Design Tradeoffs for Developing Fragmented Video Carving Tools

By

Eoghan Casey and Rikkert Zoun

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

Design Tradeoffs for Developing Fragmented Video Carving Tools

Eoghan Casey (MITRE/DC3) & Rikkert Zoun (NFI)

DFRWS2014

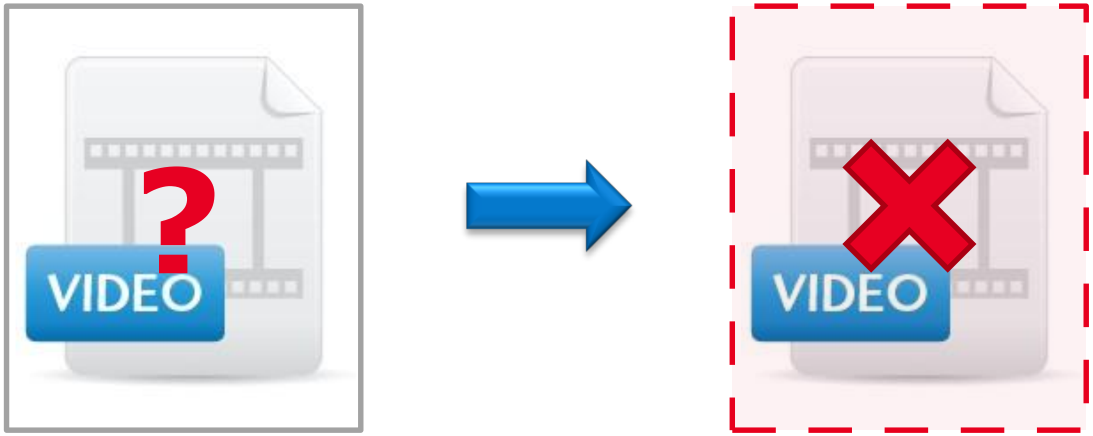
Example Scenario

Crime Recorded with smartphone camera

Smartphone is seized for forensic examination

Example Scenario

Investigation with conventional tools reveals



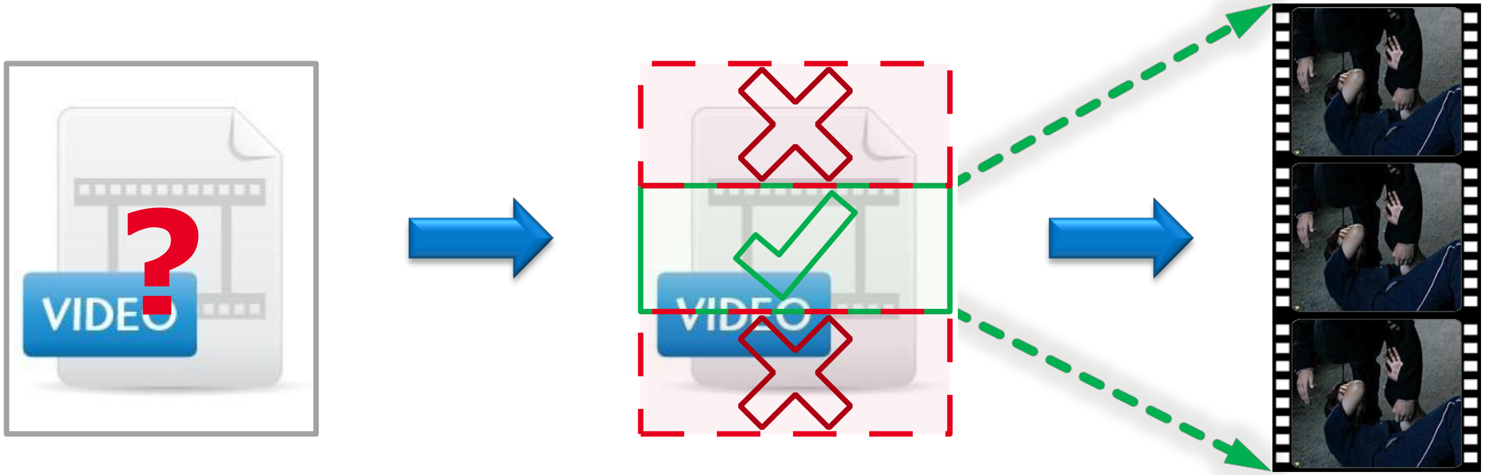
File was deleted and overwritten

No valid video file could be recovered

END OF INVESTIGATION?

Example Scenario

Closer inspection of smartphone reveals:



Deleted file was only **partly overwritten**.

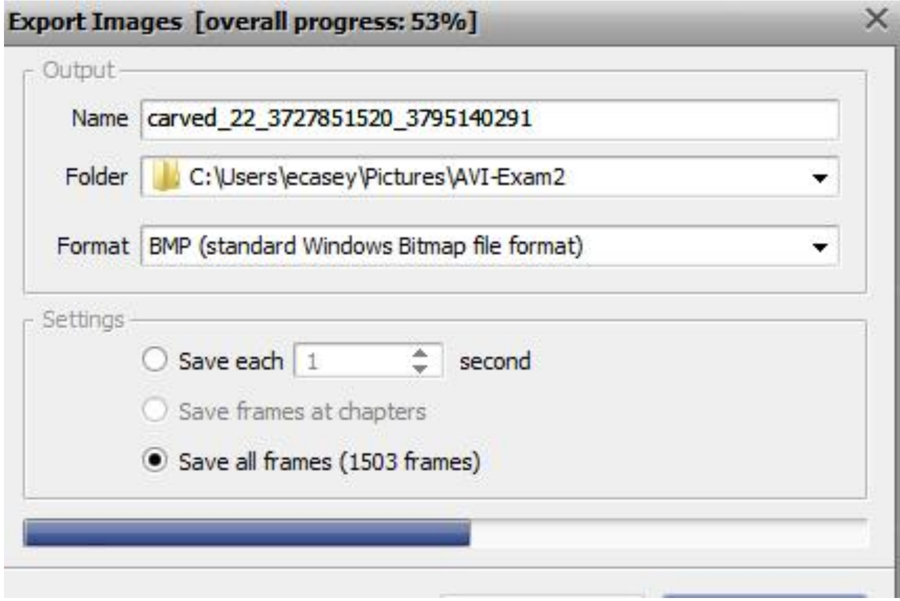
Fragment of video file was recoverable and images made viewable

Motivation

- Maximize playable video fragments
- Minimize missed fragments
- Minimize unplayable fragments

HARDER THAN YOU MIGHT THINK!

Personal Motivation



Export Images [overall progress: 53%]

Output

Name: carved_22_3727851520_3795140291

Folder: C:\Users\ecasey\Pictures\AVI-Exam2

Format: BMP (standard Windows Bitmap file format)

Settings

○ Save each 1 second

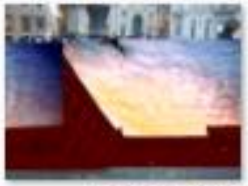
○ Save frames at chapters

● Save all frames (1503 frames)

carved_22_3727851520_3795140291_0001

carved_22_3727851520_3795140291_0002

carved_22_3727851520_3795140291_0003

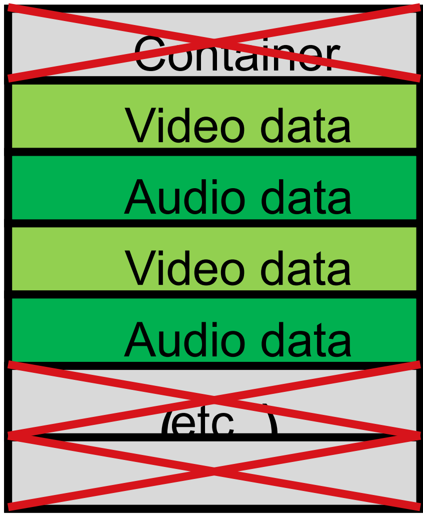


carved_22_3727851520_3795140291_0004

carved_22_3727851520_3795140291_0005

carved_22_3727851520_3795140291_0006

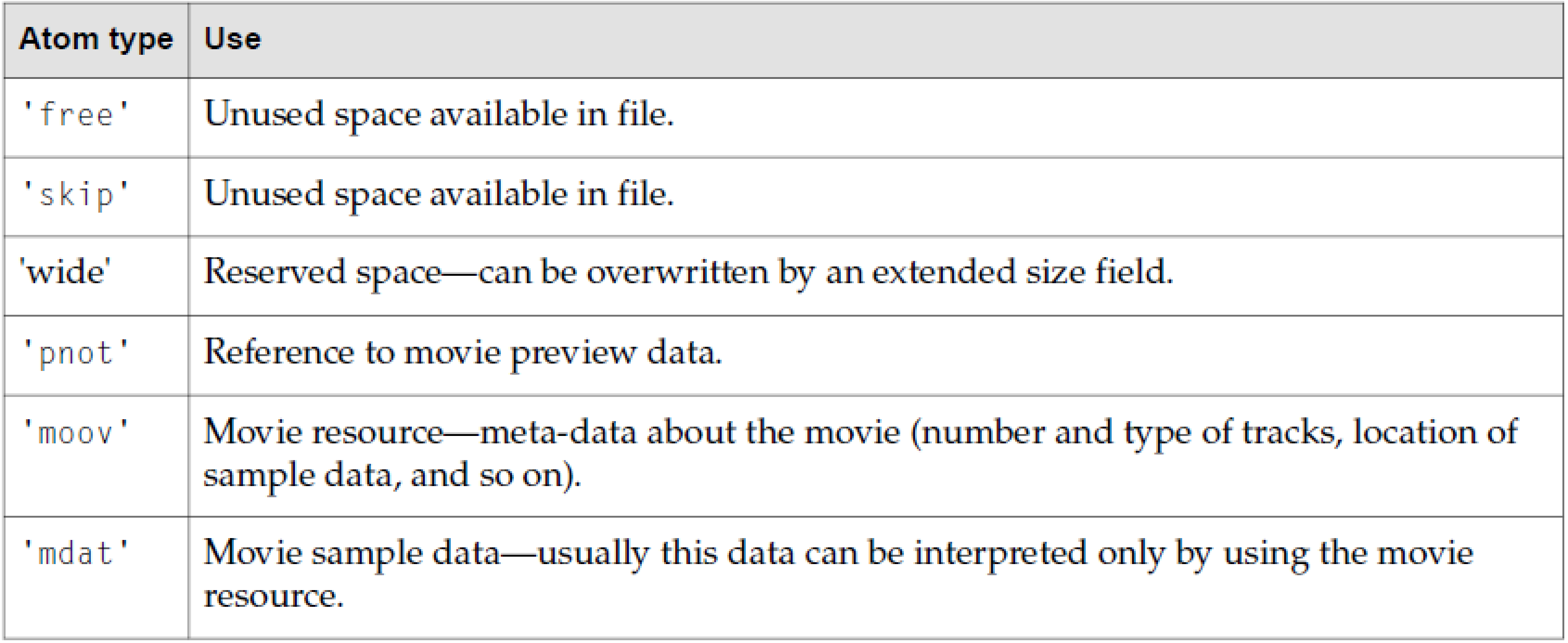
Fragmented Lessons



- DFRWS2007 Forensic Challenge
- Make use of cluster boundaries
- Fragment classification (Simson et al, 2010)
- Reassembly of compressed video data (Lewis, 2012)
- Reassembling individual frames (Na et al, 2014)

Fragmented Digital Videos

- Carving challenges
  - There are no safe assumptions
  - Flexible file specifications



Atom type	Use
'free'	Unused space available in file.
'skip'	Unused space available in file.
'wide'	Reserved space—can be overwritten by an extended size field.
'pnot'	Reference to movie preview data.
'moov'	Movie resource—meta-data about the movie (number and type of tracks, location of sample data, and so on).
'mdat'	Movie sample data—usually this data can be interpreted only by using the movie resource.

Strategy

- Rely on human review and reassembly
  - Requires person with knowledge of file formats
- Employ multiple automated methods
  - Results in more output to review, including dups

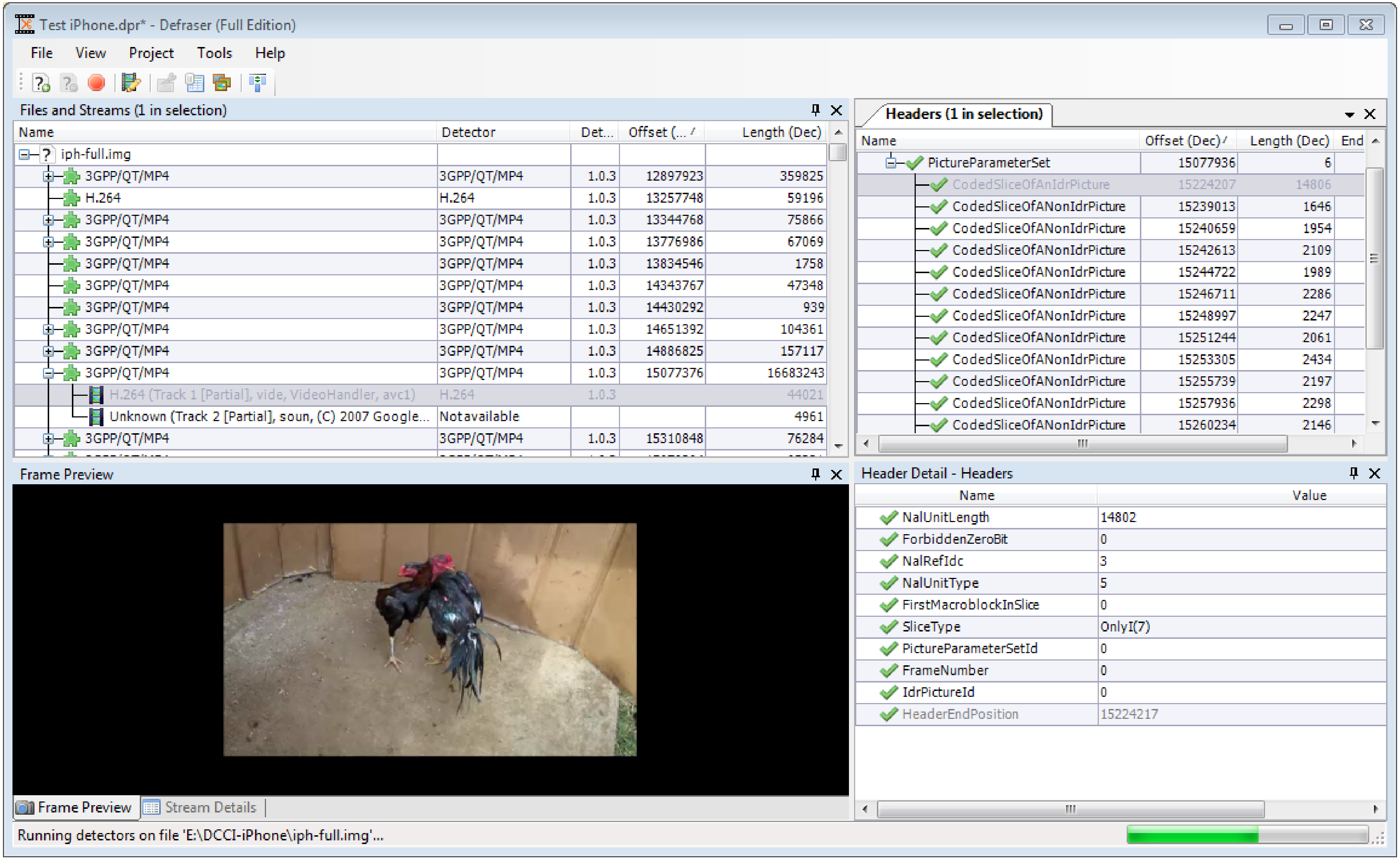
OPTIMAL COMBINATION OF HUMAN-AUTOMATED?

NFI Defraser

Digital **E**vidence **F**ragment **S**earch & **R**escue

- MPEG-1 & -2 Systems
- AVI
- 3GP / QT / MP4
- ASF / WMV
- Decoding of encoded video formats
  - MPEG-1, -2 & -4 video and H.264 (developing)
- http://defraser.sourceforge.net/

Carved 3GP Fragments (iPhone)



Test iPhone.dpr* - Defraser (Full Edition)

Files and Streams (1 in selection)

Name	Detector	Det...	Offset (...	Length (Dec)
iph-full.img				
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	12897923	359825
H.264	H.264	1.0.3	13257748	59196
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	13344768	75866
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	13776986	67069
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	13834546	1758
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	14343767	47348
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	14430292	939
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	14651392	104361
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	14886825	157117
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	15077376	16683243
H.264 (Track 1 [Partial], vide, VideoHandler, avc1)	H.264	1.0.3		44021
Unknown (Track 2 [Partial], soun, (C) 2007 Google...	Notavailable			4961
3GPP/QT/MP4	3GPP/QT/MP4	1.0.3	15310848	76284

Headers (1 in selection)

Name	Offset (Dec)	Length (Dec)	End
PictureParameterSet	15077936	6	
CodedSliceOfAnIdrPicture	15224207	14806	
CodedSliceOfANonIdrPicture	15239013	1646	
CodedSliceOfANonIdrPicture	15240659	1954	
CodedSliceOfANonIdrPicture	15242613	2109	
CodedSliceOfANonIdrPicture	15244722	1989	
CodedSliceOfANonIdrPicture	15246711	2286	
CodedSliceOfANonIdrPicture	15248997	2247	
CodedSliceOfANonIdrPicture	15251244	2061	
CodedSliceOfANonIdrPicture	15253305	2434	
CodedSliceOfANonIdrPicture	15255739	2197	
CodedSliceOfANonIdrPicture	15257936	2298	
CodedSliceOfANonIdrPicture	15260234	2146	

Frame Preview

Header Detail - Headers

Name	Value
NalUnitLength	14802
ForbiddenZeroBit	0
NalRefIdc	3
NalUnitType	5
FirstMacroblockInSlice	0
SliceType	OnlyI(7)
PictureParameterSetId	0
FrameNumber	0
IdrPictureId	0
HeaderEndPosition	15224217

Running detectors on file 'E:\DCCI-iPhone\iph-full.img'...

DC3 Carver

- Also known as DCCI_StegCarver
  - 2 methods for carving MPEG videos (contig & frag)
  - 4 method for carving AVI videos (contig & frag)
  - 3 method for carving 3GP videos (contig & frag)
  - Repair of MPEG and AVI

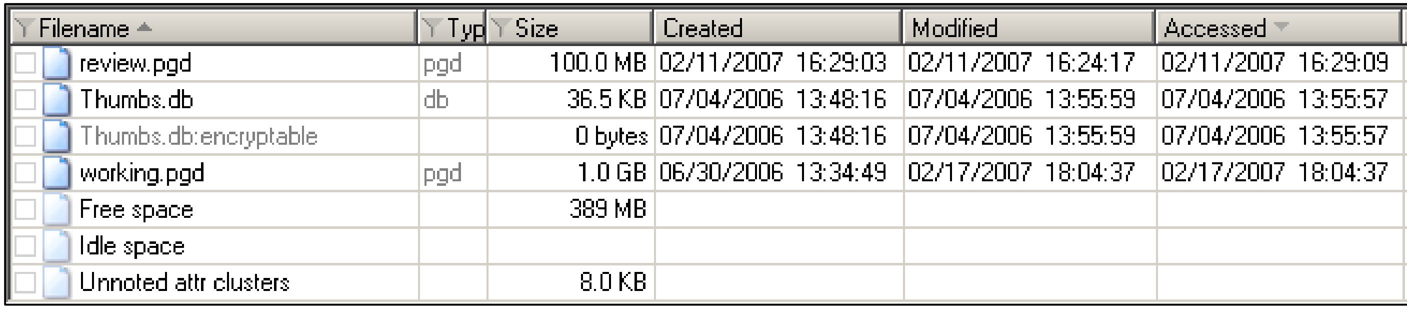
Reassembled MPEG Fragments

- DFRWS2007 Forensic Challenge

```
Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_296_44895744_44912127.MPG

Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_408_327213056_327270399.MPG

Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_295_44841984_44891135.MPG

Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_410_327419392_327812607.MPG

Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_362_245580288_245826047.MPG

Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_364_246311424_246657535.MPG

Combined Carved_MPEG_Fragment_dfrws-2007-challenge.img_301_61577728_61790719.MPG And Carved_MPEG_Fragment_dfrws-2007-challenge.img_363_245949440_246310911.MPG



Inserted 12 byte pack header copied from byte location 6144 into E:\dfrws2007\log_4_21_2011_10_23_41_AM\Logical MPEGs\Carved_8_61577728_Logical.mpg
```

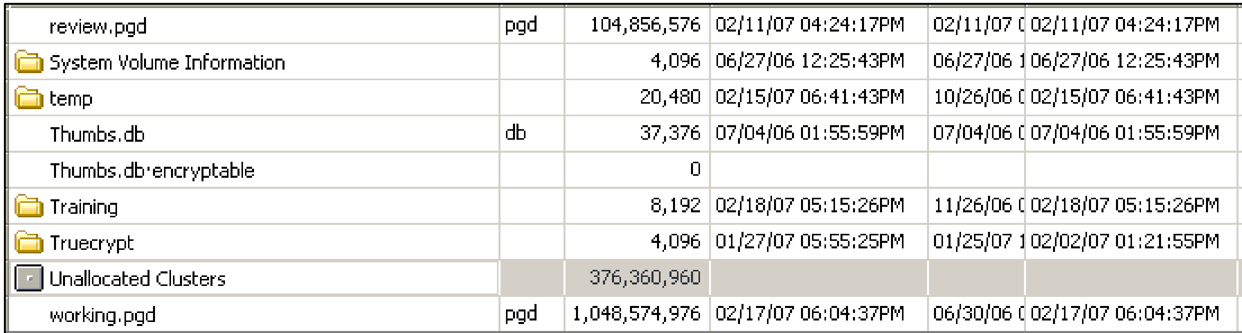
File System Considerations

- Most forensic tools
  - Unallocated = 408,068,096 bytes (389 MB)



Filename	Typ	Size	Created	Modified	Accessed
□ review.pgd	pgd	100.0 MB	02/11/2007 16:29:03	02/11/2007 16:24:17	02/11/2007 16:29:09
□ Thumbs.db	db	36.5 KB	07/04/2006 13:48:16	07/04/2006 13:55:59	07/04/2006 13:55:57
□ Thumbs.db:encryptable		0 bytes	07/04/2006 13:48:16	07/04/2006 13:55:59	07/04/2006 13:55:57
□ working.pgd	pgd	1.0 GB	06/30/2006 13:34:49	02/17/2007 18:04:37	02/17/2007 18:04:37
□ Free space		389 MB			
□ Idle space					
□ Unnoted attr clusters		8.0 KB			

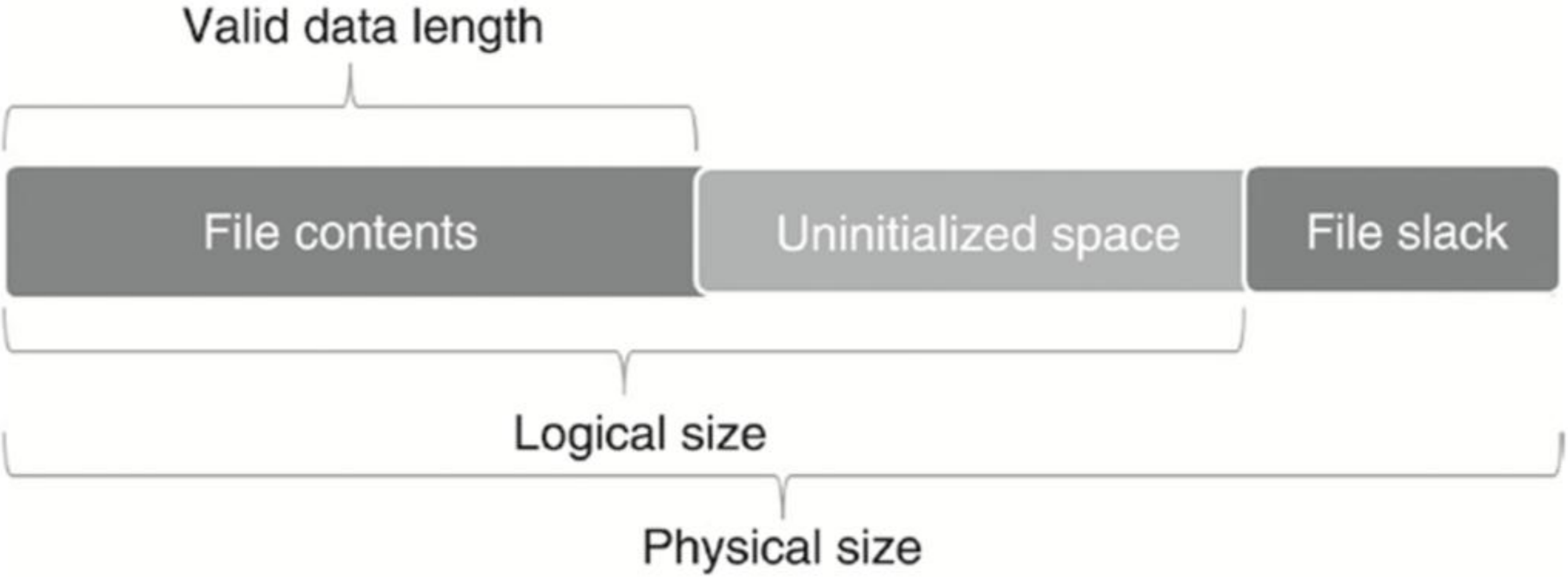
- EnCase
  - Unallocated = 376,360,960 bytes (359 MB)
  - Subtracts size of recovered deleted files + ?



review.pgd	pgd	104,856,576	02/11/07 04:24:17PM	02/11/07 0	02/11/07 04:24:17PM
System Volume Information		4,096	06/27/06 12:25:43PM	06/27/06 1	06/27/06 12:25:43PM
temp		20,480	02/15/07 06:41:43PM	10/26/06 0	02/15/07 06:41:43PM
Thumbs.db	db	37,376	07/04/06 01:55:59PM	07/04/06 0	07/04/06 01:55:59PM
Thumbs.db·encryptable		0			
Training		8,192	02/18/07 05:15:26PM	11/26/06 0	02/18/07 05:15:26PM
Truecrypt		4,096	01/27/07 05:55:25PM	01/25/07 1	02/02/07 01:21:55PM
Unallocated Clusters		376,360,960			
working.pgd	pgd	1,048,574,976	02/17/07 06:04:37PM	06/30/06 0	02/17/07 06:04:37PM

File System Considerations

- NTFS VDL Slack



Finding AVI Video Fragments

Description	Hex values	Byte range
File header “RIFF” - Total size of AVI - “AVI ”	\x52\x49\x46\x46 - 4 bytes (little endian) - \x41\x56\x49\x20	[0:3] - [4:7] - [8:b]
Header list “LIST” - Size of header list - “hdrl”	\x4C\x49\x53\x54 - 4 bytes (little endian) - \x68\x64\x72\x6C	[0:3] - [4:7] - [8:b]
AVI header “avih” - Size of avi header - Various flags - # of video frames	\x61\x76\x69\x68 - 4 bytes (little endian)	[0:3] - [4:7] - - [18:1b]
LIST structures - Size of list - List type (movi, odml or stream)	\x4C\x49\x53\x54 - 4 bytes (little endian) - [movi, odml or stream]	[0:3] - [4:7] - [8:b]
Chunk four character code (“db,” “dc,” “wb” or “tx”) - Size of chunk - Data	[Hex of db, dc, wb or tx] - 4 bytes (little endian) - [binary data]	[0:3] - [4:7] - [8:size]
Index “idx1” - Size of index - Index entries	\x69\x64\x71\x31 - 4 bytes (little endian)	[0:3] - [4:7] - [8:size]
Index entry four character code(“db”, “dc,” “wb” or “tx”) - Flags - Offset of chunk - Size of chunk	[Hex of db, dc, wb or tx] - [flags] - 4 bytes (little endian) - 4 bytes (little endian)	[0:3] - [4:7] - [8:b] - [c:f]

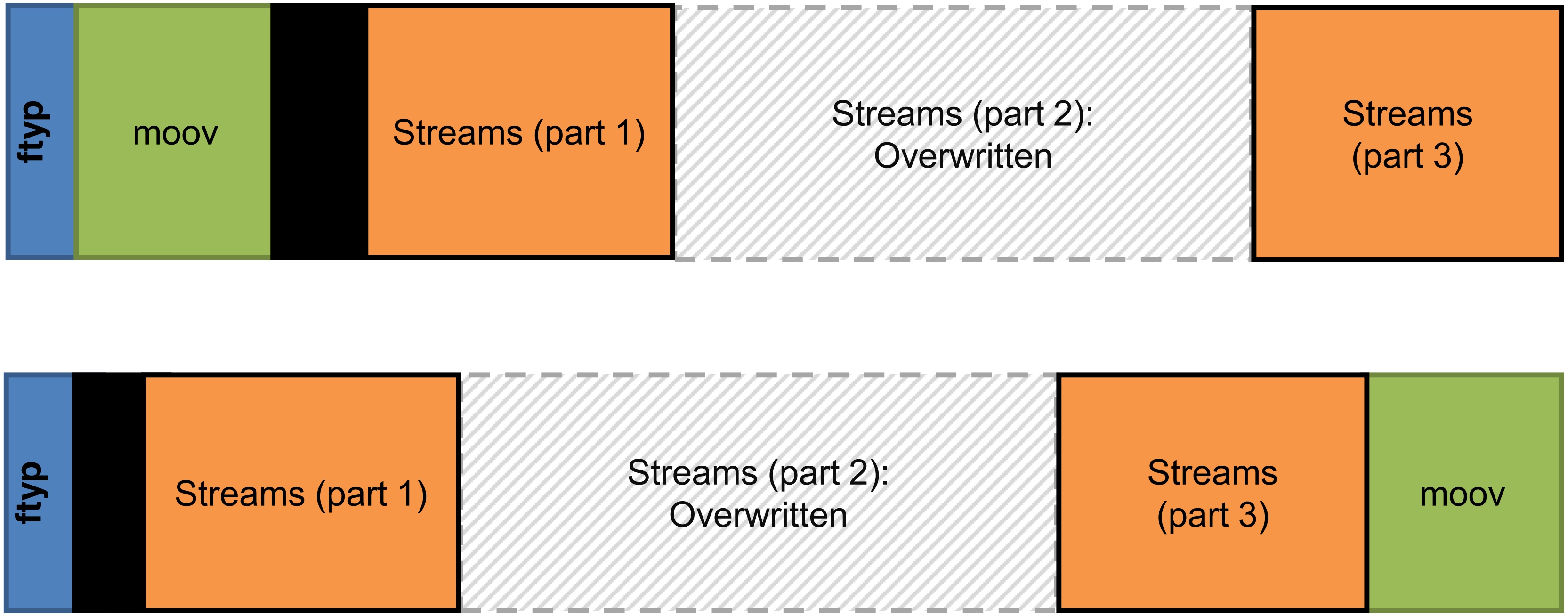
MPEG-2 fragments (DFRWS2007)

Offset	Size (bytes)	Type	Attribute
274370048	14	PackHeader	SystemClockReference=0
274370062	18	SystemHeader	
274370080	2016	PesPacket	PresentationTimeStamp=0, DecodingTimeStamp="8589930992"
274370103	12	SequenceHeader	
274370125	8	GroupOfPicturesHeader	TimeCode="00:00:00-00
…			
274372096	14	PackHeader	SystemClockReference=900
…			
274372110	2034	PesPacket	PresentationTimeStamp=0
274374144	14	PackHeader	SystemClockReference=1800
…			
274416688	12	SequenceHeader	
274416710	8	GroupOfPicturesHeader	TimeCode="00:00:00-10

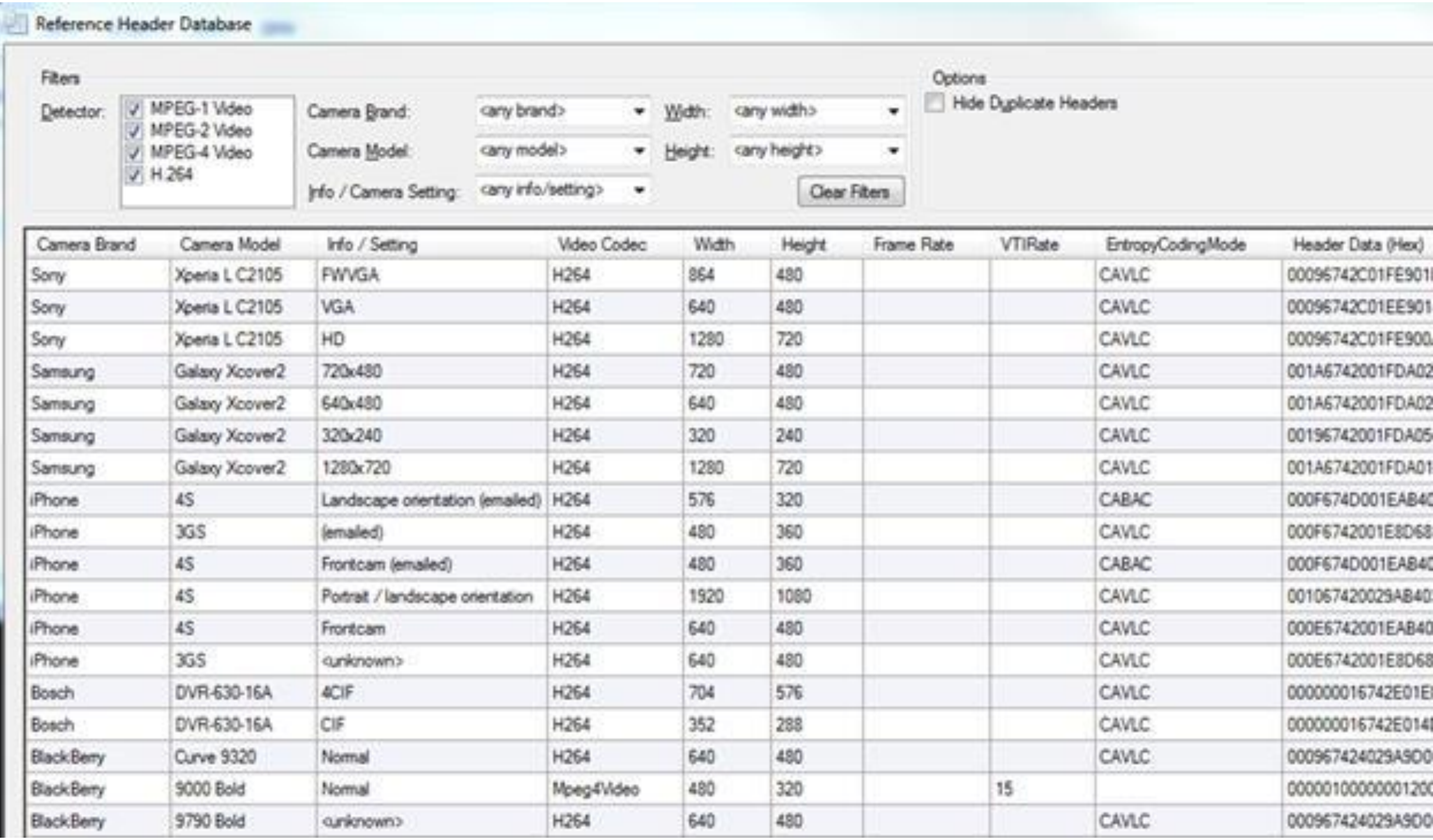
Finding MPEG-4 Video Fragments

Offset	Size (bytes)	Type	Attribute	Comment
228514304	20	ftyp	MajorBrand="isom"	CompatibleBrands="mp41"
228514324	2445504	mdat		
228514332	18457	Vop	TimeIncrement=0	CodingType="I_VOP"
228533351	3976	Vop	TimeIncrement=1	CodingType="P_VOP"
228537740	2248	Vop	TimeIncrement=2	CodingType="P_VOP"
228540402	5001	Vop	TimeIncrement=3	CodingType="P_VOP"
228545829	6195	Vop	TimeIncrement=4	CodingType="P_VOP"
228552470	4580	Vop	TimeIncrement=5	CodingType="P_VOP"
228557499	6300	Vop	TimeIncrement=6	CodingType="P_VOP"
228564245	5507	Vop	TimeIncrement=7	CodingType="P_VOP"
228570071	5339	Vop	TimeIncrement=8	CodingType="P_VOP"
228575902	5180	Vop	TimeIncrement=9	CodingType="P_VOP"
228581586	4525	Vop	TimeIncrement=10	CodingType="P_VOP"
228586643	5638	Vop	TimeIncrement=11	CodingType="P_VOP"
228592843	18946	Vop	TimeIncrement=12	CodingType="I_VOP"
228612368	4544	Vop	TimeIncrement=13	CodingType="P_VOP"
228617492	2789	Vop	TimeIncrement=14	CodingType="P_VOP"
…				
230959828	16635	moov		
230959944	4597	trak	TrackID=1	Video
230964541	11792	trak	TrackID=2	

Measure Once, Cut Twice



Repair Unassigned Fragments



Reference Header Database

Filters

Detector:
☑ MPEG-1 Video
☑ MPEG-2 Video
☑ MPEG-4 Video
☑ H.264

Camera Brand: <any brand>

Camera Model: <any model>

Info / Camera Setting: <any info/setting>

Width: <any width>

Height: <any height>

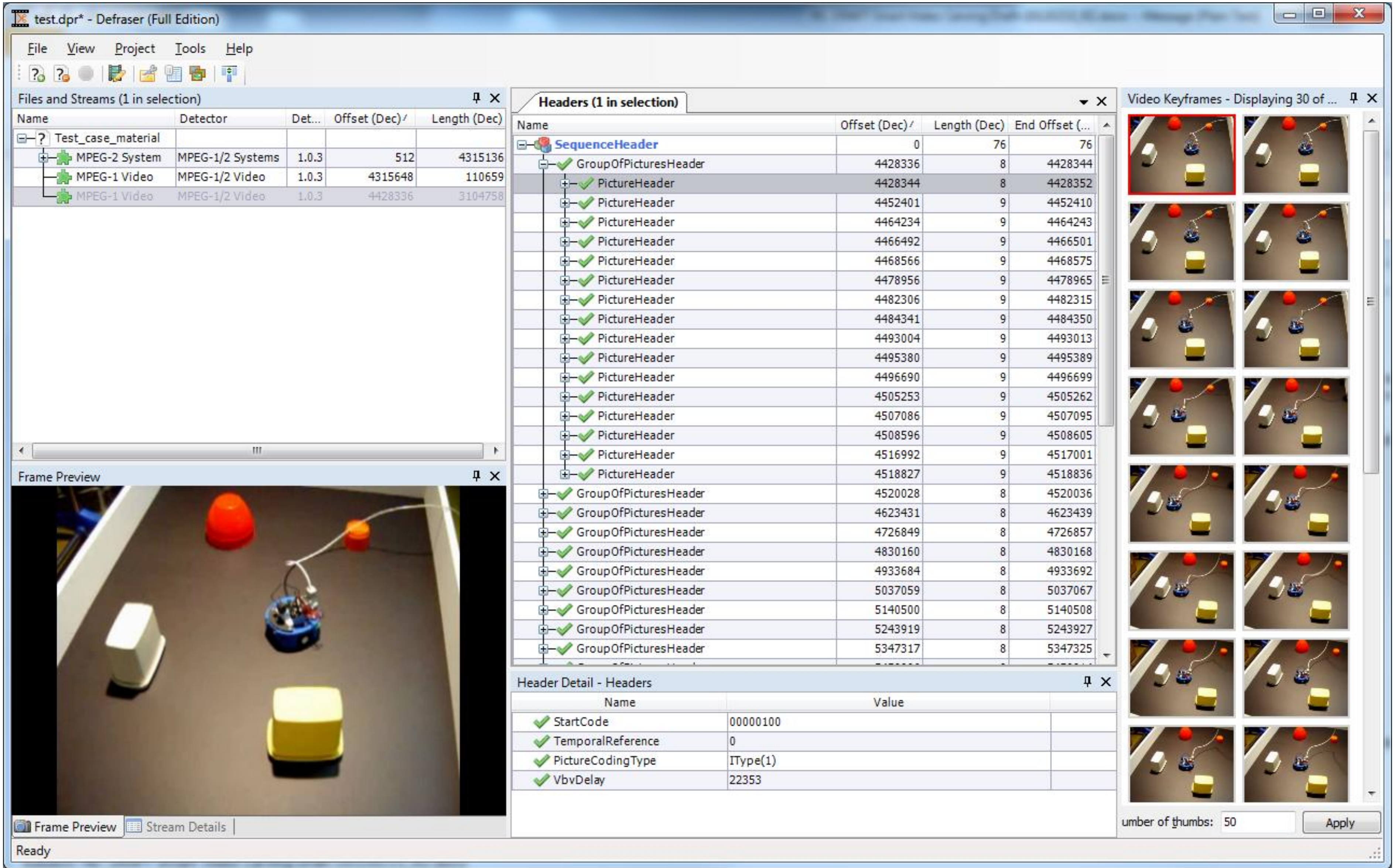
Clear Filters

Options

□ Hide Duplicate Headers

Camera Brand	Camera Model	Info / Setting	Video Codec	Width	Height	Frame Rate	VTIRate	EntropyCodingMode	Header Data (Hex)
Sony	Xperia L C2105	FWVGA	H264	864	480			CAVLC	00096742C01FE901
Sony	Xperia L C2105	VGA	H264	640	480			CAVLC	00096742C01EE901
Sony	Xperia L C2105	HD	H264	1280	720			CAVLC	00096742C01FE900
Samsung	Galaxy Xcover2	720x480	H264	720	480			CAVLC	001A6742001FDA02
Samsung	Galaxy Xcover2	640x480	H264	640	480			CAVLC	001A6742001FDA02
Samsung	Galaxy Xcover2	320x240	H264	320	240			CAVLC	00196742001FDA05
Samsung	Galaxy Xcover2	1280x720	H264	1280	720			CAVLC	001A6742001FDA01
iPhone	4S	Landscape orientation (emailed)	H264	576	320			CABAC	000F674D001EAB40
iPhone	3GS	(emailed)	H264	480	360			CAVLC	000F6742001E8D68
iPhone	4S	Frontcam (emailed)	H264	480	360			CABAC	000F674D001EAB40
iPhone	4S	Portrait / landscape orientation	H264	1920	1080			CAVLC	001067420029AB40
iPhone	4S	Frontcam	H264	640	480			CAVLC	000E6742001EAB40
iPhone	3GS	<unknown>	H264	640	480			CAVLC	000E6742001E8D68
Bosch	DVR-630-16A	4CIF	H264	704	576			CAVLC	00000016742E01E
Bosch	DVR-630-16A	CIF	H264	352	288			CAVLC	00000016742E014
BlackBerry	Curve 9320	Normal	H264	640	480			CAVLC	000967424029A9D0
BlackBerry	9000 Bold	Normal	Mpeg4Video	480	320		15		000001000000120
BlackBerry	9790 Bold	<unknown>	H264	640	480			CAVLC	000967424029A9D0

Repair Unassigned Fragments



Files and Streams (1 in selection)

Name	Detector	Det...	Offset (Dec)	Length (Dec)
Test_case_material				
MPEG-2 System	MPEG-1/2 Systems	1.0.3	512	4315136
MPEG-1 Video	MPEG-1/2 Video	1.0.3	4315648	110659
MPEG-1 Video	MPEG-1/2 Video	1.0.3	4428336	3104758

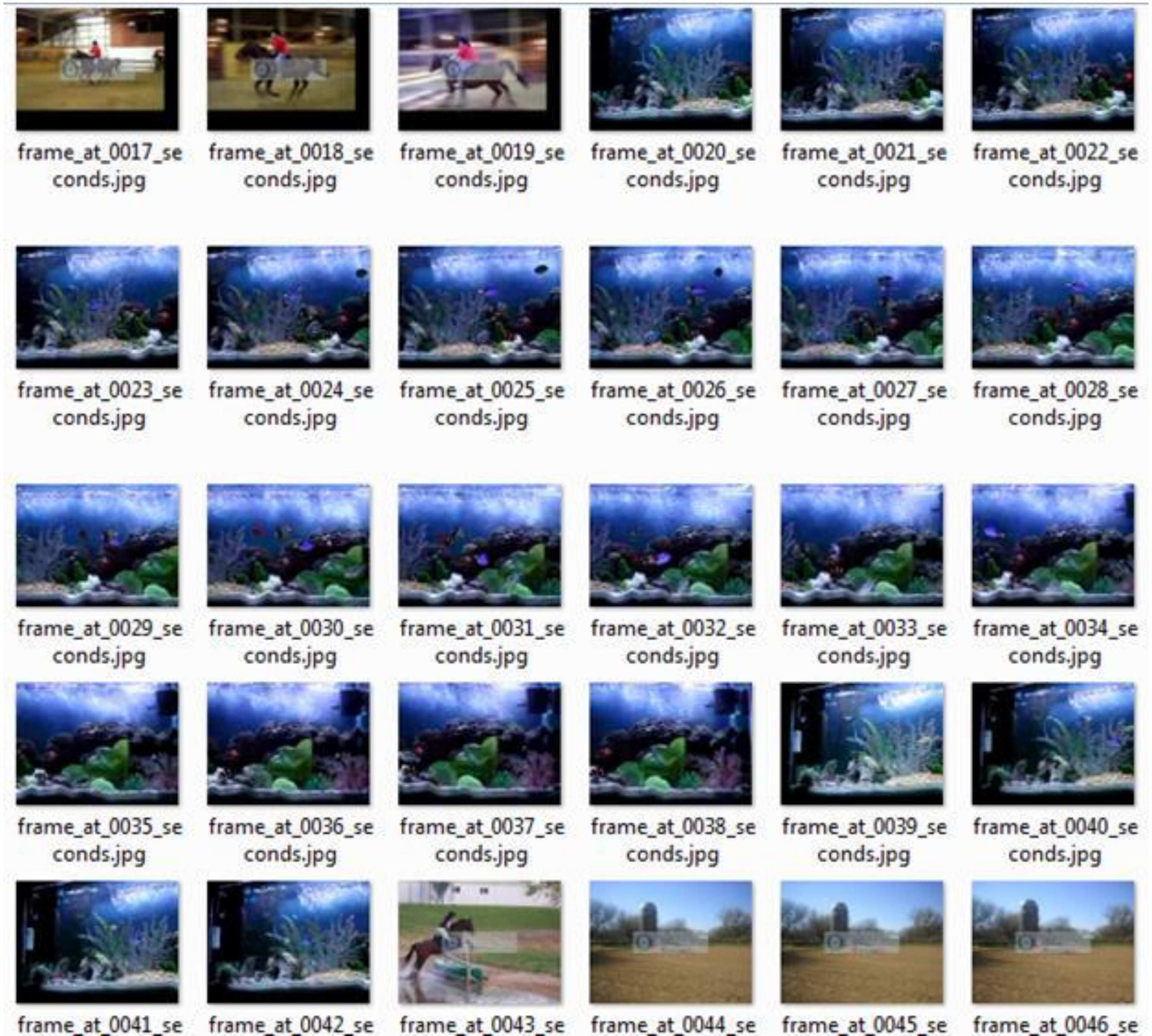
Headers (1 in selection)

Name	Offset (Dec)	Length (Dec)	End Offset (...
SequenceHeader	0	76	76
GroupOfPicturesHeader	4428336	8	4428344
PictureHeader	4428344	8	4428352
PictureHeader	4452401	9	4452410
PictureHeader	4464234	9	4464243
PictureHeader	4466492	9	4466501
PictureHeader	4468566	9	4468575
PictureHeader	4478956	9	4478965
PictureHeader	4482306	9	4482315
PictureHeader	4484341	9	4484350
PictureHeader	4493004	9	4493013
PictureHeader	4495380	9	4495389
PictureHeader	4496690	9	4496699
PictureHeader	4505253	9	4505262
PictureHeader	4507086	9	4507095
PictureHeader	4508596	9	4508605
PictureHeader	4516992	9	4517001
PictureHeader	4518827	9	4518836
GroupOfPicturesHeader	4520028	8	4520036
GroupOfPicturesHeader	4623431	8	4623439
GroupOfPicturesHeader	4726849	8	4726857
GroupOfPicturesHeader	4830160	8	4830168
GroupOfPicturesHeader	4933684	8	4933692
GroupOfPicturesHeader	5037059	8	5037067
GroupOfPicturesHeader	5140500	8	5140508
GroupOfPicturesHeader	5243919	8	5243927
GroupOfPicturesHeader	5347317	8	5347325

Header Detail - Headers

Name	Value
StartCode	00000100
TemporalReference	0
PictureCodingType	IType(1)
VbvDelay	22353

Determine Whether Playable



frame_at_0017_seconds.jpg
frame_at_0018_seconds.jpg
frame_at_0019_seconds.jpg
frame_at_0020_seconds.jpg
frame_at_0021_seconds.jpg
frame_at_0022_seconds.jpg

frame_at_0023_seconds.jpg
frame_at_0024_seconds.jpg
frame_at_0025_seconds.jpg
frame_at_0026_seconds.jpg
frame_at_0027_seconds.jpg
frame_at_0028_seconds.jpg

frame_at_0029_seconds.jpg
frame_at_0030_seconds.jpg
frame_at_0031_seconds.jpg
frame_at_0032_seconds.jpg
frame_at_0033_seconds.jpg
frame_at_0034_seconds.jpg

frame_at_0035_seconds.jpg
frame_at_0036_seconds.jpg
frame_at_0037_seconds.jpg
frame_at_0038_seconds.jpg
frame_at_0039_seconds.jpg
frame_at_0040_seconds.jpg

frame_at_0041_se
frame_at_0042_se
frame_at_0043_se
frame_at_0044_se
frame_at_0045_se
frame_at_0046_se