Cryptography

Definition and terminologies

- **Plaintext:** is a clear and readable text
- **Ciphertext:** is encrypted text transformed from plaintext using an encryption algorithm.
- **Encryption:** is a process of encoding information (converting plaint text to cipher text
- **Decryption:** is a process of decoding information (converting cipher text to plaint text)
- **Key:** is the secret information that is used to encrypt the plaint text and decrypt the cipher text
- **Key space:** is the range of the keys, the more the big the keys is, the better and strong it becomes
- **Cryptography:** is a practice and study of technique for secure information and prevent third parties or the public from reading private message The term is derived from the Greek word kryptos, which means hidden.
- **Cryptanalysis:** is code breaking or decrypting data without knowing it's encryption key
- **Cryptology:** is a process of encoding and decoding information

Types of cryptography

- Symmetric cryptography
- A symmetric cryptography

Symmetric cryptography

- is technique using single key for both encryption and decryption and it's also called private key encryption
- Example of symmetric cryptography: let's say person A want to send person B without knowing anyone else.
- let's send secret message from person A to person B
  1. person A writes down the massage which is'HELLO' and uses number 9 as a key
  2. to encrypt the word 'H' start counting 9 time from 'H' (I, J, K, L, M, N, O, P, **Q**) and the answer will be 'Q', substitute H to Q and now you have 'QELLO' repeat the process until the last word so the output or your cipher text will be 'QNUUX'

     Plaintext: HELLO
     Key: 9
     Ciphertext: QNUUX

     Now you have plaint text, key and the cipher text, to send this secret

     Message to person B, you need to send the cipher text with key (be

     More carefully sending the key because if another person finds the

     Cipher text with the key, they may discover the secret message)

3. once person B, found cipher text and the key then he/she will decrypt the secret message by using the key,
4. to decrypt the message which is ‘QNUUX’ with key 9, you need to count 9 times backward from ‘Q’ (P, O, N, M, L, K, J, I, **H**)the answer will be ‘H’, substitute Q to H and now you have ‘HNUUX’ repeat the process until the last word so the output or your plaint text will be ‘HELLO’

Cipher text:	QNUUX
Key:	9
Plain text:	HELLO

A Symmetric cryptography

- Asymmetric encryption or public key encryption is using two mathematical related keys, which is public key for encryption and private key for decryption
- The requestor or receiver creates two keys public key and private key, then sends public key to the sender and keeps private key, the sender will encrypt the message using public key and the receiver will decrypt using private key.

EXAMPLE

- Person A wants to send secret message to person B
- Person B, creates two keys (public key and private key) and sends only public key to person A
- Person A uses public key and encrypts the message, then sends to person B
- Person B uses private key to decrypt the message

Cryptanalysis

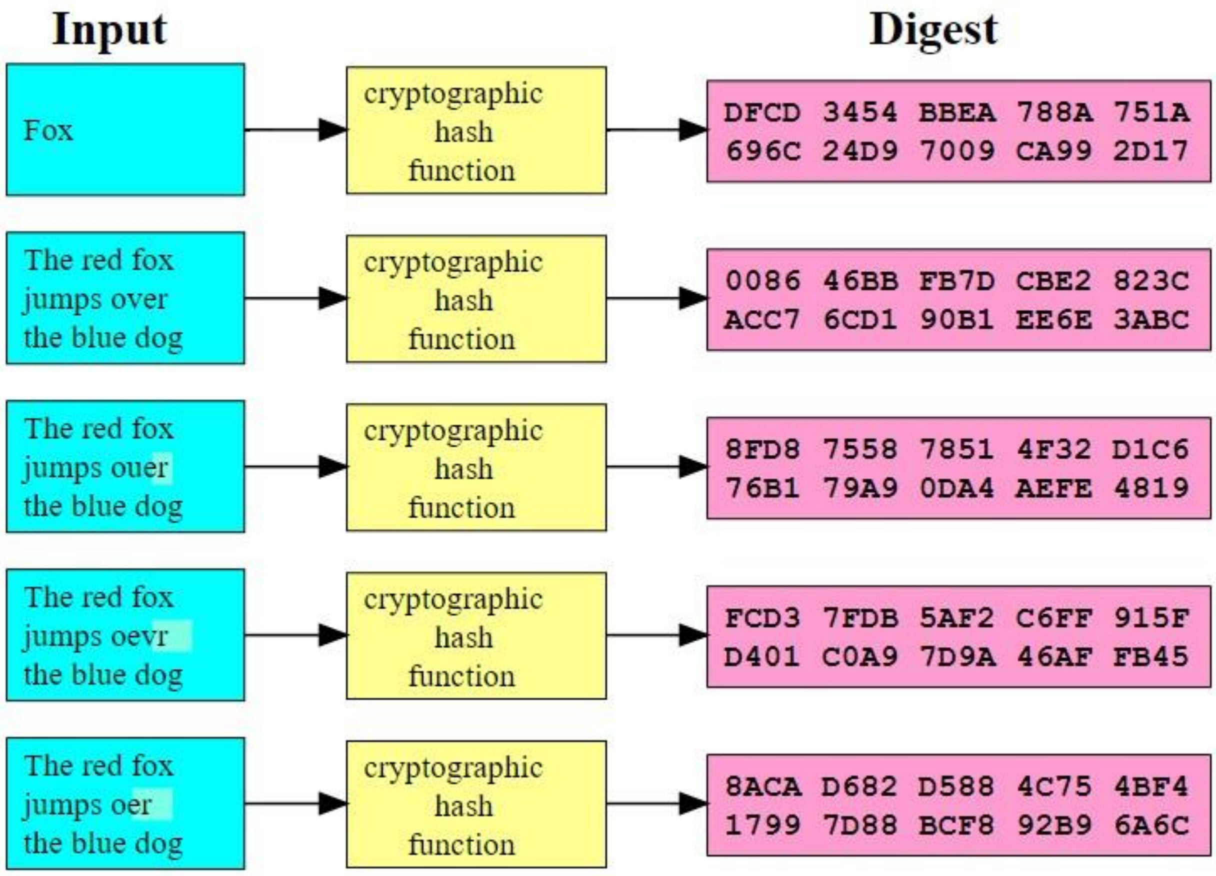
- Cryptanalysis is a process analyzing and decrypting encrypted data without knowing it is secret key and the algorithm that is used to encrypt it

Types of Cryptanalytic attacks:

- **Ciphertext only:** the attacker knows
  - Ciphertext … the attacker knows ciphertext because the attacker can access the data while it’s in network transmission
  - Encryption algorithm … when he finds it, then he will probably know what algorithm was used
- **Known plaintext:** the attacker knows
  - Ciphertext
  - Encryption algorithm
  - One or more plaint text with their cipher text … this means the attacker also know some pairs formed with secret keys

- **Chosen plaintext or chosen ciphertext:** the attacker involves the process of choosing the plaintext or ciphertext then he tries to sneak and access the secret message
- **Chosen plaintext and ciphertext:** this is like employee who has turned into attacker
- **Brute-force attack:**
    - Guessing and trying every possible key
    - Using online sources and tools can perform brute-force attacks like
        - Aircrack-ng
        - Cain and abel
        - Crack
        - DaveGrohl
        - Hashcat
        - Hydra
        - John the ripper
        - Rainbowcrack
        - Ophcrack

Hash function


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Introduction

- **Hash function:** is a one-way algorithm this means it is easy to encrypt but nearly impossible to decrypt.
- **Digest or hash value:**is the output after encryption process
- If the plaintext has different length, the digest (decrypted plaintext) will be same lengths in every algorithm; this is what makes impossible to guess.
- Every algorithm has same length of digest massage as you can see in the picture above; every SHA-1 digest massage will be 160bits, even if the plaintext is different.
- Small change even one bit of plaintext will create different digest massage as you can see in the picture, OVER, OUER, OEVR & OER
- Hash functions is primarily use for comparison purpose not for encryption, for example when you were creating Gmail account, the Gmail server saved your password as digest or hash value then the next time you are opening your account the Gmail will compare the old digest massage it saved and the new one, if it same then you alright if not you will need to enter your password again

Some types of hash algorithms

- SHA-1
- SHA-2 S
- SHA-3
- MD5
- BLAKE2
- BLAKE3
- WHIRLPOOL
- RIPEMD-160 and many more

Hash function vs encryption

1. the other hand, is one-way, meaning the plaintext is scrambled into a unique digest, through the use of a salt, that cannot be decrypted.
2. According to the output encryption isVariable Length means it depends the size of the input while hash function is fixed length
3. hash function is used for password storing and data integrity while Encryption is used to communications and signing

Free websites that you can use to encode and decode most popular algorithms

- AES encryption https://encode-decode.com/aes256-encrypt-online/
- DES encryption https://encode-decode.com/des-encrypt-online/
- RSA encryption: https://8gwifi.org/rsafunctions.jsp
- Blowfish encryption: https://encode-decode.com/blowfish-encrypt-online/

- These are free once and there are also many, many free website that you can encode and decode cryptographic algorithms (search them in google) and also there are some cheap websites which can provide reliable information

Hash function

- Unlike cryptography hash functions is more secure, but still cybercriminals hack the most protected systems like Facebook, Gmail, etc.
- IF hash function is Irreversible, the question is how cybercriminal crack passwords?
  - ✓ The answer is, they (hackers) can't reverse the hash value or digest but they use something called lookup tables or rainbow tables, these tables are stored large number of plaintexts (command used passwords) with their hash values, if your password is very easy the probability of cracking your password is very high, (.. see how hackers crack your password)

Free websites that you can use to decode hash value

Note: to understand this process find command password with their hashed in GOOGLE then use these websites to decode

1. **https://crackstation.net/**
2. **https://hashes.com/en/decrypt/hash**
3. **https://hashkiller.io/listmanager**

Steganography

Image credit: Sandro Villinger

Definition

- is a technique of hidden secret massage within an ordinary or non-secret file in order to avoid detection
- different between this technique and cryptography is, in cryptography the third party will know there is secret massage or at least something is going on became he/she may see the encrypted massage, while using Steganography the third party will not know the existence of the massage, the third part will think it is ordinary file.

Types of Steganography

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Network Steganography
6. Email Steganography

Text Steganography

- **WAY ONE:** You can easily hide, by using capital letters in ordinary texts, or something like that

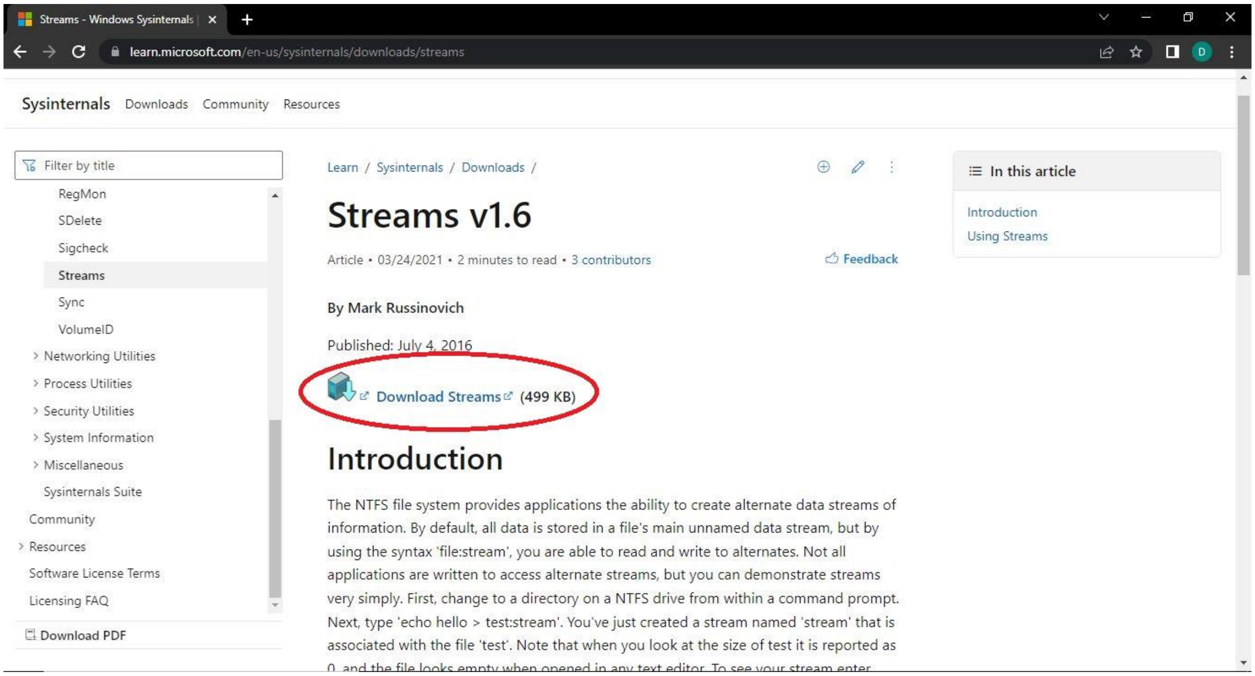
Example

- Let’s hide the word ‘ACT’ inside ordinary file by using capital letters
  Ordinary file: **A**ny fool can write code that a **C**ompute can understand, good programmers write code **T**hat humans can understand. (We used words Any, Computer and That to hide our secret message)
- **WAY TWO:** you can use software to hide secret message

Example

- Let’s use Microsoft streams to hide file

Step 1: Download and install Microsoft streams https://docs.microsoft.com/en-us/sysinternals/downloads/streams



Streams v1.6

Article • 03/24/2021 • 2 minutes to read • 3 contributors

By Mark Russinovich

Published: July 4, 2016

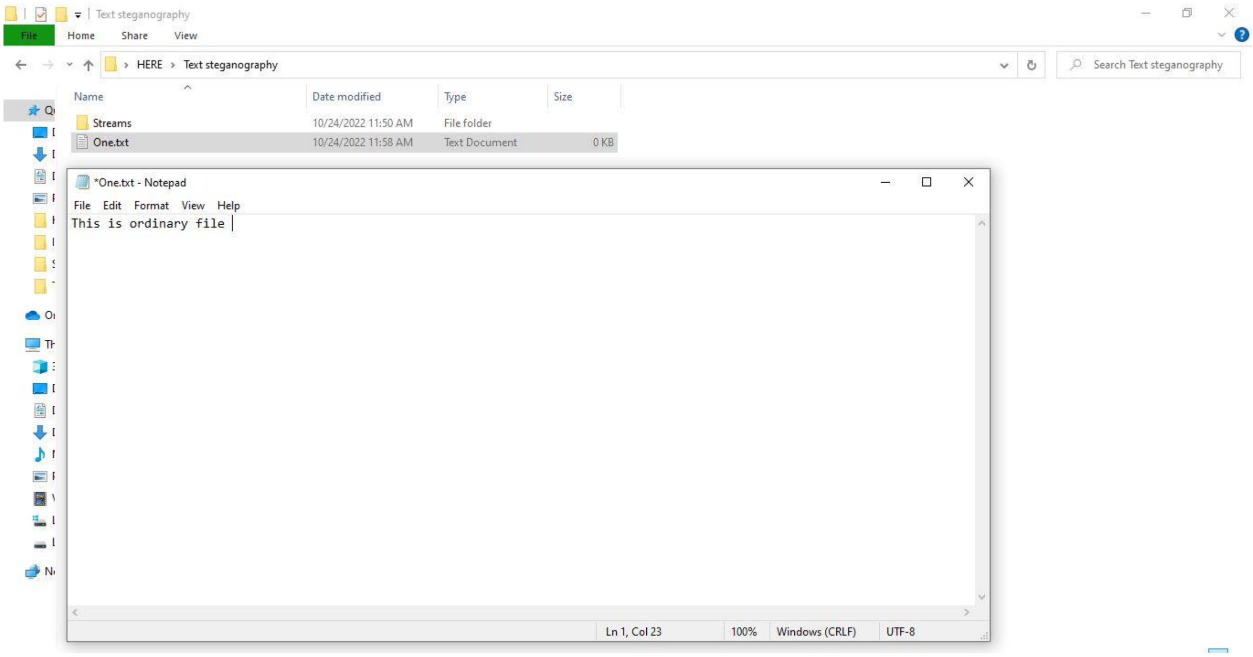
Download Streams (499 KB)

Introduction

The NTFS file system provides applications the ability to create alternate data streams of information. By default, all data is stored in a file's main unnamed data stream, but by using the syntax 'file:stream', you are able to read and write to alternates. Not all applications are written to access alternate streams, but you can demonstrate streams very simply. First, change to a directory on a NTFS drive from within a command prompt. Next, type 'echo hello > test:stream'. You've just created a stream named 'stream' that is associated with the file 'test'. Note that when you look at the size of test it is reported as 0, and the file looks empty when opened in any text editor. To see your stream enter

Step 2: extract the file

Step 3: create ordinary file example ONE.txt, write something in it and save it

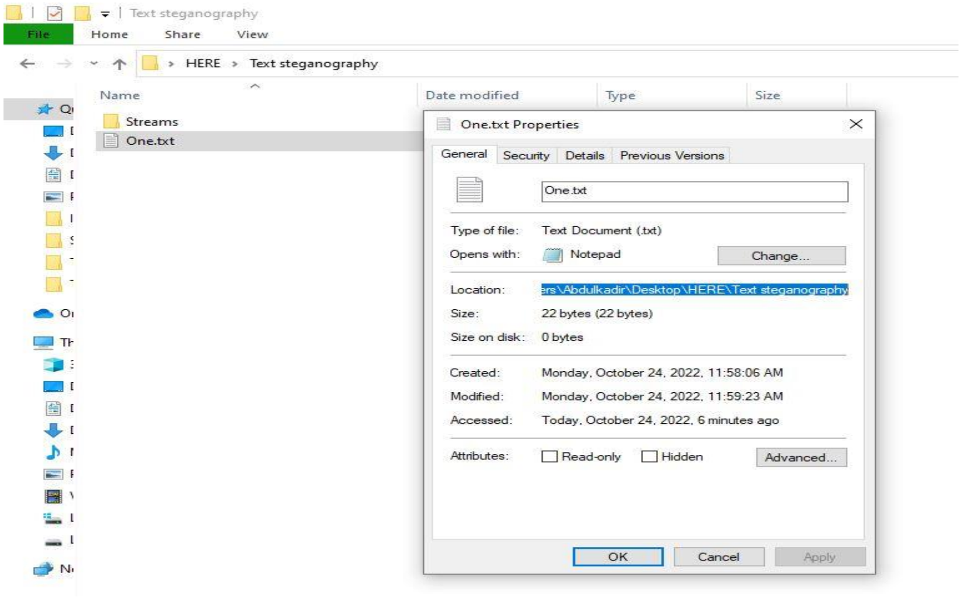


Name	Date modified	Type	Size
Streams	10/24/2022 11:50 AM	File folder	
One.txt	10/24/2022 11:58 AM	Text Document	0 KB

```
This is ordinary file
```

Ln 1, Col 23 | 100% | Windows (CRLF) | UTF-8

Step 4: know your folder's path (the location where you saved the file). To know the location of your file right click >properties and copy the location



One.txt

Type of file: Text Document (.txt)

Opens with: Notepad

Location: ers\Abdulkadir\Desktop\HERE\Text steganography

Size: 22 bytes (22 bytes)

Size on disk: 0 bytes

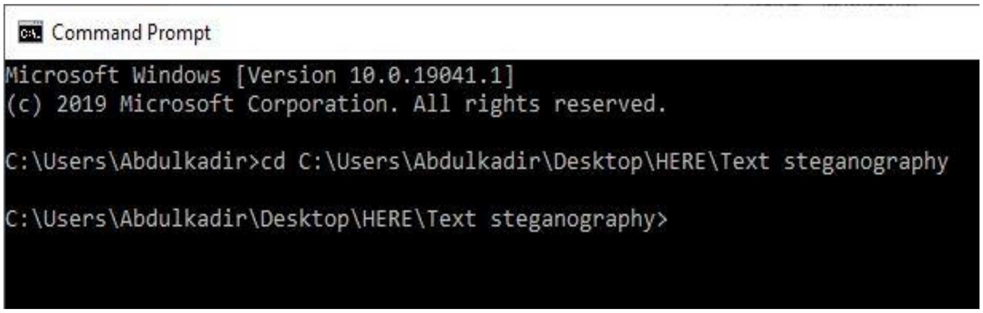
Created: Monday, October 24, 2022, 11:58:06 AM

Modified: Monday, October 24, 2022, 11:59:23 AM

Accessed: Today, October 24, 2022, 6 minutes ago

Attributes: □ Read-only □ Hidden

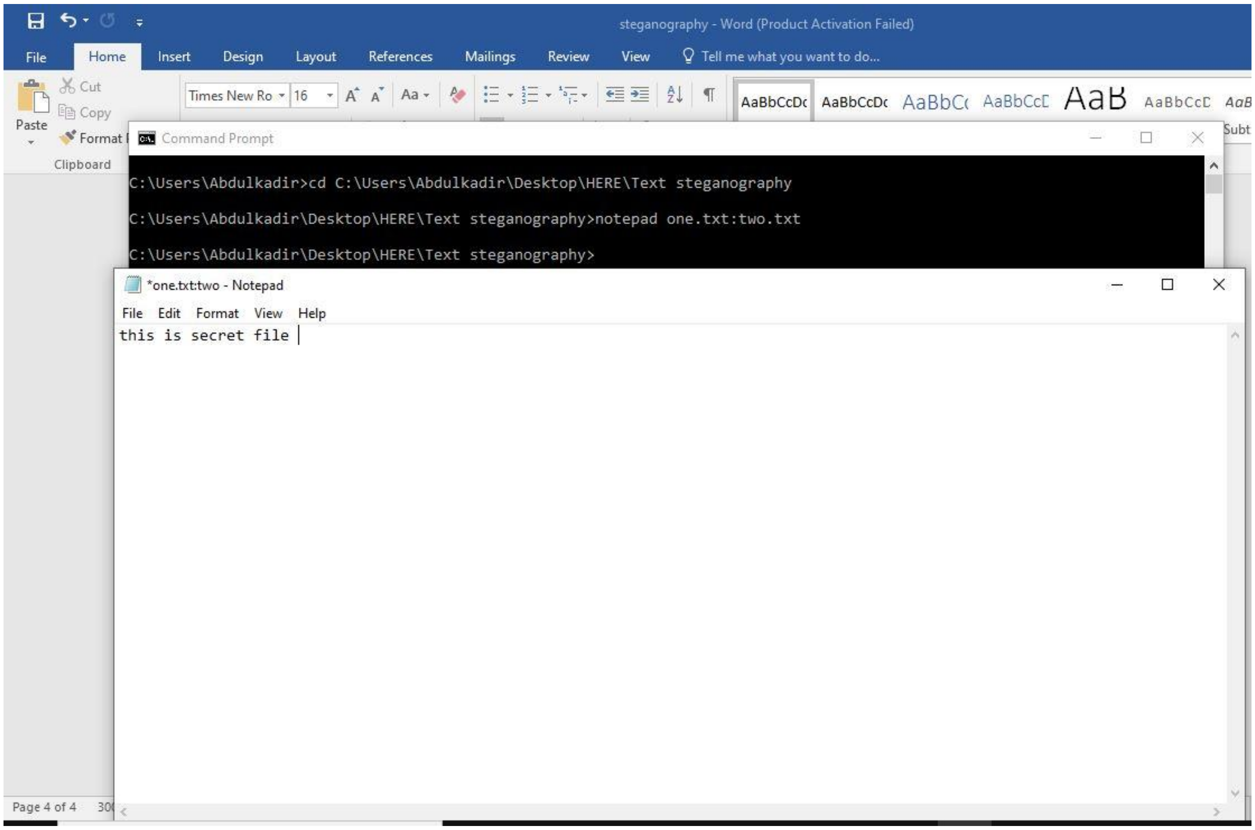
Step 5: open CMD and write cd and past your location (to past text in CMD just click right click) and click enter



```
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Abdulkadir>cd C:\Users\Abdulkadir\Desktop\HERE\Text steganography

C:\Users\Abdulkadir\Desktop\HERE\Text steganography>
```

Step 6: To create secret file in CMD use this command

Notepad one.txt:two.txtand click ok, then write the secret massage



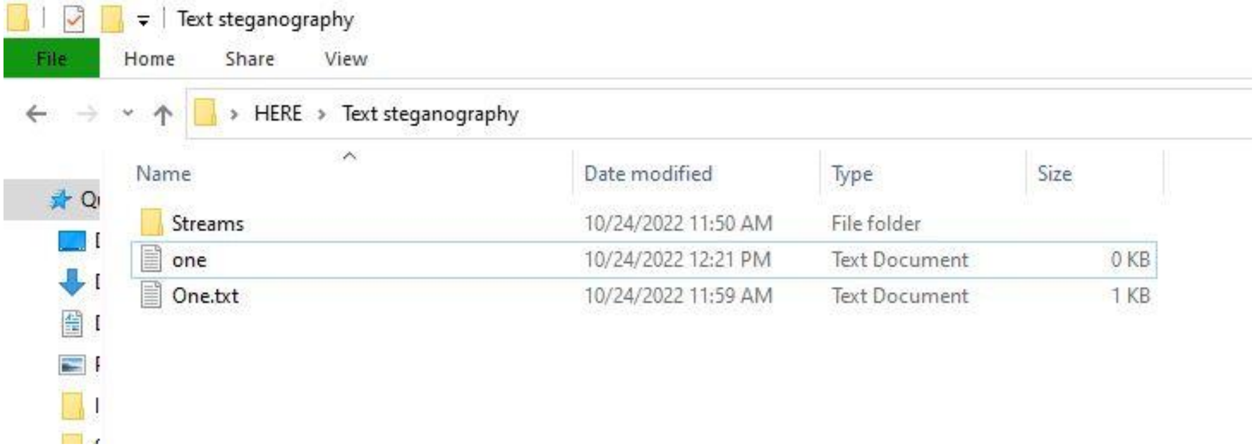
```
C:\Users\Abdulkadir>cd C:\Users\Abdulkadir\Desktop\HERE\Text steganography

C:\Users\Abdulkadir\Desktop\HERE\Text steganography>notepad one.txt:two.txt

C:\Users\Abdulkadir\Desktop\HERE\Text steganography>
```

*one.txt:two - Notepad

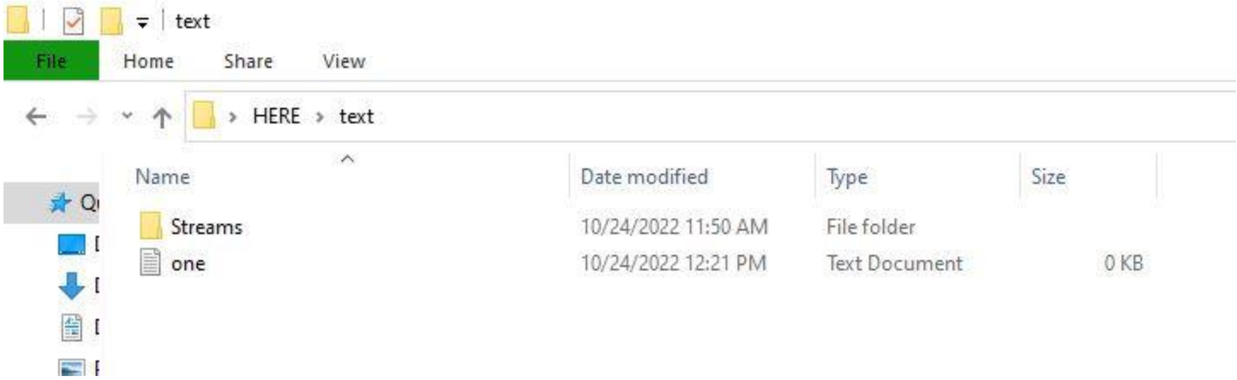
```
this is secret file
```

- ✓ **One.txt** is the first ordinary file you created in desktop
- ✓ **Two.txt** is the first secret file that hidden in the ordinary file

Once you back to your folder there will be another ordinary file, which created this command line with name **ONE** so delete the previous ordinary file **ONE.txt** and now your ordinary file is **ONE.**



Name	Date modified	Type	Size
Streams	10/24/2022 11:50 AM	File folder	
one	10/24/2022 12:21 PM	Text Document	0 KB
One.txt	10/24/2022 11:59 AM	Text Document	1 KB



Name	Date modified	Type	Size
Streams	10/24/2022 11:50 AM	File folder	
one	10/24/2022 12:21 PM	Text Document	0 KB

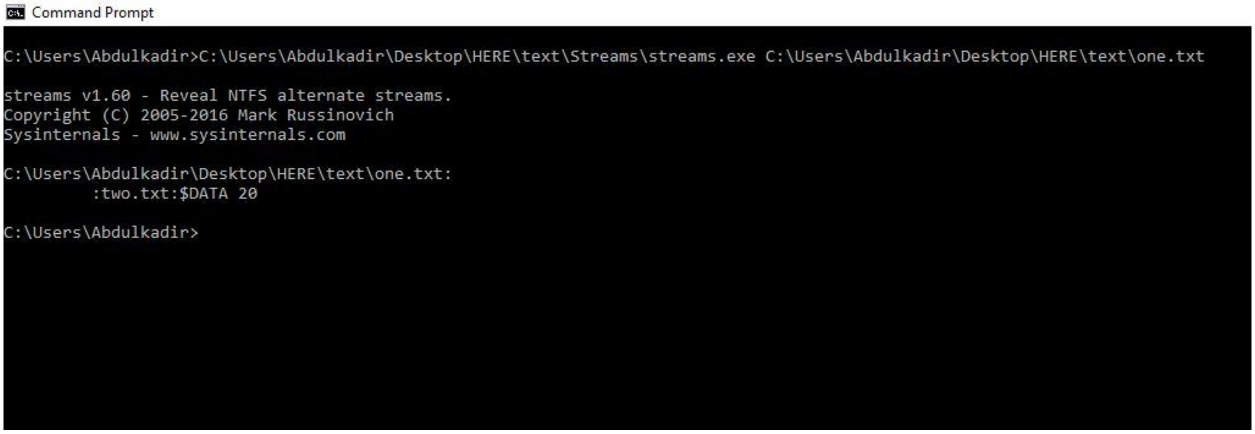
Step 7: if you want to see how many hidden file are stored in the ordinary file use this command stream.exe path + ordinary file's path example

My stream.exe path is: C:\Users\Abdulkadir\Desktop\HERE\text\Streams\streams.exe

My ordinary file's path is

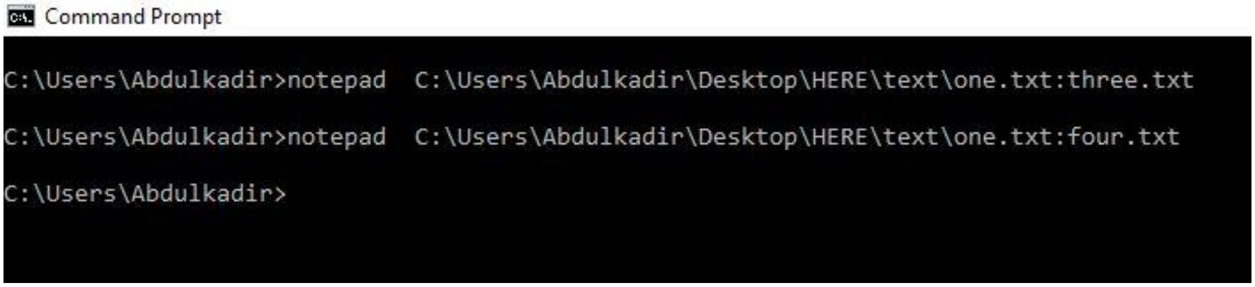
C:\Users\Abdulkadir\Desktop\HERE\text\one.txt

So combine both paths and enter in CMD

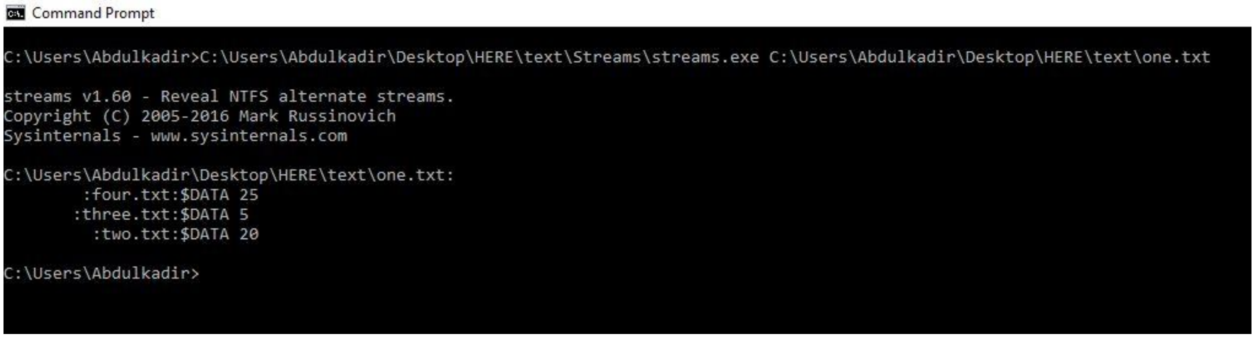


```
C:\Users\Abdulkadir>C:\Users\Abdulkadir\Desktop\HERE\text\Streams\streams.exe C:\Users\Abdulkadir\Desktop\HERE\text\one.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:
         :two.txt:$DATA 20

C:\Users\Abdulkadir>
```

- We have one hidden file (Two.txt)
- Now let's hide two more files to see if we can hide more secret files in one ordinary file, we will be using the same method, let's file **three.txt** and **four.txt** and see the result



```
C:\Users\Abdulkadir>notepad  C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:three.txt

C:\Users\Abdulkadir>notepad  C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:four.txt

C:\Users\Abdulkadir>
```

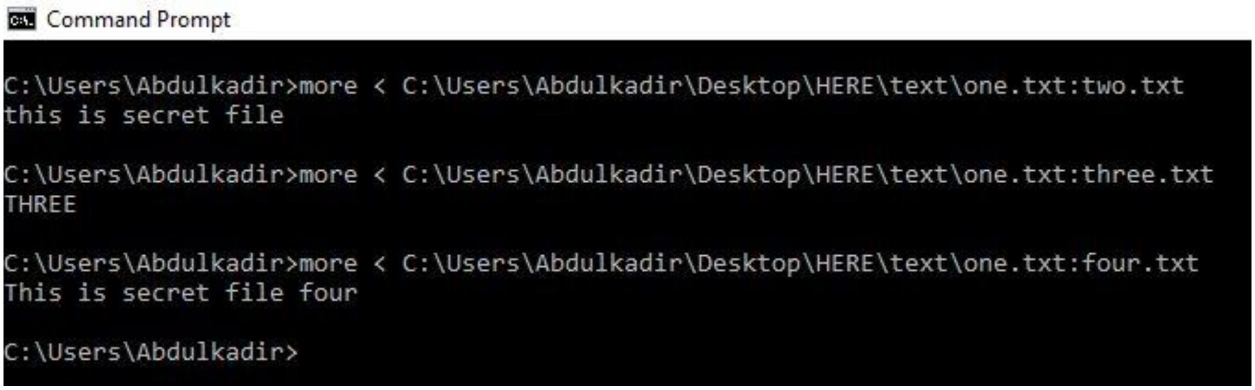


```
C:\Users\Abdulkadir>C:\Users\Abdulkadir\Desktop\HERE\text\Streams\streams.exe C:\Users\Abdulkadir\Desktop\HERE\text\one.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:
        :four.txt:$DATA 25
       :three.txt:$DATA 5
         :two.txt:$DATA 20

C:\Users\Abdulkadir>
```

- As you can see we have three hidden files, which are four.txt, three.txt and two.txt

Step 8: the final step is to see what is inside the hidden files, to open the secret file use this command line

More< path, ordinary_file_name.txt:secret_file_name.txt



```
C:\Users\Abdulkadir>more < C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:two.txt
this is secret file

C:\Users\Abdulkadir>more < C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:three.txt
THREE

C:\Users\Abdulkadir>more < C:\Users\Abdulkadir\Desktop\HERE\text\one.txt:four.txt
This is secret file four

C:\Users\Abdulkadir>
```

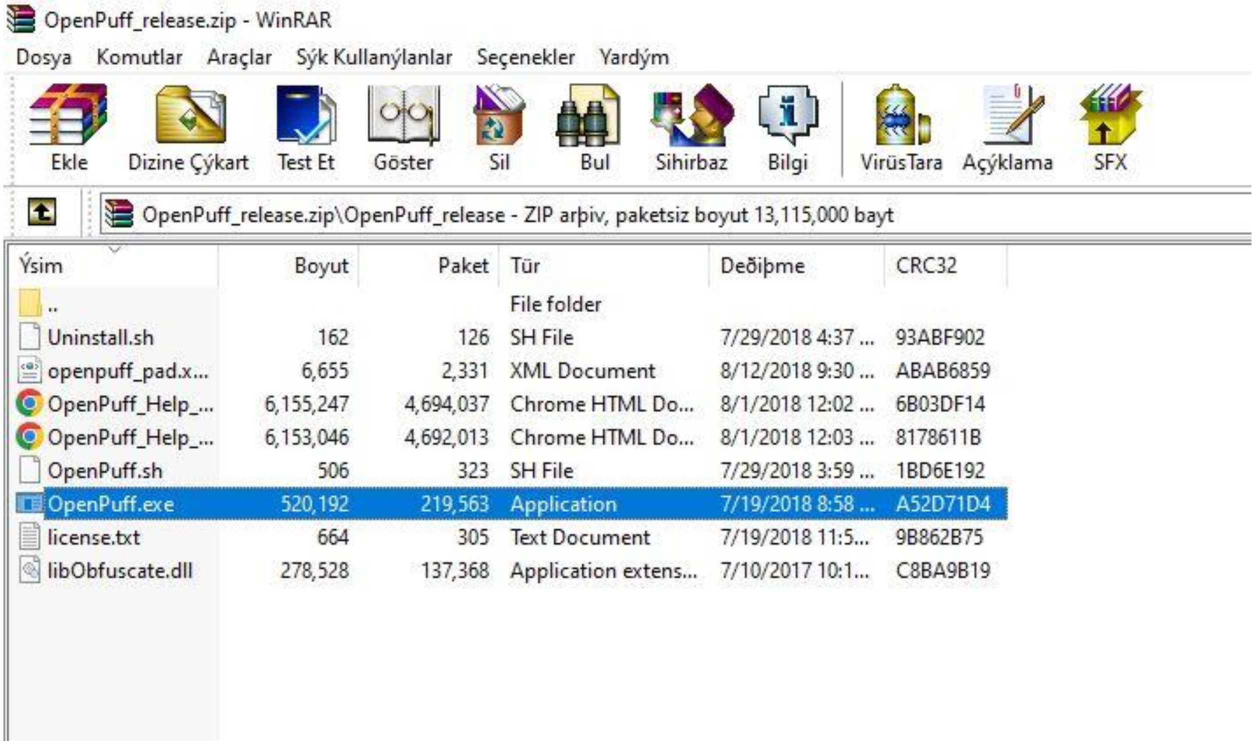
NOTE:The problem of this applications is that you cannot send the hidden files to others, because the hidden files is hidden in your PC, but it is still good way to create your own hidden massage, you may need to safe some texts like passwords etc..

Image Steganography

- Is hidden data inside image
- The original image and stego image (the image that has hidden data in it) must be the same.
- The hidden data must be undamaged even if the stego image were cropped or edited
- If the original image is not seen before then nobody will know how that image is changed, so it is better to use your own image
- **OpenPuff :** is also free application which let you hide text in image

Step 1: download the software https://www.filecroco.com/download-openpuff/download/#google_vignette

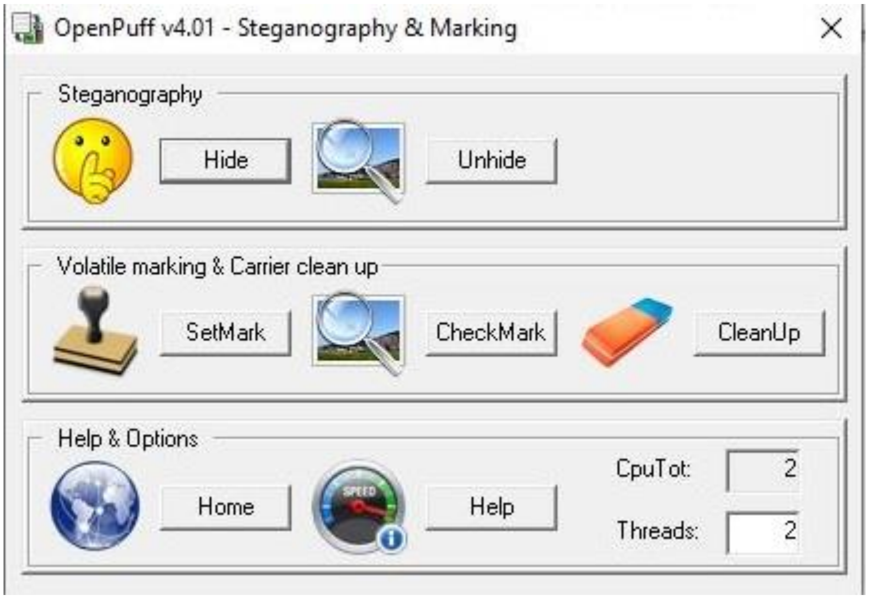
Step 2: install the application



OpenPuff_release.zip\OpenPuff_release - ZIP arþiv, paketsiz boyut 13,115,000 bayt

Ýsim	Boyut	Paket	Tür	Deðiþme	CRC32
..			File folder		
Uninstall.sh	162	126	SH File	7/29/2018 4:37 ...	93ABF902
openpuff_pad.x...	6,655	2,331	XML Document	8/12/2018 9:30 ...	ABAB6859
OpenPuff_Help_...	6,155,247	4,694,037	Chrome HTML Do...	8/1/2018 12:02 ...	6B03DF14
OpenPuff_Help_...	6,153,046	4,692,013	Chrome HTML Do...	8/1/2018 12:03 ...	8178611B
OpenPuff.sh	506	323	SH File	7/29/2018 3:59 ...	1BD6E192
OpenPuff.exe	520,192	219,563	Application	7/19/2018 8:58 ...	A52D71D4
license.txt	664	305	Text Document	7/19/2018 11:5...	9B862B75
libObfuscate.dll	278,528	137,368	Application extens...	7/10/2017 10:1...	C8BA9B19

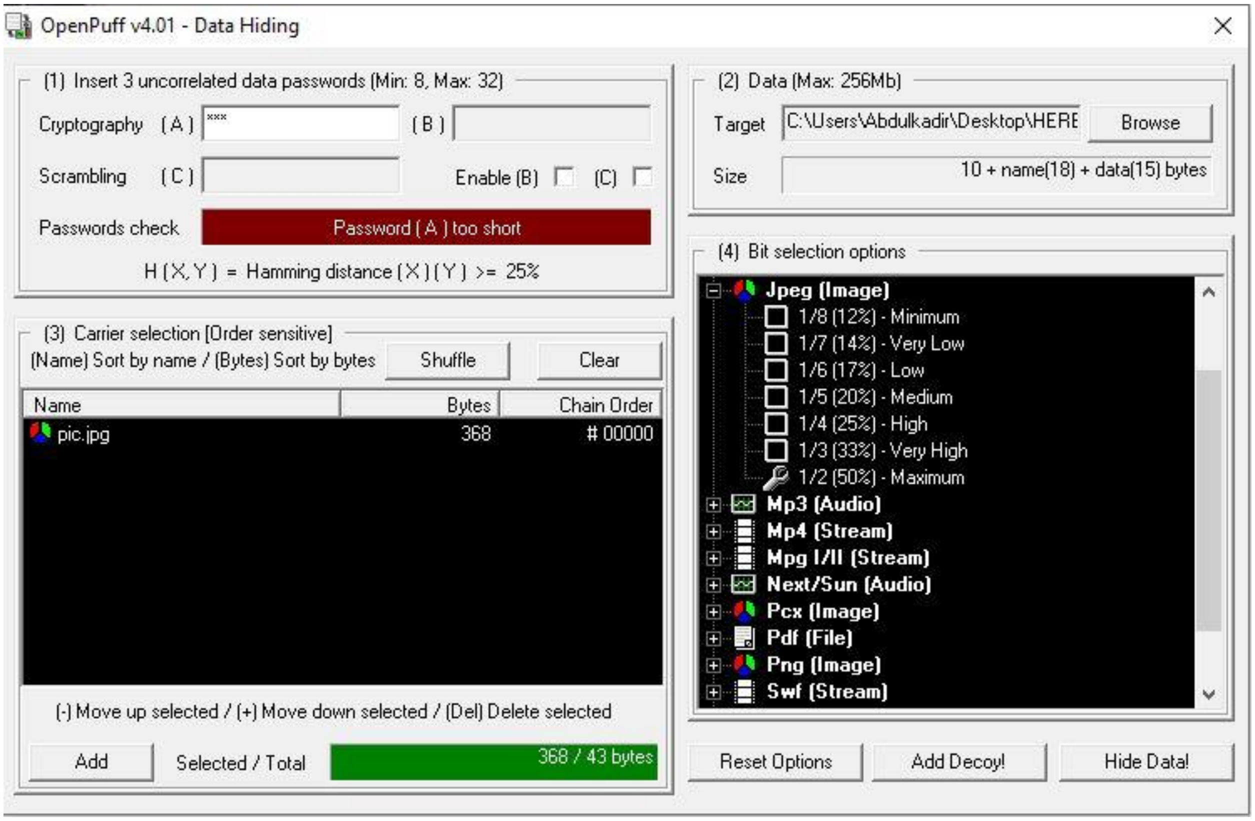
Step 3: To hide the secret massage, prepare the secret data and the cover image


OpenPuff v4.01 - Steganography & Marking
Steganography
Hide
Unhide
Volatile marking & Carrier clean up
SetMark
CheckMark
CleanUp
Help & Options
Home
Help

CpuTot: 2

Threads: 2

Click hide



OpenPuff v4.01 - Data Hiding

(1) Insert 3 uncorrelated data passwords (Min: 8, Max: 32)

Cryptography (A) *** (B)

Scrambling (C) Enable (B) □ (C) □

Passwords check: Password (A) too short

H(X,Y) = Hamming distance (X)(Y) >= 25%

(2) Data (Max: 256Mb)

Target: C:\Users\Abdulkadir\Desktop\HERE

Size: 10 + name(18) + data(15) bytes

(3) Carrier selection [Order sensitive]

(Name) Sort by name / (Bytes) Sort by bytes

Name	Bytes	Chain Order
pic.jpg	368	# 00000

(-) Move up selected / (+) Move down selected / (Del) Delete selected

Selected / Total: 368 / 43 bytes

(4) Bit selection options

- Jpeg (Image)
  - □ 1/8 (12%) - Minimum
  - □ 1/7 (14%) - Very Low
  - □ 1/6 (17%) - Low
  - □ 1/5 (20%) - Medium
  - □ 1/4 (25%) - High
  - □ 1/3 (33%) - Very High
  - 1/2 (50%) - Maximum
- Mp3 (Audio)
- Mp4 (Stream)
- Mpg I/II (Stream)
- Next/Sun (Audio)
- Pcx (Image)
- Pdf (File)
- Png (Image)
- Swf (Stream)

First Cryptograph (A) and (B): is where to enter your passwords, then uncheck the enable and (C) sections

Second Target (Browse): is where enter your secret file

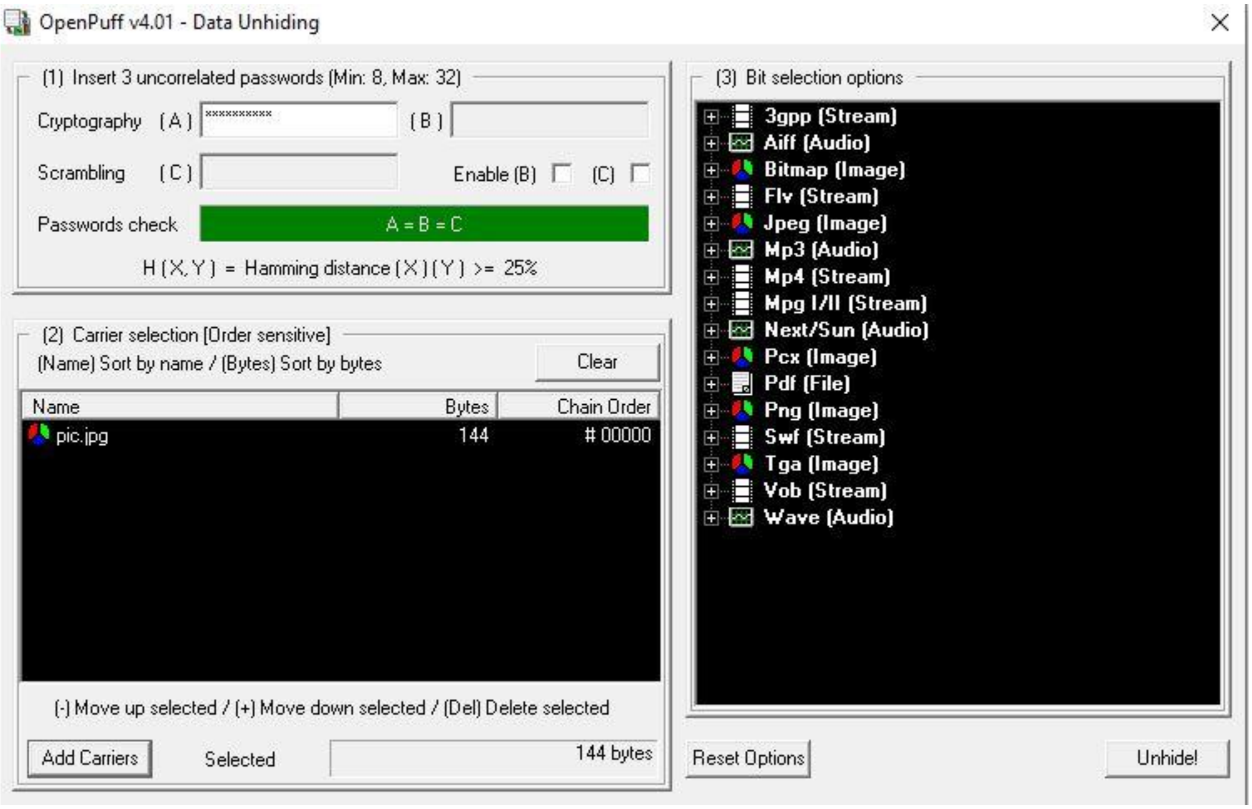
Third Add: is where you enter your cover image, when you finish these three then click

Forth in the bit selection options select JPEG then select maximum, finally click hide data! And save the image

s

- The pictures look exactly same

- Step 4: To unhide the secret massage


OpenPuff v4.01 - Data Unhiding

(1) Insert 3 uncorrelated passwords (Min: 8, Max: 32)

Cryptography (A) ********** (B)

Scrambling (C)

Enable (B) □ (C) □

Passwords check: A = B = C

H (X, Y) = Hamming distance (X) (Y) >= 25%

(2) Carrier selection [Order sensitive]

(Name) Sort by name / (Bytes) Sort by bytes

Name	Bytes	Chain Order
pic.jpg	144	# 00000

(-) Move up selected / (+) Move down selected / (Del) Delete selected

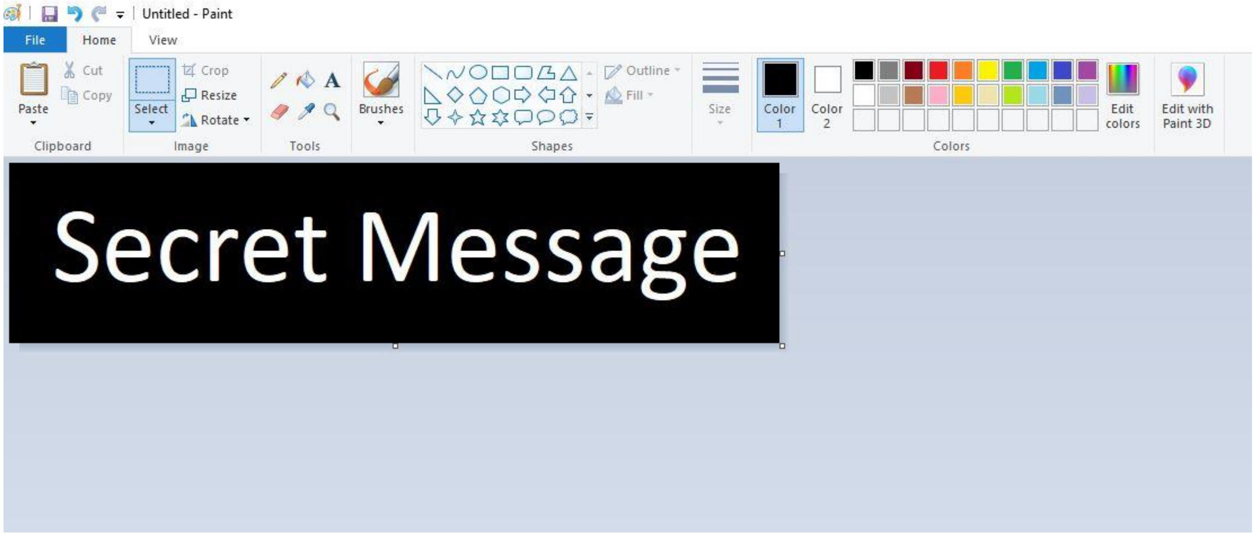
Selected: 144 bytes

(3) Bit selection options

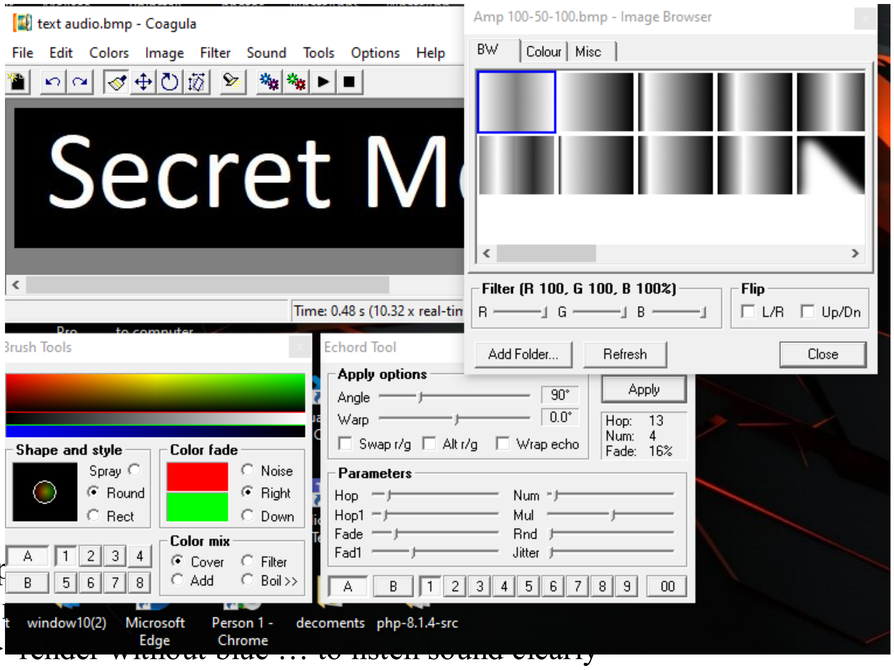
- Enter your password, uncheck the enable and (C) sections
- In add carriers add your stego-image then click unhide and save your secret file

Audio Steganography

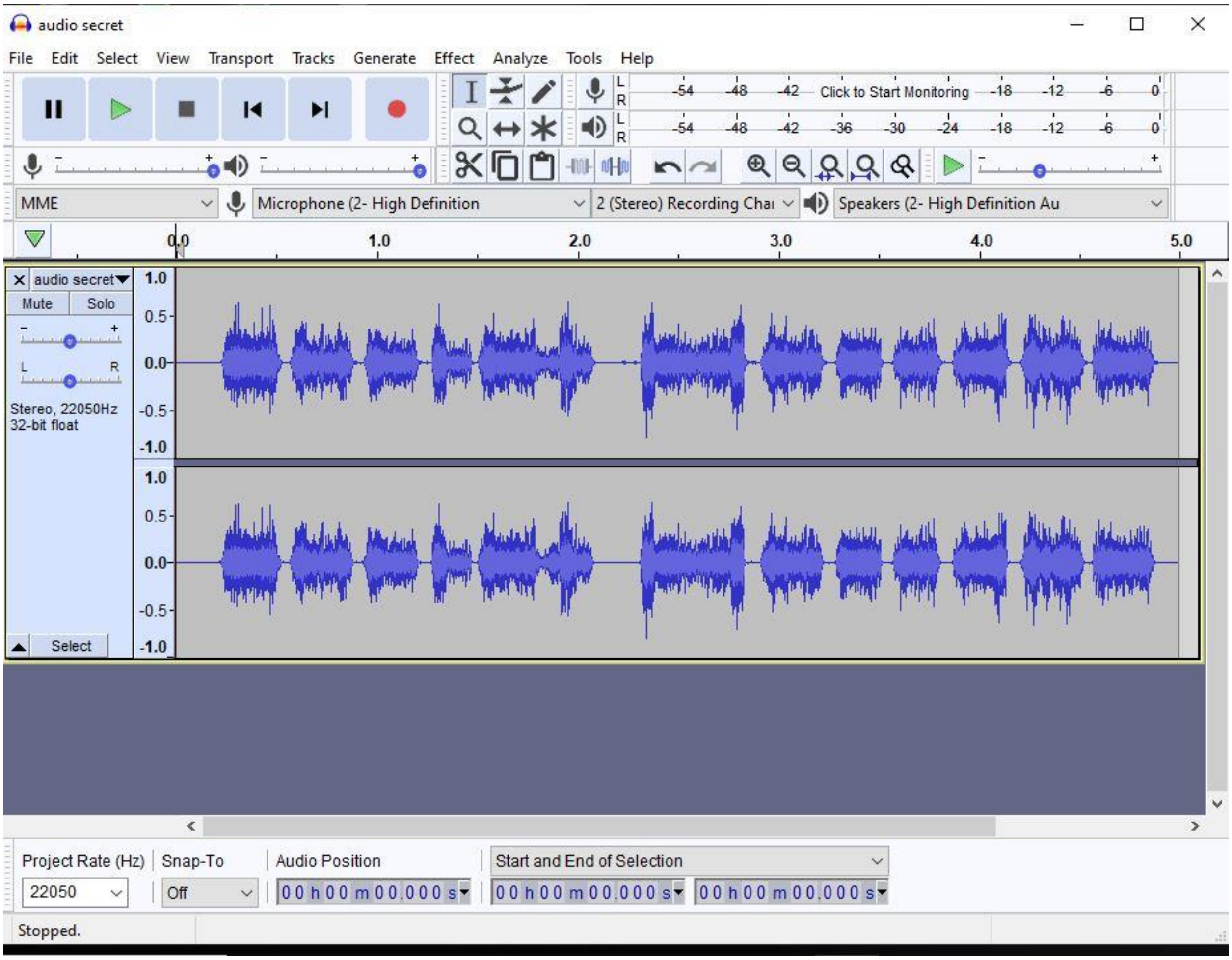
- Step 1: Create image with black background
- Write white text (hidden massage) in it, and save it as .BMP



- Step 2: Download COAGULA application to change your image into sound https://www.abc.se/~re/Coagula/Coagula.html



- File > op
- Tools > r
- Sound > render without blur … to listen sound clearly
- File > save sound as … to save the image as an audio
- Step 3: to change the audio to visible text Download AUDACITY Application and install https://getintopc.com/softwares/audio-processing/audacity-free-download/


audio secret
File Edit Select View Transport Tracks Generate Effect Analyze Tools Help
Click to Start Monitoring
MME
Microphone (2- High Definition
2 (Stereo) Recording Chai
Speakers (2- High Definition Au
audio secret
Mute
Solo
Select
0.0
1.0
2.0
3.0
4.0
5.0

Stereo, 22050Hz
32-bit float

Project Rate (Hz): 22050

Snap-To: Off

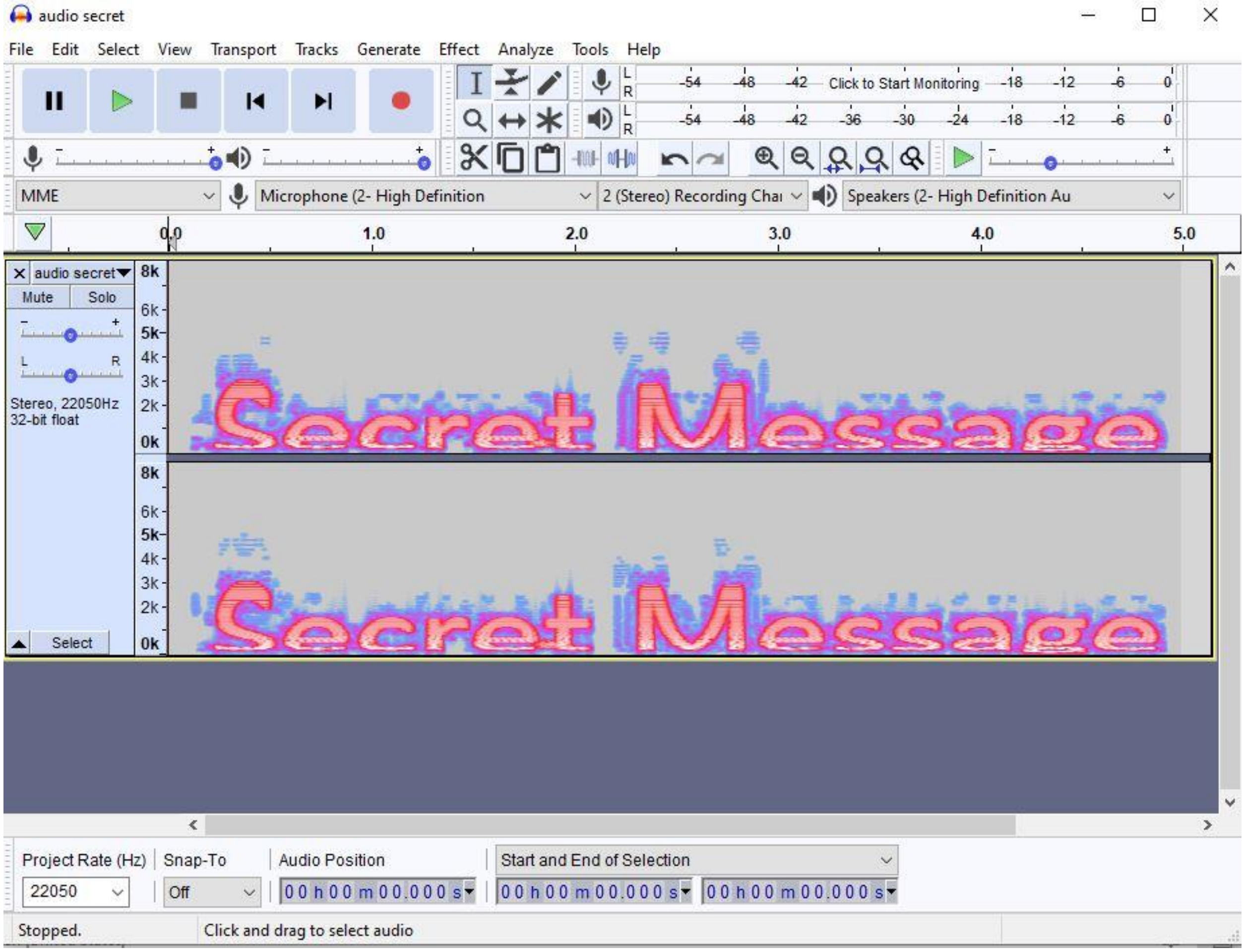
Audio Position: 00 h 00 m 00.000 s

Start and End of Selection: 00 h 00 m 00.000 s 00 h 00 m 00.000 s

Stopped.

First add the audio … file > open > and select the audio that you saved

Second to see the text inside the audio click audio secret > spectrogram


audio secret
File Edit Select View Transport Tracks Generate Effect Analyze Tools Help
Click to Start Monitoring
MME
Microphone (2- High Definition
2 (Stereo) Recording Chai
Speakers (2- High Definition Au
audio secret
Mute Solo
Stereo, 22050Hz
32-bit float
Select
Secret Message
Secret Message

Project Rate (Hz): 22050
Snap-To: Off
Audio Position: 00 h 00 m 00.000 s
Start and End of Selection: 00 h 00 m 00.000 s – 00 h 00 m 00.000 s
Stopped.
Click and drag to select audio

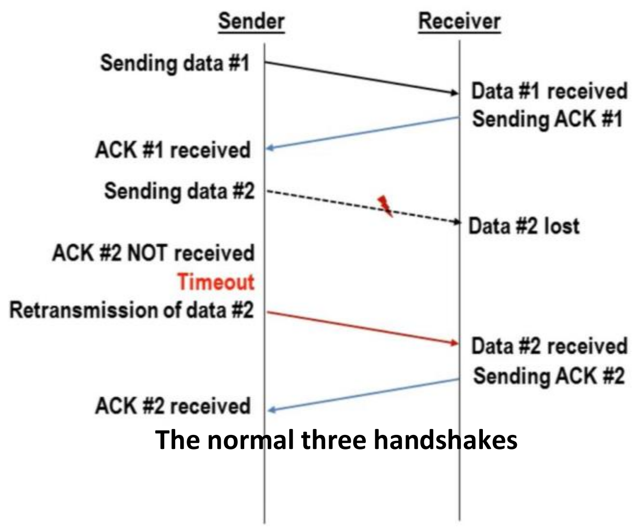
- NOTE: to make sure the hidden massage is completely invisible you can add song or other audio

Video Steganography

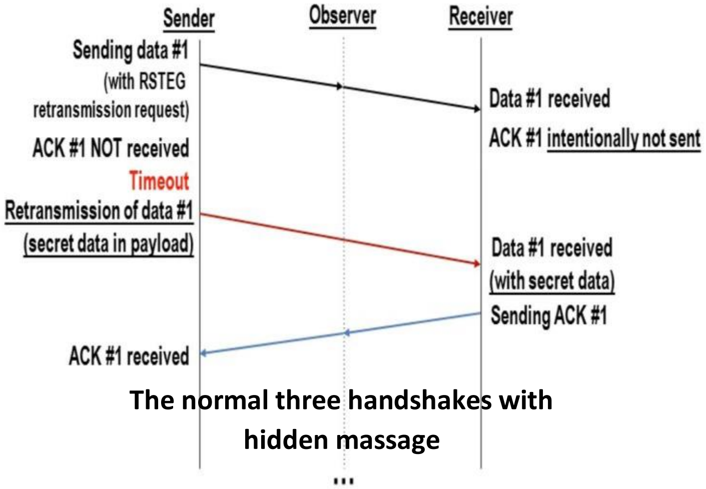
- Video Steganography is a combination of text Steganography, image Steganography and audio Steganography
- **Example of application you can create video steganography is 'DeEgger Embedder'is very easy application to hide secret file in video**

Network Steganography

- Is hidden secret massage in header of TCP, the sender replaces payload with secret massage and the receiver does not intentionally acknowledge



The normal three handshakes



The normal three handshakes with hidden massage

Email Steganography

- Hides the secret message within the email body and email addresses
- You can easily use https://www.spammimic.com/ to encode and decode texts.

Hackers and Steganography

- For hackers, hiding malicious code in an image or audio file is only half the battle. They also need a malicious or buggy program on the target's computer to run that code. That is why criminals use Steganography to deliver bad software into systems that have already been compromised

How Steganography can harm your computer system?

- Like all malware, image Steganography can be used to hide the payload within the code itself, or the code can call additional code or executables associated with attacks. That means that when an employee views the innocent-looking image, the payload is executed and can immediately start damaging the target company

Steganalysis

- To Attack and analysis hidden information may take several forms:
  - detecting
  - extracting
  - Disabling or destroying hidden information.
- The idea is same as cryptanalysis, but Steganalysis is more difficult because in Steganalysis, there is no algorithm, and no keys.

CONCLUSION of

1. In steganography, the biggest mistake is that the information is known, the information must be undetectable in the first place, even if they can't detect it they will destroy it
2. In text steganography using easy methods like, capital letters, underlines is also unsecure
3. Using well known and free software is unsecure, maybe there is a way to crack that software

4. Using public images (images you downloaded from internet), audio or video is also unsecure because if there is original image then it's easy to detect the secret