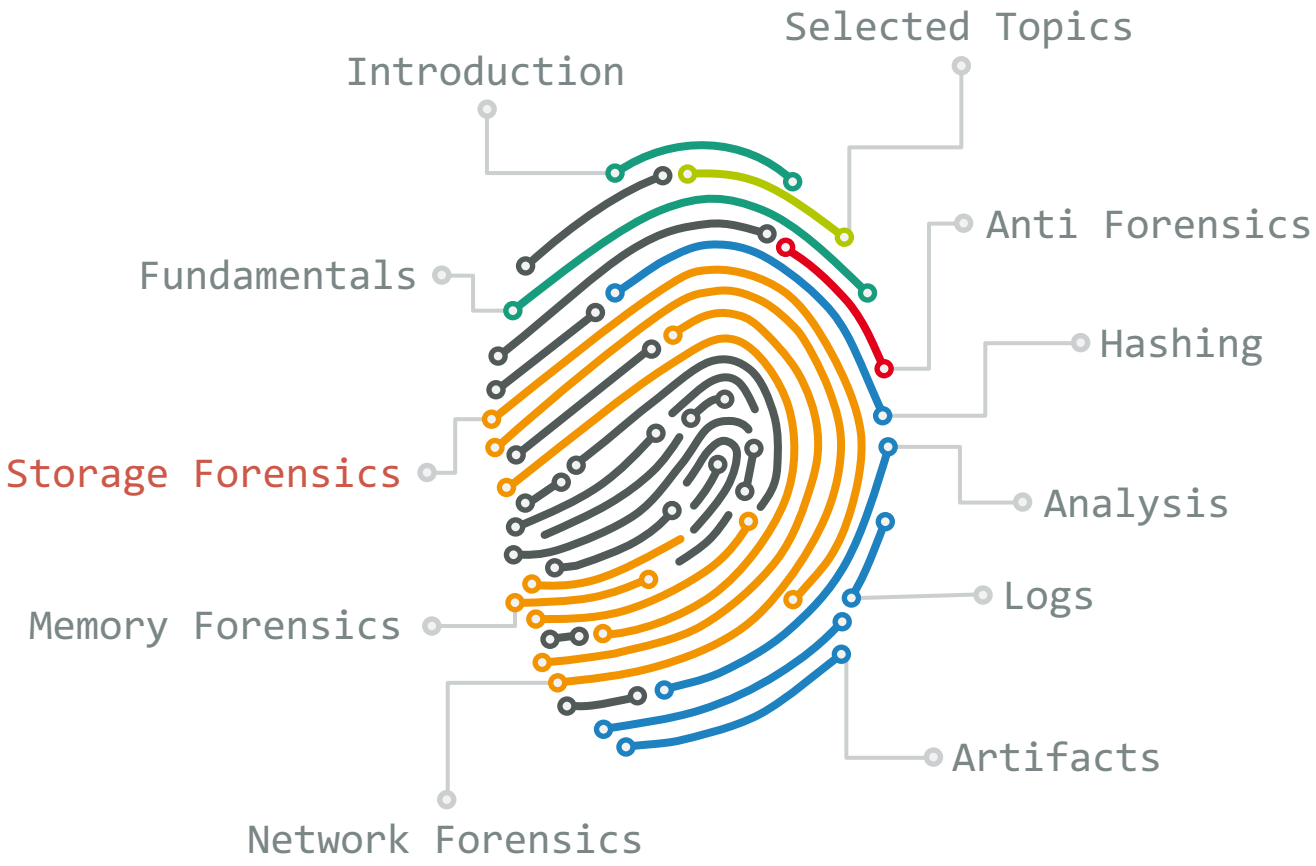
Fraunhofer FKIE

Prof. Dr. Elmar Padilla et al.

Digitale Forensik

02 - Storage Forensics



Application Artifacts

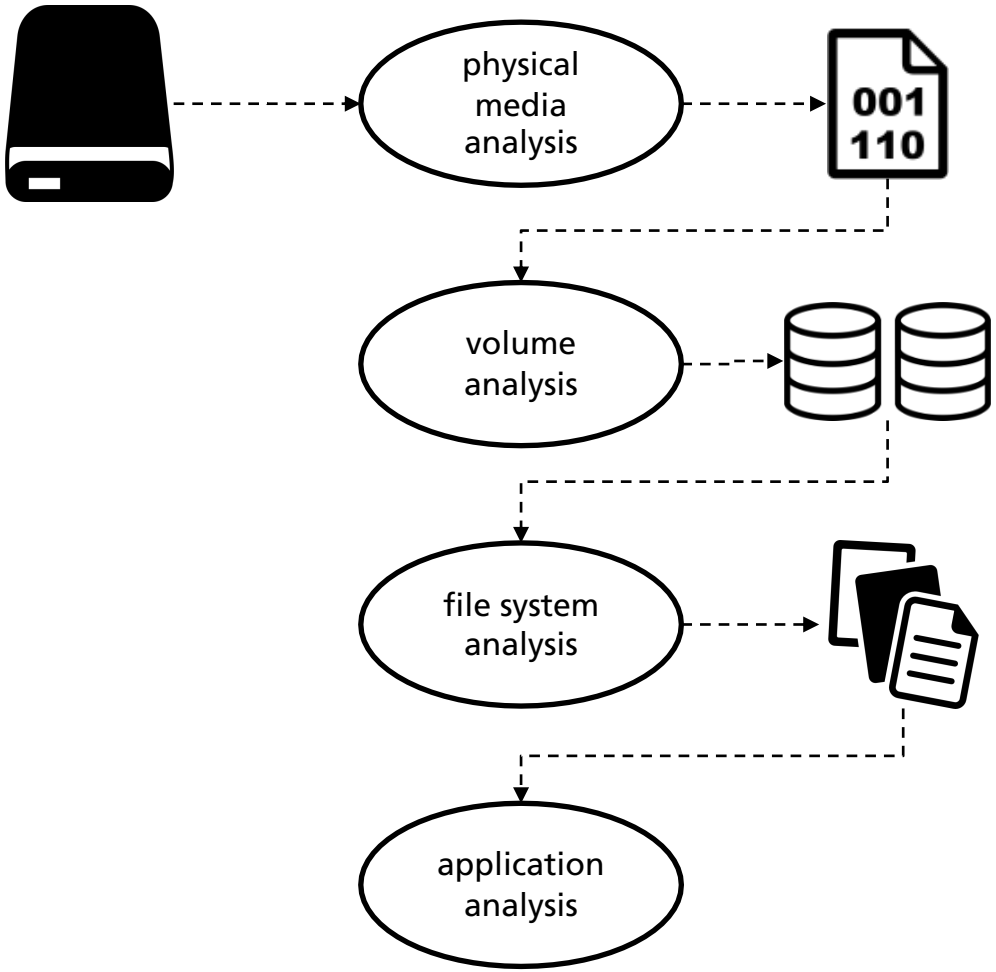
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

File System Forensic Analysis

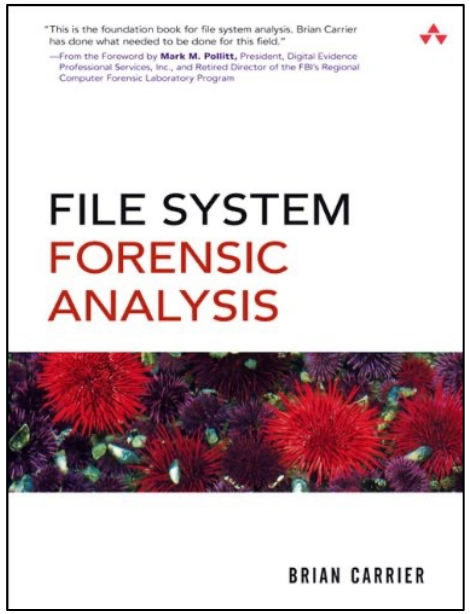
Dr. Brian Carrier

Basis Technology



Sleuth Kit

Autopsy



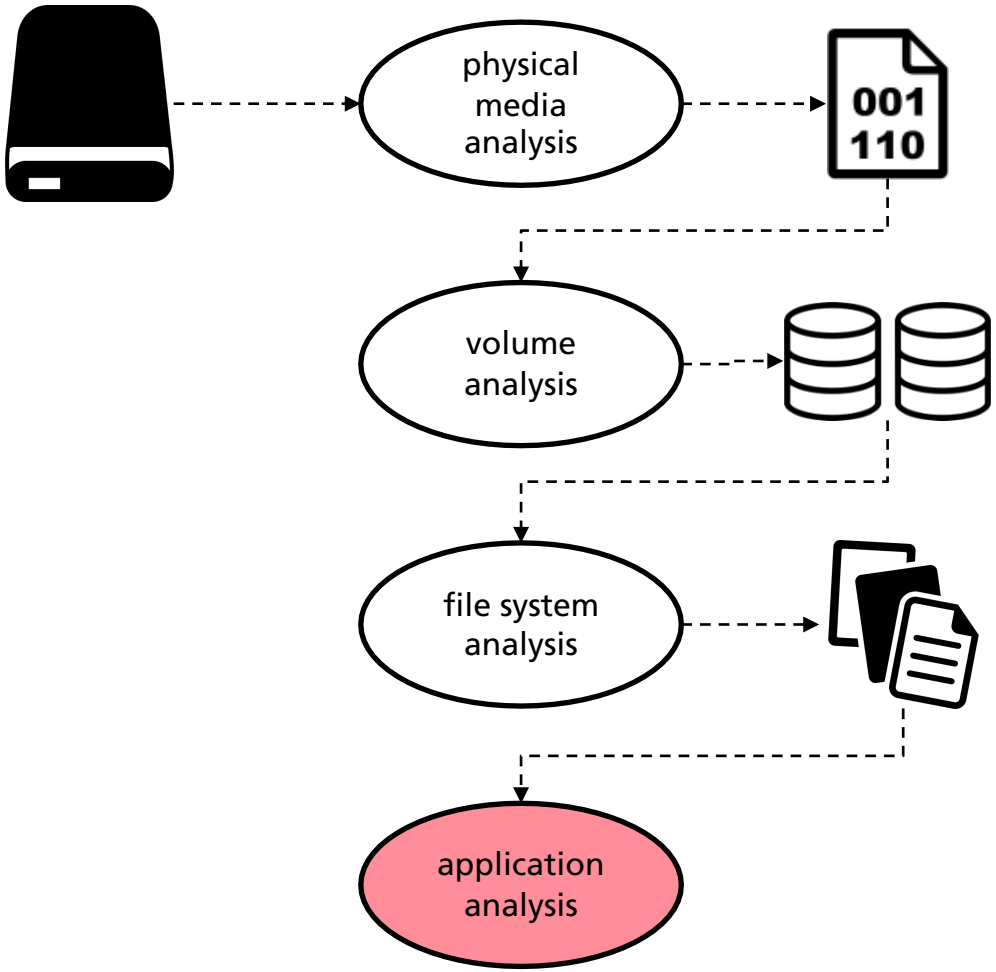
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

File System Forensic Analysis

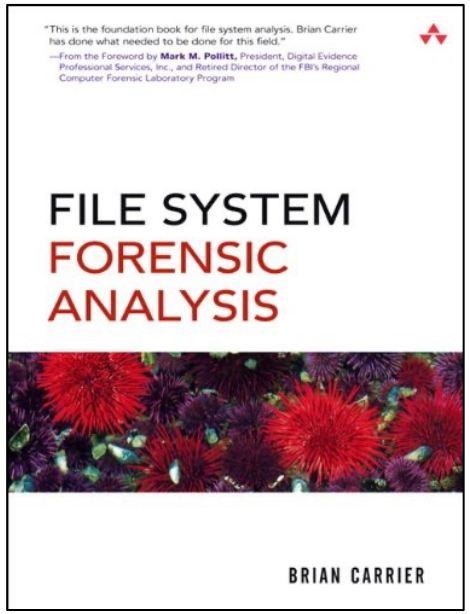
Dr. Brian Carrier

Basis Technology



Sleuth Kit

Autopsy



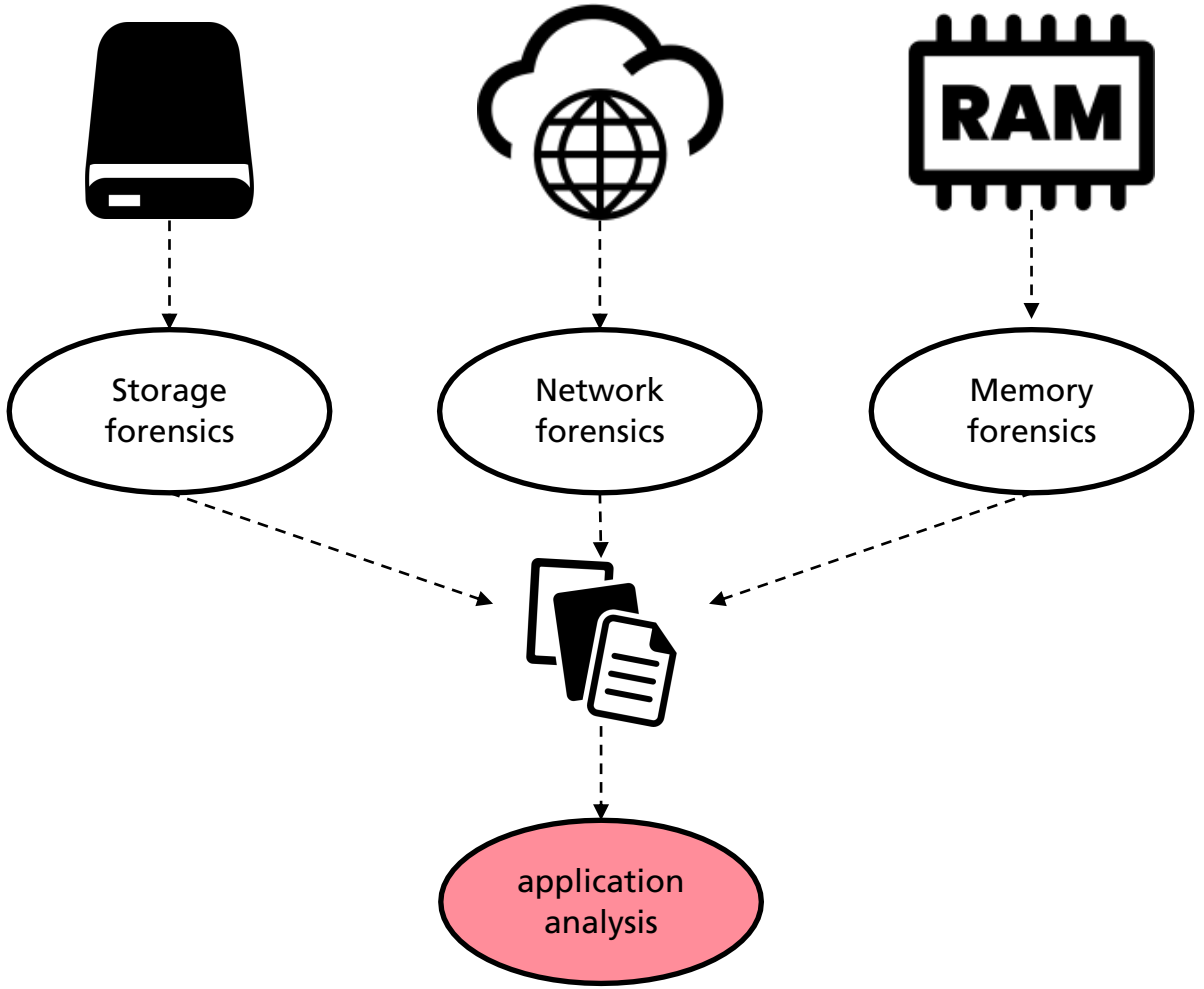
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

File System Forensic Analysis

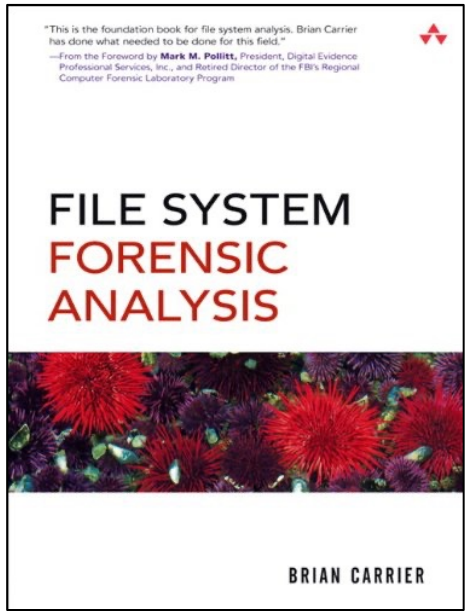
Dr. Brian Carrier

Basis Technology



Sleuth Kit

Autopsy



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

File System Forensic Analysis

Dr. Brian Carrier

Basis Technology

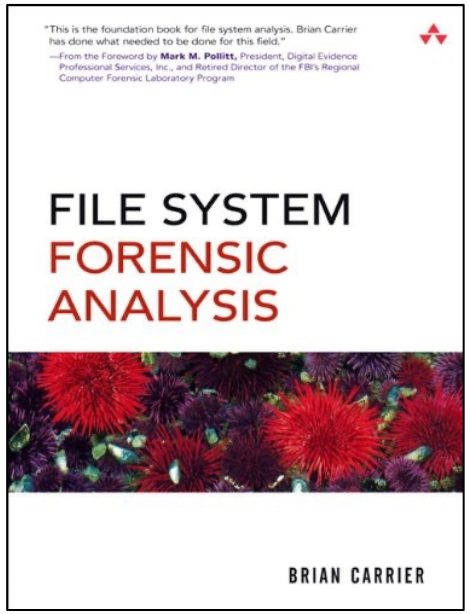
- Ingest Modules
  - Ingest Modules
  - Recent Activity Module
  - Hash Lookup Module
  - File Type Identification Module
  - Embedded File Extraction Module
  - Picture Analyzer Module
  - Keyword Search Module
  - Email Parser Module
  - Extension Mismatch Detector Module
  - Data Source Integrity Module
  - Android Analyzer Module
  - Interesting Files Identifier Module
  - PhotoRec Carver Module
  - Central Repository Module
  - Encryption Detection Module
  - Virtual Machine Extractor Module
  - Plaso
  - DJI Drone Analyzer
  - GPX Analyzer
  - iOS Analyzer (iLEAPP)
  - Android Analyzer (aLEAPP)
  - YARA Analyzer

http://sleuthkit.org/autopsy/docs/user-docs/4.19.2/

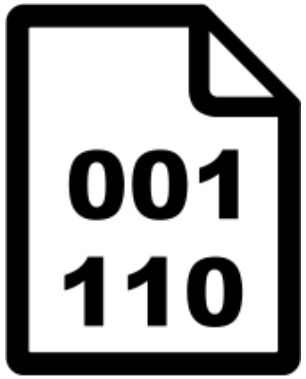
Autopsy's modules for example cover OS and application artifacts, but also provide some triage techniques.

Sleuth Kit

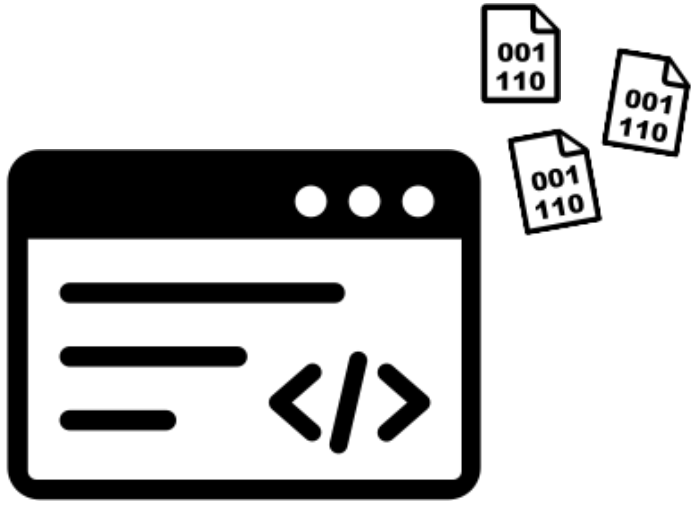
Autopsy



Application Artifacts



Filetypes



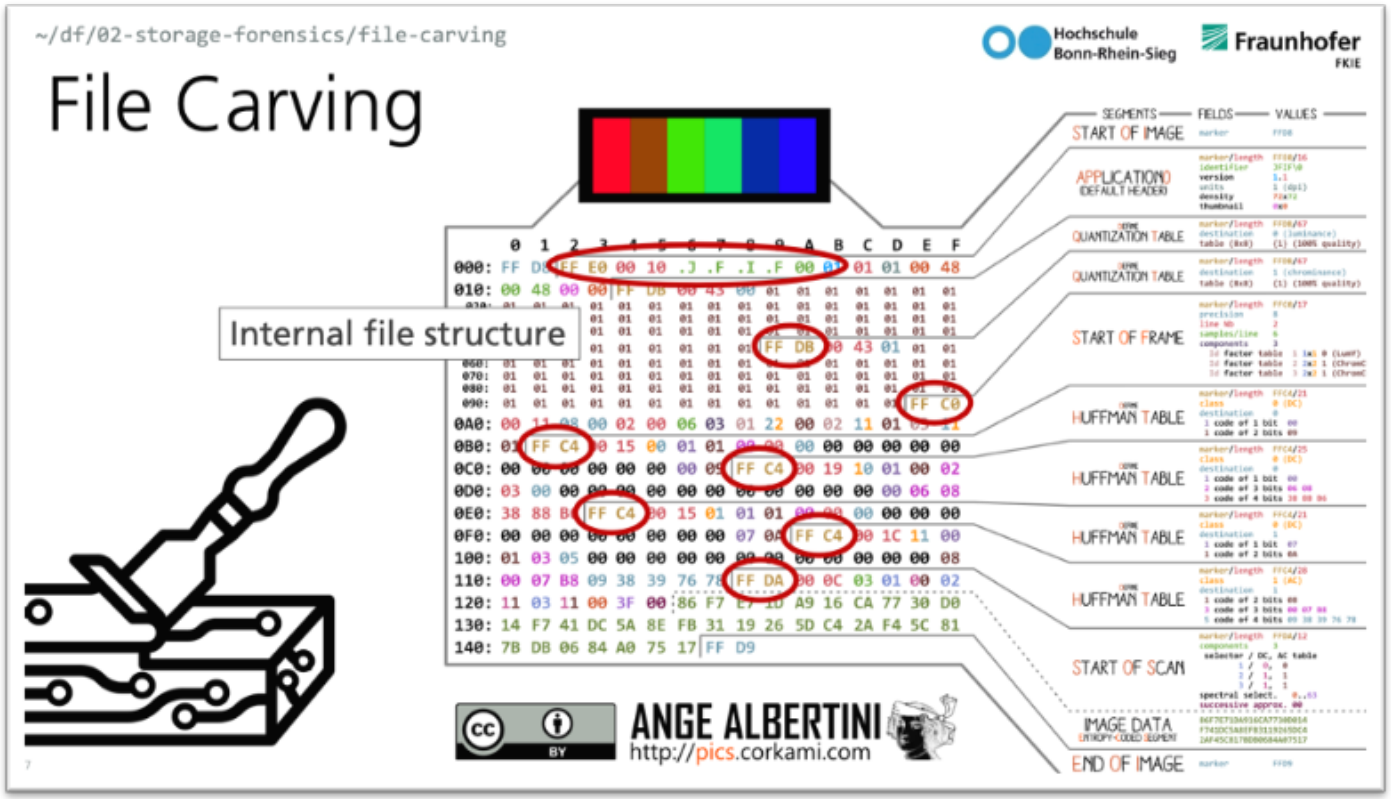
Artifacts in Applications

Filetypes

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes



File signatures are not only handy, when it comes to carving files!

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

4E 41 56 54 52 41 46 46		NAVTRAFF
49 43		IC
	DAT	TomTom traffic data file
4E 42 2A 00		NB*.
	JNT, JTP	MS Windows journal file
4E 45 53 4D 1A 01		NESM..
	NSF	NES Sound file
4E 49 54 46 30		NITF0
	NTF	National Imagery Transmission Format (NITF) file
4E 61 6D 65 3A 20		Name:
	COD	Agent newsreader character map file
4F 50 43 4C 44 41 54		OPCLDAT
	attachment	1Password 4 Cloud Keychain encrypted attachment
4F 50 4C 44 61 74 61 62		OPLDatab
61 73 65 46 69 6C 65		aseFile
	DBF	Psion Series 3 Database file
4F 54 54 4F 00		OTTO.
	OTF	OpenType font file
4F 67 67 53 00 02 00 00		OggS....
00 00 00 00 00 00		......
	OGA, OGG, OGV, OGX	Ogg Vorbis Codec compressed Multimedia file

https://www.garykessler.net/library/file_sigs.html

File signatures are not only handy, when it comes to carving files!

Filetypes

file

file(1) - Linux man page

Name

file - determine file type

Synopsis

file [-bchikLNnprsvz0] [--apple] [--mime-encoding] [--mime-type] [-e testname] [-F separator] [-f namefile] [-m magicfiles] file ...

file -C [-m magicfiles]

file [--help]

Description

file tests each argument in an attempt to classify it. There are three sets of tests, performed in this order: filesystem tests, magic tests, and language tests. The first test that succeeds causes the file type to be printed.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

```
~$ file file1
```

file1

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

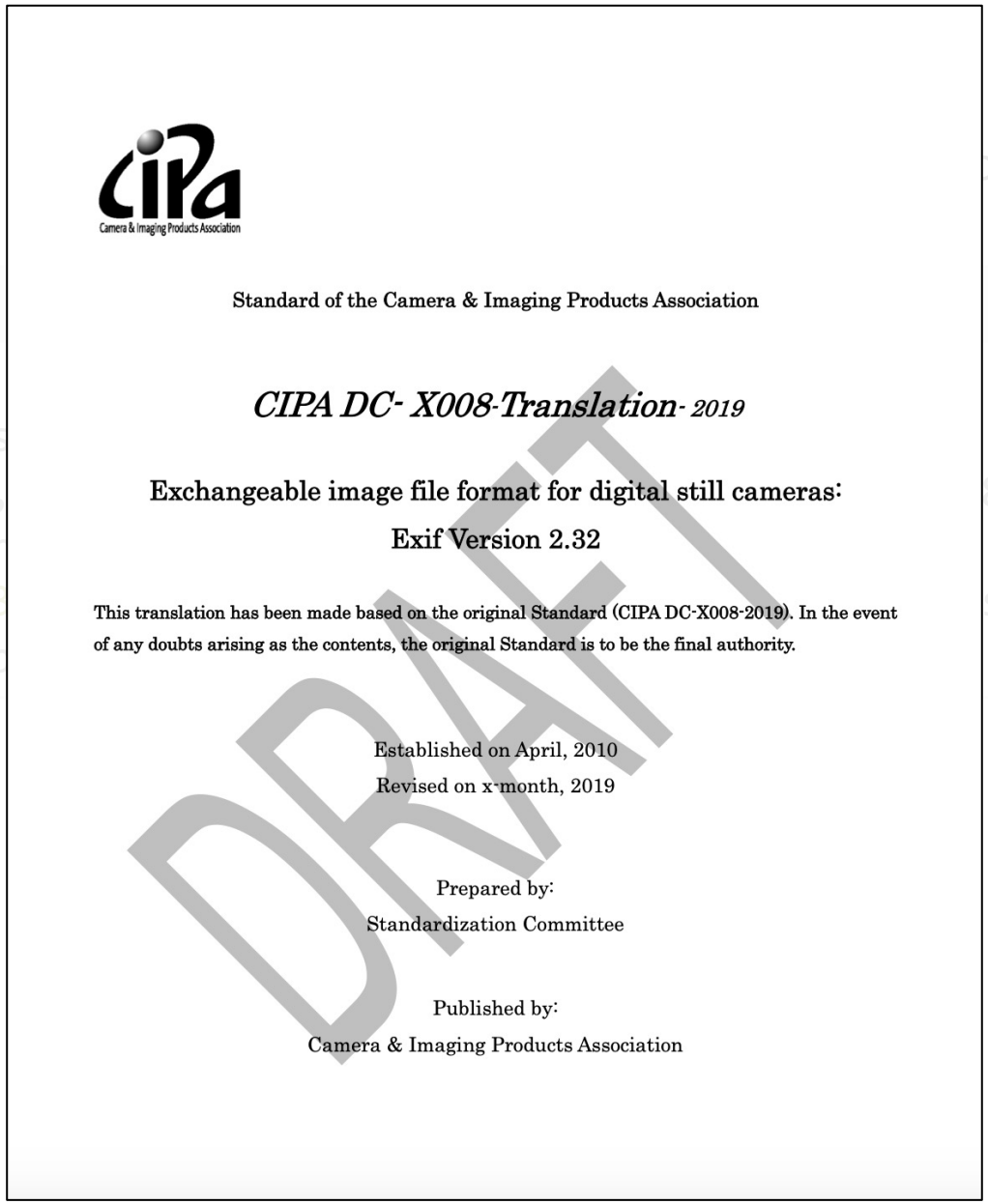
Exchangeable image file format for digital still cameras

```
~$ file file1
file1: JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=11, manufacturer=NIKON CORPORATION, model=NIKON D3200, orientation=upper-left, xresolution=180, yresolution=188, resolutionunit=2, software=Ver.1.04 , datetime=2020:12:30 16:28:47, GPS-Data], baseline, precision 8, 3008x2000, components 3
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images



Standard of the Camera & Imaging Products Association

CIPA DC- X008-Translation- 2019

Exchangeable image file format for digital still cameras:
Exif Version 2.32

This translation has been made based on the original Standard (CIPA DC-X008-2019). In the event of any doubts arising as the contents, the original Standard is to be the final authority.

Established on April, 2010
Revised on x-month, 2019

Prepared by:
Standardization Committee

Published by:
Camera & Imaging Products Association

Exif data can be embedded in various formats including JPEG, TIFF or PNG!

https://www.cipa.jp/std/documents/e/DC-X008-Translation-2019-E.pdf

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ file file1
```

```
file1: JPEG image data, Exif standard: [TIFF image data, big-endian, direntries=11, manufacturer=NIKON CORPORATION, model=NIKON D3200, orientation=upper-left, xresolution=180, yresolution=188, resolutionunit=2, software=Ver.1.04 , datetime=2020:12:30 16:28:47, GPS-Data], baseline, precision 8, 3008x2000, components 3
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
```

```
ExifTool Version Number         : 12.16
File Name                       : file1
Directory                       : .
File Size                       : 4.2 MiB
File Modification Date/Time     : 2021:01:07 22:56:33+01:00
File Access Date/Time           : 2021:01:09 02:24:29+01:00
File Inode Change Date/Time     : 2021:01:09 02:24:28+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

exiftool includes file system information

```
~$ exiftool file1
ExifTool Version Number         : 12.16
File Name                       : file1
Directory                       : .
File Size                       : 4.2 MiB
File Modification Date/Time     : 2021:01:07 22:56:33+01:00
File Access Date/Time           : 2021:01:09 02:24:29+01:00
File Inode Change Date/Time     : 2021:01:09 02:24:28+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
ExifTool Version Number         : 12.16
File Name                       : file1
Directory                       : .
File Size                       : 4.2 MiB
File Modification Date/Time     : 2021:01:07 22:56:33+01:00
File Access Date/Time           : 2021:01:09 02:24:29+01:00
File Inode Change Date/Time     : 2021:01:09 02:24:28+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
```

But also a lot of (!)
Exif information

Images

```
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2020:12:31 14:43:19
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/794
F Number                        : 1.7
Exposure Program                : Program AE
ISO                             : 100
Exif Version                    : 0220
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/794
Aperture Value                  : 1.7
Brightness Value                : 4.72
Exposure Compensation           : 0
Max Aperture Value              : 1.7
Metering Mode                   : Center-weighted average
Light Source                    : Unknown
Flash                           : Off, Did not fire
Focal Length                    : 4.2 mm
Sub Sec Time                    : 857774
Sub Sec Time Original           : 857774
Sub Sec Time Digitized          : 857774
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 4608
Exif Image Height               : 3456
Interoperability Index          : R98 - DCF basic file (sRGB)
Interoperability Version        : 0100
Sensing Method                  : Not defined
Scene Type                      : Directly photographed
Exposure Mode                   : Auto
White Balance                   : Auto
Focal Length In 35mm Format     : 25 mm
Scene Capture Type              : Standard
GPS Latitude Ref                : North
GPS Longitude Ref               : East
GPS Altitude Ref                : Above Sea Level
GPS Time Stamp                  : 13:43:19
GPS Processing Method           : GPS
GPS Date Stamp                  : 2020:12:31
Compression                     : JPEG (old-style)
Thumbnail Offset                : 1112
Thumbnail Length                : 26572
XMP Toolkit                     : Adobe XMP Core 5.1.0-jc003
Capture Mode                    : Photo
Scene                           : AutoHDR
Is HDR Active                   : False
Is Night Mode Active            : False
Scene Detect Result Ids         : [41, 41]
Scene Detect Result Confidences : [0.99999976, 0.99999976]
Lens Facing                     : Back
Image Width                     : 4608
Image Height                    : 3456
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 1.7
Image Size                      : 4608x3456
Megapixels                      : 15.9
Scale Factor To 35 mm Equivalent: 5.9
Shutter Speed                   : 1/794
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes, use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
Circle Of Confusion             : 0.005 mm
Field Of View                   : 71.5 deg
Focal Length                    : 4.2 mm (35 mm equivalent: 25.0 mm)
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
Hyperfocal Distance             : 2.08 m
Light Value                     : 11.2
```

But also a lot of (!)
Exif information

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Camera information

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Camera information

Temporal information

By default, Exif does not support any time zone information!

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify
Thumbn

GPS Al                          : 33542 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Camera information

Temporal

0x0007	7	GPSInfo	Exif.GPSInfo.GPSTimeStamp	Rational	Indicates the time as UTC (Coordinated Universal Time). <TimeStamp> is expressed as three RATIONAL values giving the hour, minute, and second (atomic clock).

https://www.exiv2.org/tags.html

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

About

ExifTool meta information reader/writer

exiftool.org/

```
~$ exiftool file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Camera information

Temporal information

GPS information

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
```

```
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool "-DateTimeOriginal-=30:0:0 0:0:0" file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 1990:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 1990:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool "-Model=iPhone" file1
```

```
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : iPhone
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 1990:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 1990:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool -GPSLatitude=1.234 -GPSLongitude=1.337 file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : iPhone
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 1990:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 1990:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 1 deg 14' 2.40" N
GPS Longitude                   : 1 deg 20' 13.20" E
[…]
GPS Position                    : 1 deg 14' 2.40" N, 1 deg 20' 13.20" E
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : iPhone
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 1990:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 1990:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 1 deg 14' 2.40" N
GPS Longitude                   : 1 deg 20' 13.20" E
[…]
GPS Position                    : 1 deg 14' 2.40" N, 1 deg 20' 13.20" E
[…]
```

Tampering Exif data could require changing multiple tags

Images

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1-edited
[…]
Software                        : GIMP 2.10.22
Modify Date                     : 2021:01:08 11:02:26
[…]
Platform                        : Windows
Time Stamp                      : 1610100199192269
Version                         : 2.10.22
Creator Tool                    : GIMP 2.10
History Software Agent          : Gimp 2.10 (Windows)
History When                    : 2021:01:08 11:03:19
Profile Date Time               : 2021:01:08 10:00:32
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2021:01:08 11:02:26.857774
[…]
```

Software may change existing Exif metadata…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1-edited
[…]
Software                        : GIMP 2.10.22
Modify Date                     : 2021:01:08 11:02:26
[…]
Platform                        : Windows
Time Stamp                      : 1610100199192269
Version                         : 2.10.22
Creator Tool                    : GIMP 2.10
History Software Agent          : Gimp 2.10 (Windows)
History When                    : 2021:01:08 11:03:19
Profile Date Time               : 2021:01:08 10:00:32
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2021:01:08 11:02:26.857774
[…]
```

… but also add new information

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1-edited
[…]
Software                        : GIMP 2.10.22
Modify Date                     : 2021:01:08 11:02:26
[…]
Platform                        : Windows
Time Stamp                      : 1610100199192269
Version                         : 2.10.22
Creator Tool                    : GIMP 2.10
History Software Agent          : Gimp 2.10 (Windows)
History When                    : 2021:01:08 11:03:19
Profile Date Time               : 2021:01:08 10:00:32
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2021:01:08 11:02:26.857774
[…]
```

Convert epoch to human-readable date and vice versa

1610100199192269 Timestamp to Human date [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **microseconds (1/1,000,000 second)**:
GMT: Friday, 8. January 2021 10:03:19.192
Your time zone: Freitag, 8. Januar 2021 11:03:19.192 GMT+01:00
Relative: A year ago

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool file1-edited
[…]
Software                        : GIMP 2.10.22
Modify Date                     : 2021:01:08 11:02:26
[…]
Platform                        : Windows
Time Stamp                      : 1610100199192269
Version                         : 2.10.22
Creator Tool                    : GIMP 2.10
History Software Agent          : Gimp 2.10 (Windows)
History When                    : 2021:01:08 11:03:19
Profile Date Time               : 2021:01:08 10:00:32
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2021:01:08 11:02:26.857774
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

```
~$ exiftool IMG0171
[…]
Software
Modify Date
[…]
Platform
Time Stamp
Version
Creator Tool
History Software Agent
History When
Profile Date Time
[…]
Create Date
Date/Time Original
Modify Date
[…]
```


Systems focusing on sharing files or messages

System	Summary	Displays correctly	Displays 4Cs?	SaveAs embedded?	Download embedded?
Dropbox	Passed through original file, preview can be SavedAs with stripped off metadata. (Not tested in 2016)	●	●	Exif IPTC	Exif IPTC
Facebook	No embedded metadata displayed. SavedAs files have no XMP metadata. A few rights related fields were retained in IIM and Exif. 2 IIM fields contain data generated by Facebook. Compared to 2016: SaveAs improved Exif metadata.	●	●	Exif IPTC IIM, IPTC XMP	●
Google Drive	Passed through original file, no SaveAs supported. (Not tested in 2016)	●	●	●	Exif IPTC
Microsoft OneDrive	Passed through original file, preview can be SavedAs with stripped off metadata. (Not tested in 2016)	●	●	Exif IPTC	Exif IPTC
Twitter	No embedded metadata displayed. Metadata is stripped off in SavedAs files. Compared to 2016: no change.	●	●	Exif IPTC	●

https://iptc.org/standards/photo-metadata/social-media-sites-photo-metadata-test-results-2019/

The more metadata standards the merrier…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

IPTC Photo Metadata Standard 2021.1

IPTC Photo Metadata Working Group – office@iptc.org – Version 2021.1 Revision 1, 2021-10-21

About the Standard

IPTC Photo Metadadata Standard 2021.1, including

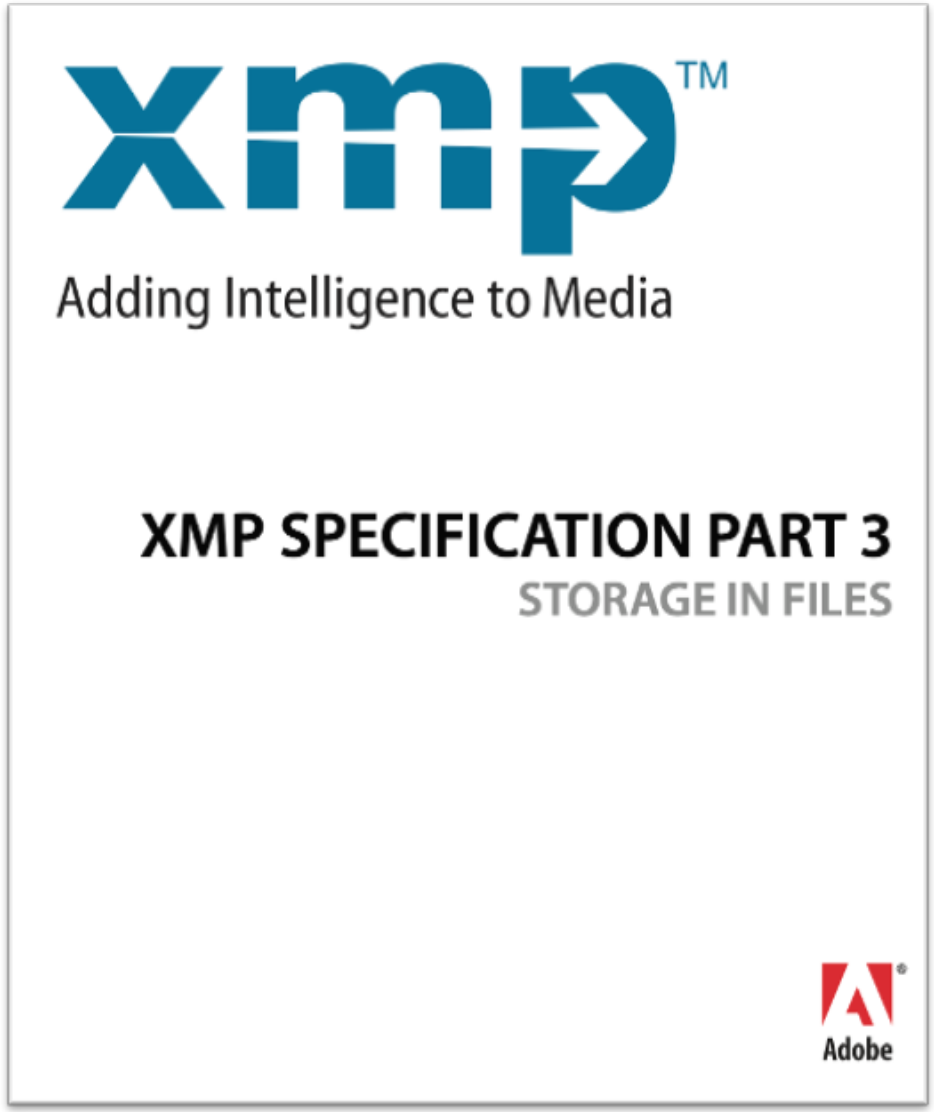
- IPTC Core Metadata Schema 1.3
- IPTC Extension Metadata Schema 1.6

Copyright

Copyright © 2021 by IPTC, the International Press Telecommunications Council - https://iptc.org. All Rights Reserved.

The IPTC Photo Metadata Standard document is published under the Creative Commons Attribution 4.0 license - see the full license agreement at http://creativecommons.org/licenses/by/4.0/. By obtaining, using and/or copying this document, you (the licensee) agree that you have read, understood, and will comply with the terms and conditions of the license.

This project intends to use materials that are either in the public domain or are available by the permission for their respective copyright holders. All materials of this IPTC standard covered by copyright shall be licensable at no charge.



XMP™

Adding Intelligence to Media

XMP SPECIFICATION PART 3

STORAGE IN FILES

Adobe

https://www.iptc.org/std/photometadata/specification/IPTC-PhotoMetadata
https://wwwimages2.adobe.com/content/dam/acom/en/devnet/xmp/pdfs/XMP%20SDK%20Release%20cc-2016-08/XMPSpecificationPart3.pdf

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

Features

- Powerful, fast, flexible and customizable
- Supports a large number of different file formats
- Reads EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP, ID3, Lyrics3 and more...
- Writes EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, ICC Profile, Photoshop IRB, AFCP and more...
- Reads and writes maker notes of many digital cameras
- Reads timed metadata (eg. GPS track) from MOV/MP4/M2TS/AVI videos
- Numerous output formatting options (including tab-delimited, HTML, XML and JSON)
- Multi-lingual output (cs, de, en, en-ca, en-gb, es, fi, fr, it, ja, ko, nl, pl, ru, sv, tr, zh-cn or zh-tw)
- Geotags images from GPS track log files (with time drift correction!)
- Generates track logs from geotagged images
- Shifts date/time values to fix timestamps in images
- Renames files and organizes in directories (by date or by any other meta information)
- Extracts thumbnail images, preview images, and large JPEG images from RAW files
- Copies meta information between files (even different-format files)
- Reads/writes structured XMP information
- Deletes meta information individually, in groups, or altogether
- Sets the file modification date (and creation date in Mac and Windows) from EXIF information
- Supports alternate language tags in XMP, PNG, ID3, Font, QuickTime, ICC Profile, MIE and MXF information
- Processes entire directory trees
- Creates text output file for each image file
- Creates binary-format metadata-only (MIE, EXV) files for metadata backup
- Automatically backs up original image when writing
- Organizes output into groups
- Conditionally processes files based on value of any meta information
- Ability to add custom user-defined tags
- Support for MWG (Metadata Working Group) recommendations
- Recognizes thousands of different tags
- Tested with images from thousands of different camera models
- Advanced verbose and HTML-based hex dump outputs

`http://exiftool.sourceforge.net/#features`

- Luckily, `exiftool` can parse and display a lot of different metadata formats!
- That is not the case for all applications, especially when multiple formats may be present.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Images

Features

- Powerful, fast, flexible and customizable
- Supports a large number of different file formats
- Reads EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, IC
- Writes EXIF, GPS, IPTC, XMP, JFIF, MakerNotes, GeoTIFF, IC
- Reads and writes maker notes of many digital cameras
- Reads timed metadata (eg. GPS track) from MOV/MP4/M2TS/A
- Numerous output formatting options (including tab-delimited, HT
- Multi-lingual output (cs, de, en, en-ca, en-gb, es, fi, fr, it, ja, ko, r
- Geotags images from GPS track log files (with time drift correcti
- Generates track logs from geotagged images
- Shifts date/time values to fix timestamps in images
- Renames files and organizes in directories (by date or by any o
- Extracts thumbnail images, preview images, and large JPEG im
- Copies meta information between files (even different-format file
- Reads/writes structured XMP information
- Deletes meta information individually, in groups, or altogether
- Sets the file modification date (and creation date in Mac and Wi
- Supports alternate language tags in XMP, PNG, ID3, Font, Quic
- Processes entire directory trees
- Creates text output file for each image file
- Creates binary-format metadata-only (MIE, EXV) files for metad
- Automatically backs up original image when writing
- Organizes output into groups
- Conditionally processes files based on value of any meta inform
- Ability to add custom user-defined tags
- Support for MWG (Metadata Working Group) recommendations
- Recognizes thousands of different tags
- Tested with images from thousands of different camera models
- Advanced verbose and HTML-based hex dump outputs

http://exiftool.sourceforge.net/#features

XMP, IPTC/IIM, or Exif; which is preferred?

```
$ exiftool -G1 -XMP-dc:des
C:caption-abstract -IFD0:i
-dc]     Description
C]       Caption-Abstract
0]       Image Description
```

Your metadata may be stored in multiple places in your media file. We took a deep dive to find out which ones are preferred by various applications.

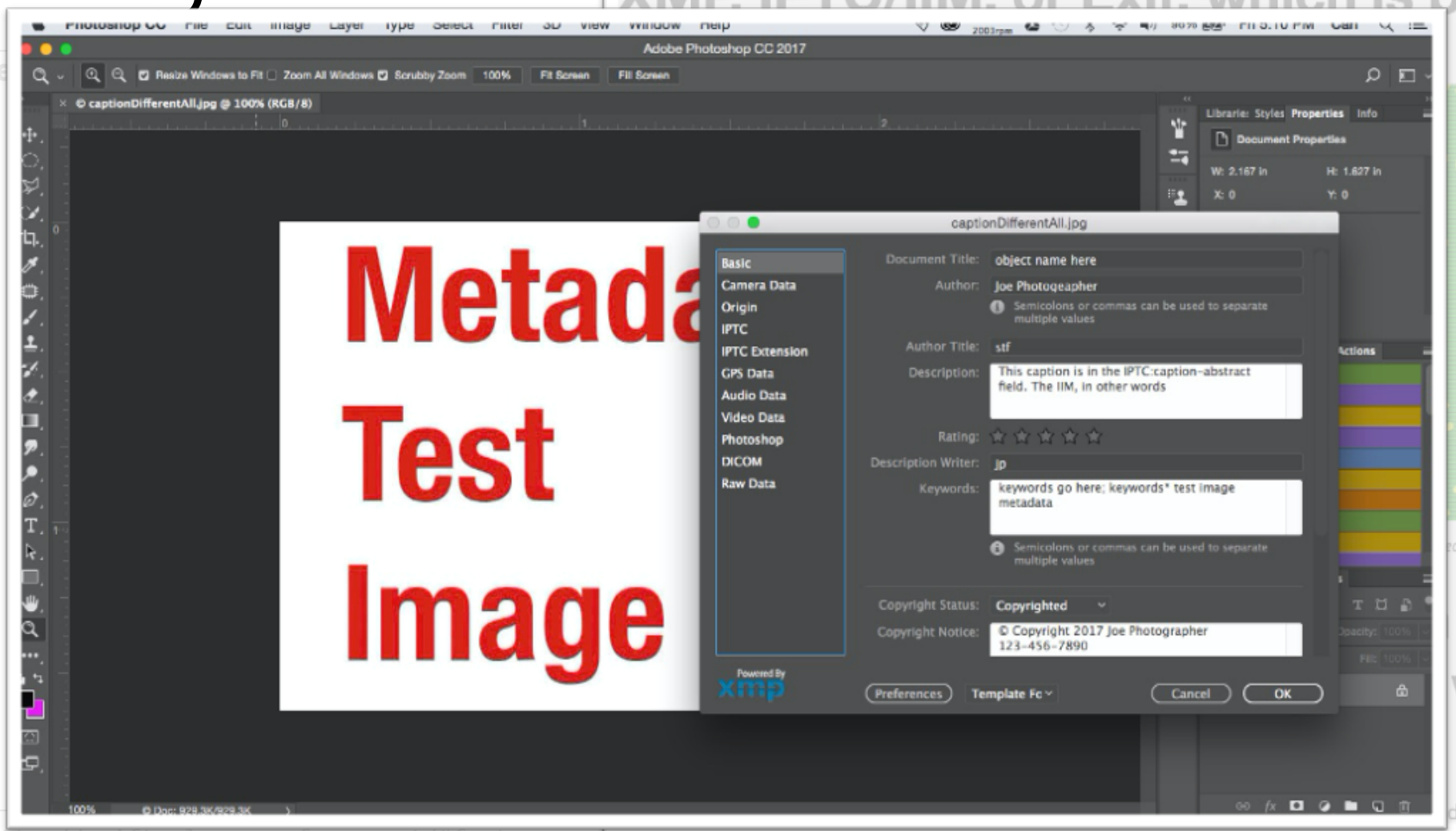
Your important metadata lives in two, maybe three, places in your file; which one are you seeing?

Which instance of the IPTC metadata does your favorite application prefer? Inquiring minds want to know.

https://www.carlseibert.com/xmp-iptciim-or-exif-which-is-preferred/

isplay
ts!
tions,
especially when multiple formats
may be present.

Images



https://www.carlseibert.com/xmp-iptciim-or-exif-which-is-preferred/

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

file2 file3 file4 file5

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ file file2
```

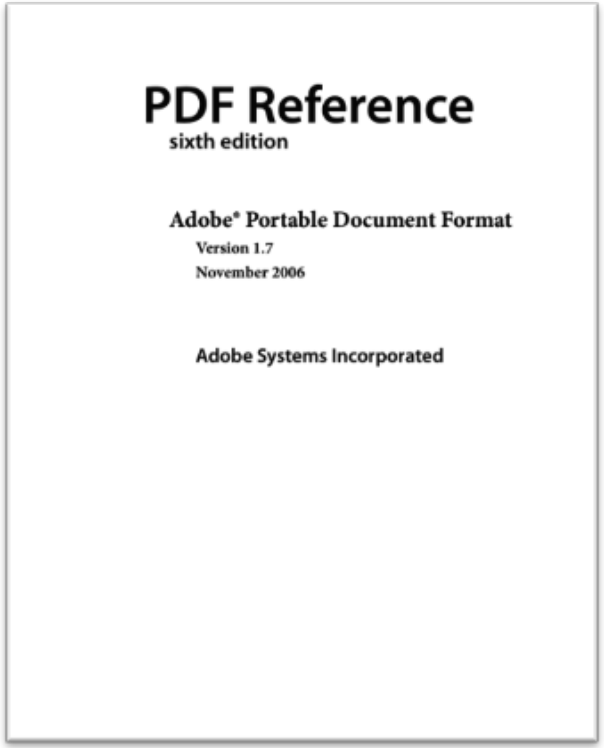
file2

Hochschule Bonn-Rhein-Sieg

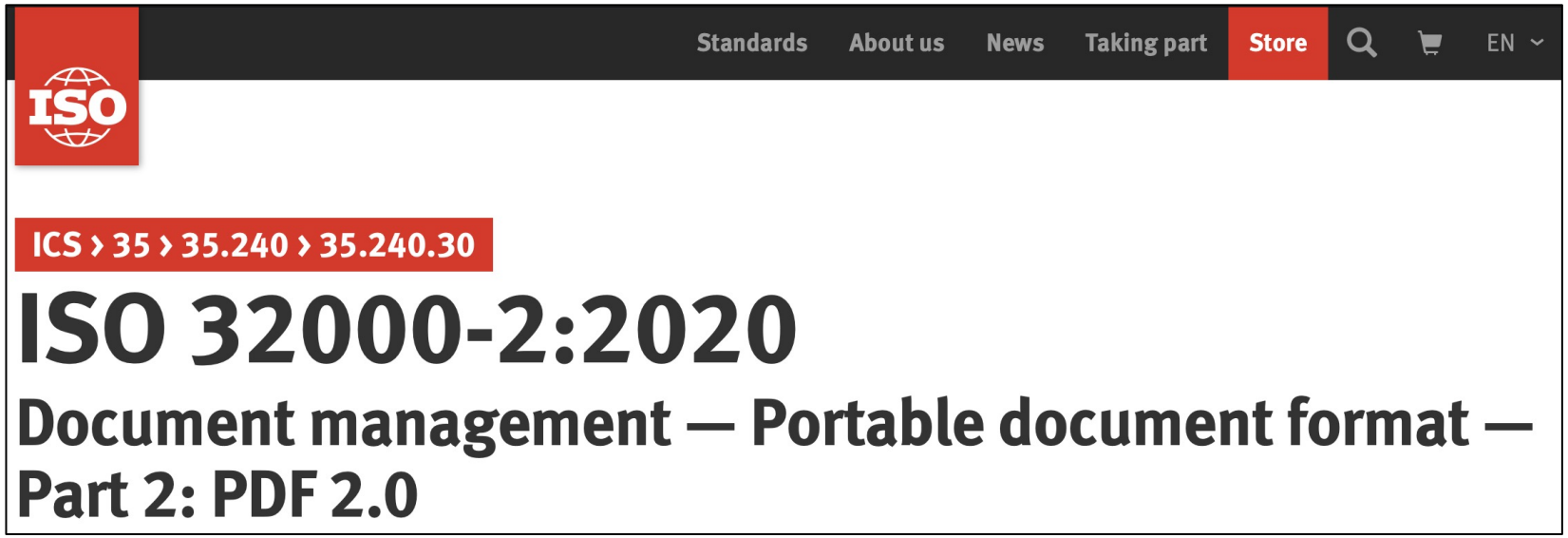
Fraunhofer FKIE

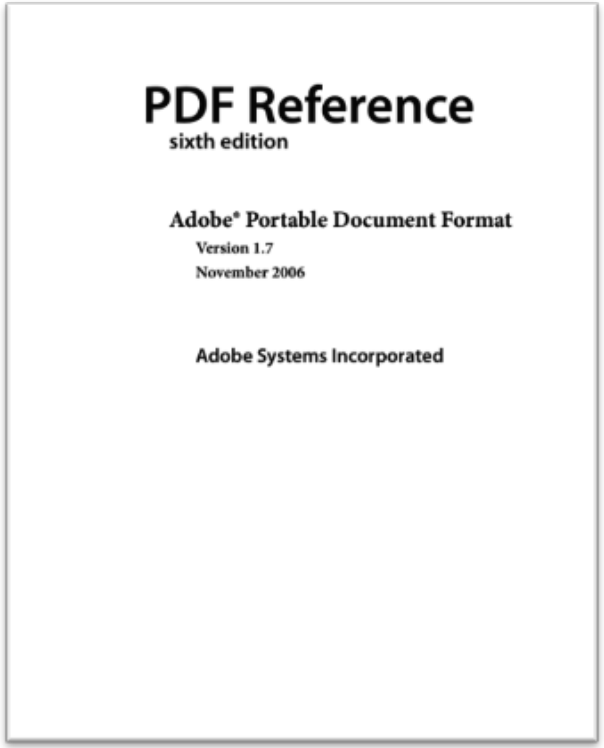
PDFs

```
~$ file file2
file2: PDF document, version 1.6
```



PDFs



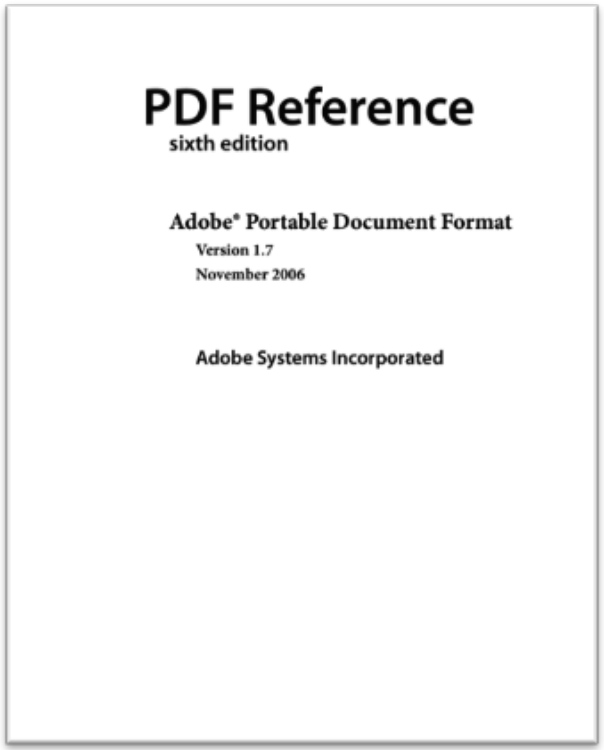


*„Although it is an open standard, one major difference compared with prior versions of PDF is that ISO now holds the copyright to the PDF specification and **thus PDF 2.0 is not freely downloadable.**“*

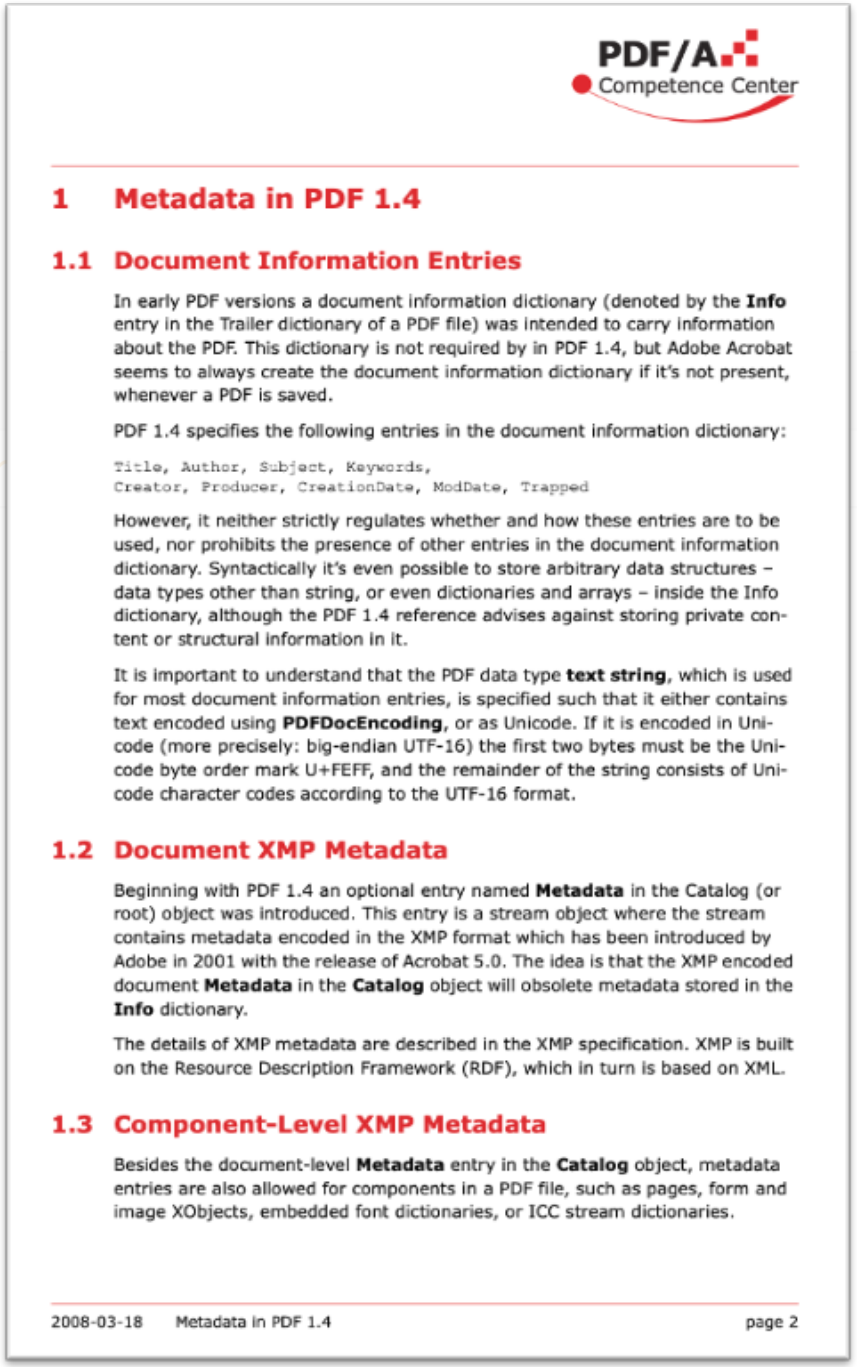
https://www.pdfa.org/resource/iso-32000-pdf/

PDFs

```
~$ file file2
file2: PDF document, version 1.6
```



PDFs



PDF/A Competence Center

1 Metadata in PDF 1.4

1.1 Document Information Entries

In early PDF versions a document information dictionary (denoted by the **Info** entry in the Trailer dictionary of a PDF file) was intended to carry information about the PDF. This dictionary is not required by in PDF 1.4, but Adobe Acrobat seems to always create the document information dictionary if it's not present, whenever a PDF is saved.

PDF 1.4 specifies the following entries in the document information dictionary:

```
Title, Author, Subject, Keywords,
Creator, Producer, CreationDate, ModDate, Trapped
```

However, it neither strictly regulates whether and how these entries are to be used, nor prohibits the presence of other entries in the document information dictionary. Syntactically it's even possible to store arbitrary data structures – data types other than string, or even dictionaries and arrays – inside the Info dictionary, although the PDF 1.4 reference advises against storing private content or structural information in it.

It is important to understand that the PDF data type **text string**, which is used for most document information entries, is specified such that it either contains text encoded using **PDFDocEncoding**, or as Unicode. If it is encoded in Unicode (more precisely: big-endian UTF-16) the first two bytes must be the Unicode byte order mark U+FEFF, and the remainder of the string consists of Unicode character codes according to the UTF-16 format.

1.2 Document XMP Metadata

Beginning with PDF 1.4 an optional entry named **Metadata** in the Catalog (or root) object was introduced. This entry is a stream object where the stream contains metadata encoded in the XMP format which has been introduced by Adobe in 2001 with the release of Acrobat 5.0. The idea is that the XMP encoded document **Metadata** in the **Catalog** object will obsolete metadata stored in the **Info** dictionary.

The details of XMP metadata are described in the XMP specification. XMP is built on the Resource Description Framework (RDF), which in turn is based on XML.

1.3 Component-Level XMP Metadata

Besides the document-level **Metadata** entry in the **Catalog** object, metadata entries are also allowed for components in a PDF file, such as pages, form and image XObjects, embedded font dictionaries, or ICC stream dictionaries.

2008-03-18 Metadata in PDF 1.4 page 2

https://www.pdfa.org

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

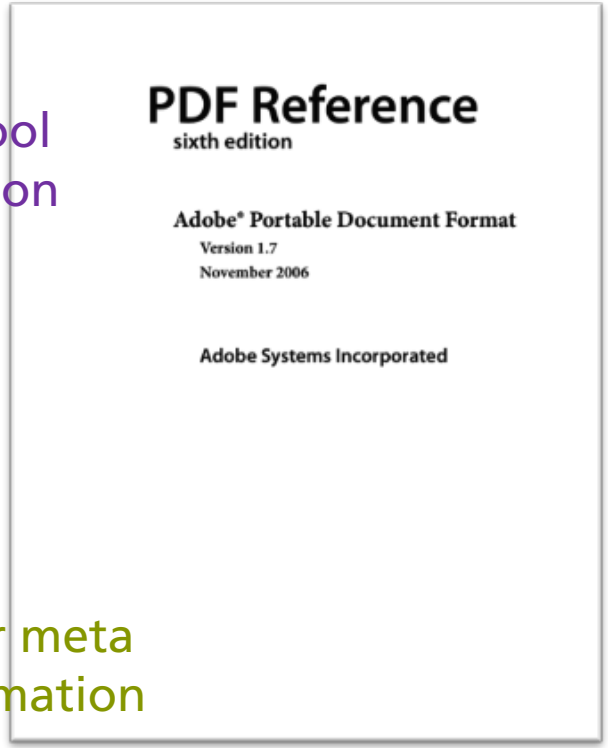
PDFs

```
~$ exiftool file2
[…]
Producer                        : Acrobat Distiller 7.0.5 (Windows)
Creator Tool                    : FrameMaker 7.2
Modify Date                     : 2006:11:18 21:10:43-03:30
Create Date                     : 2006:10:17 08:10:20Z
Metadata Date                   : 2006:11:18 21:10:43-03:30
Format                          : application/pdf
Title                           : PDF Reference, version 1.7
Creator                         : Adobe Systems Incorporated
Description                     : Adobe Portable Document Format (PDF)
Document ID                     : uuid:eeff029e-0188-4376-8950-260bbf9f2455
Instance ID                     : uuid:a3b6af41-14b1-4f82-81ea-5110da226f00
Has XFA                         : No
Page Count                      : 1310
Subject                         : Adobe Portable Document Format (PDF)
Author                          : Adobe Systems Incorporated
```

Mostly tool information

Temporal information

Other meta information

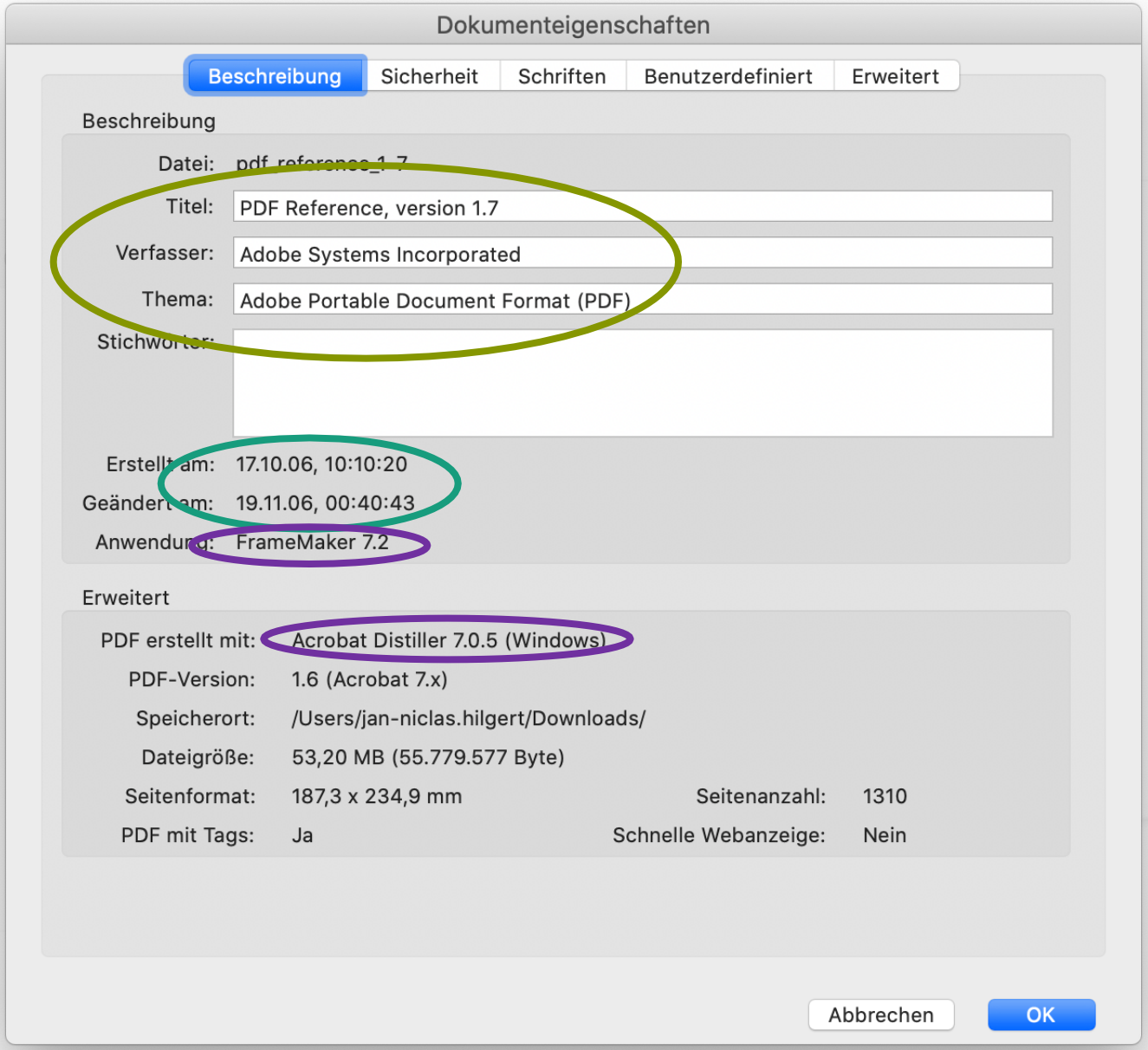


Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ exiftool pdf_refer
[…]
Producer
Creator Tool
Modify Date
Create Date
Metadata Date
Format
Title
Creator
Description
Document ID
Instance ID
Has XFA
Page Count
Subject
Author
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

2126

Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 (Coronaschutzverordnung – CoronaSchVO)

Vom 2. Dezember 2021

Auf Grund von § 32 in Verbindung mit § 28 Absatz 1, § 28a Absatz 3 bis 8, § 73 Absatz 1a Nummer 6 und 24 des Infektionsschutzgesetzes vom 20. Juli 2000 (BGBl. I S. 1045), von denen § 28 Absatz 1 zuletzt durch Artikel 1 Nummer 16 des Gesetzes vom 18. November 2020 (BGBl. I S. 2397) geändert, § 28a Absatz 3 zuletzt durch Artikel 12 Nummer 0 des Gesetzes vom 10. September 2021 (BGBl. I S. 4147) geändert, § 28a Absatz 4 bis 6 durch Artikel 1 Nummer 17 des Gesetzes vom 18. November 2020 (BGBl. I S. 2397) eingefügt, Absatz 7 durch Artikel 1 Nummer 3 des Gesetzes vom 22. November 2021 (BGBl. I S. 4906) geändert, Absatz 8 durch Artikel 1 Nummer 3 des Gesetzes vom 22. November 2021 (BGBl. I S. 4906) angefügt, § 32 durch Artikel 1 Nummer 4 des Gesetzes vom 22. April 2021 (BGBl. I S. 802) neu gefasst, § 73 Absatz 1a Nummer 6 zuletzt durch Artikel 1 Nummer 26 des Gesetzes vom 19. Mai 2021 (BGBl. I S. 1018) und § 73 Absatz 1a Nummer 24 zuletzt durch Artikel 12 Nummer 2 des Gesetzes vom 10. September 2021 (BGBl. I S. 4147) geändert werden sind, sowie von § 10 der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung vom 8. Mai 2021 (BAnz AT 10.05.2021 V1) und § 13 des Infektionsschutz- und Befugnisgesetzes vom 14. April 2020 (GV. NRW. S. 218b), der durch Artikel 1 Nummer 6 des Gesetzes vom 25. März 2021 (GV. NRW. S. 312) geändert worden ist, verordnet das Ministerium für Arbeit, Gesundheit und Soziales:

§ 1
Zielsetzung, Schutzmaßnahmen

(1) Zur Fortsetzung der erfolgreichen Bekämpfung der SARS-CoV-2-Pandemie, zur Begrenzung des erneuten Anstiegs der Infektionszahlen und insbesondere zur weiteren Gewährleistung ausreichender medizinischer Versorgungskapazitäten werden mit dieser Verordnung Maßnahmen angeordnet, die die Infektionsgefahren verringern und möglichst minimieren.
(2) Unter Wahrung des Grundsatzes der Verhältnismäßigkeit sollen die Regelungen dieser Verordnung im Zusammenwirken mit dem fortschreitenden Schutz der Bevölkerung durch die Impfung und der Eigenverantwortung der Bürgerinnen und Bürger Rahmenbedingungen für das öffentliche und private Leben setzen, die vor allem geimpften und genesenen Personen wieder eine weitgehend uneingeschränkte Nutzung von gesellschaftlichen, kulturellen, sozialen und sportlichen Angeboten und Einrichtungen ermöglichen und so eine gelebte Normalisierung aller sozialen, gesellschaftlichen, kulturellen und wirtschaftlichen Lebensbereiche ermöglichen. Dabei sind andererseits ein Wiederanstieg der Infektionszahlen und die

Hochschule Bonn-Rhein-Sieg

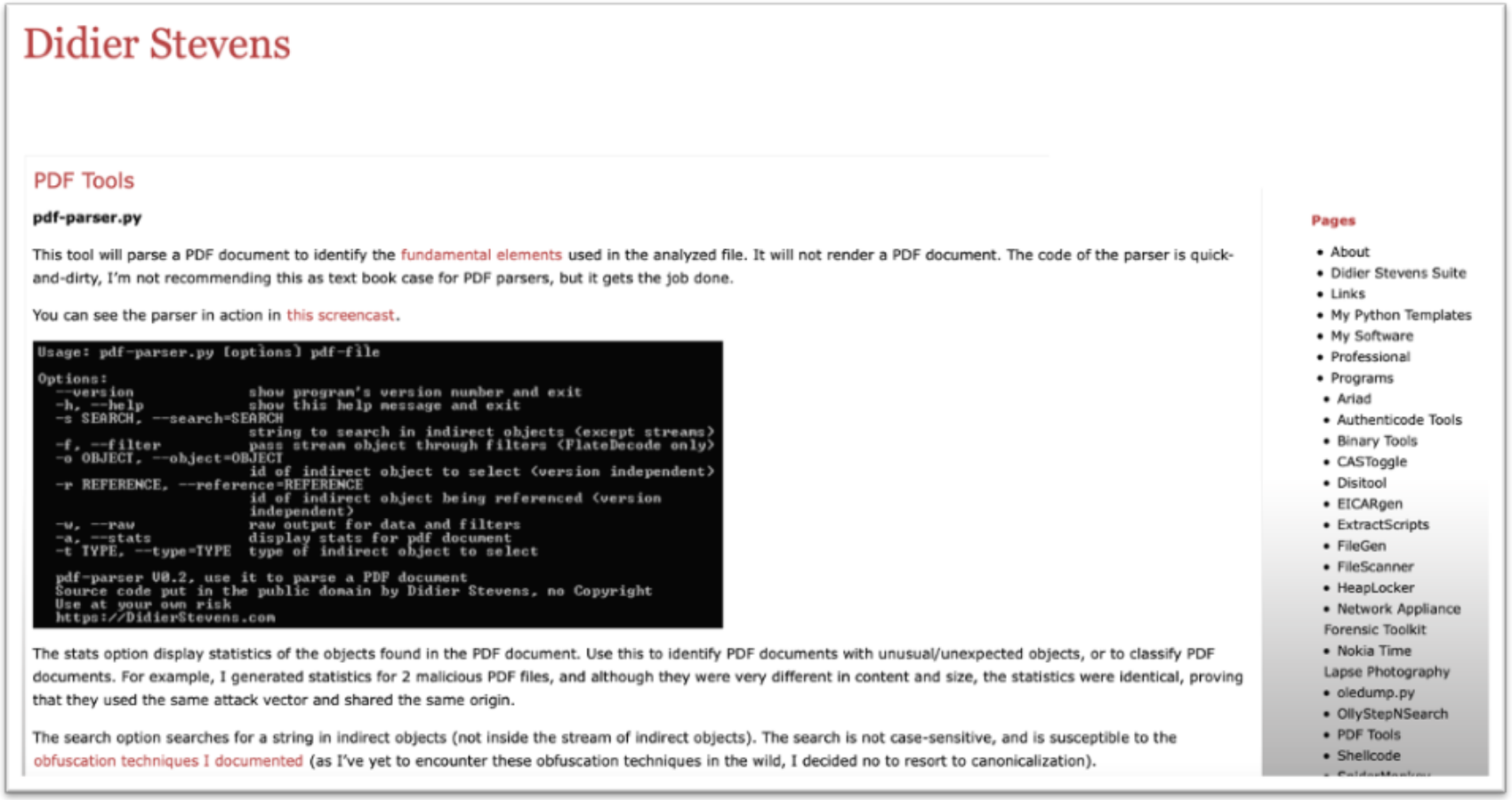
Fraunhofer FKIE

PDFs

```
~$ exiftool 2021-12-03_coronaschvo-ab-04.12.2021_final_lesefassung.pdf
ExifTool Version Number         : 12.16
File Name                       : 2021-12-03_coronaschvo-ab-
                                  04.12.2021_final_lesefassung.pdf
[…]
MIME Type                       : application/pdf
PDF Version                     : 1.7
Linearized                      : No
Page Count                      : 13
XMP Toolkit                     : XMP toolkit 2.9.1-13, framework 1.6
Producer                        : GPL Ghostscript 9.55.0
Modify Date                     : 2021:12:03 16:39:44+01:00
Create Date                     : 2021:12:03 16:39:44+01:00
Creator Tool                    : PDF24 Creator
Document ID                     : uuid:bcc70033-56aa-11ec-0000-cb1e4b21421e
Format                          : application/pdf
Title                           : Microsoft Word - 2021-12-03_CoronaSchVO ab
                                  04.12.2021_Lesefassung.docx
Creator                         : Holtg0001
Author                          : Holtg0001
```

Some applications may add useful information automatically

PDFs



Didier Stevens

PDF Tools

pdf-parser.py

This tool will parse a PDF document to identify the fundamental elements used in the analyzed file. It will not render a PDF document. The code of the parser is quick-and-dirty, I'm not recommending this as text book case for PDF parsers, but it gets the job done.

You can see the parser in action in this screencast.

```
Usage: pdf-parser.py [options] pdf-file

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -s SEARCH, --search=SEARCH
                        string to search in indirect objects (except streams)
  -f, --filter          pass stream object through filters (FlateDecode only)
  -o OBJECT, --object=OBJECT
                        id of indirect object to select (version independent)
  -r REFERENCE, --reference=REFERENCE
                        id of indirect object being referenced (version
                        independent)
  -w, --raw             raw output for data and filters
  -a, --stats           display stats for pdf document
  -t TYPE, --type=TYPE  type of indirect object to select

  pdf-parser V0.2, use it to parse a PDF document
  Source code put in the public domain by Didier Stevens, no Copyright
  Use at your own risk
  https://DidierStevens.com
```

The stats option display statistics of the objects found in the PDF document. Use this to identify PDF documents with unusual/unexpected objects, or to classify PDF documents. For example, I generated statistics for 2 malicious PDF files, and although they were very different in content and size, the statistics were identical, proving that they used the same attack vector and shared the same origin.

The search option searches for a string in indirect objects (not inside the stream of indirect objects). The search is not case-sensitive, and is susceptible to the obfuscation techniques I documented (as I've yet to encounter these obfuscation techniques in the wild, I decided no to resort to canonicalization).

Pages

- About
- Didier Stevens Suite
- Links
- My Python Templates
- My Software
- Professional
- Programs
  - Ariad
  - Authenticode Tools
  - Binary Tools
  - CASToggle
  - Disitool
  - EICARgen
  - ExtractScripts
  - FileGen
  - FileScanner
  - HeapLocker
  - Network Appliance Forensic Toolkit
  - Nokia Time Lapse Photography
  - oledump.py
  - OllyStepNSearch
  - PDF Tools
  - Shellcode

https://blog.didierstevens.com/programs/pdf-tools/

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
```

```
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Used to automatically perform an action, when the document or page is viewed or opened

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid created-with-libre-office.pdf
PDFiD 0.2.8 created-with-libre-office.pdf
 PDF Header: %PDF-1.5
 obj                   13
 endobj                13
 stream                 3
 endstream              3
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    0
 /JavaScript            0
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Not always a sign for malicious PDFs!

LibreOffice
The Document Foundation

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Used to launch an application

Launch Actions

A *launch action* launches an application or opens or prints a document. Table 8.53 shows the action dictionary entries specific to this type of action.

PDFs

TABLE 8.53 Additional entries specific to a launch action

KEY	TYPE	VALUE
S	name	*(Required)* The type of action that this dictionary describes; must be **Launch** for a launch action.
F	file specification	*(Required if none of the entries **Win**, **Mac**, or **Unix** is present)* The application to be launched or the document to be opened or printed. If this entry is absent and the viewer application does not understand any of the alternative entries, it should do nothing.
Win	dictionary	*(Optional)* A dictionary containing Windows-specific launch parameters (see Table 8.54; see also implementation note 101 in Appendix H).
Mac	(undefined)	*(Optional)* Mac OS–specific launch parameters; not yet defined.
Unix	(undefined)	*(Optional)* UNIX-specific launch parameters; not yet defined.
NewWindow	boolean	*(Optional; PDF 1.2)* A flag specifying whether to open the destination document in a new window. If this flag is **false**, the destination document replaces the current document in the same window. If this entry is absent, the viewer application should behave in accordance with the current user preference. This entry is ignored if the file designated by the **F** entry is not a PDF document.

PDF Reference 1.7

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

\JS or \JavaScript
contains JavaScript
(not necessarily malicious)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

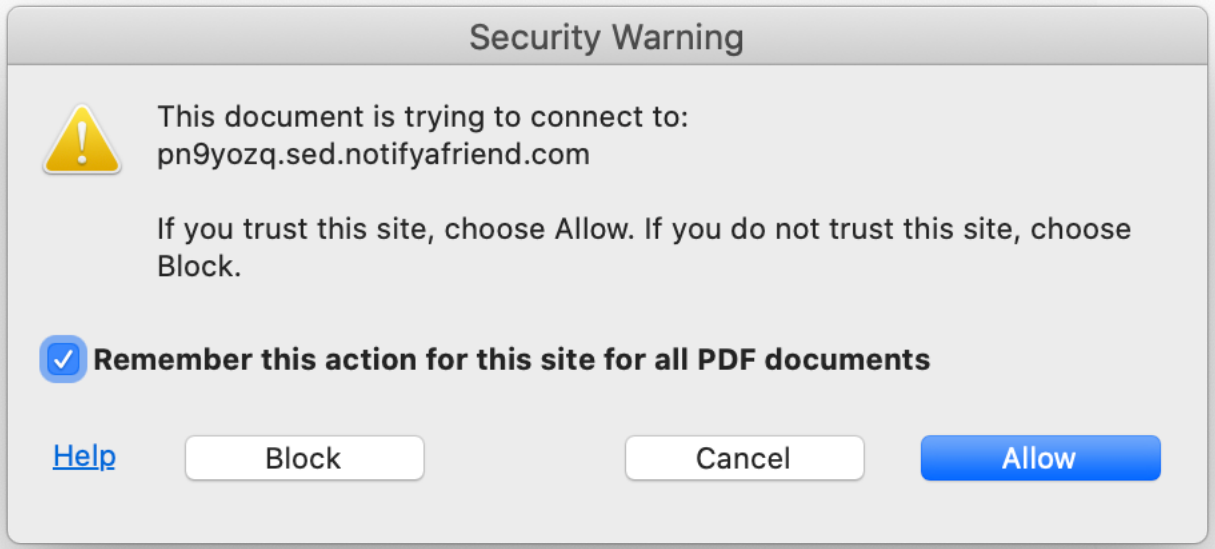
Resolves the specified URI

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```



Resolves the specified URI

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Number of embedded files inside the PDF (e.g. Word documents)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

Gives the number of object streams, which can be used to hide other objects

3.4.6 Object Streams

PDF 1.5 introduces a new kind of stream, an *object stream*, which contains a sequence of PDF objects. The purpose of object streams is to allow a greater number of PDF objects to be compressed, thereby substantially reducing the size of PDF files. The objects in the stream are referred to as *compressed objects*.

PDFs

```
~$ pdf-parser --help
```

```
Usage: pdf-parser.py [options] pdf-file|zip-file|url
pdf-parser, use it to parse a PDF document

Options:
[…]
  -w, --raw             raw output for data and filters
  -a, --stats           display stats for pdf document
  -t TYPE, --type=TYPE  type of indirect object to select
  -O, --objstm          parse stream of /ObjStm objects
  -v, --verbose         display malformed PDF elements
  -x EXTRACT, --extract=EXTRACT
                        filename to extract malformed content to
  -H, --hash            display hash of objects
  -n, --nocanonicalizedoutput
                        do not canonicalize the output
  -d DUMP, --dump=DUMP  filename to dump stream content to
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdf-parser malicious.pdf
```

```
[…]
obj 7 0
 Type: /Filespec
 Referencing: 8 0 R

  <<
    /Type /Filespec
    /F (eicar-dropper.doc)
    /EF
      <<
        /F 8 0 R
      >>
  >>

obj 8 0
 Type: /EmbeddedFile
 Referencing:
 Contains stream

  <<
    /Length 8952
    /Filter /FlateDecode
    /Type /EmbeddedFile
  >>
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdf-parser malicious.pdf
[…]
obj 9 0
 Type: /Action
 Referencing:

  <<
    /Type /Action
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "eicar-dropper.doc", nLaunch: 2 });)
  >>
[…]
```

TABLE 8.90 Additional entries specific to a JavaScript action

KEY	TYPE	VALUE
S	name	*(Required)* The type of action that this dictionary describes; must be **JavaScript** for a JavaScript action.
JS	text string or text stream	*(Required)* A text string or text stream containing the JavaScript script to be executed. ***Note:*** ***PDFDocEncoding*** *or Unicode encoding (the latter identified by the Unicode prefix U+FEFF) is used to encode the contents of the string or stream. (See implementation note 126 in Appendix H.)*

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid file1.pdf
PDFiD 0.2.8 file1.pdf
 PDF Header: %PDF-1.6
 obj                    12
 endobj                 12
 stream                  9
 endstream               9
 xref                    0
 trailer                 0
 startxref               2
 /Page                   1
 /Encrypt                0
 /ObjStm                 2
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0
```

Just a JPEG within a PDF file.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid file1.pdf
PDFiD 0.2.8 file1.pdf
 PDF Header: %PDF-1.6
 obj                    12
 endobj                 12
 stream                  9
 endstream               9
 xref                    0
 trailer                 0
 startxref               2
 /Page                   1
 /Encrypt                0
 /ObjStm                 2
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0
```

No embedded file

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdf-parser elsbeere.pdf
```

```
[…]
obj 12 0
 Type: /XObject
 Referencing: 11 0 R
 Contains stream

  <<
    /BitsPerComponent 8
    /ColorSpace /DeviceRGB
    /Filter /DCTDecode
    /Height 3456
    /Length 4416677
    /Metadata 11 0 R
    /Name /X
    /Subtype /Image
    /Type /XObject
    /Width 4608
  >>
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdf-parser -o 12 -d elsbeere.jpg elsbeere.pdf
~$ exiftool elsbeere.jpg
```

```
[…]
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : OnePlus
Camera Model Name               : ONEPLUS A6003
[…]
Modify Date                     : 2020:12:31 14:43:19
[…]
Date/Time Original              : 2020:12:31 14:43:19
Create Date                     : 2020:12:31 14:43:19
[…]
Create Date                     : 2020:12:31 14:43:19.857774
Date/Time Original              : 2020:12:31 14:43:19.857774
Modify Date                     : 2020:12:31 14:43:19.857774
Thumbnail Image                 : (Binary data 26572 bytes,
                                  use -b option to extract)
GPS Altitude                    : 535.2 m Above Sea Level
GPS Date/Time                   : 2020:12:31 13:43:19Z
GPS Latitude                    : 50 deg 23' 19.87" N
GPS Longitude                   : 6 deg 39' 58.13" E
[…]
GPS Position                    : 50 deg 23' 19.87" N, 6 deg 39' 58.13" E
[…]
```

All our metadata is still there ☺!

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

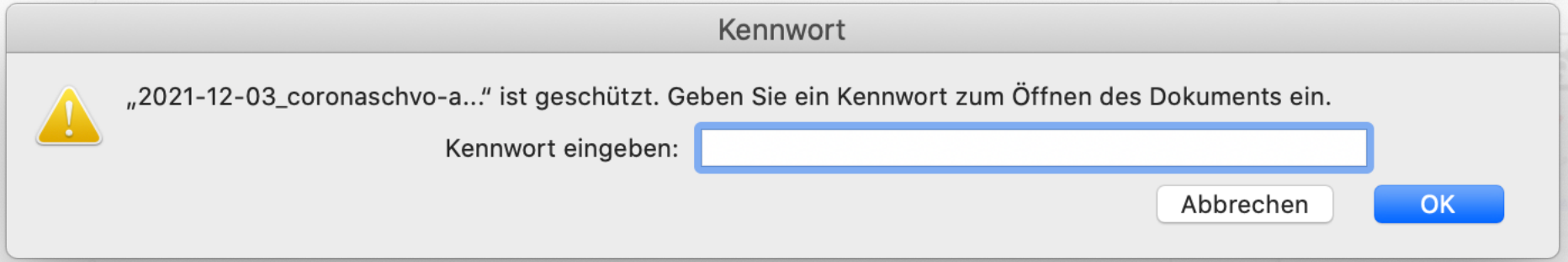
Indicates that the PDF is password protected

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ pdfid malicious.pdf
PDFiD 0.2.8 malicious.pdf
 PDF Header: %PDF-1.1
 obj                    9
 endobj                 9
 stream                 1
 endstream              1
 xref                   0
 trailer                0
 startxref              0
 /Page                  0
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1
 /AA                    0
 /OpenAction            1
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          1
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0
```

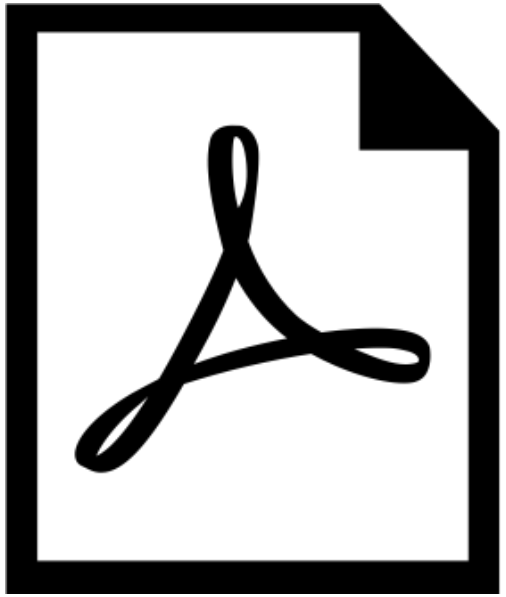


Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

PDFs

```
~$ exiftool 2021-12-03_coronaschvo-ab-04.12.2021_final_lesefassung-enc.pdf
ExifTool Version Number         : 12.16
File Name                       : 2021-12-03_coronaschvo-ab-
                                  04.12.2021_final_lesefassung-enc.pdf
[…]
MIME Type                       : application/pdf
PDF Version                     : 1.6
Linearized                      : No
Encryption                      : Standard V4.4 (128-bit)
User Access                     : Print, Modify, Copy, Annotate, Fill forms, Extract,
Assemble, Print high-res
Warning                         : Document is password protected (use Password option)
```



Encrypted PDFs may not even provide access to metadata

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

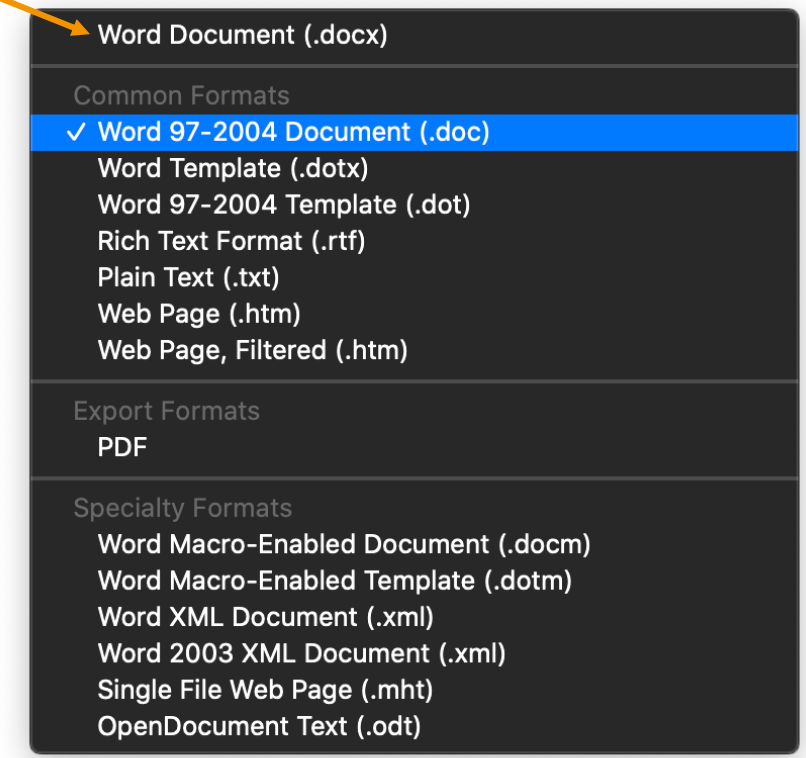
PDFs

```
~$ file file3
```

file3

Office Documents

```
~$ file file3
file3: Microsoft Word 2007+
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

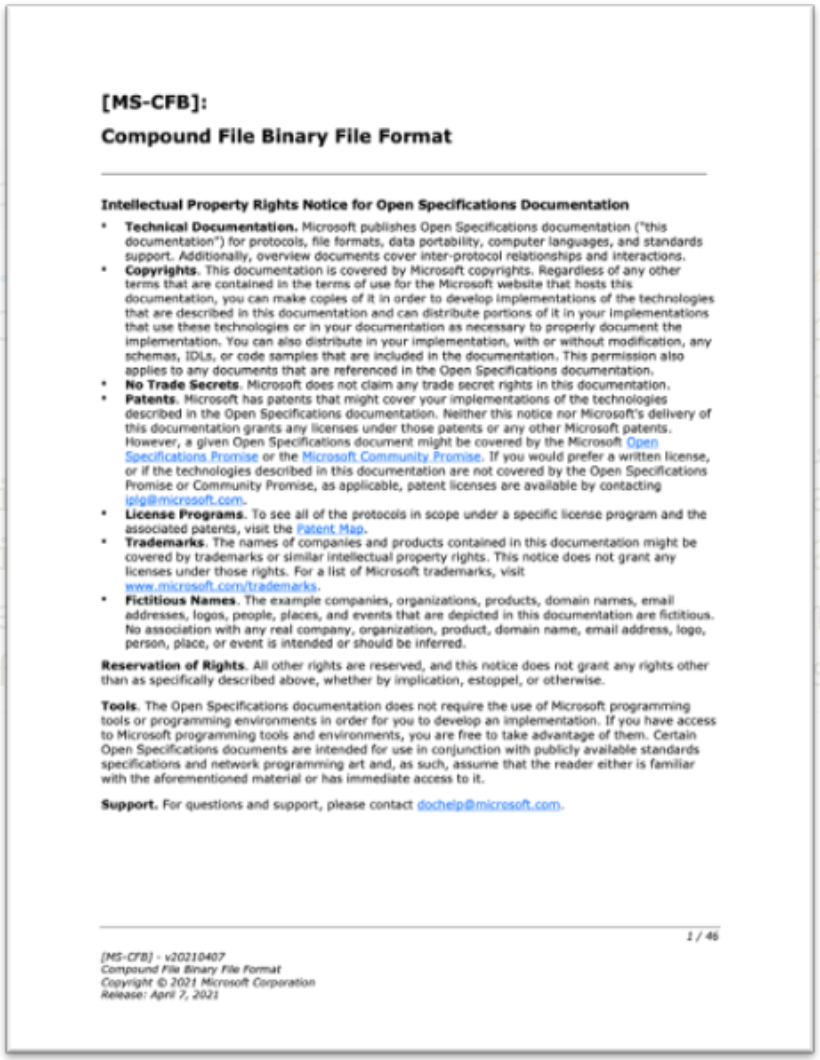
```
~$ file document.doc
```

```
document.doc: Composite Document File V2 Document, Little Endian, Os: MacOS, Version 15.10, Code page: 10000, Author: Hilgert, Jan-Niclas, Template: Normal.dotm, Last Saved By: Hilgert, Jan-Niclas, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Mon Dec 13 12:30:00 2021, Last Saved Time/Date: Mon Dec 13 12:31:00 2021, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, Security: 0
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents



[MS-CFB]:

Compound File Binary File Format

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

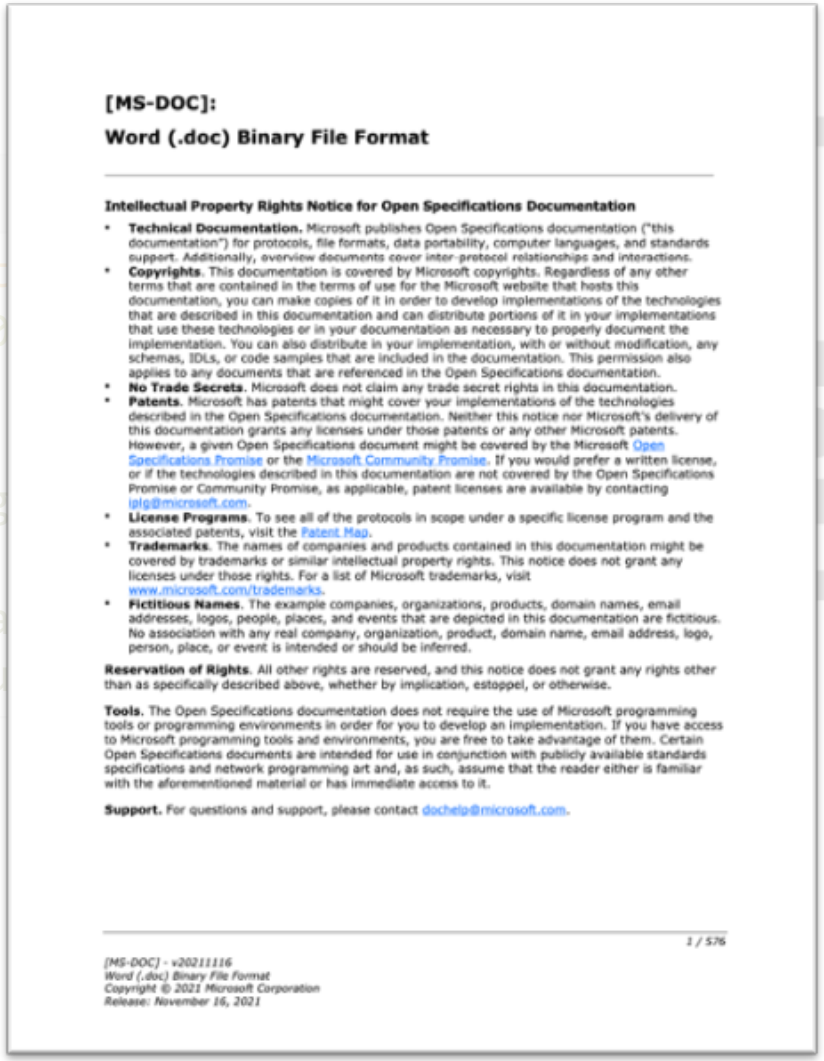
Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

1 / 46

[MS-CFB] - v20210407
Compound File Binary File Format
Copyright © 2021 Microsoft Corporation
Release: April 7, 2021

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cfb/



[MS-DOC]:

Word (.doc) Binary File Format

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

1 / 576

[MS-DOC] - v20211116
Word (.doc) Binary File Format
Copyright © 2021 Microsoft Corporation
Release: November 16, 2021

https://docs.microsoft.com/en-us/openspecs/office_file_formats/ms-doc

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

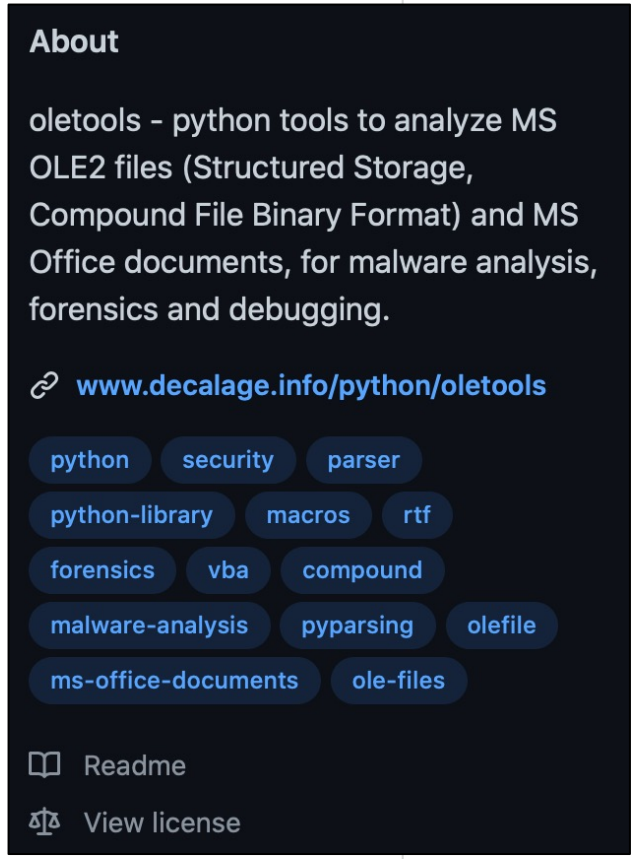
```
~$ file document.doc
```

```
document.doc: Composite Document File V2 Document, Little Endian, Os: MacOS, Version 15.10, Code page: 10000, Author: Hilgert, Jan-Niclas, Template: Normal.dotm, Last Saved By: Hilgert, Jan-Niclas, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Mon Dec 13 12:30:00 2021, Last Saved Time/Date: Mon Dec 13 12:31:00 2021, Number of Pages: 1, Number of Words: 0, Number of Characters: 0, Security: 0
```

Office Documents

```
~$ olemeta document.doc
```

```
[…]
Properties from the SummaryInformation stream:
+---------------------+------------------------------+
|Property             |Value                         |
+---------------------+------------------------------+
|codepage             |10000                         |
|title                |                              |
|subject              |                              |
|author               |Hilgert, Jan-Niclas           |
|keywords             |                              |
|comments             |                              |
|template             |Normal.dotm                   |
|last_saved_by        |Hilgert, Jan-Niclas           |
|revision_number      |1                             |
|total_edit_time      |60                            |
|create_time          |2021-12-13 12:30:00           |
|last_saved_time      |2021-12-13 12:31:00           |
|num_pages            |1                             |
|num_words            |0                             |
|num_chars            |0                             |
|creating_application |Microsoft Office Word         |
|security             |0                             |
+---------------------+------------------------------+
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ olemeta document.doc
```

```
[…]
Properties from the SummaryInformation stream:
+---------------------+------------------------------+
|Property             |Value                         |
+---------------------+------------------------------+
|codepage             |10000                         |
|title                |                              |
|subject              |                              |
|author               |Hilgert, Jan-Niclas           |
|keywords             |                              |
|comments             |                              |
|template             |Normal.dotm                   |
|last_saved_by        |Hilgert, Jan-Niclas           |
|revision_number      |1                             |
|total_edit_time      |60                            |
|create_time          |2021-12-13 12:30:00           |
|last_saved_time      |2021-12-13 12:31:00           |
|num_pages            |1                             |
|num_words            |0                             |
|num_chars            |0                             |
|creating_application |Microsoft Office Word         |
|security             |0                             |
+---------------------+------------------------------+
```

Last author is interesting, but is there more?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ olemeta blair.doc
```

```
[…]
+--------------------+------------------------------+
|codepage            |1252                          |
|title               |Iraq- ITS INFRASTRUCTURE OF   |
|                    |CONCEALMENT, DECEPTION AND    |
|                    |INTIMIDATION                  |
|subject             |                              |
|author              |default                       |
|keywords            |                              |
|comments            |                              |
|template            |Normal.dot                    |
|last_saved_by       |MKhan                         |
|revision_number     |4                             |
|total_edit_time     |180                           |
|last_printed        |2003-01-30 21:33:00           |
|create_time         |2003-02-03 09:31:00           |
|last_saved_time     |2003-02-03 11:18:00           |
|num_pages           |1                             |
|num_words           |3875                          |
|num_chars           |22090                         |
|creating_application|Microsoft Word 8.0            |
|security            |0                             |
+--------------------+------------------------------+
```

IRAQ – ITS INFRASTRUCTURE OF CONCEALMENT, DECEPTION AND INTIMIDATION

This report draws upon a number of sources, including intelligence material, and shows how the Iraqi regime is constructed to have, and to keep, WMD, and is now engaged in a campaign of obstruction of the United Nations Weapons Inspectors.

Part One focusses on how Iraq's security organisations operate to conceal Weapons of Mass Destruction from UN Inspectors. It reveals that the inspectors are outnumbered by Iraqi intelligence by a ratio of 200 to 1.

Part Two gives up to date details of Iraq's network of intelligence and security organisations whose job it is to keep Saddam and his regime in power, and to prevent the international community from disarming Iraq.

Part Three goes on to show the effects of the security apparatus on the ordinary people of Iraq.

While the reach of this network outside Iraq may be less apparent since the Gulf War of 1990/1991, inside Iraq, its grip is formidable over all levels of society. Saddam and his inner circle control the State infrastructure of fear.

January 2003

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

Microsoft Word bytes Tony Blair in the butt

Home > **Privacy** > **Blair's Iraq Dossier**

Richard M. Smith (rms@computerbytesman.com)
June 30, 2003

Microsoft Word documents are notorious for containing private information in file headers which people would sometimes rather not share. The British government of Tony Blair just learned this lesson the hard way.

Back in February 2003, 10 Downing Street published a dossier on Iraq's security and intelligence organizations. This dossier was cited by Colin Powell in his address to the United Nations the same month. Dr. Glen Rangwala, a lecturer in politics at Cambridge University, quickly discovered that much of the material in the dossier was actually plagiarized from a U.S. researcher on Iraq.

You can read Dr. Rangwala's original analysis of the dossier from Feb. 5, 2003 at this URL:

http://www.casi.org.uk/discuss/2003/msg00457.html

Blair's government made one additional mistake: they published the dossier as a Microsoft Word file on their Web site. When I first heard from Dr. Rangwala about the dossier, I decided to try to learn who had worked on the document. I downloaded the Word file containing the dossier from the 10 Downing Street Web site (http://www.number-10.gov.uk/) and found the following revision log in the file:

```
Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"

Most Word document files contain a revision log which is a listing of the last 10 edits of a document, showing the names of the people who worked with the document and the names of
the files that the document went under. Revision logs are hidden and cannot be viewed in Microsoft Word. However I wrote a small utility for extracting and displaying revision logs
and other hidden information in Word .DOC files.
```

https://dfir.com.br/wp-content/uploads/2014/02/blair.htm

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

Microsoft Word bytes Tony Blair in the butt

Home > Privacy > Blair's Iraq Dossier

Richard M. Smith (rms@computerbytesman.com)
June 30, 2003

Microsoft Word documents are notorious for containing private information in file headers which people would sometimes rather not share. The British government of Tony Blair just learned this lesson the hard way.

Back in February 2003, 10 Downing Street published a dossier on Iraq's security and intelligence organizations. This dossier was cited by Colin Powell in his address to the United Nations the same month. Dr. Glen Rangwala, a lecturer in politics at Cambridge University, quickly discovered that much of the material in the dossier was actually plagiarized from a U.S. researcher on Iraq.

You can read Dr. Rangwala's original analysis of the dossier from Feb. 5, 2003 at this URL:

http://www.casi.org.uk/discuss/2003/msg00457.html

Blair's government made one additional mistake: they published the dossier as a Microsoft Word file on their Web site. When I first heard from Dr. Rangwala about the dossier, I decided to try to learn who had worked on the document. I downloaded the Word file containing the dossier from the 10 Downing Street Web site (http://www.number-10.gov.uk/) and found the following revision log in the file:

```
Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd"
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"
```

Most Word document files contain a revision log which is a listing of the last 10 edits of a document, showing the names of the people who worked with the document and the names of the files that the document went under. Revision logs are hidden and cannot be viewed in Microsoft Word. However I wrote a small utility for extracting and displaying revision logs and other hidden information in Word .DOC files.

https://dfir.com.br/wp-content/uploads/2014/02/blair.htm

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

Microsoft Word bytes Tony Blair in the butt

Home > Privacy > Blair's Iraq Dossier

Richard M. Smith (rms@computerbytesman.com)
June 30, 2003

Microsoft Word documents are notorious for containing private information in file headers which people would sometimes rather not share. The British government of Tony Blair just learned this lesson the hard way.

Back in February 2003, 10 Downing Street published a dossier on Iraq's security and intelligence organizations. This dossier was cited by Colin Powell in his address to the United Nations the same month. Dr. Glen Rangwala, a lecturer in politics at Cambridge University, quickly discovered that much of the material in the dossier was actually plagiarized from a U.S. researcher on Iraq.

You can read Dr. Rangwala's original analysis of the dossier from Feb. 5, 2003 at this URL:

http://www.casi.org.uk/discuss/2003/msg00457.html

Blair's government made one additional mistake: they published the dossier as a Microsoft Word file on their Web site. When I ... angwala about the dossier, I decided to try to learn who had worked on the document. I downloaded the Word file containing the dossier from the 10 Downing Street Web site (http://www.number- ... following revision log in the file:

```
Rev. #1: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security
Rev. #2: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security
Rev. #3: "cic22" edited file "C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security
Rev. #4: "JPratt" edited file "C:\TEMP\Iraq - security.doc"
Rev. #5: "JPratt" edited file "A:\Iraq - security.doc"
Rev. #6: "ablackshaw" edited file "C:\ABlackshaw\Iraq - security.doc"
Rev. #7: "ablackshaw" edited file "C:\ABlackshaw\A;Iraq - security.doc"
Rev. #8: "ablackshaw" edited file "A:\Iraq - security.doc"
Rev. #9: "MKhan" edited file "C:\TEMP\Iraq - security.doc"
Rev. #10: "MKhan" edited file "C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc"
```

Most Word document files contain a revision log which is a listing of the last 10 edits of a documen... the files that the document went under. Revision logs are hidden and cannot be viewed in Microsoft W... and other hidden information in Word .DOC files.

https://dfir.com.br/wp-content/uploads/2014/02/blair.htm

- `.doc` files (or CFBF files) may still occur during an investigation
- Tools like `oletools` [1] and `oledump` [2] can be used for further analysis

[1] https://github.com/decalage2/oletools
[2] https://github.com/DidierStevens/DidierStevensSuite

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ file file3
file3: Microsoft Word 2007+
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

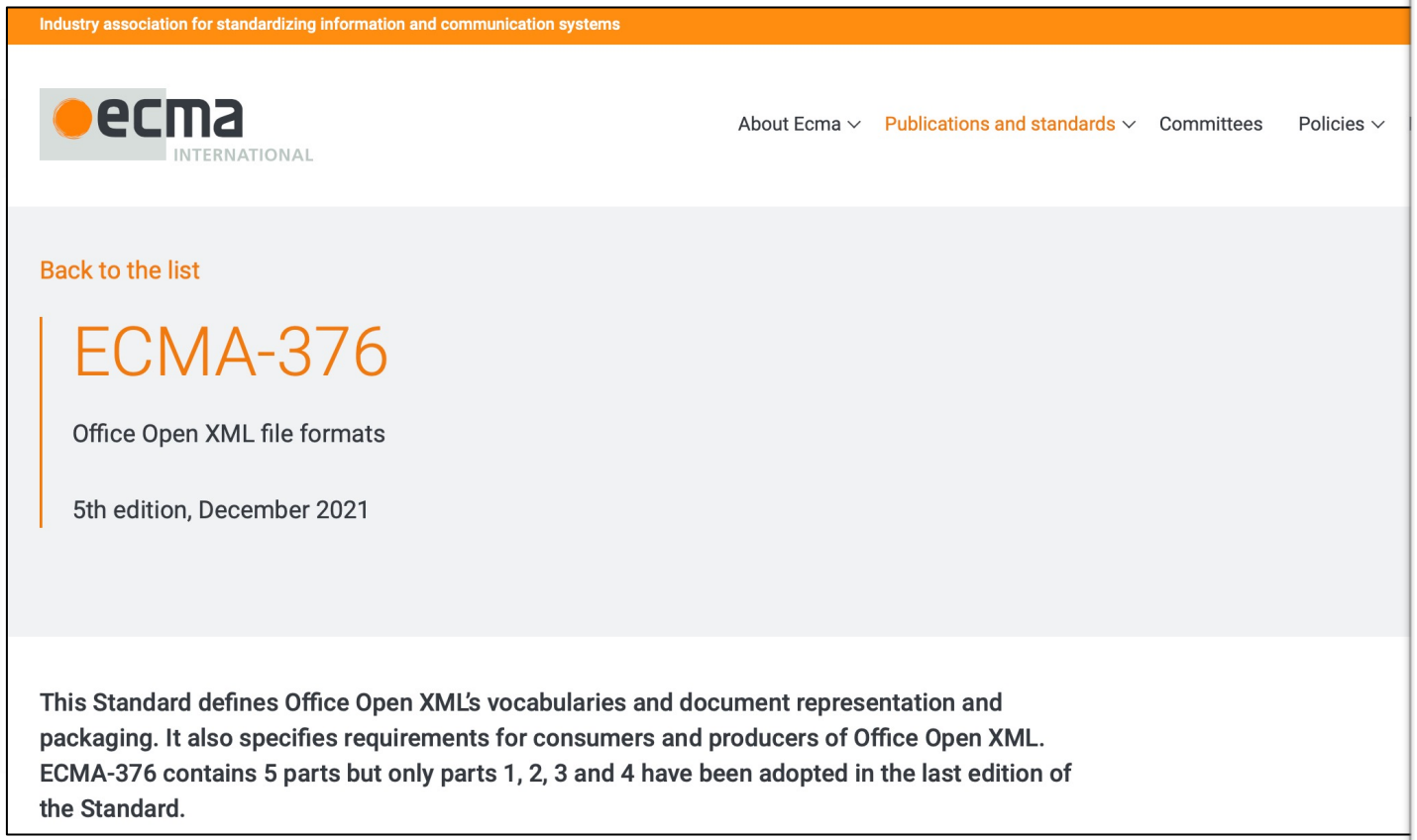
Office Documents

```
~$ exiftool file3
[…]
Zip Required Version           : 20
Zip Bit Flag                   : 0x0006
Zip Compression                : Deflated
Zip Modify Date                : 1980:01:01 00:00:00
Zip CRC                        : 0x6cd2a4df
Zip Compressed Size            : 346
Zip Uncompressed Size          : 1312
Zip File Name                  : [Content_Types].xml
[…]
```

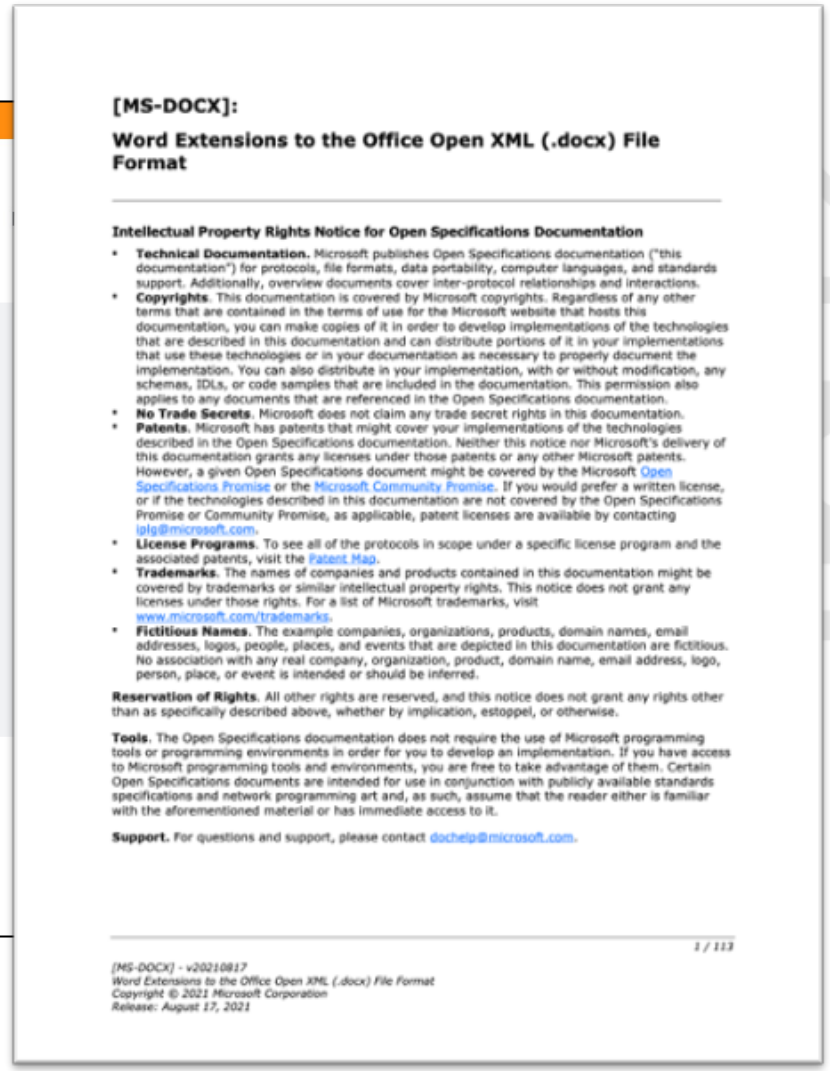
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents



https://www.ecma-international.org/publications-and-standards/standards/ecma-376/



https://docs.microsoft.com/en-us/openspecs/office_standards/ms-docx/

Office Documents

```
~$ unzip file3 -d file3
```

```
Archive:  file3
  inflating: file3/[Content_Types].xml
  inflating: file3/_rels/.rels
  inflating: file3/word/_rels/document.xml.rels
  inflating: file3/word/document.xml
  inflating: file3/word/theme/theme1.xml
  inflating: file3/word/settings.xml
  inflating: file3/docProps/core.xml
  inflating: file3/word/fontTable.xml
  inflating: file3/word/webSettings.xml
  inflating: file3/word/styles.xml
  inflating: file3/docProps/app.xml
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ tree file3
file3
├── [Content_Types].xml
├── _rels
├── docProps
│   ├── app.xml
│   └── core.xml
└── word
    ├── _rels
    │   └── document.xml.rels
    ├── document.xml
    ├── fontTable.xml
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    └── webSettings.xml

5 directories, 10 files
```

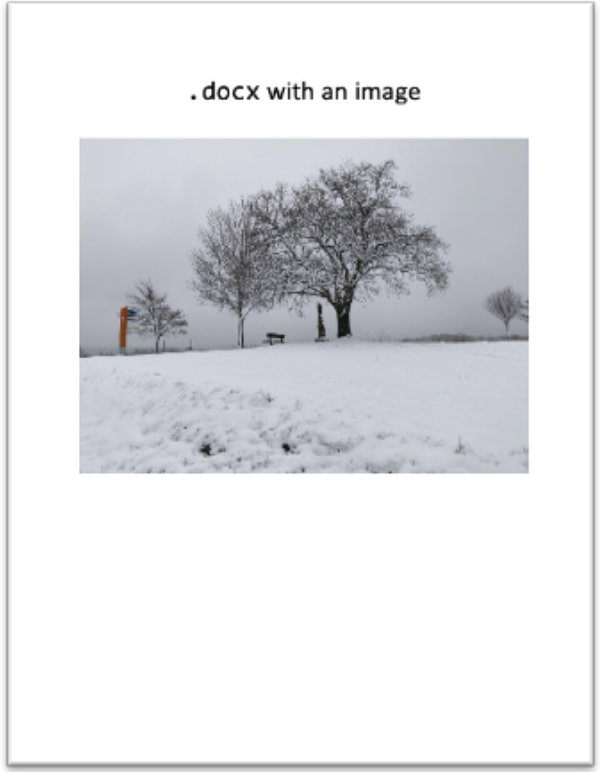
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ tree docx-with-image
docx-with-image
├── [Content_Types].xml
├── _rels
├── docProps
│   ├── app.xml
│   └── core.xml
└── word
    ├── _rels
    │   └── document.xml.rels
    ├── document.xml
    ├── fontTable.xml
    ├── media
    │   └── image1.jpeg
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    └── webSettings.xml

6 directories, 11 files
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ tree docx-with-image
docx-with-image
├── [Content_Types].xml
├── _rels
├── docProps
│   ├── app.xml
│   └── core.xml
└── word
    ├── _rels
    │   └── document.xml.rels
    ├── document.xml
    ├── fontTable.xml
    ├── media
    │   └── image1.jpeg
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    └── webSettings.xml

6 directories, 11 files
```

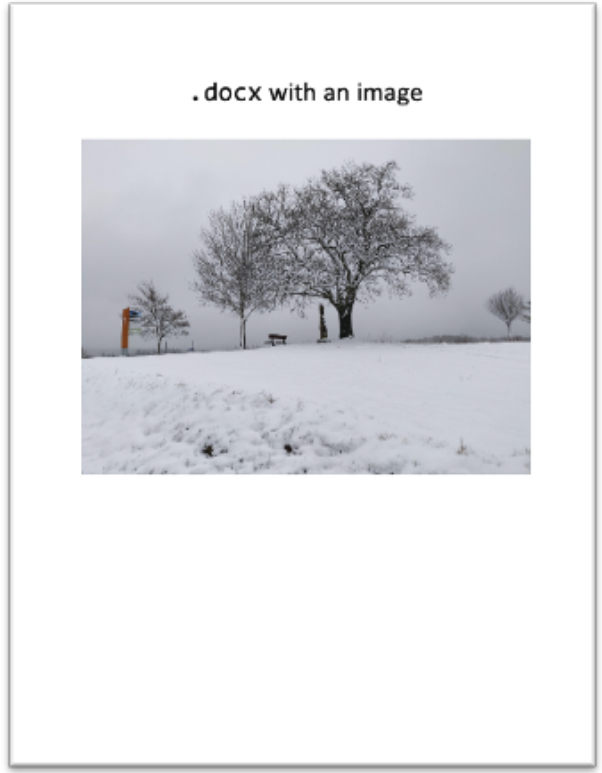
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ exiftool docx-with-image/word/media/image1.jpeg
ExifTool Version Number         : 12.16
File Name                       : image1.jpeg
Directory                       : word/media
File Size                       : 469 KiB
File Modification Date/Time     : 1980:01:01 00:00:00+01:00
File Access Date/Time           : 1980:01:01 00:00:00+01:00
File Inode Change Date/Time     : 2021:12:13 17:08:31+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 220
Y Resolution                    : 220
Resolution Unit                 : inches
Color Space                     : sRGB
Exif Image Width                : 1430
Exif Image Height               : 1072
Current IPTC Digest             : d41d8cd98f00b204e9800998ecf8427e
IPTC Digest                     : d41d8cd98f00b204e9800998ecf8427e
Image Width                     : 1430
Image Height                    : 1072
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1430x1072
Megapixels                      : 1.5
```

Original timestamps may be removed



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

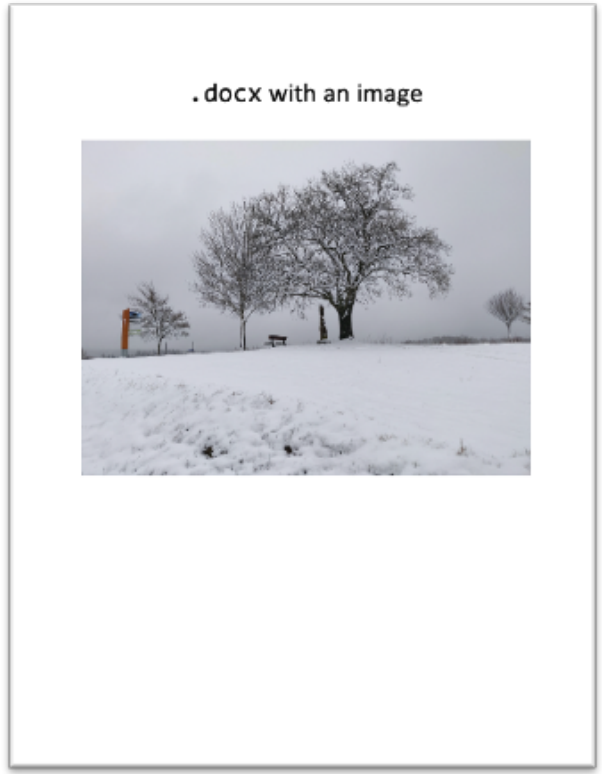
Office Documents

```
~$ exiftool docx-with-image/word/media/image1.jpeg
ExifTool Version Number         : 12.16
File Name                       : image1.jpeg
Directory                       : word/media
File Size                       : 469 KiB
File Modification Date/Time     : 1980:01:01 00:00:00+01:00
File Access Date/Time           : 1980:01:01 00:00:00+01:00
File Inode Change Date/Time     : 2021:12:13 17:08:31+01:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 220
Y Resolution                    : 220
Resolution Unit                 : inches
Color Space                     : sRGB
Exif Image Width                : 1430
Exif Image Height               : 1072
Current IPTC Digest             : d41d8cd98f00b204e9800998ecf8427e
IPTC Digest                     : d41d8cd98f00b204e9800998ecf8427e
Image Width                     : 1430
Image Height                    : 1072
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1430x1072
Megapixels                      : 1.5
```

Original timestamps may be removed

Timestamp of unzipping

All our metadata is gone ☹!



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

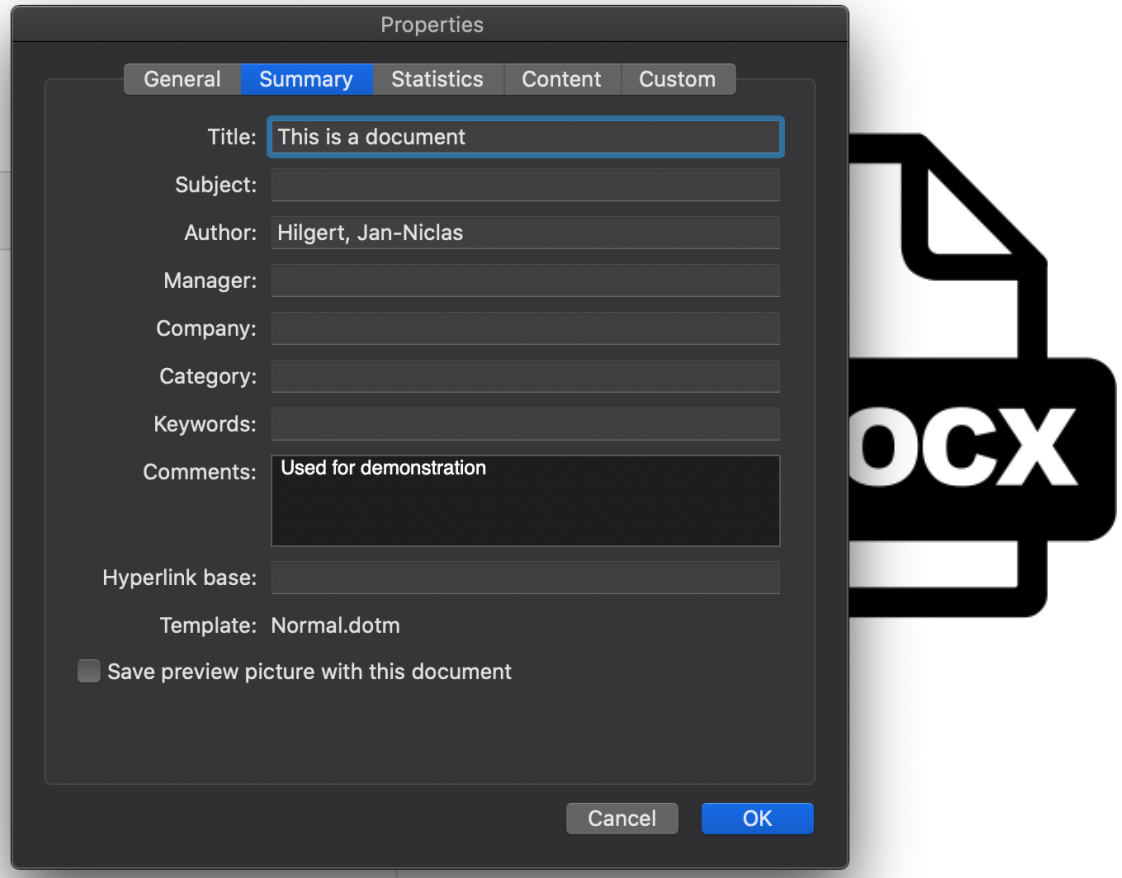
```
~$ exiftool file3
[…]
Title                           : This is a document
Subject                         :
Creator                         : Hilgert, Jan-Niclas
Keywords                        :
Description                     : Used for demonstration
Last Modified By                : Hilgert, Jan-Niclas
Revision Number                 : 4
Create Date                     : 2021:12:13 16:08:00Z
Modify Date                     : 2021:12:13 17:48:00Z
Template                        : Normal.dotm
Total Edit Time                 : 1 minute
Pages                           : 1
Words                           : 4
Characters                      : 16
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 3
Paragraphs                      : 1
Scale Crop                      : No
Company                         :
Links Up To Date                : No
Characters With Spaces          : 8
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ exiftool file3
[…]
Title                           : This is a document
Subject                         :
Creator                         : Hilgert, Jan-Niclas
Keywords                        :
Description                     : Used for demonstration
Last Modified By                : Hilgert, Jan-Niclas
Revision Number                 : 4
Create Date                     : 2021:12:13 16:08:00Z
Modify Date                     : 2021:12:13 17:48:00Z
Template                        : Normal.dotm
Total Edit Time                 : 1 minute
Pages                           : 1
Words                           : 4
Characters                      : 16
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 3
Paragraphs                      : 1
Scale Crop                      : No
Company                         :
Links Up To Date                : No
Characters With Spaces          : 8
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```

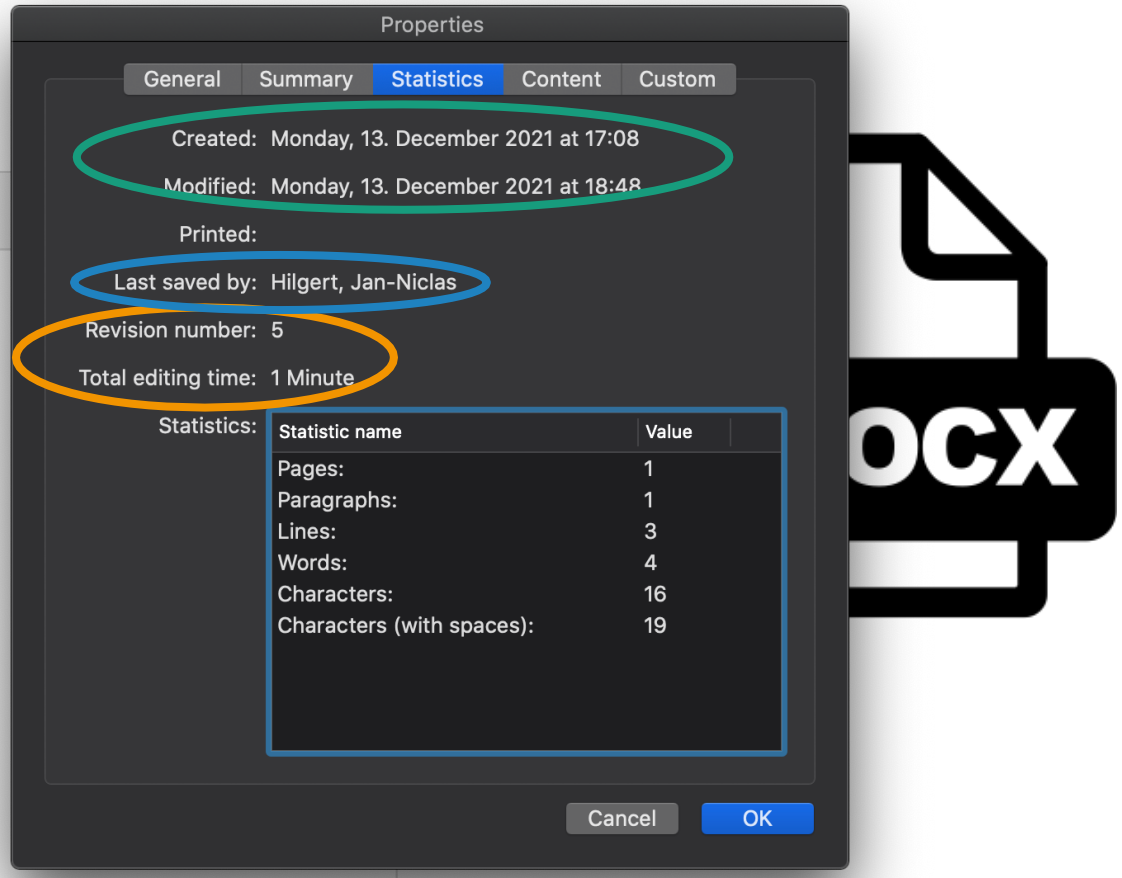


Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ exiftool file3
[…]
Title                           : This is a document
Subject                         :
Creator                         : Hilgert, Jan-Niclas
Keywords                        :
Description                     : Used for demonstration
Last Modified By                : Hilgert, Jan-Niclas
Revision Number                 : 4
Create Date                     : 2021:12:13 16:08:00Z
Modify Date                     : 2021:12:13 17:48:00Z
Template                        : Normal.dotm
Total Edit Time                 : 1 minute
Pages                           : 1
Words                           : 4
Characters                      : 16
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 3
Paragraphs                      : 1
Scale Crop                      : No
Company                         :
Links Up To Date                : No
Characters With Spaces          : 8
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ exiftool file3
[…]
Title                           : This is a document
Subject                         :
Creator                         : Hilgert, Jan-Niclas
Keywords                        :
Description                     : Used for demonstration
Last Modified By                : Hilgert, Jan-Niclas
Revision Number                 : 4
Create Date                     : 2021:12:13 16:08:00Z
Modify Date                     : 2021:12:13 17:48:00Z
Template                        : Normal.dotm
Total Edit Time                 : 1 minute
Pages                           : 1
Words                           : 4
Characters                      : 16
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 3
Paragraphs                      : 1
Scale Crop                      : No
Company                         :
Links Up To Date                : No
Characters With Spaces          : 8
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ cat file3/docProps/core.xml
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties"
xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/"
xmlns:dcmitype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"><dc:title>This is a document</dc:title><dc:subject></dc:subject><dc:creator>Hilgert, Jan-
Niclas</dc:creator><cp:keywords></cp:keywords><dc:description>Used for
demonstration</dc:description><cp:lastModifiedBy>Hilgert, Jan-
Niclas</cp:lastModifiedBy><cp:revision>6</cp:revision><dcterms:created xsi:type="dcterms:W3CDTF">2021-
12-13T16:08:00Z</dcterms:created><dcterms:modified xsi:type="dcterms:W3CDTF">2021-12-
13T17:48:00Z</dcterms:modified><cp:category></cp:category></cp:coreProperties>
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ oleid file3
```

```
oleid 0.60.dev1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: file3
```

Indicator	Value	Risk	Description
File format	MS Word 2007+ Document (.docx)	info	
Container format	OpenXML	info	Container type
Encrypted	False	none	The file is not encrypted
VBA Macros	No	none	This file does not contain VBA macros.
XLM Macros	No	none	This file does not contain Excel 4/XLM macros.
External Relationships	0	none	External relationships such as remote templates, remote OLE objects, etc

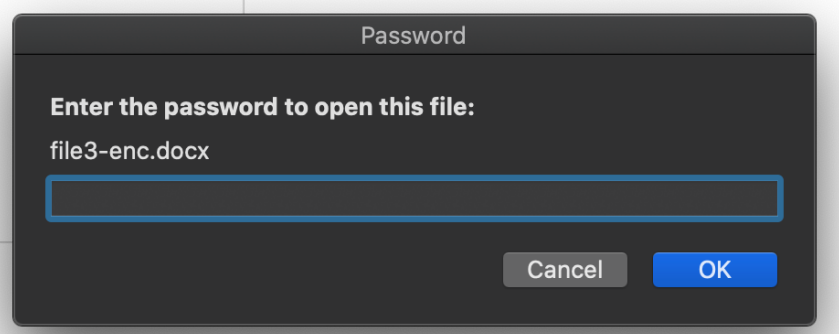
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ oleid file3-enc.docx
oleid 0.60.dev1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: file3-enc.docx
+--------------------+--------------------+----------+--------------------------
|Indicator           |Value               |Risk      |Description
+--------------------+--------------------+----------+--------------------------
|File format         |Generic OLE file /  |info      |Unrecognized OLE file.
|                    |Compound File.      |          |Root CLSID:  - None
|                    |(unknown format)    |          |
+--------------------+--------------------+----------+--------------------------
|Container format    |OLE                 |info      |Container type
+--------------------+--------------------+----------+--------------------------
|Encrypted           |True                |low       |The file is encrypted. It
|                    |                    |          |may be decrypted with
|                    |                    |          |msoffcrypto-tool
+--------------------+--------------------+----------+--------------------------
[…]
```



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ exiftool file3-enc.docx
```

```
ExifTool Version Number         : 12.16
File Name                       : file3-enc.docx
Directory                       : .
File Size                       : 494 KiB
File Modification Date/Time     : 2021:12:14 03:13:26+01:00
File Access Date/Time           : 2021:12:14 03:13:26+01:00
File Inode Change Date/Time     : 2021:12:14 03:13:26+01:00
File Permissions                : rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-
officedocument.wordprocessingml.document
```


```
~$ file file3-enc.docx
```

```
file3-enc.docx: CDFV2 Encrypted
```

No metadata accessible after encryption is enabled

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Office Documents

```
~$ oleid malicious.doc
```

```
oleid 0.60.dev1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: malicious.doc
+--------------------+--------------------+----------+--------------------------
|Indicator           |Value               |Risk      |Description
+--------------------+--------------------+----------+--------------------------
|File format         |MS Word 2007+ Macro |info      |
|                    |Enabled-Document    |          |
|                    |(.docm)             |          |
+--------------------+--------------------+----------+--------------------------
|Container format    |OpenXML             |info      |Container type
+--------------------+--------------------+----------+--------------------------
|Encrypted           |False               |none      |The file is not encrypted
+--------------------+--------------------+----------+--------------------------
|VBA Macros          |Yes, suspicious     |HIGH      |This file contains VBA
|                    |                    |          |macros. Suspicious
|                    |                    |          |keywords were found. Use
|                    |                    |          |olevba and mraptor for
|                    |                    |          |more info.
+--------------------+--------------------+----------+--------------------------
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

file4

file5

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

```
~$ file file4
```

file4

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

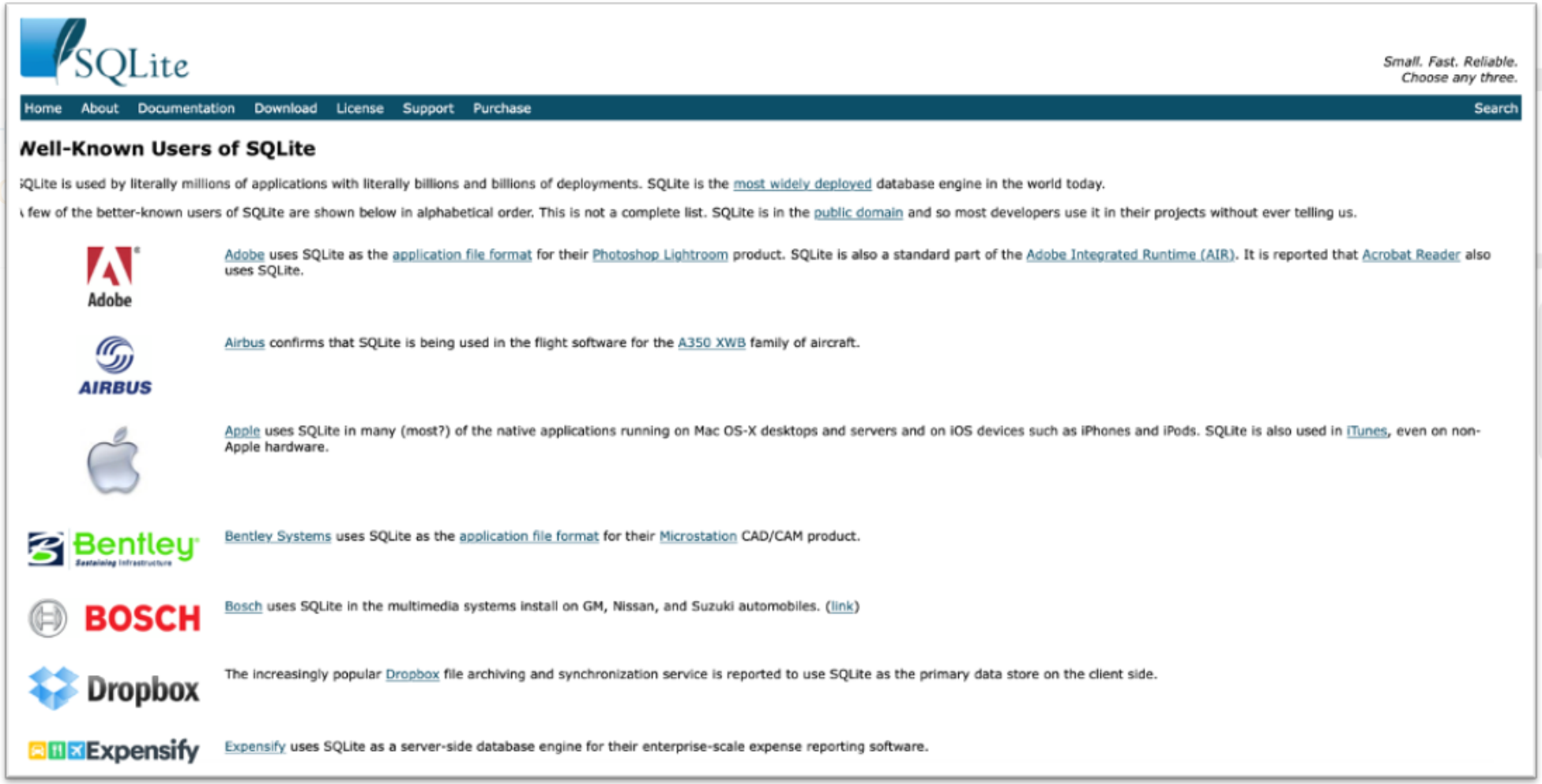
SQLite

```
~$ file file4
file4: SQLite 3.x database, last written using SQLite version 3020001
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite



SQLite

Small. Fast. Reliable. Choose any three.

Home About Documentation Download License Support Purchase Search

Well-Known Users of SQLite

SQLite is used by literally millions of applications with literally billions and billions of deployments. SQLite is the most widely deployed database engine in the world today.

A few of the better-known users of SQLite are shown below in alphabetical order. This is not a complete list. SQLite is in the public domain and so most developers use it in their projects without ever telling us.

Adobe

Adobe uses SQLite as the application file format for their Photoshop Lightroom product. SQLite is also a standard part of the Adobe Integrated Runtime (AIR). It is reported that Acrobat Reader also uses SQLite.

AIRBUS

Airbus confirms that SQLite is being used in the flight software for the A350 XWB family of aircraft.

Apple uses SQLite in many (most?) of the native applications running on Mac OS-X desktops and servers and on iOS devices such as iPhones and iPods. SQLite is also used in iTunes, even on non-Apple hardware.

Bentley

Bentley Systems uses SQLite as the application file format for their Microstation CAD/CAM product.

BOSCH

Bosch uses SQLite in the multimedia systems install on GM, Nissan, and Suzuki automobiles. (link)

Dropbox

The increasingly popular Dropbox file archiving and synchronization service is reported to use SQLite as the primary data store on the client side.

Expensify

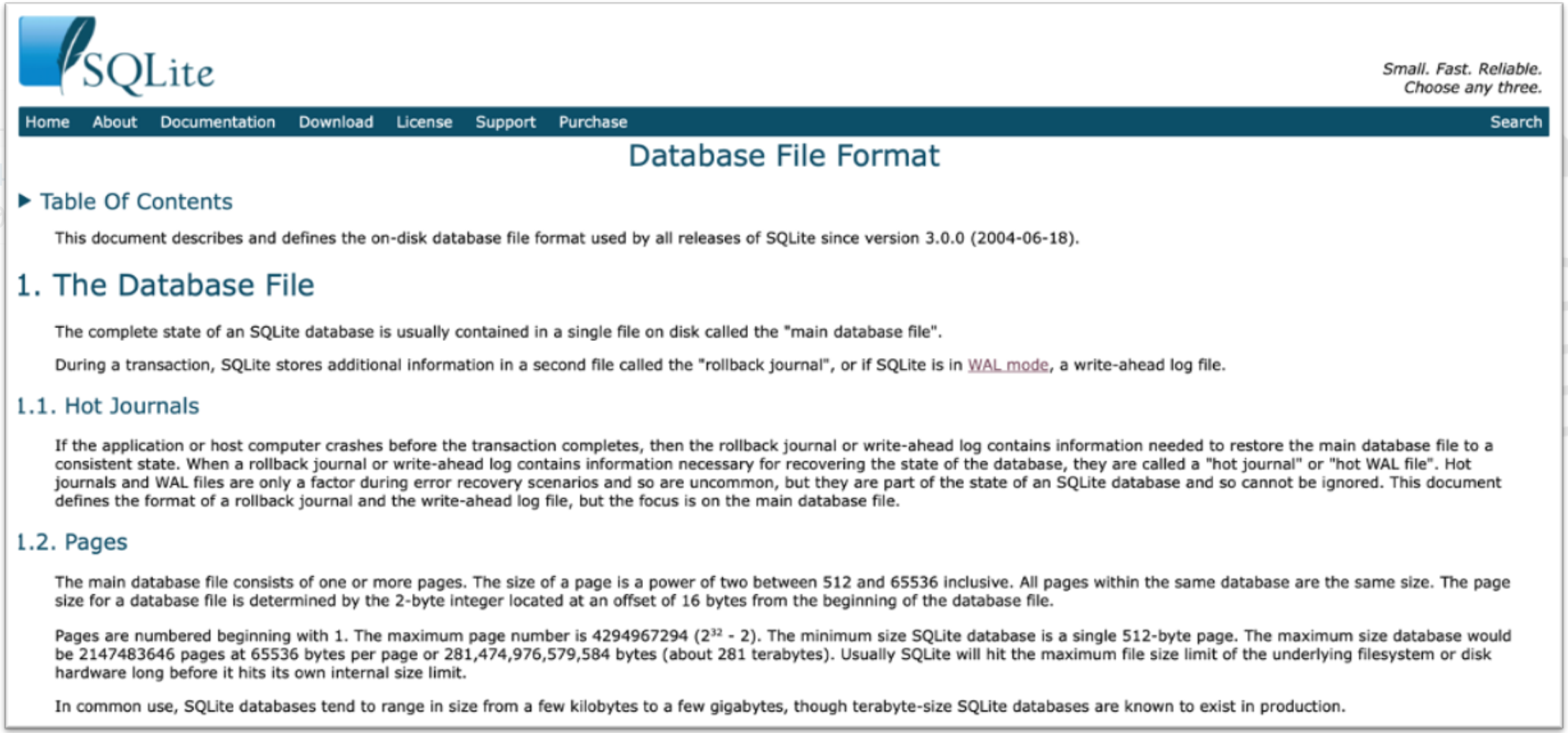
Expensify uses SQLite as a server-side database engine for their enterprise-scale expense reporting software.

https://www.sqlite.org/famous.html

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite



SQLite

Small. Fast. Reliable. Choose any three.

Home About Documentation Download License Support Purchase Search

Database File Format

▶ Table Of Contents

This document describes and defines the on-disk database file format used by all releases of SQLite since version 3.0.0 (2004-06-18).

1. The Database File

The complete state of an SQLite database is usually contained in a single file on disk called the "main database file".

During a transaction, SQLite stores additional information in a second file called the "rollback journal", or if SQLite is in WAL mode, a write-ahead log file.

1.1. Hot Journals

If the application or host computer crashes before the transaction completes, then the rollback journal or write-ahead log contains information needed to restore the main database file to a consistent state. When a rollback journal or write-ahead log contains information necessary for recovering the state of the database, they are called a "hot journal" or "hot WAL file". Hot journals and WAL files are only a factor during error recovery scenarios and so are uncommon, but they are part of the state of an SQLite database and so cannot be ignored. This document defines the format of a rollback journal and the write-ahead log file, but the focus is on the main database file.

1.2. Pages

The main database file consists of one or more pages. The size of a page is a power of two between 512 and 65536 inclusive. All pages within the same database are the same size. The page size for a database file is determined by the 2-byte integer located at an offset of 16 bytes from the beginning of the database file.

Pages are numbered beginning with 1. The maximum page number is 4294967294 (2^{32} - 2). The minimum size SQLite database is a single 512-byte page. The maximum size database would be 2147483646 pages at 65536 bytes per page or 281,474,976,579,584 bytes (about 281 terabytes). Usually SQLite will hit the maximum file size limit of the underlying filesystem or disk hardware long before it hits its own internal size limit.

In common use, SQLite databases tend to range in size from a few kilobytes to a few gigabytes, though terabyte-size SQLite databases are known to exist in production.

https://www.sqlite.org/fileformat.html

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ sqlite3 file4
SQLite version 3.28.0 2019-04-15 14:49:49
Enter ".help" for usage hints.
sqlite>
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ sqlite3 file4
SQLite version 3.28.0 2019-04-15 14:49:49
Enter ".help" for usage hints.
sqlite> .tables
audio_data
available_message_view
away_messages
call_log
call_log_participant_v2
chat
chat_view
conversion_tuples
deleted_chat_job
deleted_messages_ids_view
deleted_messages_view
frequent
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ sqlite3 file4
SQLite version 3.28.0 2019-04-15 14:49:49
Enter ".help" for usage hints.
sqlite> select * from messages;
1|-1|0|-1|-1|0||0|||-1|-1||||0|0|0.0|0.0|||-1|-1|-1|-1|||||||0|||0|||||||
1001|MessageFromToday@s.whatsapp.net|0|keyId-0001-001|0|0|This message has been
sent yesterday|1639063015000|||0|0||||0|1|0.0|0.0|||1639063015000|-1|-1|-
1|||||||0|||0|||||||
1002|MessageFromToday@s.whatsapp.net|0|keyId-0001-002|0|0|This message has been
sent today|1639149415000|||0|0||||0|1|0.0|0.0|||1639149415000|-1|-1|-
1|||||||0|||0|||||||
2001|0-Text@s.whatsapp.net|0|keyId-0002-001|0|0|Hey was
geht?|1420034400000|||0|0||||0|1|0.0|0.0|||1420034400000|-1|-1|-
1|||||||0|||0|||||||
2002|0-Text@s.whatsapp.net|1|keyId-0002-002|0|0|Disdas
diggi|1420034500000|||0|0||||0|1|0.0|0.0|||1420034500000|-1|-1|-
1|||||||0|||0|||||||
2003|0-Text@s.whatsapp.net|0|keyId-0002-003|0|0|Wollen wir uns
treffen?|1420034600000|||0|0||||0|1|0.0|0.0|||1420034600000|-1|-1|-
1|||||||0|||0|||||||
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ sqlite3 file4
SQLite version 3.28.0 2019-04-15 14:49:49
Enter ".help" for usage hints.
sqlite> select * from messages;
1|-1|0|-1|-1|0||0|||-1|-1||||0|0|0.0|0.0|||-1|-1|-1|-1|||||||0|||0|||||||
1001|MessageFromToday@s.whatsapp.net|0|keyId-0001-001|0|0|This message has been
sent yesterday|1639063015000|||0|0||||0|1|0.0|0.0|||1639063015000|-1|-1|-
1|||||||0|||0|||||||
1002|MessageFromToday@s.whatsapp.net|0|keyId-0001-002|0|0|This message has been
sent today|1639149415000|||0|0||||0|1|0.0|0.0|||1639149415000|-1|-1|-
1|||||||0|||0|||||||
2001|0-Text@s.whatsapp.net|0|keyId-0002-001|0|0|Hey was
geht?|1420034400000|||0|0||||0|1|0.0|0.0|||1420034400000|-1|-1|-
1|||||||0|||0|||||||
2002|0-Text@s.whatsapp.net|1|keyId-0002-002|0|0|Disdas
diggi|1420034500000|||0|0||||0|1|0.0|0.0|||1420034500000|-1|-1|-
1|||||||0|||0|||||||
2003|0-Text@s.whatsapp.net|0|keyId-0002-003|0|0|Wollen wir uns
treffen?|1420034600000|||0|0||||0|1|0.0|0.0|||1420034600000|-1|-1|-
1|||||||0|||0|||||||
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ sqlite3 file4
```

```
SQLite version 3.28.0 2019-04-15 14:49:49
Enter ".help" for usage hints.
sqlite> .headers on
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ sqlite3 file4
SQLite version 3.28.0 2019-04-15 14:49:49
Enter ".help" for usage hints.
sqlite> select * from messages;
_id|key_remote_jid|key_from_me|key_id|status|needs_push|data|timestamp|media_url
|media_mime_type|media_wa_type|media_size|media_name|media_caption|media_hash|me
dia_duration|origin|latitude|longitude|thumb_image|remote_resource|received_time
stamp|send_timestamp|receipt_server_timestamp|receipt_device_timestamp|read_devi
ce_timestamp|played_device_timestamp|raw_data|recipient_count|participant_hash|s
tarred|quoted_row_id|mentioned_jids|multicast_id|edit_version|media_enc_hash|pay
ment_transaction_id|forwarded|preview_type|send_count|lookup_tables|future_messa
ge_type
1|-1|0|-1|-1|0||0|||-1|-1||||0|0|0.0|0.0|||-1|-1|-1|-1|||||||0|||0|||||||
1001|MessageFromToday@s.whatsapp.net|0|keyId-0001-001|0|0|This message has been
sent yesterday|1639063015000|||0|0||||0|1|0.0|0.0|||1639063015000|-1|-1|-
1|||||||0|||0|||||||
1002|MessageFromToday@s.whatsapp.net|0|keyId-0001-002|0|0|This message has been
sent today|1639149415000|||0|0||||0|1|0.0|0.0|||1639149415000|-1|-1|-
1|||||||0|||0|||||||
[…]
```

That's pretty hard to read…

SQLite

DB Browser for SQLite - /private/tmp/file4

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Create Table | Create Index | Print

Name	Type	Schema
Tables (137)		
audio_data		CREATE TABLE audio_data (message_row_id INTEGER PRIMARY KEY, waveform BLOB)
away_messages		CREATE TABLE away_messages (_id INTEGER PRIMARY KEY AUTOINCREMENT, jid TEXT UNIQUE NOT NULL)
call_log		CREATE TABLE call_log (_id INTEGER PRIMARY KEY AUTOINCREMENT, jid_row_id INTEGER, from_me INTEGER, call_id TEXT,
call_log_participant_v2		CREATE TABLE call_log_participant_v2 (_id INTEGER PRIMARY KEY AUTOINCREMENT, call_log_row_id INTEGER, jid_row_id IN
chat		CREATE TABLE chat (_id INTEGER PRIMARY KEY AUTOINCREMENT,jid_row_id INTEGER UNIQUE,hidden INTEGER,subject TE
conversion_tuples		CREATE TABLE conversion_tuples (jid_row_id INTEGER PRIMARY KEY, data TEXT, source TEXT, biz_count INTEGER, has_user_
deleted_chat_job		CREATE TABLE deleted_chat_job (_id INTEGER PRIMARY KEY AUTOINCREMENT, chat_row_id INTEGER NOT NULL, block_size
frequent		CREATE TABLE frequent (_id INTEGER PRIMARY KEY AUTOINCREMENT, jid_row_id INTEGER NOT NULL, type INTEGER NOT I
frequents		CREATE TABLE frequents (_id INTEGER PRIMARY KEY AUTOINCREMENT, jid TEXT NOT NULL, type INTEGER NOT NULL, mes
group_notification_version		CREATE TABLE group_notification_version (group_jid_row_id INTEGER PRIMARY KEY, subject_timestamp INTEGER NOT NULL,
group_participant_device		CREATE TABLE group_participant_device (_id INTEGER PRIMARY KEY AUTOINCREMENT, group_participant_row_id INTEGER I
group_participant_user		CREATE TABLE group_participant_user (_id INTEGER PRIMARY KEY AUTOINCREMENT, group_jid_row_id INTEGER NOT NULL
group_participants		CREATE TABLE group_participants (_id INTEGER PRIMARY KEY AUTOINCREMENT, gjid TEXT NOT NULL, jid TEXT NOT NULL
group_participants_history		CREATE TABLE group_participants_history (_id INTEGER PRIMARY KEY AUTOINCREMENT, timestamp DATETIME NOT NULL,
invoice_transactions		CREATE TABLE invoice_transactions (message_row_id INTEGER PRIMARY KEY,pay_transaction_id INTEGER)
jid		CREATE TABLE jid (_id INTEGER PRIMARY KEY AUTOINCREMENT, user TEXT NOT NULL, server TEXT NOT NULL, agent INTE
joinable_call_log		CREATE TABLE joinable_call_log (call_log_row_id INTEGER PRIMARY KEY,call_id TEXT NOT NULL,joinable_video_call INTEGER
keywords		CREATE TABLE keywords (_id INTEGER PRIMARY KEY AUTOINCREMENT, keyword TEXT UNIQUE NOT NULL)
labeled_jid		CREATE TABLE labeled_jid (_id INTEGER PRIMARY KEY AUTOINCREMENT, label_id INTEGER NOT NULL, jid_row_id INTEGER
labeled_jids		CREATE TABLE labeled_jids (_id INTEGER PRIMARY KEY AUTOINCREMENT, label_id INTEGER NOT NULL, jid TEXT)
labeled_messages		CREATE TABLE labeled_messages(_id INTEGER PRIMARY KEY AUTOINCREMENT,label_id INTEGER NOT NULL,message_row_
labeled_messages_fts		CREATE VIRTUAL TABLE labeled_messages_fts USING FTS3()
labeled_messages_fts_content		CREATE TABLE 'labeled_messages_fts_content'(docid INTEGER PRIMARY KEY, 'c0content')
labeled_messages_fts_segdir		CREATE TABLE 'labeled_messages_fts_segdir'(level INTEGER,idx INTEGER,start_block INTEGER,leaves_end_block INTEGER,er

UTF-8

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

Database to SQL file...
Table(s) as CSV file...
Table to JSON...

DB Browser for SQLite - /private/tmp/file4

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages

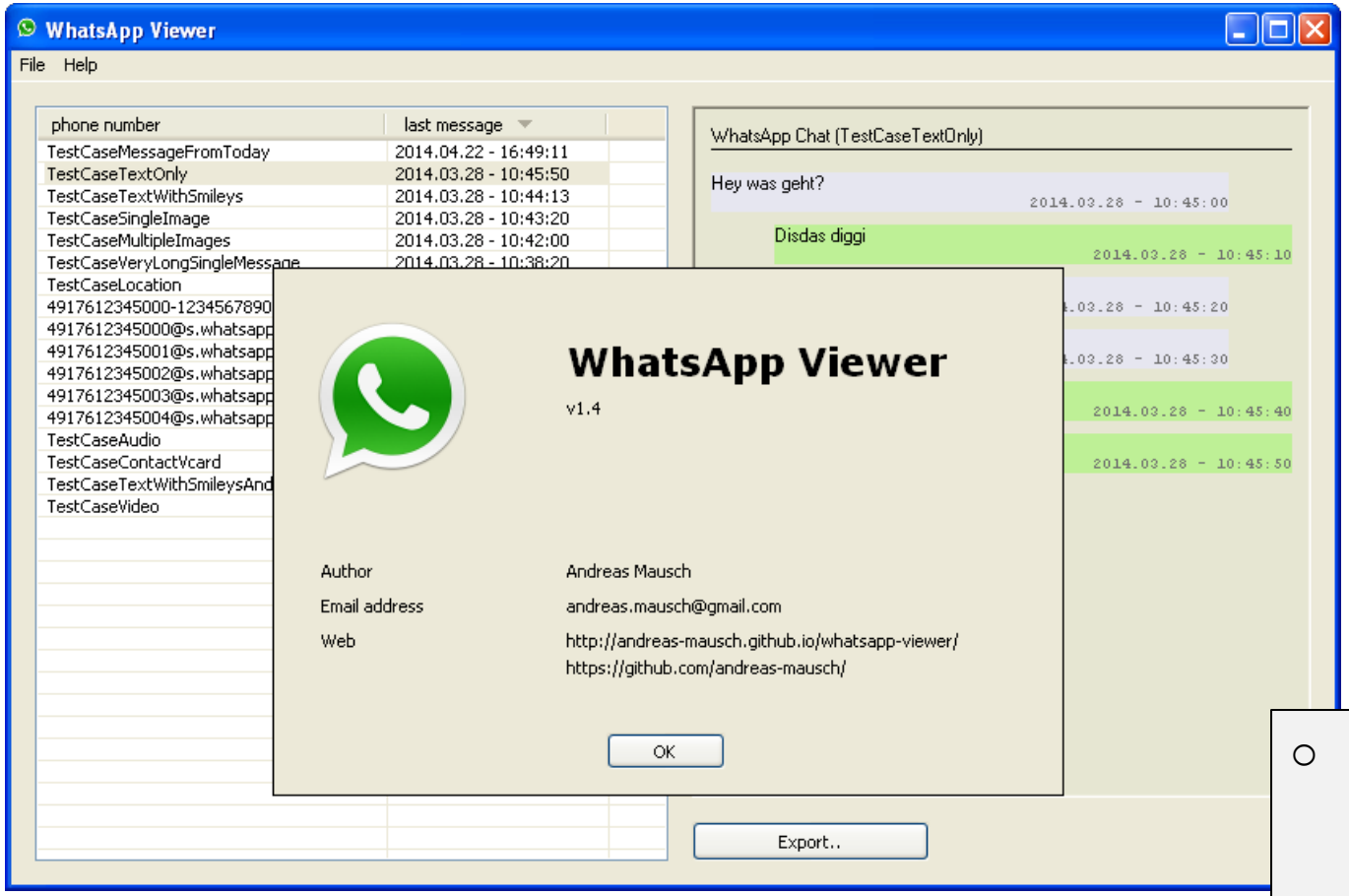
Filter in any column

	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timestamp	me
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	-1	0	-1	-1	0	NULL	0	NULL
2	1001	MessageFromToday@s.whatsapp.net	0	keyId-0001-001	0	0	This message has been sent yesterday	1639063015000	NULL
3	1002	MessageFromToday@s.whatsapp.net	0	keyId-0001-002	0	0	This message has been sent today	1639149415000	NULL
4	2001	0-Text@s.whatsapp.net	0	keyId-0002-001	0	0	Hey was geht?	1420034400000	NULL
5	2002	0-Text@s.whatsapp.net	1	keyId-0002-002	0	0	Disdas diggi	1420034500000	NULL
6	2003	0-Text@s.whatsapp.net	0	keyId-0002-003	0	0	Wollen wir uns treffen?	1420034600000	NULL
7	2004	0-Text@s.whatsapp.net	0	keyId-0002-004	0	0	So gegen 15:30 Uhr?	1420034700000	NULL
8	2005	0-Text@s.whatsapp.net	1	keyId-0002-005	0	0	OK. Wo denn?	1420034800000	NULL
9	2006	0-Text@s.whatsapp.net	1	keyId-0002-006	0	0	?	1420034900000	NULL
10	3001	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-001	0	0	Kiss: □	1419948000000	NULL
11	3002	0-Text-WithSmileys@s.whatsapp.net	1	keyId-0003-002	0	0	Thumb up: □	1419948100000	NULL
12	3003	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-003	0	0	Big smile: □	1419948200000	NULL
13	3004	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-004	0	0	UTF SMILING FACE WITH OPEN MOUTH 1F603: 😃	1419948300000	NULL
14	3005	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-005	0	0	Male: □; Female: □; House: □; long long text until next …	1419948400000	NULL
15	3006	0-Text-WithSmileys@s.whatsapp.net	1	keyId-0003-006	0	0	Smiley mix: …	1419948500000	NULL
16	4001	0-Text-Long@s.whatsapp.net	0	keyId-0004-001	0	0	💞Handbook 2013💞…	1419861600000	NULL
17	5001	0-Text-InvalidUTF8@s.whatsapp.net	0	keyId-0005-001	0	0	BLOB	1419775200000	NULL
18	6001	0-Quote@s.whatsapp.net	0	keyId-0006-001	0	0	Text of first user	1419688800000	NULL
19	6002	0-Quote@s.whatsapp.net	1	keyId-0006-002	0	0	I've quoted you	1419688900000	NULL

1 - 19 of 43 | Go to: 1

UTF-8

SQLite



https://andreas-mausch.de/whatsapp-viewer/

- In some cases there may already be tools to parse, interpret and visualize databases of an application
- In other cases there aren't

SQLite

SQLite Database

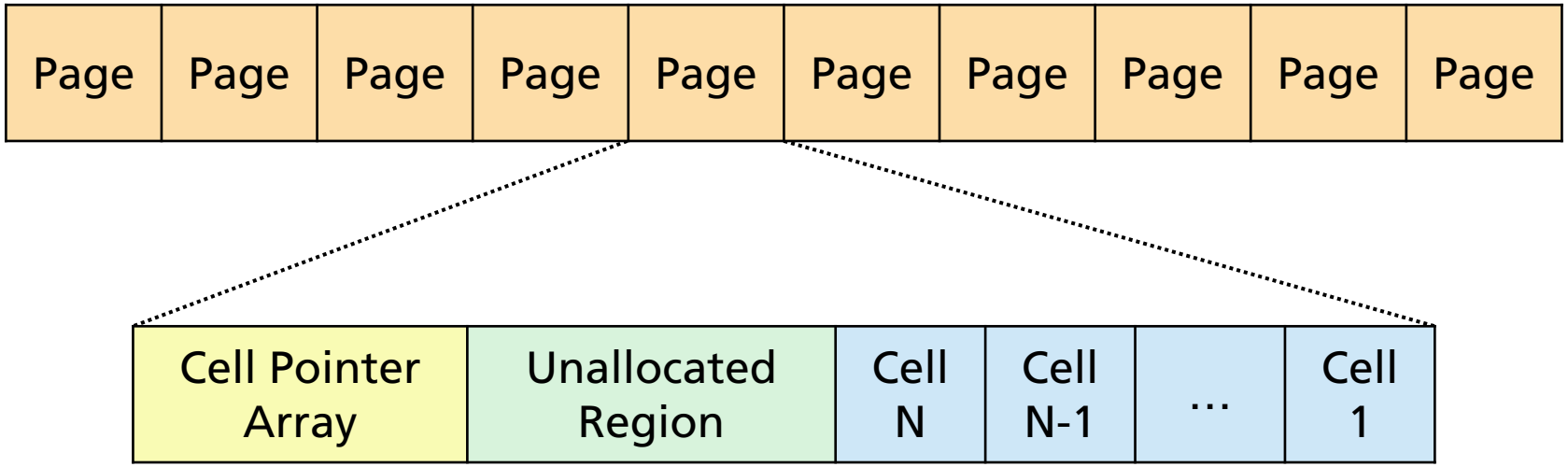
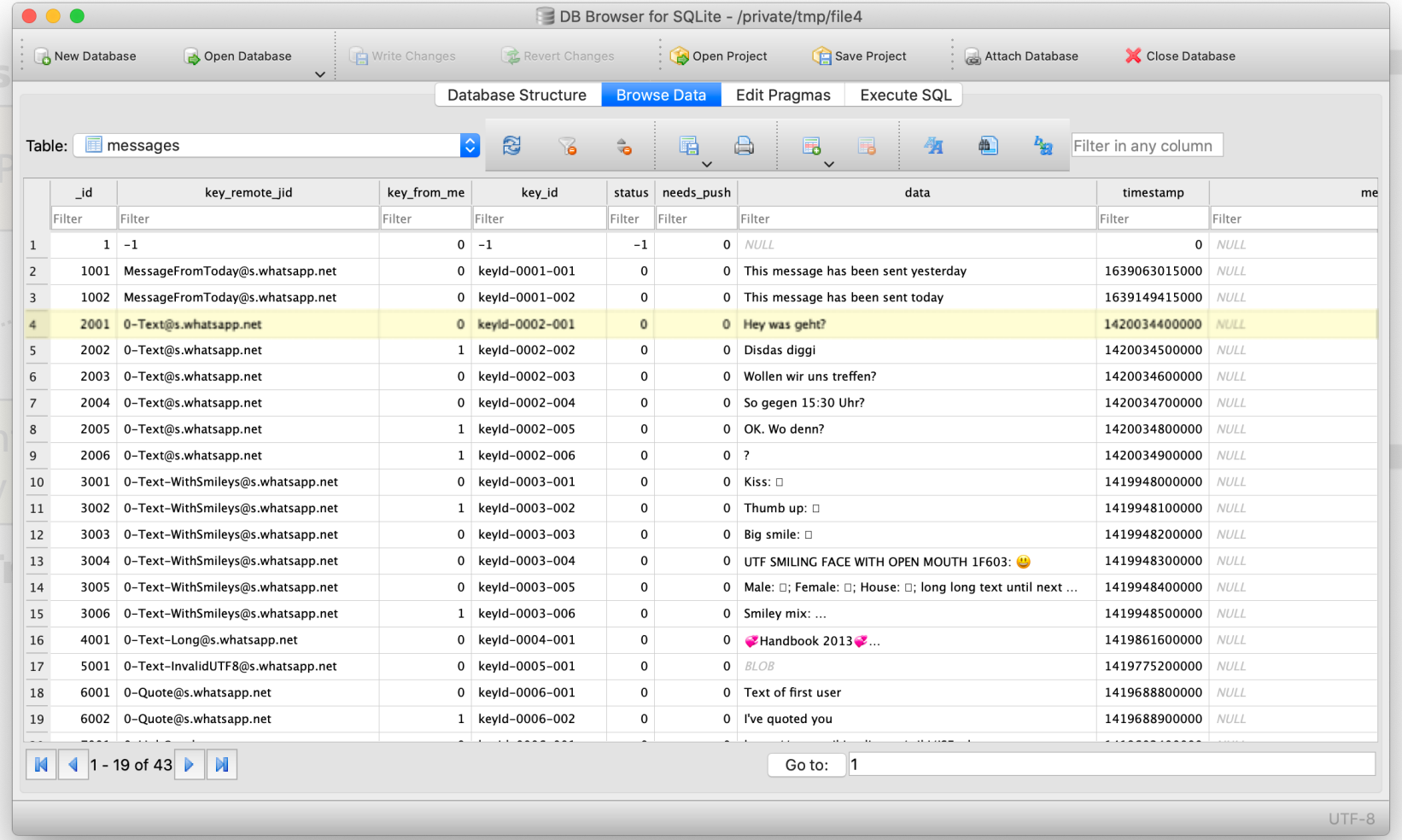


Table B-Tree Leaf Cell

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite



	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timestamp	me
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	-1	0	-1	-1	0	NULL	0	NULL
2	1001	MessageFromToday@s.whatsapp.net	0	keyId-0001-001	0	0	This message has been sent yesterday	1639063015000	NULL
3	1002	MessageFromToday@s.whatsapp.net	0	keyId-0001-002	0	0	This message has been sent today	1639149415000	NULL
4	2001	0-Text@s.whatsapp.net	0	keyId-0002-001	0	0	Hey was geht?	1420034400000	NULL
5	2002	0-Text@s.whatsapp.net	1	keyId-0002-002	0	0	Disdas diggi	1420034500000	NULL
6	2003	0-Text@s.whatsapp.net	0	keyId-0002-003	0	0	Wollen wir uns treffen?	1420034600000	NULL
7	2004	0-Text@s.whatsapp.net	0	keyId-0002-004	0	0	So gegen 15:30 Uhr?	1420034700000	NULL
8	2005	0-Text@s.whatsapp.net	1	keyId-0002-005	0	0	OK. Wo denn?	1420034800000	NULL
9	2006	0-Text@s.whatsapp.net	1	keyId-0002-006	0	0	?	1420034900000	NULL
10	3001	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-001	0	0	Kiss: □	1419948000000	NULL
11	3002	0-Text-WithSmileys@s.whatsapp.net	1	keyId-0003-002	0	0	Thumb up: □	1419948100000	NULL
12	3003	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-003	0	0	Big smile: □	1419948200000	NULL
13	3004	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-004	0	0	UTF SMILING FACE WITH OPEN MOUTH 1F603: 😃	1419948300000	NULL
14	3005	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-005	0	0	Male: □; Female: □; House: □; long long text until next …	1419948400000	NULL
15	3006	0-Text-WithSmileys@s.whatsapp.net	1	keyId-0003-006	0	0	Smiley mix: …	1419948500000	NULL
16	4001	0-Text-Long@s.whatsapp.net	0	keyId-0004-001	0	0	💞Handbook 2013💞…	1419861600000	NULL
17	5001	0-Text-InvalidUTF8@s.whatsapp.net	0	keyId-0005-001	0	0	BLOB	1419775200000	NULL
18	6001	0-Quote@s.whatsapp.net	0	keyId-0006-001	0	0	Text of first user	1419688800000	NULL
19	6002	0-Quote@s.whatsapp.net	1	keyId-0006-002	0	0	I've quoted you	1419688900000	NULL

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff6b 8f51  ...0.J.......k.Q
000e9e40: 2b00 3708 2908 0827 0500 000f 0800 0000  +.7.)..'........
000e9e50: 0809 0808 000d 0501 0101 0000 0000 0000  ................
000e9e60: 0800 0008 0000 0000 0000 0030 2d54 6578  ...........0-Tex
000e9e70: 7440 732e 7768 6174 7361 7070 2e6e 6574  t@s.whatsapp.net
000e9e80: 6b65 7949 642d 3030 3032 2d30 3031 4865  keyId-0002-001He
000e9e90: 7920 7761 7320 6765 6874 3f01 4aa0 a55f  y was geht?.J.._
000e9ea0: 0030 014a a0a5 5f00 ffff ff81 0887 6a2b  .0.J.._.......j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff6b 8f51  ...0.J.......k.Q
000e9e40: 2b00 3708 2908 0827 0500 000f 0800 0000  +.7.)..'........
000e9e50: 0809 0808 000d 0501 0101 0000 0000 0000  ................
000e9e60: 0800 0008 0000 0000 0000 0030 2d54 6578  ...........0-Tex
000e9e70: 7440 732e 7768 6174 7361 7070 2e6e 6574  t@s.whatsapp.net
000e9e80: 6b65 7949 642d 3030 3032 2d30 3031 4865  keyId-0002-001He
000e9e90: 7920 7761 7320 6765 6874 3f01 4aa0 a55f  y was geht?.J.._
000e9ea0: 0030 014a a0a5 5f00 ffff ff81 0887 6a2b  .0.J.._.......j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Content of the cell for entry 2001

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

(0x8f – 0x80) * 0x80 + 0x51 = 2001

https://sqlite.org/src4/doc/trunk/www/varint.wiki

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff6b 8f51  ...0.J.......k.Q
000e9e40: 2b00 3708 2908 0827 0500 000f 0800 0000  +.7.)..'........
000e9e50: 0809 0808 000d 0501 0101 0000 0000 0000  ................
000e9e60: 0800 0008 0000 0000 0000 0030 2d54 6578  ...........0-Tex
000e9e70: 7440 732e 7768 6174 7361 7070 2e6e 6574  t@s.whatsapp.net
000e9e80: 6b65 7949 642d 3030 3032 2d30 3031 4865  keyId-0002-001He
000e9e90: 7920 7761 7320 6765 6874 3f01 4aa0 a55f  y was geht?.J.._
000e9ea0: 0030 014a a0a5 5f00 ffff ff81 0887 6a2b  .0.J.._.......j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Content of the cell for entry 2001

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff00 0000  ...0.J..........
000e9e40: 6e00 3708 2908 0827 0500 000f 0800 0000  n.7.)..'........
000e9e50: 0809 0808 000d 0501 0101 0000 0000 0000  ................
000e9e60: 0800 0008 0000 0000 0000 0030 2d54 6578  ...........0-Tex
000e9e70: 7440 732e 7768 6174 7361 7070 2e6e 6574  t@s.whatsapp.net
000e9e80: 6b65 7949 642d 3030 3032 2d30 3031 4865  keyId-0002-001He
000e9e90: 7920 7761 7320 6765 6874 3f01 4aa0 a55f  y was geht?.J.._
000e9ea0: 0030 014a a0a5 5f00 ffff ff81 0887 6a2b  .0.J.._.......j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Content of the cell after `DELETE FROM messages where _id = 2001;`

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff00 0000  ...0.J..........
000e9e40: 6e00 3708 2908 0827 0500 000f 0800 0000  n.7.)..'........
000e9e50: 0809 0808 000d 0501 0101 0000 0000 0000  ................
000e9e60: 0800 0008 0000 0000 0000 0030 2d54 6578  ...........0-Tex
000e9e70: 7440 732e 7768 6174 7361 7070 2e6e 6574  t@s.whatsapp.net
000e9e80: 6b65 7949 642d 3030 3032 2d30 3031 4865  keyId-0002-001He
000e9e90: 7920 7761 7320 6765 6874 3f01 4aa0 a55f  y was geht?.J.._
000e9ea0: 0030 014a a0a5 5f00 ffff ff81 0887 6a2b  .0.J.._.......j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Partially overwritten

Content of the cell after `DELETE FROM messages where _id = 2001;`

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

DB Browser for SQLite - /private/tmp/file4-deleted

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: messages

Filter in any column

	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timestamp	
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	-1	0	-1	-1	0	NULL	0	NULL
2	1001	MessageFromToday@s.whatsapp.net	0	keyId-0001-001	0	0	This message has been sent yesterday	1639063015000	NULL
3	1002	MessageFromToday@s.whatsapp.net	0	keyId-0001-002	0	0	This message has been sent today	1639149415000	NULL
4	2002	0-Text@s.whatsapp.net	1	keyId-0002-002	0	0	Disdas diggi	1420034500000	NULL
5	2003	0-Text@s.whatsapp.net	0	keyId-0002-003	0	0	Wollen wir uns treffen?	1420034600000	NULL
6	2004	0-Text@s.whatsapp.net	0	keyId-0002-004	0	0	So gegen 15:30 Uhr?	1420034700000	NULL
7	2005	0-Text@s.whatsapp.net	1	keyId-0002-005	0	0	OK. Wo denn?	1420034800000	NULL
8	2006	0-Text@s.whatsapp.net	1	keyId-0002-006	0	0	?	1420034900000	NULL
9	3001	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-001	0	0	Kiss: □	1419948000000	NULL
10	3002	0-Text-WithSmileys@s.whatsapp.net	1	keyId-0003-002	0	0	Thumb up: □	1419948100000	NULL
11	3003	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-003	0	0	Big smile: □	1419948200000	NULL
12	3004	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-004	0	0	UTF SMILING FACE WITH OPEN MOUTH 1F603: 😃	1419948300000	NULL
13	3005	0-Text-WithSmileys@s.whatsapp.net	0	keyId-0003-005	0	0	Male: □; Female: □; House: □; long long text until next …	1419948400000	NULL
14	3006	0-Text-WithSmileys@s.whatsapp.net	1	keyId-0003-006	0	0	Smiley mix: …	1419948500000	NULL
15	4001	0-Text-Long@s.whatsapp.net	0	keyId-0004-001	0	0	💞Handbook 2013💞…	1419861600000	NULL
16	5001	0-Text-InvalidUTF8@s.whatsapp.net	0	keyId-0005-001	0	0	BLOB	1419775200000	NULL
17	6001	0-Quote@s.whatsapp.net	0	keyId-0006-001	0	0	Text of first user	1419688800000	NULL
18	6002	0-Quote@s.whatsapp.net	1	keyId-0006-002	0	0	I've quoted you	1419688900000	NULL
19	7001	0-Link@s.whatsapp.net	0	keyId-0006-001	0	0	https://en.m.wikipedia.org/wiki/JSFuck	1419602400000	NULL

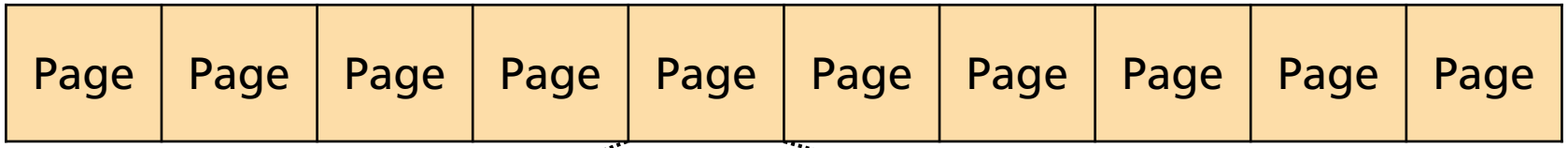
1 - 20 of 42

Go to: 1

UTF-8

SQLite

SQLite Database



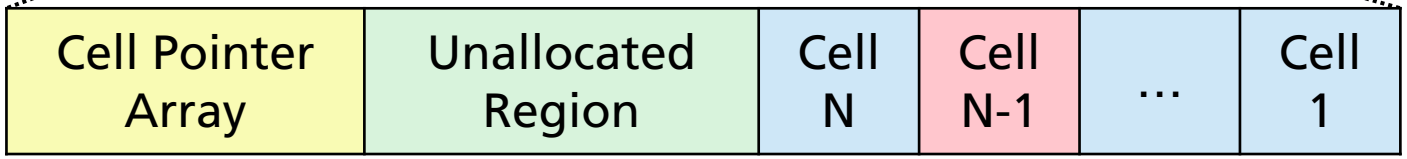


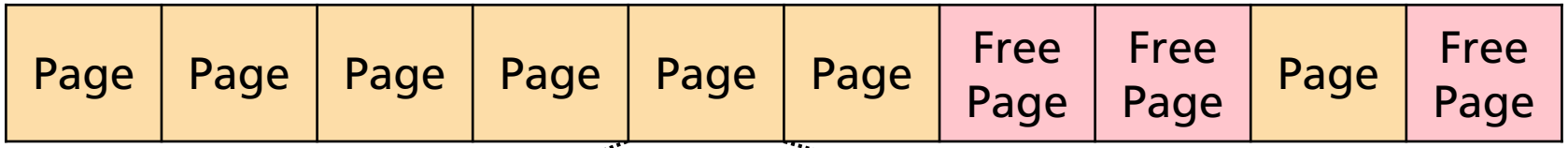
Table B-Tree Leaf Cell

Deleted entries not accessible by parsing “active” data

SQLite

Free pages not accessible by parsing “active” data

SQLite Database



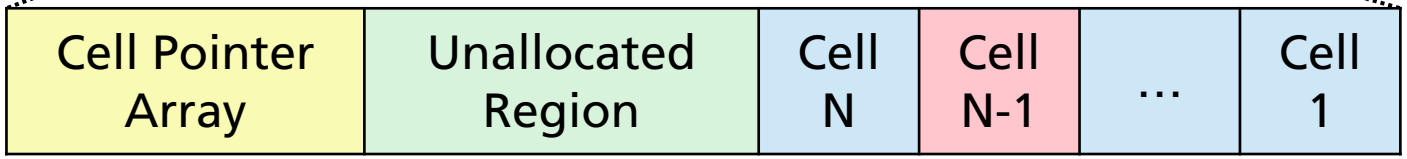


Table B-Tree Leaf Cell

Deleted entries not accessible by parsing “active” data

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

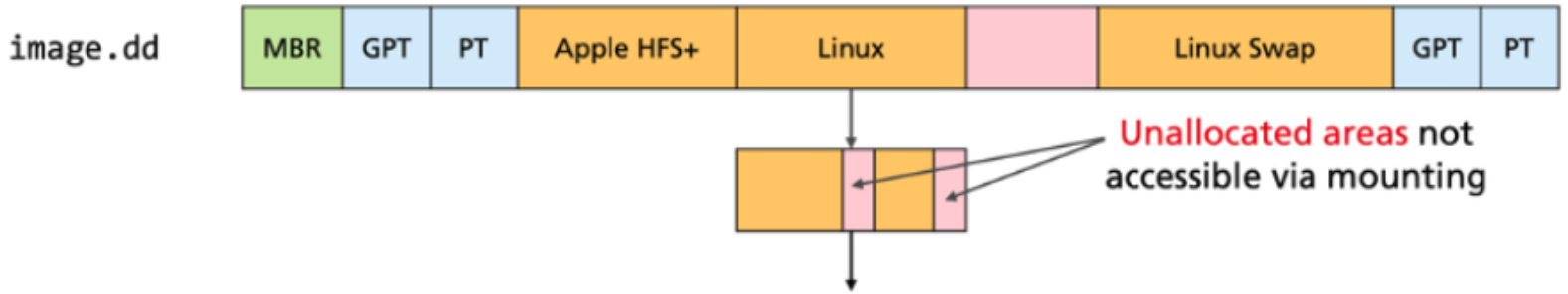
SQLite

Free pages not accessible

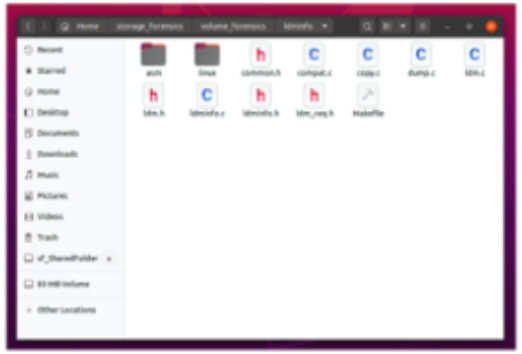
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

File System Analysis



- Analysis depends on the used implementation
- Not all available information may be accessible
- Deleted files are not mounted



- Use an independent analysis tool
- Make sure all important information is easily accessible
- Perform the analysis on the whole volume

14

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

```
~$ recoversqlite.py file4
```

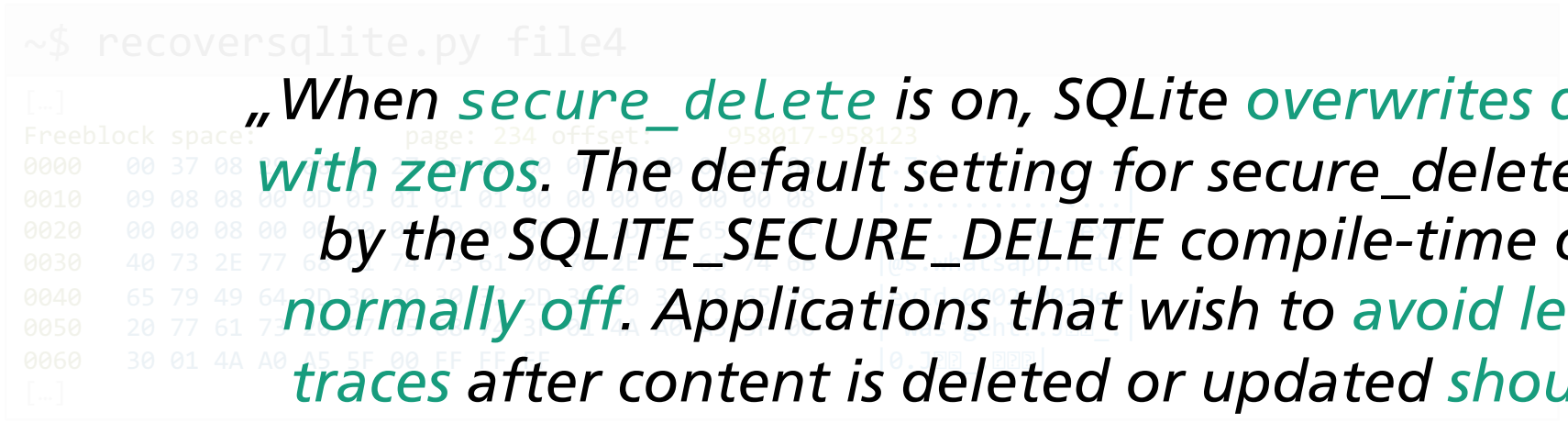
```
[…]
Freeblock space:          page: 234 offset:     958017-958123
0000   00 37 08 29 08 08 27 05 00 00 0F 08 00 00 00 08    |.7.)..'.........|
0010   09 08 08 00 0D 05 01 01 01 00 00 00 00 00 00 08    |................|
0020   00 00 08 00 00 00 00 00 00 00 30 2D 54 65 78 74    |..........0-Text|
0030   40 73 2E 77 68 61 74 73 61 70 70 2E 6E 65 74 6B    |@s.whatsapp.netk|
0040   65 79 49 64 2D 30 30 30 32 2D 30 30 31 48 65 79    |eyId-0002-001Hey|
0050   20 77 61 73 20 67 65 68 74 3F 01 4A A0 A5 5F 00    | was geht?.J□□_.|
0060   30 01 4A A0 A5 5F 00 FF FF FF                      |0.J□□_.□□□|
[…]
```

https://github.com/aramosf/recoversqlite

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite



„When `secure_delete` is on, SQLite overwrites deleted content with zeros. The default setting for secure_delete is determined by the SQLITE_SECURE_DELETE compile-time option and is normally off. Applications that wish to avoid leaving forensic traces after content is deleted or updated should enable the `secure_delete` pragma prior to performing the delete or update, or else run VACUUM after the delete or update.“

https://sqlite.org/pragma.html#pragma_secure_delete

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

2. Description

The VACUUM command rebuilds the database file, repacking it into a minimal amount of disk space. There are several reasons an application might do this:

- Unless SQLite is running in "auto_vacuum=FULL" mode, when a large amount of data is deleted from the database file it leaves behind empty space, or "free" database pages. This means the database file might be larger than strictly necessary. Running VACUUM to rebuild the database reclaims this space and reduces the size of the database file.
- Frequent inserts, updates, and deletes can cause the database file to become fragmented - where data for a single table or index is scattered around the database file. Running VACUUM ensures that each table and index is largely stored contiguously within the database file. In some cases, VACUUM may also reduce the number of partially filled pages in the database, reducing the size of the database file further.
- When content is deleted from an SQLite database, the content is not usually erased but rather the space used to hold the content is marked as being available for reuse. This can allow deleted content to be recovered by a hacker or by forensic analysis. Running VACUUM will clean the database of all traces of deleted content, thus preventing an adversary from recovering deleted content. Using VACUUM in this way is an alternative to setting PRAGMA secure_delete=ON.
- Normally, the database page_size and whether or not the database supports auto_vacuum must be configured before the database file is actually created. However, when not in write-ahead log mode, the page_size and/or auto_vacuum properties of an existing database may be changed by using the page_size and/or pragma auto_vacuum pragmas and then immediately VACUUMing the database. When in write-ahead log mode, only the auto_vacuum support property can be changed using VACUUM.

By default, VACUUM only works only on the main database. Attached databases can be vacuumed by appending the appropriate schema-name to the VACUUM statement.

Compatibility Warning: The ability to vacuum attached databases was added in version 3.15.0 (2016-10-14). Prior to that, a schema-name added to the VACUUM statement would be silently ignored and the "main" schema would be vacuumed.

https://sqlite.org/lang_vacuum.html

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

SQLite

VACUUM and SECURE_DELETE enabled

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff6b 8f51  ...0.J.......k.Q
000e9e40: 2b00 3708 2908 0827 0500 000f 0800 0000  +.7.)..'........
000e9e50: 0809 0808 000d 0501 0101 0000 0000 0000  ................
000e9e60: 0800 0008 0000 0000 0000 0030 2d54 6578  ...........0-Tex
000e9e70: 7440 732e 7768 6174 7361 7070 2e6e 6574  t@s.whatsapp.net
000e9e80: 6b65 7949 642d 3030 3032 2d30 3031 4865  keyId-0002-001He
000e9e90: 7920 7761 7320 6765 6874 3f01 4aa0 a55f  y was geht?.J.._
000e9ea0: 0030 014a a0a5 5f00 ffff ff81 0887 6a2b  .0.J.._.......j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Content of the cell for entry 2001

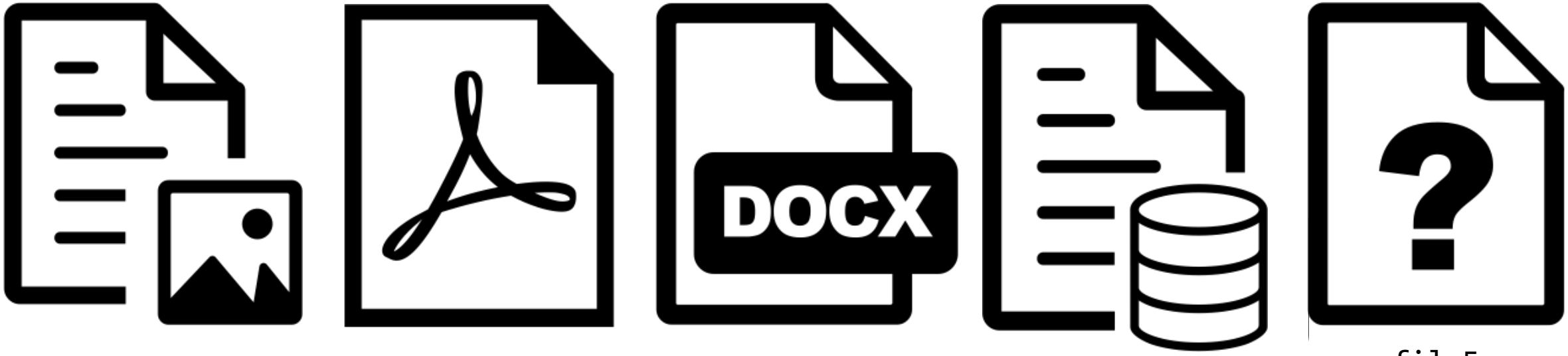
SQLite

VACUUM and SECURE_DELETE enabled

```
~$ xxd file4
[…]
000e9e00: 5465 7874 4073 2e77 6861 7473 6170 702e  Text@s.whatsapp.
000e9e10: 6e65 746b 6579 4964 2d30 3030 322d 3030  netkeyId-0002-00
000e9e20: 3244 6973 6461 7320 6469 6767 6901 4aa0  2Disdas diggi.J.
000e9e30: a6e5 a030 014a a0a6 e5a0 ffff ff00 0000  ...0.J..........
000e9e40: 6e00 0000 0000 0000 0000 0000 0000 0000  n...............
000e9e50: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000e9e60: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000e9e70: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000e9e80: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000e9e90: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000e9ea0: 0000 0000 0000 0000 0000 0081 0887 6a2b  .0.J._.....j+
000e9eb0: 004b 0829 0808 4d05 0000 0f08 0000 0008  .K.)..M.........
000e9ec0: 0908 0800 0d05 0101 0100 0000 0000 0008  ................
000e9ed0: 0000 0800 0000 0000 0000 4d65 7373 6167  ..........Messag
000e9ee0: 6546 726f 6d54 6f64 6179 4073 2e77 6861  eFromToday@s.wha
000e9ef0: 7473 6170 702e 6e65 746b 6579 4964 2d30  tsapp.netkeyId-0
000e9f00: 3030 312d 3030 3254 6869 7320 6d65 7373  001-002This mess
000e9f10: 6167 6520 6861 7320 6265 656e 2073 656e  age has been sen
000e9f20: 7420 746f 6461 7901 7da4 eb2a 5830 017d  t today.}..*X0.}
000e9f30: a4eb 2a58 ffff ff81 0c87 692b 004b 0829  ..*X......i+.K.)
000e9f40: 0808 5505 0000 0f08 0000 0008 0908 0800  ..U.............
000e9f50: 0d05 0101 0100 0000 0000 0008 0000 0800  ................
[…]
```

Content of the cell after `DELETE FROM messages where _id = 2001;`

Filetypes



file5

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

```
~$ file file5
file5: PE32 executable (GUI) Intel 80386, for MS Windows
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Filetypes

```
~$ file file5
file5: PE32 ex
```

Fraunhofer FKIE

Prof. Dr. Elmar Padilla et al.

Malware Analysis

02 – Malware Analysis