Windows Live system disk imagining instruction

1 Preparation (on standalone machine)

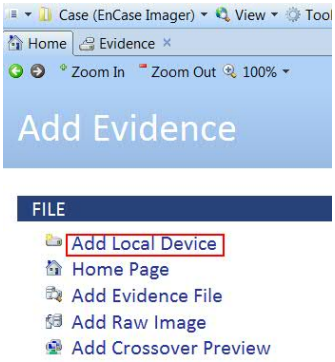
1. IBM X-Force IRIS recommends using 'EnCase Forensics Imager' for disk imagining – below steps guide through this process. If using other tool, follow instructions of that provider.
2. 'EnCase Forensics Imager' is available in 32 or 64 bit versions. Choose version matching OS bit version of target machine. It can be obtained for free from official website: https://www.guidancesoftware.com/encase-forensic-imager (it is required to provide contact details to receive a download link.
3. 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.
4. 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.
5. Copy 'EnCase Forensics Imager' and if necessary '7zip Portable 'onto the media.

2 Information capture (on target machine)

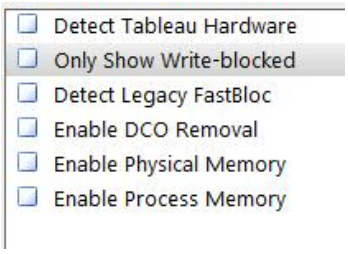
It is **required is to have administrative rights on the machine**. Connect prepared previously external media and launch EnCase Forensics Imager.

2.1 Add device

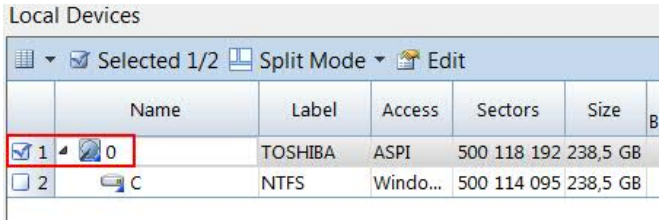
1. On the home screen choose 'Add Local Device'.



2. In new window, uncheck all checkboxes and click 'Next'.



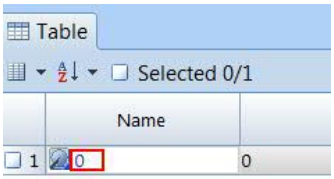
3. Identify physical disk (not a windows drive letter, eg. C) which needs to be imaged (marked with small "HDD-like" icon and check it. Then Click Finish.



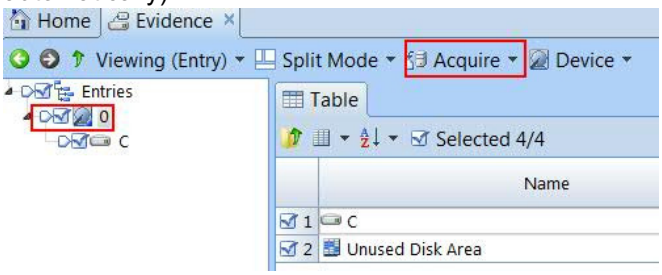
2.2 Acquire image

Disk added in previous step should now be visible in a current window.

1. Click on the text under 'Name' column in the row of a device added before, usually this will be a number. A new tab 'Evidence' will be opened.

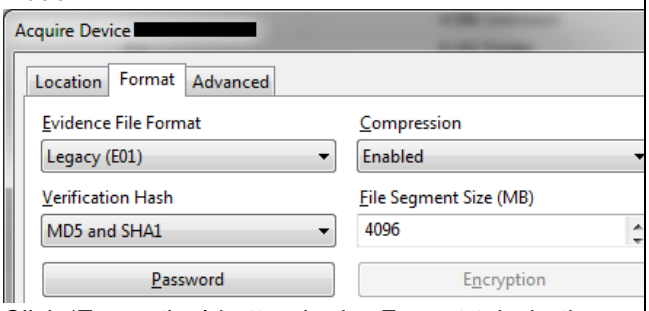


2. Check a checkbox of the hard drive in a tree on the left hand side (other checkboxes could be checked automatically).

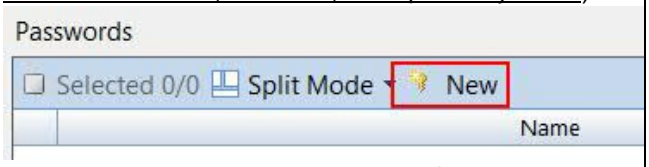


3. Choose the 'Acquire' button from top menu and then choose 'Acquire' option.
4. In a new window 'Acquire Device X', fill in necessary options accordingly:
   a. Location tab: provide a hostname in the 'Name' field, your name in 'Examiner Name', Output Path pointing to external media.
   b. Format tab: Evidence File Format to 'Legacy (E01)', Verification Hash to 'MD5 and SHA1', Compression to 'Enabled', File Segment Size to

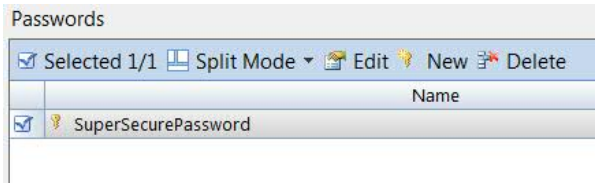
'4096'.



c. Click 'Encryption' button in the Format tab: in the lower 'Password' part of the window, using 'New' button add complex password (16 characters, mixed case letters, numbers, and special symbols).

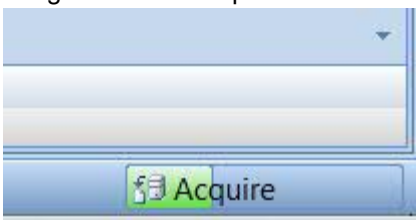


It will be displayed in the window, verify whether the password is correct. Close 'OK' to close this window



d. Click 'OK' to start acquisition process.

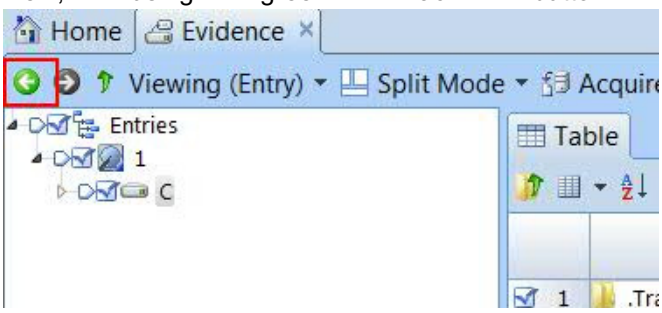
e. Wait for acquisition process to finish. Status can be tracked in the right bottom corner of the EnCase Imager window. Elapsed time should be presented.



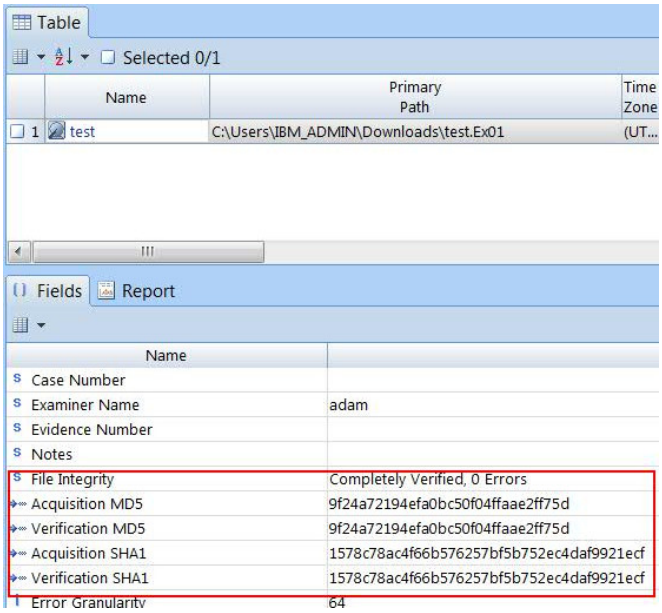
f. After acquisition has finished, a pop up window will appear asking for a password (the one set up previously) to perform image verification. Enter the password and continue. Verification status can also be checked in the right bottom corner.

2.3 Check created image

1. When verification has finished, go back to the Table view, using green 'Back' button.



2. In the row with imaged device a path to the image file should appear in the 'Primary Path' column.
3. In the bottom part of the EnCase Imager window, under 'Fields' tab, scroll down to MD5 and SHA1 hashes section, ensure that following fields:
   a. 'File Integrity' contain 'Completely Verified, 0 Errors'
   b. 'Acquisition' and 'Verification' MD5 hashes are be identical.
   c. 'Acquisition' and 'Verification' SHA1 hashes are be identical.

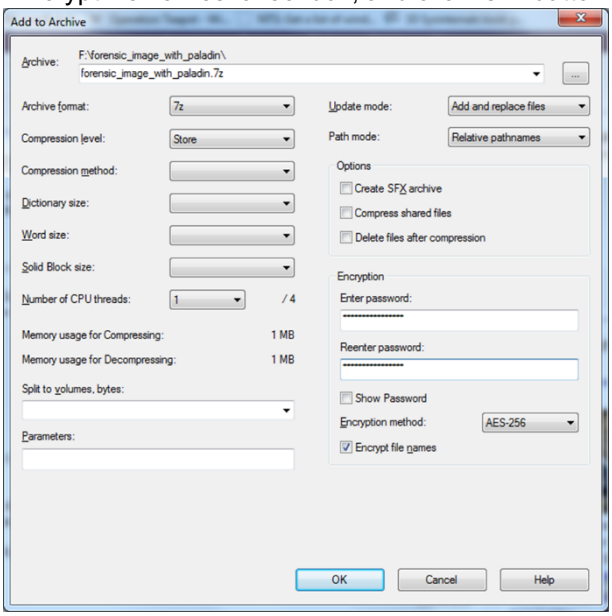


When completed, close application and safely disconnect media from the system.

3 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 **single file** with **extension E01** and click 'Add' from toolbar. **ONLY** add **file** with E01 extension to the archive.
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.
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.