Computer Forensics

Week 7: Recovering Graphics Files

Kumi University
Lecturer: Lemi Agrey Oliver
codingissweet@gmail.com

Content

- Overview of graphic file recovery
- Recognizing a Graphics File
- Understanding Bitmap and Raster Images
- Understanding Digital Photograph File Formats
- Steps in Searching for and Recovering Digital Photograph
- Understanding Data Compression
- Understanding Steganography in Graphics Files
- Understanding Copyright Issues with Graphics

Overview of graphic file recovery

- Recovering Graphics Files is a crucial aspect of digital forensics, especially when investigating cases involving image manipulation, distribution of illicit material, or identifying visual evidence
- The process of recovering graphics files in a forensic context involves several steps to ensure the integrity and admissibility of the evidence.
- These steps includes;
- Identifying the storage devices (such as hard drives, memory cards, or USB drives) that may contain the graphics files of interest.
- Using forensic tools to create a forensic image of the storage media. This ensures that the original data remains unchanged and can be analyzed without compromising its integrity.

Overview of graphic file recovery+

- Employing file carving techniques to recover graphics files that may have been deleted, damaged, or partially overwritten. File carving involves searching for file signatures or patterns in unallocated space on the storage media to reconstruct files.
- Examining the metadata embedded within graphics files to gather additional information about their creation, modification, and location. Metadata can provide valuable context for forensic investigations.
- Conducting keyword searches on the acquired data to locate relevant graphics files. Keywords may include file names, metadata, or other identifiers related to the graphics.

Overview of graphic file recovery++

- Verifying the integrity of the recovered graphics files through cryptographic hash verification and validation processes. This ensures that the recovered data has not been altered or tampered with since acquisition.
- Documenting the forensic process, including the steps taken, tools used, and findings. Prepare a detailed forensic report that presents the recovered graphics files as evidence in a clear and concise manner.
- Adhering to legal and procedural requirements throughout the forensic investigation process. Ensure that the recovered graphics files are handled and presented in a manner that maintains their admissibility in court.

Recognizing a Graphics File

- Graphics files encompass various types of visual data, including digital photographs, line art, 3D images, and scanned copies of printed pictures.
- Programs like Microsoft Paint, Adobe Photoshop, or Gnome GIMP are commonly used for creating or editing images.
- Graphics programs generate three main types of graphics files: bitmap, vector, and metafile.
- Bitmap images consist of pixels arranged in a grid pattern, while vector graphics are based on mathematical instructions defining shapes like lines and curves.
- Metafile graphics combine aspects of bitmap and vector images.

Recognizing a Graphics File+

- Two primary types of software for working with graphics files are graphics editors and image viewers.
- Graphics editors enable the creation, modification, and saving of bitmap, vector, and metafile graphics.
- Image viewers allow opening and viewing of graphics files without altering their content.
- Graphics files can be saved in various formats like BMP, GIF, and JPEG, each with unique characteristics such as color depth and compression.
- Converting graphics files between formats can affect image quality.

Understanding Bitmap and Raster Images

- Bitmap and raster images consist of grids of pixels, known as picture elements, arranged in rows for easy printing.
- Resolution determines the level of detail displayed on a monitor, which depends on hardware and software factors.
- Monitors can support various resolutions, with higher resolutions yielding sharper images.
- The quality of displayed images is influenced by the capabilities of the video card, including its memory and electronics.
- High-resolution images have smaller pixels compared to low-resolution ones.

Understanding Bitmap and Raster Images+

- Software, such as drivers and image editing programs, also impacts image quality.
- Professionals prefer software supporting high resolutions for better control over bitmap image display.
- Enlarging bitmap images, especially those with low resolution, often results in quality loss.
- The number of colors displayed on a monitor affects image quality, with different bits per pixel supporting varying color ranges.
- Bitmap and raster files utilize the available color palette, but saving them may alter resolution and color, depending on the original file and format compatibility.

Understanding Vector Graphics

- Vector graphics employ lines instead of dots, distinguishing them from bitmap and raster images.
- In vector files, only calculations for drawing lines and shapes are stored, not actual images, resulting in smaller file sizes.
- Vector graphics programs like CorelDRAW and Adobe Illustrator use these calculations to render images, offering scalability without loss of quality.
- Enlarging a vector graphic involves mathematical computation rather than simply stretching pixels, ensuring consistent image quality at any size.

Understanding Metafile Graphics

- Metafile graphics integrate aspects of both raster and vector graphics, combining characteristics from each type.
- For instance, if you combine a scanned photograph (bitmap image) with vector drawings like text or arrows, you produce a metafile graphic.
- Despite possessing qualities of both bitmap and vector files, metafile graphics inherit limitations from both types.
- Enlarging a metafile graphic may result in the loss of resolution in the bitmap portion while maintaining sharpness and clarity in the vector-drawn areas.

Understanding Graphics File Formats

- Graphics files are typically created and edited in graphics editors like Microsoft Paint, Adobe Freehand MX, Adobe Photoshop, or Gnome GIMP.
- Some editors specialize in vector graphics only, while others support both vector and bitmap formats.
- Most graphics editors allow saving files in various standard graphics file formats.
- Common bitmap formats include Portable Network Graphic (.png), Graphics Interchange Format (.gif), Joint Photographic Experts Group (.jpg or .jpeg), Tagged Image File Format (.tif or .tiff), and Windows Bitmap (.bmp).
- Standard vector formats encompass Hewlett-Packard Graphics Language (.hpgl) and AutoCad (.dxf).

Understanding Graphics File Formats+

- Less common, proprietary, newer, and obsolete formats also exist, such as Targa (.tga), Raster Transfer Language (.rtl), Photoshop (.psd), Illustrator (.ai), Freehand (.fh11), Scalable Vector Graphics (.svg), and Paintbrush (.pcx).
- Standard formats are preferable for digital forensics due to compatibility with most graphics programs.
- Nonstandard formats may require investigative skills to identify and specialized tools for viewing.
- To identify a file format or find a program for viewing nonstandard graphics files, web searches or dictionary websites like www.webopedia.com can be helpful.

Understanding Graphics File Formats++

- For instance, if encountering a file with a .tga extension, one can consult resources like www.garykessler.net/library/file_sigs.html or perform searches on sites like www.webopedia.com to understand the format and find suitable viewing tools.

Understanding Digital Photograph File Formats

- Digital photographs are prevalent in digital forensics, easily created by witnesses or suspects using smartphones, cameras, or surveillance systems.
- Forensic investigators often need to analyze digital photos, such as those captured by witnesses to accidents or related to crimes like child pornography.
- Understanding the data structures of graphics files can provide crucial evidence in investigations.
- Knowledge of how digital photos are created and store unique information enhances credibility when presenting evidence.
- Most digital cameras produce photos in raw or Exif format, which will be further explained.

Examining the Raw File Format

- The raw file format, often termed as a digital negative, is commonly used in high-end digital cameras.
- Unlike other formats, raw files contain unprocessed data directly captured by the camera's sensors, preserving the highest picture quality.
- However, raw files are proprietary and not all image viewers can display them, posing a challenge from a digital forensics perspective.
- To view raw graphics files, specialized viewing and conversion software from the camera manufacturer may be required.
- Each manufacturer provides its own software with algorithms to convert raw data to standard formats like JPEG or TIF.
- The process of converting raw picture data to another format is known as demosaicing.

Examining the Exchangeable Image File Format

- The Exchangeable Image File (Exif) format is widely used for storing metadata in digital photographs, developed by the Japan Electronics and Information Technology Industries Association (JEITA).
- Exif files contain information about the device used (such as model, make, and serial number) and settings (like shutter speed, focal length, resolution, date, and time) embedded within the graphics file.
- Most digital devices store graphics files as Exif JPEG files, and if GPS capability is present, latitude and longitude location data may also be recorded.
- Examining Exif metadata can provide insights into the type of digital device and the circumstances under which photos were taken, aiding investigations.

Examining the Exchangeable Image File Format

- Special programs like Exif Reader, IrfanView, or Magnet Forensics AXIOM are required to view Exif metadata.
- Exif is an enhancement of JPEG and TIF formats, modifying the file's beginning to allow metadata insertion, unlike standard JPEG or TIF files.
- Differences between Exif and standard JPEG file headers are evident, with Exif files containing additional metadata.

Understanding Data Compression

- Graphics file formats like GIF and JPEG often employ data compression to conserve disk space and decrease transmission time.
- Unlike formats such as BMP, which compress data inefficiently or not at all, compression tools can be utilized to condense data and diminish file size.
- Data compression involves encoding data from a larger form to a smaller form, a process utilized by graphics files and most compression tools.
- Two primary data compression schemes are employed: lossless and lossy compression, each with distinct methods and implications for image alteration.
- Understanding these compression schemes is crucial for comprehending the effects of image modification.

Lossless Compression

- **Lossless compression** is a class of data compression algorithms that allows the original data to be perfectly reconstructed from the compressed data. Lossless compression methods are reversible. [2]
- Reduces file size without removing any data, ensuring that all information is restored upon decompression.
- Utilized in file formats like GIF and Portable Network Graphics (PNG), employing algorithms such as Huffman or Lempel-Ziv-Welch (LZW) coding to represent data mathematically.
- Algorithms use codes to represent redundant bits, significantly reducing storage requirements while maintaining data integrity.

Lossy Compression

- In information technology, lossy compression or irreversible compression is the class of data compression methods that uses inexact approximations and partial data discarding to represent the content. [4]
- Permanently discards bits of information in the file to compress data, resulting in a reduction in image quality.
- Although some discarded bits are redundant, others are not, impacting image quality, especially when printing on high-resolution printers or resizing images.
- Formats like JPEG employ lossy compression, automatically reapplying compression when saving the file, which further reduces image quality.

Lossy Compression+

- Vector quantization (VQ) is another form of lossy compression, using complex algorithms to determine which data to discard based on vectors in the graphics file.
- While lossless compression utilities include WinZip, PKZip, StuffIt, and FreeZip, lossy compression utilities like Lzip are also available.

Comparison

- Lossless compression ensures an exact replica of the original data after decompression, while lossy compression typically produces an altered replica of the data.
- Lossless compression is preferred when data integrity is paramount, while lossy compression is suitable when reducing file size at the expense of minor data loss is acceptable.

Locating and Recovering Graphics Files

- In digital forensics investigations involving graphics files, locating and recovering all files from the suspect drive is essential, even if they're not in standard graphics formats.
- Built-in tools in some operating systems for recovering graphics files are inefficient and challenging to verify, prompting the use of dedicated digital forensics tools.
- Developing standard procedures for analysis is crucial for consistency and efficiency, allowing other investigators to benefit from collective experience.
- Graphics files contain headers with display instructions, aiding in identifying file formats; comparing suspected file headers with known headers helps determine alterations.

Locating and Recovering Graphics Files +

- Reconstructing fragmented graphics files may be necessary before examining the header, requiring identification of data patterns used in the file.
- Known header information can serve as a baseline for analysis, allowing for comparison and identification of alterations in suspected file headers.
- Repairing damaged headers and rebuilding them enables forensic analysis of graphics files, enhancing investigation techniques.

Identifying Graphics File Fragments

- Identifying fragmented graphics files across disk areas requires recovering all fragments before reconstructing the file, a process known as carving or salvaging.
- Carving involves extracting graphics file data from file slack space and free space, relying on knowledge of data patterns in known graphics file types.
- Many digital forensics programs, such as X-Ways Forensics, OSForensics, EnCase, and FTK, can automatically recognize these data patterns and carve graphics files from slack and free space.
- After recovering file fragments, they are restored for further examination, often utilizing tools like Autopsy and WinHex to copy known data patterns from recovered files and restore this information for viewing.

Repairing Damaged Headers

- When examining recovered fragments from files in slack or free space, damaged header data may be encountered, requiring reconstruction for readability.
- Reconstructing damaged headers involves comparing hexadecimal values of known graphics file formats with the pattern of the recovered header data.
- Each graphics file type has a unique header value, aiding in the identification of partially overwritten headers in file slack or free space.
- For instance, a JPEG file typically begins with the hexadecimal header value FFD8, followed by the label JFIF for a standard JPEG or Exif file at offset 6.

Repairing Damaged Headers+

- In investigations such as intellectual property theft, thorough searches for hidden data are necessary, utilizing tools like Autopsy's search function with hexadecimal search strings to locate known data in various places.

Searching for and Carving Data from Unallocated Space

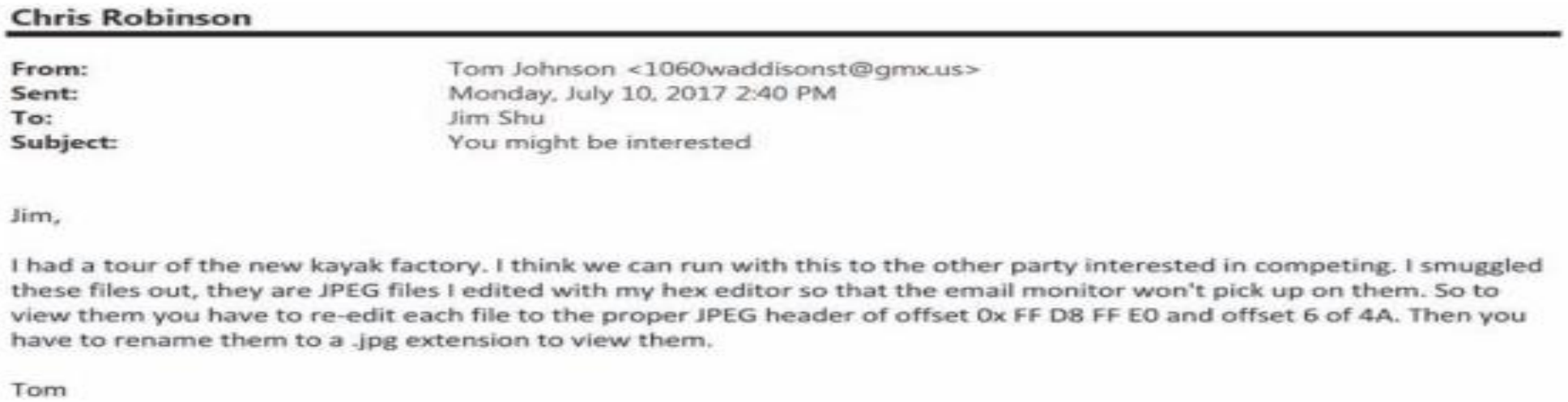
- When searching for information in emails and on mail servers, it's essential to consider what to look for and make assumptions based on available information.
- Analyzing the content of emails can reveal valuable insights, such as matching email addresses with known individuals and examining timestamps to establish the sequence of events.
- For instance, comparing timestamps in emails can suggest the sender of the original message and provide clues about the communication chain.
- Detailed examination of email content, including messages and attachments, can uncover crucial information, such as discussions about sensitive topics or suspicious activities.
- By combining gathered facts with knowledge of file structures, such as JPEG files, investigators can employ specific techniques to validate or refute allegations presented in the emails.

Planning Your Examination[3]

- In an email from Tom Johnson to Jim Shu, Tom instructs to re-edit each file to the proper JPEG header of offset 0xFFD8FFE0 and offset 6 of 4A.
- From this instruction, it can be assumed that any kayak photographs from the email or on the drive contain unknown characters in the first four bytes and the sixth byte, while the seventh, eighth, and ninth bytes retain the original correct information for the JPEG file.
- The difference between a standard JFIF JPEG and an Exif JPEG file lies in the first four bytes, where JFIF format has 0xFFD8FFE0 and Exif format has 0xFFD8FFE1, and the sixth byte indicating the JPEG label as JFIF or Exif.
- Jim Shu mentions 0xFFD8FFE0, indicating a JFIF JPEG format, and instructs to change the sixth byte to 0x4A, representing the uppercase letter "J" in ASCII.

Planning Your Examination[3]+

- Given that the files have been extracted from the mail server, a thorough examination and analysis of all sectors of the drive for deleted files, both allocated and unallocated space, is necessary.
- In the following section, Autopsy for Windows is utilized to search for and recover these JPEG files, ensuring comprehensive examination and analysis.



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 1: Email with attachment[6]

Searching for and Recovering Digital Photograph Evidence

- Searching for digital photograph evidence involves examining various data sources, including email accounts, mail servers, and storage devices, to locate relevant files.
- Deleted files and fragments in allocated and unallocated space should be thoroughly searched to ensure no evidence is overlooked.
- Utilizing forensic tools like Autopsy for Windows facilitates the search process, enabling the recovery of JPEG files and other digital photograph evidence.
- Techniques such as hexadecimal search strings can be employed to identify known data patterns and recover files that may contain valuable evidence.
- Following standard procedures and protocols ensures a systematic and comprehensive approach to searching for and recovering digital photograph evidence in forensic investigations.

Searching for and Recovering Digital Photograph Evidence+

- Autopsy for Windows is utilized in this section to search for and extract potential evidence of JPEG files from the USB drive provided by the EMTS manager.
- The search string "FIF" is employed for this examination, as it is part of the label name of the JFIF JPEG format.
- It's important to note that the presence of other JPEG files on the USB drive may result in false hits, known as false positives.
- False positives require careful examination of each search hit to determine if it's relevant to the investigation.
- Autopsy includes an Exif parser, which aids in the examination and analysis of recovered JPEG files

Steps in Searching for and Recovering Digital Photographs [5]

- Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, type **C08InChp** for the case name, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**. In the Additional Information window, type **C08InChp** for the case number, enter your name for the examiner, and then click **Finish**.
- In the Add Data Source window, leave the default selection **Disk Image or VM file** in the Type of Data Source to Add section, and then click **Next**.
- In the Select Data Source window, click the **Browse** button, navigate to your work folder, click **C08InChp.dd**, and click **Open**. Then click **Next**.

Steps in Searching for and Recovering Digital Photograph[5]+

- In the Configure Ingest Modules window, you can select what type of processing you want, such as a hash lookup or an Exif parser Leave the default selections, click **Next**, and then click **Finish**.
- In the left pane of Autopsy's main window, click to expand **Extracted Content**, if necessary, and then click **EXIF Metadata**. Examine the files displayed in the upper-right pane. As you scroll through these files, notice that the hexadecimal codes haven't been altered. (In the e-mail Tom Johnson sent, the JFIF code was supposedly altered.)

Steps in Searching for and Recovering Digital Photograph [5]++

- Click the **Keyword Search** down arrow at the upper right. To verify that no other codes have been altered, you should check whether a change has been made to the FIF format. In the text box, type **FIF** (all uppercase letters), click the **Exact Match** option, and then click **Search**. There are no results. Next, type **fif** (all lowercase letters), click the **Substring Search** option, and then click **Search**.
- To view the changes made to the file header, you need to see the hexadecimal code. To do this, click the **Hex** tab in the lower-right pane, if necessary, and scroll down through the files until you see “zzzz” in the file header. You should be viewing the gametour2.exe file.

Steps in Searching for and Recovering Digital Photograph [5]+++

- Click the **File Metadata** tab to view the written, accessed, and created dates and times along with the sectors used by the file
- In the search results, right-click the **gametour2.exe** file and click **Extract File(s)**. In the Save As dialog box, navigate to your work folder, type **Recover1.jpg** for the filename, and then click **Save**. Autopsy then creates an Export subfolder of your work folder to store this file. In the confirmation message box, click **OK**, and then exit Autopsy

Rebuilding File Headers

- Before editing a recovered graphics file, attempt to open it with an image viewer like Microsoft's default tool.
- Double-click the file in File Explorer to check if it opens.
- If the image opens successfully, consider the file recovered.
- If the image doesn't display, manually inspect and correct header values.
- If header data is corrupt, more pieces of the file may need recovery.

Reconstructing File Fragments

- Data corruption can hinder data fragment recovery for files.
- Examination of suspect drives and extraction of data fragments are essential for reconstructing files for evidentiary purposes.
- Tools in digital forensics can trace links between clusters for FAT and NTFS file systems.
- Occasionally, FAT or NTFS Master File Table (MFT) files may lack pointer information.

Fragmented File Recovery Procedure

- Locate and export all sectors of the fragmented file.
- Identify starting and ending cluster numbers for each fragmented sector group.
- Copy fragmented sector groups in correct sequence to a recovery file.
- Rebuild the file's header for readability in a graphics viewer.
- Append a .txt extension to all copied sectors.

Rebuilding Files

- Use previously described techniques for file header rebuilding.
- Save updated recovered data with a .jpg extension.
- Similar techniques apply to other files with altered header information.
- For files larger than 200 KB, data extraction may require splitting into multiple files.
- Overwritten data in the first file can be repaired, then combined with the second file.
- Disk editors like WinHex or Hex Workshop are suitable for these tasks

Tools for Viewing Images

- After learning about file formats, compression techniques, and recovering graphics files, utilizing an image viewer is crucial.
- There are numerous image viewers available, each capable of reading various graphics file formats, although no single viewer can handle all formats.
- It's advisable to have multiple viewer programs for investigations due to the diversity of file formats encountered.
- Many viewer utilities, often freeware or shareware, can handle a wide range of graphics file formats.
- GUI forensics tools typically include image viewers focusing on common formats like GIF and JPEG, common in internet-related investigations.

Tools for Viewing Images+

- Less common formats such as PCX might not be recognized by integrated viewers, potentially hindering critical evidence discovery.
- It's essential to analyze and inspect every unknown file on a drive to ensure no evidence is overlooked.

Understanding Steganography in Graphics Files

- Graphics files opened in image viewers might not initially reveal relevant information, as they could contain hidden data through steganography.
- Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.[1]
- Steganography, an ancient technique, involves concealing messages within a host file, akin to how Greek rulers tattooed messages on messengers' scalps.
- Two major forms of steganography exist insertion, which embeds data into the host file, and substitution, which replaces bits of the host file with hidden data.

Understanding Steganography in Graphics Files+

- Detecting hidden data can be challenging and time-consuming, requiring careful analysis of file structure and comparison between displayed content and actual file contents.
- In substitution steganography, bits of the host file are replaced with hidden data, typically focusing on the least significant bits to minimize noticeable changes.
- Steganalysis tools are used to detect steganography techniques by analyzing file alterations that may not be visible to the human eye.
- Inspecting files for evidence of steganography is crucial, especially when dealing with technically skillful suspects or observing suspicious indicators like duplicate files with different hash values or installed steganography software.

Using Steganalysis Tools

- Steganalysis tools, also known as "steg tools," are utilized to detect, decode, and document concealed data, even in files that have been renamed for secrecy.
- These tools can identify variations in images and determine file formats from headers, even if the file has been renamed.
- While steganalysis tools aid in identifying hidden data, detecting steganography itself is generally challenging.
- Correctly executed steganography often escapes detection unless a comparison is made between the altered and original files.
- Changes in file size, image quality, or extensions may indicate the presence of steganography.

Using Steganalysis Tools+

- An illustrative example of steganography's elusive nature is a study by Niels Provos and Peter Honeyman at the University of Michigan, where over two million images from eBay auctions were analyzed without revealing hidden messages.

Understanding Copyright Issues with Graphics

- Steganography is utilized for embedding digital watermarks in files to protect copyrighted material.
- Digital investigators, especially in corporate environments, must understand copyright laws when dealing with graphics files.
- They may need to ascertain if a photo is sourced from copyrighted material, like a news photo used without permission.
- Copyright laws, particularly concerning the internet, can be complex, varying by country and often requiring legal action for enforcement.
- International copyright treaties exist, but enforcing them typically necessitates legal proceedings in the country of infringement.

Understanding Copyright Issues with Graphics+

- The U.S. Copyright Office defines eligible copyright works broadly, covering various forms of expression such as literary, musical, and graphic works.
- Anything created digitally that would typically be copyrighted through traditional means is also protected.
- Digital watermarks can be visible (like logos) or unnoticeable, with invisible ones not altering file appearance or quality.
- Fair use allows for limited use of copyrighted material without permission, such as short quotes for news or educational purposes, but the rules can be complicated.
- Utilizing copyrighted material for noncommercial and educational purposes generally falls under fair use, though there are distinctions, like the distinction between personal copying and commercial reproduction.

Understanding Copyright Issues with Graphics+

- Even with freely available graphics, providing attribution to the creator is good practice, offering credit and clarity about the source.
- Ensuring the right to use graphics is crucial, whether by obtaining permission, using public domain graphics, or creating original ones, to prevent copyright infringement.

Reference

[1]Kaspersky. (2023, May 10). *What is steganography? definition and explanation*. www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-steganography

[2] MozDevNet. (n.d.). *Lossless compression - MDN web docs glossary: Definitions of web-related terms: MDN*. MDN Web Docs. https://developer.mozilla.org/en-US/docs/Glossary/Lossless_compression

[3] Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning.

[4] Wikimedia Foundation. (2024, April 5). *Lossy compression*. Wikipedia. https://en.wikipedia.org/wiki/Lossy_compression

[5] Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* Course Technology Cengage Learning. Page 352, 350