

Explore Compare It Tool to Compare of two files for Forensic Investigation

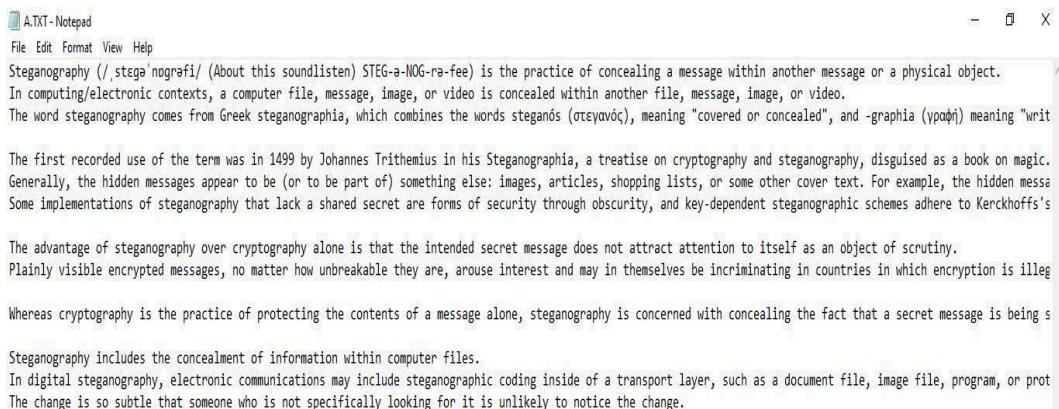
AIM:

The main aim is to comparison of two files for forensics investigation by COMPARE IT tool

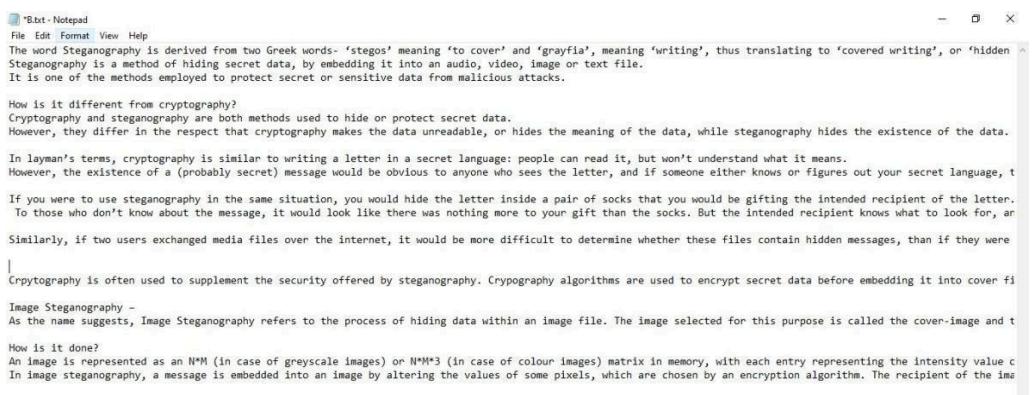
PROCEDURE:

- COMPARE IT is software that displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke, and of course, you have the ability to edit files directly in comparison window.
- It can make colored printout of differences report, exactly as it's on the screen.
First of all, install the Compare It from the Link given below.
<http://www.grisoft.com/wincmp3.htm> it is a 1.7 Mb Software package Click on Compare It Tool, It will show a window to select the files to be compared.
- First, select the first file and click on open and then select the second file and click on open.

STEP 1: open the notepad and create a first text file with the extension .txt and save with a file name

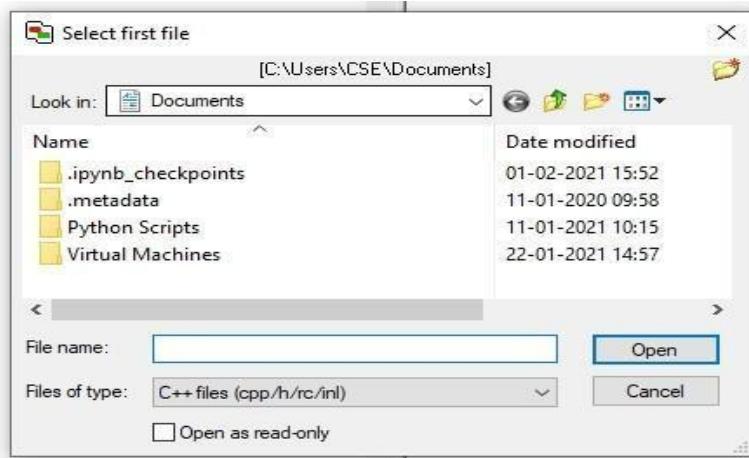


Step 2: create a second text file with the extension .txt

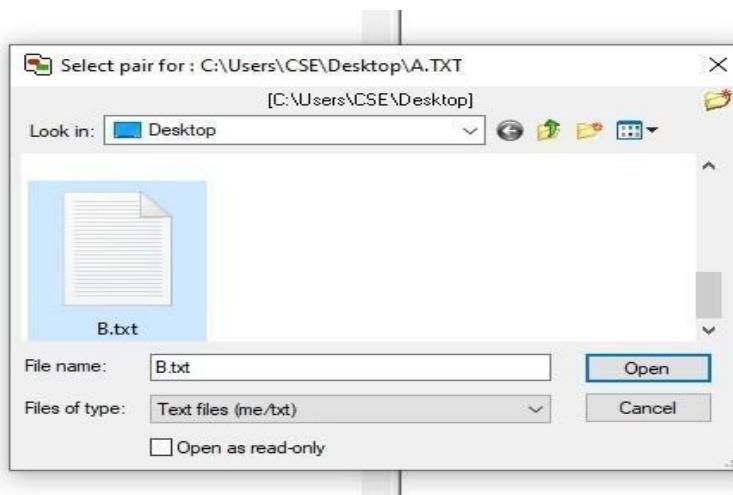


Step 3: Download the compare it tool install the Compare It from the Link given below. <http://www.grisoft.com/wincmp3.htm> it is a 1.7 Mb Software package Click on Compare It Tool, It will show a window to select the files to be compared.

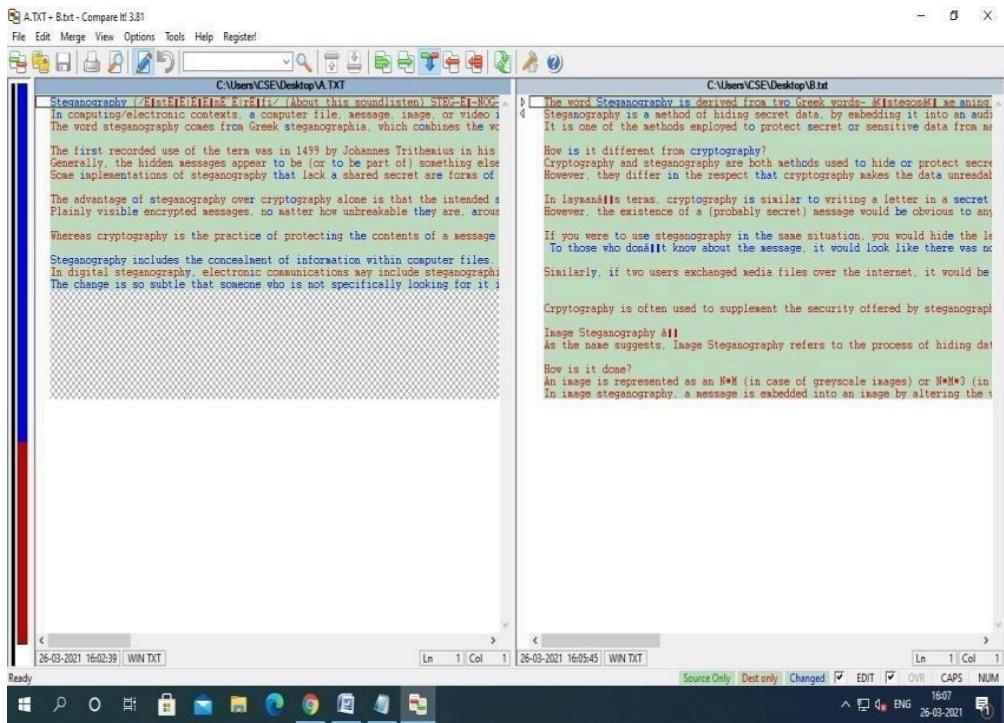
Step 4: Upload the first file to the compare it tool



Step 5: upload the second file to the compare it tool



Step 6: Displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke



STEP 7: It also gives you Print report of the difference in the file as follows

The word **Steganography** is derived from two Greek words- **stego**=weaving; **graphia**=writing. Steganography is a method of hiding secret data, by embedding it into an audio, video or image file. In computing/electronic contexts, a computer file, message, image, or video is hidden within another message or a physical object.

In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or soundtrack. Steganography is used for steganographic transmission because of the large amount of data that can be hidden. Steganography often begins with an innocuous image file and adjust the color of every hundred thousand pixels to correspond to a letter in the alphabet.

The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.

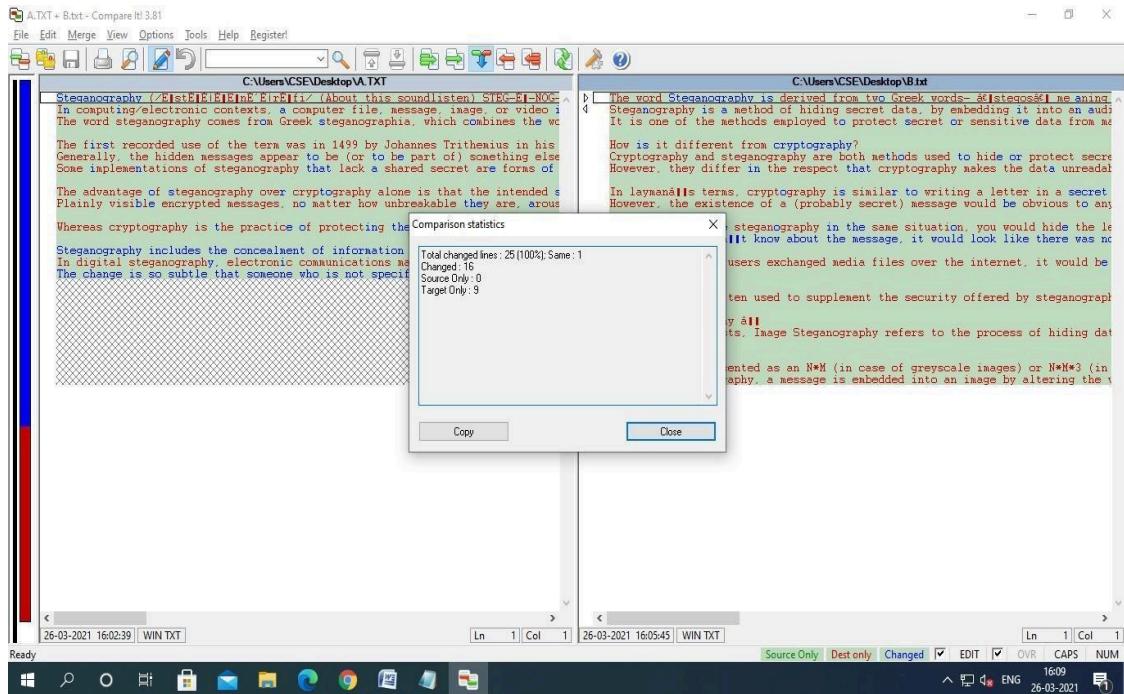
How is it different from cryptography?

Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable. In layman's terms, cryptography is similar to writing a letter in a secret code, so that only the intended recipient can understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either intercepts the message or reads it, then your message can easily be read.

If you were to use steganography in the same situation, you would hide the letter inside a pair of socks that you were going to wash, and when you took them out, and finds the message hidden in them.

Similarly, if you were exchanging files over the internet, it would be more difficult to determine whether these files contain hidden messages, or if they were communicating using cryptography.

STEP 8: the comparison result is get display.



RESULT:

The main aim is to comparison of two files for forensics investigation by COMPARE IT tool is executed successful

1. Create Two Sample Files

nano file1.txt

(Add some text → save with CTRL+O, exit with CTRL+X)

nano file2.txt

(Add slightly different text → save and exit)

2. Compare Files Using diff

diff file1.txt file2.txt

- This shows line-by-line differences.
- Lines starting with < are from **file1**, and > are from **file2**.

3. Use cmp for Byte-Level Comparison

cmp -l file1.txt file2.txt

- Prints the exact **byte offset and difference** between the files.
- Useful in forensic investigation to detect tampering at a binary level.

4. Use vimdiff for Side-by-Side Colored View

vimdiff file1.txt file2.txt

- Opens both files in **Vim with color highlighting** for differences.
- Very close to “Compare It” visual style.

Navigation:

-]c → Jump to next change
- [c → Jump to previous change
- :qa! → Quit both files

5. Use meld (GUI Tool – Similar to Compare It)

If you want a **GUI comparison like Compare It**:

sudo apt update

sudo apt install meld -y

Then run:

```
meld file1.txt file2.txt
```

- Shows side-by-side differences with **colored highlights**, very close to Compare It's Windows tool.
- Can also save/print difference reports.

6. Generate a Forensic Report

You can export results to a file:

```
diff -u file1.txt file2.txt > diff_report.txt
```

- -u gives a unified diff format, commonly used in forensics.
- You can attach this report as evidence in investigation.

