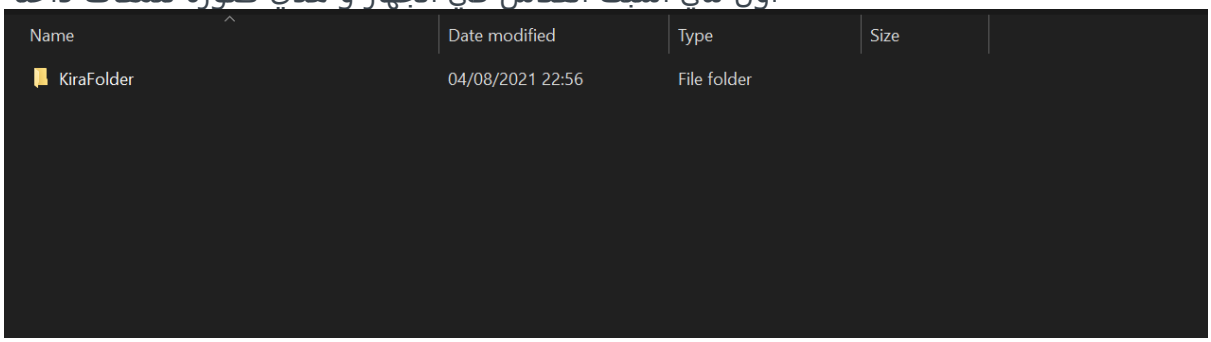
USB Forensics

الشرح بيكون كيف تفحص و تجيب الملفات المحذوفه من الفلاش

هذا الفلاش اللي راح استخدمة في الشرح

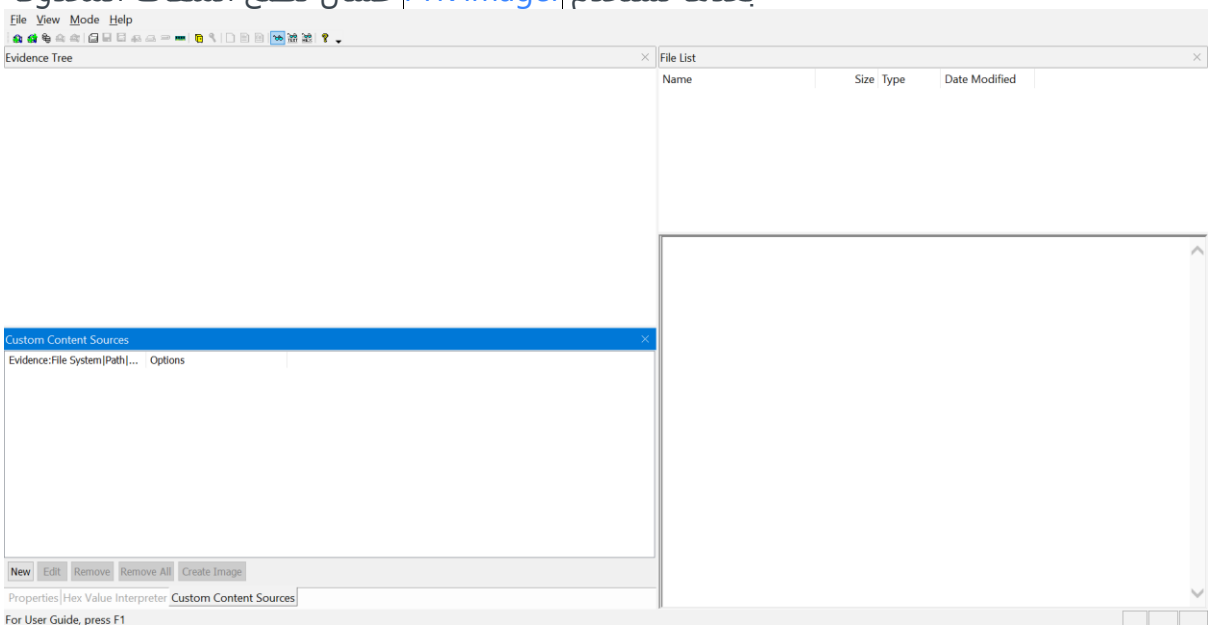
اول شي اشبك الفلاش في الجهاز و هذي صوره للمفات داخله



ملفات الفلاش

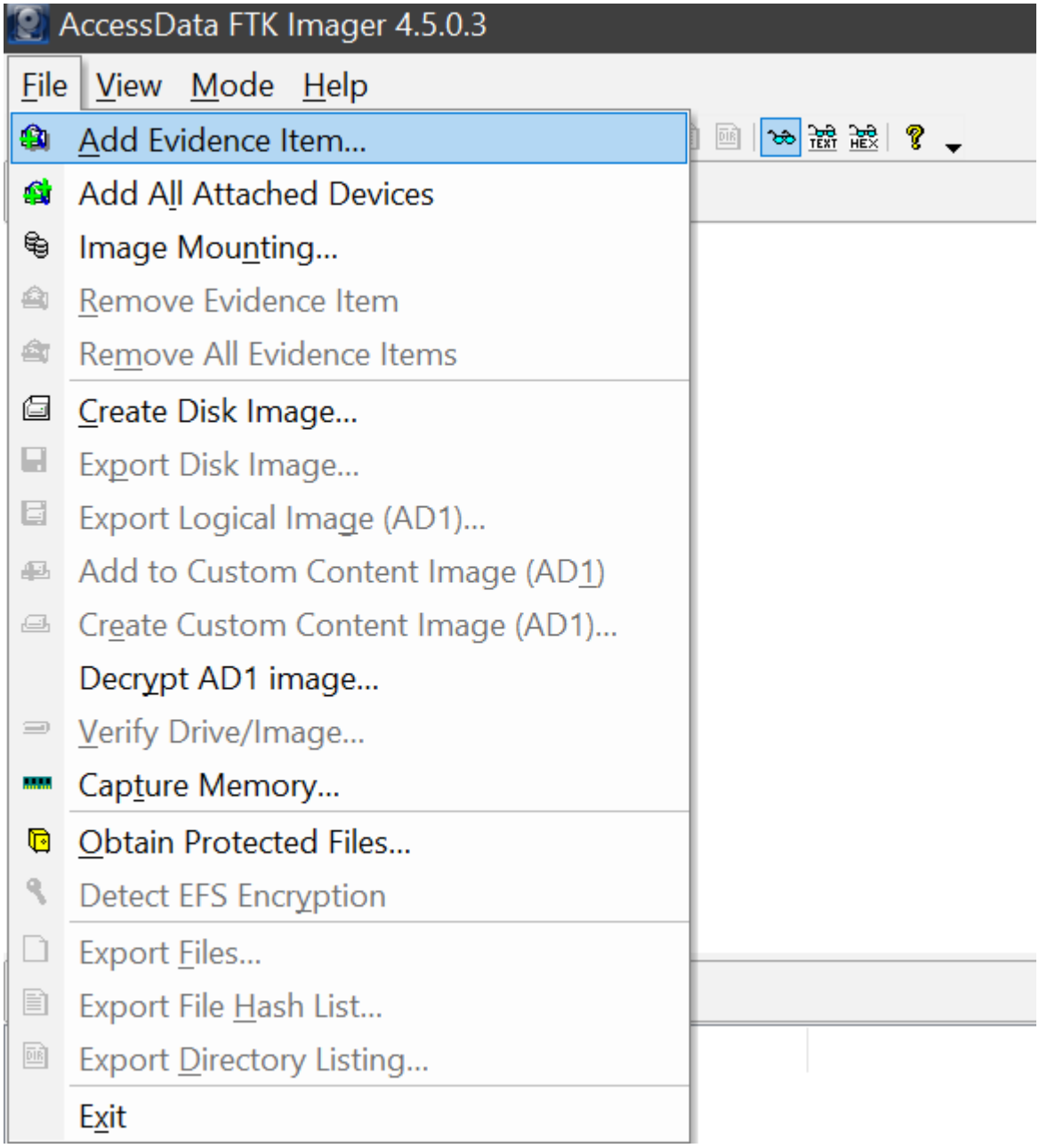
استرجاع البيانات من الفلاش

بعدها نستخدم FTK imager عشان نطلع الملفات المحذوفه



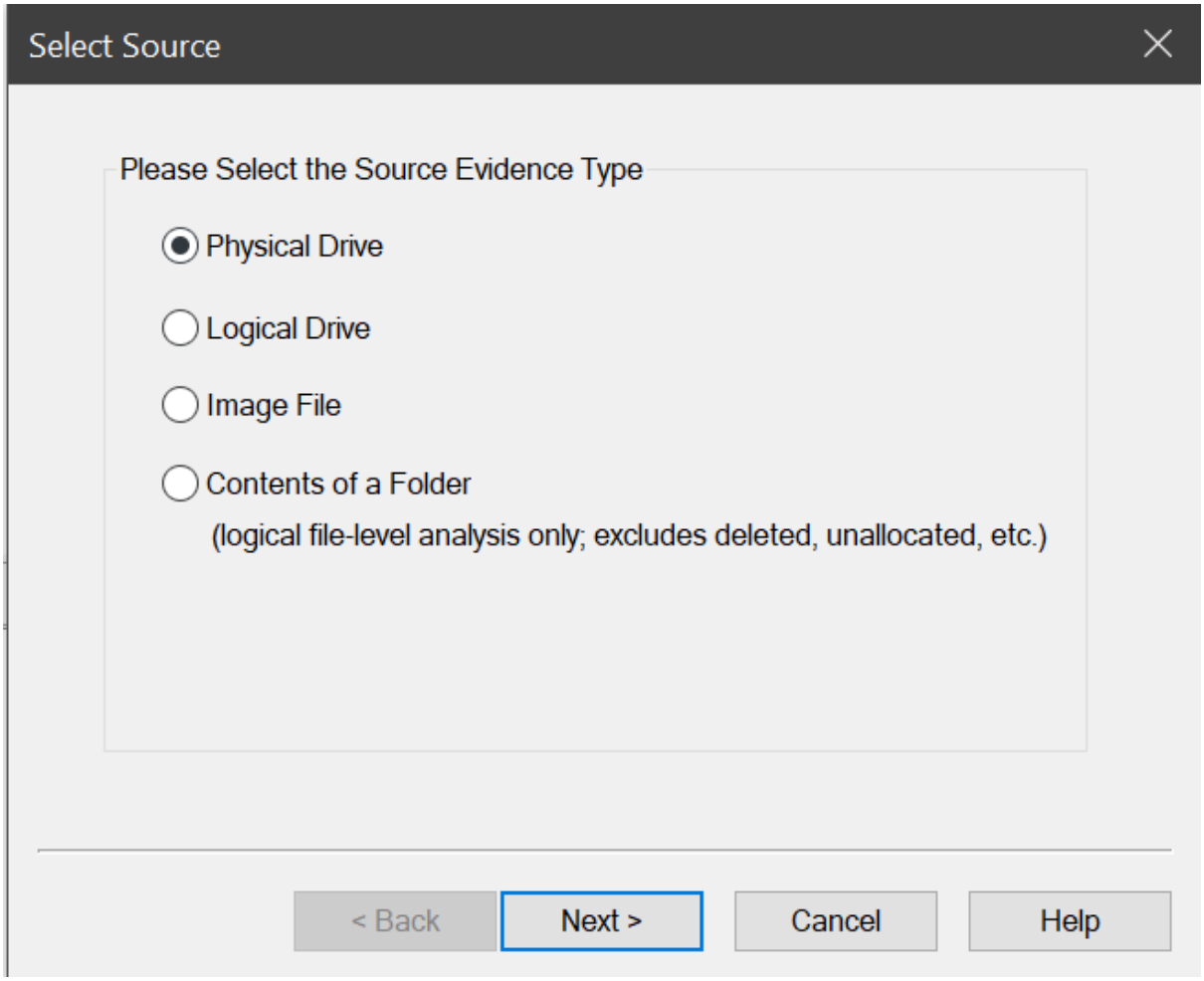
FTK imager

تفتحه بصلاحيات مدير النظام

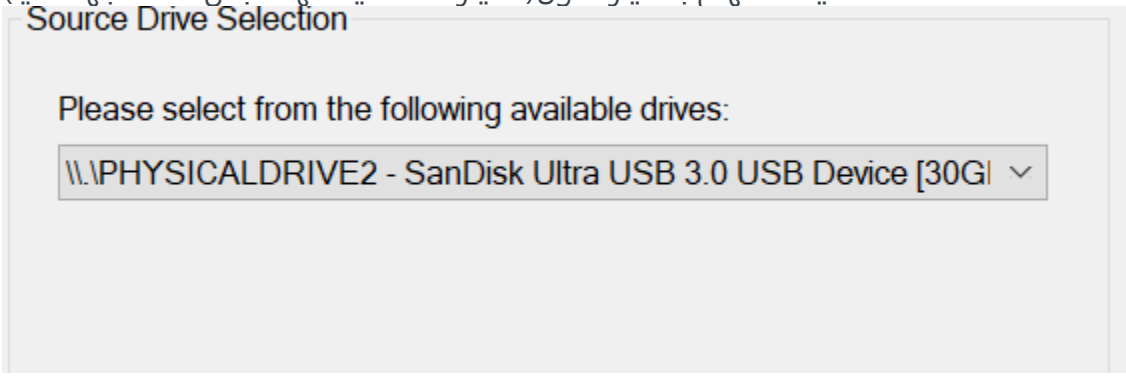


FTK imager add item

بعد ما نضغط بتجيك هذي الخيارات

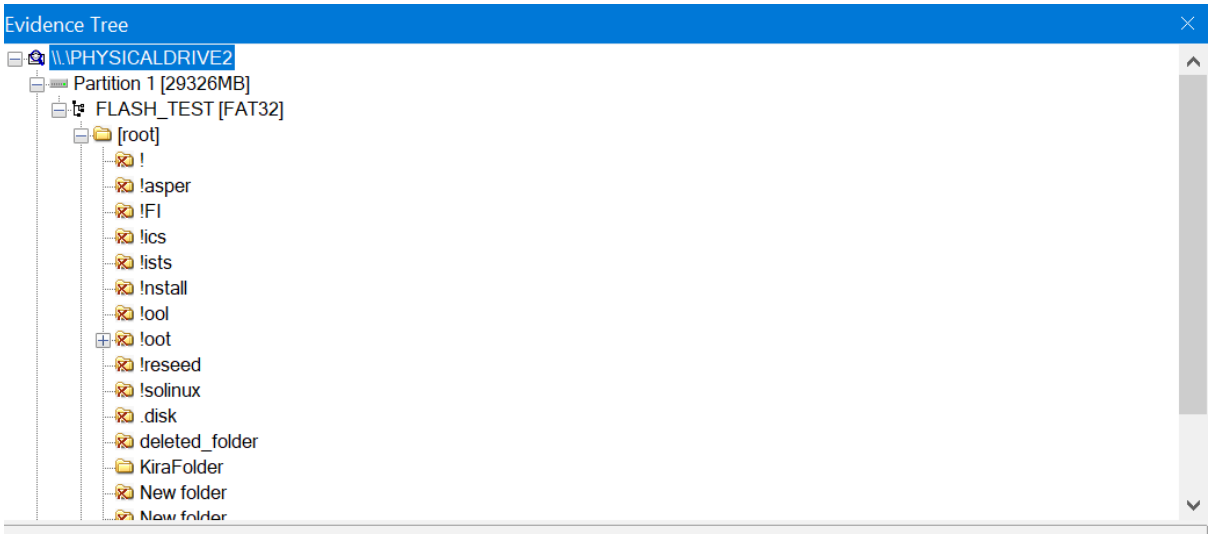


حاليا حنا نهتم بالخيار الاول(الخيارات الثانية مهمة بس مانحتاجها حاليا)



choose usb flash

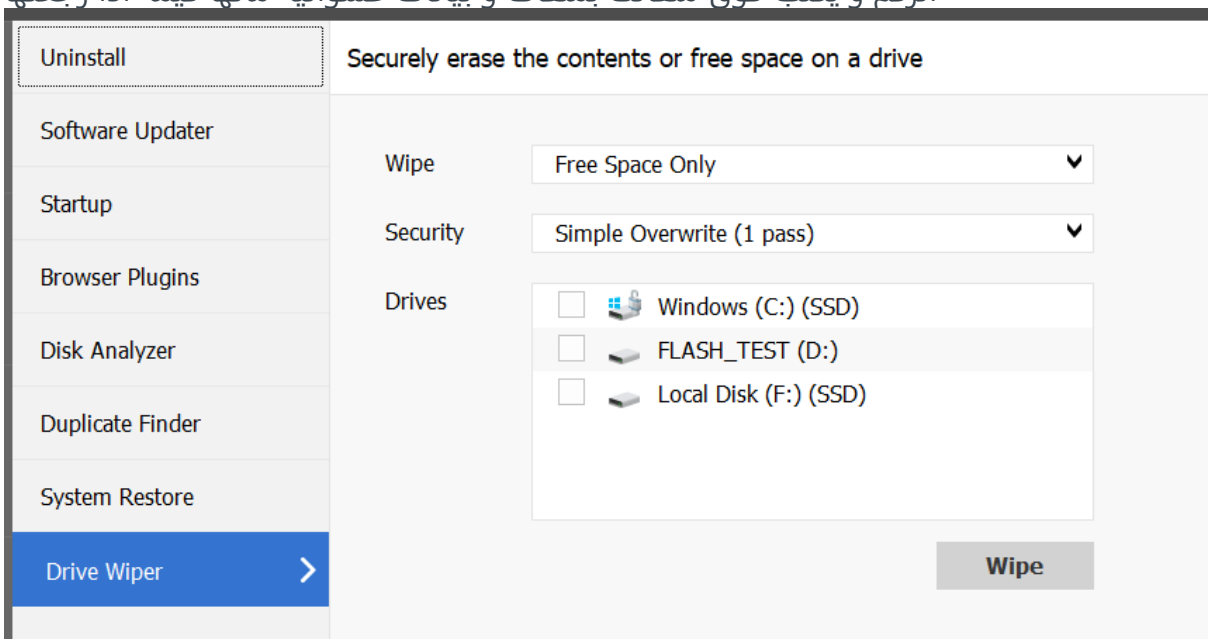
حاليا اخترت فلاش sandisk 30GB نضغط انهاء(finish)



بعد ما تضغط علامة الزائد بتجيك المجلدات و الملفات كلها هنا اللي عليها علامة اكس هذي الملفات المحذوفه 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 فوقة او لا لو تلاحظون فيه ملفات غريبة موجوة محذوفة هذا لأن الفلاش كان فيه نظام اوبينتو

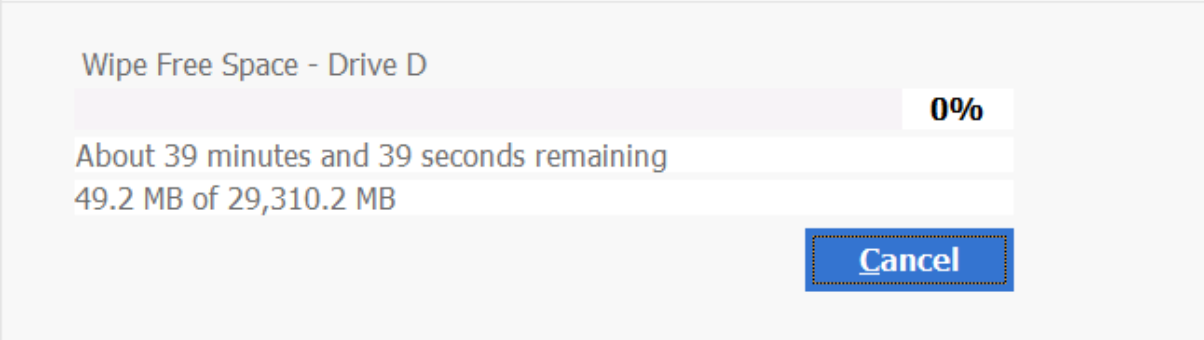
حماية من استرجاع البيانات

اذا احتجت تمنع احد من الوصول الى البيانات حقتك فيه بعض البرامج زي ccleaner بس قبل ما نستخدمة كيف يحذفها و مايقدر احد يرجعها؟ الموضوع مو سحر الفكرة انه يكتب فوق البيانات المحذوفه 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

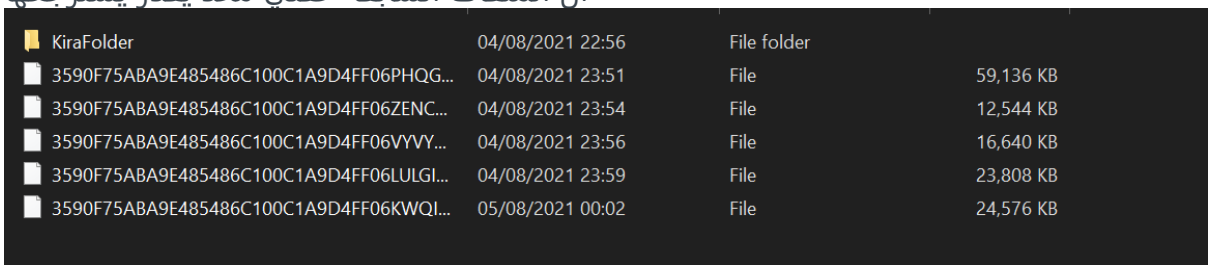


بعد ما تحملة تخش الادوات(tools) و بتلاقيها زي كذا الخيار الاول يقولك تبي تحذف جميع الملفات في الفلاش او يخليها و يكتب بس في المساحة الفاضية بالنسبة لي بخليها المساحة

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



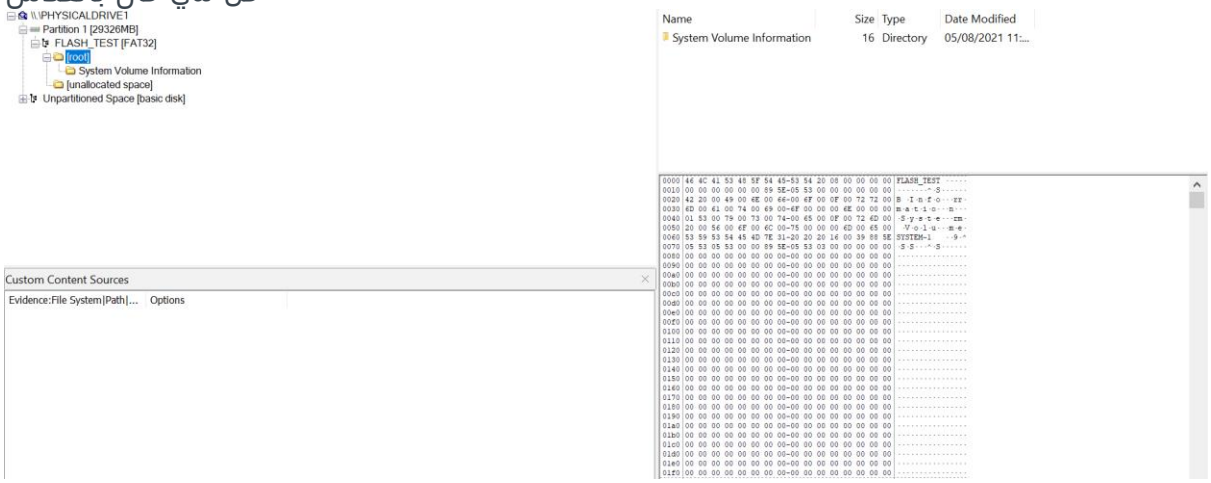
اخترت كتابة فوقها 7 مرات سرعة الانتهاء تختلف حسب عدد مرات الكتابة و المساحة بالنسبة لنا 7 مرات و 30 قيقا بايت نكتب فوقها يعني يعبي الفلاش 30 قيقا و يفضيه 7 مرات عشان يتأكد ان الملفات السابقة حقتي محد يقدر يسترجعها



هذي البيانات العشوائية اللي تنضاف

فورمات للفلاش

ممكن 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