**Steganography Detection Tools**

Steganography Detection Tools are used to find other concealed information, as well as hidden data within photos and audio recordings.

**The use of steganography detection tools by investigators**

Finding concealed Information: To examine photos, audio files, and other media for possible concealed information, investigators use steganography detection tools. These programs can show whether the files have been altered to hide private information, such as hidden files or messages.

Finding Covert Communications: Investigators can find covert communication channels that criminals can use to share sensitive information or conduct illicit operations with the use of steganography detection technologies.

Investigators use these technologies to recover hidden data from files and media during evidence extraction. In criminal investigations or cybersecurity issues, this concealed information may be essential evidence.

Analysis of Digital Forensics: Steganography techniques used to conceal information within digital assets can be quickly found and analyzed by investigators thanks to the integration of steganography detection tools into digital forensic procedures.

**Misuse of Steganography Detection Tools by Hackers:**

Avoiding detection: To evade detection by security measures or antivirus software, hackers may employ steganography techniques to conceal harmful code or sensitive data into genuine files.

Hackers can use steganography to covertly exfiltrate critical data from a hacked system without drawing attention to themselves by hiding the data inside of seemingly benign images or files.

Steganography enables hackers to exchange information in media files that are undetectable to ordinary monitoring or security systems, allowing them to communicate covertly and conceal their operations.

Hackers may employ steganography to conceal malware payloads inside of photographs or documents, enabling them to spread harmful software undetectedly.

Ex: NSA’s slowglobe.