vishwaCTF

CHALLENGE NAME: [Lost Code of the Past]

DEV : [Rakshika Batra]

CATEGORY:

[Cryptography]

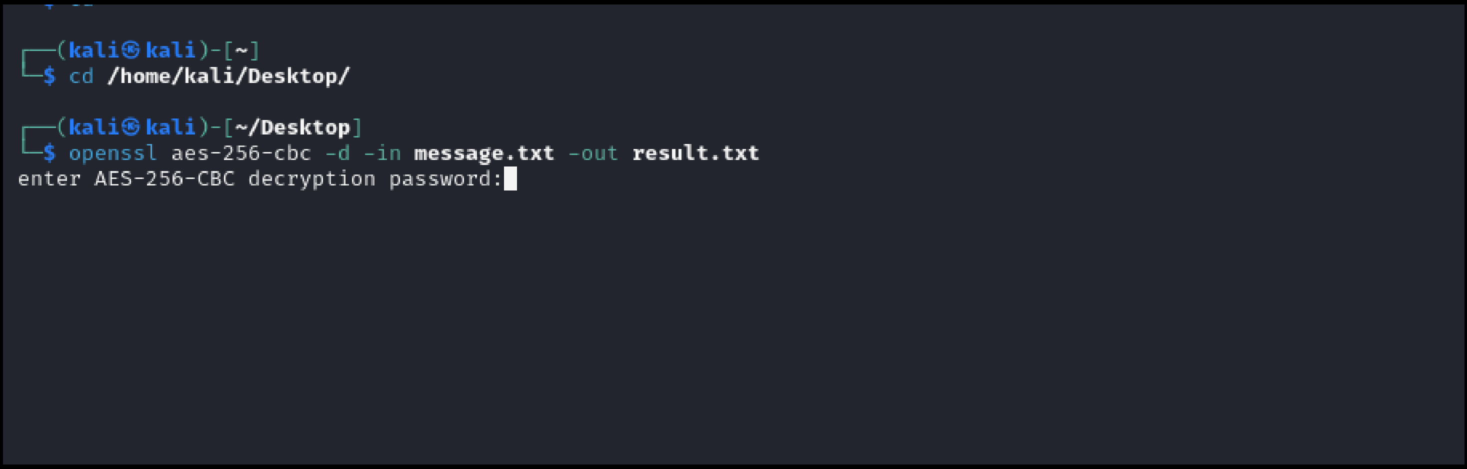
LEVEL: [Medium]

2025

Challenge Description:
A crucial wartime message was intercepted, its secrets buried in message.txt. Within it, a series of hidden numbers await decryption. The key lies in history, with clues concealed in an accompanying image. Look closely—small details may hold the answer. Can you uncover the flag hidden within the numbers?

Solution:

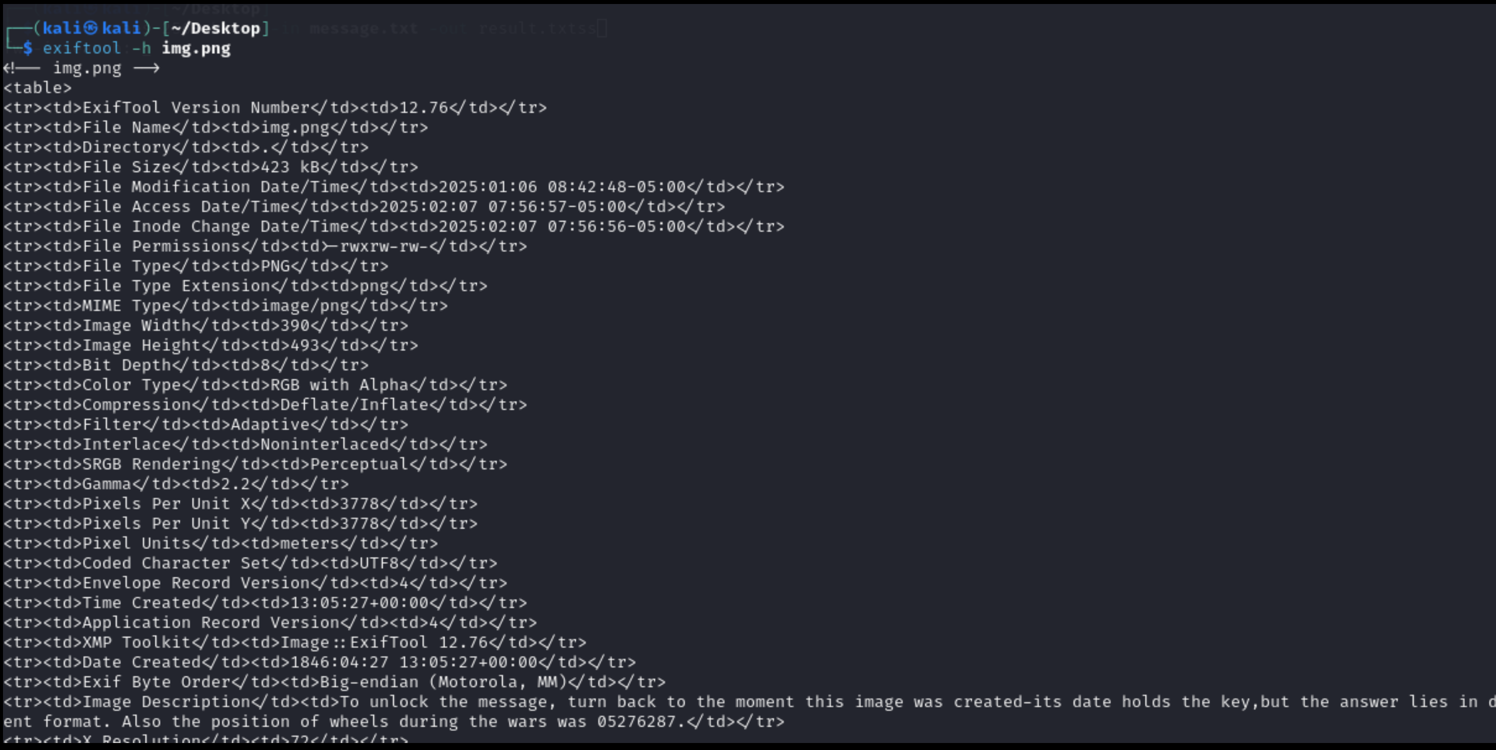
The given file message.txt is encrypted using openssl.



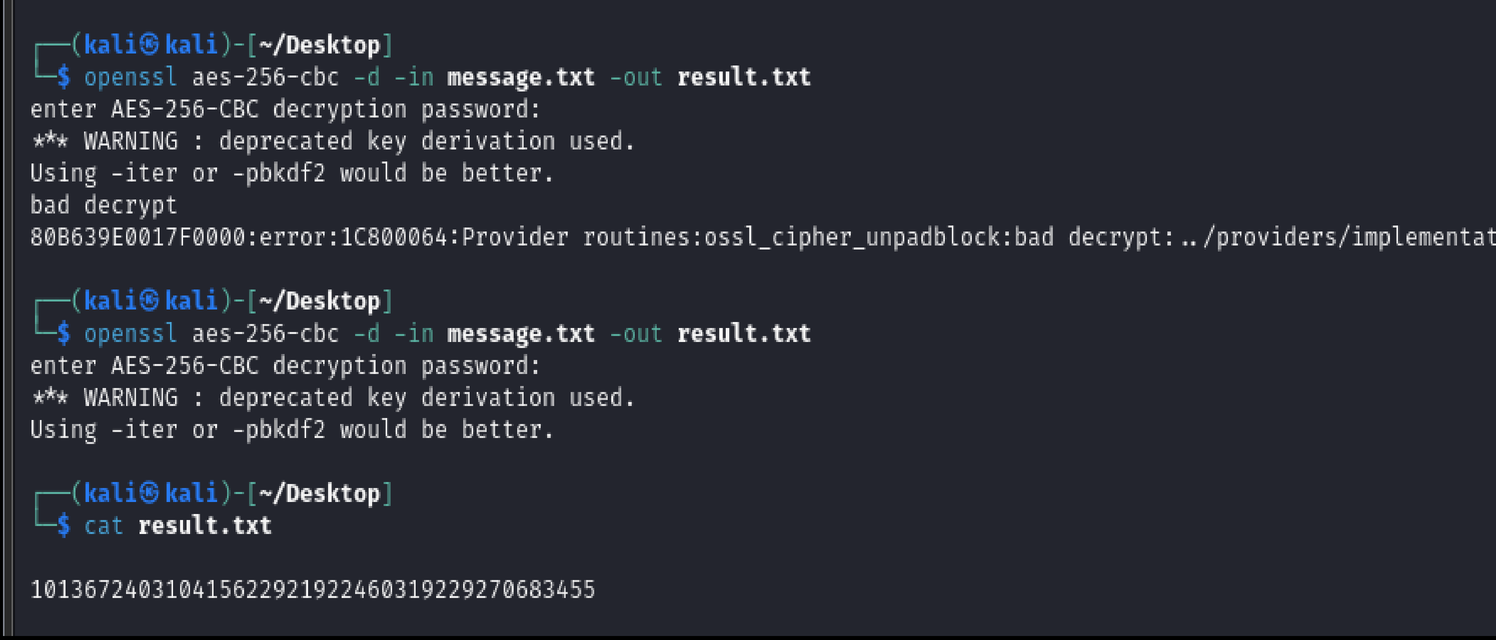
```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/Desktop/

┌──(kali㉿kali)-[~/Desktop]
└─$ openssl aes-256-cbc -d -in message.txt -out result.txt
enter AES-256-CBC decryption password:
```

To decrypt this file password is needed. As given in description" The key lies in history, with clues concealed in an accompanying image." **Password is in metadata of image. In image description the statement" To unlock the message, turn back to the moment this image was created-its date holds the key,but the answer lies in different format. Also, the position of wheels during the wars was 05276287." Hints that password is the date on which the image is created. Therefore, password is 27041846.**



```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool -h img.png
<!-- img.png -->
<table>
<tr><td>ExifTool Version Number</td><td>12.76</td></tr>
<tr><td>File Name</td><td>img.png</td></tr>
<tr><td>Directory</td><td>.</td></tr>
<tr><td>File Size</td><td>423 kB</td></tr>
<tr><td>File Modification Date/Time</td><td>2025:01:06 08:42:48-05:00</td></tr>
<tr><td>File Access Date/Time</td><td>2025:02:07 07:56:57-05:00</td></tr>
<tr><td>File Inode Change Date/Time</td><td>2025:02:07 07:56:56-05:00</td></tr>
<tr><td>File Permissions</td><td>-rwxrw-rw-</td></tr>
<tr><td>File Type</td><td>PNG</td></tr>
<tr><td>File Type Extension</td><td>png</td></tr>
<tr><td>MIME Type</td><td>image/png</td></tr>
<tr><td>Image Width</td><td>390</td></tr>
<tr><td>Image Height</td><td>493</td></tr>
<tr><td>Bit Depth</td><td>8</td></tr>
<tr><td>Color Type</td><td>RGB with Alpha</td></tr>
<tr><td>Compression</td><td>Deflate/Inflate</td></tr>
<tr><td>Filter</td><td>Adaptive</td></tr>
<tr><td>Interlace</td><td>Noninterlaced</td></tr>
<tr><td>SRGB Rendering</td><td>Perceptual</td></tr>
<tr><td>Gamma</td><td>2.2</td></tr>
<tr><td>Pixels Per Unit X</td><td>3778</td></tr>
<tr><td>Pixels Per Unit Y</td><td>3778</td></tr>
<tr><td>Pixel Units</td><td>meters</td></tr>
<tr><td>Coded Character Set</td><td>UTF8</td></tr>
<tr><td>Envelope Record Version</td><td>4</td></tr>
<tr><td>Time Created</td><td>13:05:27+00:00</td></tr>
<tr><td>Application Record Version</td><td>4</td></tr>
<tr><td>XMP Toolkit</td><td>Image::ExifTool 12.76</td></tr>
<tr><td>Date Created</td><td>1846:04:27 13:05:27+00:00</td></tr>
<tr><td>Exif Byte Order</td><td>Big-endian (Motorola, MM)</td></tr>
<tr><td>Image Description</td><td>To unlock the message, turn back to the moment this image was created-its date holds the key,but the answer lies in d
ent format. Also the position of wheels during the wars was 05276287.</td></tr>
<tr><td>X Resolution</td><td>72</td></tr>
```



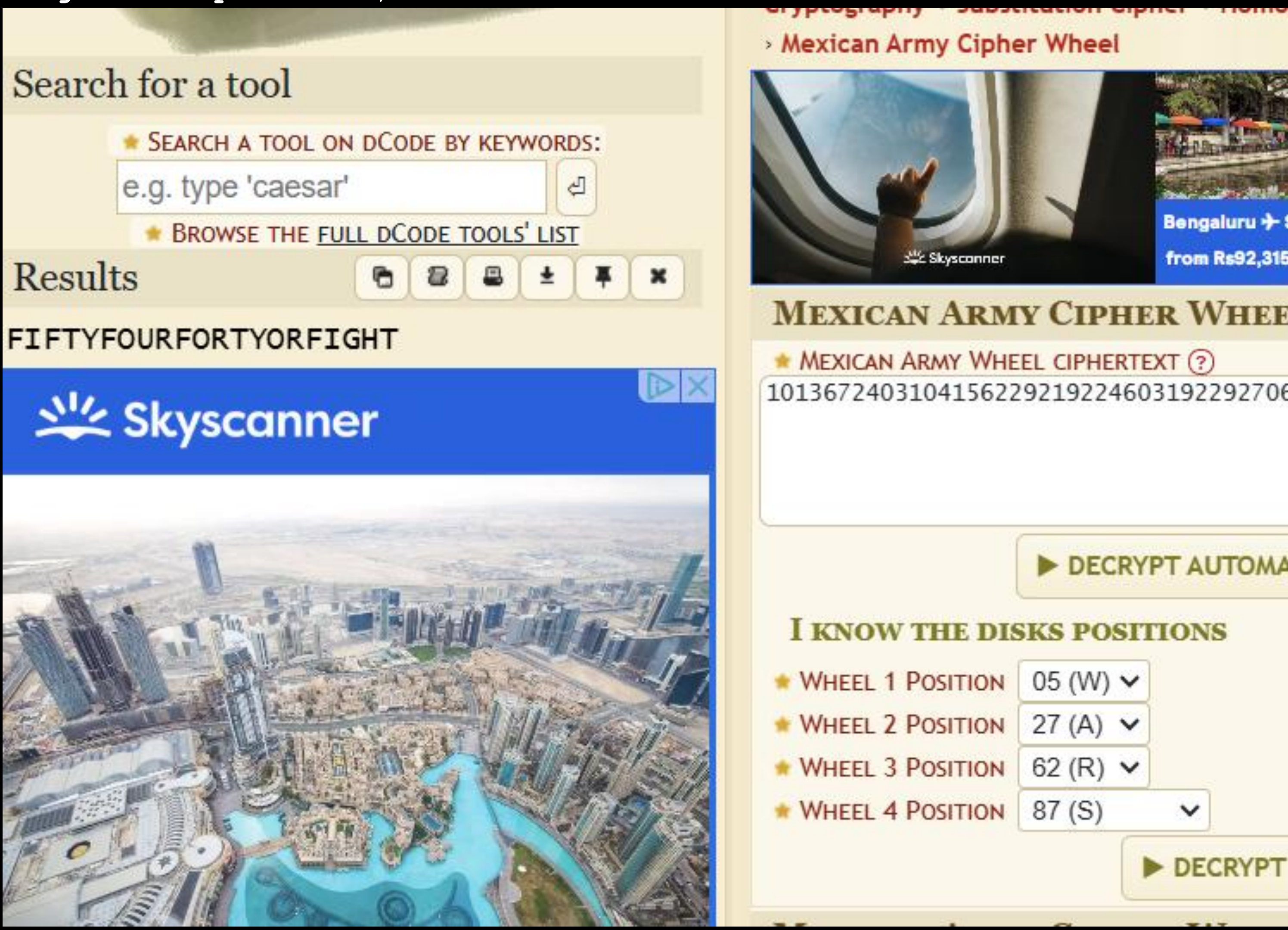
```
┌──(kali㉿kali)-[~/Desktop]
└─$ openssl aes-256-cbc -d -in message.txt -out result.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bad decrypt
80B639E0017F0000:error:1C800064:Provider routines:ossl_cipher_unpadblock:bad decrypt:../providers/implementat

┌──(kali㉿kali)-[~/Desktop]
└─$ openssl aes-256-cbc -d -in message.txt -out result.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

┌──(kali㉿kali)-[~/Desktop]
└─$ cat result.txt

101367240310415622921922460319229270683455
```

Now the final number series is 101367240310415622921922460319229270683455. The keywords in question "history"," wartime" suggests that cipher is related to past. In Mexican Army Wheel cipher position is disk is 05276287 as given in image description. So, the final answer is FIFTYFOURFORTYORFIGHT.



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'caesar'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

FIFTYFOURFORTYORFIGHT

› Mexican Army Cipher Wheel

MEXICAN ARMY CIPHER WHEE

★ MEXICAN ARMY WHEEL CIPHERTEXT

1013672403104156229219224603192292706

▶ DECRYPT AUTOMA

I KNOW THE DISKS POSITIONS

★ WHEEL 1 POSITION 05 (W)

★ WHEEL 2 POSITION 27 (A)

★ WHEEL 3 POSITION 62 (R)

★ WHEEL 4 POSITION 87 (S)

▶ DECRYPT

Flag: VishwaCTF{FIFTYFOURFORTYORFIGHT}