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

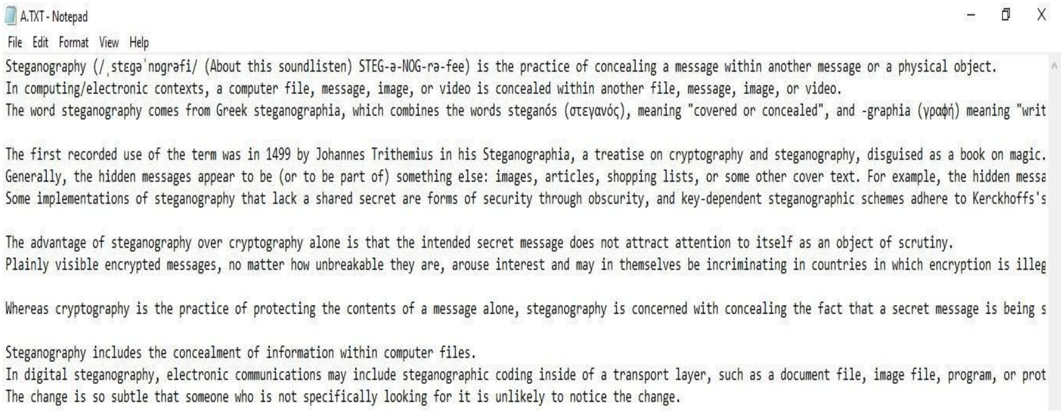
AIM:

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

PROCEDURE:

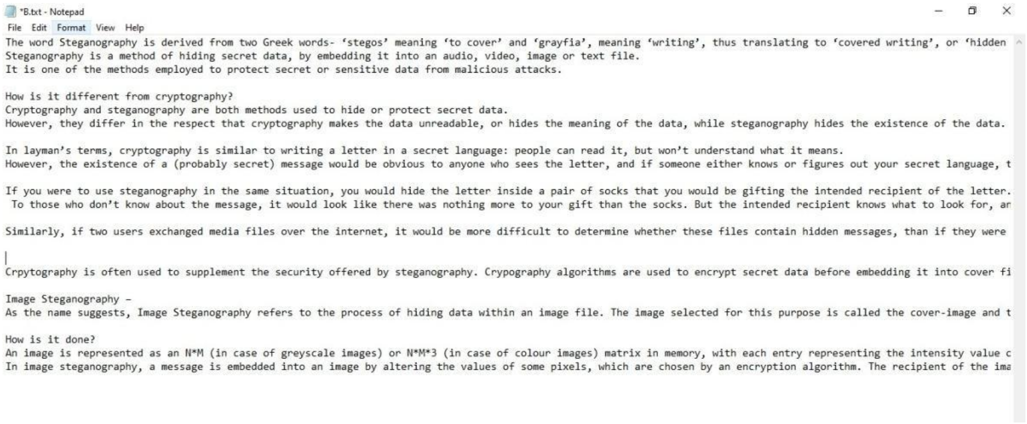
- COMPARE IT is software that displays 2 files side by side, with colored differences sections to simplify analyzing. You can move changes between files with a single mouse click or keystroke, and of course, you have the ability to edit files directly in comparison window.
- It can make colored printout of differences report, exactly as it‟s on the screen. First of all, install the Compare It from the Link given below. http://www.grigsoft.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 savewith a file name



```
Steganography (/ˌstɛɡəˈnɒɡrəfi/ (About this soundlisten) STEG-ə-NOG-rə-fee) is the practice of concealing a message within another message or a physical object.
In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video.
The word steganography comes from Greek steganographia, which combines the words steganós (στεγανός), meaning "covered or concealed", and -graphia (γραφή) meaning "writ

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic.
Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden messa
Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffs's

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.
Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illeg

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being s

Steganography includes the concealment of information within computer files.
In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or prot
The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.
```

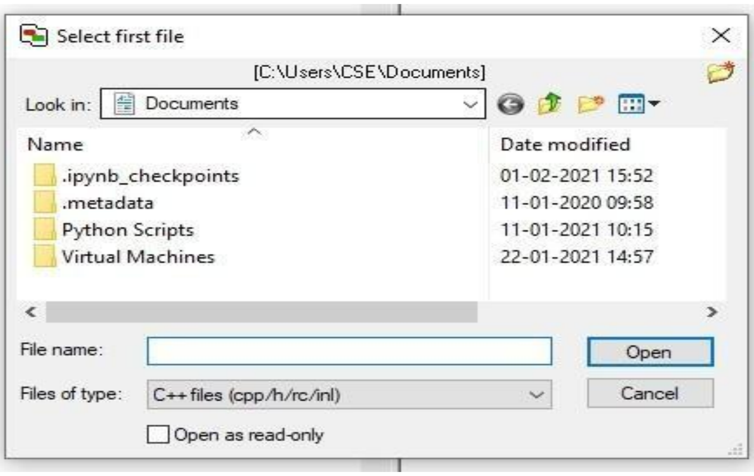
Step 2: create a second text file with the extension .txt



```
The word Steganography is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden
Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file.
It is one of the methods employed to protect secret or sensitive data from malicious attacks.

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, or hides the meaning of the data, while steganography hides the existence of the data.

In layman’s terms, cryptography is similar to writing a letter in a secret language: people can read it, but won’t 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 knows or figures out your secret language, t

If you were to use steganography in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter.
 To those who don’t know about the message, it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for, an

Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages, than if they were


Crpytography is often used to supplement the security offered by steganography. Crypography algorithms are used to encrypt secret data before embedding it into cover fi

Image Steganography –
As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and t

How is it done?
An image is represented as an N*M (in case of greyscale images) or N*M*3 (in case of colour images) matrix in memory, with each entry representing the intensity value c
In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the ima
```

Step 3: Download the compare it tool install the Compare It from the Link given below. http://www.grigsoft.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



Select first file

[C:\Users\CSE\Documents]

Look in: Documents

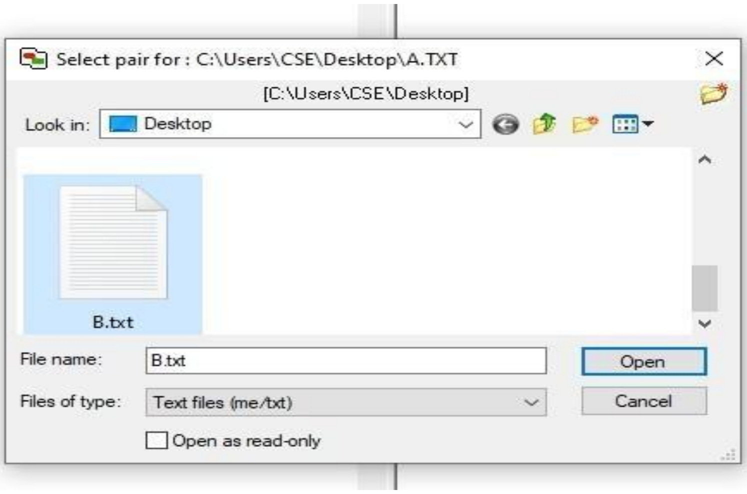
Name	Date modified
.ipynb_checkpoints	01-02-2021 15:52
.metadata	11-01-2020 09:58
Python Scripts	11-01-2021 10:15
Virtual Machines	22-01-2021 14:57

File name:

Files of type: C++ files (cpp/h/rc/inl)

□ Open as read-only

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



Select pair for : C:\Users\CSE\Desktop\A.TXT

[C:\Users\CSE\Desktop]

Look in: Desktop

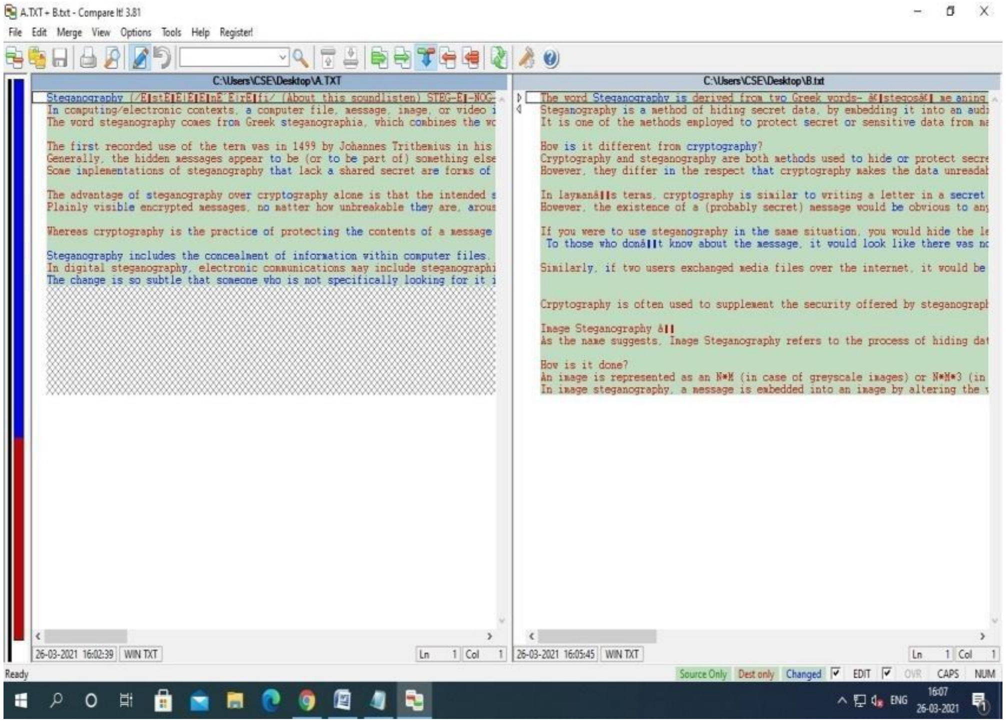
B.txt

File name: B.txt

Files of type: Text files (me/txt)

□ Open as read-only

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


A.TXT + B.txt - Compare It! 3.81
File Edit Merge View Options Tools Help Register!
Ready
Source Only Dest only Changed ☑ EDIT ☑ OVR CAPS NUM
ENG 16:07 26-03-2021

C:\Users\CSE\Desktop\A.TXT

```
Steganography (/ËˌstÉ›É¡É™ËˆnÉ’É¡rÉ™fi/ (About this soundlisten) STEG-É™-NOG-
In computing/electronic contexts, a computer file, message, image, or video i
The word steganography comes from Greek steganographia, which combines the wo

The first recorded use of the term was in 1499 by Johannes Trithemius in his
Generally, the hidden messages appear to be (or to be part of) something else
Some implementations of steganography that lack a shared secret are forms of

The advantage of steganography over cryptography alone is that the intended s
Plainly visible encrypted messages, no matter how unbreakable they are, arous

Whereas cryptography is the practice of protecting the contents of a message

Steganography includes the concealment of information within computer files.
In digital steganography, electronic communications may include steganographi
The change is so subtle that someone who is not specifically looking for it i
```

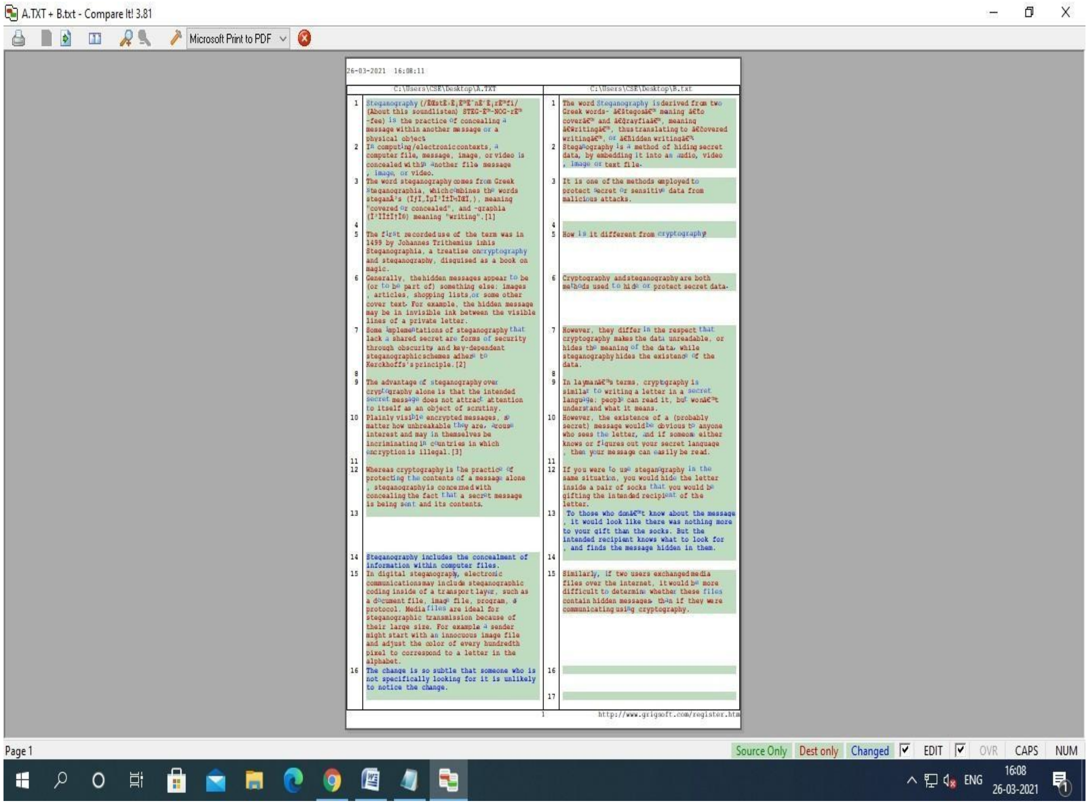
26-03-2021 16:02:39 WIN TXT Ln 1 Col 1

C:\Users\CSE\Desktop\B.txt

```
The word Steganography is derived from two Greek words- â€œstegosâ€ me aning
Steganography is a method of hiding secret data, by embedding it into an audi
It is one of the methods employed to protect secret or sensitive data from ma

How is it different from cryptography?
Cryptography and steganography are both methods used to hide or protect secre
However, they differ in the respect that cryptography makes the data unreadab

In laymanâ€™s terms, cryptography is similar to writing a letter in a secret
However, the existence of a (probably secret) message would be obvious to any

If you were to use steganography in the same situation, you would hide the le
 To those who donâ€™t know about the message, it would look like there was no

Similarly, if two users exchanged media files over the internet, it would be


Crpytography is often used to supplement the security offered by steganograph

Image Steganography â€
As the name suggests, Image Steganography refers to the process of hiding dat

How is it done?
An image is represented as an N*M (in case of greyscale images) or N*M*3 (in
In image steganography, a message is embedded into an image by altering the v
```

26-03-2021 16:05:45 WIN TXT Ln 1 Col 1

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

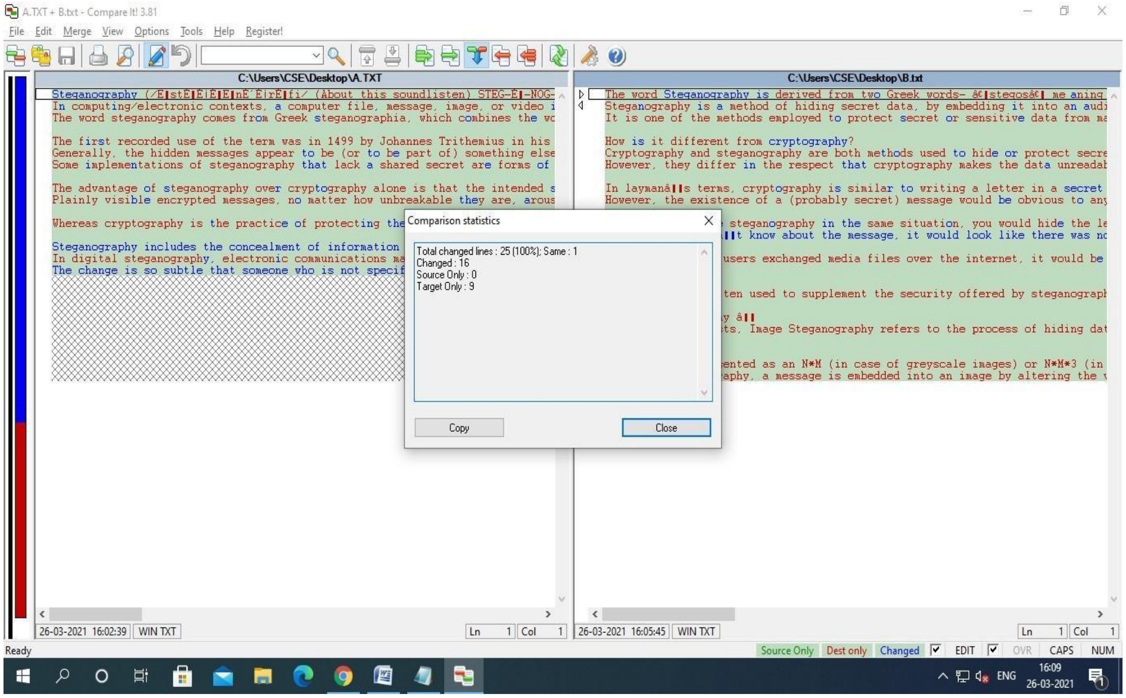

A.TXT + B.txt - Compare It! 3.81
Microsoft Print to PDF
Page 1
Source Only Dest only Changed ☑ EDIT ☑ OVR CAPS NUM
ENG 16:08 26-03-2021

26-03-2021 16:08:11

	C:\Users\CSE\Desktop\A.TXT		C:\Users\CSE\Desktop\B.txt
1	Steganography (/ËŒstÉ›É¡É™ËˆnÉ’É¡rÉ™fi/ (About this soundlisten) STEG-É™-NOG-rÉ™-fee) is the practice of concealing a message within another message or a physical object	1	The word Steganography is derived from two Greek words- â€œstegosâ€™ maning â€œto coverâ€™ and â€œgrayfiaâ€™, meaning â€œwritingâ€™, thus translating to â€œcovered writingâ€™, or â€œhidden writingâ€™
2	In computing/electronic contexts, a computer file, message, image, or video is concealed within another file message , image, or video.	2	Steganography is a method of hiding secret data, by embedding it into an audio, video , image or text file.
3	The word steganography comes from Greek steganographia, which combines the words steganÃ³s (ÏƒÏ„ÎµÎ³Î±Î½ÏŒÏ‚), meaning "covered or concealed", and -graphia (Î³ÏÎ±Ï†Î®) meaning "writing".[1]	3	It is one of the methods employed to protect secret or sensitive data from malicious attacks.
4		4	
5	The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic.	5	How is it different from cryptography?
6	Generally, the hidden messages appear to be (or to be part of) something else: images , articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter.	6	Cryptography and steganography are both methods used to hide or protect secret data.
7	Some implementations of steganography that lack a shared secret are forms of security through obscurity and key-dependent steganographic schemes adhere to Kerckhoffs's principle.[2]	7	However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data.
8		8	
9	The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny.	9	In laymanâ€™s terms, cryptography is similar to writing a letter in a secret language: people can read it, but wonâ€™t understand what it means.
10	Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.[3]	10	However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language , then your message can easily be read.
11		11	
12	Whereas cryptography is the practice of protecting the contents of a message alone , steganography is concerned with concealing the fact that a secret message is being sent and its contents.	12	If you were to use steganography in the same situation, you would hide the letter inside a pair of socks that you would be gifting the intended recipient of the letter.
13		13	To those who donâ€™t know about the message , it would look like there was nothing more to your gift than the socks. But the intended recipient knows what to look for , and finds the message hidden in them.
14	Steganography includes the concealment of information within computer files.	14	
15	In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographic transmission because of their large size. For example a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet.	15	Similarly, if two users exchanged media files over the internet, it would be more difficult to determine whether these files contain hidden messages, than if they were communicating using cryptography.
16	The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.	16	
		17	

1 http://www.grigsoft.com/register.htm

STEP 8: the comparison result is get display.



```
Steganography (/ˌstɛɡəˈnɒɡrəfi/ (About this soundlisten) STEG-ə-NOG-
In computing/electronic contexts, a computer file, message, image, or video i
The word steganography comes from Greek steganographia, which combines the wo

The first recorded use of the term was in 1499 by Johannes Trithemius in his
Generally, the hidden messages appear to be (or to be part of) something else
Some implementations of steganography that lack a shared secret are forms of

The advantage of steganography over cryptography alone is that the intended s
Plainly visible encrypted messages, no matter how unbreakable they are, arous

Whereas cryptography is the practice of protecting the

Steganography includes the concealment of information
In digital steganography, electronic communications ma
The change is so subtle that someone who is not specif
```

```
The word Steganography is derived from two Greek words- â€▌steqosâ€▌ me aning
Steganography is a method of hiding secret data, by embedding it into an audi
It is one of the methods employed to protect secret or sensitive data from ma

How is it different from cryptography?
Cryptography and steganography are both methods used to hide or protect secre
However, they differ in the respect that cryptography makes the data unreadab

In laymanâ▌▌s terms, cryptography is similar to writing a letter in a secret
However, the existence of a (probably secret) message would be obvious to any

 steganography in the same situation, you would hide the le
▌▌t know about the message, it would look like there was no

users exchanged media files over the internet, it would be


ten used to supplement the security offered by steganograph

y â▌▌
ts, Image Steganography refers to the process of hiding dat


ented as an N*M (in case of greyscale images) or N*M*3 (in
aphy, a message is embedded into an image by altering the v
```

Comparison statistics

Total changed lines : 25 (100%); Same : 1
Changed : 16
Source Only : 0
Target Only : 9

Copy Close

RESULT:

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

Steps to Compare Two Files for Forensic Investigation in Kali Linux

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.