eForensics Magazine

MAGAZINE

METADATA FORENSICS

DATA CARVING CORRUPT IMAGES TO EXTRACT METADATA

LEAK COMPANY DATA - DATA EXFILTRATION

TROJAN HORSES IN CRIMINAL INVESTIGATIONS

VOL.07 NO.04
ISSUE 04/20178 (81) APRIL
ISSN 2300 6986

eForensics Magazine

TEAM

Editor-in-Chief:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editors:

Marta Strzelec
marta.strzelec@eforensicsmag.com

Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@haking.com

Bartek Adach
bartek.adach@pentest.com

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP:
Marta Strzelec
marta.strzelec@eforensicsmag.com

Dominika Zdrodowska
dominika.zdrodowska@eforensicsmag.com

Cover Design:
Hiep Nguyen Duc

Publisher:
Haking Media Sp. z o.o.
02-676 Warszawa
ul. Postępu 17D
Phone: 1 917 338 3631

www.eforensicsmag.com

word from the team

Dear Readers,

Welcome to the newest issue of eForensics Magazine! Hope you have a great time during holiday. This month our magazine is related to the topic of metadata in cyber forensics - inside you will find the article on the topic by Cybercopsam, which raises questions such as "why do we need metadata?", "carving or metadata?" and shows examples of extracting metadata. Moreover, we have also an article for you by Hector Barquero, entitled "Data Carving Corrupt Images to Extract Metadata". This article' ll help you understand metadata hex-editors, how to repair a header after corrupt conversion or proprietary file-type disagreements and how to hide your metadata on your next graphic file upload. This article is available to download in the preview. You can read it for free!

But of course that's not all! The issue opens with an article "Analysing Fileless Malware" by Andrei Modan in which the author as a proof of concept takes Win7 SP1 Virtual Machine, which is infected with Win32/Poweliks. Although there are many methods to perform forensics analysis, in this situation he uses just the memory dump of the infected machine, and investigates it using Volatility framework and some Linux commands. Further, we have a really interesting unit about data exfiltration (which is nowadays widely used to steal information from organizations) by Fabricio Salomao & Paulo Trindade.

In the second section of the issue you will have a chance to read a very captivating interview with Silvio Montanari about his tool: code-forensics. It's a kind of preview of our next issue connected with digital forensic open-source tools (Stay tuned!).

We hope you enjoy the issue - let us know your thoughts if you have any, we'd love to receive a feedback from you!

As always, many, many thanks to our reviewers and proofreaders - you are irreplaceable. We're extremely grateful!

Hope you'll have a great read,
Dominika Zdrodowska
and the eForensics Magazine Editorial Team

Table Of Contents

Digital Forensics; Data Carving Corrupt Images to Extract Metadata

by Hector Barquero

The purpose of this document is to understand technical recovery details of graphic files when corrupt header hex values on file type conversions exists, and to determine how metadata is removed from Windows OS.

The Internet and The Problem with Convenience; Oversharing

The internet has become a popular and necessary life-tool with an estimated 3.8 billion users across the globe (nearly 51% of the world population) as reported by the World Internet Usage Statistics in 2017.

Roughly 2.5 quintillion bytes of new data is created each day with 90% of the data being created in the past three years. This is created by "…not just mobile devices, but Smart TV's, cars, airplanes, you name it—the internet of things is producing an increasing amount of data." (Shultz)

It's a staggering amount of cat photos.

But through all the graphic files flowing through the internet is an embedded layer of information waiting to be uncovered by the Digital Forensic enthusiast or more concerningly—malicious internet users.

Present application availability allows ease of use for all, regardless of technological skills, and with that the capability to post content freely and seamlessly. This comes at a price.

With a quick snap, click and post, your graphic file is uploaded and often private information is shared on the internet.

Information is inherently overshared. This is because each photo has metadata information with relevant personal data. In an article I recently published, titled "Digital Forensics – Tracking & Target Locating .Jpegs via Metadata (Exif)"-- I showed that with nothing more than time and free software, you could uncover details including location, time, date, technical information and even the originators name or identifiable information under certain conditions.

Check out the blog on eForensics Magazine for the details on the article and to better understand how convenience can cause security risks.

For now, this article discusses:

1. What a graphic file really is,
2. Metadata hex-editors, how to repair a header after corrupt conversion or proprietary file-type disagreements, and;
3. How to hide your metadata on your next graphic file upload.

Graphics Files: Back to Basics

Graphics files are large file types that contain digital photographs, three-dimensional images or even line art. They are identified in the following categories:

Bitmap Images – a collection of digital dots displayed in grids of pixels. Raster images branch from this as they are also collections of pixels but are stored in rows, which enable improved printing.

Vector Graphics – describes aspects covering mathematical instructions, using lines rather than dots, storing only calculations for the positioning of lines and shape. A vector graphic file size is typically smaller than a bitmap file because of its arithmetic approach and preserves quality when enlarged, a bonus for graphic illustrators who create logos and images.

Metafile Graphics – a combination of bitmap and vector, graphical information that is capable of being transferred and exchanged between different systems, devices and software clients. Typical metafile graphics will combine vector and raster images, sharing both the beneficial qualities and lesser-desired traits.

Standard bitmap file formats can include:

- Portable Network Graphic .PNG,
- Graphic Interchange Format .GIF,
- Tagged Image File .TIF/TIFF,
- Window Bitmap .BMP and
- Joint Photographic Experts Group .JPEG/JPG.

Vector file types, although slightly less common, may be typically viewed as the Autocad .DXF extension type or Hewlett Packard Graphics Language .HPGL file type.

Graphics Files: Digital Negatives, Demosaicing & Corruption

When a camera takes a photograph, the sensor in the digital camera will record pixels on the camera's memory card, which builds the raw file format or digital negative. This is commonly on higher-end cameras, but with today's competitive tech driven economy, more and more devices are being equipped with better cameras, meeting this capability.

Raw formats maintain the best picture quality but are often proprietary and therefore cause difficulties viewing the image with common image viewers. These formats are required to be converted from raw picture data to compressed extension-types to act as a container for the larger file, a process known as demosaicing or "debayering".

A Bayer filter is a mosaic, filled with a color-filter array (CFA) for arranging RGB color filters on a square grid of photosensors. The unique and specific arrangement of filters is used in most single-chip digital image sensors used in modern cameras that create graphics images.

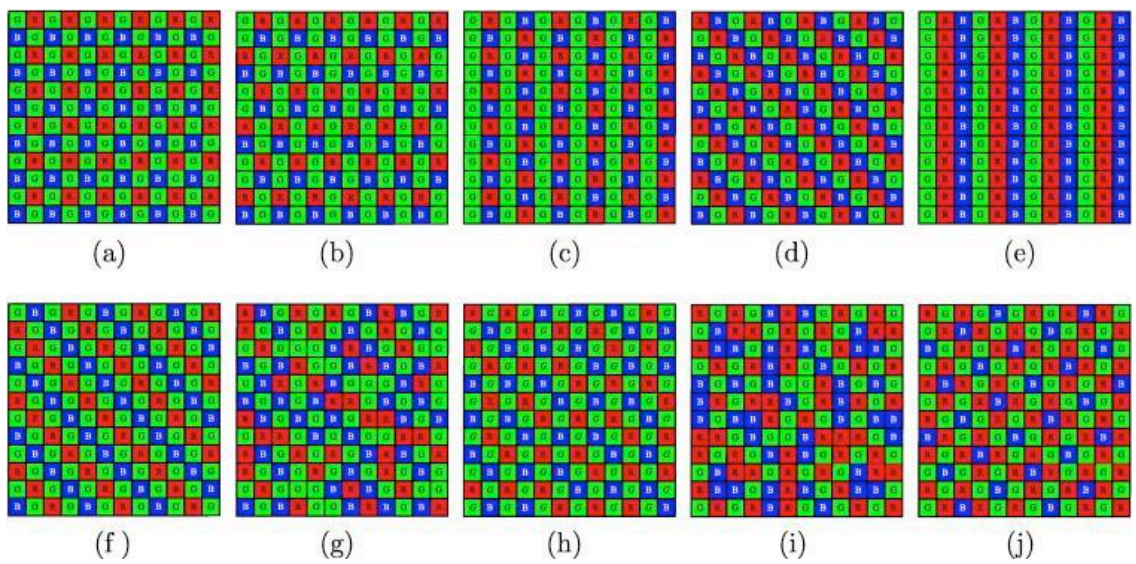


Figure 1 The Bayer Filter, Journal of Visual Communication and Image Representation Volume 25, Issue 7 Oct 2014

JEITA's solution to debayering, the Exif format, is a standard for storing metadata in .jpeg and .TIF files. This will include the model, serial number, make of camera, shutter speed, resolution, focal length, time, date, and the latitude and longitude for location—even the name of the originator or other pertinent information can be shared when the device is statically named, i.e. "John's Samsung S8".

Exif files collect metadata, data that further describes the image, but require unique software to view in its raw form. Generally, the end-user is less concerned with metadata and more interested in image quality, file size or compatibility, which may spark the sudden desire to change a file type. The end-user may undergo a similar process by doing so, sometimes causing broken headers in the hex code of the metadata within the graphic image file in an area that could corrupt the Exif data.

Remember: not all file types use the same compression algorithms.

Hex-Editors, Hex Code and Data Carving: Recovering Corrupt Metadata

Hex-Editors allow the viewing of a digital image in hexadecimal code and provide modification capabilities of binary data, which builds the computer file itself. WinHex is free to use and I often use this software to repair file types or modify them to include hidden data (the practice of Steganography, a topic for a later date).

With this software, repairing and salvaging corrupt headers or metadata when compression fails can be made possible, a digital forensic process known as data carving.

The process:

1. Attempt to open the image with different image-viewers, if the image doesn't display,

2. Examine the file header. Research the file type for the correct header, compare and

3. Repair the header if needed with ASCII text or the proper Hex code values.

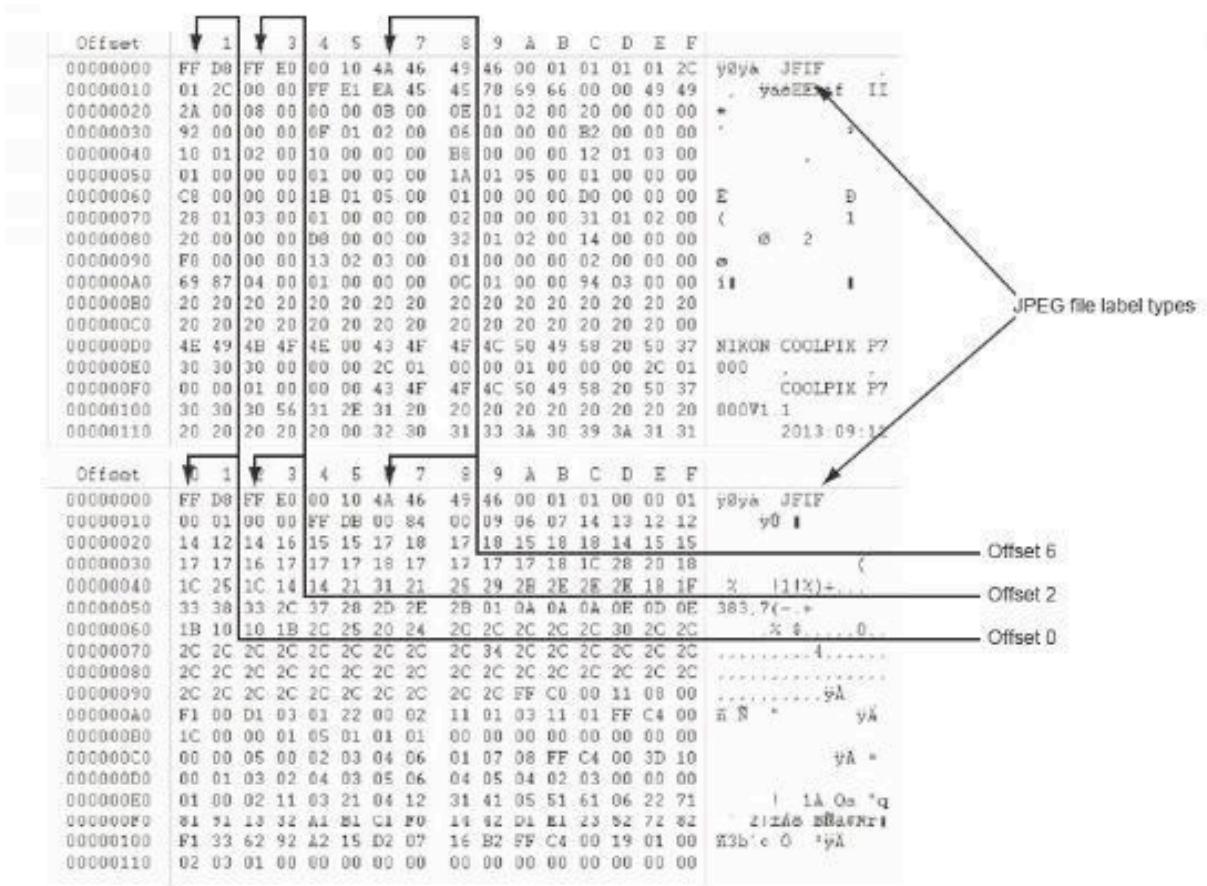


Figure 2 Hex code is positioned in offsets, ASCII code listed to the right in WinHex. Exif metadata is usually stored in the beginning of the file but other file types are indicated by the hex, i.e. 49 49 2A (TIFF). Courtesy of X-Ways AG

With an astonishing amount of resources available online for reference to proper header formats, file types and software to edit the hex as needed, it's possible to repair the graphic image to be viewable in its full integrity.

Writing down common file types, headers and hex code you encounter along the way to familiarize yourself with the encoded details of a graphics file will quickly allow you to identify the markers, application markers, start of stream (SOS), start of image (SOI) and end of image (EOI) hex identifiers that help identify data clusters and blocks.

Creating Safe Graphics Files: Stripping Personal Information From Images (Windows OS)

As an Infosec and Network/Software Security enthusiast, I find myself constantly breaking systems and software distributions during my off-time to find weaknesses or loopholes in hopes of providing more secure solutions.

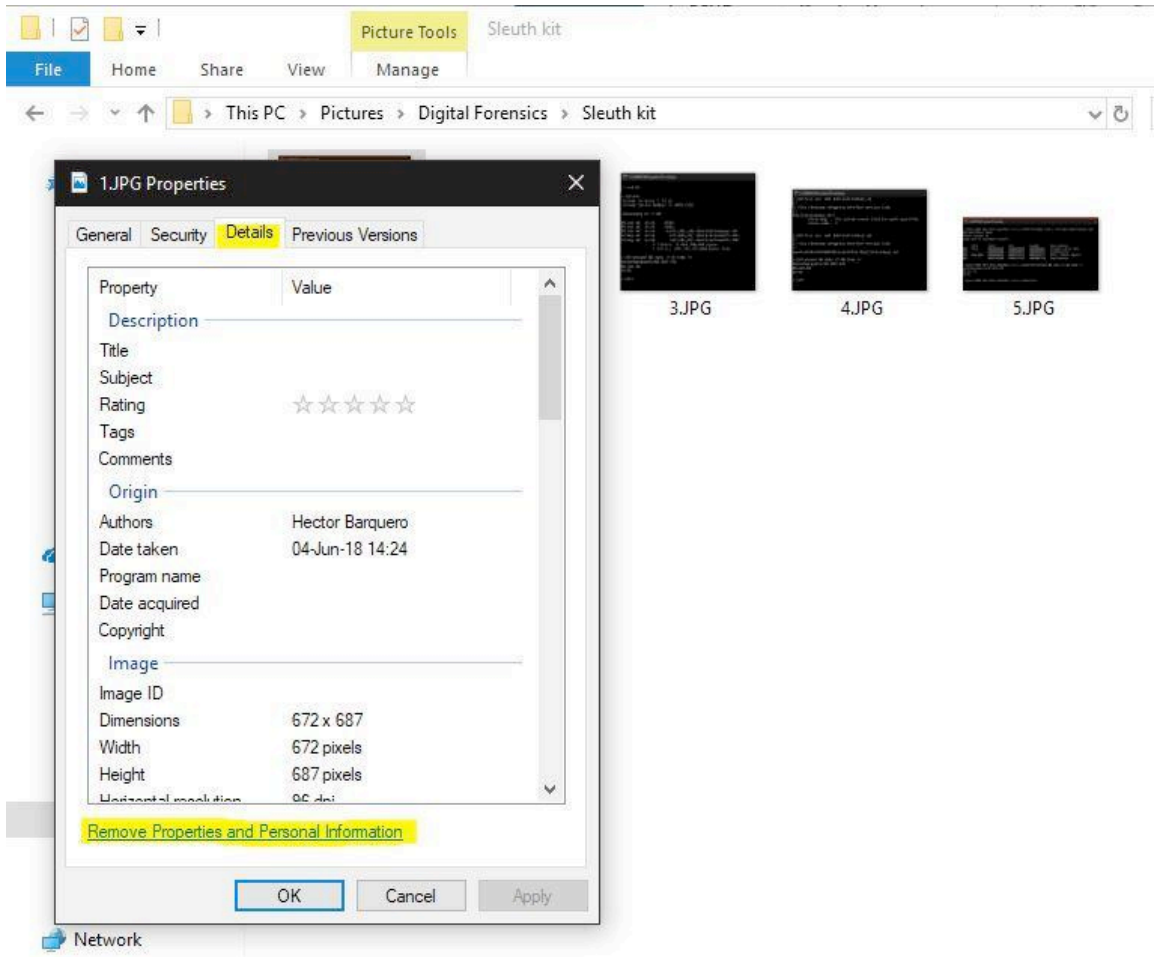
I am not constantly looking for a problem, but I am pursuing proof that an expectation exists and end-users should be able to use their computers securely, sharing data and photographs on the internet without compromising their privacy unwillingly or unknowingly.

With Exif metadata being repaired in the header via WinHex, a graphics file may do just that.

As a solution to this problem, users can opt to remove their personal information from graphics files.

In a few simple steps using Windows Operating System (OS), the problem can be greatly reduced, if not entirely eliminated by the following:

1. Open File explorer via the Search feature or hot-key Windows + E
2. Locate the image you are wanting to deprive of personal information
3. Right click and select properties to open up more details about the image
4. Select the Details tab and 'Remove Properties and Personal Information' at the bottom
5. Opt to create a new copy without the information, or strip the present copy



With this adjustment to your graphics files, whether they are corrupt, carved and repaired or not, you'll be able to share and distribute your images with more trust in knowing your personal and technical details are kept private.

All the best,

Hector Barquero

Referenced Works:

1. Internet World Usage Statistics 2017. (n.d.). Retrieved July 23, 2018, from https://www.internetworldstats.com/stats.html

2. Micro Focus Blog. (n.d.). Retrieved from https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/, Jeff Shultz

Here you can find "Digital Forensics - Tracking & Target Locating .Jpegs via Metadata (Exif)" by Hector Barquero, mentioned in this article: https://eforensicsmag.com/digital-forensics-tracking-target-locating-jpegs-via-metadata-exif-by-hector-barquero/

Hector Barquero is completing his MSc in Computing Science while serving as a Reservist in the Canadian Armed Forces; an Army Communication and Information Systems Specialist. Hector expresses an active interest in computer, software, and network security by consistently building new networks, testing systems and writing/examining malware for security research on his own time. Hector actively pursues certifications in information security, network security and ethical hacking while maintaining a presence in his local community as a volunteer mentor for youth code camps and a guest speaker, educating teens in safe online-use.

His portfolio includes over 140 examples of malware, software, ethical hacking tests, network designs, servers, and more. Hector anticipates his CISSP Associate certification, CEH and CCNA – Security designation by Fall of 2018.

His full profile is available on LinkedIn: https://ca.linkedin.com/in/hectorbarquero