

Your Mission: Leverage the power of X-Ways to work with an F-Response FCTar archive



Important Note

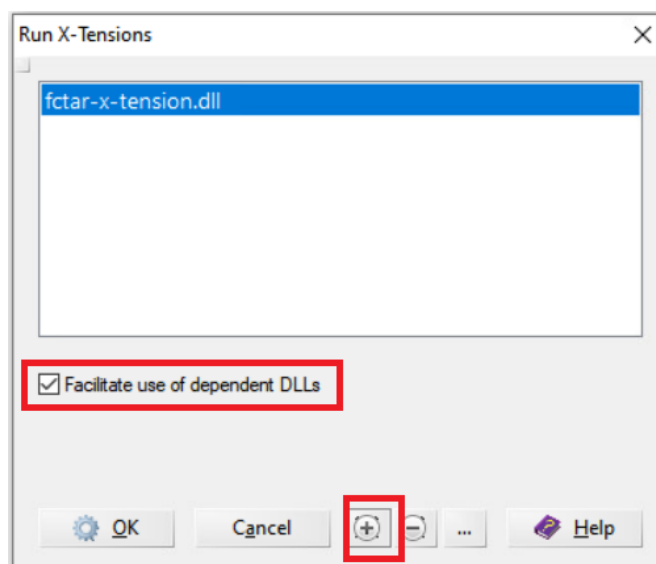
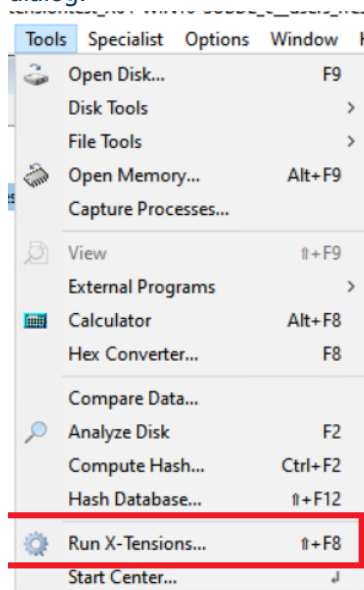
You will need a licensed copy of X-Ways Forensics, the F-Response Collect FCTar X-tension dll (fctar-x-tension.dll), and your FCTar file created with F-Response Collect to perform the steps in this guide.

The fctar-x-tension.dll is part of F-Response Collect version 8.7.1.36+ and can be found in your program files\f-response collect folder on your examiner computer.

The standard format for targeted custom collections using F-Response Collect is FCTar. It's an internally designed archive similar to the historical Tape Archive Format (TAR). We provide functionality in F-Response Collect to extract these FCTar archives to the destination of your choice. However, there is also an option to extract individual files or do more in-depth processing of the FCTAR archive contents without extraction by leveraging the power of X-Ways Forensics.

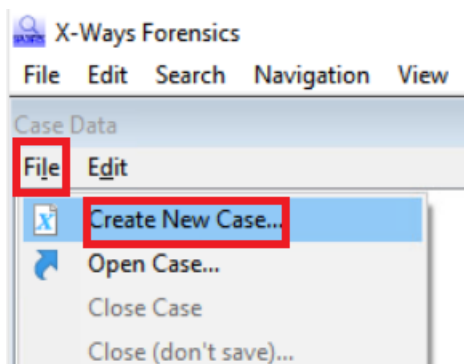
Step 1: Add the X-tension

Open X-Ways Forensics and navigate to *Tools – Run X-Tensions...* click the add button and navigate to the fctar-x-tension.dll to enable FCTar functionality. Do not press OK. Use the "X" to close the dialog.

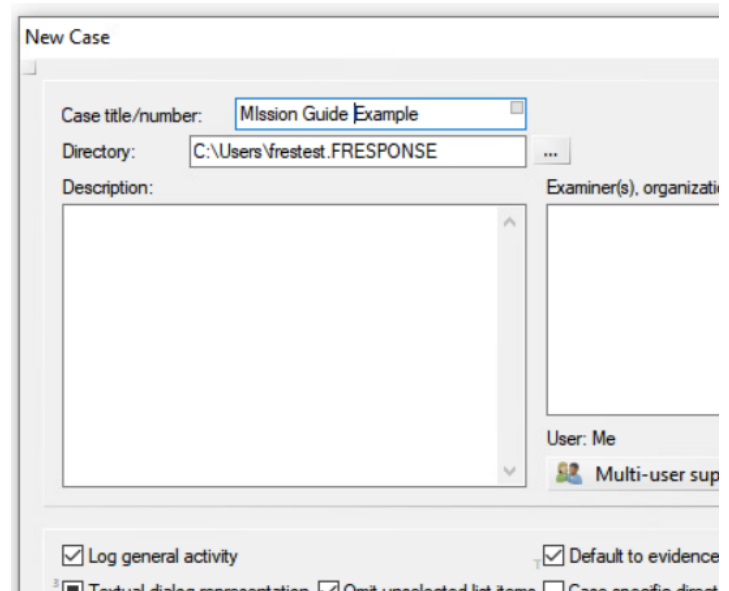


Step 2: Create a case in X-Ways.

Next, you'll need to create a new case in X-Ways.

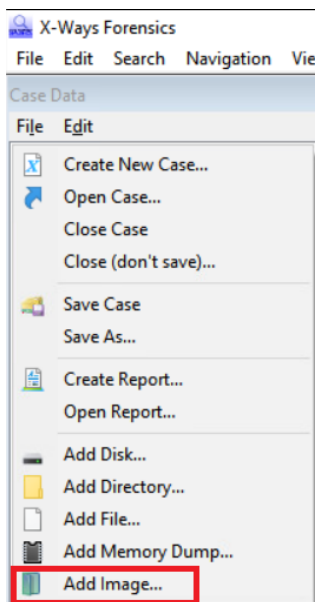


Assign a name to your case and fill in any additional options as needed.

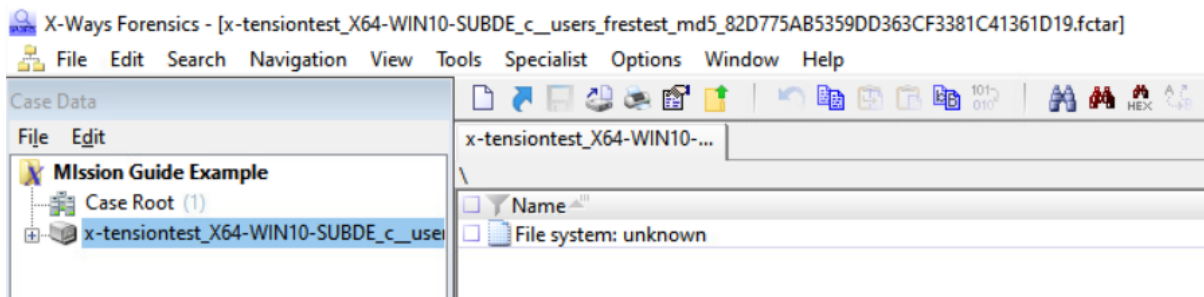


Step 3: Add your FCTar file to the newly created case

Under **Case Data** in your newly created case go to **File – Add Image...**

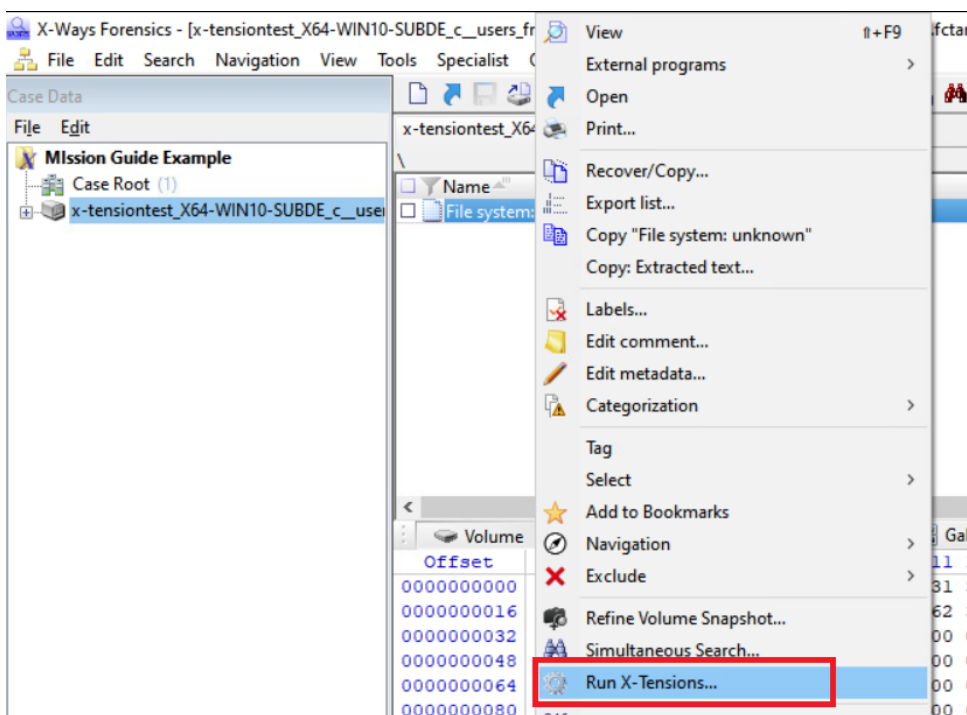


Navigate to your FCTar file and add it to the newly created case.

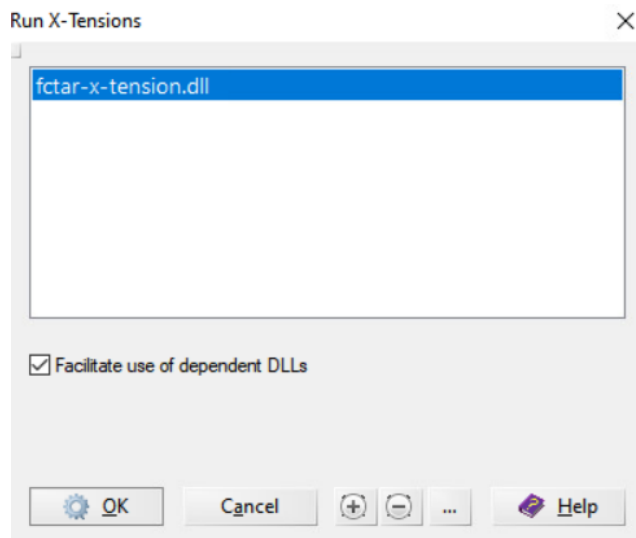


Step 4: Apply the X-Tension to your FCTar file

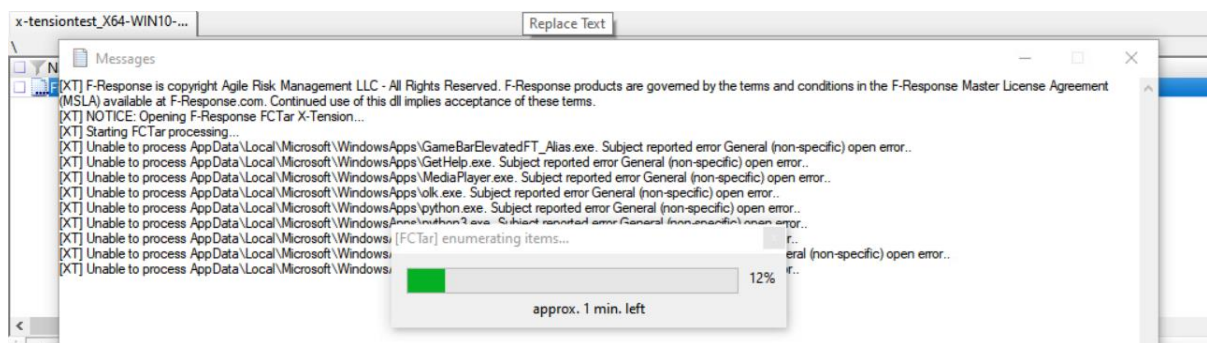
The image file will appear in your case with an unknown file system. Right click on **File system: unknown** (your image file) and select **Run X-tensions...**



Choose **fctar-x-tension.dll** from your list of x-tensions and then click **OK**

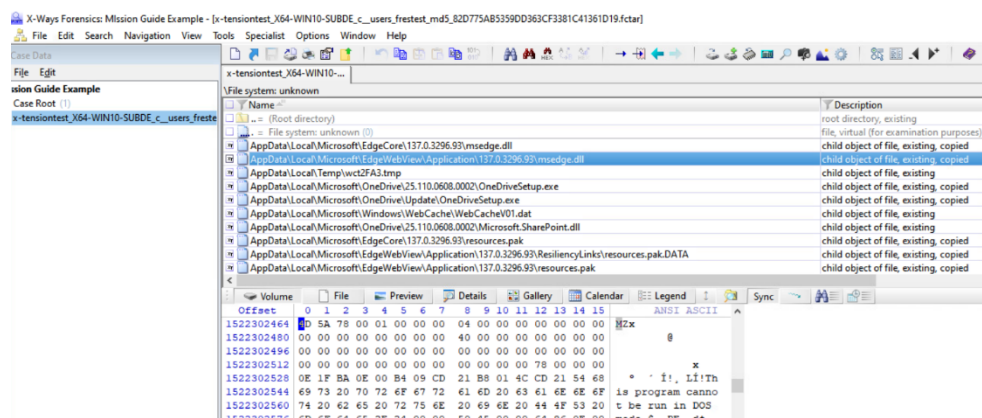


X-Ways will begin processing your FCTar file. You may see some errors. These are completely normal, as some files may not have been collected. Any errors will be reported in the Messages window.



Step 5: Review the Completed Collection

Once processing completes, close the Messages window and right-click on your image file again. Choose **Explore**:



You now can review/analyze/extract specific files from your FCTar archive.

Troubleshooting and FAQ