Forensic Analysis of Video File Formats

By

Thomas Gloe, Andre Fischer and Matthias Kirchner

Presented At

The Digital Forensic Research Conference

DFRWS 2014 EU Amsterdam, NL (May 7th - 9th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

dence
digital evidence

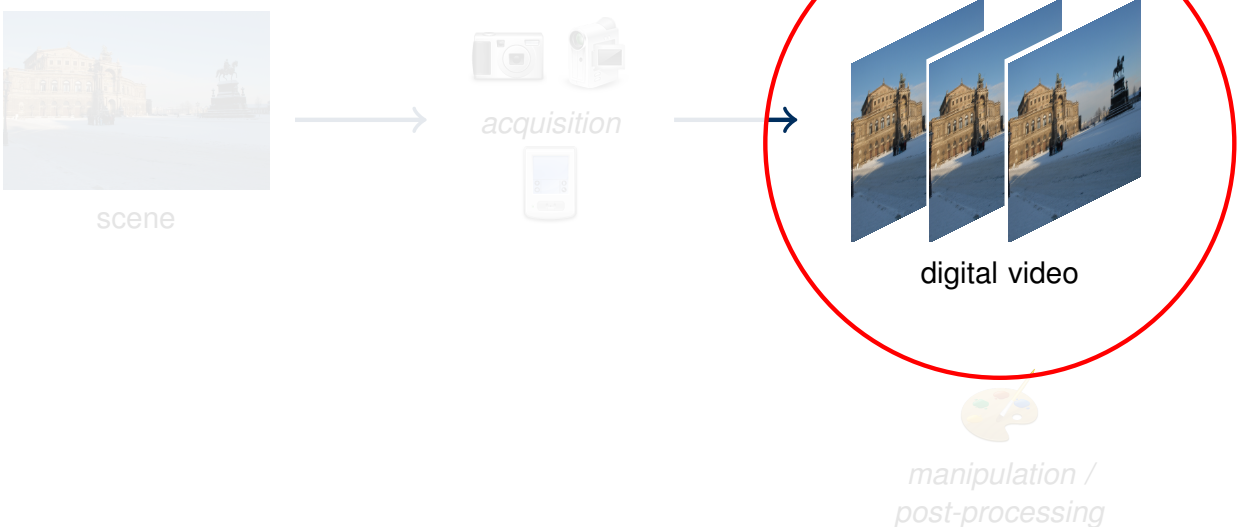
Forensic Analysis of Video File Formats

Thomas Gloe ■ André Fischer ■ Matthias Kirchner

Digital Forensics Research Workshop Europe

07.05. – 09.05.2014 ■ Amsterdam

Investigation of Digital Video



Typical questions

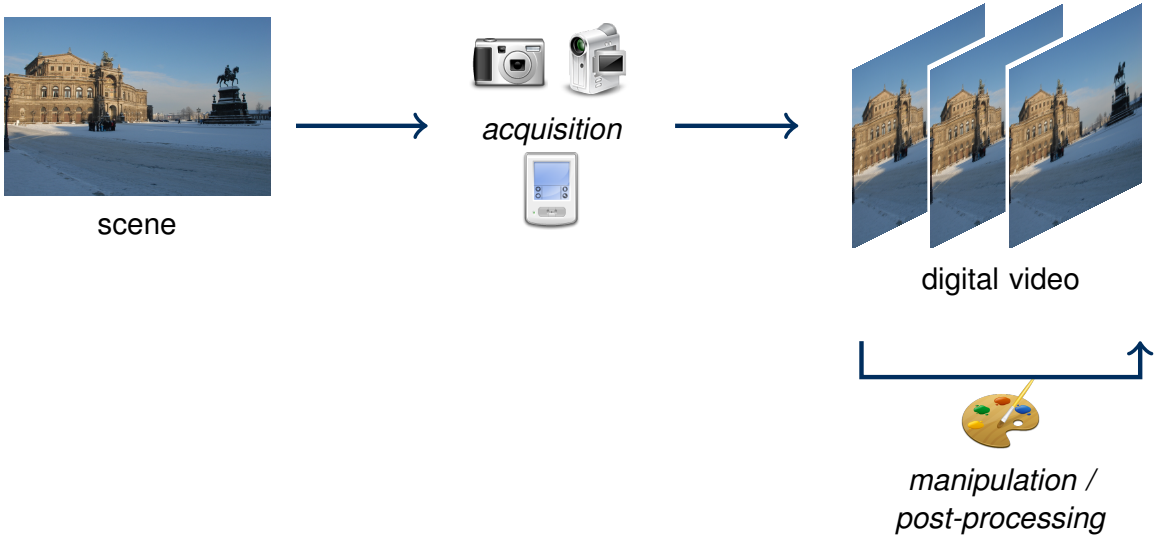
- semantic interpretation
- source / author
- video original or altered?

Investigation of Digital Video

Typical questions

- semantic interpretation
- **source** / **author**
- video original or altered?

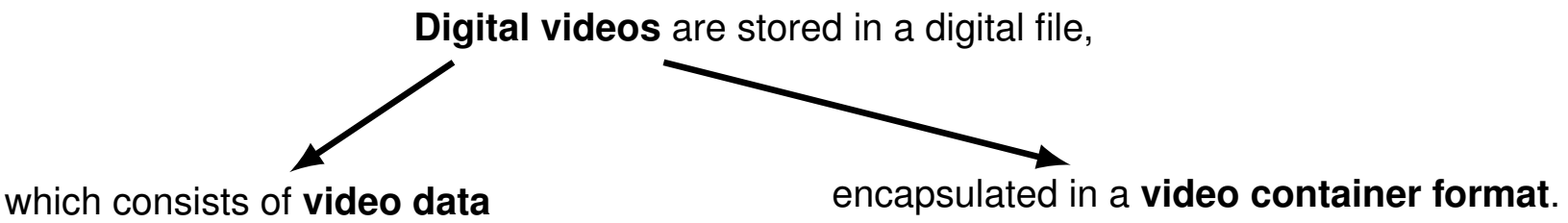
Investigation of Digital Video



Typical questions

- semantic interpretation
- **source / author**
- **video original or altered?**

Forensic Analysis of Digital Videos



Forensic Analysis of Digital Videos

Digital videos are stored in a digital file,

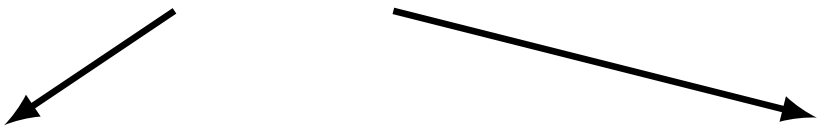
which consists of **video data**

- Sequence of image and audio information
- Statistical analysis to detect traces of manipulations / post processing and to determine the employed source device
  - ▷ e.g., (re-)compression artefacts, noise

encapsulated in a **video container format**.

Forensic Analysis of Digital Videos

Digital videos are stored in a digital file,



which consists of **video data**

- Sequence of image and audio information
- Statistical analysis to detect traces of manipulations / post processing and to determine the employed source device
  - ▷ e.g., (re-)compression artefacts, noise

encapsulated in a **video container format**.

- Auxiliary information (image/audio parameters, metadata, . . .)

Forensic Analysis of Digital Videos

Digital videos are stored in a digital file,

which consists of **video data**

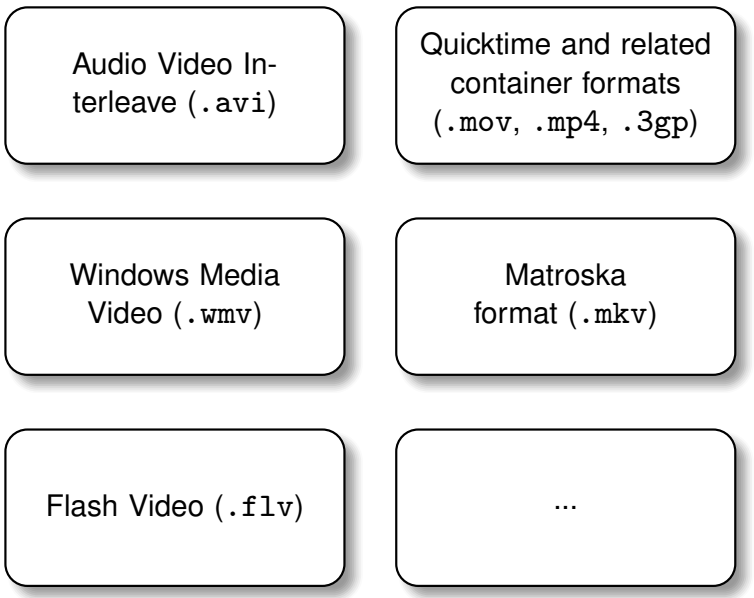
- Sequence of image and audio information
- Statistical analysis to detect traces of manipulations / post processing and to determine the employed source device
  - ▷ e.g., (re-)compression artefacts, noise

encapsulated in a **video container format**.

- Auxiliary information (image/audio parameters, metadata, . . .)

?

Overview Video Container Formats



- Test setup: 19 different digital camera models, 14 mobile phone models (all quality settings)

Overview Video Container Formats

Audio Video Interleave (`.avi`)	Quicktime and related container formats (`.mov`, `.mp4`, `.3gp`)	Motion JPEG (MJPG)	PCM
Windows Media Video (`.wmv`)	Matroska format (`.mkv`)	MP4V, H.263, H.264	MP2, MP4A
Flash Video (`.flv`)	...	DivX, Xvid	Adaptive Multi-rate Codec (AMR)

- Test setup: 19 different digital camera models, 14 mobile phone models (all quality settings)
- Digital cameras / mobile phones typically use AVI or Quicktime-based container formats and selected compression codecs

Overview Video Container Formats

Audio Video Interleave (`.avi`)	Quicktime and related container formats (`.mov`, `.mp4`, `.3gp`)	Motion JPEG (MJPG)	PCM
Windows Media Video (`.wmv`)	Matroska format (`.mkv`)	MP4V, H.263, H.264	MP2, MP4A
Flash Video (`.flv`)	...	DivX, Xvid	Adaptive Multi-rate Codec (AMR)

- Test setup: 19 different digital camera models, 14 mobile phone models (all quality settings)
- Digital cameras / mobile phones typically use AVI or Quicktime-based container formats and selected compression codecs

- Video editing software support different container formats and codecs

Overview Video Container Formats

Audio Video Interleave (`.avi`)	Quicktime and related container formats (`.mov`, `.mp4`, `.3gp`)	Motion JPEG (MJPG)	PCM
Windows Media Video (`.wmv`)	Matroska format (`.mkv`)	MP4V, H.263, H.264	MP2, MP4A
Flash Video (`.flv`)	...	DivX, Xvid	Adaptive Multi-rate Codec (AMR)

- Test setup: 19 different digital camera models, 14 mobile phone models (all quality settings)
- Digital cameras / mobile phones typically use AVI or Quicktime-based container formats and selected compression codecs

- Video editing software support different container formats and codecs
- Different video and audio compression codecs are used

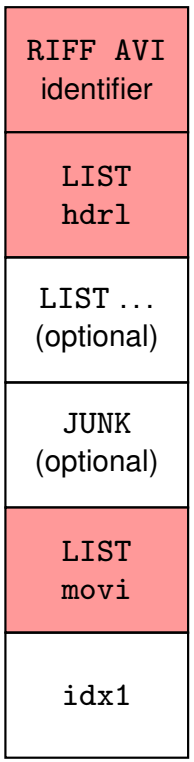
Overview Video Container Formats

Audio Video Interleave (`.avi`)	Quicktime and related container formats (`.mov`, `.mp4`, `.3gp`)	Motion JPEG (MJPG)	PCM
Windows Media Video (`.wmv`)	Matroska format (`.mkv`)	MP4V, H.263, H.264	MP2, MP4A
Flash Video (`.flv`)	...	DivX, Xvid	Adaptive Multi-rate Codec (AMR)

- Test setup: 19 different digital camera models, 14 mobile phone models (all quality settings)
- Digital cameras / mobile phones typically use AVI or Quicktime-based container formats and selected compression codecs

- Video editing software support different container formats and codecs
- Different video and audio compression codecs are used
- ▷ Focus on lossless video editing (FFMpeg, Virtual Dub, . . .)

Audio Video Interleave (AVI)



RIFF AVI header (file length, format identifier AVI)

video parameters necessary to decompress video

additional lists (e.g., storing metadata)

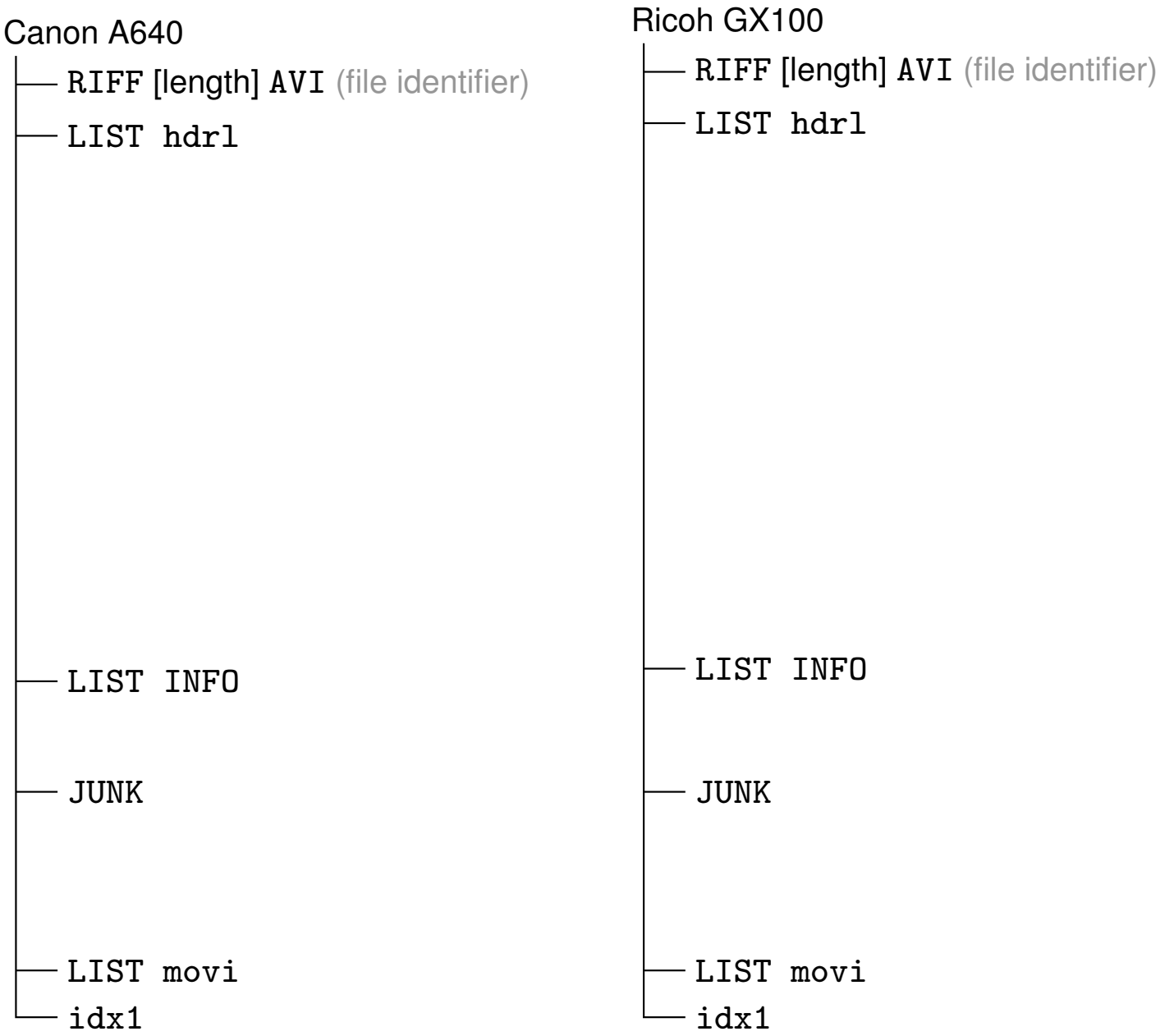
junk (e.g., padding bytes or manufacturer-specific metadata)

video and audio data

indexes to data chunk and their location in `LIST movi`

- Commonly used by digital cameras
- No strict specification defining sequence and occurrence of lists and chunks

AVI Example Structures – Original Videos



AVI Example Structures – Original Videos

Canon A640

- RIFF [length] AVI (file identifier)
- LIST hdrl
  - avih (main AVI header)
  - LIST strl (video stream)
    - strh (header)
    - strf (format)
  - LIST strl (audio stream)
    - strh (header)
    - strf (format)
  - IDIT: 'SAT APR 06 (date) 09:09:07 2013'
- LIST INFO
- JUNK
- LIST movi
- idx1

Ricoh GX100

- RIFF [length] AVI (file identifier)
- LIST hdrl
  - avih (main AVI header)
  - LIST strl (video stream)
    - strh (header)
    - strf (format)
  - LIST strl (audio stream)
    - strh (header)
    - strf (format)
  - IDIT: '2009:02:22 (date) 22:26:09'
- LIST INFO
- JUNK
- LIST movi
- idx1

AVI Example Structures – Original Videos

Canon A640

- RIFF [length] AVI (file identifier)
- LIST hdrl
  - avih (main AVI header)
  - LIST strl (video stream)
    - strh (header)
    - strf (format)
  - LIST strl (audio stream)
    - strh (header)
    - strf (format)
  - IDIT: 'SAT APR 06 (date) 09:09:07 2013'
- LIST INFO
  - ISFT: CanonMV102
- JUNK
- LIST movi
- idx1

Ricoh GX100

- RIFF [length] AVI (file identifier)
- LIST hdrl
  - avih (main AVI header)
  - LIST strl (video stream)
    - strh (header)
    - strf (format)
  - LIST strl (audio stream)
    - strh (header)
    - strf (format)
  - IDIT: '2009:02:22 (date) 22:26:09'
- LIST INFO
  - INAM: 0x20 20 20 20 20 20 20 20 20 00
  - ...
- JUNK
  - ucmt: ASCII
  - mnrt (Ricoh maker notes)
  - ...
- LIST movi
- idx1

AVI Example Structures – Video after Editing

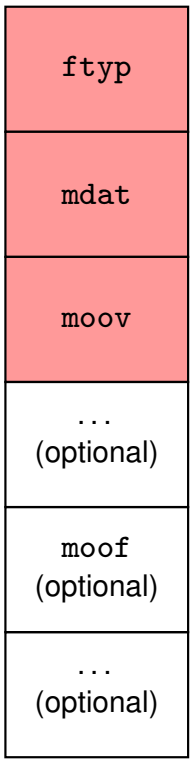
Canon A640

- RIFF [length] AVI (file identifier)
- LIST hdrl
  - avih (main AVI header)
  - LIST strl (video stream)
    - strh (header)
    - strf (format)
  - LIST strl (audio stream)
    - strh (header)
    - strf (format)
  - IDIT (date)
- LIST INFO
  - ISFT: CanonMV102
- JUNK
- LIST movi
- idx1

Virtual Dub

- RIFF [length] AVI (file identifier)
- LIST hdrl
  - avih (main AVI header)
  - LIST strl (video stream)
    - strh (header)
    - strf (format)
    - JUNK
  - LIST strl (audio stream)
    - strh (header)
    - strf (format)
    - JUNK
  - LIST odml (OpenDML AVI header)
- JUNK: VirtualDub build 32842/release
- LIST movi
- idx1
- LIST INFO
  - ISTF: CanonMV102

Quicktime-based Container Formats (MOV, MP4, 3GP)



file type atom (compatible file types)

movie data (video and audio data)

metadata (compression parameters, . . .)

movie fragments (shorter data chunks of movie data)

- Common in mobile phones and recent digital cameras with HD-video mode
- Similar to AVI no strict specification defining sequence and occurrence of atoms (or boxes)
- Nesting of Atoms results in complex organization

Quicktime-based Example Structures

Google Nexus 7

- `ftyp` (file identifier)
- `mdat` (media data)
- `moov` (metadata)
  - `mvhd` (movie header)
  - `udta` (user data)
  - `trak` (individual track or stream)
    - `tkhd` (track header)
    - `mdia` (media information in track)
      - `mdhd` (media header)
      - `hdlr` (handler declaring media type)
      - `minf` (media information)
        - `vmhd` (video media header)
        - `dinf` (data information box)
        - `stbl` (sample table box, time/space map)
          - `stsd` (sample descriptions)
          - `stts` (decoding time to sample)
          - `stss` (sync sample table)
          - `stsz` (sample size)
          - `stsc` (sample to chunk)
          - `stco` (chunk offset)
  - `trak` ...

Quicktime-based Example Structures

Google Nexus 7

- ftyp (file identifier)
- mdat (media data)
- moov (metadata)
  - mvhd (movie header)
  - udta (user data)
  - trak (individual track or stream)
    - tkhd (track header)
    - mdia (media information in track)
      - mdhd (media header)
      - hdlr (handler declaring media type)
      - minf (media information)
        - vmhd (video media header)
        - dinf (data information box)
        - stbl (sample table box, time/space map)
          - stsd (sample descriptions)
          - stts (decoding time to sample)
          - stss (sync sample table)
          - stsz (sample size)
          - stsc (sample to chunk)
          - stco (chunk offset)
  - trak ...

Motorola Milestone

- ftyp
- mdat
- moov
  - mvhd
  - udta
  - trak
    - tkhd
    - mdia
      - mdhd
      - hdlr
      - minf
        - smhd
        - dinf
        - stbl
          - stsd
          - stts
          - stsc
          - stsz
          - stco
  - trak ...

Major and Compatible Brands in `ftyp` (Selection)

model / **container**: model	major brand	compatible brands
Apple IPhone 4	qt	qt
BlackBerry 8310, Palm Pre	3gp4	3gp5, 3gp4, isom
Canon 7D	qt	qt, CAEP
Google Nexus 7	3gp4	isom, 3gp4
Kodak M1063	—	—
LG KU990	3gp5	3gp5, 3gp4
Minolta DiMAGE Z1	—	—-
Motorola MileStone	3gp4	3gp4, mp41, 3gp6
3GP: Nokia 6710, E61i, E65	3gp4	3gp4, 3g2a, isom
MP4: Nokia 6710, E61i, E65	mp42	mp42, 3gp4, isom
Samsung GT-5500i (H.263)	3gp4	3gp4, 3gp6
FFmpeg	isom	isom, iso2, mp41
YAMB	mp42	isom, mp42, 3gp5
Adobe Premiere CS 5	3gp5	isom, 3gp4, mp41, mp42

Additional Atoms (Selection)

model	atoms
Apple iPhone 4	`wide`, `free`, `meta`
Benq S88	`mvex`, `mdat` file end, `moof`
BlackBerry 8310	
Canon 7D	`udta`
Google Nexus 7	`udta`
Kodak M1063	`skip`, `edts`
LG KU990	
Minolta Z1	`pnot`, `PICT`
Motorola MileStone	`udta`
Palm Pre	`udta`
Samsung GT-5500i	`udta`
FFmpeg	`free`, `edts`, `udta`
YAMB	`iods`, `tref`, `nmhd`, `free`, `mdat` file end
Adobe Premiere CS5	`iods`, `udta`, `uuid`, `mdat` file end

MJPEG Compression

- MJPEG compressed-video consists of a sequence of JPEG full frames
- Each JPEG full frame uses a normal JPEG container (JIF or JFIF)

marker id	short value	JIF	JFIF	EXIF	description
SOI	0xFF D8	×	×	×	start of image
APPn	0xFF E*n*				application data
APP0	0xFF E0		×		(e.g., JFIF application data)
APP1	0xFF E1			×	(e.g., EXIF application data)
DQT	0xFF DB	×	×	×	define quantisation tables
DHT	0xFF C4	(×)	×	×	define Huffman tables
SOF	0xFF C*n*	×			start of frame
SOF	0xFF C0		×	×	(e.g., baseline DCT)
SOS	0xFF DA	×	×	×	start of scan
DRI	0xFF DD				define restart interval
RST*n*	0xFF D*n*				*n*th restart
COM	0xFF FE				comment
EOI	0xFF D9	×	×	×	end of image

Structure of JPEGs in MJPEG-Compressed Video

model	sequence of JPEG marker segments
Agfa DC-504, Sensor530s	SOI, DQT, SOF0, DHT, COM, SOS, EOI
Agfa DC-733s, DC-830i	SOI, APP0(AVI1), DQT, DHT, SOF0, SOS, EOI
Agfa Sensor505-X, Nikon CoolPix S3300	SOI, APP0(AVI1), DRI, DQT, DHT, SOF0, SOS, EOI
Canon PowerShot A640	SOI, APP0(AVI1), DRI, DQT, SOF0, SOS, EOI
Canon S45, S70, Ixus IIs	SOI, APP0(AVI1), DRI, DQT, SOF0, APP2, SOS, EOI
Casio EX-M2, Ricoh GX100	SOI, APP0(AVI1), DQT, SOF0, SOS, EOI
Kodak M1063	SOI, APP0(AVI1), DRI, APP0(JFIF), DQT, DQT, SOF0, DHT, DHT, DHT, DHT, SOS, EOI
Minolta DiMAGE Z1	SOI, DHT, DHT, DHT, DHT, DQT, DQT, SOF0, SOS, EOI
Pentax Optio W60	SOI, APP0(AVI1), DRI, DQT, SOF0, DHT, SOS, EOI
Praktica DC2070	SOI, APP1(0x0000 mjpg), DQT, DHT, SOF0, SOS, EOI
thumbnail: Nikon CoolPix S3300	SOI, DQT, DHT, SOF0, SOS, EOI
thumbnail: Pentax Optio W60, Ricoh GX100	SOI, DQT, SOF0, DHT, SOS, EOI

- Structure depends on the used camera
- Structure in MJPEG-compressed video is different to ‘normal’ JPEG photographs

dence
digital evidence

Structure of JPEGs in MJPEG-Compressed Video

model	sequence of JPEG marker segments
Agfa DC-504, Sensor530s	SOI, DQT, SOF0, DHT, COM, SOS, EOI
Agfa DC-733s, DC-830i	SOI, APP0(AVI1), DQT, DHT, SOF0, SOS, EOI
Agfa Sensor505-X, Nikon CoolPix S3300	SOI, APP0(AVI1), DRI, DQT, DHT, SOF0, SOS, EOI
Canon PowerShot A640	SOI, APP0(AVI1), DRI, DQT, SOF0, SOS, EOI
Canon S45, S70, Ixus IIs	SOI, APP0(AVI1), DRI, DQT, SOF0, APP2, SOS, EOI
Casio EX-M2, Ricoh GX100	SOI, APP0(AVI1), DQT, SOF0, SOS, EOI
Kodak M1063	SOI, APP0(AVI1), DRI, APP0(JFIF), DQT, DQT, SOF0, DHT, DHT, DHT, DHT, SOS, EOI
Minolta DiMAGE Z1	SOI, DHT, DHT, DHT, DHT, DQT, DQT, SOF0, SOS, EOI
Pentax Optio W60	SOI, APP0(AVI1), DRI, DQT, SOF0, DHT, SOS, EOI
Praktica DC2070	SOI, APP1(0x0000 mjpg), DQT, DHT, SOF0, SOS, EOI
thumbnail: Nikon CoolPix S3300	SOI, DQT, DHT, SOF0, SOS, EOI
thumbnail: Pentax Optio W60, Ricoh GX100	SOI, DQT, SOF0, DHT, SOS, EOI

- Structure depends on the used camera
- Structure in MJPEG-compressed video is different to ‘normal’ JPEG photographs
- MJPEG stores sometimes incomplete JPEG images to save disk memory

Summary

- Container format standards are not thrilling literature
- . . . and their complexity give room for different interpretations and implementations.
- **Occurrence and order of data structures** as well as all kinds of **parameters** depend on the camera / post-processing software.
- Software for lossless editing of videos preserving compression settings is available,
- ▷ . . . but software does not take the file structure into account.
- ▷ Similar analysis strategies are possible for other file formats (including JPEG, PDF, . . .).

dence
digital evidence

Forensic Analysis of Video File Formats

Questions or Comments?

Thomas Gloe ■ André Fischer ■ Matthias Kirchner

Contact: thomas.gloe@dence.de

Digital Forensics Research Workshop Europe

07.05. – 09.05.2014 ■ Amsterdam

dence
digital evidence

Quantisation Tables in MJPEG Videos

camera model	Y / CbCr
Agfa DC-504	1 / 1
Agfa DC-733s	589 / 390
Agfa DC-830i	489 / 314
Agfa Sensor505-X	893 / 286
Agfa Sensor530s	1 / 1
Canon Ixus IIs	5 / 5
Canon A640	6 / 6
Canon S45	6 / 6
Canon S70	8 / 8
Casio EX-M2	121 / 121
Kodak M1063	10 / 10
Minolta DiMAGE Z1	13 / 13
Nikon CoolPix S3300	465 / 111
Pentax Optio W60	73 / 73
Praktica DC2070	1 / 1
Ricoh GX100	924 / 338 (2×)
$\sum$ unique quantization tables	2914 / 1279