Defraser 1.4.1 – Quick overview of new ‘reference header’ feature

By Rikkert Zoun – Netherlands Forensic Institute – version: 11 December 2013

The main change from version 1.3.5 is the ‘*reference header*’ feature. This feature allows a user to specify one or more reference headers for each type of CODEC detector before scanning a file. If, while scanning, video frames are found that do not include the headers that are critical for playback, Defraser will try to use the set reference header(s) for decoding the video frame. Any (sequence of) frames that are decoded this way, will show up in the *Header* pane, including the reference header that was used. So, the frames are automatically ‘repaired’, without the need for manual repair using a *Workpad*. The automatically repaired video frames can be saved or sent to a third party player, just as before.

Reference header database

Defraser allows a database of reference headers to be created (see *Tools* → *Reference Header Database*). In the database screen (see figure 1), the reference headers for each CODEC detector that are already in the database can be viewed. The database can be exported (in XML-format), so it can be shared with others. When importing an existing database, it will be merged with the current database.

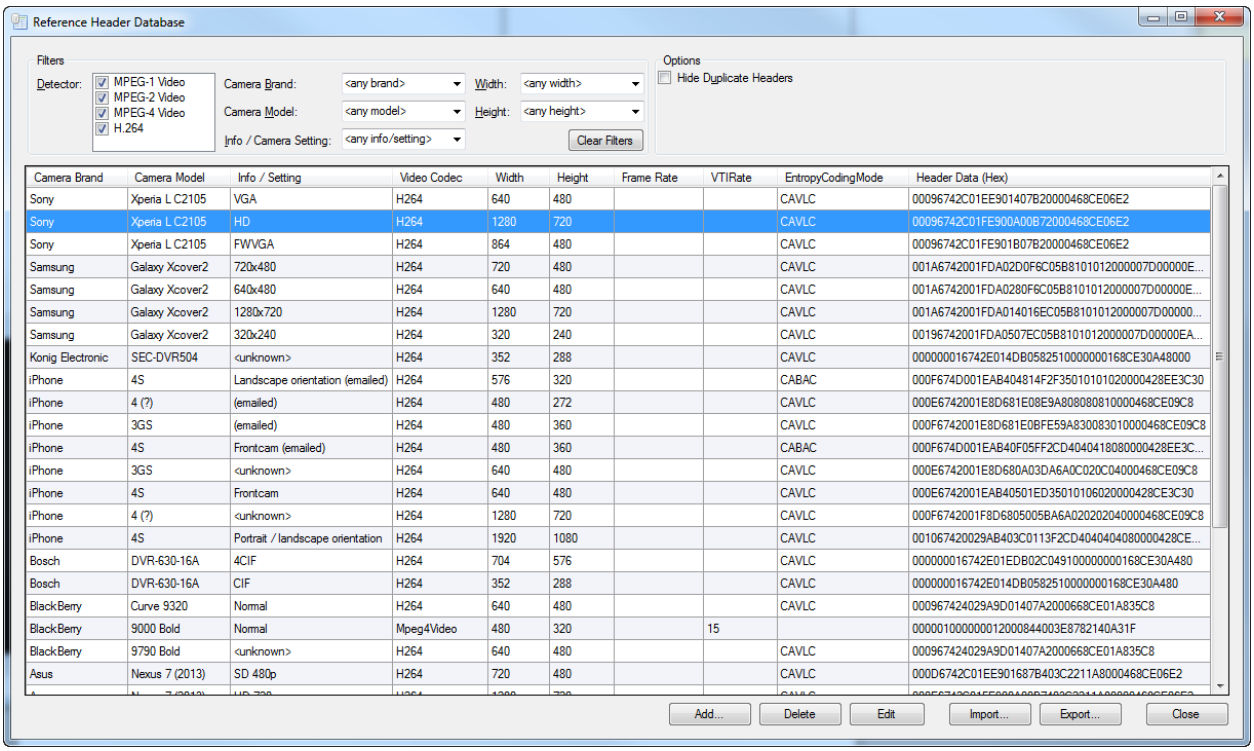


Figure 1: View of the reference header database management screen

To add a reference header to a database, simply click *Add…* and point to a file that contains a proper video header (for instance, a playable 3GP file recorded with a smartphone). Defraser will consequently scan the file with all of the CODEC detectors, and automatically determine which kind of video encoding was used. When an MPEG-1, -2, -4 or H.264 header is found, it is added to the database with a default name based on the name of the saved file. The record can be edited to show a more useful name. Any changes to the database will be saved when exiting Defraser. Note that the database will NOT store any of the video file image content in the database; only the headers specifically required for playback will be stored. The data that is stored is shown (in Hex) in the *Header Data* column.

Using reference headers

Setting reference headers to be used for scanning can be done in the *Add File* menu, see figure 2.

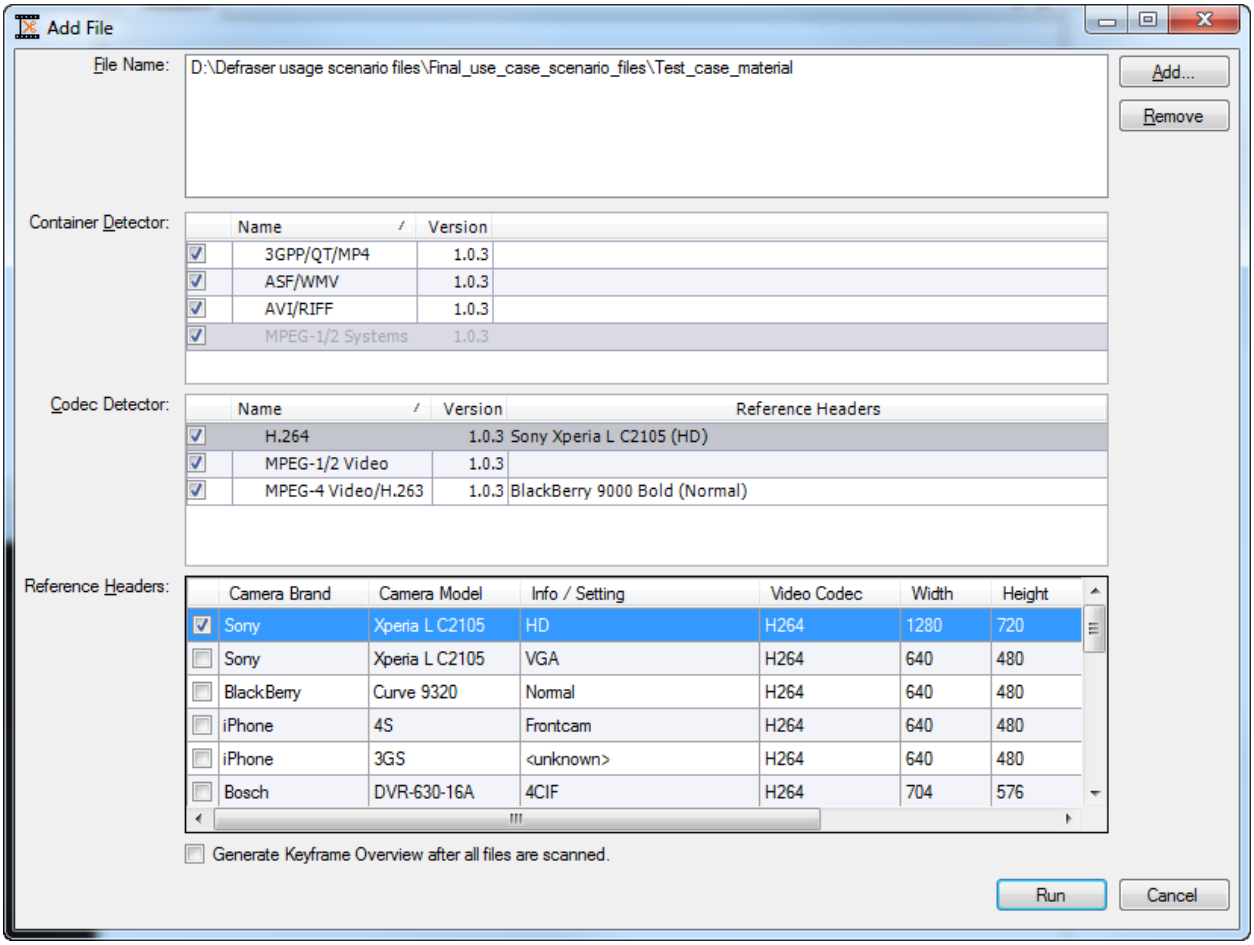


Figure 2: Activating reference headers in the Add File dialog

When selecting a CODEC detector, the reference headers that are available for that particular video encoding are shown. Check the ones that are to be used, and *Run* the scan as usual. Active *Reference Headers* are shown in the *Reference Headers* column for each CODEC detector. They will stay active for any files to be scanned within the project until turned off.

Using scan results with reference headers

At any point where reference headers were used for decoding video frames, they will show up in purple in the *Header* pane, see figure 3. To save the repaired fragment, select all headers in the Header pane, invoke the context menu by right-clicking, and choose *Save Selection As* (or, for H.264 fragments, choose *Convert To H.264 Byte Stream*[1] and then *Save Selection As*). In a similar way, the repaired fragment can be sent to an external program such as a media player by choosing the *Send Selection To* option from the context menu (also see *Tools* → *Edit Send To List…*).

[1] Note that H.264 video fragments that originate from a container file (such as 3GP or AVI) should be converted to the so-called *Byte Stream* format before saving or sending it to a media player. For any H.264 headers that do not already have this format, the context menu will show the *Convert To H.264 Byte Stream…* option, which can be followed by the *Save Selection As* or *Send Selection To* option as normal.

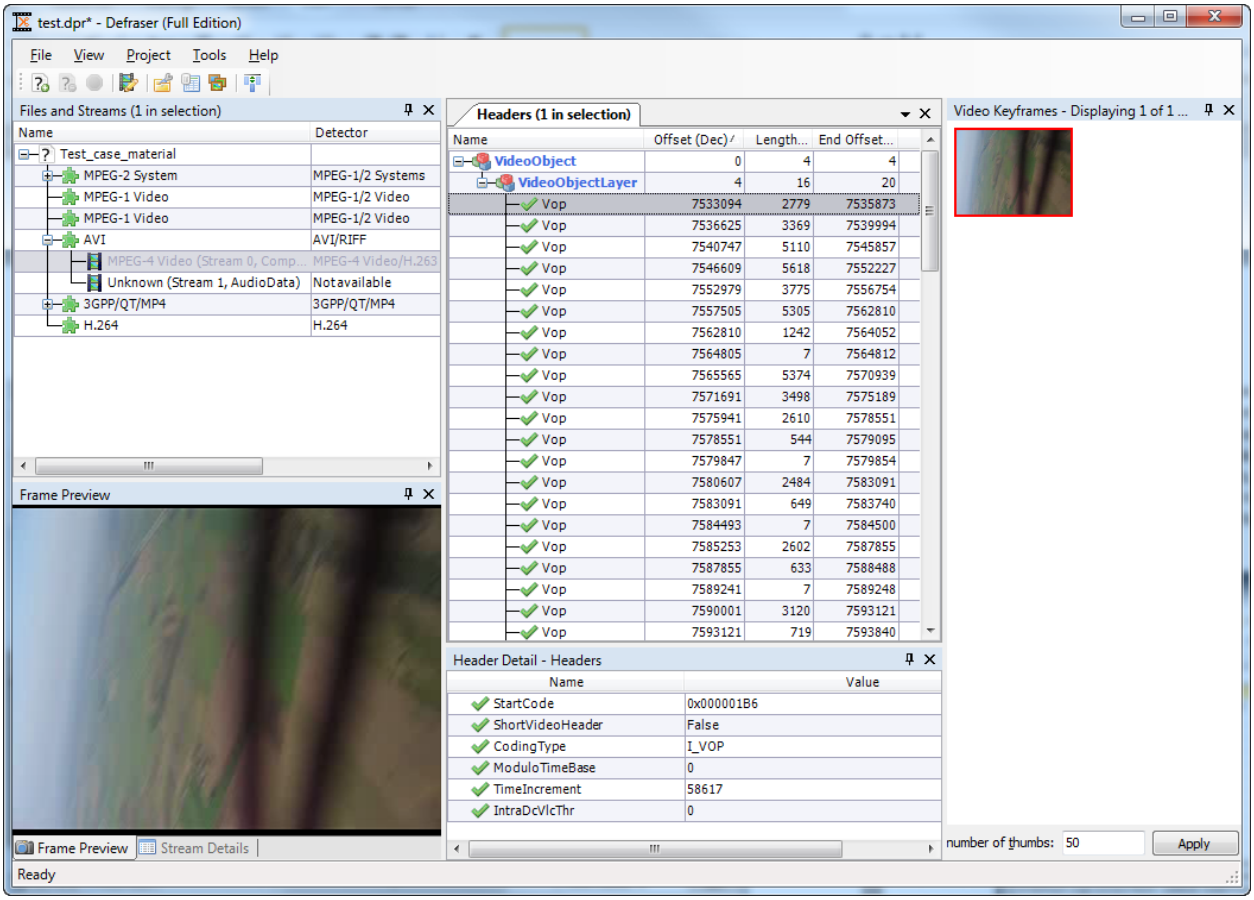


Figure 3: Header pane showing the reference headers (purple) that were used to decode some MPEG-4 Video frames

Reference headers vs. default headers

The new *Reference Header* functionality may sound quite similar to the already existing *Default Header* functionality, but there are some differences, see table 1.

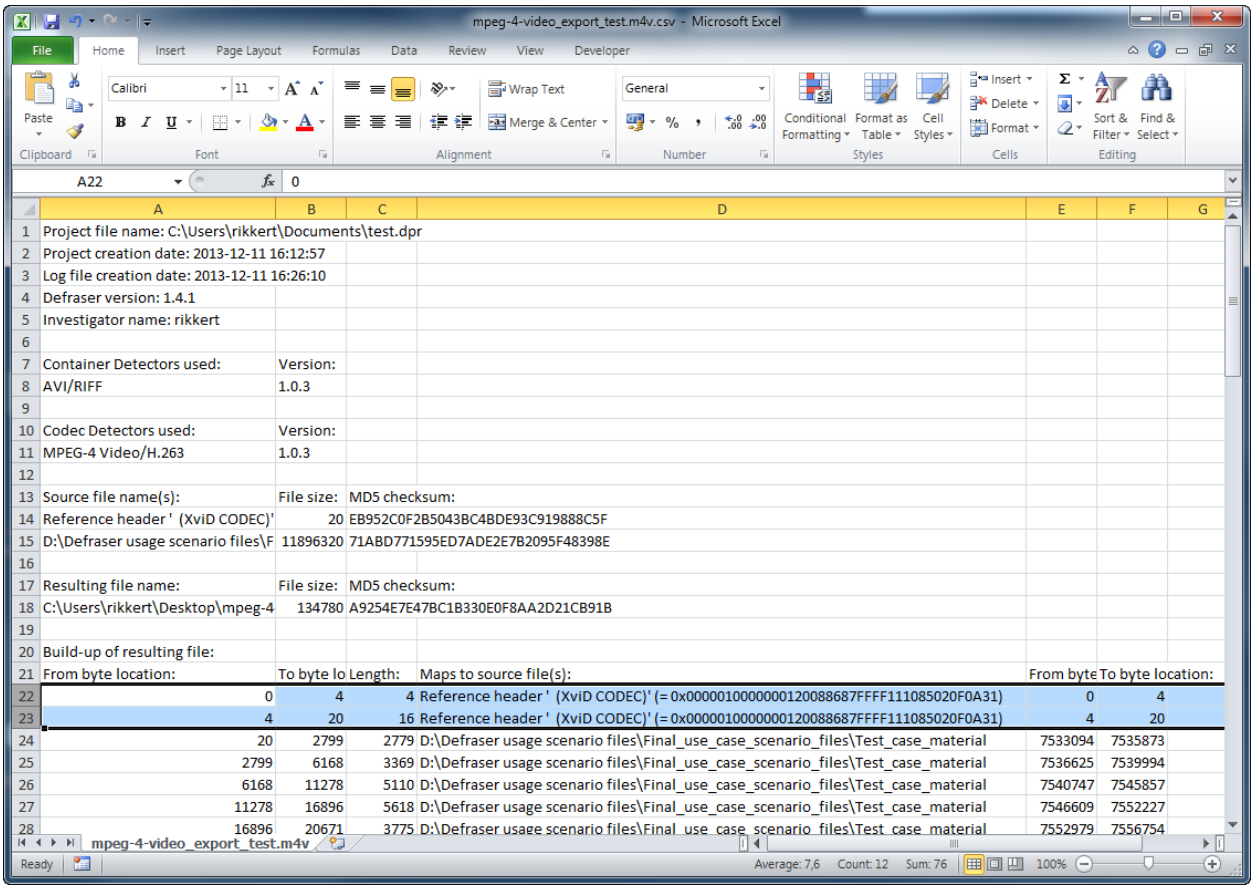
Reference Header	**Default Header**
Must be selected from a database of reference headers	Must be selected from a list of (video) files that are currently part of the project and were already scanned
Must be set BEFORE scanning a file	Can be set AFTER having scanned a file
Can be specified for each file to be scanned, so can be different for each scanned file in the project	Will be used for ALL keyframes in the project that use the relevant video encoding
Automatically adds the header to video file fragments that are decodable with the reference header (so: automatic repair)	Only shows result of using default header on keyframes, WITHOUT actually adding the header. Workpad functionality still has to be used for manual repair (so: just a preview, no automatic repair)
Usage can be recognized by purple-colored headers in *Header* pane	Usage can be recognized by yellow border around decoded keyframe

Table 1: Differences between Reference Header and Default header functionality

In some future version, the Reference Header functionalities will be expanded so that one can also rescan (part of) an already scanned fragment using a reference header of choice. Then, the Default Header functionality no longer has added value and will be removed.

Reference headers and the forensic integrity log

When saving any of the scan results, a forensic integrity log can optionally be saved as a comma-separated file (.csv) with the same name (see *Tools → Options → Create forensic integrity report for exports*). When your saved file contains a reference header, this will be noted in the forensic integrity log, see figure 4.



	A	B	C	D	E	F	G
1	Project file name: C:\Users\rikkert\Documents\test.dpr						
2	Project creation date: 2013-12-11 16:12:57						
3	Log file creation date: 2013-12-11 16:26:10						
4	Defraser version: 1.4.1						
5	Investigator name: rikkert						
6							
7	Container Detectors used:	Version:					
8	AVI/RIFF	1.0.3					
9							
10	Codec Detectors used:	Version:					
11	MPEG-4 Video/H.263	1.0.3					
12							
13	Source file name(s):	File size:	MD5 checksum:				
14	Reference header ' (XviD CODEC)'	20	EB952C0F2B5043BC4BDE93C919888C5F				
15	D:\Defraser usage scenario files\F	11896320	71ABD771595ED7ADE2E7B2095F48398E				
16							
17	Resulting file name:	File size:	MD5 checksum:				
18	C:\Users\rikkert\Desktop\mpeg-4	134780	A9254E7E47BC1B330E0F8AA2D21CB91B				
19							
20	Build-up of resulting file:						
21	From byte location:	To byte lo	Length:	Maps to source file(s):	From byte	To byte location:	
22	0	4	4	Reference header ' (XviD CODEC)' (= 0x00000100000000120088687FFFF111085020F0A31)	0	4	
23	4	20	16	Reference header ' (XviD CODEC)' (= 0x00000100000000120088687FFFF111085020F0A31)	4	20	
24	20	2799	2779	D:\Defraser usage scenario files\Final_use_case_scenario_files\Test_case_material	7533094	7535873	
25	2799	6168	3369	D:\Defraser usage scenario files\Final_use_case_scenario_files\Test_case_material	7536625	7539994	
26	6168	11278	5110	D:\Defraser usage scenario files\Final_use_case_scenario_files\Test_case_material	7540747	7545857	
27	11278	16896	5618	D:\Defraser usage scenario files\Final_use_case_scenario_files\Test_case_material	7546609	7552227	
28	16896	20671	3775	D:\Defraser usage scenario files\Final_use_case_scenario_files\Test_case_material	7552979	7556754	

Figure 4: Forensic integrity log showing which reference header was used in the saved file

Preventing incorrect usage of reference headers

In some cases, Defraser will think a video frame can be decoded with the set reference header, while it is in actuality not a suitable header. In such cases, no image information (grey image) or a garbled image is shown in the keyframe preview. To prevent this, it is advised to only use a reference header that is really expected to be used in the video file fragments in your case. For instance, when looking for video file fragments recorded by a BlackBerry 9000 Bold smartphone in a forensic copy of a memory card, only use a BlackBerry 9000 Bold reference header. That smartphone produces 3GP video files containing MPEG-4 Video, so the reference header should be set for the MPEG-4 Video CODEC detector (if present in the database, otherwise, make a reference recording and add it to the database first). Please note that most recorders have a variety of camera settings that can be used (such as the video resolution). Each setting may use a different header, so when investigating, make sure to try reference headers from each setting.

In some future version, some checks will be implemented to prevent usage of reference headers with video fragments that produce nonsensical results.