Magnet User Summit – April 12th 2022 Nashville, TN

How do you know it works as intended?

Kathryn Hedley

Why are you talking to me?

- Why examiners shouldn't rely on tools to 'just work'
  - True of both hardware and software
- Processes to validate tools
  - Example for file carving tools
- When to validate tools
- Resources to help

But why?!

- Tools can get things wrong:
  - Existing artifact not fully understood / parsed
  - New artifact not understood
  - Artifact format changes so no longer parsed
  - Artifact moves location so no longer found

- Can result in:
  - Omission of data
  - Incorrect output
  - Invalid output

Khyrenz Ltd

So… when?!

- Upon receipt, before first use
- After every major software/firmware update
  - Or, selected updates
  - Only use versions that have been validated on casework
- For hardware, also periodically
  - Once a year is a good guide
  - Remember: all hardware will fail eventually

Khyrenz Ltd

How?!

- Draw up known test data set(s)
- Document ‘correct’ expected result based on each data set

- Tool validation process:
  - Document the test data set(s) used
  - Document the tool and version you are validating
  - Use the test data set(s) with the tool and document all features tested
  - Document the actual results output from the tool for each data set
  - Document the comparison between actual and expected results
  - Document any limitations of the test

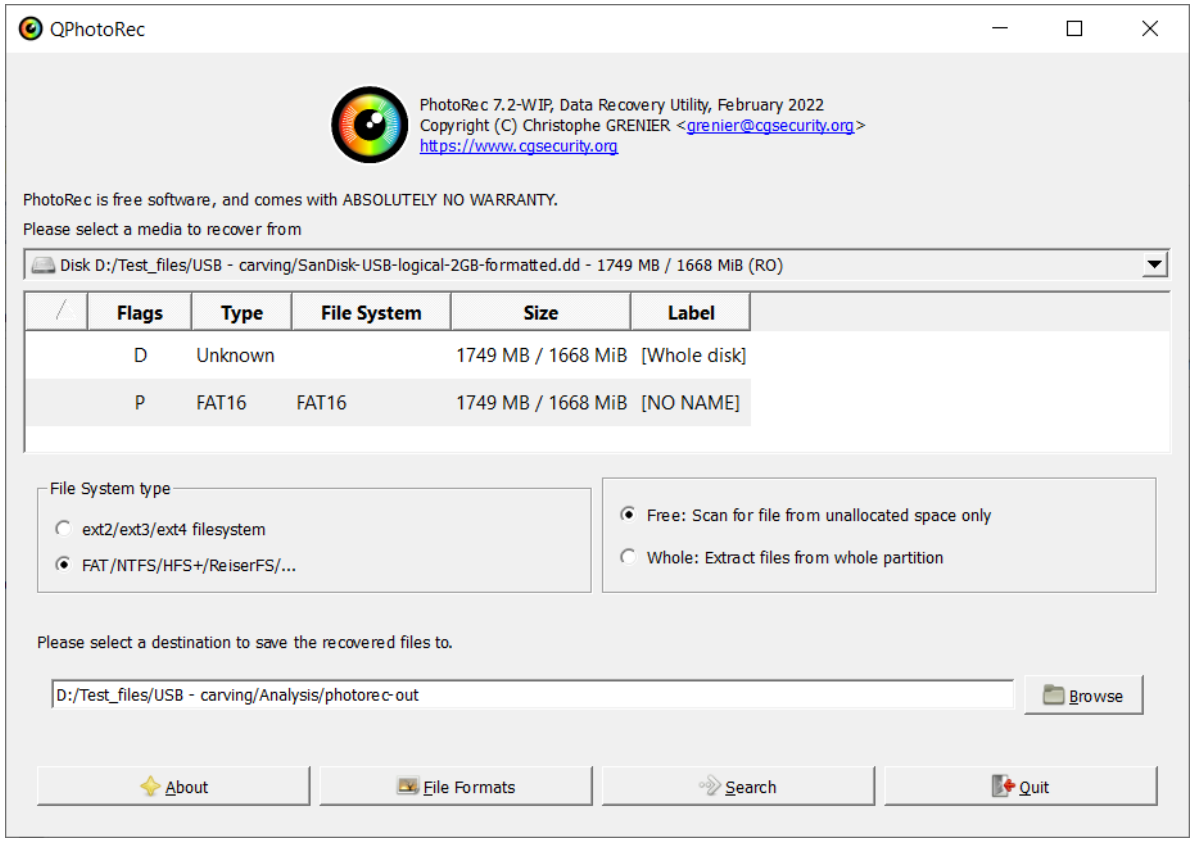
Khyrenz Ltd

Example – validating file carving tools

File Type	Filename	Origin	Size (KB)	MD5	SHA1
7z	AVI-7z	Created from AVI folder containing files above	20,393	ef75e866f686d0b96327db868beeeb49	fd4d1be9e8ffec39701d358838fed10437b0561b
7z	BMP.7z	Created from BMP folder containing files above	35,524	80135a9318bab1c3f7ecad273bd27588	e13b931de505c1c51ed6653273de8d9d2df67dcc
7z	DOC-XLS-PPT.7z	Created from DOC-XLS-PPT folder containing files above	6,935	7beb21147d65204836978 3cd804856b1d	edb13fe1559ba71696bb309840bfcff002222f799
7z	GIF.7z	Created from GIF folder containing files above	10,674	e37f6d192c7d14438be8cfe7b6d0554e	a70caf51870383aa5364cfc97b5db82879a3aa54
7z	JPEG.7z	Created from JPEG folder containing files above	10,790	49fc11289e554ce7b1382bb5173bbf08	4ccebb50966356b852883b9925fcd9e58f410fa2e
AVI	1280.avi	https://www.appsloveworld.com/avi-video-clips-free-download/	11,006	474b92e17b1ec3eeebadbf1297364f1b	8351e1bd6f08fe3419907140edd6fcbf00acc46e
AVI	Bubble Turning Into Ice.avi	https://www.appsloveworld.com/avi-video-clips-free-download/	8,850	3ed46e52a25b14bc4703b79de27163f0	85bc0cafcacdd41f6b81ace58bd33fba0c432c7d
AVI	file_example_AVI_1920_2_3MG.avi	https://file-examples.com/index.php/sample-video-files/sample-avi-files-download/	2,227	c52759dcc482673b861465339db8f6c2	573400d5d649e6ce8d9c02725e70618a17cd631f
AVI	file_example_AVI_480_750kB.avi	https://file-examples.com/index.php/sample-video-files/sample-avi-files-download/	726	9d22d2bfe1d41272 63cadf0fa96ef8d	a188ed66e68ff77729b8cfac92913427ab6b1677f
AVI	sample-avi-file.avi	https://www.learningcontainer.com/sample-avi-video-file-download/	8,130	b8358ab72a4d60eb29926278fc2d1f4e	246eecb40534 87a61914510389ec300bdef7f3c6
BMP	GRN.BMP	https://www.fileformat.info/format/bmp/sample/index.htm	85	64982d68b32b3fc0f7d1178f8efe6d7	b367e7e0d05e6f1bd769f39bd3b5e2e7d4e6bb62
BMP	MARBLES.BMP	https://www.fileformat.info/format/bmp/sample/index.htm			2740b0426 19b4
BMP	RAY.BMP	https://www.fileformat.info/format/bmp/sample/index.htm			6dc4040b805e43b6
BMP	sample_5184×3456.bmp	https://filesamples.com/formats/bmp			45d441d771b418e
BMP	Small Sample BMP Image File Download.bmp	https://www.learningcontainer.com/sample-bmp-file-for-testing/			8d3e652c5d64604
BMP	Yellow_star.bmp	Created by khedley			eccdd28ee7f76fb
DOC	file-example_1MB.doc	https://file-examples.com/index.php/sample-documents-download/			1f4cc6f4acc92c
DOC	SampleDOCFile_200kb.doc	https://sample-videos.com/download-sample-doc-file.php			37327550c22da8e
DOC	SampleDOCFile_5000kb.doc	https://sample-videos.com/download-sample-doc-file.php			0545659d6d0c2e3
DOC	USB connection artifacts.doc	Created by khedley			7a14e6b12cdf6ec
DOCX	15-MB-docx-file-download.docx	https://www.learningcontainer.com/sample-docx-file-for-testing/			223e2ef253de8fc
DOCX	file-example_500kB.docx	https://file-examples.com/index.php/sample-documents-download/			4b43c0320b9dd11e
DOCX	sample-docx-file-for-testing.docx	https://www.learningcontainer.com/sample-docx-file-for-testing/			97cefe067e237f8d
DOCX	Using WSL.docx	Created by khedley			43513f0198efb6f
GIF	giphy (1).gif	https://giphy.com/gifs/hatutah-sesame-street-yippers-Gd8gSo			432109f321feb9
GIF	giphy (2).gif	https://giphy.com/gifs/bicycle-beta-howtomob-OJYL1FFrCx00			de58888f3d6416b95
GIF	giphy.gif	https://giphy.com/gifs/internet-pizza-computer-ZH5o2IacOA8Y			21565d7e6ec96c18
GIF	How+do+I+computer+I+decided+to+try+myself+at+	https://funnyjunk.com/channel/ponytime/How+do+I+computer			1aeb08292b1b4f
GIF	undefined - Imgur.gif	https://imgur.com/gallery/NVoF3Zl			4108943d8d45a
JPEG	file_example_JPG_500kB.jpg	https://file-examples-com.github.io/uploads/2017/10/file_exa			f4693952dc7cd1845
JPEG	IMG_2575.JPG	Created by khedley			8b0cd850f22936d
JPEG	IMG_3385_cropped.jpg	Created by khedley			3f4080646cf7ee
JPEG	IMG_3973.JPG	Created by khedley			80226eb2edc7d2fe
JPEG	IMG_3977.JPG	Created by khedley			c1313a952810bd45
JPEG	istockphoto-1304263738-170667a.jpg	https://unsplash.com/s/photos/jpg			62b700212eee44b
JPEG	photo-1533450718592-29d45635f0a9.jfif	https://unsplash.com/s/photos/jpg			f9446efe0a7c22b
MOV	720.mov	https://www.appsloveworld.com/sample-mov-file-download/			2b5b3eed397d97e0
MOV	Cloud Formation Video.mov	https://www.appsloveworld.com/sample-mov-file-download/			26f00d5888a3951
MOV	file_example_MOV_480_700kB.mov	https://file-examples.com/index.php/sample-video-files/sample			5f697fe949f9daf2
MOV	sample_960x400_ocean_with_audio.mov	https://filesamples.com/formats/mov			cd17e425effed954
MOV	sample-mov-file.mov	https://www.learningcontainer.com/mp4-sample-video-files-d			fc3942e9a71ed896
MP3	file_example_MP3_700KB.mp3	https://file-examples.com/index.php/sample-audio-files/sample			190680715ee10c3
MP3	Kalimba.mp3	https://www.learningcontainer.com/sample-audio-file/			468bd762beda405e
MP3	sample3.mp3	https://filesamples.com/formats/mp3			29d8fda9dbefad5
MP3	sample4.mp3	https://filesamples.com/formats/mp3			761b6b1d16549a
MP3	Symphony No.6 (1st movement).mp3	https://filesamples.com/formats/mp3			775ce775e518dac
MP4	file_example_MP4_1920_18MG.mp4	https://file-examples.com/index.php/sample-video-files/sample			bdf41b69229 1730
MP4	giphy360p (1).mp4	https://giphy.com/explore/download			e76b4b45d851c
MP4	giphy360p.mp4	https://giphy.com/explore/download			02e2dbdb765dccc2
MP4	sample_1280x720_surfing_with_audio.mp4	https://filesamples.com/formats/mp4			88aa548eeddc3e1
MP4	sample_960x540.mp4	https://filesamples.com/formats/mp4			a0ed9757cf78cbc
MP4	sample-mp4-file.mp4	https://www.learningcontainer.com/mp4-sample-video-files-d			1c17309e0f941
PDF	file-example_PDF_1MB.pdf	https://file-examples.com/index.php/sample-documents-download/			0d1851216975fdf
PDF	file-example_150kB.pdf	https://file-examples.com/index.php/sample-documents-download/			1d3e066cfe712b0e
PDF	pdf.pdf	http://www.pdf995.com/samples/pdf.pdf			e784d7c1e27fc68
PDF	PinePhone_Data_Locations_Cheatsheet_khedley.pdf	Created by khedley			e45377ebe800bd3
PDF	PinePhone_Poster_khedley.pdf	Created by khedley			4e05bcaf9fbd3b
PDF	sample.pdf	http://www.africau.edu/images/default/sample.pdf			64f926a5f59b72
PNG	2cd43b_16d40260a2274e6fb87d101c321eac17	https://www.freepngs.com/dragon-png-images			529eb3c1ebe3aa5
PNG	2cd43b_dae95a985dde42a3af5a63b597f45ac9	https://www.freepngs.com/dragon-png-images			f58aaa431944e6a
PNG	pngwing.com (1).png	https://www.pngwing.com/en/free-png-zwfuf			5defb5eeafee28
PNG	pngwing.com.png	https://www.pngwing.com/en/free-png-byvsx			8326693a4899e3d
PNG	transparent-maple-leaf-5f8ec1dd91fa41.5756616	https://www.subpng.com/png-dxqbtf/			89e6ecf90f7372
PNG	transparent-owl-icon-autumn-icon-60b5ed3257	https://www.subpng.com/png-iqhnv2/			33293bcb84d7749d
PPT	file_example_PPT_1MB.ppt	https://file-examples.com/index.php/sample-documents-download/			fb650cf4da6ae23
PPT	file_example_PPT_250kB.ppt	https://file-examples.com/index.php/sample-documents-download/			2ea72ebe53dbe386
PPT	PinePhone Forensics.ppt	Created by khedley			1e97a54adf02aa44
PPTX	160930-artificial-intelligence-template-16x9.ppt	https://www.free-power-point-templates.com/free-machine-le			5d5171e2afacf10e
PPTX	pptx1.pptx	https://www.appsloveworld.com/sample-ppts-file/			7690c1bb6313c2a
PPTX	pptx2.pptx	https://www.appsloveworld.com/sample-ppts-file/			9fae0d5f79f1596
TIFF	CCITT_1.TIF	https://www.fileformat.info/format/tiff/sample/			61bbebe44a23568
TIFF	file_example_TIFF_10MB.tiff	https://file-examples.com/index.php/sample-images-download/			7065616ffbc3b9e
TIFF	FLAG_T24.TIF	https://www.fileformat.info/format/tiff/sample/			0739004 2f84e92b
TIFF	Sample-Tiff-File-download-for-Testing.tiff	https://www.learningcontainer.com/sample-tiff-file-for-testing/			0225838430424c
TIFF	Tiff-Image-File-Download.tiff	https://www.learningcontainer.com/sample-tiff-file-for-testing/			0ef99c8150196f
WAV	BabyElephantWalk60.wav	https://www2.cs.uic.edu/~i101/SoundFiles/			1f256a90d0e9745
WAV	bird_cow2.wav	https://www.wavsource.com/animals/animals.htm			7a8adca5735b63
WAV	crickets.wav	https://www.wavsource.com/animals/animals.htm			324d2b11764ed6d
WAV	Fanfare60.wav	https://www2.cs.uic.edu/~i101/SoundFiles/			64f959d419cf875
WAV	file_example_WAV_5MG.wav	https://file-examples.com/index.php/sample-audio-files/sample			c9ed9edcca07100e
WAV	taunt.wav	https://www2.cs.uic.edu/~i101/SoundFiles/			40bf9123880c5758
WMV	1280.wmv	https://www.appsloveworld.com/sample-wmv-video-file-free-d			9e0cd664c98a8e5ec
WMV	file_example_WMV_480_1_2MB.wmv	https://file-examples.com/index.php/sample-video-files/sample			fbca695b377b189
WMV	sample_3840x2160.wmv	https://filesamples.com/formats/wmv			3ee48e05ba392a2b
WMV	sample-wmv-file.wmv	https://www.learningcontainer.com/sample-wmv-video-file-do			21585c206a9b08a3
WMV	Video2.WMV	https://www.lehman.edu/faculty/hoffmann/itc/techteach/video/Video_samples.html	85	0ffd852019e8ed67440fdfd16a5abb30	66d457ecfcb8ee65c9f841f77ae757ab91aaa11c
XLS	file_example_XLS_10.xls	https://file-examples.com/index.php/sample-documents-download/sample-xls-download/	9	f7c4094f7ede3169e9214e155a22fbe4	e0cdb9c8a7da39f978772934 5fd9bd617d02d539
XLS	file_example_XLS_1000.xls	https://file-examples.com/index.php/sample-documents-download/sample-xls-download/	657	5b938869b5e945cf909959f23f83af8ed	3e0d4a8ecb77244d2580b15cd9f0766cd317b073
XLS	USB_artifacts.xls	Created by khedley	28	6f5e4bd5edc16736b453693aed21e88b	39e4e8f0a7895 78d55951d9fc5e00a5ec86d6b16
XLSX	file_example_XLSX_1000.xlsx	https://file-examples.com/index.php/sample-documents-download/sample-xls-download/	42	60f55bf2cb2676af14074764c2b8291	0dce77e811e9f631913c88e1b04991a868fcc93d
XLSX	file_example_XLSX_50.xlsx	https://file-examples.com/index.php/sample-documents-download/sample-xls-download/	8	5c256f2de57126cac5acfc29ce42ca754	cd49970 94ad009f938017fd94a1d44a1241003b6
XLSX	sample3.xlsx	https://filesamples.com/formats/xlsx	13	127e8da71a8d424253 74f47c7e7d6f21	4cd2c22ee2a7478fc0d0ddaa5d3cd565ff269520
ZIP	DOCX-XLSX-PPTX.zip	Created from DOCX-XLSX-PPTX folder containing files above	45,381	e7eb188cc57c57c9d64c5eac0ecdfec77	3bc958d3d36d7342d4a209def63d89a3b9c55ca
ZIP	MOV.zip	Created from MOV folder containing files above	47,973	619f41b8d49d88f8c93f4881a28401c4	d45075b85ebb217305eb6bac10e7f5e9a1edaeb9
ZIP	MP3.zip	Created from MP3 folder containing files above	25,633	1760d65e5ae53dbf0f80908 8291a14dc6	7a144bcd5232c3e6936669e1ef6121ac3b94d3128
ZIP	PDF.zip	Created from PDF folder containing files above	2,646	d91df102df627f877f8a2ad79ff237aad	a1ea6e40d9161d0dc9fc546cd8b239689065cb464
ZIP	PNG.zip	Created from PNG folder containing files above	8,002	67e71fe0ae6904a3c45fe0e21e9a24be6	0a342d01ac70cb9cae282 5805bceed415f949f9

Row Labels	Count of Filename
7z	5
AVI	5
BMP	6
DOC	4
DOCX	4
GIF	5
JPEG	7
MOV	5
MP3	5
MP4	6
PDF	6
PNG	6
PPT	3
PPTX	3
TIFF	5
WAV	6
WMV	5
XLS	3
XLSX	3
ZIP	5
Grand Total	**97**

PhotoRec 7.2



- Add a raw disk image…
- Select destination folder
- Search

https://www.cgsecurity.org/wiki/TestDisk_Download

Khyrenz Ltd

Executive Summary

PhotoRec version 7.2 was run in its default configuration against the test image Khyrenz-FileCarvingImage-USB-logical-2GB-formatted.dd[1].

The below table is a summary of the test files that PhotoRec carved from this image.

File Type	Number of Test Files	Exact match	Usable match	Not found	False positive	Invalid file
7z	5	5				
AVI	5	5				
BMP	6	5	1			
DOC	4	4				
DOCX	4	4				
GIF	5	5				
JPEG	7	2		5		
MOV	5	5				
MP3	5	4		1		1
MP4	6	6				
PDF	6	6				
PNG	6	6				
PPT	3	3				
PPTX	3	3				
TIFF	5		5			
WAV	6	6				
WMV	5	2		3		
XLS	3	3				
XLSX	3	3				
ZIP	5	5				
Total	**97**	**82**	**6**	**9**	**0**	**1**
Percentage		**84.54%**	**6.19%**	**9.28%**		

As this table shows, 84.54% of the test files were recovered exactly; the SHA1 file hashes were a match to the original files. In total, 90.73% of the original files were recovered in a usable state and could be successfully viewed, with the remaining 9.28% of the original files not carved.

Eight of the original test files were not found within the image by PhotoRec. These were all JPEG or WMV file formats.

- Full validation report at:

https://www.khyrenz.com/resources/

Categories:

1. **Exact match**: SHA1 match to an original test file
2. **Usable match**: Carved file can be successfully opened and viewed, and appears similar to an original test file
3. **Not found**: No output resembling original file
4. **False positive**: Carved file is valid and can be opened/viewed, but is not similar to an original file
5. **Invalid file**: Carved file cannot be opened or viewed

Example – comparing file carving tools

MAGNET AXIOM™

X-Ways

```
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]
```

AXIOM 5.10.0.30634

- PROCESSING DETAILS (enable):
  - Calculate hash values
  - Find more artifacts
- ARTIFACT DETAILS (enable):
  - CUSTOM ARTIFACTS: Carved Archives
  - DOCUMENTS: Excel, Microsoft Office, PDF, PowerPoint, Word
  - MEDIA (all)
- Ignored carved embedded JPEG & PNG files

X-Ways Forensic 20.4

- F10 → File header signature search & Compute hash (MD5 and SHA1) → OK → <select all> → OK

Foremost 1.5.7

- foremost –i SanDisk-USB-logical-2GB-formatted.001 –o foremost-out
- md5deep foremost-out/*/* > foremost_md5.txt

Supported File Types By Default

```
BUILTIN FORMATS
      Recover files from a disk image based on file types specified by the user using the -t switch.

      jpg    Support for the JFIF and Exif formats including implementations used in modern digital cameras.

      gif

      png

      bmp    Support for windows bmp format.

      avi

      exe    Support for Windows PE binaries, will extract DLL and EXE files along with their compile times.

      mpg    Support for most MPEG files (must begin with 0x000001BA)

      wav

      riff   This  will  extract  AVI  and RIFF since they use the same file format (RIFF). note faster than running
             each separately.

      wmv    Note may also extract wma files as they have similar format.

      mov

      pdf

      ole    This will grab any file using the OLE file structure.  This includes PowerPoint, Word,  Excel,  Access,
             and StarWriter

      doc    Note  it  is  more  efficient to run OLE as you get more bang for your buck.  If you wish to ignore all
             other ole files then use this.

      zip    Note is will extract .jar files as well because they use a similar format.  Open Office docs  are  just
             zip'd  XML  files so they are extracted as well.  These include SXW, SXC, SXI, and SX? for undetermined
             OpenOffice files.  Office 2007 files are also XML based (PPTX,DOCX,XLSX)

      rar

      htm

      cpp    C source code detection, note this is primitive and may generate documents other than C code.

      mp4    Support for MP4 files.

      all    Run all pre-defined extraction methods. [Default if no -t is specified]
```

MAGNET AXIOM

Name	Description	Extensions
This field is required.	This field is optional.	This field is optional.
WordPerfect Files	WordPerfect Files	WP;WPD;WPG;WPP;WP5;WP6;WPF
Google WebP Images	WebP files - Header WEBPVP8	webp
Carved Audio	Carving for mp3 files with ID3 v2 header	
Carved Audio	Carving for mp3 files with ID3 v3 header	
Carved Audio	Carving for mp3 files with ID3 v4 header	
Carved Audio	Carving for WAV files - HEADER WAVEfmt	
Carved Audio	Carving for WAV files - HEADER WAVEJUNK	
Carved Archives	Zip header 1. Contents of Carved Archive files are not opened and searched.	
Carved Archives	Zip header 2. Contents of Carved Archive files are not opened and searched.	
Carved Archives	7zip. Contents of Carved Archive files are not opened and searched.	
Carved Archives	rar and rar5. Contents of Carved Archive files are not opened and searched.	

- Some file types not carved by default
  - Others can be added

```
foremost version 1.5.7
```

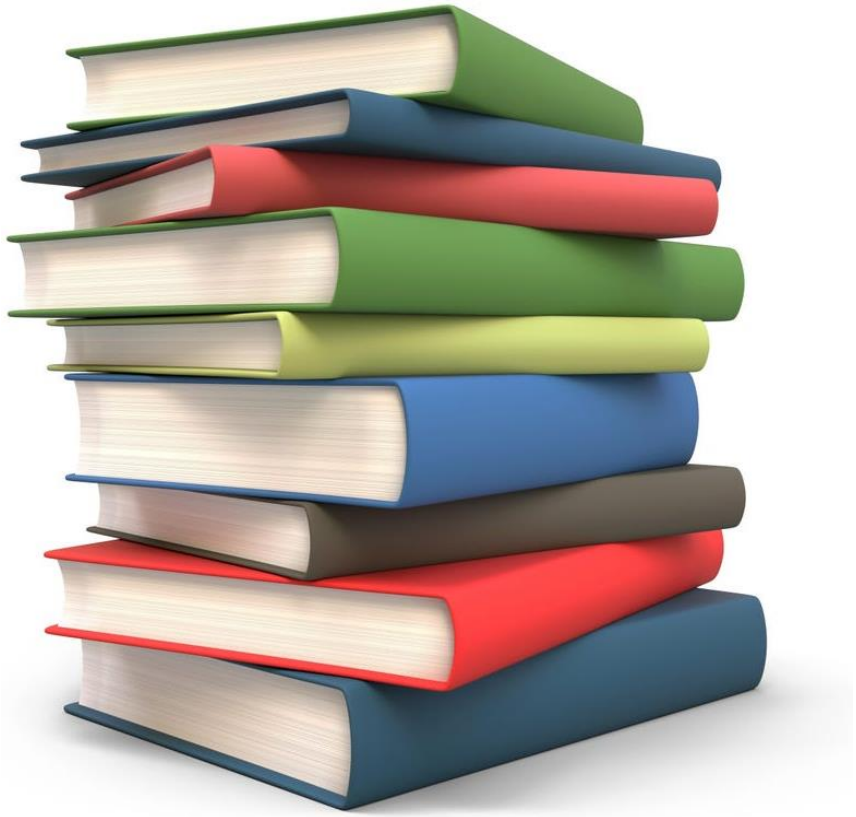
Tool Comparison Against 'Known' Data

Tool	Version	Hash match	Usable	Not Found	False Positive	Invalid	Found	Not Found
AXIOM	5.10.0.30634	55	12	30	0	22	**69.07%**	**30.93%**
Foremost	1.5.7	35	22	40	79	995	**58.76%**	**41.24%**
PhotoRec	7.2	82	6	9	0	1	**90.72%**	**9.28%**
X-Ways Forensic	20.4	81	16	0	1	2	**100.00%**	**0.00%**

*Caveat: This is ONE test against ONE dataset & ONE tool version

Khyrenz Ltd

Other Resources



- NIST Computer Forensics Tool Testing (CFTT) program
  - https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt
- SWGDE Guidelines for Validation Testing
  - https://drive.google.com/file/d/1vakqb14EJzq3eNkwv5ui40WYGP7IGCsD/view
- Sample carving test images (Brian Carrier):
  - http://dftt.sourceforge.net/

Khyrenz Ltd

Website: khyrenz.com
LinkedIn: https://uk.linkedin.com/in/kathryn-hedley-15638435
Twitter: https://twitter.com/4enzikat0r

Khyrenz Ltd