

METADATA

Reem Bashir

WHAT IS METADATA

- Metadata is the information attached to the files that consist of:
 - Comments
 - Tracked changes
 - Revision marks
 - File properties:
 - Type of the camera/ Type of the document
 - to personal information:
 - Name
 - Company's details
 - Timestamps
 - Headers, footers
 - Watermarks
 - Location

PHOTO'S METADATA

- One of the main metadata collectors is the EXIF block that is added to graphic files.
- The Exchangeable Image File Format standard was developed by the Japanese Electronics and IT Association (JEITA) and first published in 1995.
- EXIF was developed for JPEG and TIFF files.
- Other popular formats such as PNG and GIF might also contain similar metadata in particular, Adobe's XMP-based metadata.
- Camera vendors might use a proprietary metadata format, partially redundant with EXIF.

WHY TO REMOVE THE METADATA

- Metadata answers who, what, when, where, why and how
- Why?
 - To protect your privacy.
 - To prevent from reveal things to the wrong people
 - To prevent being track and find more photos taken by you
 - To prevent sharing EU citizens data without there permission, the General Data Protection Regulation (GDPR).
 - To make the photo's size smaller, like JPEG, is often held in a separate file.

METADATA CASE

- In 2012 John McAfee was wanted by the Belize police because of his connection of a murder.
- The VICE magazine posted photo without deleting the metadata, which revealed John McAfee location.



Frank Rieger

@frank_rieger



Ooops. #Vice forgot to clean (or faked?) the GPS-location from the EXIF-tag on their picture with #McAfee : vice.com/read/we-are-wi

...

8:44 PM - Dec 3, 2012



We Are with John McAfee Right Now, Suckers

VICE editor-in-chief Rocco Castoro and photographer/videographer Robert King have been following John McAfee for the past four days, vice.com

<https://thenextweb.com/insider/2012/12/03/vice-leaves-metadata-in-photo-of-john-mcafee-pinpointing-him-to-a-location-in-guatemala/>

METADATA VIEWER TOOLS

- ExifTool
- Metadata Extraction Tool
- Hex Workstation
- Strings
- Windows file system

EXIFTOOL

- ExifTool is a open source platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files.
- For Windows and macOS
- Problem:
 - Writer Limitations
 - Delete by antivirus software
 - long processing times in Windows
 - In Windows, ExifTool will not process files with Unicode characters in the file name.
 - There is a bug in a number of Adobe utilities.
 - There is a bug in the Apple RAW file support (OS X 10.4.11) which prevents some edited Pentax PEF images from being displayed
- Licence:
 - <https://www.sno.phy.queensu.ca/~phil/exiftool/#license>


```
C:\Users\admin\Desktop>exiftool.exe CTEC3754-Lab-2-network-behaviour.pdf
ExifTool Version Number      : 10.82
File Name                    : CTEC3754-Lab-2-network-behaviour.pdf
Directory                   : .
File Size                    : 330 kB
File Modification Date/Time   : 2018:01:26 11:18:24+00:00
File Access Date/Time        : 2018:01:26 11:18:22+00:00
File Creation Date/Time      : 2018:01:26 11:18:24+00:00
File Permissions              : rw-rw-rw-
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.5
Linearized                   : No
Page Count                   : 4
Language                     : en-GB
Tagged PDF                   : Yes
Author                       : Suleiman Yerima
Creator                      : Microsoft Word 2010
Create Date                  : 2018:01:25 15:35:28+00:00
Modify Date                  : 2018:01:25 15:35:28+00:00
Producer                     : Microsoft Word 2010
```

Administrator: C:\Windows\System32\cmd.exe

```
C:\Users\admin\Desktop>exiftool.exe Picture1.jpg
ExifTool Version Number      : 10.82
File Name                    : Picture1.jpg
Directory                   : .
File Size                    : 60 kB
File Modification Date/Time   : 2018:01:12 14:07:28+00:00
File Access Date/Time        : 2018:01:12 14:07:28+00:00
File Creation Date/Time      : 2018:01:12 14:07:28+00:00
File Permissions              : rw-rw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                  : 105
Y Resolution                  : 134
Image Width                   : 721
Image Height                  : 478
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                    : 721x478
Megapixels                    : 0.345
```

C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>cd Desktop

C:\Users\admin\Desktop>exiftool.exe USB-Rubber-Ducky-master.zip
ExifTool Version Number      : 10.82
File Name                    : USB-Rubber-Ducky-master.zip
Directory                   : .
File Size                    : 68 MB
File Modification Date/Time   : 2018:02:27 15:52:50+00:00
File Access Date/Time        : 2018:02:27 15:52:17+00:00
File Creation Date/Time      : 2018:02:27 15:52:17+00:00
File Permissions              : rw-rw-rw-
File Type                    : ZIP
File Type Extension          : zip
MIME Type                    : application/zip
Zip Required Version          : 10
Zip Bit Flag                  : 0
Zip Compression               : None
Zip Modify Date               : 2015:04:19 14:28:05
Zip CRC                       : 0x00000000
Zip Compressed Size           : 0
Zip Uncompressed Size         : 0
Zip File Name                 : USB-Rubber-Ducky-master/

C:\Users\admin\Desktop>
```

METADATA REMOVABLE TOOLS

**Image MetaData
Stripper**

Version 1.0

**MAT: Metadata
Anonymisation
Toolkit**

Version 0.6

IMAGE METADATA STRIPPER

- A lightweight and handy tool that clean and remove metadata from images.
- The image quality is not altered in any way.
- GNU/GPL
- Only work in Windows and Mac OS
- Source code
 - http://codewelt.com/dl/stripper/Image_MetaData_Stripper_10-Source.zip

Open Image File(s)

Clear Log

☒ Keep Image Backups

☐ Close this Application when done

1 File opened.

Processing C:/Users/Administrator/Pictures/20170517_033051.jpg ...

Nothing stripped. - Details - Image Width: 4128; Image Height: 2322; Image Format: RGB32;
No alpha channel found

Nothing to do. The input does not contain MetaData.

1 File opened.

Processing C:/Users/Administrator/Pictures/20170517_033113.jpg ...

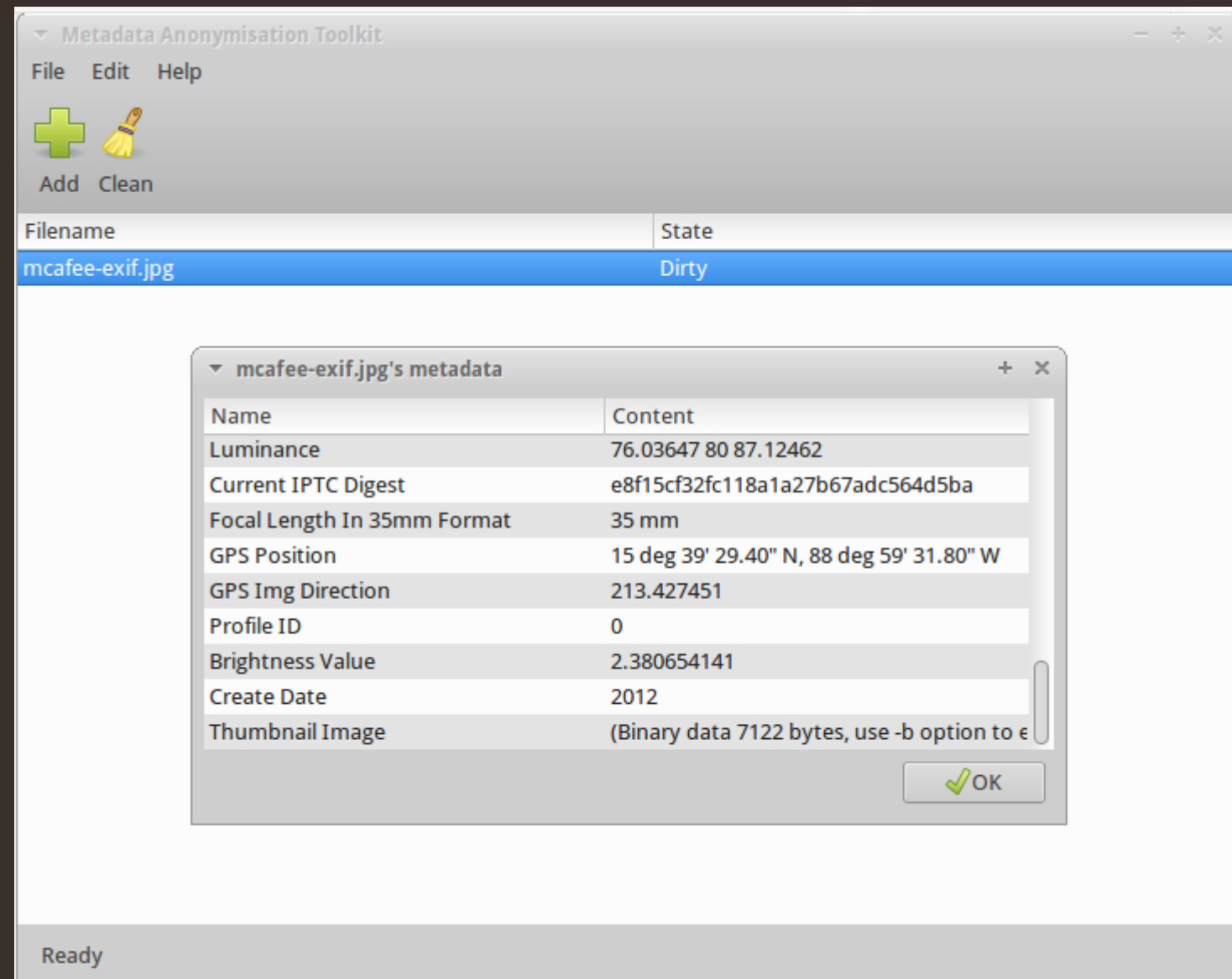
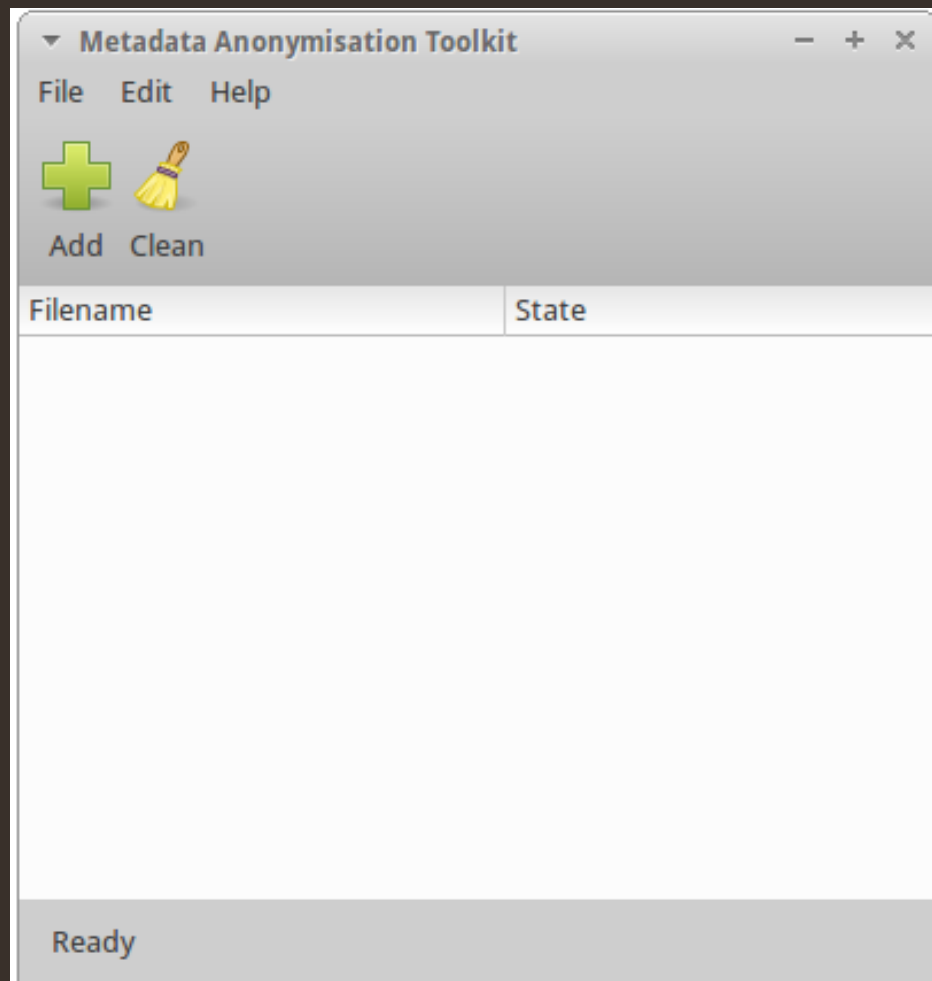
26 Bytes Removed! - Details - Image Width: 4128; Image Height: 2322; Image Format:
RGB32; No alpha channel found

A Total of 26 Bytes were Stripped!

Done.

MAT: METADATA ANONYMISATION TOOLKIT

- Python application to remove the metadata from photos, open documents, office OpenXml, PDF, archives MPEG audio, Ogg Vorbis, Free Lossless Audio Codec and torrent.
- Toolbox composed of a GUI application, a CLI application and a library, to remove metadata.
- It is not really efficient at scrubbing embedded media inside complex formats. For examples, images embedded inside PDF may not be cleaned.
- For Linux only.
- Source code
 - <https://oxacab.org/mat/mat>



LETS TRY IT

- **Image MetaData Stripper**

- Windows

- http://codewelt.com/dl/stripper/Image_MetaData_Stripper_10-Win32-MSVC2008.zip

- Mac OS X

- http://codewelt.com/dl/stripper/Image_MetaData_Stripper_10-MacOSX-x86.zip

- **MAT: Metadata Anonymisation Toolkit**

- Linux

- <https://mat.boum.org/files/>