CSE 469: Computer and Network Forensics

Topic 5: Image Forensics

Dr. Mike Mabey | Spring 2019

Forensics for Graphics Files

- Types of graphics file formats
- Type of data compression
- How to locate and recover graphics files

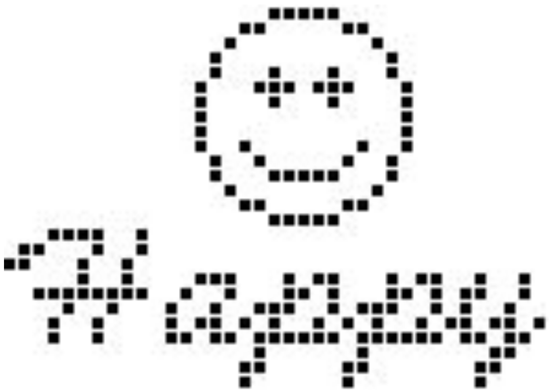
Image Basics

- Pixel:
  - Picture element.
  - Smallest unit that can be displayed on a screen.

- Simplest graphics are black and white:
  - 0 – white
  - 1 – black

Simple Graphics

```
00000000000000000011110000000000000000
00000000000000001100001100000000000000
00000000000000010000000010000000000000
00000000000000100000000001000000000000
00000000000000100010001001000000000000
00000000000001000111011100100000000000
00000000000001000010001000100000000000
00000000000001000000000000100000000000
00000000000001000000000000100000000000
00000000000001001000000100100000000000
00000000000000100100001001000000000000
00000000000000100011110001000000000000
00000000000000010000000010000000000000
00000000000000001100001100000000000000
00000000000000000011110000000000000000
00011110010000000000000000000000000000
01100010010000000000000000000000000000
11000100100000000000000000000000000000
00000100100001110001011000101100100100
00111111110010010001101000110101100100
00001001000100100111001011100101001000
00010010000101101010010101001011011010
00010010000110110111111011111101101100
00000000000000000100000010000000011000
00000000000000001100000110000000110000
00000000000000001000000100000000100000
```

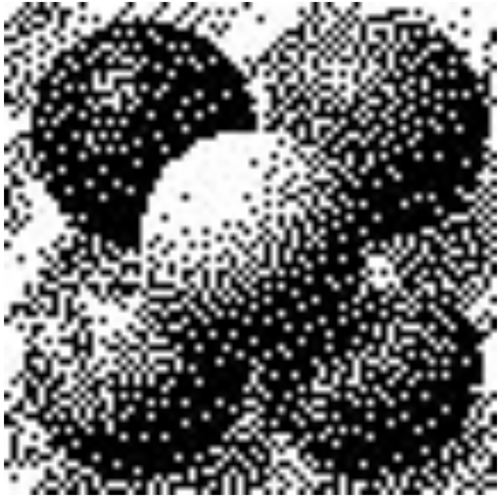


Bit Depth

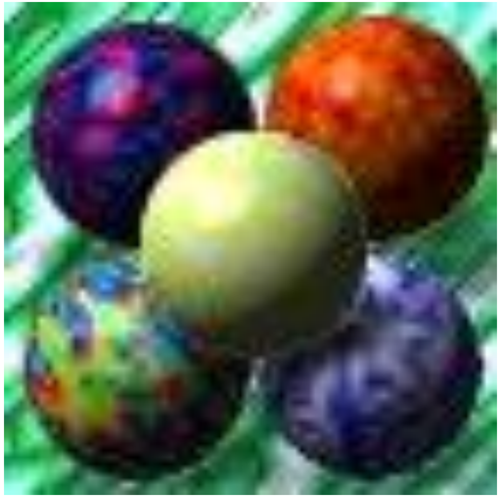
- Number of bits per pixel:
  - 1 bit – black and white
  - 4 bits – 16 colors (2^4)
  - 8 bits – 256 colors (2^8)
  - 16 bits – 65,536 colors (2^{16})
  - 24 bits – 16,777,216 colors (2^{24})

- Bit depth controls image file size:
  - Higher the bit depth = larger file

Bit Depth Samples



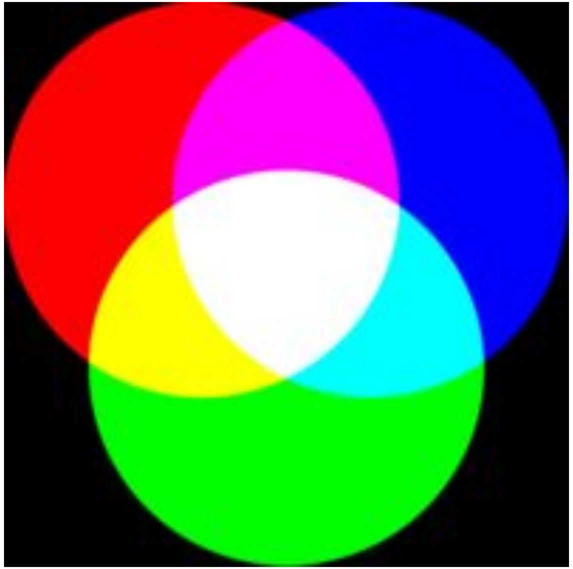
1 bit
781 bytes



16 bits
11,982 bytes

RGB Color Model

- Red – Green – Blue
- Additive model combines varying amounts of these 3 colors:



RGB Value Storage

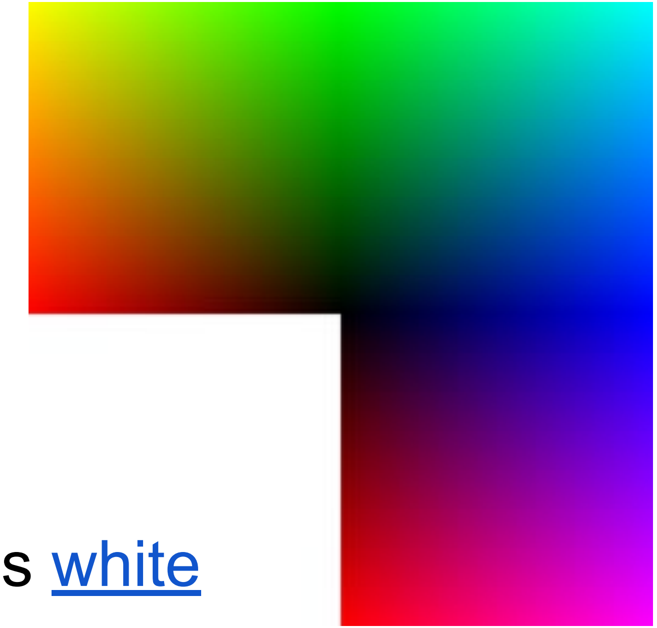
- Individual pixels represented in memory as a
  - Red value
  - Green value
  - Blue value
- Values represent **intensity**:
  - If red is more intense, the color perceived is towards the red.
- 24-bit pixel value means:
  - 8 bits for each RGB value
    - Values expressed as 0 – 255
  - 256 possible values for each primary color

Image Basics

(0, 255, 0) is green

(255, 255, 0) is yellow

(0, 255, 255) is cyan



(255, 0, 0) is red

(0, 0, 255) is blue

(0, 0, 0) is black
(255, 255, 255) is white

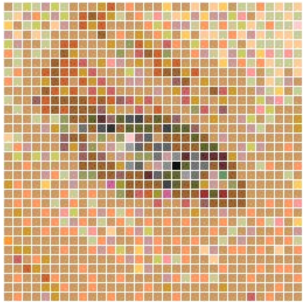
(255, 0, 255) is magenta

Recognizing a Graphics File

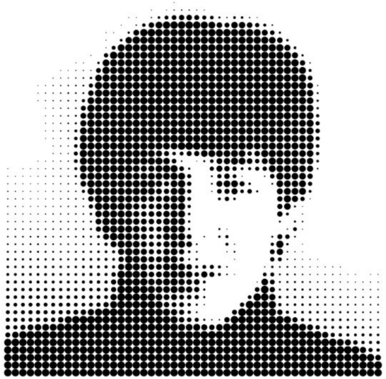
- Contains digital photographs, line art, three-dimensional images, and scanned replicas of printed pictures.
  - Bitmap images: collection of dots
  - Vector graphics: based on mathematical instructions
  - Metafile graphics: combination of bitmap and vector

Bitmap vs Raster Images

- Bitmap images
  - Grid of individual pixels



- Raster image
  - Pixels are stored in rows
  - Better for printing

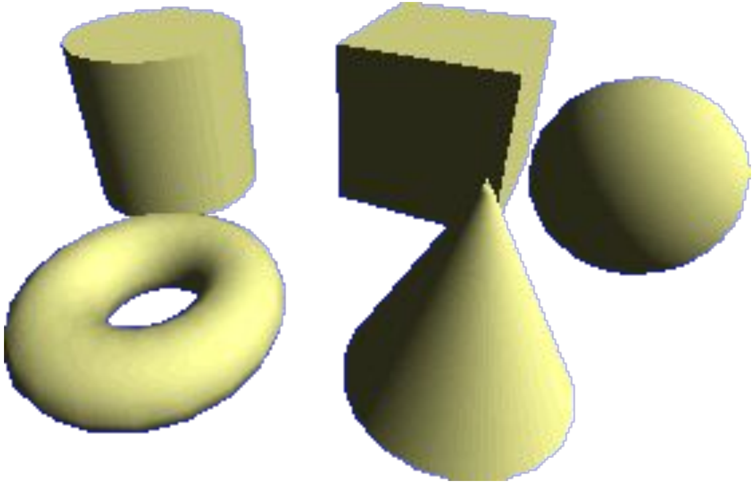


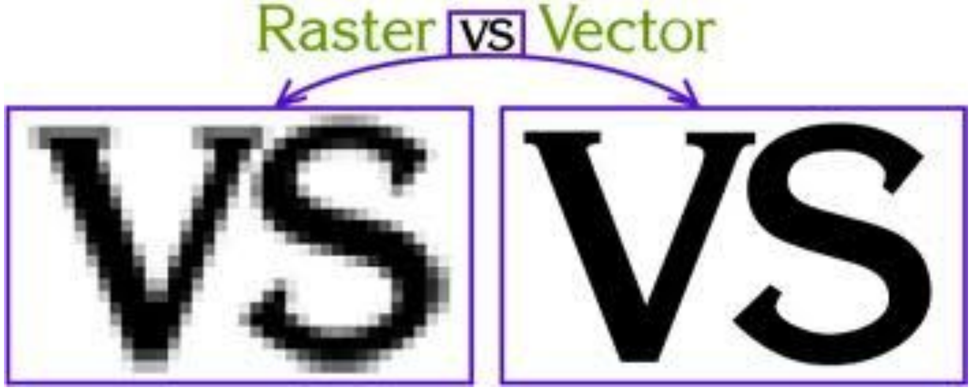
Bitmap and Raster Images: Quality

- Quality is measured in two dimensions:
  - Resolution:
    - Number of pixels per unit of measurement
      - dpi = dots (pixels) per inch
    - Higher resolution equals sharper image
  - Bit Depth:
    - Number of color bits used per colored pixel
      - 1 bit = 2 colors
      - 4 bits = 16 colors
      - 32 bits = 4,294,967,296 colors

Vector Graphics

- Characteristics:
  - Lines and geometric primitives instead of dots.
  - Store only the calculations for drawing lines and shapes.
  - For example: CorelDraw, Adobe Illustrator, Inkscape.





Vector Graphics

- Example of vector data for a circle:
  - Radius
  - Center
  - Line style and color
  - Fill style and color
- Advantages of vector system:
  - Smaller file sizes
  - Resizing does not change image
  - Easy modification of parameters
    - Moving, Scaling, Rotating and Filling

Metafile Graphics

- Combine raster and vector graphics
- Example: scanned photo (bitmap) with text (vector)
- Share advantages and disadvantages of both types
    - When enlarged, bitmap part loses quality

Graphics File Formats (1)

- Standard bitmap file formats:
  - 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)

Graphics File Formats (2)

- Nonstandard graphics file formats:
  - Targa (.tga)
  - Raster Transfer Language (.rtl)
  - Adobe Photoshop (.psd) and Illustrator (.ai)
  - Freehand (.fh9)
  - Scalable Vector Graphics (.svg)
  - Paintbrush (.pcx)

Image Data Compression

- Some image formats compress their data:
  - GIF, JPEG, PNG
- Others, like BMP, do not compress their data:
  - Use data compression tools for those formats.
- Data compression:
  - Coding of data from a larger to a smaller form.
  - Types:
    - **Lossless** compression and **lossy** compression

Lossless Compression (GIF, PNG)

- Reduces file size without removing data.
- Based on Huffman or Lempel-Ziv-Welch coding:
  - For representing redundant bits of data.
  - 200 red bytes represented as:
    - 1 byte for red color
    - 1 byte for specification of 200 red bytes
- Utilities: WinZip, PKZip, StuffIt, and FreeZip.

Lossy Compression (JPEG)

- Permanently discards bits of information
- Vector quantization (VQ)
  - Determines what data to discard based on vectors in the graphics file
- Utility: Lzip

Lossless vs Lossy Compression

- Lossless compression produces **an exact replica of the original data** after it has been uncompressed, whereas lossy compression typically produces **an altered replica of the data**.

Digital Camera File Formats

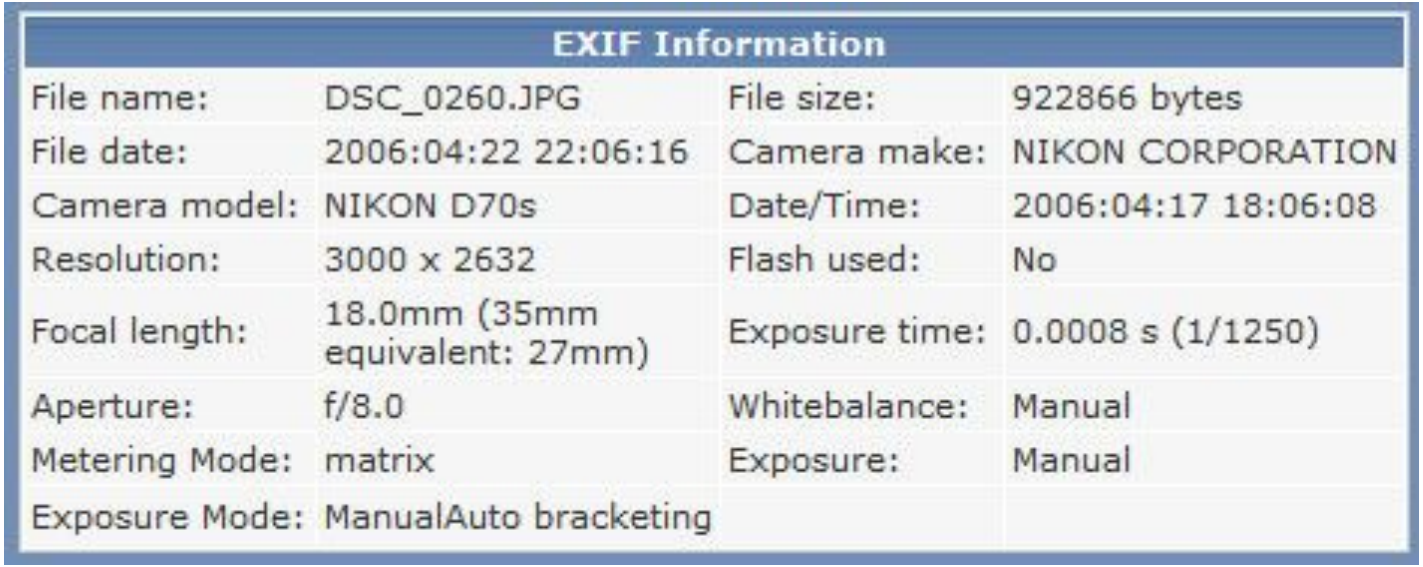
- Witnesses or suspects can create their own digital photos:
  - Identify victims
  - Discover additional evidence
  - Completeness and credibility

Examining the Raw File Format

- Raw file format:
  - Referred to as a digital negative.
  - Typically found on many higher-end digital cameras.
- Sensors in the digital camera simply record pixels on the camera’s memory card.
- Raw format maintains the **best picture quality**.
- The biggest disadvantage is that it’s **proprietary**:
  - Not all image viewers can display these formats.
- The process of converting raw picture data to another format is referred to as ***demosaicing***.

Examining EXIF Format

- Exchangeable Image File (EXIF) format:
  - Developed by JEIDA as a standard for storing metadata in JPEG and TIFF files.
  - Stores **metadata** at the beginning of the file:
    - Investigators can learn more about the type of digital camera and the environment in which pictures were taken.



EXIF Information			
File name:	DSC_0260.JPG	File size:	922866 bytes
File date:	2006:04:22 22:06:16	Camera make:	NIKON CORPORATION
Camera model:	NIKON D70s	Date/Time:	2006:04:17 18:06:08
Resolution:	3000 x 2632	Flash used:	No
Focal length:	18.0mm (35mm equivalent: 27mm)	Exposure time:	0.0008 s (1/1250)
Aperture:	f/8.0	Whitebalance:	Manual
Metering Mode:	matrix	Exposure:	Manual
Exposure Mode:	ManualAuto bracketing		