Case Summariser

X-Tension

User Manual

Introduction

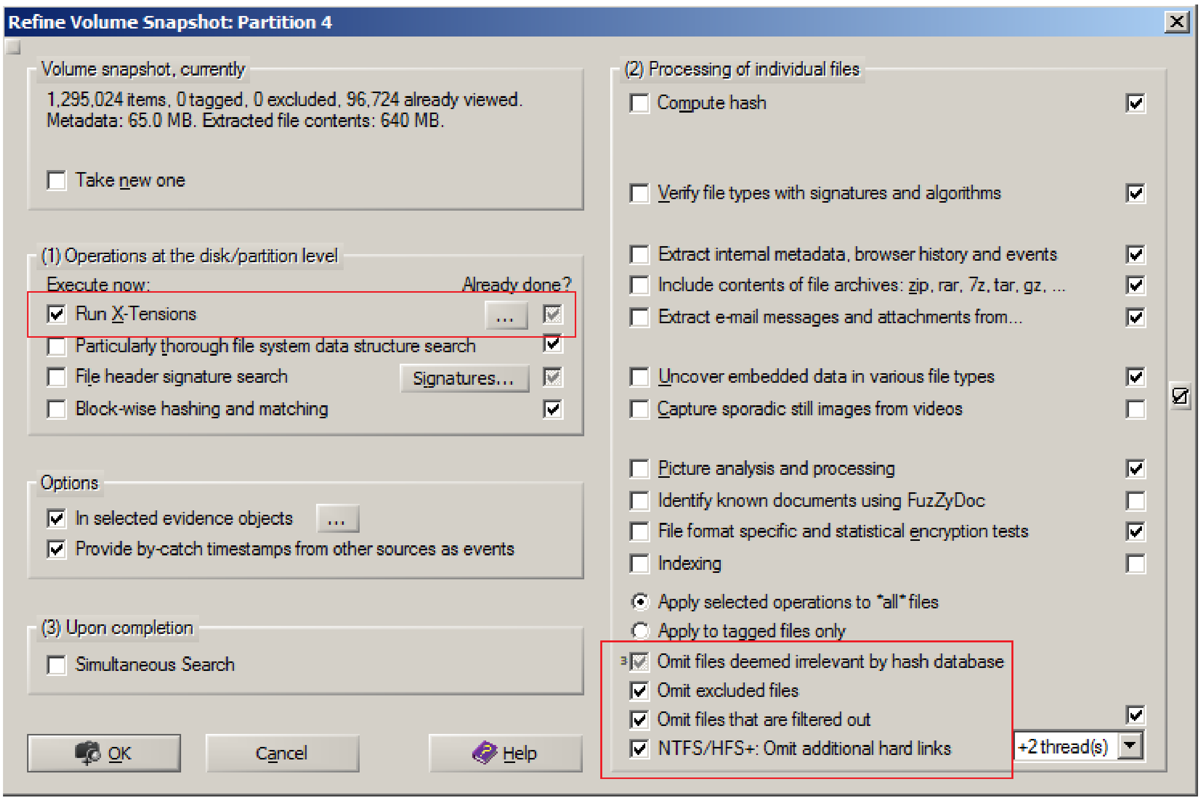
The Case Summariser X-Tension is 64-bit DLL for X-Ways Forensics x64. When loaded and executed via the 'Refine Volume Snapshot' feature of X-Ways Forensics, it will traverse the selected evidence object(s) and create an HTML web based report to a folder of the users choosing. The report features a table of figures that give the user or investigation team an indication of the volume of data for that evidence object, by file type category.

For example MyPhoto.jpeg and MyPhoto.png are two different types of picture file type (2 files), but they are both in the file category of "Pictures", so "Pictures" = 2. This X-Tension reports category count, not type count.

How to use

The X-Tension requires XWF v18.9 or above. The ability to call the file category was only made available to the API in v18.9, so if users try to execute with earlier versions, the output will not be correct.

1) Launch X-Ways Forensics.
2) Open a case
3) View the RVS (Refine Volume Snapshot) dialog via "Specialist → Refine Volume Snapshot" dialog window (or press F10). Tick the box for "Execute X-Tensions" and navigate to the DLL. Tick the box for "In selected evidence objects" and ensure your evidence object(s) are chosen. Also be careful with regard to filtering and exclusion options, because the X-Tension will skip files in accordance with these settings. Click OK. The X-Tension will ask the user for an output location. Trailing slash will be added if not done so by the user. As it runs it will display some output in the messages window and a progress indicator window.
4) On completion, HTML files will be saved to the user output location, named individually by evidence object.



Volume snapshot, currently

1,295,024 items, 0 tagged, 0 excluded, 96,724 already viewed.
Metadata: 65.0 MB. Extracted file contents: 640 MB.

☐ Take new one

(1) Operations at the disk/partition level

Execute now: Already done?

☑ Run X-Tensions ... ☑
☐ Particularly thorough file system data structure search ☑
☐ File header signature search Signatures... ☑
☐ Block-wise hashing and matching ☑

Options

☑ In selected evidence objects ...
☑ Provide by-catch timestamps from other sources as events

(3) Upon completion

☐ Simultaneous Search

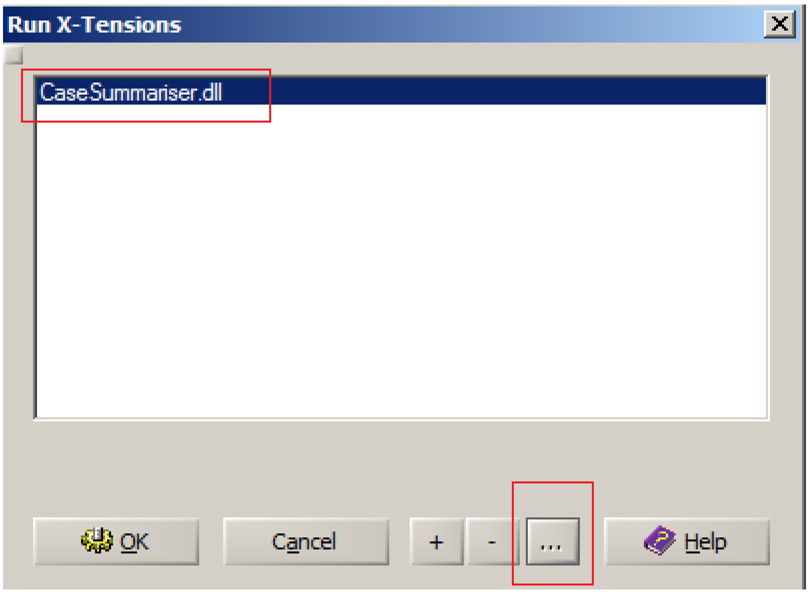
(2) Processing of individual files

☐ Compute hash ☑
☐ Verify file types with signatures and algorithms ☑
☐ Extract internal metadata, browser history and events ☑
☐ Include contents of file archives: zip, rar, 7z, tar, gz, ... ☑
☐ Extract e-mail messages and attachments from... ☑
☐ Uncover embedded data in various file types ☑
☐ Capture sporadic still images from videos ☐
☐ Picture analysis and processing ☑
☐ Identify known documents using FuzZyDoc ☐
☐ File format specific and statistical encryption tests ☑
☐ Indexing ☐

● Apply selected operations to "all" files
○ Apply to tagged files only

☑ Omit files deemed irrelevant by hash database
☑ Omit excluded files
☑ Omit files that are filtered out ☑
☑ NTFS/HFS+: Omit additional hard links +2 thread(s)

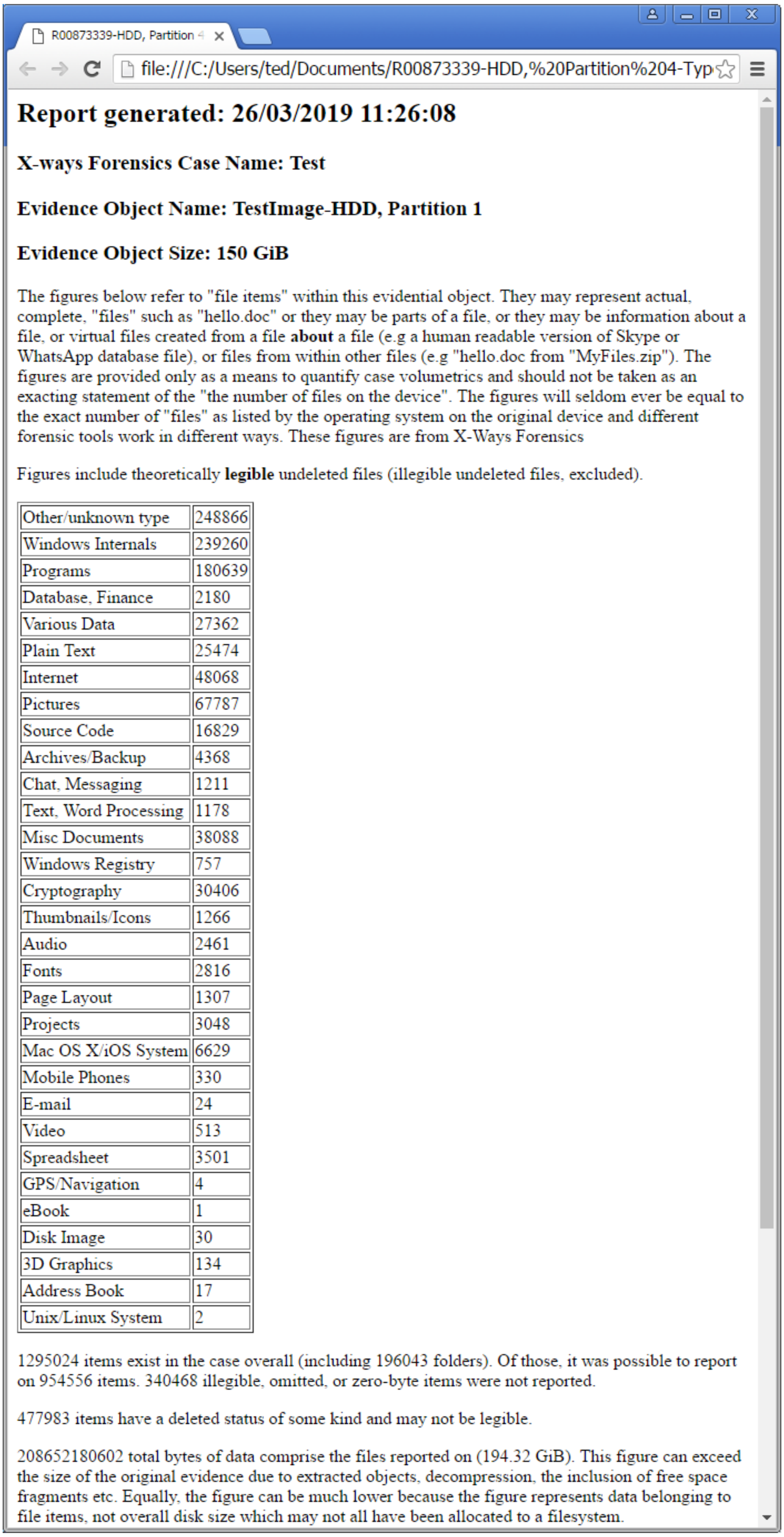
Figure 1 - RVS dialog window of XWF v19.7



CaseSummariser.dll

Figure 2 The X-Tension successfully loaded into XWF

The user can also read an “About” dialogue for the X-Tension by clicking the ellipsis (‘…’) button, as well as loading other X-Tensions to be executed at the same time.


R00873339-HDD, Partition 4
file:///C:/Users/ted/Documents/R00873339-HDD,%20Partition%204-Typ

Report generated: 26/03/2019 11:26:08

X-ways Forensics Case Name: Test

Evidence Object Name: TestImage-HDD, Partition 1

Evidence Object Size: 150 GiB

The figures below refer to "file items" within this evidential object. They may represent actual, complete, "files" such as "hello.doc" or they may be parts of a file, or they may be information about a file, or virtual files created from a file **about** a file (e.g a human readable version of Skype or WhatsApp database file), or files from within other files (e.g "hello.doc from "MyFiles.zip"). The figures are provided only as a means to quantify case volumetrics and should not be taken as an exacting statement of the "the number of files on the device". The figures will seldom ever be equal to the exact number of "files" as listed by the operating system on the original device and different forensic tools work in different ways. These figures are from X-Ways Forensics

Figures include theoretically **legible** undeleted files (illegible undeleted files, excluded).

Other/unknown type	248866
Windows Internals	239260
Programs	180639
Database, Finance	2180
Various Data	27362
Plain Text	25474
Internet	48068
Pictures	67787
Source Code	16829
Archives/Backup	4368
Chat, Messaging	1211
Text, Word Processing	1178
Misc Documents	38088
Windows Registry	757
Cryptography	30406
Thumbnails/Icons	1266
Audio	2461
Fonts	2816
Page Layout	1307
Projects	3048
Mac OS X/iOS System	6629
Mobile Phones	330
E-mail	24
Video	513
Spreadsheet	3501
GPS/Navigation	4
eBook	1
Disk Image	30
3D Graphics	134
Address Book	17
Unix/Linux System	2

1295024 items exist in the case overall (including 196043 folders). Of those, it was possible to report on 954556 items. 340468 illegible, omitted, or zero-byte items were not reported.

477983 items have a deleted status of some kind and may not be legible.

208652180602 total bytes of data comprise the files reported on (194.32 GiB). This figure can exceed the size of the original evidence due to extracted objects, decompression, the inclusion of free space fragments etc. Equally, the figure can be much lower because the figure represents data belonging to file items, not overall disk size which may not all have been allocated to a filesystem.

Figure 3 Sample output in Google Chrome (may differ to the most recent version of the product)