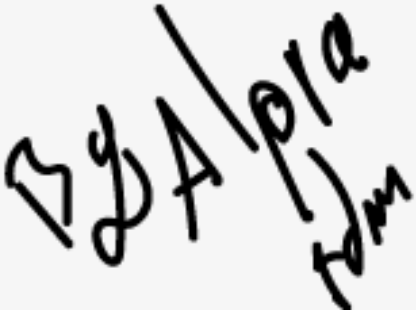
DISCLAMER

La idea, proceso y resultado final de" MANUAL PARA AMIGOS VERDES: INTRODUCCIÓN Y HERRAMIENTAS WINDOWS" es de fines educativos. Cualquier mal uso que se le dé a la información y herramientas de esté, serán responsabilidad del lector.

Agradezco el apoyo a la cuenta y a las personas que han hecho que crezca, el material creado es con el fin de que entiendas los riesgos en el mundo de la tecnología, estos escritos tómalos como divulgación ya que estudiar seguridad informática requiere años de estudio y prácticas.

No te desmotives y, al contrario, prepara tu curiosidad para aprender cualquier tema que se te ponga de frente. Lograr inspirarte a el camino STEAM es algo que me motiva, Latinoamérica está llena de personas capaces, tú estás ahí, ten diciplina y no olvides soñar en grande.

S	**Science**	**Ciencia**
T	**Technology**	**Tecnología**
E	**Engineering**	**Ingeniería**
A	**Arts**	**Arte**
M	**Maths**	**Matemáticas**



Hackers, colores y fantasías

Apuesto que desde que comenzaste a usar internet has escuchado la importancia de que no te hackeen, después te has preguntado ¿Cómo puedo hackear a alguien?, miraste uno o dos tutoriales y te diste cuenta de que tal vez no era tan sencillo como parecía. Pues intentemos sacarte esa espinita, pero primero que nada aclaremos que es un hacker.

Hace unos años la RAE definía “hacker” como “pirata informático”, hoy la definición ha cambiado a una más acertada:

“**Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora**”.

Este cambio se debe a que la primera definición denigraba el trabajo de grandes hackers tachándolos de ciber delincuentes. Es como comparar a un militar con un ladrón por el hecho de usar un arma. La gran diferencia es el conocimiento, la aplicación y la intención con la que se actúa.

En la comunidad de ciberseguridad la definición de hacker es poco estandarizada, también se llega a definir como hacker a una “persona que puede romper las reglas de un sistema para mejorar el proceso o resultado” o también a creadores muy respetados como “Julian Assange” o “Linus Torvalds” que han hecho aportes extremadamente grandes al mundo de la tecnología.

Algo en común es que el concepto de hacker siempre se tiene como el mayor logro dentro del gremio, es por eso por lo que en la actualidad existe un dilema de cómo se debe preparar alguien que posee este título y quien lo puede otorgar.

No desde hace muchos años se comenzó a tratar de estandarizar el tipo de hacker que se podía llegar a ser, utilizando colores de sombrero o colores de equipo, así que veamos un poco de cómo han avanzado las clasificaciones durante el tiempo.

Antes (Aún se usan estos conceptos)

Hackers: se les considera expertos a lo referente a la informática como en: lenguajes de programación de bajo y alto nivel, arquitectura de software, redes, protocolos, servidores, etc.

Crackers: Básicamente los hackers malos :)

Sniffers: Personas que interceptan, leen y buscan administrar el tráfico de la red.

Phreakers: Personas que trataban de obtener llamadas gratis a través de sabotear las redes telefónicas.

Spammers: Personas que saturaban los servicios de correos electrónicos para colapsar los servidores.

Piratas informáticos: Personas que se dedican a romper la seguridad del software pago para distribuir el mismo, pero de forma gratuita e ilegal.

Lammers, Scripts kiddies, clic kiddies: Aquellos que usan las herramientas de los hackers, pero no comprenden el trasfondo del funcionamiento.

Cabe aclarar que no hay mucha diferencia de tiempo entre el antes y ahora, estaríamos hablando de 3 o 4 décadas

Ahora

Por Sombreros (directamente se les hace llamar hackers, pero se les separa por la intención):

Black hat: Hackers que se dedican a atacar el sistema y sacar provecho personal.

Gray hat: Hackers que se dedican a un punto intermedio.

Ejemplo: Encuentran una vulnerabilidad en un sistema y lo notifican, a la vez que esperan un pago por corregirlo.

White hat: Hackers que se dedican a proteger el sistema de manera que los usuarios permanezcan seguros.

Por equipos:

Red team: Equipos especializados en romper la seguridad de un sistema.

Purple team: Equipos encargados de optimizar la seguridad a través del uso de técnicas del red team y blue team.

Blue team: Equipos especializados en proteger la seguridad de un sistema.

Fantasía

A mí me parecer depende del concepto que tengas de “Hacker”, si para ti ser hacker es defender y atacar un sistema sin importar si entiendes lo que haces, solo usar herramientas de terceros y no saber ni programar, pues tal vez sí, pero no esperes encontrar trabajo ni que la comunidad de la tecnología te tome enserio, incluso por la descripción te habrás dado cuenta de que serias un Script Kiddie.

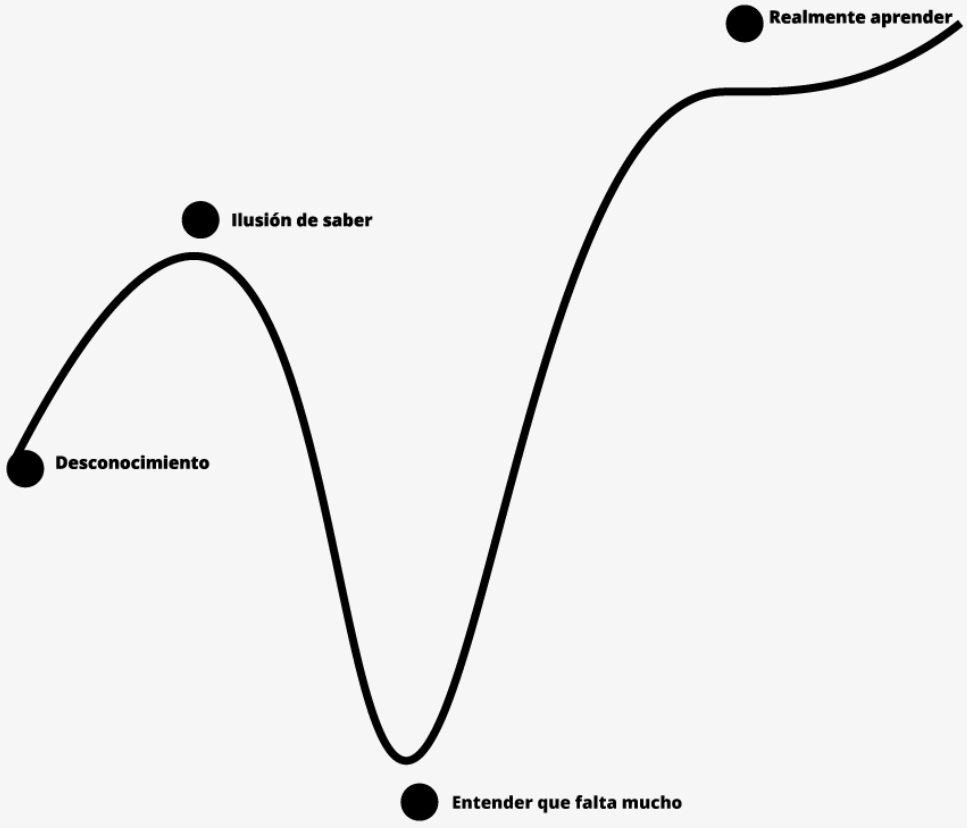
Es como buscar un guardaespaldas, das por entendido que sabe usar arma, como funciona y que hacer en caso de que falle. El secreto de como eres percibido ante el gremio depende de cómo te autoproclames y por qué. No es lo mismo decir “tome un curso de un mes, soy hacker” a “tome un curso de un mes, ahora estudio para ser hacker”.

Esto tampoco debe mal interpretarse con la curiosidad de experimentar pues también puede ser una buena introducción y motivación para aprender a profundidad. Conocer un poco de este tipo de herramientas para aprender cómo no ser víctima de ellas tampoco está mal.

Demos un respiro y recordemos algo vital para cualquier cosa que quieres aprender.

Así se ve el paso del aprendizaje, así que disfruta el proceso.

En caso de que empieces en este camino te deseo el mayor de los éxitos.



Pentesting

Prueba de penetración

Un pen-testing, es un conjunto de procedimientos que buscan vulnerabilidades en un sistema informático con el fin de reportarlas y corregirlas.

Existen distintos pasos a seguir en un pen-test, pero podemos resumirlas en estas cinco:

- Reconocimiento
- Análisis
- Explotación
- Post - explotación
- Documentación

Por ahora no te llenare de datos acerca de estos pasos, ya que hare un manual enfocado al pen-testing.

Algo que no hemos dejado claro totalmente es que si eres un hacker bueno y profesional (Hacker ético), puedes conseguir trabajo.


CIBERSEGURIDAD

Google y Microsoft acuerdan con Biden invertir 30 mil millones en ciberseguridad

El presidente de EU, mantuvo una reunión con representantes líderes del sector privado y de la educación para discutir el esfuerzo necesario para abordar las amenazas para la seguridad cibernética que tiene por delante el país.


Hace 1 mes

Recomendada

Ethical Hacker Sr

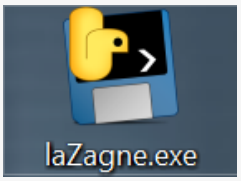
$45,000 - $47,000 Mensual

- Seguro de vida
- Seguro de gastos médicos
- Flex time (home office, viernes corto)

Mnemo Evolution & ...

Polanco I Sección, Miguel Hidalgo, CDMX

MNEMO



La Zagne

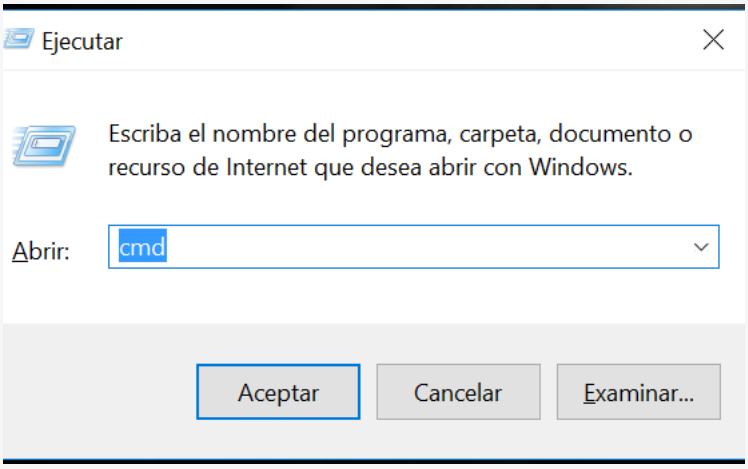
Por si las dudas, solo te recuerdo que: Acceder a información de terceros sin autorización es un delito.

Reto:

https://github.com/AlessandroZ/LaZagne/releases/

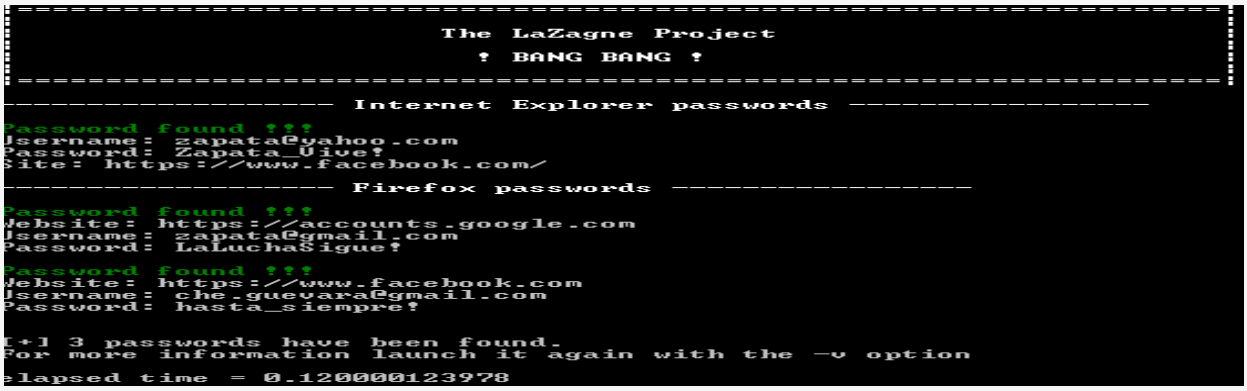
Te recomiendo desactivar Windows defender o tu antivirus

Abrimos la consola con win + r y escribimos cmd



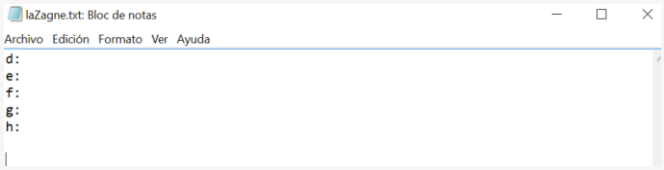
Escribimos la ruta de la aplicación en la consola

Y veras la magia :)

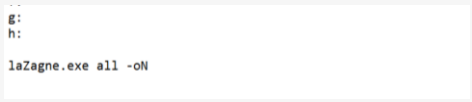


Automatizar el proceso en una USB:

En este proceso se indicará en un documento de texto plano que busque los puertos de salida más comunes para encontrar la memoria.



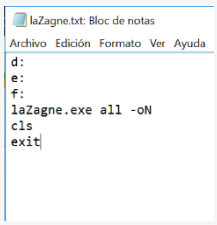
Después indicaremos que abra nuestra aplicación.



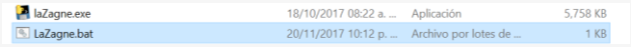
Escribimos

Cls para que limpie la pantalla

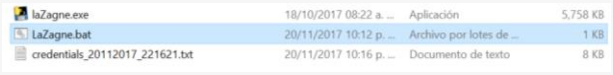
Exit para Salir



Cambiamos la extensión de .txt a .bat



Al ejecutar el .bat nos guardara un txt con las credenciales



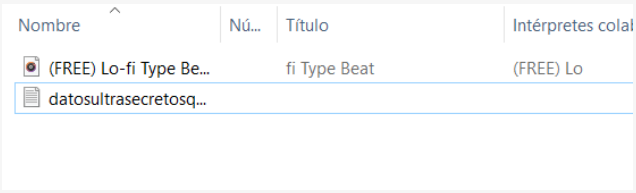
Deep sound

http://jpinsoft.net/DeepSound/Download.aspx?Download=LastVersion

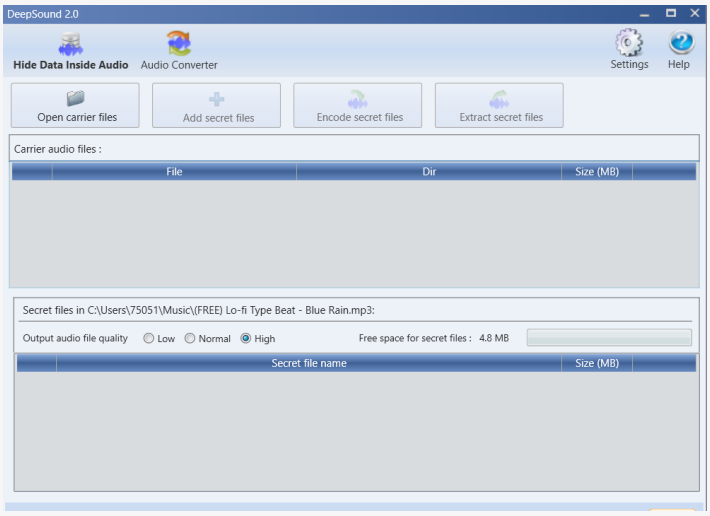
Vamos a ocultar datos en una canción, en este caso un archivo de texto, pero también puedes intentar con otro formato de archivos

Reto: intenta ocultar distintos tipos de archivos.

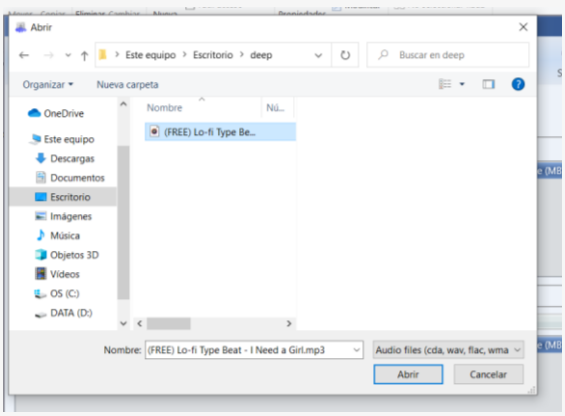
Alistamos en una carpeta 2 archivos, una canción (.mp3) y un texto(.txt)



Al iniciar el programa vamos a seleccionar la opción de “Open Carrier files”

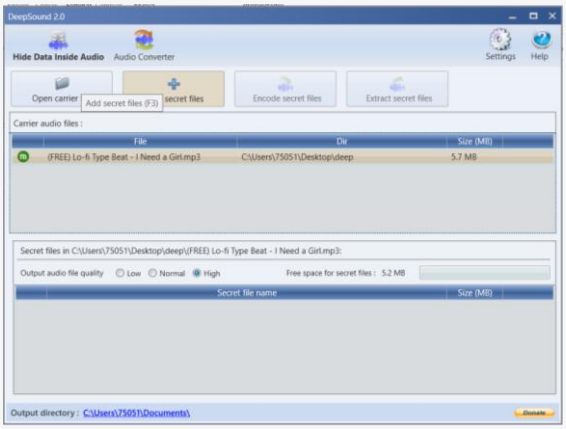


Vamos a dirigirnos a la carpeta donde tenemos nuestros archivos y elegimos la canción.

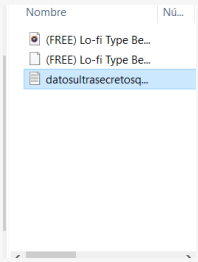


Podremos ver que el archivo ya fue cargado en el programa.

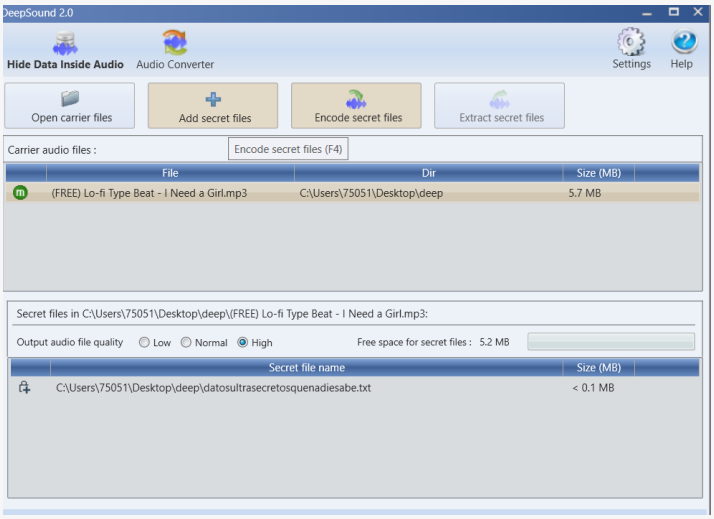
Seguido a esto elegimos la opción “add secret files”.



Aquí seleccionaremos el archivo a esconder, recuerda hacer el reto 👀

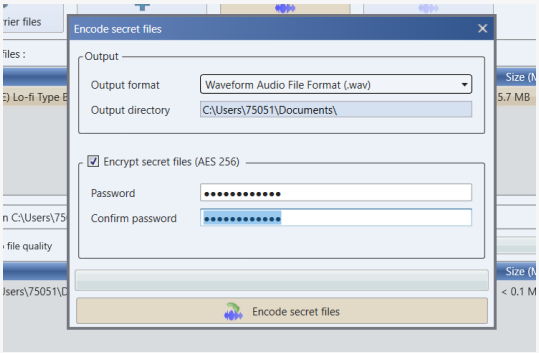


Cuando demos clic en “Encode secret files”, se hara la codificación para que nuestros archivos secretos se oculten en la canción.

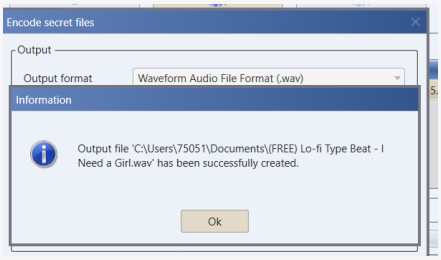


Ya casi finalizamos, solo nos falta configurar el nombre y la constraseña en caso de que lo requieras.

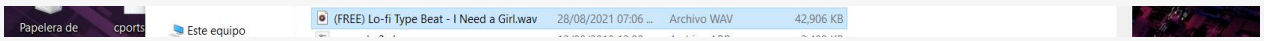
En este mismo apartado veremos la ruta donde se encontrara el archivo que resultara despues de finalizado el proceso de codificación.



Al final nos mostrara una notificación cuando el proceso haya terminado.

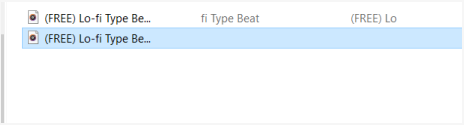


Al finalizar podremos verificar que nos develve un archivo de audio.



Proceso inverso

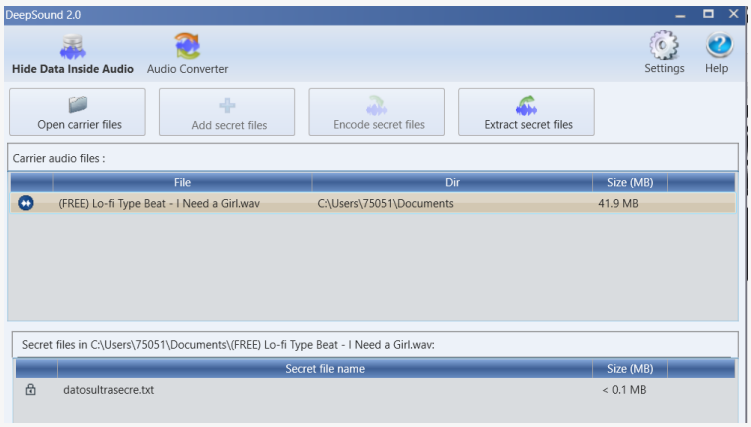
Aquí vamos a tomar el archivo de audio codificado y extraer la información oculta



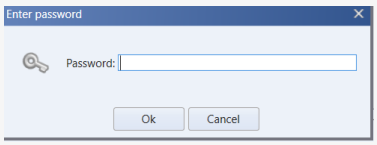
Arrastramos la canción codificada o damos clic en open carrier files.

En automatico el progrmama detecta si hay un archivo escondido, si aparece un candado a lado del nombre del archivo oculto quiere decir que tiene contraseña.

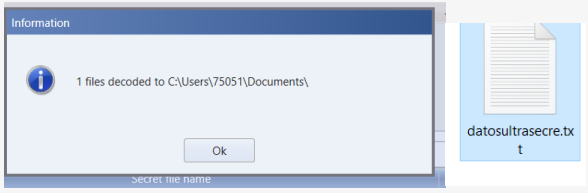
Elegimos la opcion “extract secret files”



Nos mostrará una ventana donde nos pedirá la contraseña.



Cuando hayamos introducido la contraseña el progrma nos enviara una notificación con la ruta del archivo que acaba de extraer



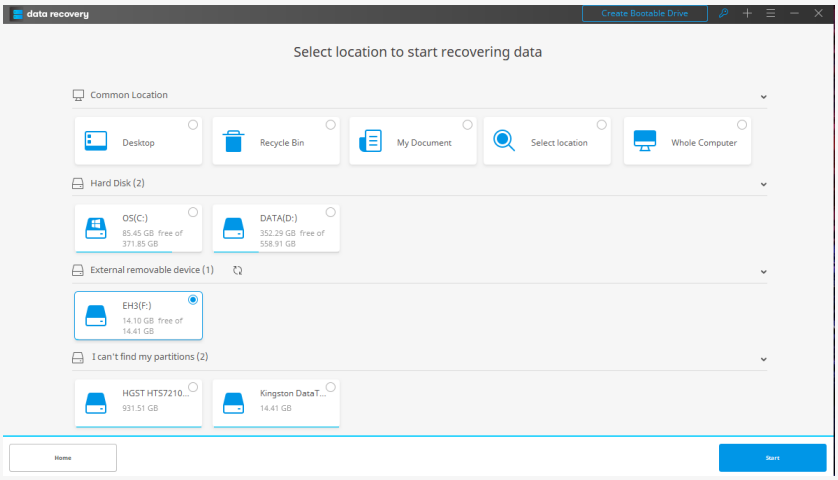
WONDERSHARE DATA RECOVERIT

Es una herramienta que ayuda a recuperar archivos eliminados.

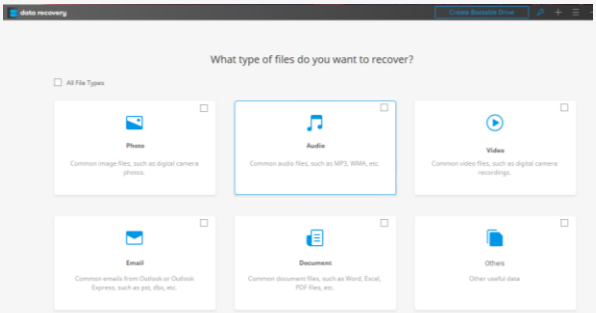
Funciona en Windows y Mac, pero tiene un precio por suscripción mensual.

Supongamos que ya hiciste tu suscripción mensual

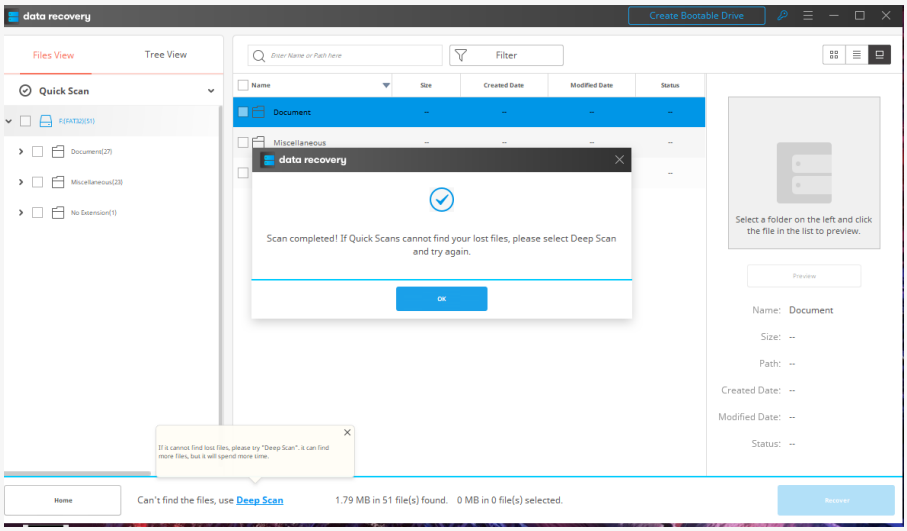
Cuando abrimos el programa comenzara aescanear nuestra computadora para comprobar si hay algun dispositivo externo como una USB, una vez finalizado nos arrojara las opciones de las locaciones donde puede hacer una recuperación.



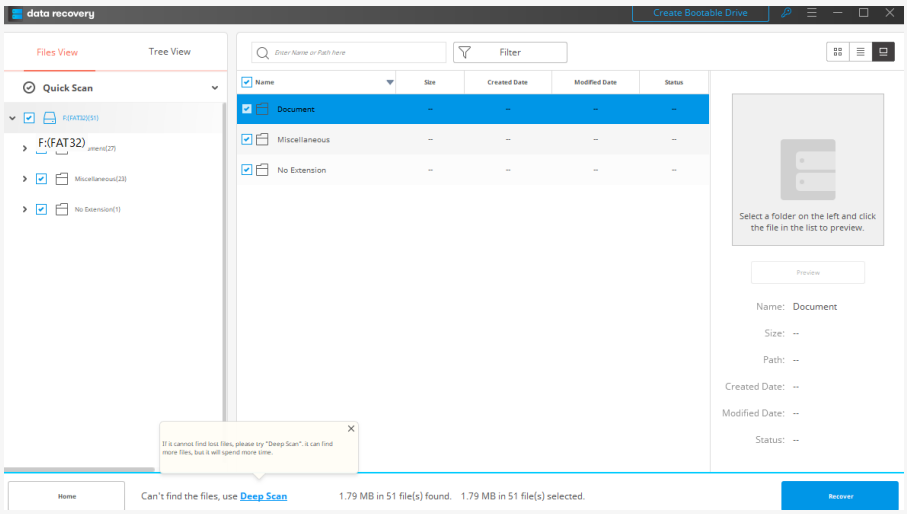
Seguido de este paso, nos mostrara el tipo de archivos que puede recuperar, en caso de que busquemos alguno en específico, si no es el caso, marcamos la casilla de “All file types” para recuperar todo lo que podamos.



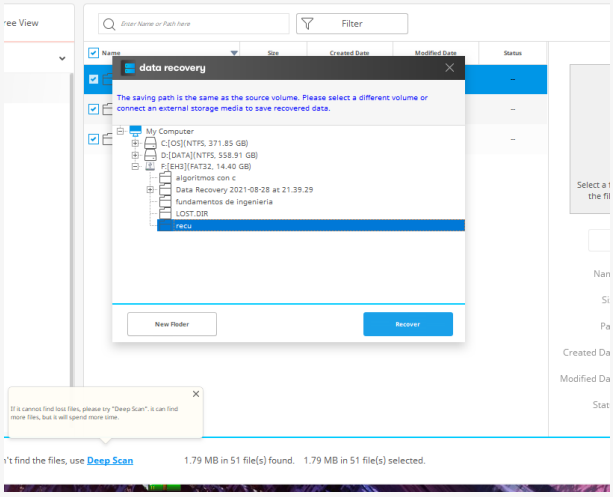
Al dar continuar en el paso anterior, se mostrara una barra de avanze en la parte superior del prgrama donde nos indica el progreso de analisis de archivos que se pueden recuperar.



En el siguiente paso nos mostara cuantos archivos encontro, en la parte lateral izquierda marcaremos las casillas de los archivos que queremos recuperar.



Una vez finalizado nos pedira indicar la ruta de la carpeta donde queremos guardar nuestros archivos recuperados.



Términos básicos

Hola amistad verde 👀

Al inicio pensé inundarte con términos de redes para que entendieras un poco el trasfondo de las técnicas que se muestran en las stories destacadas. Por otra parte, motivar tu curiosidad en estos temas puede hacer que puedas desarrollarte como profesional en un futuro.

En caso de querer adentrarse más:

Te reto a que indagues en estos temas lo mas que puedas, no basta una pequeña búsqueda en Google, busca libros, temas relacionados y entiende el concepto a profundidad. Un pequeño esfuerzo ahora marcara la diferencia en si llegas a convertirte en un o una gran Hacker

En caso de solo querer saber lo necesario para cuidarte en internet, te recomiendo buscar algunos videos que te expliquen estos temas.

- Lenguajes de programación de alto y bajo nivel:
- Redes LAN/WAN/MAN:
- Servidores:
- Modelos OSI:
- Protocolo TCP/IP:
- Ataques pasivos en el hacking:
- Ataques activos en el hacking:
- IP:
- Algoritmo:
- Sistemas operativos:
- Virus:
- 0-day:
- Ingeniería social:

¿Qué por que no te los explico yo?

A pesar de poder hacerlo y posiblemente hacerlo en otra edición de este manual, quiero que saques a relucir tu lado autodidacta.

:)

Notas

Para que te animes, empiezo yo: La primera fotografía astronómica **de** la Luna fue capturada en 1840 por el profesor de química William Draper.