

## Uncovering Steganography (Hidden Information)



[www.cybersciencelab.com](http://www.cybersciencelab.com)

**A Program of the National Institute of Justice**

*This is to be used as an informational guide only.  
Please refer to our disclaimer at [www.cybersciencelab.com](http://www.cybersciencelab.com).*



## Uncovering Steganography

**Indications that steganography (hidden information) may have been used:**



- The presence of steganography embedding software [www.stegoarchive.com](http://www.stegoarchive.com)
- Multiple copies of identical files including: **Images, Audio, Video, Executables, Text**  
If identical files are found, perform the following analysis:
  - >> **FOR 8-BIT GRAPHIC IMAGE FILES:** Compare each of the images' color palettes for differences
  - >> **FOR ALL FILES:** Perform a bit analysis using a hex editor that will compare the two files for differences
- The existence of 24-bit bitmap files
- Files that contain less data in comparison to their size

- Files that do not fit the suspect's profile
- Log files that indicate the transfer of many graphic image files
- Poor quality graphic image files (i.e., noise/distortions)
- Numerous emails containing random graphic image files as attachments
- The existence of many grayscale graphic image files

*If instances of steganography have been discovered, further analysis can be accomplished by utilizing a steganography detection tool*