

Auto F

Table of Contents

- 1. Auto F..... 2
- 2. Settings 2
 - 2.1 Force Scan 2
 - 2.2 Folder Skip..... 2
 - 2.3 Node Config 2
 - 2.4 General Options 3
 - 2.5 Profiles 3
- 3. Standard operation 4
- 4. One Case 5
- 5. Case Mode 5
- 6. Node Mode 6
- 7. xCombine 7
- 8. UFDR 7
- 9. Dual Tool 7
- 10. Concurrent 7
- 11. Tools..... 9
- 12. Bug Reporting 9

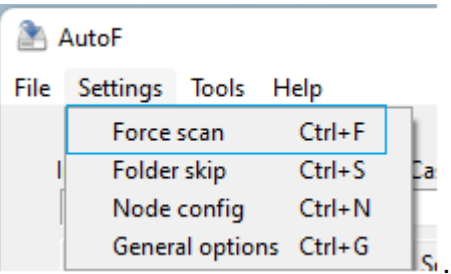
1. Auto F

2. Settings

All settings are stored in an SQLite database called settings.db, this must be located inside the Settings folder within your install.

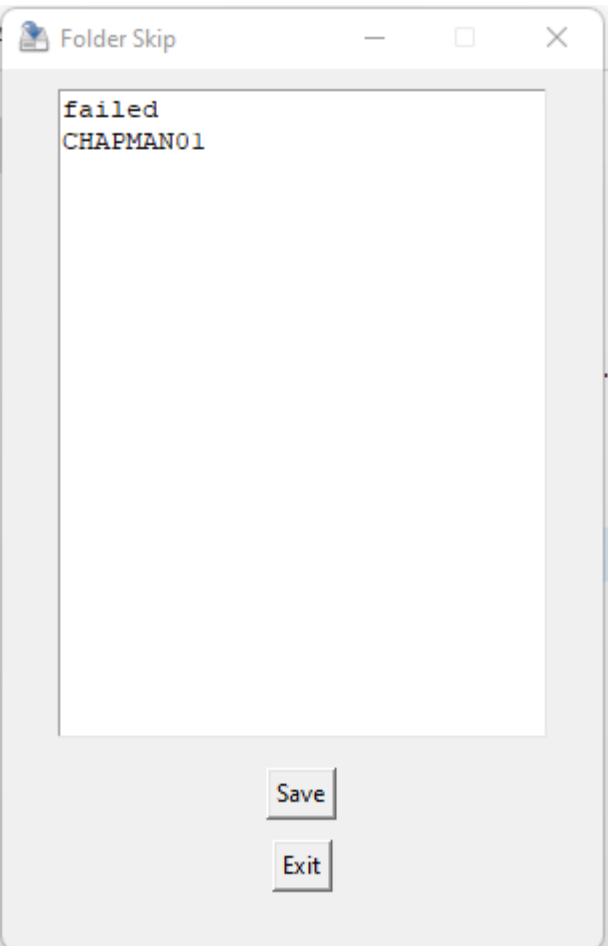
2.1 Force Scan

When AutoF starts for the first time it scans your C drive for all instances of X-Ways, CFG files and Nuix. If you update or install new versions of software you can use force scan to rescan your selected drive(s). Your drives can be set in [General Options](#)



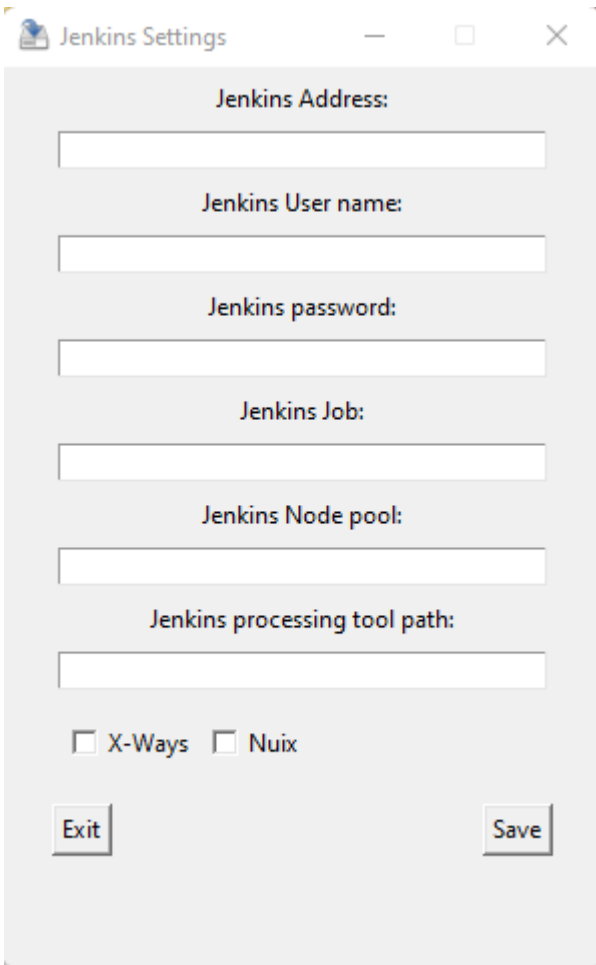
2.2 Folder Skip

Folder Skip will filter out images that are hit by the terms inserted. For instance if you have some failed images in your image path directory, you can insert failed, put them in a folder called failed and they will not be processed. The same applies if you have already processed some exhibits and want the software to ignore them. These are persistent and stored in a SQLite database.



2.3 Node Config

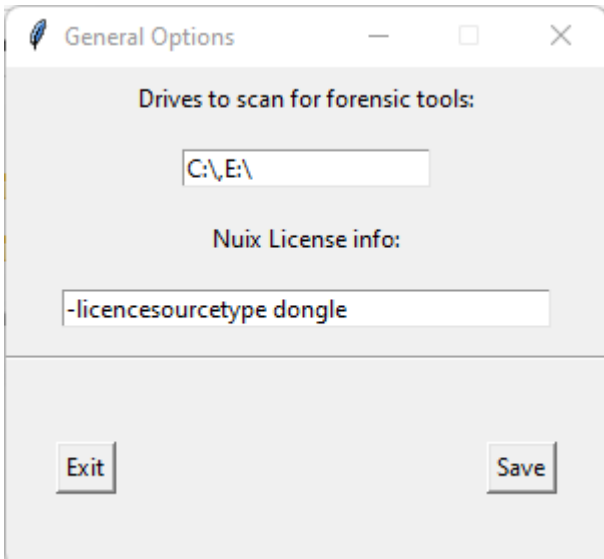
This stores your [Node Mode](#)(Jenkins) settings. The password is purposely left blank after setting it. You can save separate settings based on the tool.



2.4 General Options

General options is currently limited to Selecting you drives for scanning for tools and CFG files. in the format of C:\. you can select multiple drives to scan by seperating them with a colon.

The nuix licence type must also be popultated. By default it is set to use a donlge, if you have a licence server you can input that information run nuix_console.exe for instructions.



2.5 Profiles

Inside your settings folder you will find \X-ways profiles\ and \Nuix\. This is where you save your profiles for processing. The included profiles are for demonstration purposes only.

X-Ways:

You can copy your current WinHex.cfg file from you x-ways installation folder. This retains the last selections (including sub windows) you used when processing/using X-ways. To

create a new one create a small test image and RVS it. once complete close X-ways and copy the file to the settings\X-ways profiles\ folder giving it a pertinent name.

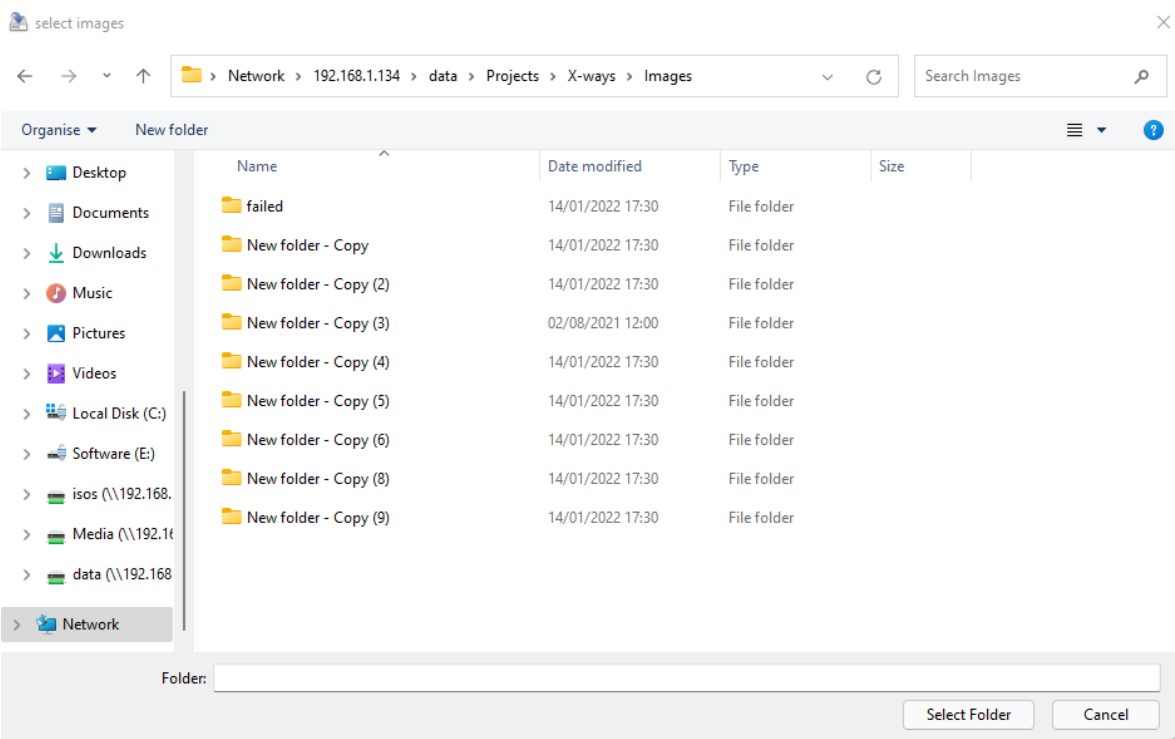
Nuix:

Nuix profile are Ruby scripts, and example script is included that was created during Nuix training. Nuix have all scripting options avalinle on thier developer portal. Copy any scripts to \Settings\Nuix\Scripts\.

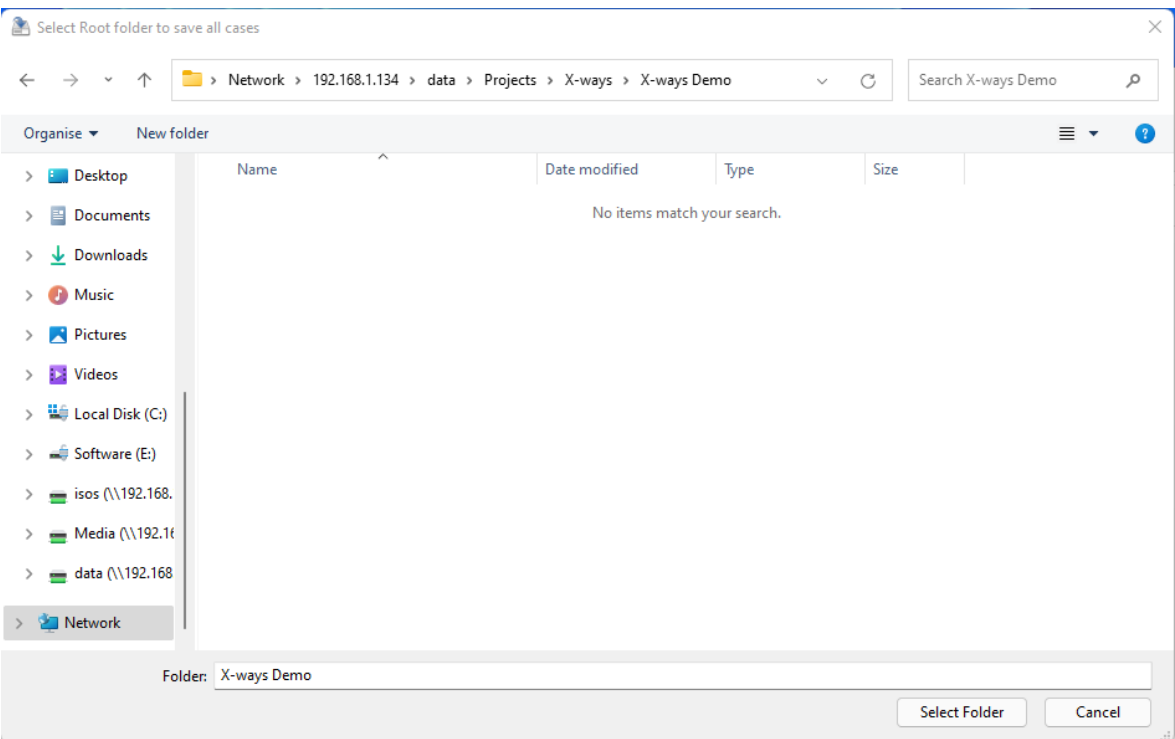
3. Standard operation

A demonstration of using X-Ways Forensics to select multiple images and process them to individual cases. X-ways must have access to a license to operate. Each cases name is derived form the image name.

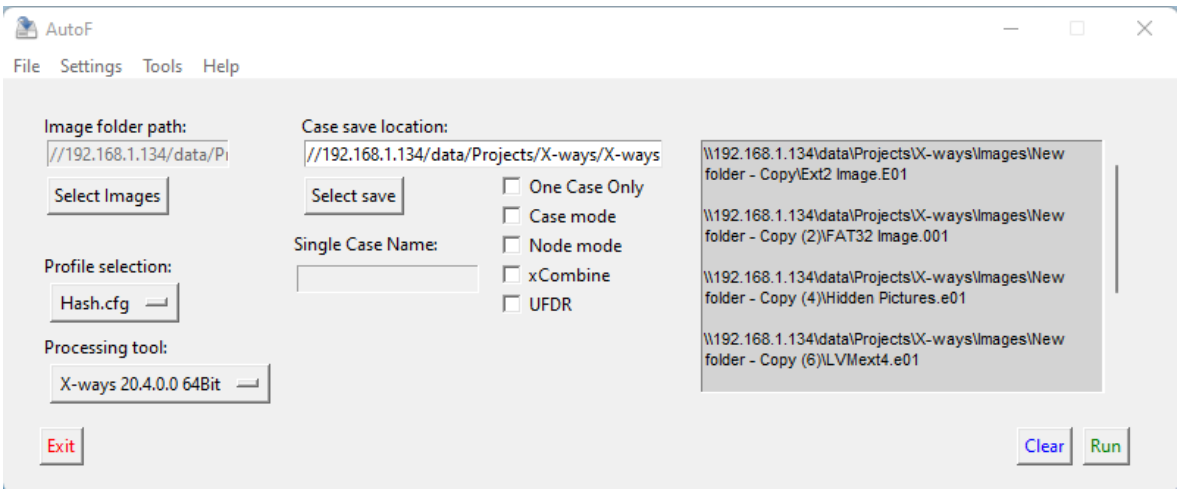
Select your image/exhibit directory:



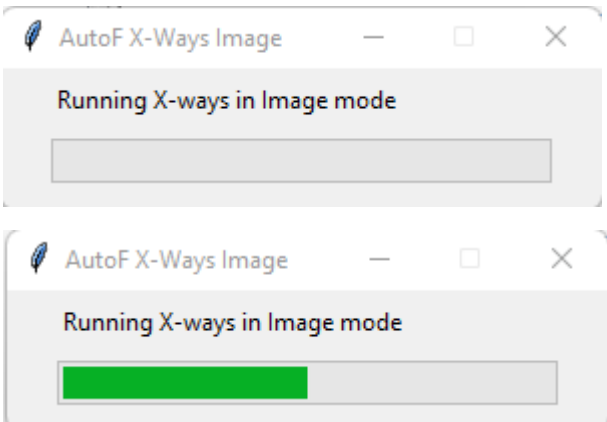
Select you directory to save your cases:



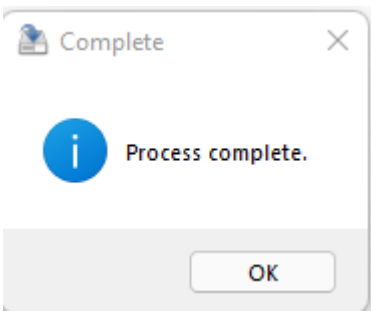
Select your version of tool and profile and hit run:



The tool will now process each forensic image, create an X-ways case and automatically RVS it.



Once complete you will get a completion window.



The same methodology applies for Nuix.

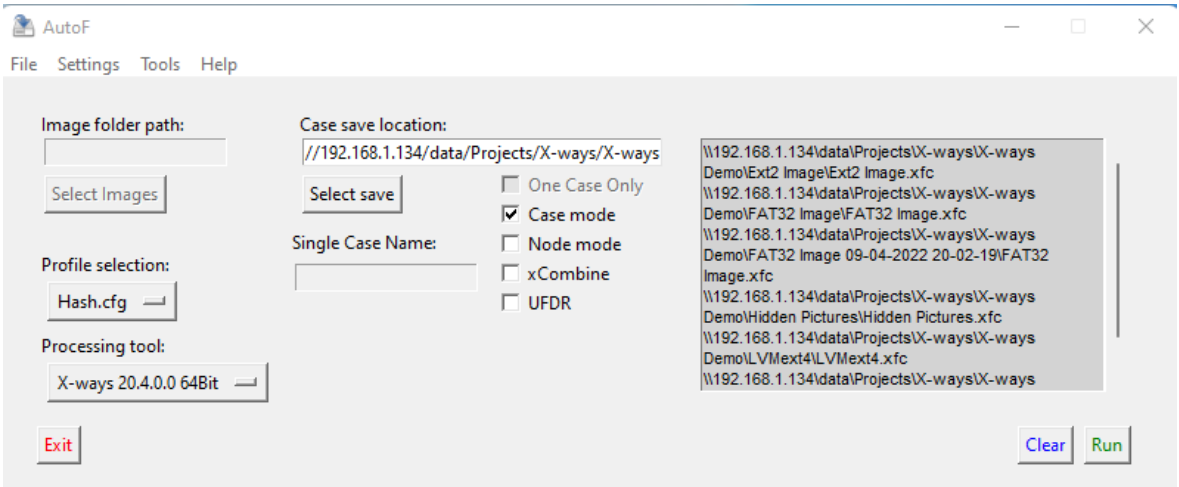
4. One Case

The methodology for One Case is the same as [Standard Operation](#) . But this will create one case with all of the images in it.

5. Case Mode

Case Mode is only support for X-ways Forensics cases, because they make it very simple to do!

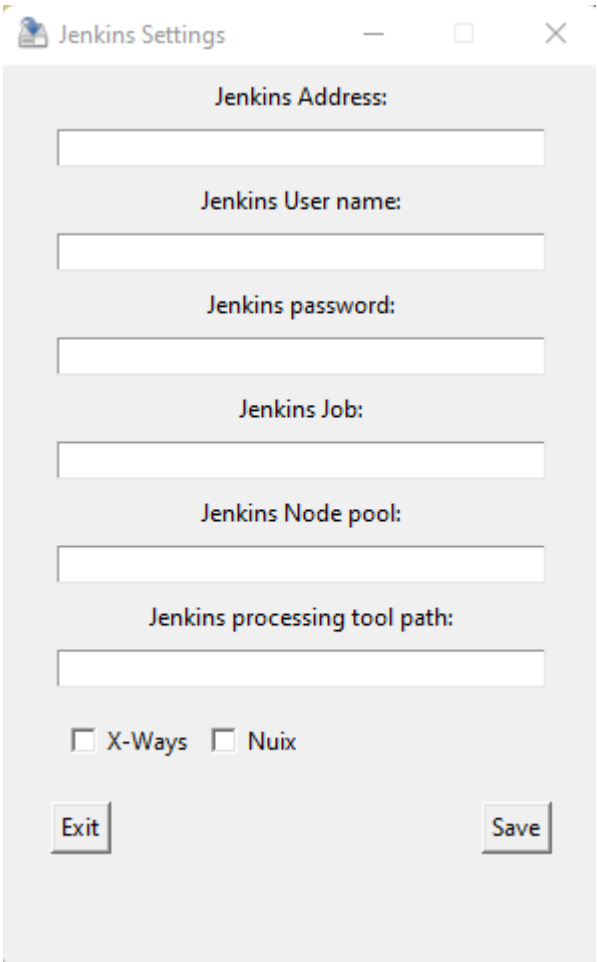
Select your version of X-ways, then select the top directory where you cases are stored. The software will automatically search for all cases within. Select Case mode then your new processing profile.



6. Node Mode

Node mode will pass jobs to Jenkins so it can distribute the jobs across agents. Two sample jobs are included that work with Nuix and X-ways in the settings folder.

The following settings must be set, they can be set per tool. Thw main issue is the Jwnkins processing tool path. For node mode tool version selection does not work. You must pre setup this aspect in the settings of Auto F.



Auto F passes the following paremeters to Jenkins for X-ways:

Profile path.

CopyPath (The version of X-ways 32/64 bit)

path (tool path on the remote machine)

CasePath (Where the case will be saved)

Images

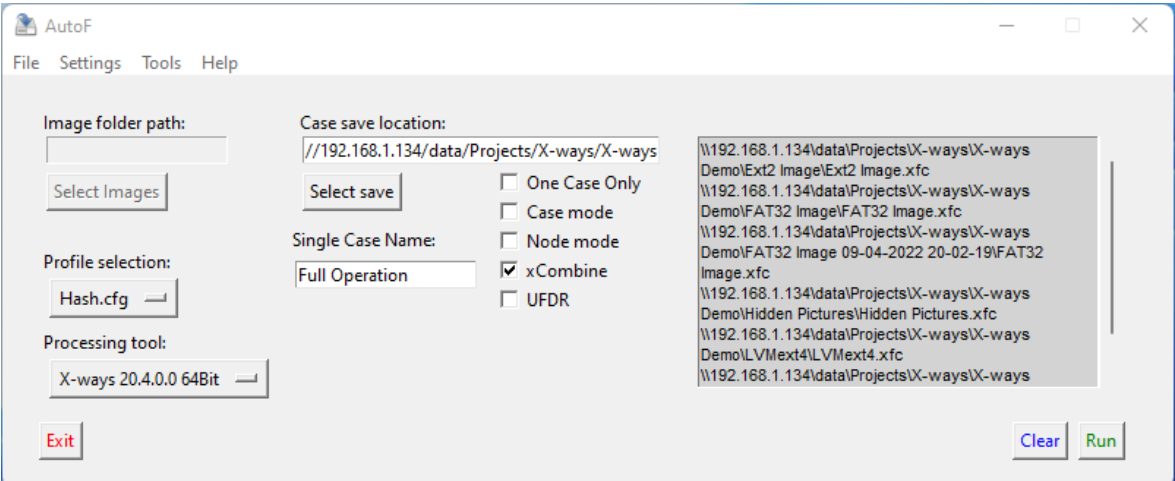
Auto F passes the following paremeters to Jenkins for Nuix:

Path (Path of nuix console)

script (your ruby profile)

7. xCombine

xCombine will take all evidence objects from all selected cases and combine them into one case, retaining thier RVS. Select your case directory, select xCombine (X-ways 20.3 +) and input the new cases name in the Single Case Name entry.

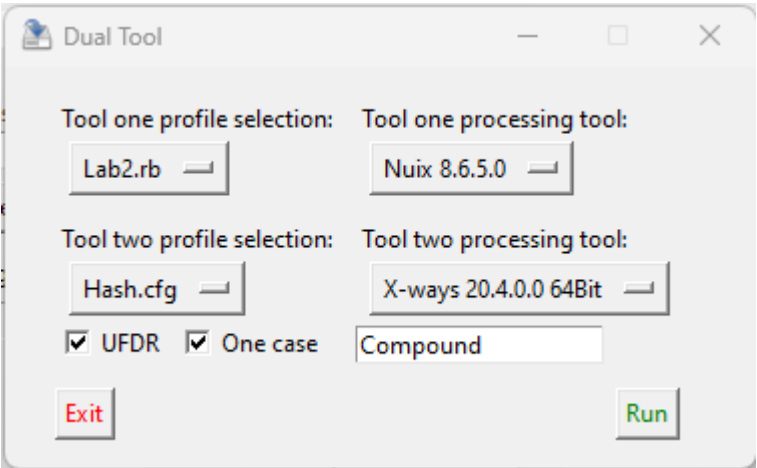


8. UFDR

UFDR mode works the same as [Standard operation](#) . Though will only show\process UFDR files.

9. Dual Tool

Dual tool will process the dame evidence* in two different tools. Select you image repository and case path, select Dual tool and hit run, the following window populates.



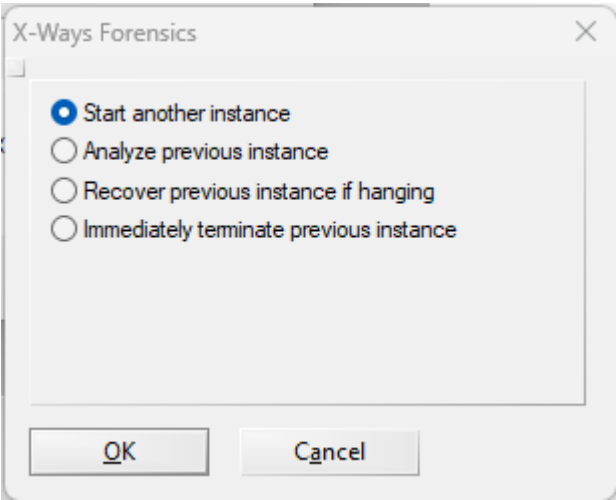
From here you can select UFDR or One case.

* The selected tools will only process compatible images. The output from each tool may be different.

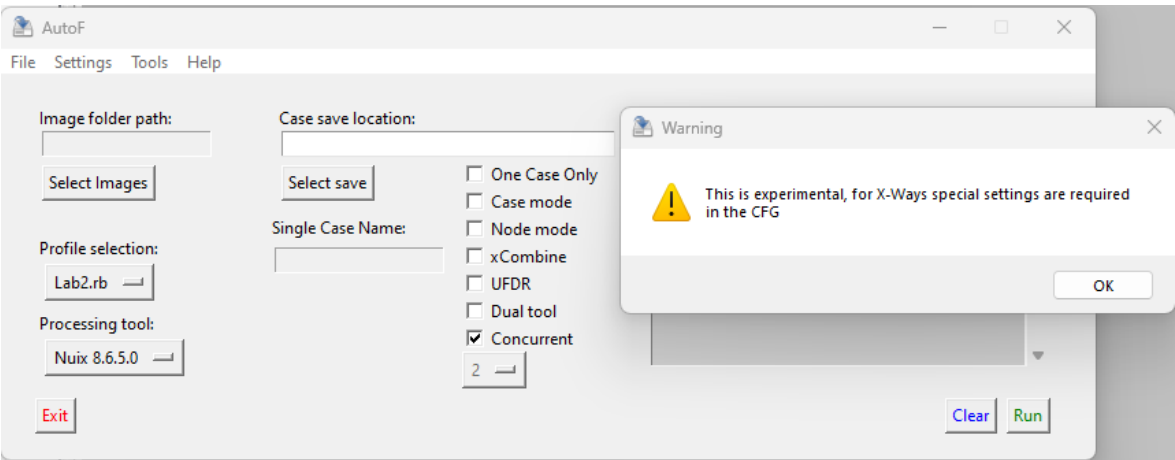
10. Concurrent

This will run the selected count of cases at the same time. This is still experimental and is resource intensive.

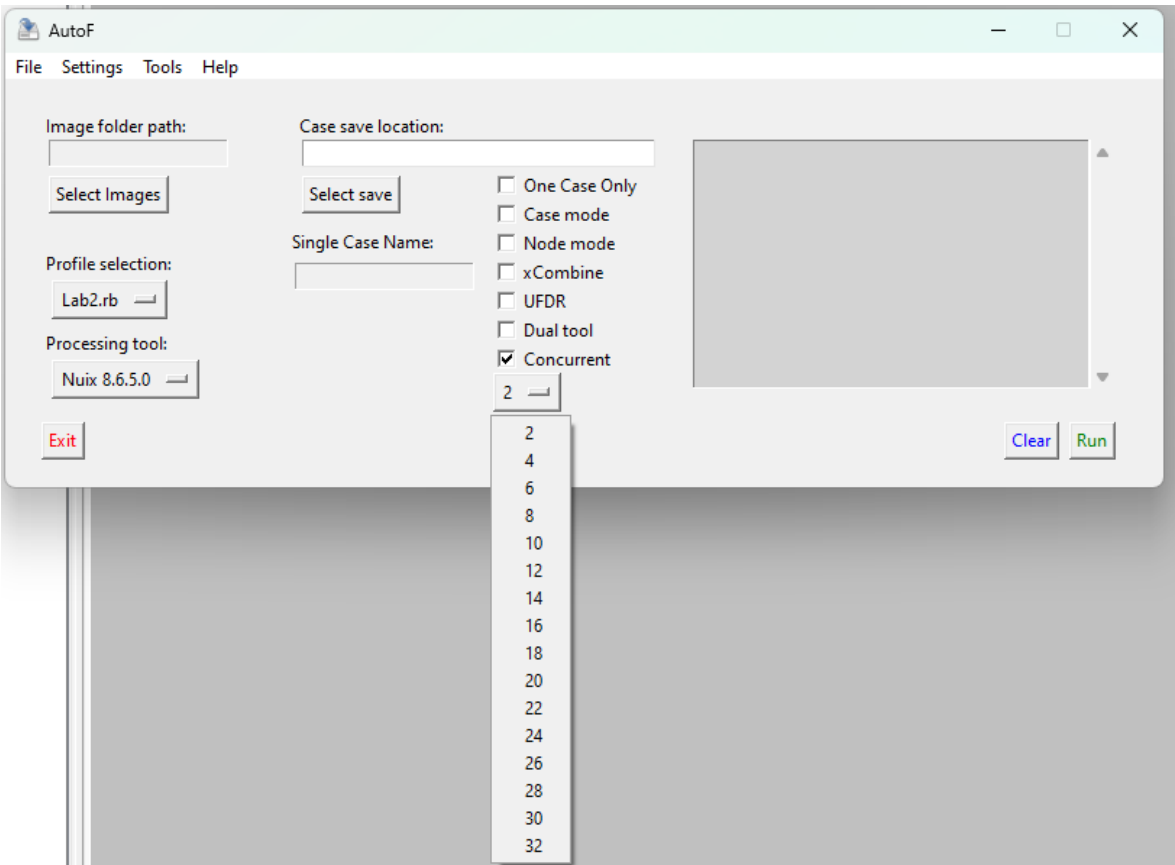
The CFG will need to include the following selection:



The tool will warn this is experimental.



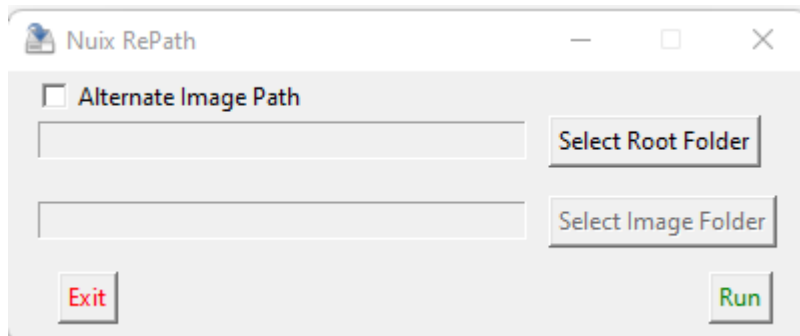
Select how many instances you would like to run, currently this only works with standard modes.



11. Tools

Nuix RePath:

Nuix RePath, will find all cases within the given directory, inspect the evidence locations and update them if it can find them. This is useful if you need to move your data. If your images and cases do not share a root directory you can select an alternative path for the images. A report of changes is created and all evidence stores are backed up before changing.



Case Info:

Case Info will produce a report informing the user of the case path and its current version. Useful if you have recently upgraded software and want to check what version to use before a case is automatically upgraded.



12. Bug Reporting

Email: admin@autof.uk

Forum: www.autof.uk/Forum/