

USB Forensics

الشرح سيكون كيف تفحص و تجيب الملفات المحذوفه من الفلاش



هذا الفلاش اللي راح استخدمه في الشرح

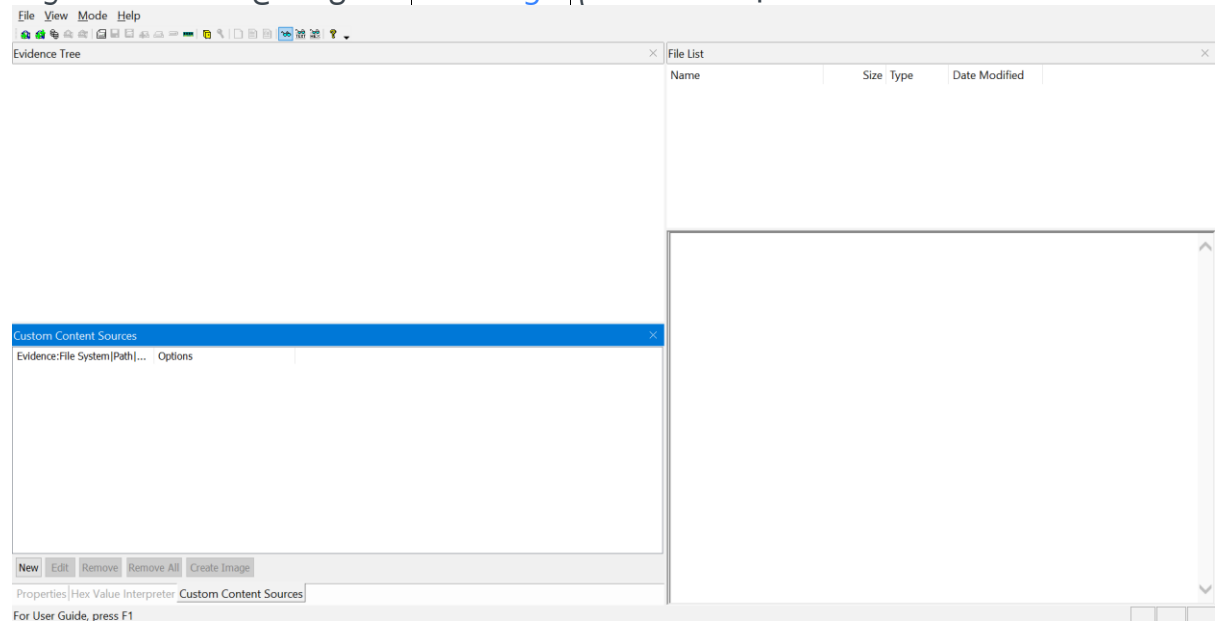
اول شي اشيك الفلاش في الجهاز و هذي صوره للمفات داخله

Name	Date modified	Type	Size
KiraFolder	04/08/2021 22:56	File folder	

ملفات الفلاش

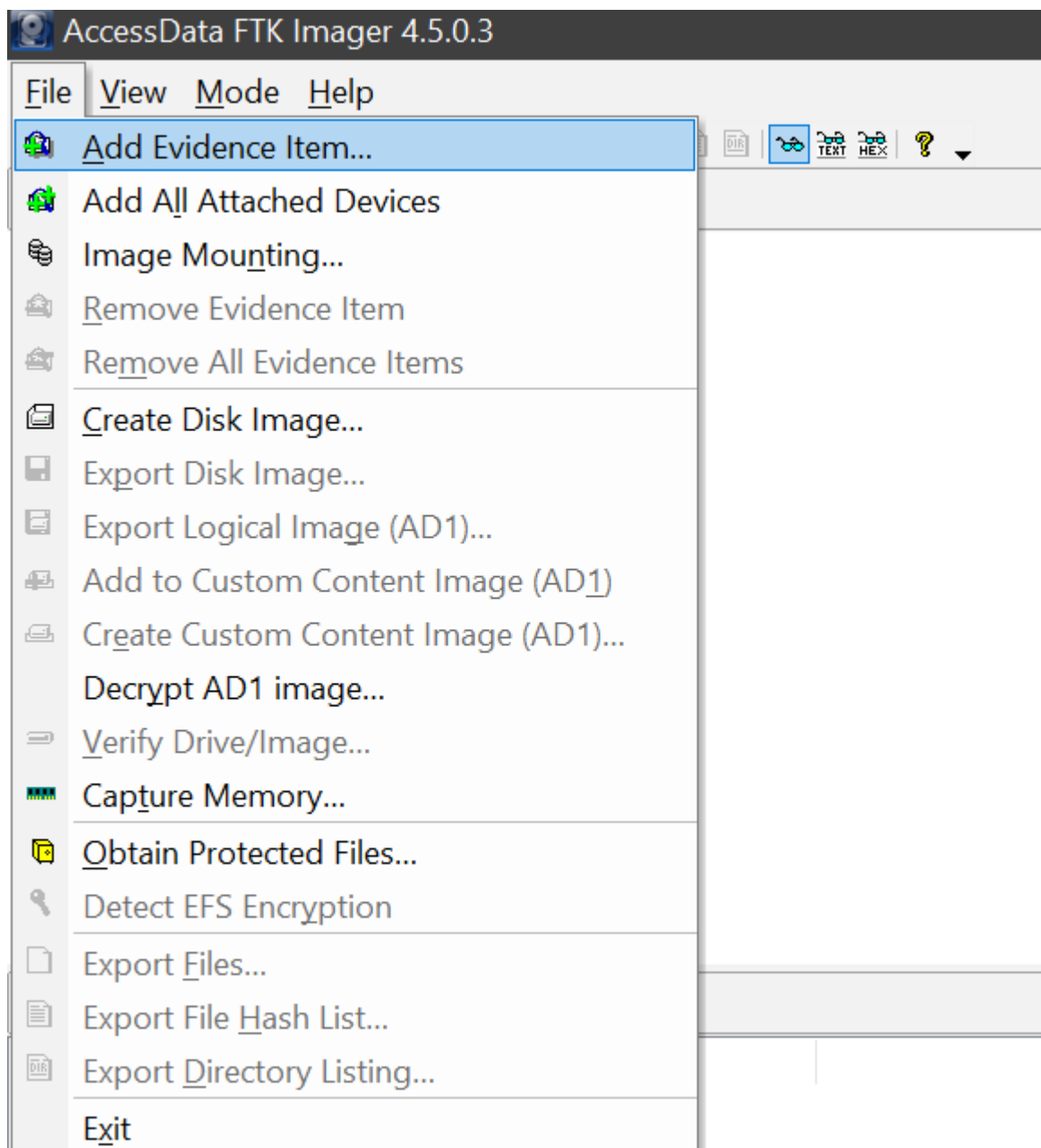
استرجاع البيانات من الفلاش

بعدها نستخدم **FTK imager** عشان نطلع الملفات المحذوفه



FTK imager

تفتحه بصلاحيات مدير النظام



FTK imager add item

بعد ما نضغط بتجيك هذي الخيارات

Select Source

Please Select the Source Evidence Type

☒ Physical Drive

☐ Logical Drive

☐ Image File

☐ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

< Back Next > Cancel Help

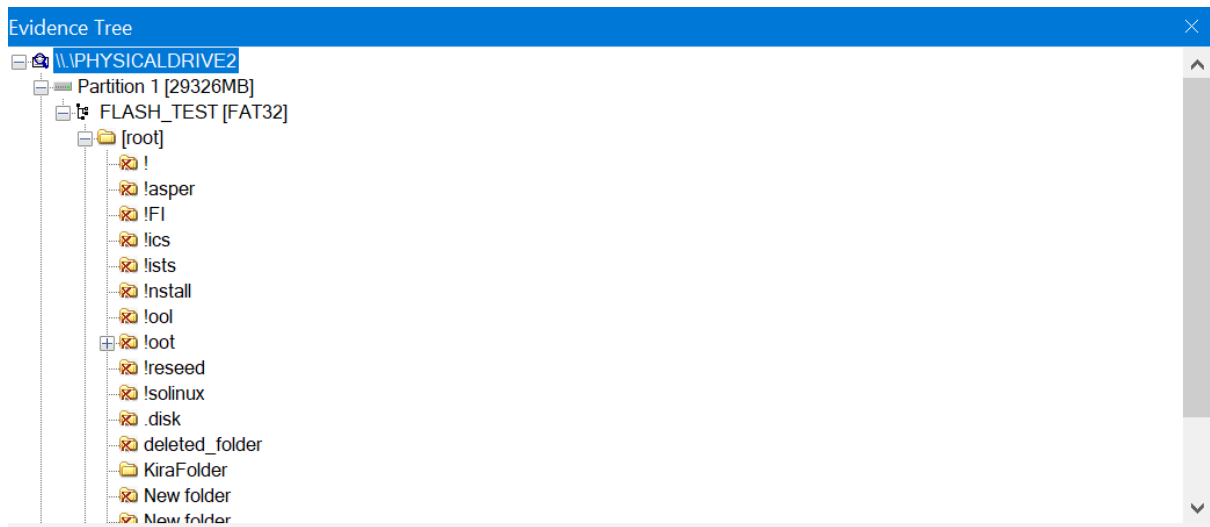
حاليا حنا نهتم بالخيار الاول(الخيارات الثانية مهمة بس مانحتاجها حاليا)
Source Drive Selection

Please select from the following available drives:

\\\\.\\PHYSICALDRIVE2 - SanDisk Ultra USB 3.0 USB Device [30GB] ▼

choose usb flash

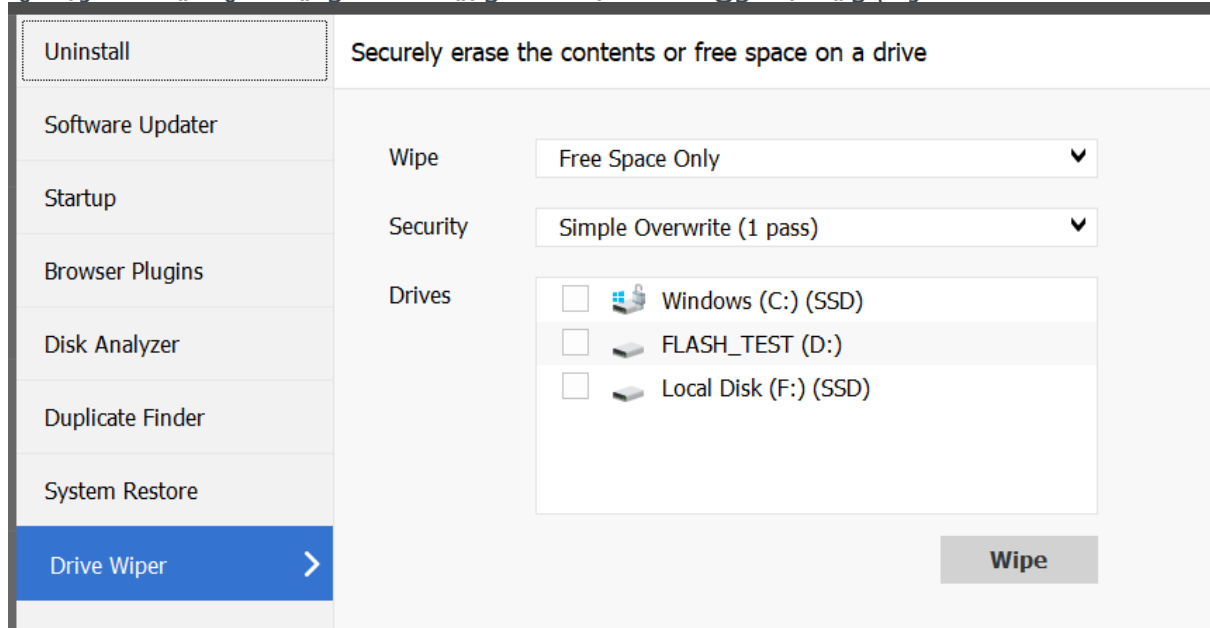
حاليا اخترت فلاش sandisk 30GB نضغط انتهاء(finish)



بعد ما تضغط علامة الزائد بتجيك المجلدات و الملفات كلها هنا اللي عليها علامة اكس هذي الملفات المحذوفة و من بينها و بينهم ملف **deleted_folder** بعد ما تحدد على المجلد اللي تبي ترجع ملفاته تضغط كلك يمين بعدين export files و بترجع الملفات المحذوفة ماراح يرجع لك كل شي من اول ما اشتريت الفلاش فية عوامل زي متى حذفت الملف و هل تم الكتابة فوقه او لا لو تلاحظون فيه ملفات غريبة موجوة محذوفة هذا لأن الفلاش كان فيه نظام اوبينتو

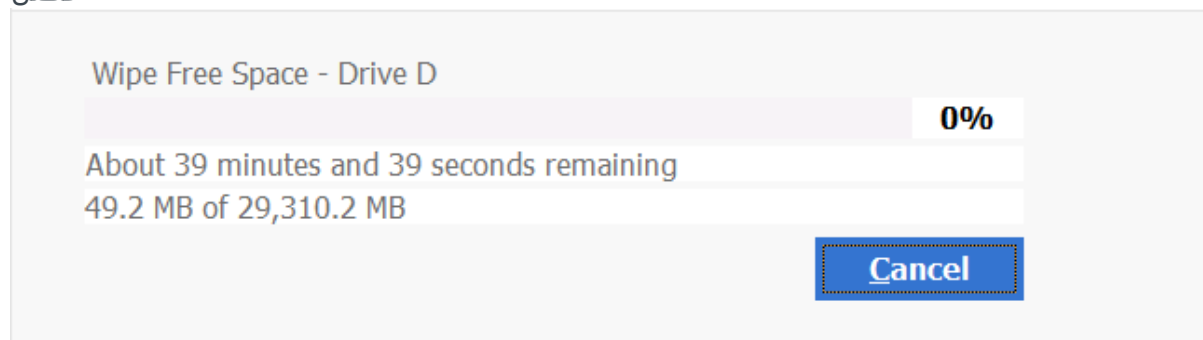
حماية من استرجاع البيانات

اذا احتجت تمنع احد من الوصول الى البيانات حقتك فيه بعض البرامج زي [ccleaner](#) بس قبل ما نستخدمه كيف يحذفها و مايقدر احد يرجعها؟ الموضوع مو سحر الفكرة انه يكتب فوق البيانات المحذوفة اكثر من مره يعني؟ اذا حذفت الملفات تبقى فيه بقايا ما تنحذف علطول ف ممكن يتم استرجاعها ف الطريقة اللي يشتغل فيها يكتب فوق الفلاش مرة مرتين ثلاث..... انت تحدد الرقم و يكتب فوق ملفاتك بملفات و بيانات عشوائية مالها قيمة اذا رجعتها



بعد ما تحملة تخش الادوات (tools) و بتلاقيها زي كذا الخيار الاول يقولك تبي تحذف جميع الملفات في الفلاش او يخليها و يكتب بس في المساحة الفاضية بالنسبة لي يخليها المساحة

الفاضية بس لأنني ابي الملفات حقتي(الغير محذوفة) بعدين تحدد مرات الكتابة كل مازادت كان افضل



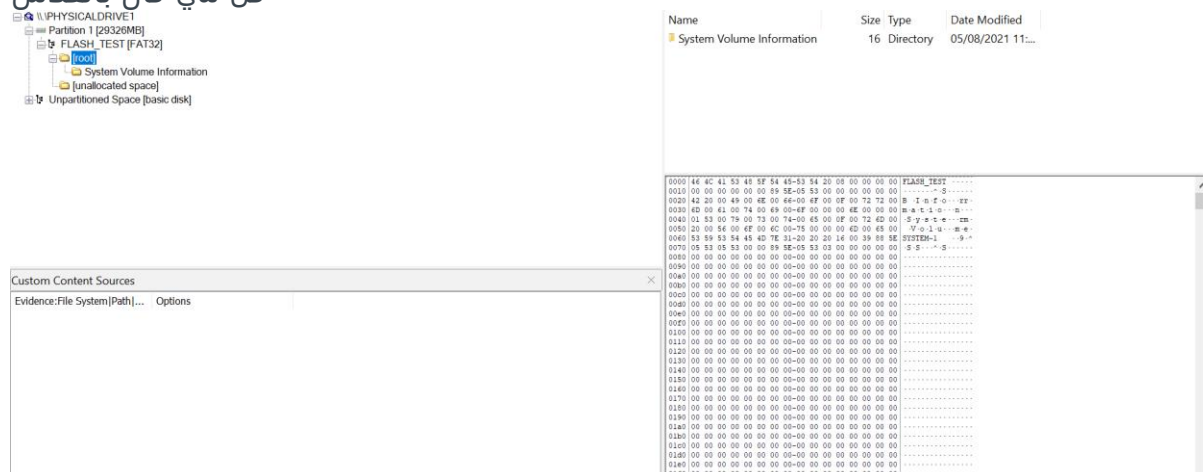
اخترت كتابة فوقها 7 مرات سرعة الانتهاء تختلف حسب عدد مرات الكتابة و المساحة بالنسبة لنا 7 مرات و 30 قيقا بايت نكتب فوقها يعني يعبي الفلاش 30 قيقا و يفضيه 7 مرات عشان يتأكد ان الملفات السابقة حقتي محد يقدر يسترجعها

KiraFolder	04/08/2021 22:56	File folder	
3590F75ABA9E485486C100C1A9D4FF06PHQG...	04/08/2021 23:51	File	59,136 KB
3590F75ABA9E485486C100C1A9D4FF06ZENC...	04/08/2021 23:54	File	12,544 KB
3590F75ABA9E485486C100C1A9D4FF06VYVY...	04/08/2021 23:56	File	16,640 KB
3590F75ABA9E485486C100C1A9D4FF06LULGI...	04/08/2021 23:59	File	23,808 KB
3590F75ABA9E485486C100C1A9D4FF06KWQI...	05/08/2021 00:02	File	24,576 KB

هذي البيانات العشوائية اللي تنضاف

فورمات للفلاش

ممکن بعد اذا ماعندك وقت تكتب فوقها تسوي فورمات للفلاش مع العلم الفورمات راح يحذف كل شي كان بالفلاش



FTK imager after flash format

هذي صورة بعد ما سوينا فورمات للفلاش و حاولنا نسترجع الملفات اللي كانت عليه

ان شاء الله يكون الشرح واضح و بسيط و وصلت المعلومة بشكل مبسط