

# Análisis Forense Informático

---

Hidder Buddy

**Octavio Meneses Ramos**

**Carlos Moreno Jaqués**

**Alejandro Esteras Marco**

**Víctor Santiago Martínez Picardo**

1. ¿Qué es Hider Buddy?
2. Instalación de Hider Buddy
3. Uso de Hider Buddy
4. Práctica: Automatización con Hider Buddy

## 1. ¿QUÉ ES HIDERBUDDY?

HiderBuddy es un software de ocultación de ficheros de baja complejidad, que trabaja con los atributos de ficheros en el sistema NTFS de Windows.

Se basa en un wrapper del comando **attrib** escrito en el lenguaje AutoHotkey.

Las ventajas de usar Hider Buddy es que es completamente portable, permite ejecutarse en modo GUI y/o modo Consola.

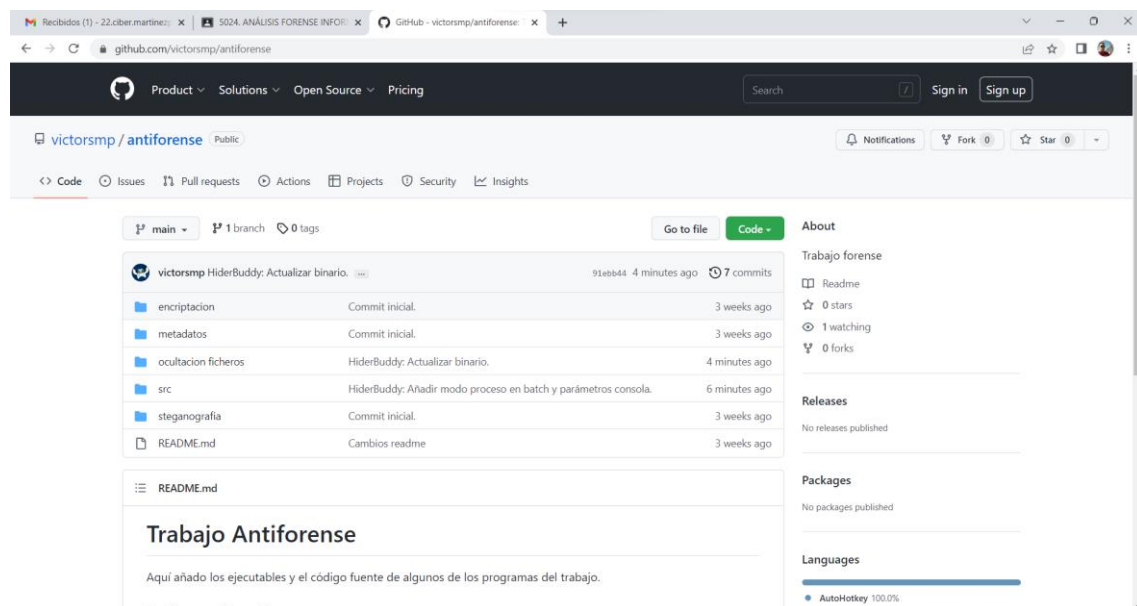
El código es totalmente abierto y público.

## 2. INSTALACIÓN DE HIDERBUDDY

HiderBuddy no requiere de instalación, se puede añadir al path o a la carpeta system32 para disponer de él desde cualquier directorio en el entorno de consola de Windows.

Para descargar HiderBuddy, accedemos al repositorio del proyecto en GitHub:

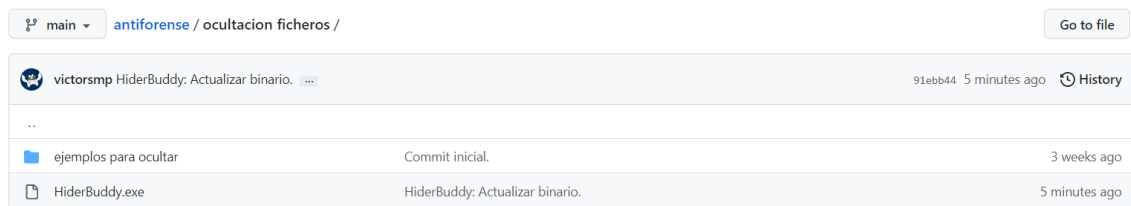
<https://github.com/victorsmp/antiforenses>



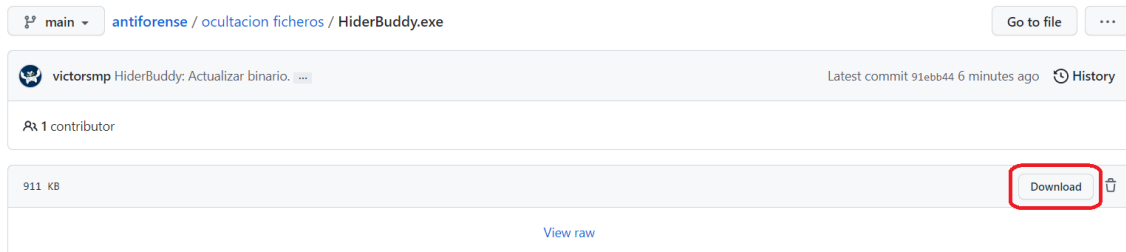
Accedemos a la carpeta “ocultación ficheros”:

victorsmp HiderBuddy: Actualizar binario. ...			91ebb44 5 minutes ago	7 commits
encryption	Commit inicial.		3 weeks ago	
metadatos	Commit inicial.		3 weeks ago	
ocultacion ficheros	HiderBuddy: Actualizar binario.		5 minutes ago	
src	HiderBuddy: Añadir modo proceso en batch y parámetros consola.		7 minutes ago	
steganografia	Commit inicial.		3 weeks ago	
README.md	Cambios readme		3 weeks ago	

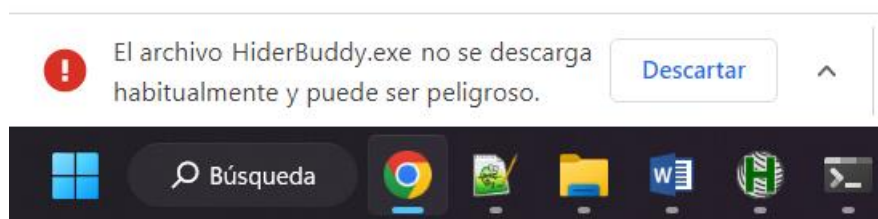
Y pulsamos en **HiderBuddy.exe**:



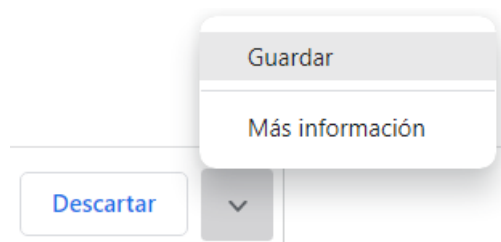
Y en la siguiente ventana pulsamos en **Download**:



Dado que es un fichero no firmado, es común que aparezca esta advertencia:



Guardaremos el fichero de todas formas:



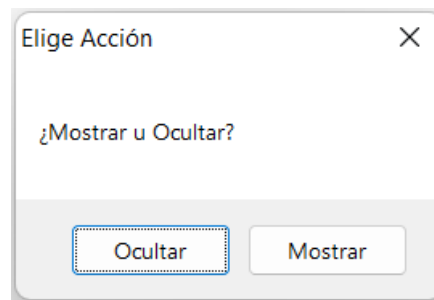
Con esto ya tendremos HiderBuddy en nuestro equipo:



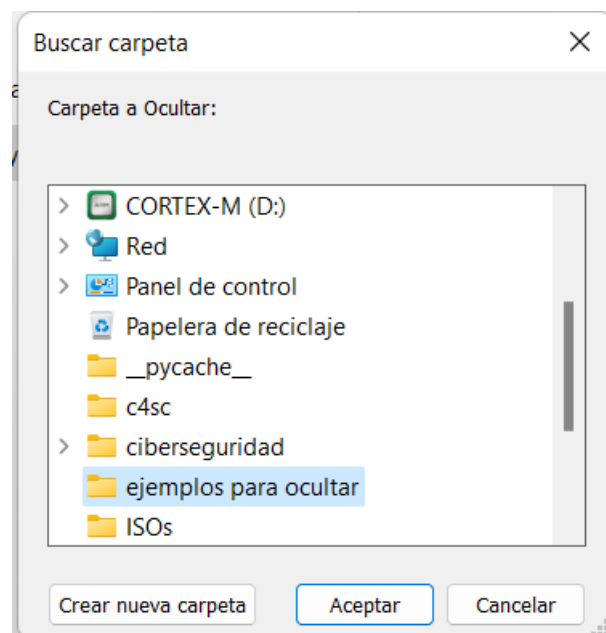
HiderBuddy.exe

### 3. USO DE HIDERBUDDY

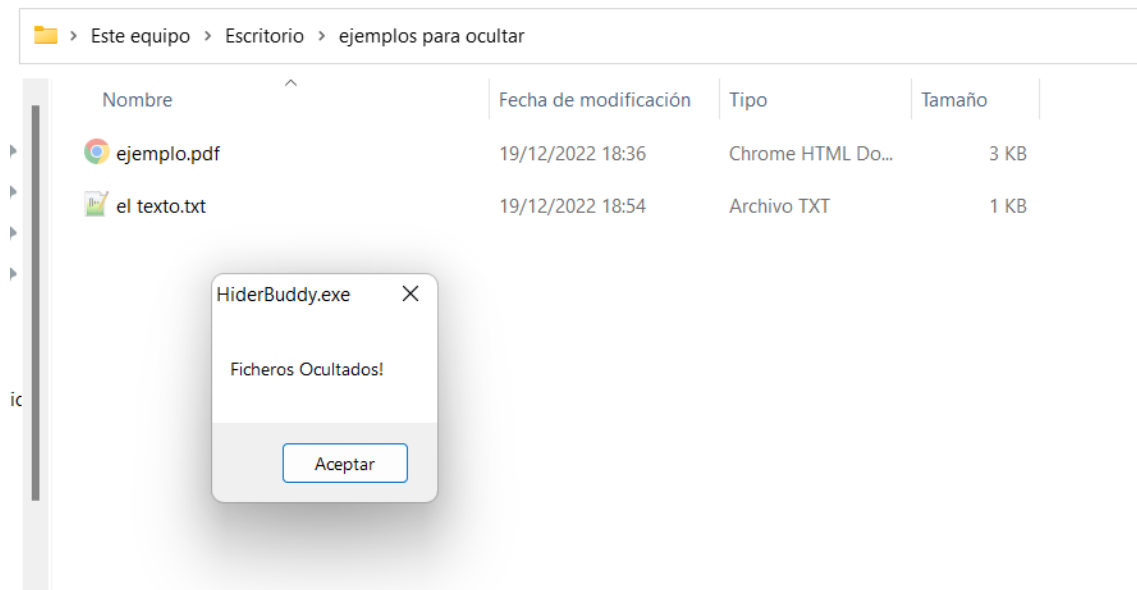
Si hacemos doble click sobre el ejecutable de HiderBuddy, obtendremos el siguiente diálogo:



Seleccionaremos el uso que le queramos dar, en mi caso voy a ocultar los ficheros de una carpeta que tengo en el escritorio, por lo tanto, pulso en **Ocultar**:



Voy a seleccionar la carpeta llamada “**ejemplos para ocultar**”:



Vemos como los ficheros se han puesto translúcidos o han desaparecido.

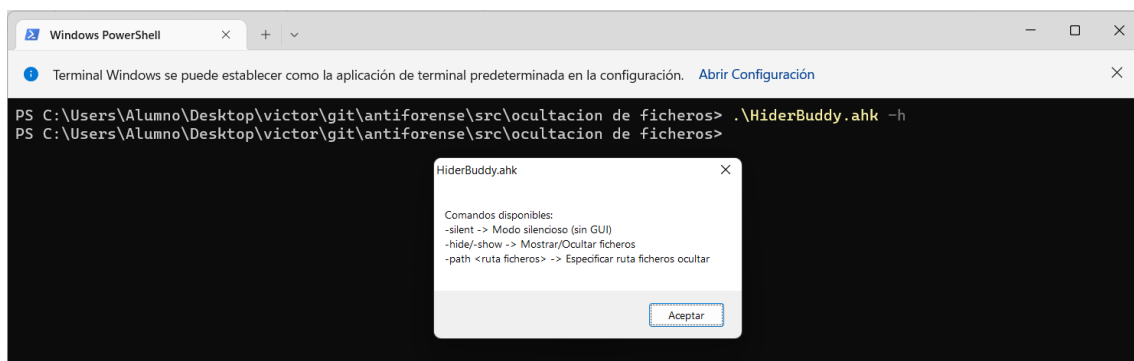
En caso de verse translúcidos, con pulsar F5, o cambiar de carpeta y volver, estos desaparecerían de la interfaz.

Cabe destacar que esta ocultación es muy débil, desde consola con permisos de administrador y/o desde un live cd, estos ficheros son visibles.

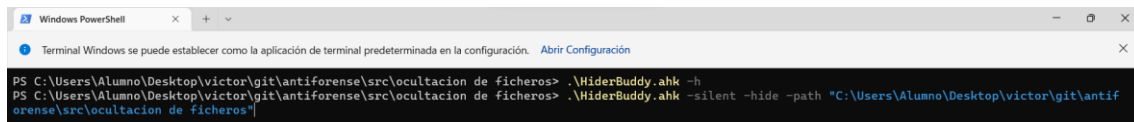
Una buena forma de protegerlos sería combinando la herramienta que creamos con crypt.exe junto con HiderBuddy.

Otro de los usos de HiderBuddy es mediante el modo consola:

Si ejecutamos **HiderBuddy -h** obtenemos la ayuda del modo consola:



Este es un ejemplo de ocultación de ficheros desde el modo consola:



```
PS C:\Users\Alumno\Desktop\victor\git\antiforenses\src\ocultacion de ficheros> .\HiderBuddy.ahk -h
PS C:\Users\Alumno\Desktop\victor\git\antiforenses\src\ocultacion de ficheros> .\HiderBuddy.ahk -silent -hide -path "C:\Users\Alumno\Desktop\victor\git\antiforenses\src\ocultacion de ficheros"
```

.\HiderBuddy.exe -silent -hide -path "C:\Users\Alumno\Desktop\victor\git\antiforenses\src\ocultacion de ficheros"

#### 4. PRÁCTICA: AUTOMATIZACIÓN CON HIDERBUDDY

Dirígete a la ruta de tu usuario y ejecuta HiderBuddy en modo **Mostrar** sobre esta carpeta, revelando de esta forma la carpeta oculta: **AppData**

