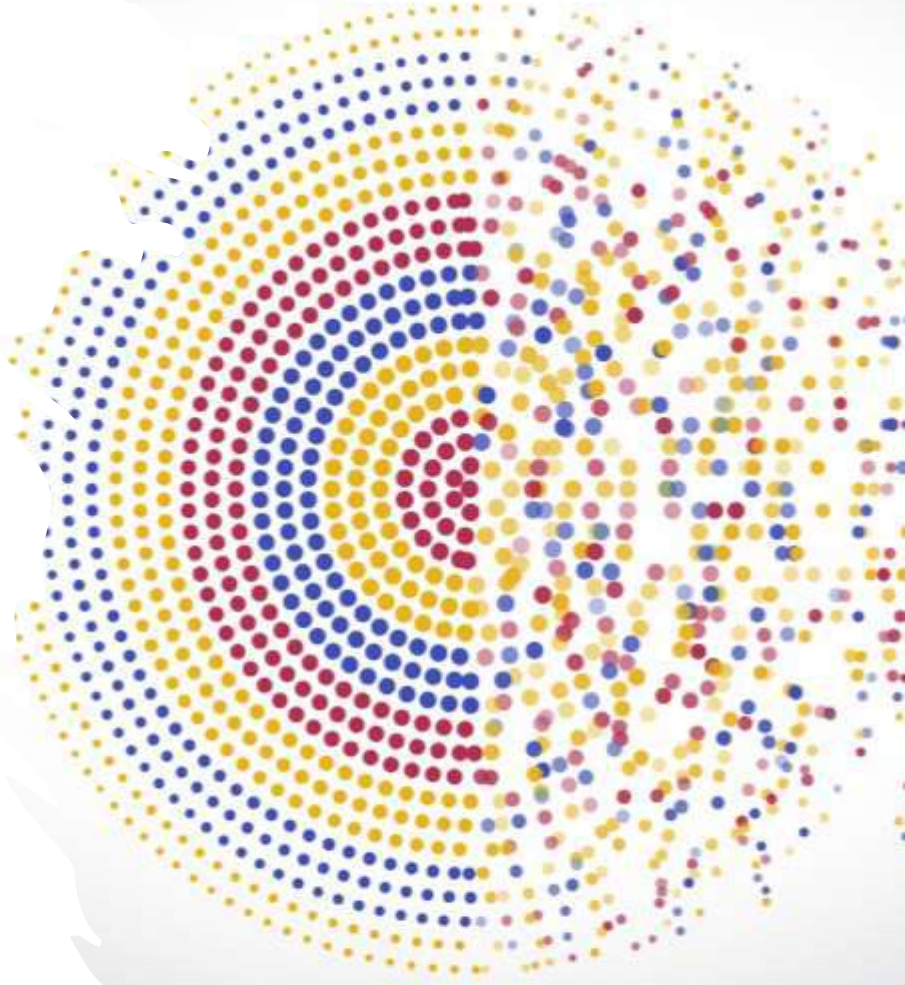
Guide to Computer Forensics and Investigations Sixth Edition

Chapter 8

Recovering Graphics Files



Objectives

- Describe types of graphics file formats
- Explain types of data compression
- Explain how to locate and recover graphics files
- Describe how to identify unknown file formats
- Explain copyright issues with graphics

Introduction

- Many digital forensics investigations involve graphics especially the ones downloaded from the Web and emails.
- To investigate these images we need to understand the basics of the computer graphics including the:
  - Characteristics,
  - Formats,
  - Compression,
  - Reducing the data size,

Recognizing a Graphics File

Graphic files contain digital photographs, line art, three-dimensional images, text data converted to images, and scanned replicas of printed pictures.

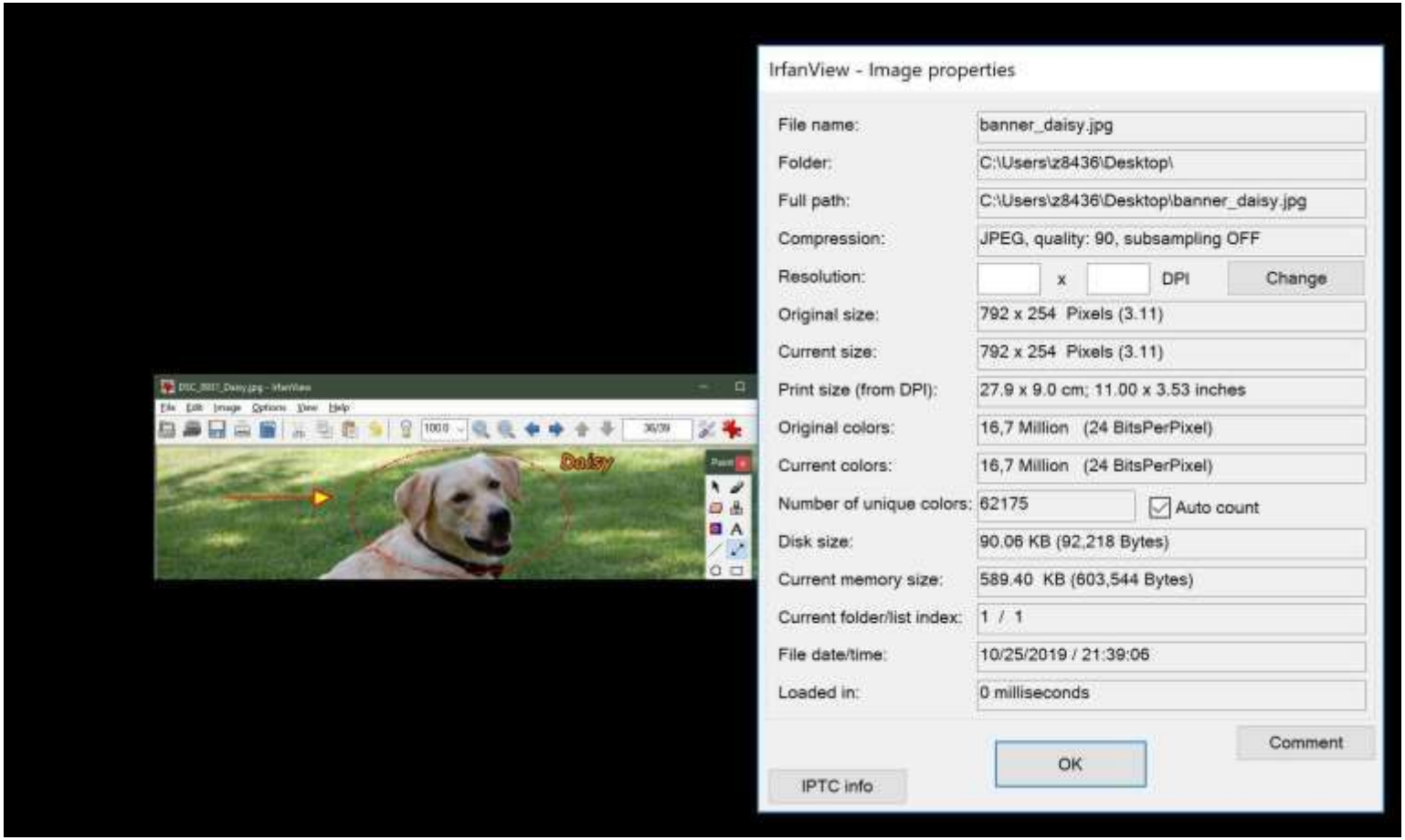
- Graphic program creates 3 types of image file
  - **Bitmap images**: a **collection of dots/pixels (represented as a resolution on display)**
  - **Vector graphics: based on mathematical instructions- they too are pixels but are stored in a vector, making it easy to print**
    - Adding text (vector) to a photograph (bitmap)
    - Are usually smaller than bitmap
  - **Metafile graphics: a combination of bitmap and vector**
- Types of programs to edit image files
  - Graphics editors (create, modify and save)
  - Image viewers (Open and view no changes to the content)
- When using these tools, you open image files such as BMP, GIF, and JPEG.
- These files have different qualities, including color, compression,

Understanding Bitmap and Raster Images

- **Bitmap images-**store graphics in Grids of individual **pixels**
- **Raster images** - also collections of pixels
  - Pixels are stored in rows
  - Better for printing
- Image quality is governed by
  - Screen **resolution** - determines the amount of detail

Understanding Bitmap and Raster Images

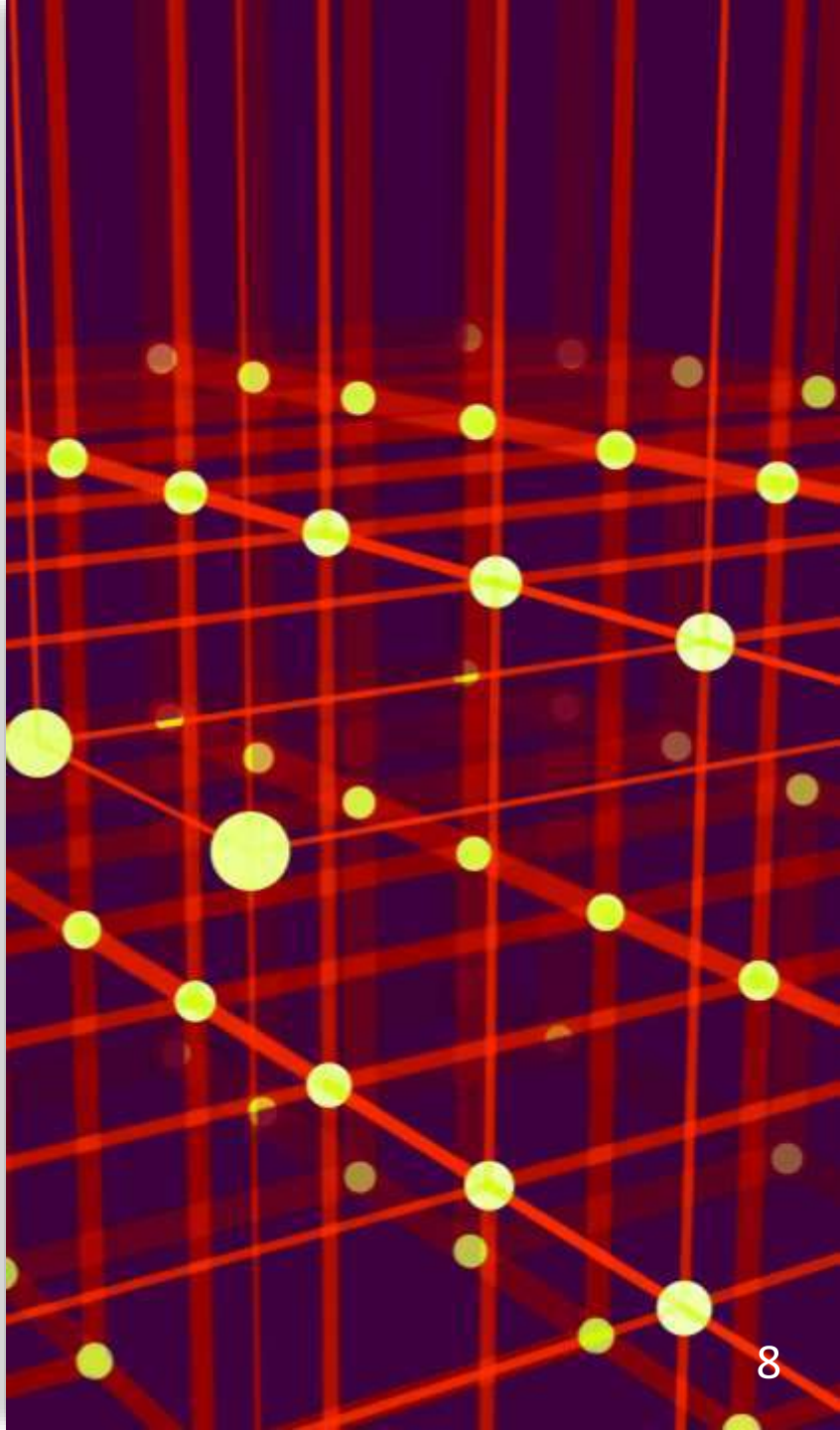
- Software contributes to image quality (drivers which set the video card's display parameters)
  - Number of color bits used per pixel
  - The other effect image is the number of colors the monitor displays.
- Amount of color per pixel, the following are list of bits per colored pixel:
  - 1 bit = 2 colors
  - 4 bits =16 colors
  - 16 bits =256 colors
  - etc



7

Understanding Vector Graphics

- Vector graphics are unlike the Bitmap image and raster images
  - Uses lines instead of dots
  - Store only the calculations for drawing lines and shapes;
  - A graphic program converts these calculations into an image;
  - Smaller than bitmap files;
  - Preserve quality when image is enlarged,
- CorelDRAW, Adobe Illustrator



Understanding Metafile Graphics

- Metafile graphics combine raster and vector graphics
- Example
  - Scanned photo (bitmap) with text or arrows (vector)
- Share the advantages and disadvantages of both Bitmap and Vector files.
  - For example when enlarged, the bitmap part loses resolution quality, but the vector formats remain sharp and clear.

Understanding Graphics File Formats (1 of 3)

- Graphic files created and saved in graphic editors, such as:
  - MS Paint,
  - Adobe Freehand MX,
  - Adobe Photoshop
  - Gnome GIMP (Linux app)
- Some editors work for Vectors graphics (Freehand MX) and others work for both such as Photoshop
- Most Graphic editors can create and save files in one or more of the Standard Graphic Formats

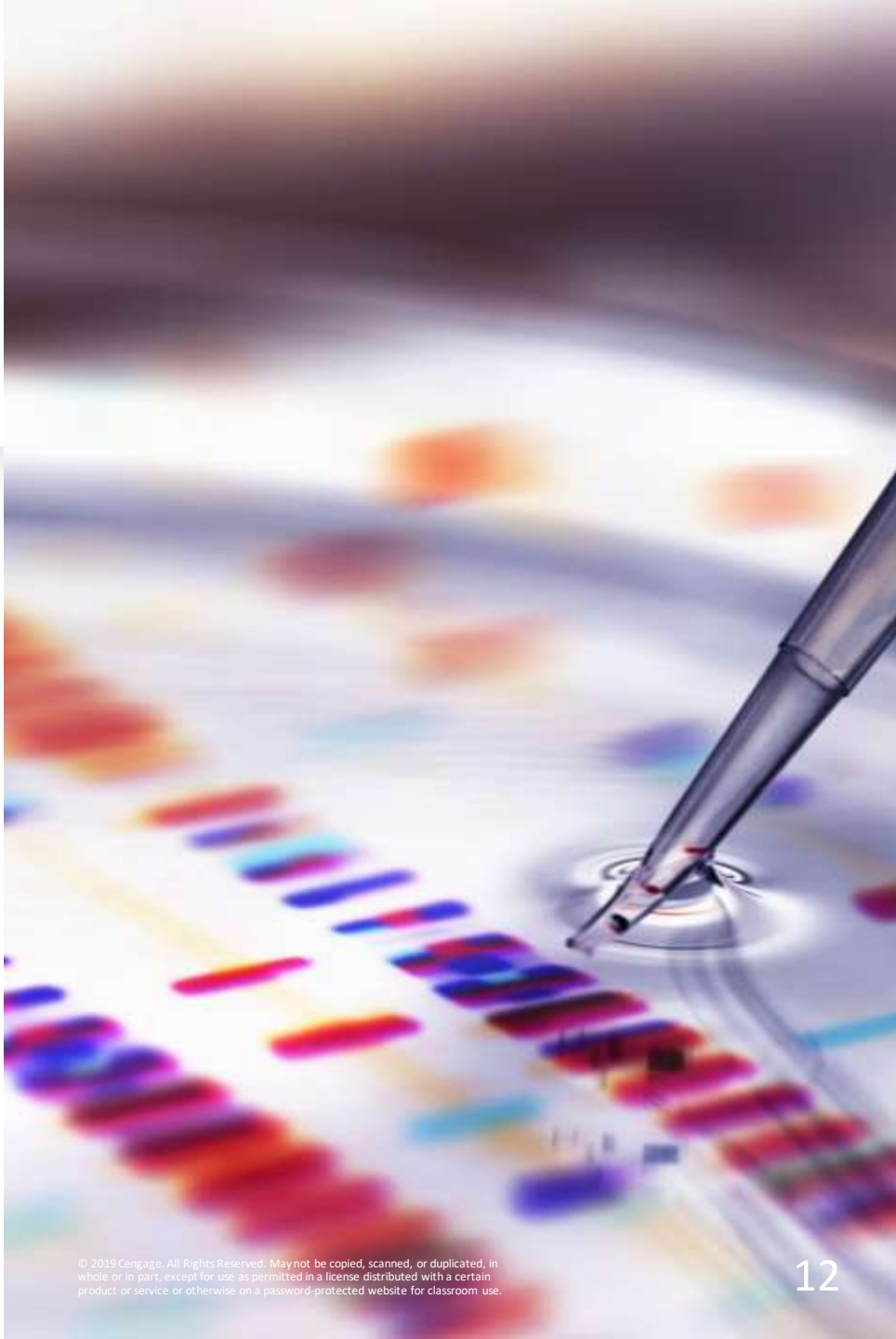
10

Understanding Graphics File Formats (2 of 3)

- **Standard graphics file formats**
  - Standard bitmap file formats
    - *Portable Network Graphic (.png)*
    - *Graphic Interchange Format (.gif)*
    - *Joint Photographic Experts Group (.jpeg, .jpg)*
    - *Tagged Image File Format (.tiff, .tif)*
    - *Window Bitmap (.bmp)*
  - Standard vector file formats
    - Hewlett Packard Graphics Language (.hpgl)
    - Autocad (.dxf)

Understanding Graphics File Formats (3 of 3)

- **Nonstandard graphics file formats**
  - *Targa (.tga)*
  - *Raster Transfer Language (.rtl)*
  - *Adobe Photoshop (.psd) and Illustrator (.ai)*
  - *Freehand (.fh11)*
  - *Scalable Vector Graphics (.svg)*
  - *Paintbrush (.pcx)*
- Search the Web for software to manipulate unknown image formats



Understanding Graphics File Formats (3 of 3)

- Imagine that you are an investigator, and you have a graphic file in a non-standard format your workstation tools can not identify the format and you suspect that file has crucial evidence…what can you do?
- Solution can be:
- Some websites give some help such as www.garykessler.net/library/file_signs.html
- www.webopedia.com

Understanding Digital Photograph File Formats

- Witnesses or suspects can create their own digital photos
- These photos can be created using , smart phones, digital cameras and closed- circuit television surveillance.
- Knowing such photos format can help the investigators on their evidences search, cases like child pornography.
- Most cameras produce Raw or EXIF photos formats.
  - **Raw file format**
    - Referred to as a digital negative
    - Typically found on many higher-end digital cameras
  - Sensors in the digital camera record pixels on the camera's memory card
  - Raw format maintains the best picture quality.

Understanding Digital Photograph File Formats

- Examining the raw file format (cont'd)
  - The biggest disadvantage is that it's proprietary
    - And not all image viewers can display these formats
  - The process of converting raw picture data to another format is referred to as **demosaicing**

Understanding Digital Photograph File Formats (7 of 8)

- Examining the Exchangeable Image File format (cont'd)
  - With tools such as Autopsy and Exif Reader
    - You can extract metadata as evidence for your case
  - EXIF JPEG file metadata requires a particular program such as EXIF Reader (e.g *IrfanView* tool, *Magnet Forensics AXIOM* has a built-in EXIF viewer

Understanding Digital Photograph File Formats

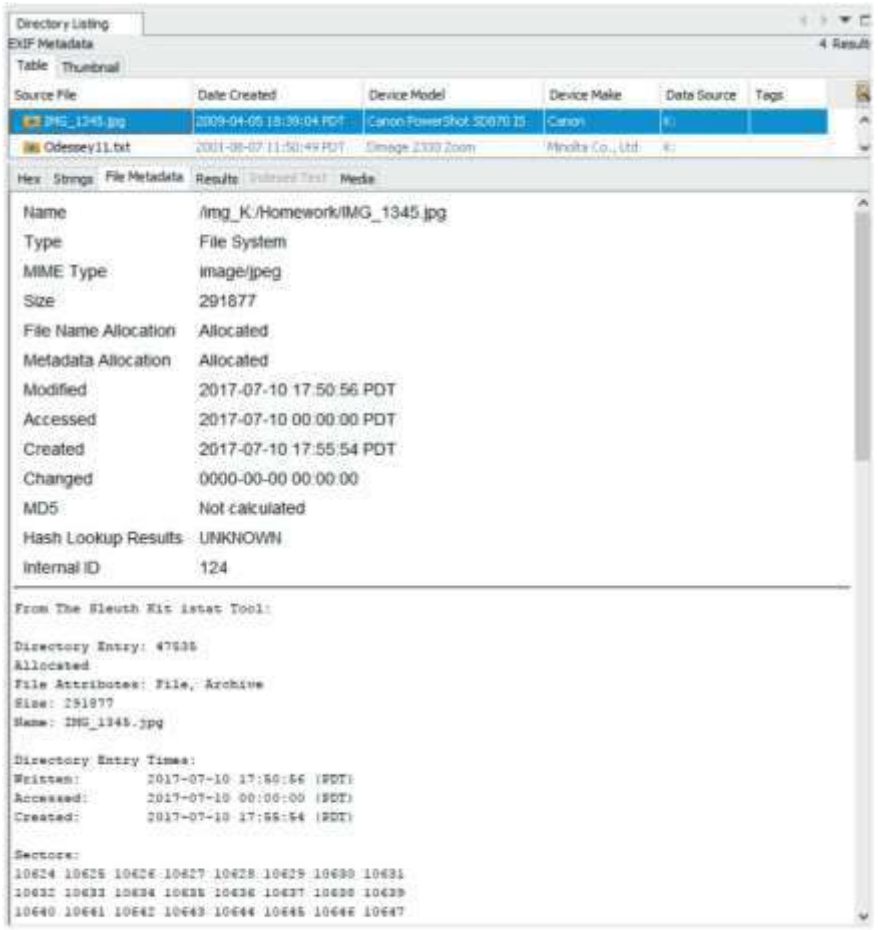
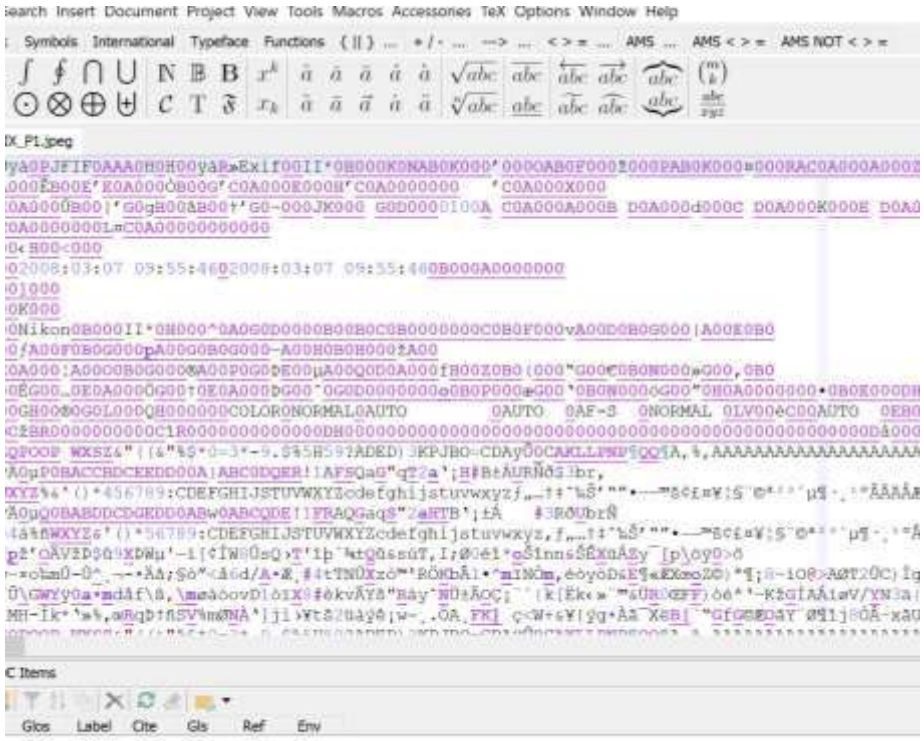
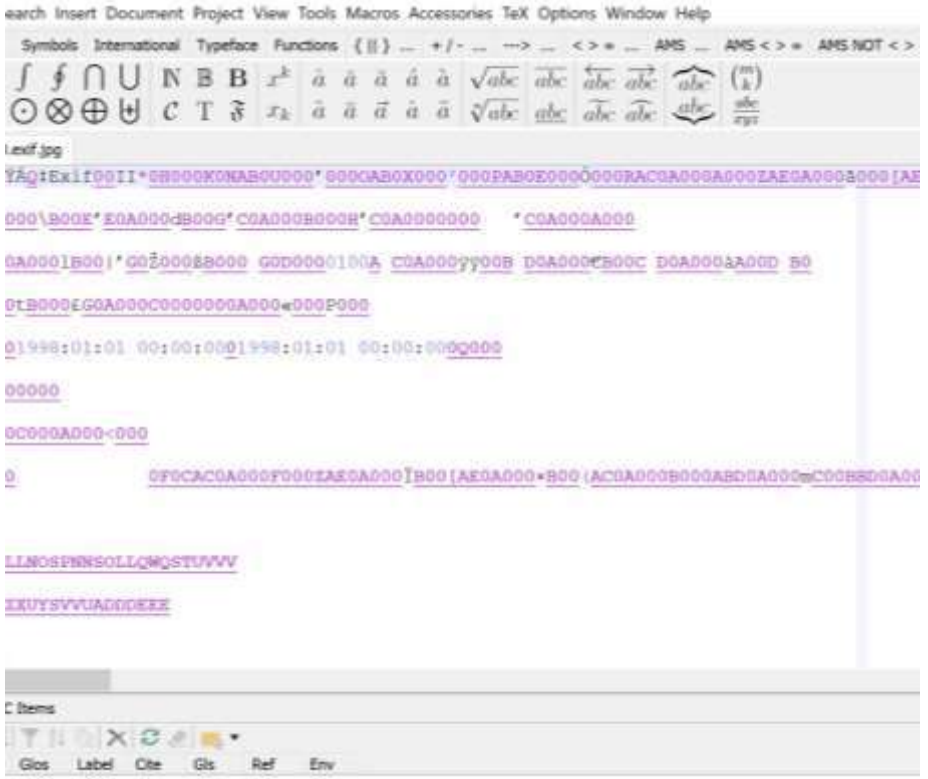


Figure 8-4 Autopsy displaying metadata from an Exif JPEG file

Source: *www.sleuthkit.org*

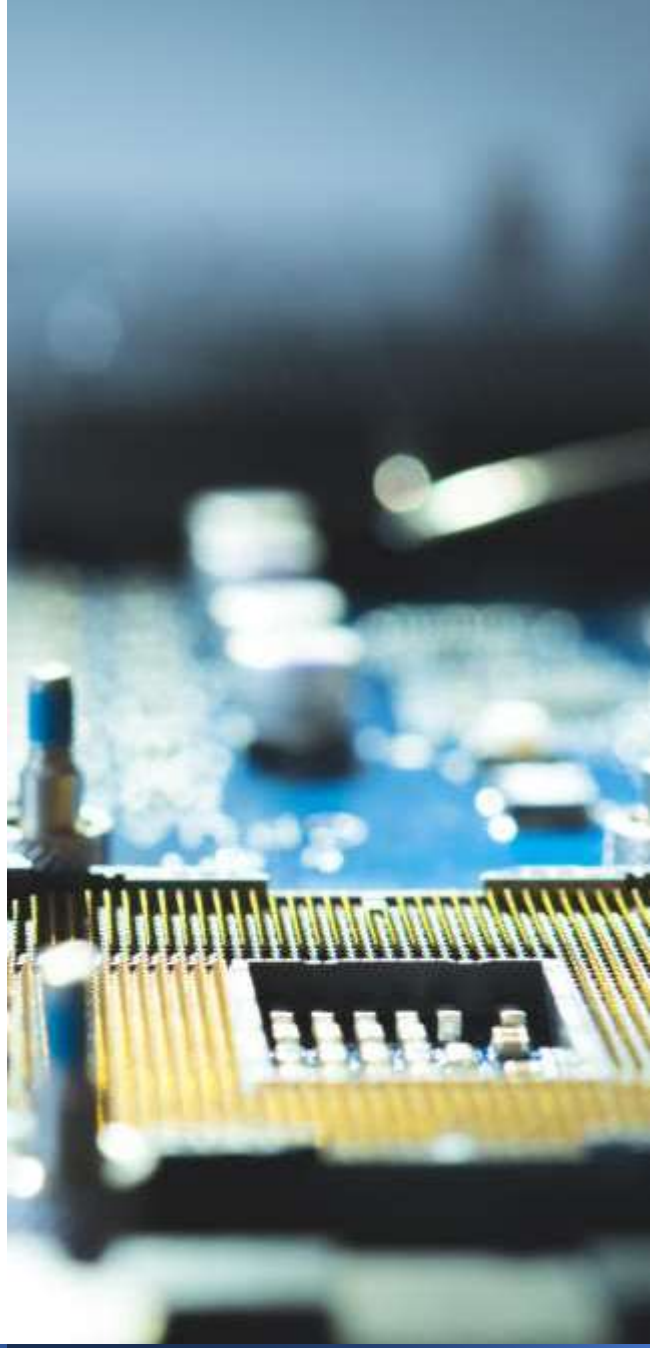
Differences of EXIF and JPEG Header Info





Understanding Data Compression

- Most graphics file formats compress their data
  - GIF and JPEG
- Others, like BMP, do not compress their data
  - Use data compression tools for those formats
- **Data compression**
  - Coding data from a larger to a smaller form
  - Compression Scheme Types
    - Lossless compression and
    - lossy compression



Lossless and Lossy Compression

- **Lossless compression**
  - Reduces file size without removing data
  - Eg. PNG, reduce file size with Lossless Compression,
  - Uses Mathematical formulas to represent data in a file.
  - Based on Huffman or Lempel-Ziv-Welch (LZW) coding,
  - Each code uses a code to represent redundant bits of data.
  - Eg. 1 byte can specify 200 bytes instead of specifying 200 bytes.
  - Utilities: WinZip, PKZip, StuffIt, and FreeZip
- **Lossy compression**
  - Permanently discards bits of information
  - **Vector quantization (VQ)**
    - Determines what data to discard based on vectors in the graphics file
  - Utility: Lzip

Locating and Recovering Graphics Files

- Operating system tools are
  - Time consuming
  - Results are difficult to verify
- Digital forensics tools:
  - Used to analyze graphics files based on the information on the graphics files.
  - Each graphic file has a header that identify the file format
  - Header are complex.
  - Should not remember the format but it is advised to compare the good file header with suspect file.
  - Eg. If you have an image that you suspect is a jpeg but can not display with a bitmap graphic program, do compare it with a header of a known jpeg file to decide if the header is altered.
  - Before doing this comparison, you might need to test if the suspect graphic file header has some damage parts or overwritten with other data.
  - This damage header needed to be repaired by rebuilding the file header before doing the forensics analysis.

Identifying Graphics File Fragments

- If a graphic files is fragmented across the areas on the disk, one needs to recover these fragments before re-creating the file.
- Recovering any type of files fragments is called **Carving or salvaging** (save good parts from a damage object).
- To carve a graphic files data from file slack space and free space, one should be familiar with the data pattern of the known graphic file types.
- Many Digital forensics tools
  - Can carve from file slack and free space.
  - Help identify image files fragments and put them together.
  - Examples of these Forensics tools are :
    - X-Ways forensics, OSForensics, FTK and Encase

Repairing Damaged Headers (1 of 5)

- When examining recovered fragments from files in slack or free space
  - You might find data that appears to be a header
- If header data is partially overwritten, you must reconstruct the header to make it readable
  - By comparing the hexadecimal values of known graphics file formats with the pattern of the file header you found Each graphics file has a unique header value

Repairing Damaged Headers (2 of 5)

- Example:
  - A JPEG file has the hexadecimal header value FFD8, followed by the label JFIF for a standard JPEG or Exif file at offset 6

Repairing Damaged Headers (3 of 5)

- Exercise:
  - Case details:
  - Two cousins; tom Johnson and Jim Shu. Jim Shu has been terminated. Bob Aspen is an external contractor and investor who gets strange email from Terry Sadler about Jim Shu's new project. Chris Robinson (President of the company) to inquire about this new project. Chris also forward this email to the IT consultant to examine the attachment of the email.
  - The IT Consultant examines the attachment and the result shows some hidden data.
  - The following Slides shows the emails exchanged.

Repairing Damaged Headers (4 of 5)

Chris Robinson

From: Bob Aspen <b_aspen@aol.com>
Sent: Monday, July 10, 2017 3:32 PM
To: cr-superior@outlook.com
Subject: FW: More info

Chris,
I got cc'd this odd message from Terry Sadler.
Do you have any projects that might need some capital investment?
Bob

-----Original Message-----
From: Terry Sadler [mailto:t_sadler@zoho.com]
Sent: Monday, July 10, 2017 3:28 PM
To: Jim Shu
Subject: Re: More info

Do you have a name for the project?

On 7/10/2017 3:04 PM, Jim Shu wrote:
> Terry,
>
> Here a few more photos from Tom.
>
> How much you willing to pay for these?
>
> Jim
>

Figure 8-5 An e-mail from Terry Sadler

Repairing Damaged Headers (4 of 4)

Chris Robinson

From: Tom Johnson <1060waddisonst@gmx.us>
Sent: Monday, July 10, 2017 2:40 PM
To: Jim Shu
Subject: You might be interested

Jim,

I had a tour of the new kayak factory. I think we can run with this to the other party interested in competing. I smuggled these files out, they are JPEG files I edited with my hex editor so that the email monitor won't pick up on them. So to view them you have to re-edit each file to the proper JPEG header of offset 0x FF D8 FF E0 and offset 6 of 4A. Then you have to rename them to a .jpg extension to view them.

Tom

Figure 8-6 The e-mail with attachments IT found

Searching for and Carving Data from Unallocated Space

- By looking the case above and the first email:
- First, we need to think about what to look for in the email and the email server.
- The images sent are similar and matching.
- Check the time and dates of the exhanged emails
- When second email was examined the followings are found the following piece of information.
  - Jim has a tour of the Kayak factory,
  - Another company might be interested in competing
  - Jim Shu, smuggled some jpg files since he altered
  - ‚Jim Shu gave instruction to how to reedit the digital photos and add the .jpeg extension

Rebuilding the Header

- Locate the noncontiguous clusters that make up a deleted file
- Steps
  - Locate and export all clusters of the fragmented file
  - Determine the starting and ending cluster numbers for each fragmented group of sectors
  - Copy each fragmented group of sectors in their correct sequence to a recovery file
  - Rebuild the file's header to make it readable in a graphics viewer
  - Add a .txt extension on all the copied sectors

Searching for and Carving Data from Unallocated Space

- Steps
  - Planning your examination
  - Searching for and recovering digital photograph evidence
    - Use Autopsy for Windows to search for and extract (recover) possible evidence of JPEG files
    - False hits are referred to as **false positives**

Activities

Searching for and Carving Data from Unallocated space: Do the activities on page 351 -355

- **Planning Your Examination**
- **Searching for and Recovering Digital photograph Evidence**

Rebuilding File Headers: Do the activities on page 356 -360

Identifying Unknow file format: Introduction

- With the growing and changes in Technology and digital graphics you will find more unfamiliar graphics file format.
- Suspect might use older system and program to create unfamiliar formats
- Therefore, part of the investigator job is to research the old and new file format and how data is stored on them.
- Many web sites list information about the “file format” and “file type”.
- ***Webopedia*** is a good web source to search about different file format like the TGA file format.
- Should always search for latest web sites that list the new file extension. It is good to change the search keyword when using the search engine.
- One of the nonstandard graphics file format is “XIF”.
- Google search engine can help in looking for such file format.

Identifying Unknow file format: Introduction

- ***Nuance Paperport*** tool is a scanning tools that produces images in the XIFF format. This image is a drive version of the TIF file format.
- The ***Nuance Paperport*** has a free view utility for XIFF files
- Another tool will be ***Solveusoft file view pro***
- Therefore there are many web sites that have info about images and graphic , these web sites can be identified
- *-www.fileformat.info/format/all.html*
- *-http://extension.informer.com/*

Identifying Unknow file format: Analyzing Graphic File Header

- Analyzing graphic file header is done for a new or a unique file type that forensics tools don't recognize it.
- The simplest way is to use a hexadecimal editor tool such WinHex.
- Record the hexadecimal values in the header and use them for defining the Graphic file type.
- Suppose you encounter an XIF file, and no much information on it is available.
- Need to search for the hidden or deleted XIF files by building your own search string. For example, use the WinHex editor and read the header of TiF and XIF and compare the outcome.

Identifying Unknow file format: Analyzing Graphic File Header

- The TIF is a well-known file format for transmitting faxes and printing publications.
- TIF files header start at offset "0" with hexadecimal 49 49 2A, which translate to the letter "II" in ASCII.
- The first 3 bytes of an XIF file are the same as TIF file followed by other hexadecimal values.
- The XIF start with Hexadecimal values 49 49 2A and has offset of 4 bytes of

5C 00 00 20 65 58 74 65 6E 64 65 64 20 03
See the textbook example

- Knowing the header of the TIF you may detect the XIF file.
- For more information you may check the following :
  - www.fileformat.info/info/mimetype/image/vnd.xiff/index.html

Identifying Unknow file format: Tools for Viewing Images

- So far for this chapter we have been learning on:
- *Recognizing File format, using compression techniques, Salvaging header information, Recovering graphics files, saving your modification*
- It is always good to find the best image viewer to finish the forensic process.
- For GIF and JPEG (often used in the Internet investigation), many GUI forensics tools are available.
- For uncommon ones, such as PCX integrated viewer tools might be of a good help.
- Not knowing the format might prevent you from finding the critical evidences in any case.

Identifying Unknow file format: Understanding Steganography in graphics files

- When you read some graphics files in an image viewer, They might not seem to contain information related to the investigation case.
- In any case, someone might have hidden information inside an image, using a ***data hidden techniques, called Steganography***
- Steganography hides information inside image files
  - An ancient technique
- Ancient Greek use different method for covering/hiding data e.g.
- " message hidden beneath the hair, the shave the hair to show messages" , not efficient

Identifying Unknow file format: Understanding Steganography in graphics files

- Two major forms of steganography: insertion and substitution
- Insertion
  - Hidden data is not displayed when viewing host file in its associated program
    - You need to analyze the data structure carefully to reveal the hidden message.
  - Example: Web page
  - You may create a web page with Html. You might display images and text in a web browser without revealing the HTML code
  - To detect hidden text, you need to compare the file display and what the file contains.

The Other type of Steganography is substitution:

Here you substitute or replace bits of the host file with other bits of the data

Example: with Bitmap image file, you might replace bits used for pixels and colors with hidden data.

To avoid detection you need substitute only bits that can not make any changes on the image.

For example: if you use 8 bits of data, containing info about the color each display on the screen.

Normally, the bits are prioritized from left to right:

Identifying Unknow file format: Understanding Steganography in graphics files

- Normally, the bits are prioritized from left to right:

Example: take 11101100

Most Significant Bit (MSB) is “first bit on the left”

Least Significant Bit (LSB) is “last bit on the right”

Example :of an image being altered by embedding a secret message into a picture you alter the last two bits of four pixels, by breaking the binary form into section of two and insert the bits on the last 2 bits, see below table:

Original Pixel	Altered Pixel	MSB	LSB
1010 1010	1010 1001	x	
1001 1101	1001 1110	x	x
1111 0000	1111 0011	x	x
0011 1111	0011 1100	x	x

Identifying Unknow file format:
Using Steganalysis Tools

- You may use several Steganalysis tools (Steg Tools), to detect, decode, and record hidden data, even in file that have been renamed to protect their contents.
- The Steg tools can also detect the variation of an image.
- The steg tool can identify the alternation with the file header.

Understanding Copyright Issues With Graphics

Please read this section page 367-368