# CTF

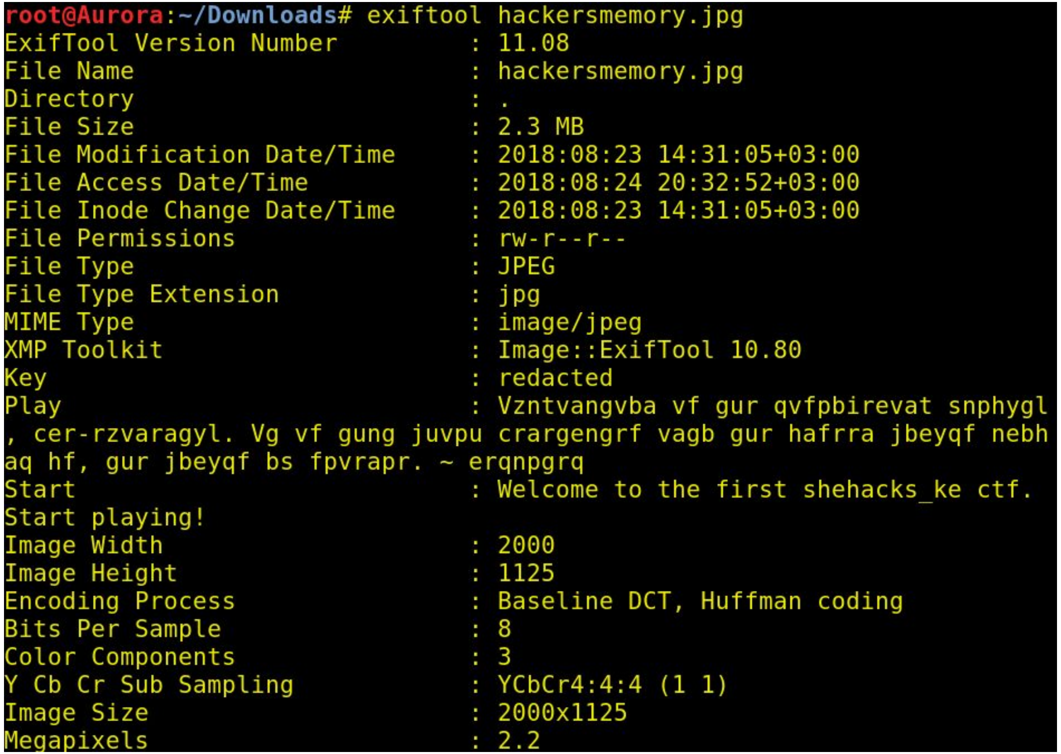
http://178.128.236.27:4000/

1.048596
0.3345
Linux3rror
0.571024

# Rome

Exiftool:used for reading and writing meta information in a variety of file types.

Metadata: summarizes basic **information** about data/file.

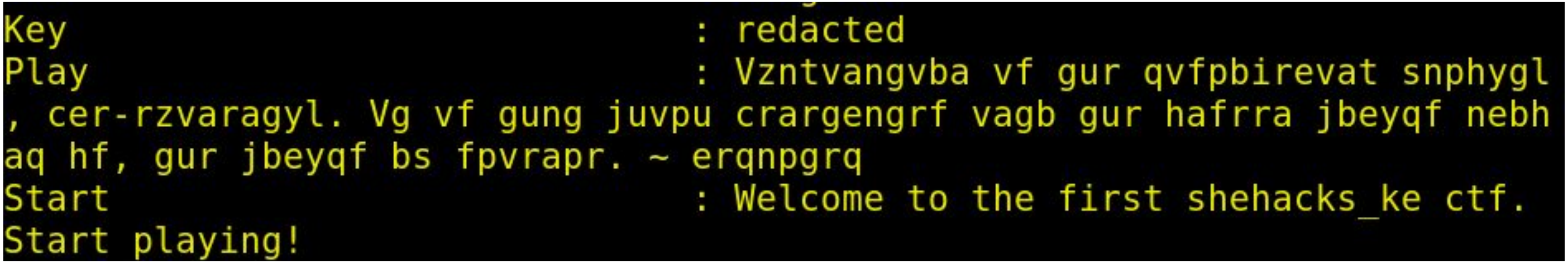


```
root@Aurora:~/Downloads# exiftool hackersmemory.jpg
ExifTool Version Number         : 11.08
File Name                       : hackersmemory.jpg
Directory                       : .
File Size                       : 2.3 MB
File Modification Date/Time     : 2018:08:23 14:31:05+03:00
File Access Date/Time           : 2018:08:24 20:32:52+03:00
File Inode Change Date/Time     : 2018:08:23 14:31:05+03:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
XMP Toolkit                     : Image::ExifTool 10.80
Key                             : redacted
Play                            : Vzntvangvba vf gur qvfpbirevat snphygl
, cer-rzvaragyl. Vg vf gung juvpu crargengrf vagb gur hafrra jbeyqf nebh
aq hf, gur jbeyqf bs fpvrapr. ~ erqnpgrq
Start                           : Welcome to the first shehacks_ke ctf.
Start playing!
Image Width                     : 2000
Image Height                    : 1125
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 2000x1125
Megapixels                      : 2.2
```

# Rome

Play: !! Encrypted Data !!

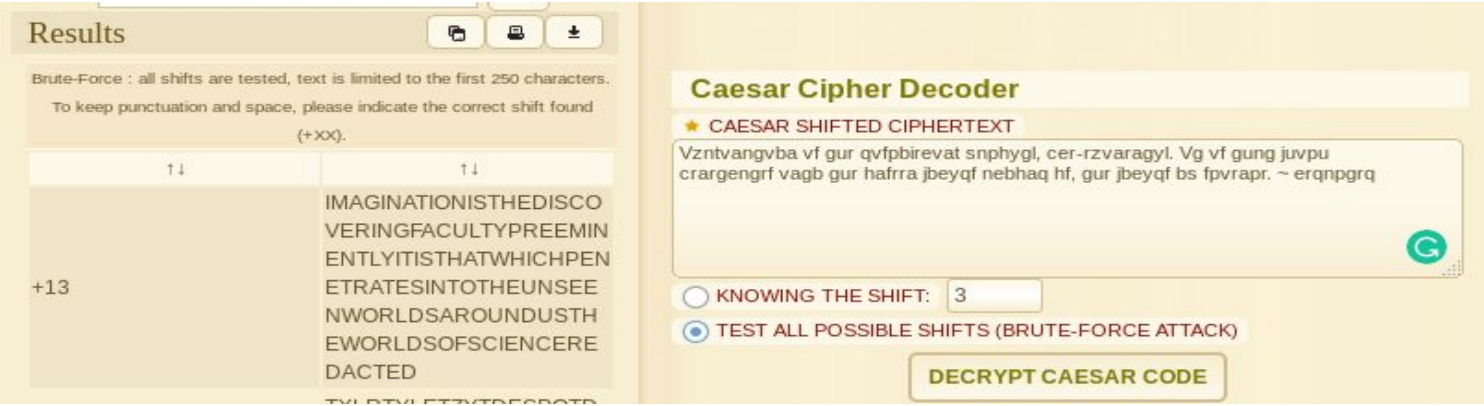
Type: ceasar cipher text.



```
Key                                : redacted
Play                               : Vzntvangvba vf gur qvfpbirevat snphygl
, cer-rzvaragyl. Vg vf gung juvpu crargengrf vagb gur hafrra jbeyqf nebh
aq hf, gur jbeyqf bs fpvrapr. ~ erqnpgrq
Start                              : Welcome to the first shehacks_ke ctf.
Start playing!
```

# Rome

Decrypting  the cipher | online tool -> https://www.dcode.fr/caesar-cipher



Results

Brute-Force : all shifts are tested, text is limited to the first 250 characters. To keep punctuation and space, please indicate the correct shift found (+XX).

| ↑↓ | ↑↓ |
|---|---|
| +13 | IMAGINATIONISTHEDISCOVERINGFACULTYPREEMINENTLYITISTHATWHICHPENETRATESINTOTHEUNSEENWORLDSAROUNDUSTHEWORLDSOFSCIENCEREDACTED |

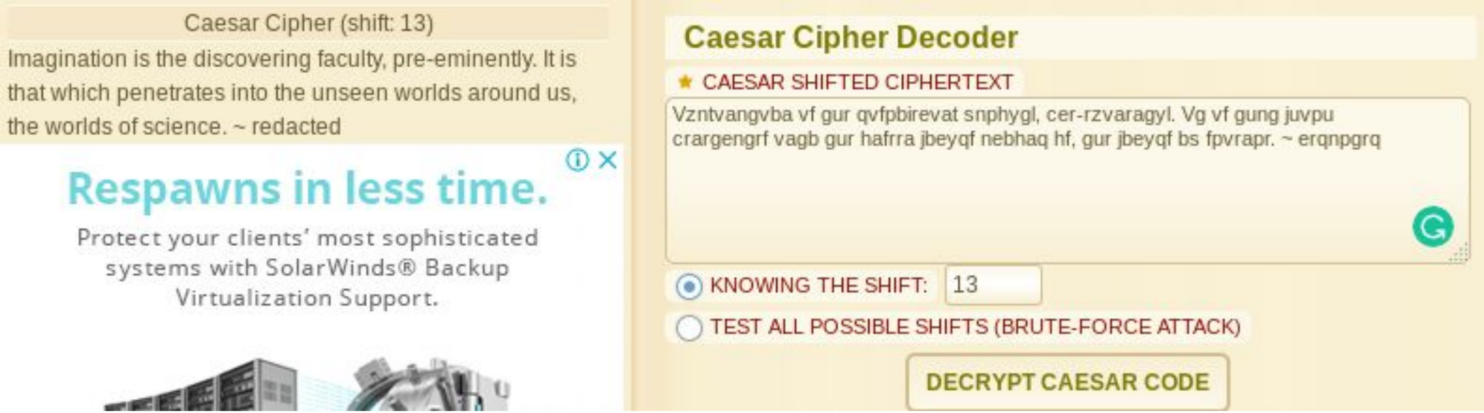
Caesar Cipher Decoder

★ CAESAR SHIFTED CIPHERTEXT

Vzntvangvba vf gur qvfpbirevat snphygl, cer-rzvaragyl. Vg vf gung juvpu crargengrf vagb gur hafrra jbeyqf nebhaq hf, gur jbeyqf bs fpvrapr. ~ erqnpgrq

○ KNOWING THE SHIFT: 3

● TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)



Caesar Cipher (shift: 13)

Imagination is the discovering faculty, pre-eminently. It is that which penetrates into the unseen worlds around us, the worlds of science. ~ redacted

Caesar Cipher Decoder

★ CAESAR SHIFTED CIPHERTEXT

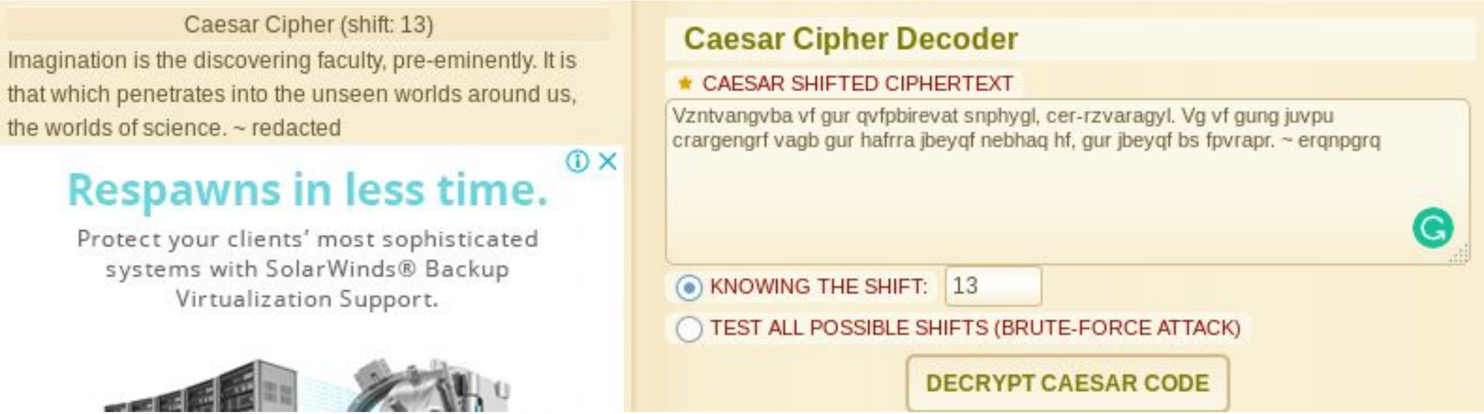
Vzntvangvba vf gur qvfpbirevat snphygl, cer-rzvaragyl. Vg vf gung juvpu crargengrf vagb gur hafrra jbeyqf nebhaq hf, gur jbeyqf bs fpvrapr. ~ erqnpgrq

● KNOWING THE SHIFT: 13

○ TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)

# Rome

!!SOLVED!!



Caesar Cipher (shift: 13)

Imagination is the discovering faculty, pre-eminently. It is that which penetrates into the unseen worlds around us, the worlds of science. ~ redacted

Caesar Cipher Decoder

★ CAESAR SHIFTED CIPHERTEXT

Vzntvangvba vf gur qvfpbirevat snphygl, cer-rzvaragyl. Vg vf gung juvpu crargengrf vagb gur hafrra jbeyqf nebhaq hf, gur jbeyqf bs fpvrapr. ~ erqnpgrq

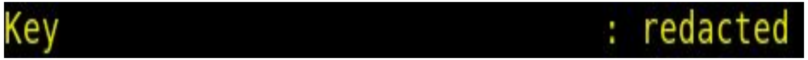
● KNOWING THE SHIFT: 13

○ TEST ALL POSSIBLE SHIFTS (BRUTE-FORCE ATTACK)

Flag = Imagination is the discovering faculty, pre-eminently. It is that which penetrates into the unseen worlds around us, the worlds of science. ~ redacted

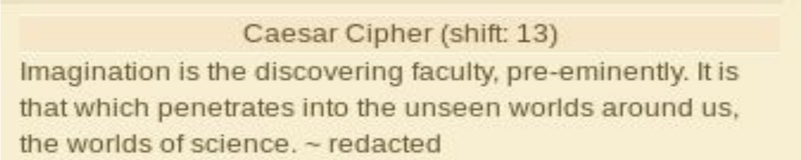
# Hidden in Plain Sight

So we have two clues:

1. 

```
Key                                                  : redacted
```

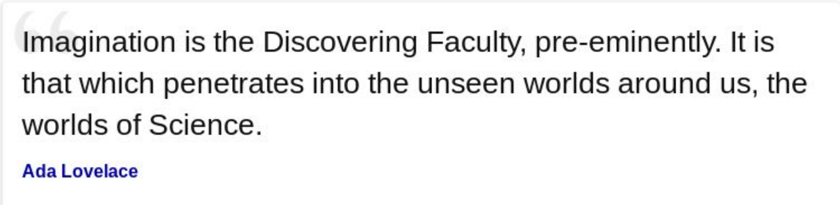
From exiftool --- results.

2. 

Caesar Cipher (shift: 13)

Imagination is the discovering faculty, pre-eminently. It is that which penetrates into the unseen worlds around us, the worlds of science. ~ redacted

Tool: Google



Imagination is the Discovering Faculty, pre-eminently. It is that which penetrates into the unseen worlds around us, the worlds of Science.

Ada Lovelace

Flag = Ada Lovelace

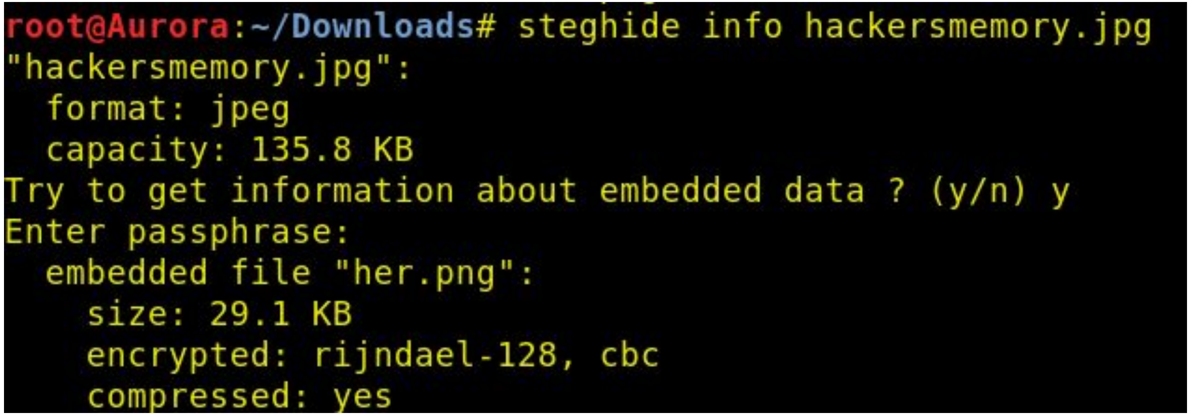
Decrypted result at the end ~ redacted. Joining the dots ...

# Hidden in Plain Sight

Key = Ada Lovelace

?? What Next ??

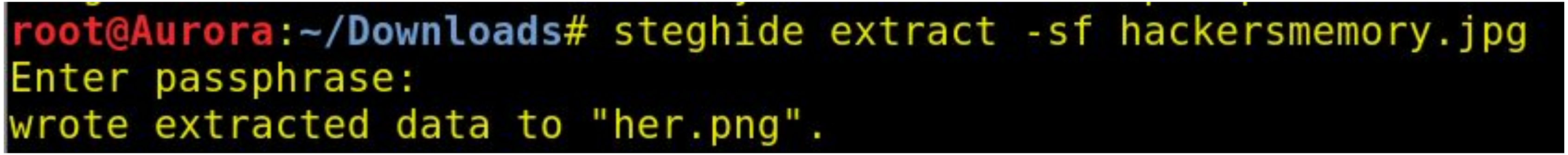
TOOL: Steghide; is a steganography program that is various kinds of image- and audio-files.



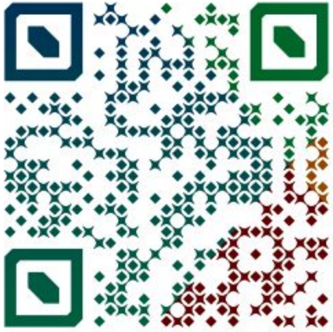
```
root@Aurora:~/Downloads# steghide info hackersmemory.jpg
"hackersmemory.jpg":
  format: jpeg
  capacity: 135.8 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "her.png":
    size: 29.1 KB
    encrypted: rijndael-128, cbc
    compressed: yes
```

# Hidden in Plain Sight

!! EXTRACTING EMBEDDED DATA!!



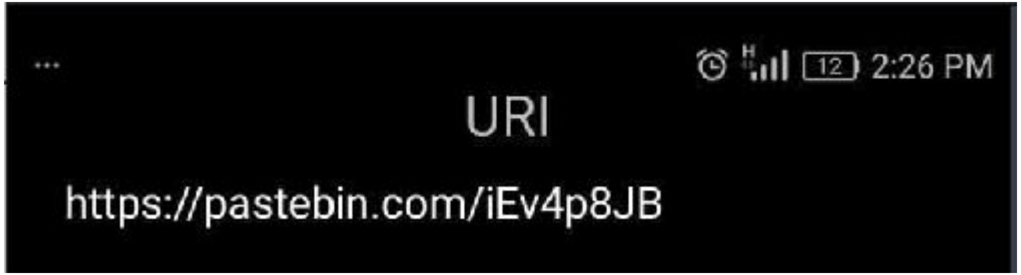
```
root@Aurora:~/Downloads# steghide extract -sf hackersmemory.jpg
Enter passphrase:
wrote extracted data to "her.png".
```



her.png

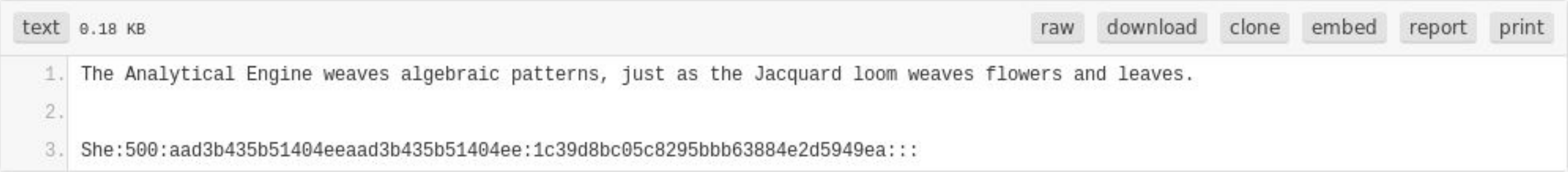
# Breaches and Dumps

## QRCODE SCAN RESULTS



URI

https://pastebin.com/iEv4p8JB

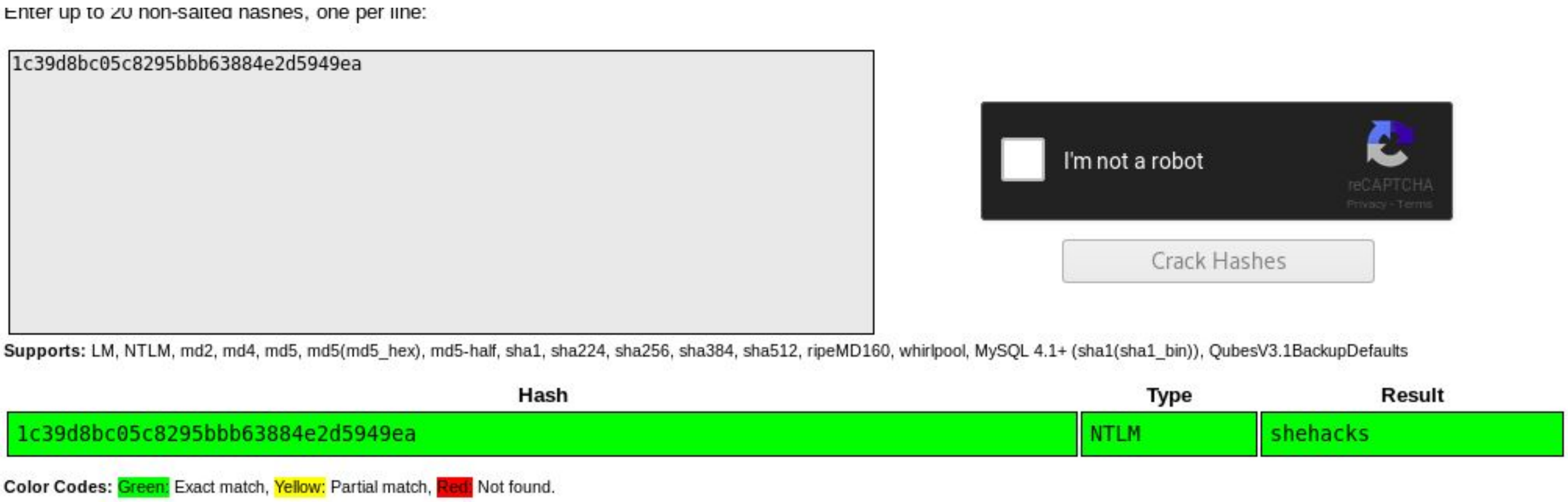


```
The Analytical Engine weaves algebraic patterns, just as the Jacquard loom weaves flowers and leaves.

She:500:aad3b435b51404eeaad3b435b51404ee:1c39d8bc05c8295bbb63884e2d5949ea:::
```

username:USID:LM-Hash:NTLM-

# Breaches and Dumps



Enter up to 20 non-salted hashes, one per line:

```
1c39d8bc05c8295bbb63884e2d5949ea
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

| Hash | Type | Result |
|---|---|---|
| 1c39d8bc05c8295bbb63884e2d5949ea | NTLM | shehacks |

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

Tool: crackstation.net

Flag: shehacks  << it was that !! EASY !!