Memory and disk acquisition for Windows OS

Note: We will first acquire live memory (RAM) from a Windows system based on the concept of "Order of Volatility" which states that more volatile data must be acquired before acquiring other data that may be less volatile. Live memory of a system i.e. the RAM is more volatile than the data on the hard disk(s) so it must be acquired first.

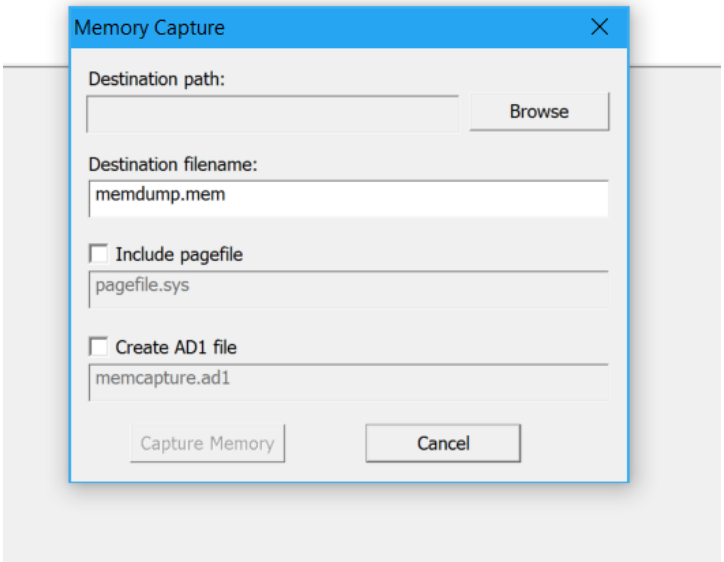
1 Preparation (on standalone machine)

1. A single tool "FTK Imager Lite" is required for both activities. A portable version of this may be downloaded from: http://marketing.accessdata.com/ftkimagerlite3.1.1
2. Ensure that you have compression software capable of creating encrypted ZIP archives available in your system. If not, IBM X-Force IRIS recommends using 7-Zip Portable, available from official website: http://portableapps.com/apps/utilities/7-zip_portable or any other tool of your choice.
3. Prepare storage media, with at least the same size as media in target machine. Tool allows forensic images to be stored on external hard drive attached to target machine. Perform a quick format of a storage media with NFTS file system – all data on this media may be irrecoverably lost! If it is not possible to use external storage media, network shared can be used as an alternative.
4. Copy "FTK Imager Lite" and if necessary "7zip Portable" onto the media.

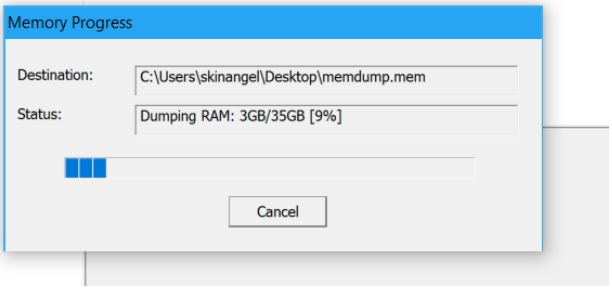
Data created with this manual must be saved directly to the external USB media or network share. It is not allowed to save them locally and then copy to external storage.

2 Acquiring live Memory (on target machine)

1. Execute FTK Imager Lite icon in the FTK Imager Lite folder to start the program.
2. In FTK Imager Lite, select **File → Capture Memory** …
3. Select destination path for the memory image file. This should be a folder in the **external media** connected to the target Windows system. Also select a memory dump file name following the pattern <hostname-date> (i.e. clien01-2018mar03).



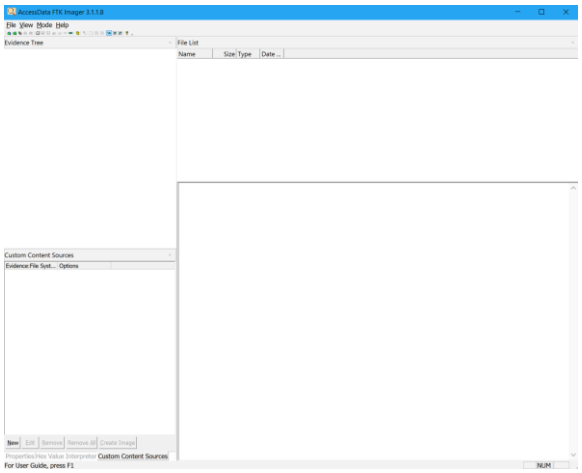
4. Click **"Capture Memory"** button on the same screen to begin the live memory acquisition process.



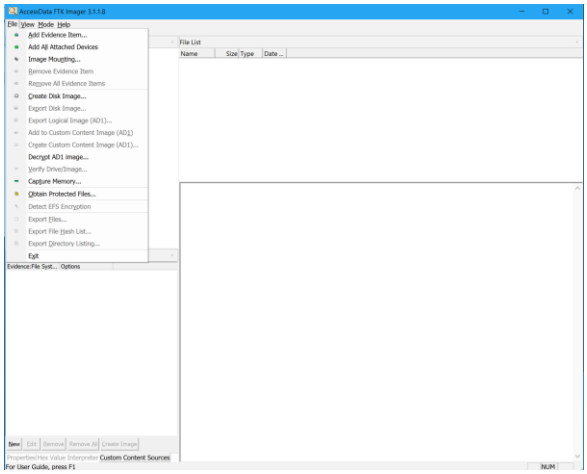
5. At the end of the process you will have the memory dump file created in the desired folder on the external media.

3 Acquiring Hard Disk Image

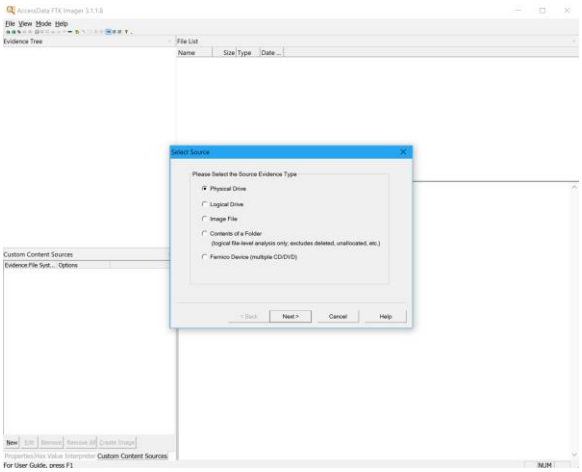
1. Execute FTK Imager Lite icon in the FTK Imager Lite folder to start the program.



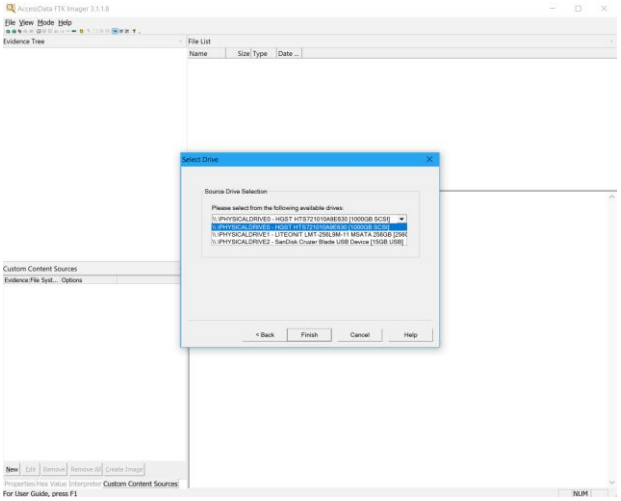
2. Next, select **File → Create Disk Image**



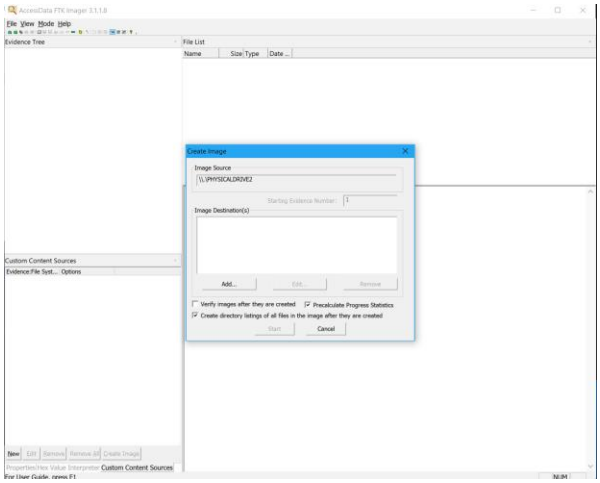
3. Choose Source Evidence Type as “**Physical Drive**” and click “**Next**”



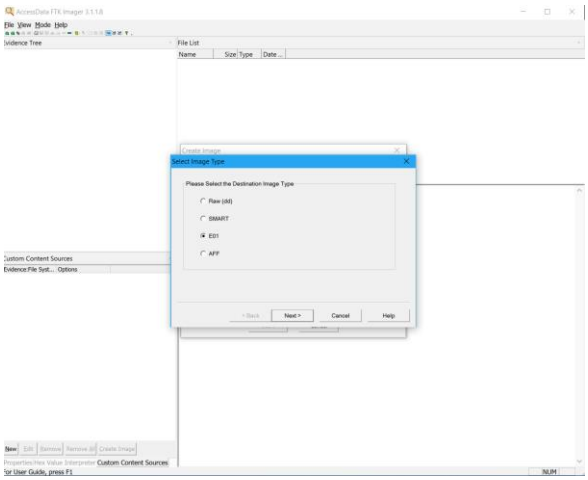
4. Select the physical drive to be imaged from the drop down of all available physical drives and click “**Finish**”



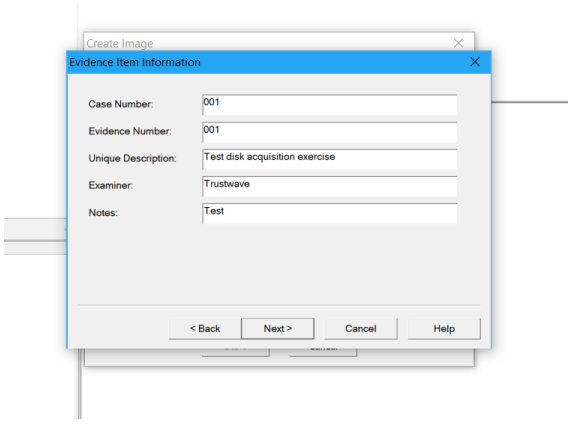
5. Now it’s time to choose where to store the image file, type of image file to create and other options:



6. Click on “**Add**” to select image file location and type of image to be created. Select Destination image type as “**E01**” when prompted and click “**Next**” (See below)



7. In the next screen type details such as case and evidence numbers, description of the activity, Examiner’s name and other notes (optional).



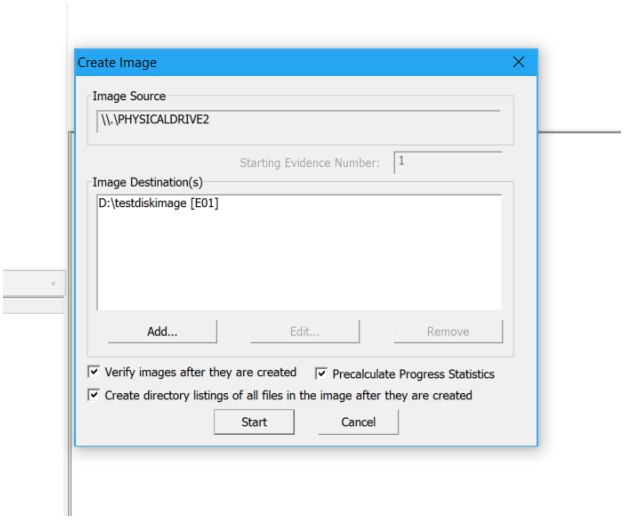
8. In the next screen, select the folder where the image file will be stored. Choose the location to be the **external media** connected to the target computer. Provide a unique name for the image file following the pattern <hostname-drive letter-date> (i.e. client01-C-2018mar03); the extension (.E01 in our case) will be appended automatically. Leave all other options such as Image Fragment Size, Compression, etc. to their default values. Now click on “**Finish**”.

9. Now we are ready to start acquiring the disk image. To do this first “check” the following boxes on the screen below before clicking on the “**Start**” button:

    a. Verify images after they are created

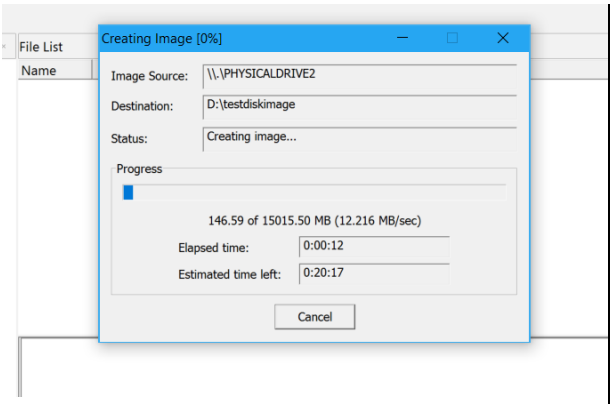
    b. Pre-calculate Progress Statistics

    c. Create directory listings of all files in the image after they are created

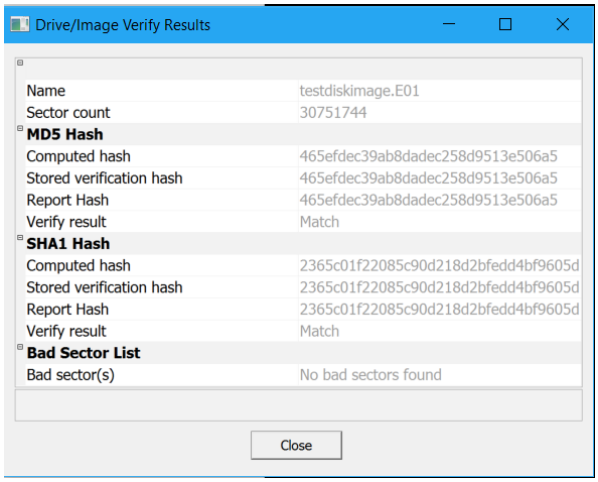


10. Initiate the imaging process by selecting “**Start**”

11. Once the disk imaging process is underway you should see the following progress dialog box:



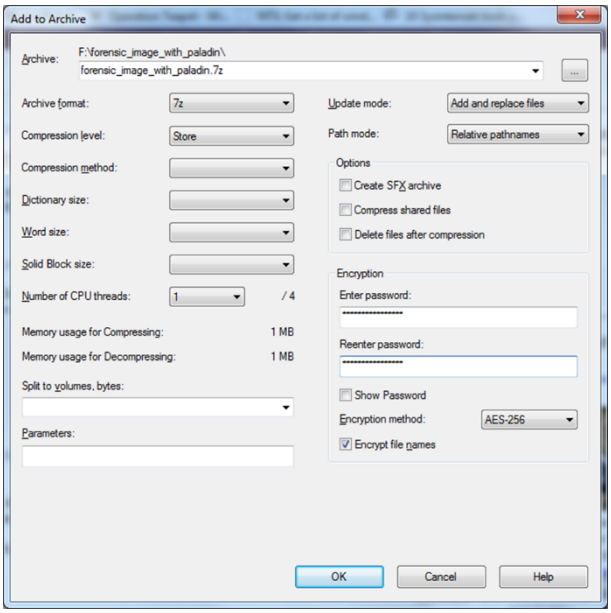
12. Once the disk image is successfully acquired, you should see the following confirmation box. Click on "**Close**" on this box:



13. Perform steps 3-12 for any additional hard drives that may be attached to the Windows systems. Make sure you choose the physical drive carefully to avoid duplicate images or acquiring image of a wrong drive. Also make sure to choose different folders and/or different image file names to be able to clearly distinguish between images acquired from different physical drives.

4 Preparation for delivery to IBM X-Force IRIS team (on standalone machine)

1. Attach external hard drive with previously acquired forensic image or mount file share containing previously acquired forensic image.
2. Create compressed encrypted archive with below options, eg. using 7-Zip Portable.
3. Open the folder containing previously created evidence files and select **only** 2 files: memory dump with *.mem extension and first file of disk image with *.E01 extension Then click 'Add' from toolbar.
4. In '**Add to Archive**' window choose '**7z'** from 'Archive format' dropdown menu, choose 'Store' from 'Compression level' dropdown menu, enter complex (16 characters, mixed case letters, numbers, and special symbols) password in '**Enter password**' and '**Reenter password**' fields, choose '**AES-256**' from '**Encryption method**' dropdown menu and tick '**Encrypt file names**' checkbox, and click '**OK**' button.



5. After encryption is completed, use 7-Zip to open newly created file with 7z extension, provide password and click 'OK' button, then click 'Test' from toolbar. If test completes without errors, encryption was successful.
6. Use method approved within your organization to securely erase file with previously chosen unique and descriptive name and extension E01 and MEM.
7. Newly created 7z file and other files on external hard drive are ready for delivery to IBM X-Force IRIS team via agreed method of delivery.
8. Share complex password used to for encryption with IBM X-Force IRIS team using different communication channel then used to share forensic image.