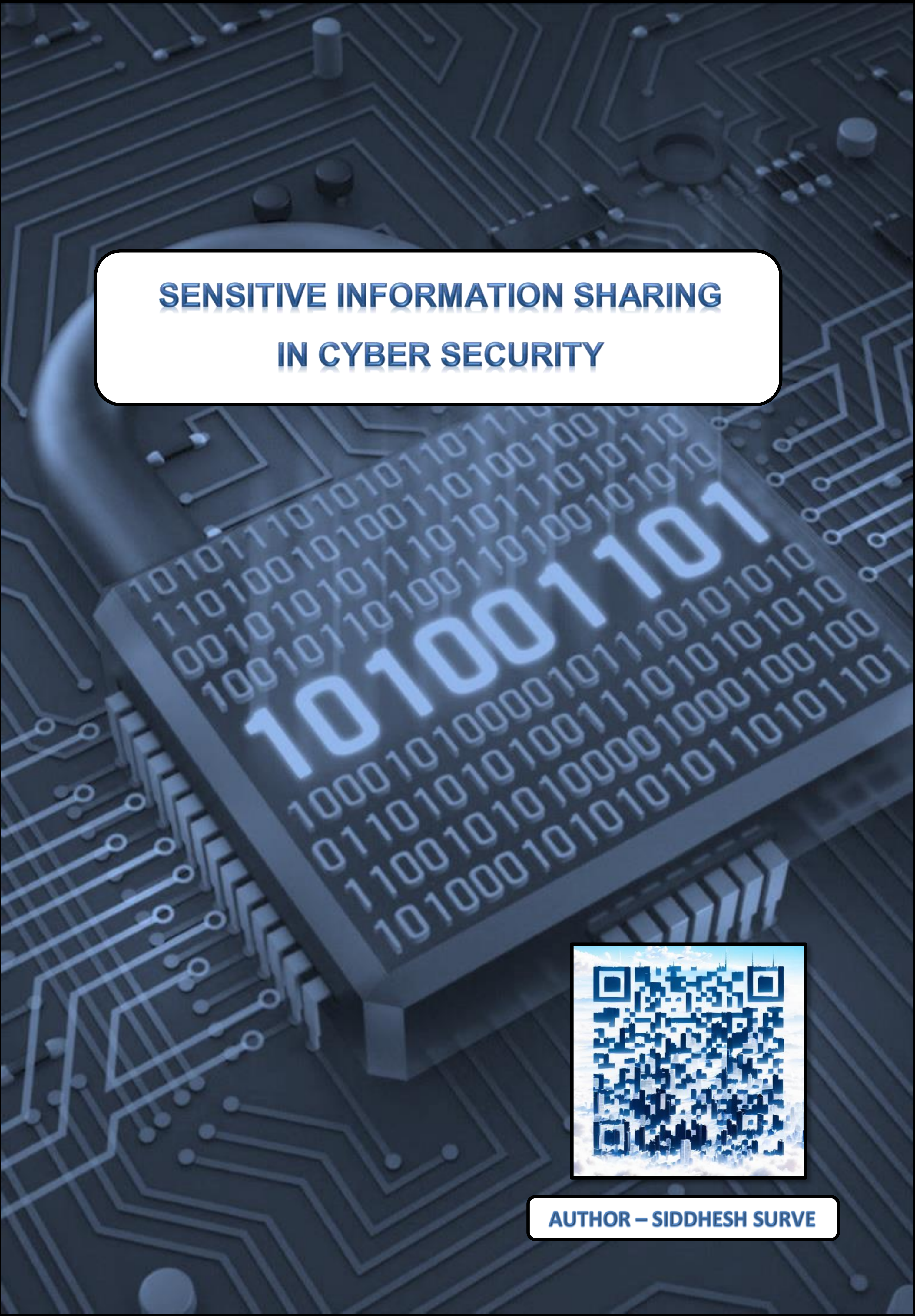
SENSITIVE INFORMATION SHARING IN CYBER SECURITY



AUTHOR – SIDDHESH SURVE

⚠ DISCLAIMER ⚠

This E - Book is for Educational Purpose only & does not Promote or Encourage performing Illegal Activities

It is recommended to use the Content only after Legal Advice

If any of Suspicious Activity or Misuse of Content is Suspected or Found, The Author of this E - Book & the respected Tools Authorities are not Responsible

Introduction

In this Era of Cyber Crime and Cyber Terrorism Attacks, basic and the most important factor is Beginning of Crime or War through Planning.
Planning in Cyber Crime or Cyber Terrorism is done through Communicating, Between the Team of Thefts and Cyber Criminals.
There are many Cyber Security Members and Cyber Crime Investigators, also the Ethical Hackers who follow these Techniques to share their Confidential Conversation or Data.

This Sharing of Secret Message or Data is not a Big Task. When u eventually Learn to perform, it is going to be just a Piece of Cake for you.
No Specific Hardware Requirements are needed except your Laptops or Computers, as this is not the only Technique or the way to Share Sensitive Information.
There are N numbers of Different Advanced Tools and Techniques to perform and I am Sharing One of them, also which I have Personally Created by Gaining some Juicy Knowledge and Learning Security Stuffs.

In Short, Let’s Understand the Scenario in Two Steps:

This Communication is achieved through a Brief Scenario –

- Part 1: Communication through Dark Web using Secret Message Sending & Receiving Functionality.
- Part 2: Encoding of Message Link / URL and then by using Encryption Technique to Secure and keep it Confidential between two Communicators.

What You Will Learn

What you are going to learn from this, is to Securely Share your Data without getting leaked or Spoofed by any Anonymous Hacker or their Teams.

Sharing of Secret Message through Encoding and Image Steganography Techniques and Using of Deep & Dark Web in TOR Browser.

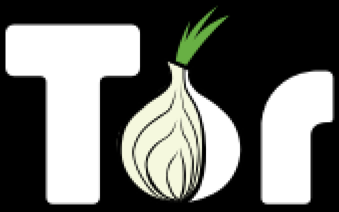
In this Short E-Book you'll understand and start to work on the above Scenario, without having any deep knowledge of Cyber Security.

I have already Developed Python Script and added all Settings and Documentation to Use the Tools and Technique, so u only need is to run and try executing the Project and using it only for Educational and Security Purpose Only.

Let’s Understand!

TOR BROWSER & ONION LINKS

First Let’s Understand, What actually is ‘TOR’ & it’s Browser -



Tor [The Onion Router] - A Decentralized Network that enhances online privacy and anonymity.

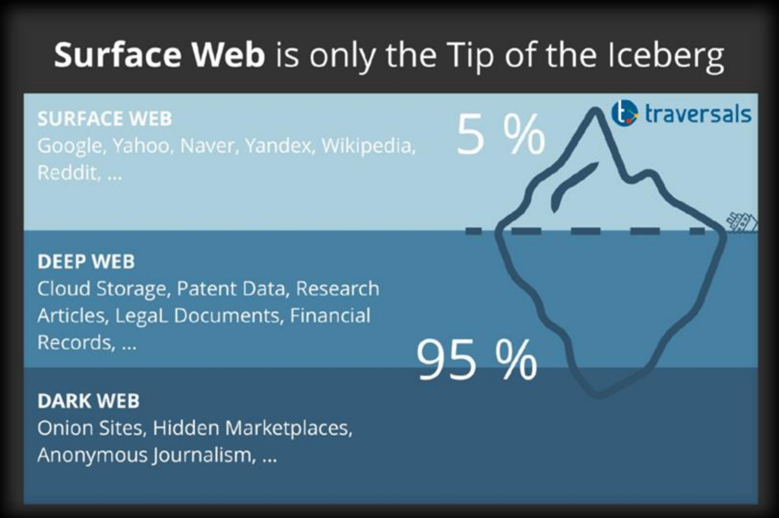
Here the Anonymity is very similar to Incognito Mode, which all of us use in Chrome or Firefox, Only point to know is Anonymity not only hide tracking of Data such as History or Cache, but also allows to hide IP Address while surfing on Web and much more extra features.

Tor Browser - Tor Browser is a Secure Web browser that incorporates the Tor network for enhanced privacy and anonymity. It is based on the Mozilla Firefox browser and includes additional features to protect user’s online activities. The Basic Search Engine Tor Browser uses is Duck Duck Go, a Highly Secure and privacy maintained Search Engine.

.onion - Like other domains such as .com, .in, .edu, .org, etc. The Tor Browser also executes .onion URL’s as these are the one used in Dark & Deep Web. These are also known as Tor links or hidden services, are websites or services that can only be accessed through the Tor network.

DEEP WEB & DARK WEB

The deep web refers to the portion of the internet that is not indexed by search engines and is inaccessible through regular web browsers. It includes private databases, password-protected websites, and other resources that require specific access permissions. The deep web is vast and contains legitimate content such as academic research, subscription-based services, and private intranets.


Surface Web is only the Tip of the Iceberg
SURFACE WEB
Google, Yahoo, Naver, Yandex, Wikipedia, Reddit, ...
5 %
traversals
DEEP WEB
Cloud Storage, Patent Data, Research Articles, LegaL Documents, Financial Records, ...
95 %
DARK WEB
Onion Sites, Hidden Marketplaces, Anonymous Journalism, ...

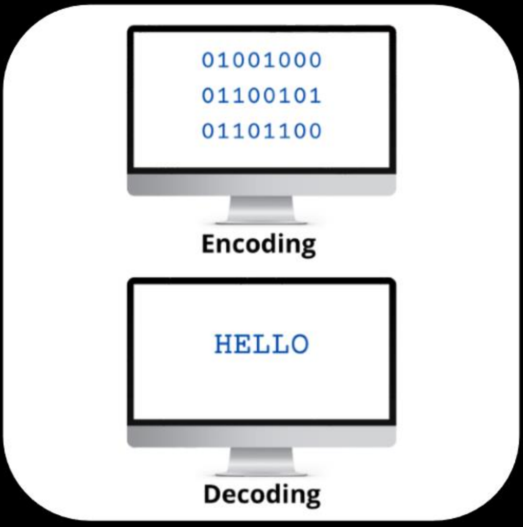
Dark Web, the Darkest Part of the World of Internet. A subset of the deep web, is a hidden network that can only be accessed using specialized software like Tor. It is known for hosting illicit activities, including illegal marketplaces, hacking forums, and sites offering stolen data or illegal services.

The Surface Web is what actually we use in our day to day life, normal searching, social media, Entertainment, etc.

Encoding Techniques & Image Steganography

Encoding -

Encoding is the process of applying a specific code, such as letters, symbols and numbers, to data for conversion into an equivalent cipher.



Some common encoding techniques -

- ASCII (American Standard Code for Information Interchange): ASCII is a character encoding standard that uses a 7-bit code to represent characters. It assigns numerical values to letters, numbers, and symbols, allowing computers to understand and display text.

- Unicode: Unicode is an international character encoding standard that aims to represent all characters from all writing systems. It uses a variable-length encoding scheme, allowing the representation of a vast range of characters, including various scripts, symbols, and emojis.

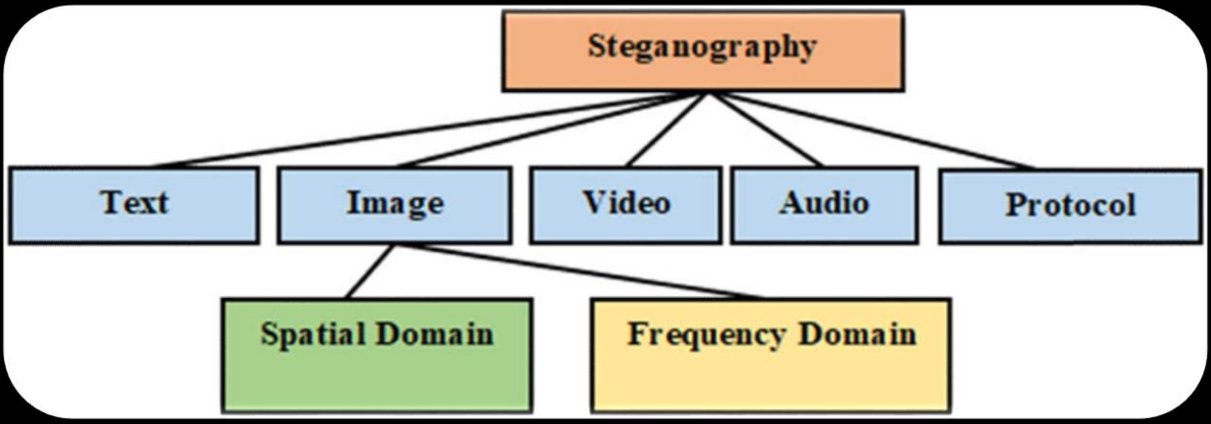
- Binary Encoding: Binary encoding represents data using a base-2 system, utilizing only two symbols: 0 and 1. It is commonly used in computing to store and process data at the lowest level, where each bit represents a binary value.

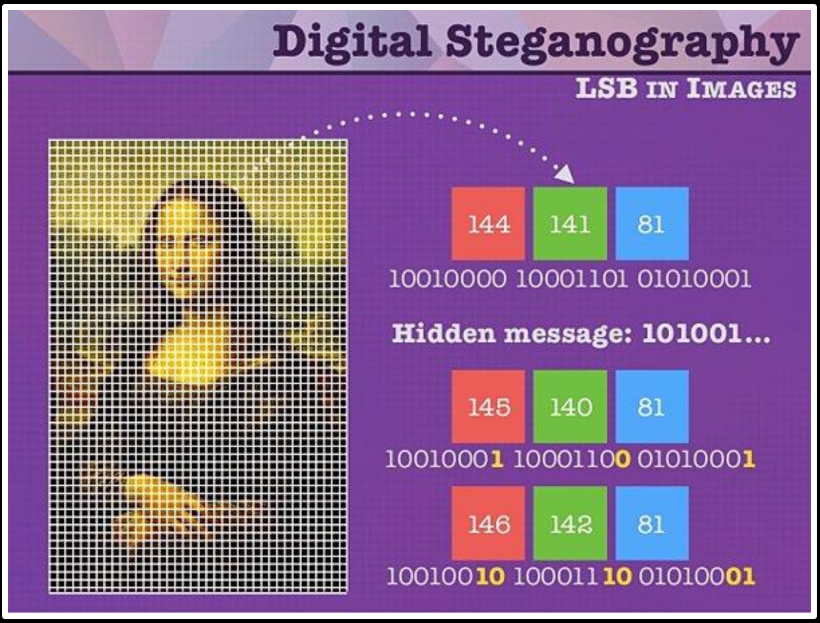
- Base64 Encoding: Base64 encoding convert's binary data into ASCII characters. It is often used to transmit binary data, such as images or files, over channels that only support ASCII characters, such as email or text-based protocols.

These are just a four examples of encoding techniques, and there are many more variations and specialized methods used in different domains and applications.

Image Steganography -

Image steganography is a technique used to hide secret information within an image without altering its visual appearance significantly. It involves embedding data, such as text, another image, or a file, into the pixels of an image in a way that is imperceptible to the human eye.





Here's a brief overview of how image steganography works:

- Selecting Cover Image: A cover image is chosen as the carrier for the secret data. It could be any digital image in common formats like JPEG, PNG, or BMP.

- Secret Data Embedding: The secret data is divided into smaller units, such as individual bits or groups of pixels. The cover image's pixel values are modified slightly to accommodate the secret data. The changes are often subtle and imperceptible.

- Encoding Algorithm: An encoding algorithm determines how the secret data is embedded into the cover image. Common techniques include Least Significant Bit (LSB) substitution, where the least significant bits of pixel values are replaced with secret data bits.

- Steganography Tools: Various software tools and libraries are available that automate the process of image steganography. These tools provide easy-to-use interfaces for embedding and extracting hidden data.

- Decoding and extraction: To extract the hidden data, the stego-image (the modified cover image) is processed using a compatible decoding algorithm. The algorithm reverses the embedding process and retrieves the secret data.

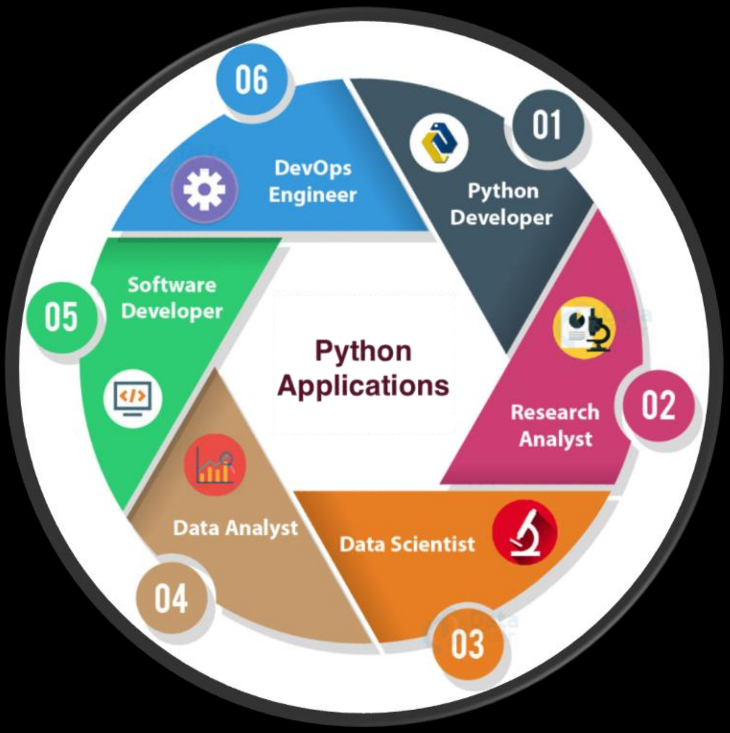
PYTHON PROGRAMMING LANGUAGE

Python is a popular high-level programming language known for its simplicity, readability, and versatility.

It offers a clean syntax and supports multiple programming paradigms, including procedural, object-oriented, and functional programming.

Python comes with a comprehensive standard library that provides pre-built modules for various tasks, reducing the need for external dependencies.

It is cross-platform compatible, making it suitable for different operating systems.

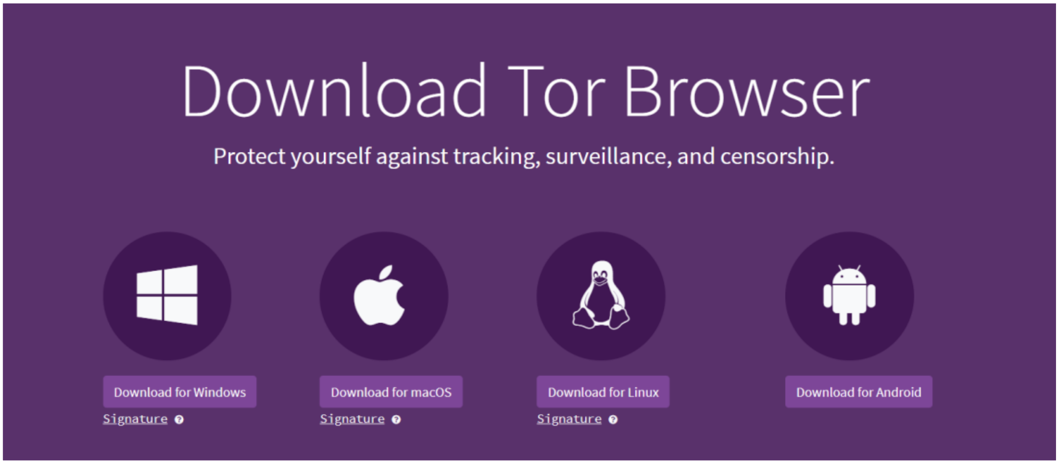


Let’s Execute!

Note: We are going to implement all the steps in following TOR Browser only, to maintain Security and Anonymity of Sharing, Every Link used to Encode-Decode or to shorten the URL, we are going to perform only in this Browser.

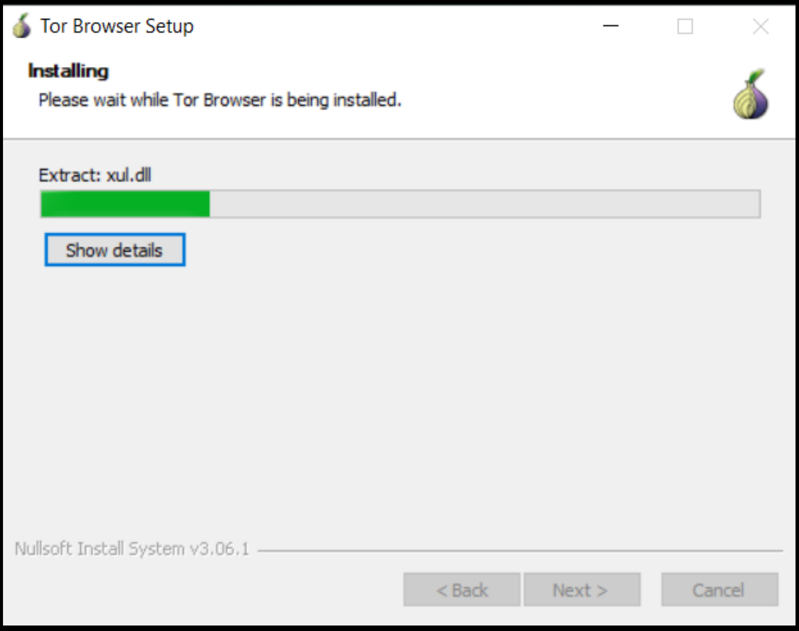
Creating & Encoding Secret Message through Link / URL using Tor Web Browser

- Download & Install Latest Version of TOR Browser from below Website https://www.torproject.org/download/ - Click on Download for Windows



Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.



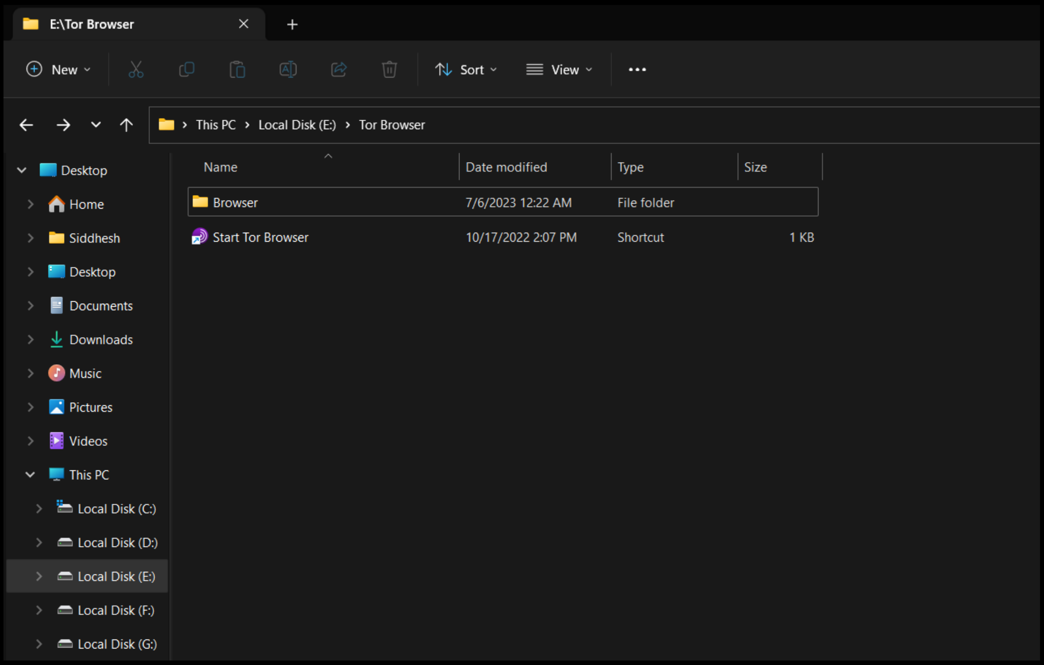
Tor Browser Setup

Installing

Please wait while Tor Browser is being installed.

Extract: xul.dll

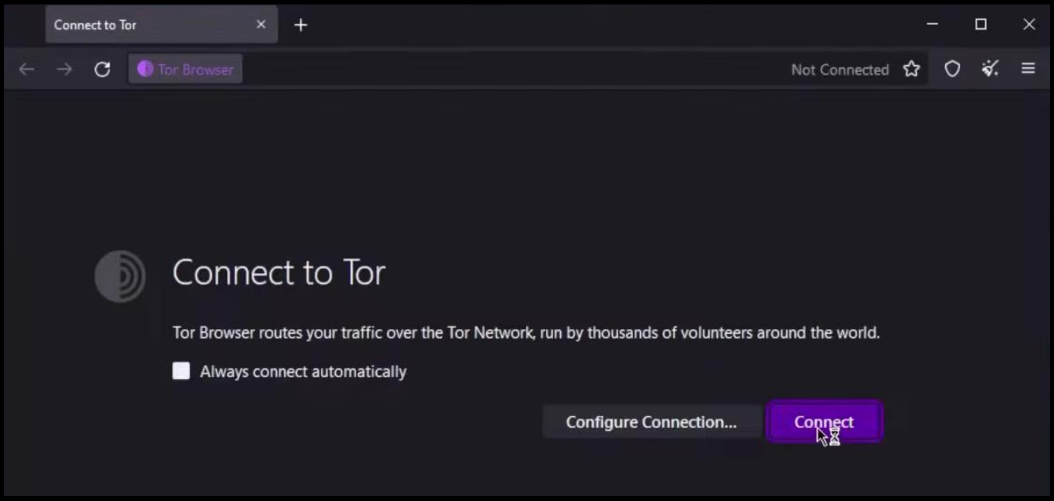
- After Installing the Tor Browser Setup, Go to the Installed Folder & click on Start Tor Browser



Name	Date modified	Type	Size
Browser	7/6/2023 12:22 AM	File folder	
Start Tor Browser	10/17/2022 2:07 PM	Shortcut	1 KB

- Click on checkbox Always connect automatically & Click on Connect.

- Wait for a While to Load the Browser & Search Engine.



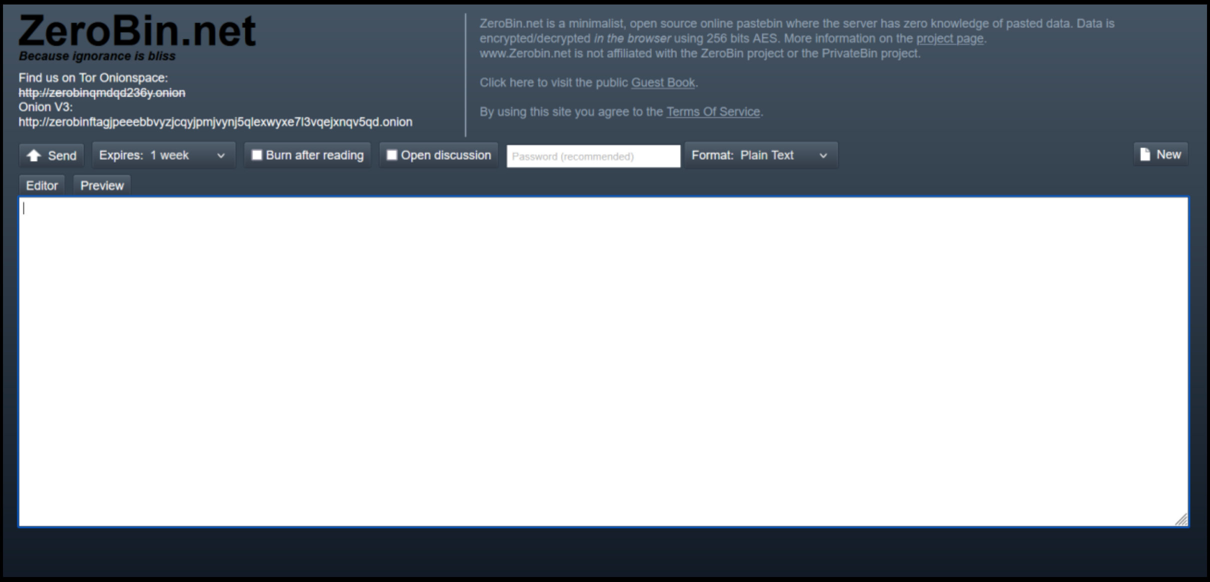
Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

□ Always connect automatically

Note: To visit Dark Web in Tor Browser, you should have different types of Onion URLs which are not similar to our regular Websites or URLs, in our case it is Secret Message Sending & Receiving.

- ➢ Visit the Onion Website given Below
  http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/



ZeroBin.net

Because ignorance is bliss

Find us on Tor Onionspace:
~~http://zerobinqmdqd236y.onion~~
Onion V3:
http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion

ZeroBin.net is a minimalist, open source online pastebin where the server has zero knowledge of pasted data. Data is encrypted/decrypted *in the browser* using 256 bits AES. More information on the project page.
www.Zerobin.net is not affiliated with the ZeroBin project or the PrivateBin project.

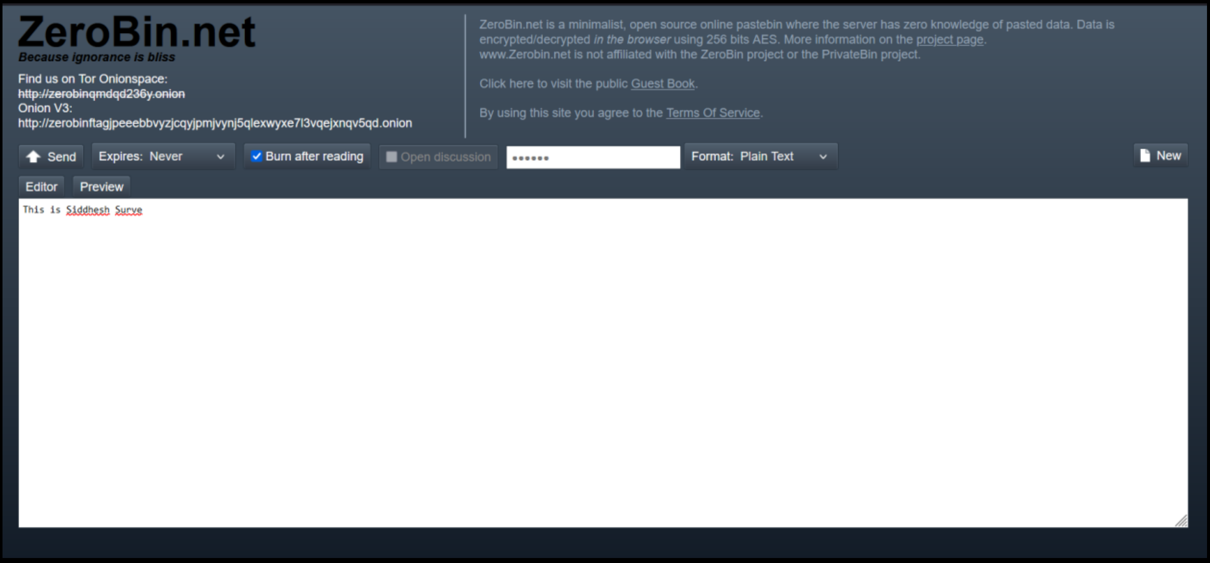
Click here to visit the public Guest Book.

By using this site you agree to the Terms Of Service.

Securities to follow when creating Message Link –

- Select Expires - Never or as per your Sending and Receiving Period
- Select Checkbox Burn after Reading
- Enter Password for more Security

- Below is the Snapshot of Custom Message Creation



ZeroBin.net
Because ignorance is bliss

Find us on Tor Onionspace:
~~http://zerobinqmdqd236y.onion~~
Onion V3:
http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion

ZeroBin.net is a minimalist, open source online pastebin where the server has zero knowledge of pasted data. Data is encrypted/decrypted *in the browser* using 256 bits AES. More information on the project page.
www.Zerobin.net is not affiliated with the ZeroBin project or the PrivateBin project.

Click here to visit the public Guest Book.

By using this site you agree to the Terms Of Service.

```
This is Siddhesh Surve
```

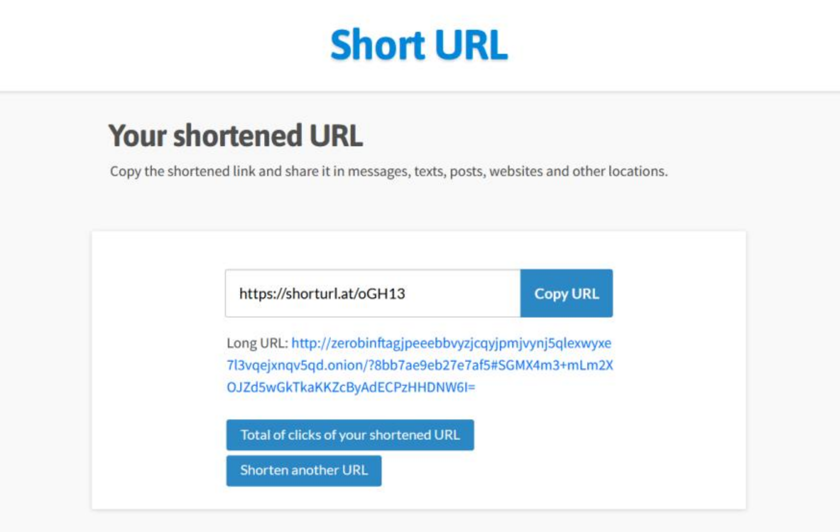
- Click on Send and you will get a Message Link
  For eg:

http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/?8bb7ae9eb27e7af5#SGMX4m3+mLm2XOJZd5wGkTkaKKZcByAdECPzHHDNW6I=

Copy the link and paste it in notepad for a while

- Shorten the Message Link in - https://shorturl.at/

- Copy the Shortened link from the website



Short URL

Your shortened URL

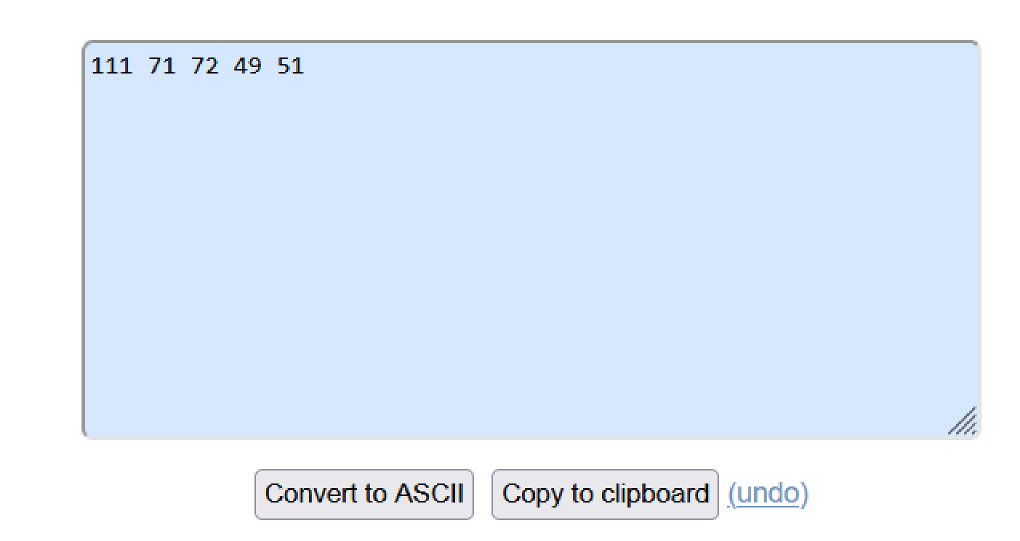
Copy the shortened link and share it in messages, texts, posts, websites and other locations.

https://shorturl.at/oGH13

Long URL: http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/?8bb7ae9eb27e7af5#SGMX4m3+mLm2XOJZd5wGkTkaKKZcByAdECPzHHDNW6I=

- Copy the Last Five Characters of Link for eg: https://shorturl.at/oGH13 then the last five characters are – oGH13 and paste it in notepad for a while

- Convert the Copied Text into Ascii from below Website https://www.browserling.com/tools/text-to-ascii



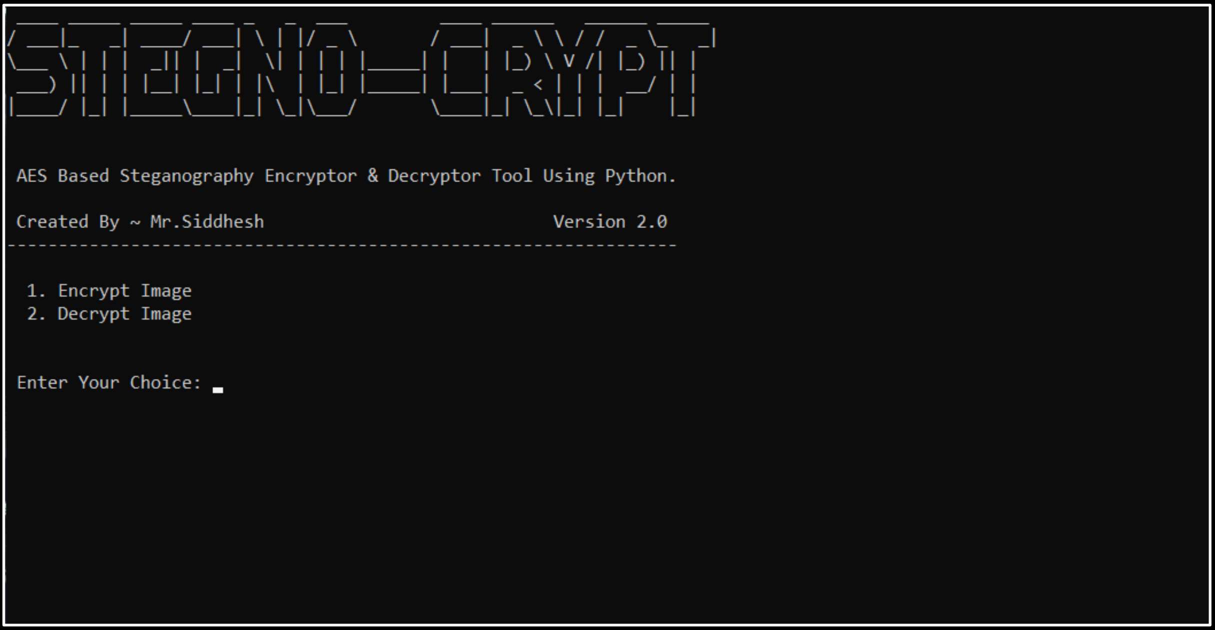
```
111 71 72 49 51
```

oGH13 → 111 71 72 49 51

- Copy the Converted Ascii Code for eg: 111 71 72 49 51 and paste it into notepad for a while

Encrypting Secret Code in an Image using Image Steganography

- Use Stegno-Crypt Python Tool to Encrypt the Ascii Code in the provided logo.png Image, Steps to do the following is mentioned in the Tool’s Folder & Documentation.



```
 ____ _____ _____ ____ _   _  ___         ____ ______   ______ _____
/ ___|_   _| ____/ ___| \ | |/ _ \       / ___|  _ \ \ / /  _ \_   _|
\___ \ | | |  _|| |  _|  \| | | | |_____| |   | |_) \ V /| |_) || |
 ___) || | | |__| |_| | |\  | |_| |_____| |___|  _ < | | |  __/ | |
|____/ |_| |_____\____|_| \_|\___/       \____|_| \_\|_| |_|    |_|


 AES Based Steganography Encryptor & Decryptor Tool Using Python.

 Created By ~ Mr.Siddhesh                                    Version 2.0
-----------------------------------------------------------------

  1. Encrypt Image
  2. Decrypt Image


 Enter Your Choice:
```

The Image used to Encrypt the Code -

logo.png

Here, I have created a Python Script to Encrypt and Decrypt Hidden Data in an Image, The Following Code works on the below artefacts -

- AES [Advanced Encryption Standard] Algorithm:

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm. AES has become a standard for securing sensitive information and is used in various applications and protocols. Same key is used for both encryption and decryption. The encryption and decryption processes are symmetric operations. AES operates on blocks of data and supports key sizes of 128, 192, and 256 bits.

- LSB [Least Significant Bit] Encoding Technique:

A technique used in digital steganography to hide information within the least significant bits of a carrier signal, such as an image or audio file. It takes advantage of the fact that changing the least significant bit of a pixel value or sample in an audio file typically does not significantly alter the perceptual quality of the signal. The binary representation of the secret message is embedded by replacing the least significant bit of each pixel or sample in the carrier signal with a bit from the secret message.

After Hiding the Data inside the Image Pixels, the image is as follows -

Logo_enc.png

So, What is changed here! The Image looks the same right?

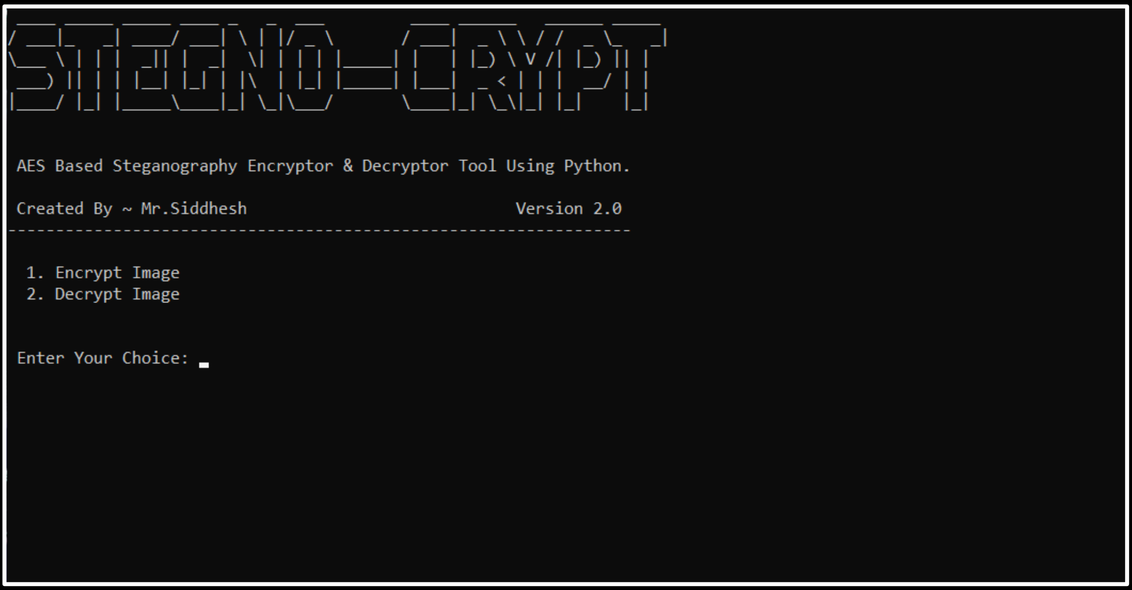
Answer is simply No, when you look closer in the Image u will find at a point, there are some particular pixel values which have been replaced but it doesn’t affect the Image Quality, but the Size here is bit increased from 27 kb to 84 kb.

In above Snapshot, The Image is zoomed up to 200 times until we get to see the change in pixel values of the Image. The grey colour line indicates the pixels contain some hidden information.

Here we have achieved the Sharing Element from our Side (Sender’s Side), now this Image is sent through mail or other social media source (Note: while Sending or Receiving the Image through Social Media, It should be only sent through form of Document, so the pixel values or other data is not replaced or compressed.)

Receiving & Fetching Hidden Data from the Image [Receiver’s side]

- The Receiver decrypts the Image using the respective tool.



```
 ____ _____ _____ ____ _   _  ___         ____ ______   ______ _____
/ ___|_   _| ____/ ___| \ | |/ _ \       / ___|  _ \ \ / /  _ \_   _|
\___ \ | | |  _|| |  _|  \| | | | |_____| |   | |_) \ V /| |_) || |
 ___) || | | |__| |_| | |\  | |_| |_____| |___|  _ < | | |  __/ | |
|____/ |_| |_____\____|_| \_|\___/       \____|_| \_\|_| |_|    |_|


 AES Based Steganography Encryptor & Decryptor Tool Using Python.

 Created By ~ Mr.Siddhesh                                   Version 2.0
-----------------------------------------------------------------

  1. Encrypt Image
  2. Decrypt Image


 Enter Your Choice: _
```

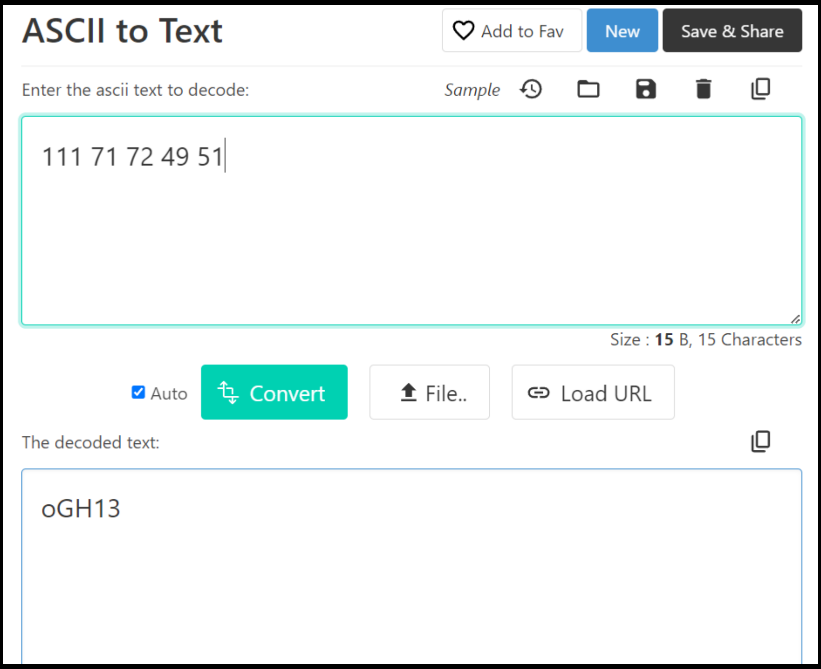
- The Ascii Code hidden inside the Image is Obtained

- Copy the Converted Ascii Code for eg: 111 71 72 49 51 and paste it into notepad for a while

- Now we need to decode the Ascii code to fetch the last characters of link.

- Paste the Ascii code into –

  https://codebeautify.org/ascii-to-text



Enter the ascii text to decode:

111 71 72 49 51

Size : **15** B, 15 Characters

☑ Auto

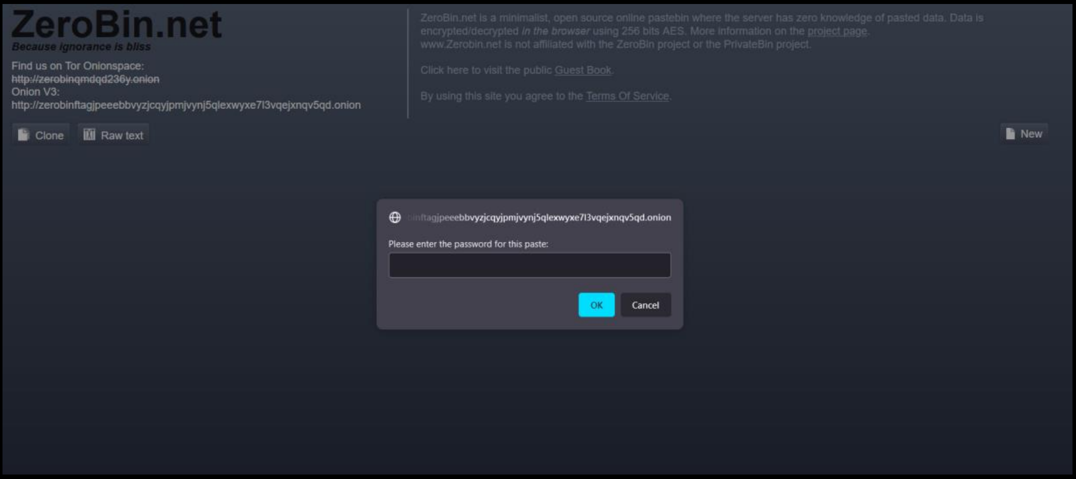
The decoded text:

oGH13

111 71 72 49 51 → oGH13

- Copy the Decoded characters for eg: oGH13 and paste it into notepad for a while
- Now, the Receiver is aware about the Shorten Link so, we paste the Characters simply after the / in the link.
- The Link will look like - https://shorturl.at/oGH13

- The original .onion link will load as shown below



ZeroBin.net

Because ignorance is bliss

Find us on Tor Onionspace:
~~http://zerobinqmdqd236y.onion~~
Onion V3:
http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion

ZeroBin.net is a minimalist, open source online pastebin where the server has zero knowledge of pasted data. Data is encrypted/decrypted *in the browser* using 256 bits AES. More information on the project page.
www.Zerobin.net is not affiliated with the ZeroBin project or the PrivateBin project.

Click here to visit the public Guest Book.

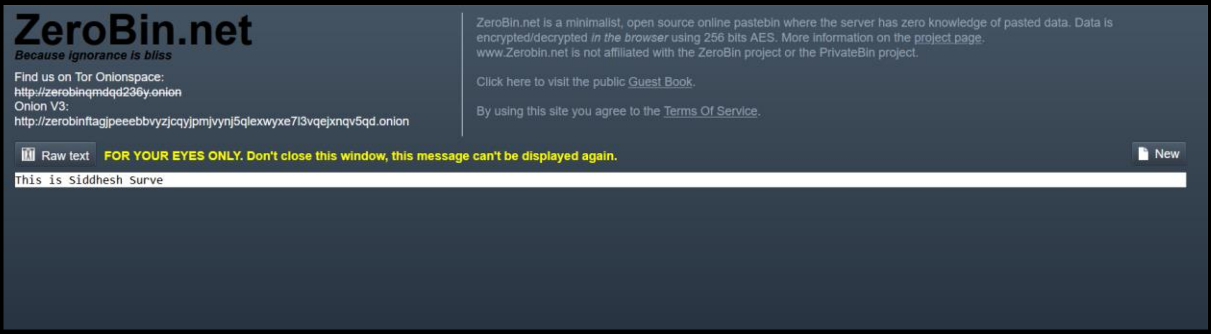
By using this site you agree to the Terms Of Service.

…inftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion

Please enter the password for this paste:

Note: Here the Password is the one which we kept while creating the Message Link, the Same Password should be used while creating each Link as it is only as the Password is only known by Sender and the Receiver.

- Enter the Password, to finally Reveal the Secret Message or Data Shared



ZeroBin.net

Because ignorance is bliss

Find us on Tor Onionspace:
~~http://zerobinqmdqd236y.onion~~
Onion V3:
http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion

ZeroBin.net is a minimalist, open source online pastebin where the server has zero knowledge of pasted data. Data is encrypted/decrypted *in the browser* using 256 bits AES. More information on the project page.
www.Zerobin.net is not affiliated with the ZeroBin project or the PrivateBin project.

Click here to visit the public Guest Book.

By using this site you agree to the Terms Of Service.

FOR YOUR EYES ONLY. Don't close this window, this message can't be displayed again.

```
This is Siddhesh Surve
```

Here we have achieved the Message, so here we already applied some securities while creating the link, the condition here is – If the Link is refreshed or reloaded, it will be destroyed and will not display again.

Next Level Security Right! → No Chances to trace-back the Link or the Message.

- Simply take the Screenshot of the Message before it is Vanished

- Want more Privacy & Anonymity, so that the Message is only readable by you without letting known by other third party.

  Just Encrypt the Message using the Image Steganography Tool!
  So, no need to worry about Privacy issues, Decrypt anytime you want!

As I said earlier, At the End of this E - Book you are going to achieve one of the Advanced and Easy Way to Share Sensitive & Confidential Information through Cyber Security.

I Hope this will help you to learn and understand the topics covered in this Short E - Book.

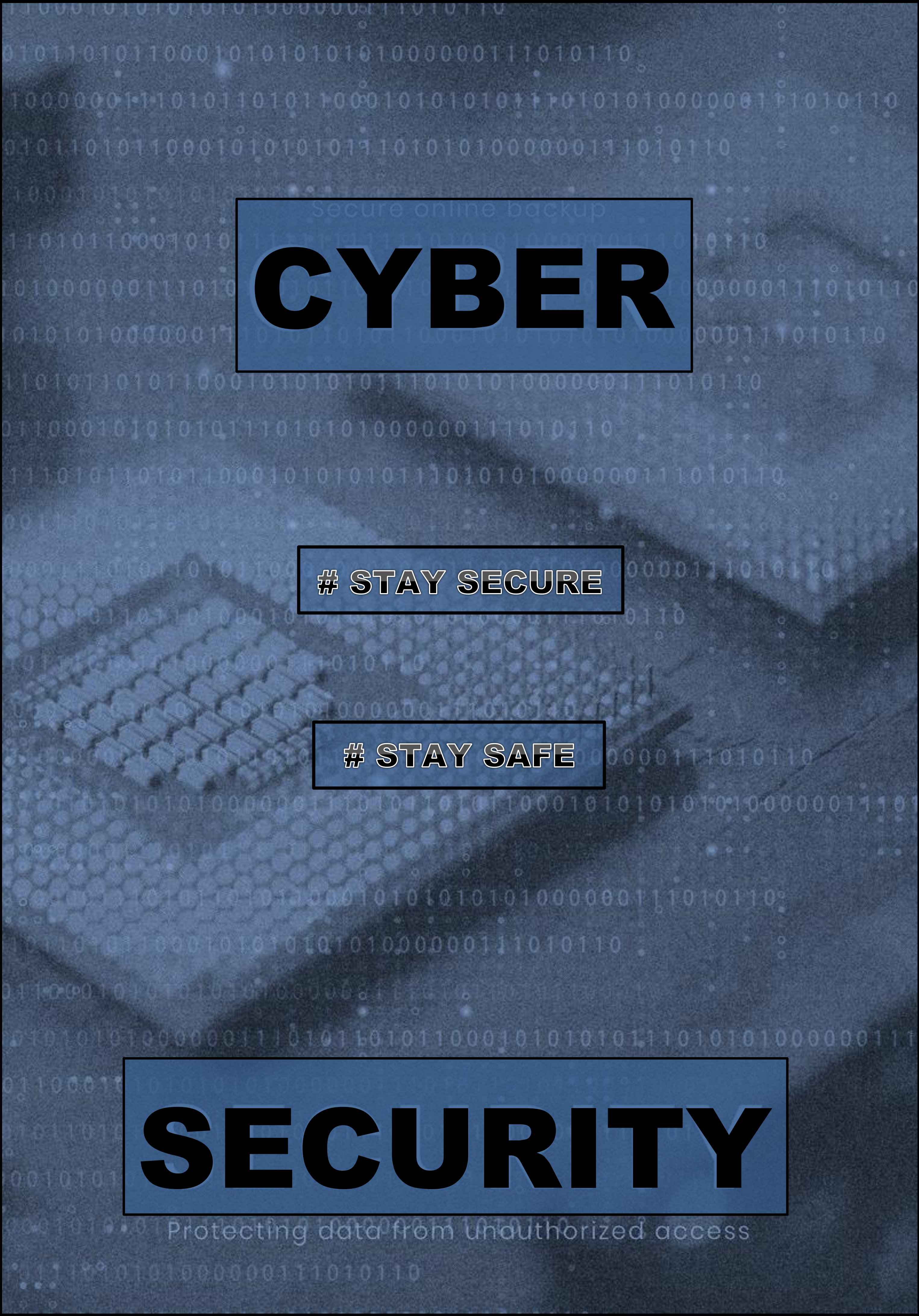
More Cyber Security related Stuff is coming….

Do Scan the QR Code on the very First Page, to follow me on GitHub and Checkout the tools I have built till now.

To Download the Python Image Steganography Tool & other Requirements from the Below Link

https://github.com/WhiteHat-Hunter/Sensitive-Information-Sharing

THANKYOU !



Secure online backup

CYBER

STAY SECURE

STAY SAFE

SECURITY

Protecting data from unauthorized access