

Decrypting Meditullium

Users will first be confronted with an image from Lewis Carroll's "Alice's Adventures in Wonderland," that has a QR code placed within the picture.



FIGURE 1 – RED/BLUE

Red and Blue, Deducing the Clue

Users can either utilize a QR Reader on their smart device such as Norton Snap, decode the QR code by hand, or use an online QR code reader.

Upon scanning, the QR code will lead the user to this image on Imgur, which has some layered text.

Are you here for the Red Queen's letter????
Did you come on your own, or via an abetter?
(That's really of no matter.)

The queen loves to win, and loves to play games,
So being able to read her prolific letter outright,
Would not be her aim, and would be rather lame.

To seek the true meaning, you must.
Look a layer deeper.-
Good luck on Puzzle 3,
will you be the first to
break this teaser?



FIGURE 2 – RED/BLUE

Are you here for the Red Queen's letter?????
Did you come on your town, or via an abetter?
(That's really of no matter.)

The queen loves to win, and loves to play games,
So being able to read her prolific letter outright,
Would not be her aim, and would be rather lame.

To seek the true meaning, you must.
Look a layer deeper.-
Good luck on Puzzle 3,
Will you be the first to
break this teaser?

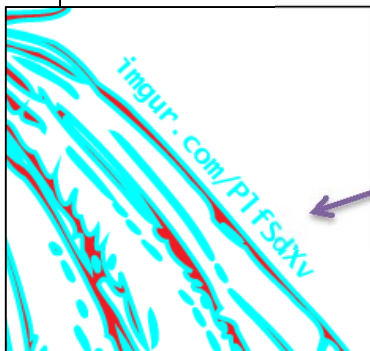


FIGURE 3 – RED/BLUE.JPG – A CLOSER LOOK

The user may notice an imgur hyperlink. This is just a red herring, which is meant to hint to the user to look deeper in this image and pull out the cyan text.

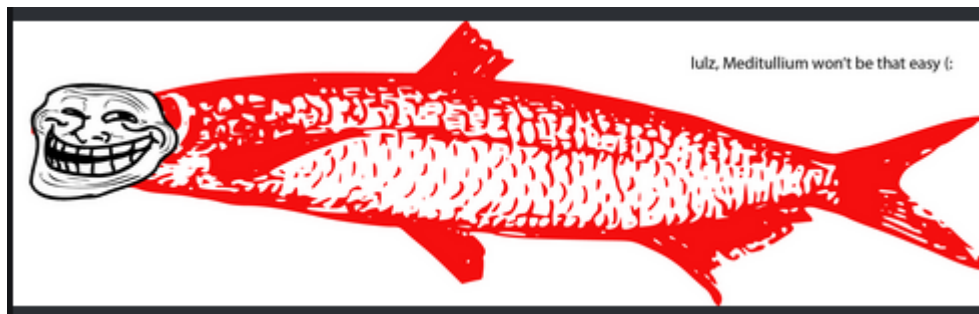


FIGURE 4 – RED HERRING

In order to properly see the cyan text beneath the red text, the user will have to apply a filter to wash out the red color and bring out the cyan. The user may also notice the following imgur link, which leads the user to a png that will filter out the red text:



FIGURE 5 – IMGUR LINK TO DECODER

Following that URL will lead the user to this image. The user should download this png.

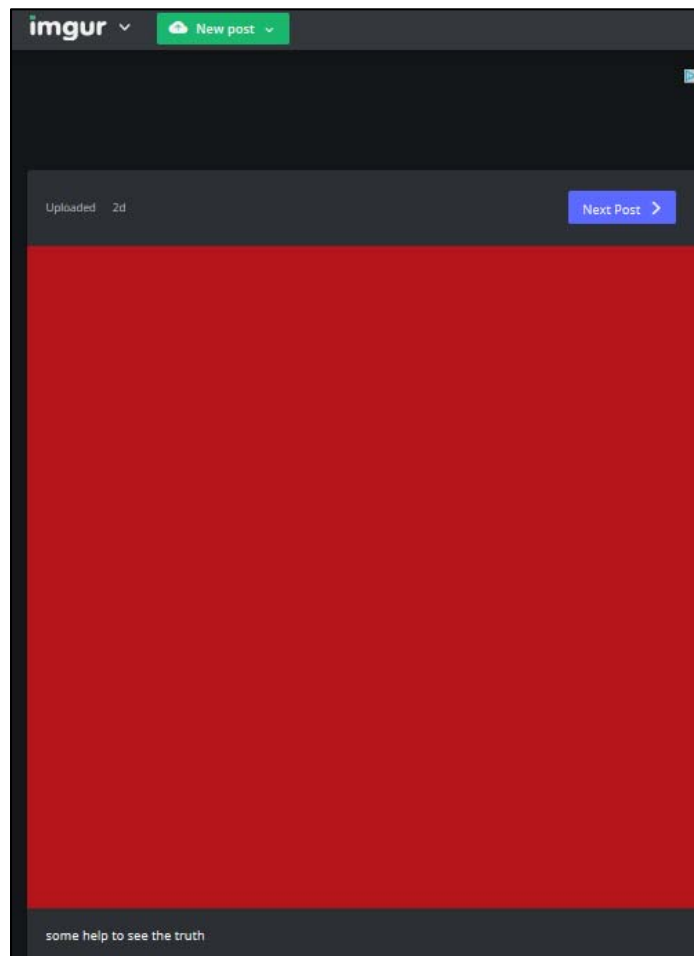


FIGURE 6 – IMGUR DECODER

With the caption “some help to see the truth” the user should be able to deduce that this png should be applied over the original letter. The user can do this by copying the original cyan/red image and apply the decoder over the image.

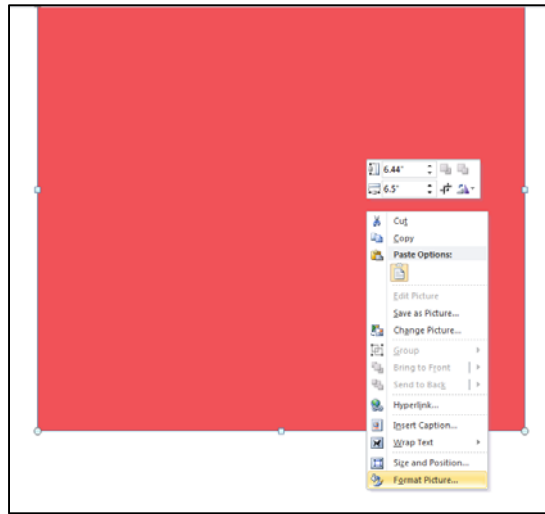
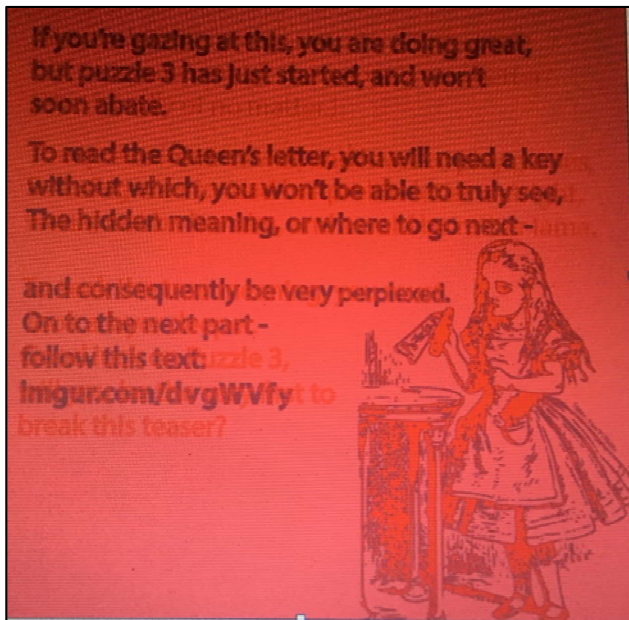


FIGURE 7 – APPLYING THE DECODER

By applying the filter over the image, the user will see the cyan text:



If you're gazing at this, you are doing great, but puzzle 3 has just started, and won't soon abate.

To read the Queen's letter, you will need a key without which, you won't be able to truly see, The hidden meaning, or where to go next -

And consequently be very perplexed.
on to the next part -
follow this text:
[Imgur.com/dvgWVfy](https://imgur.com/dvgWVfy)

FIGURE 8 – DECODING THE MESSAGE

We're all Mad here, and Enciphered, and Backwards

The aforementioned Imgur link will lead the user to the following image:



FIGURE 9 – CHESHIRE CIPHER

Upon further inspection, the user should see that the Cheshire cat's eyebrows contain some vital information on where to go next in order to continue the puzzle.

The strings are enciphered with a ROT13 cipher, and are also reflected so that the text is backward. To decrypt these strings, the user can simply reverse the image, as shown in the following figure:

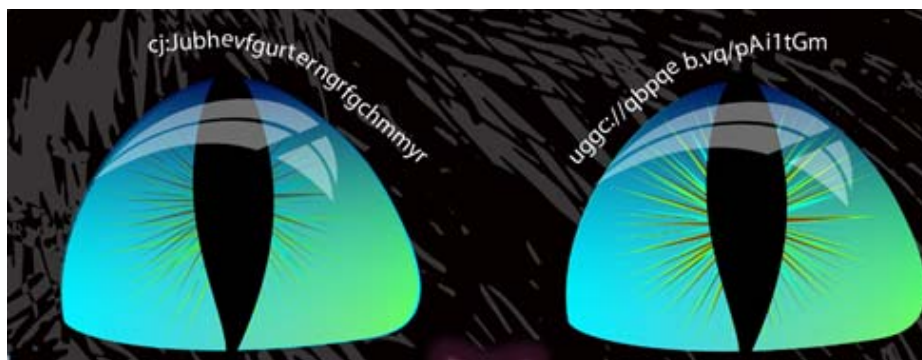


FIGURE 10 – REVERSING THE CHESHIRE CIPHER

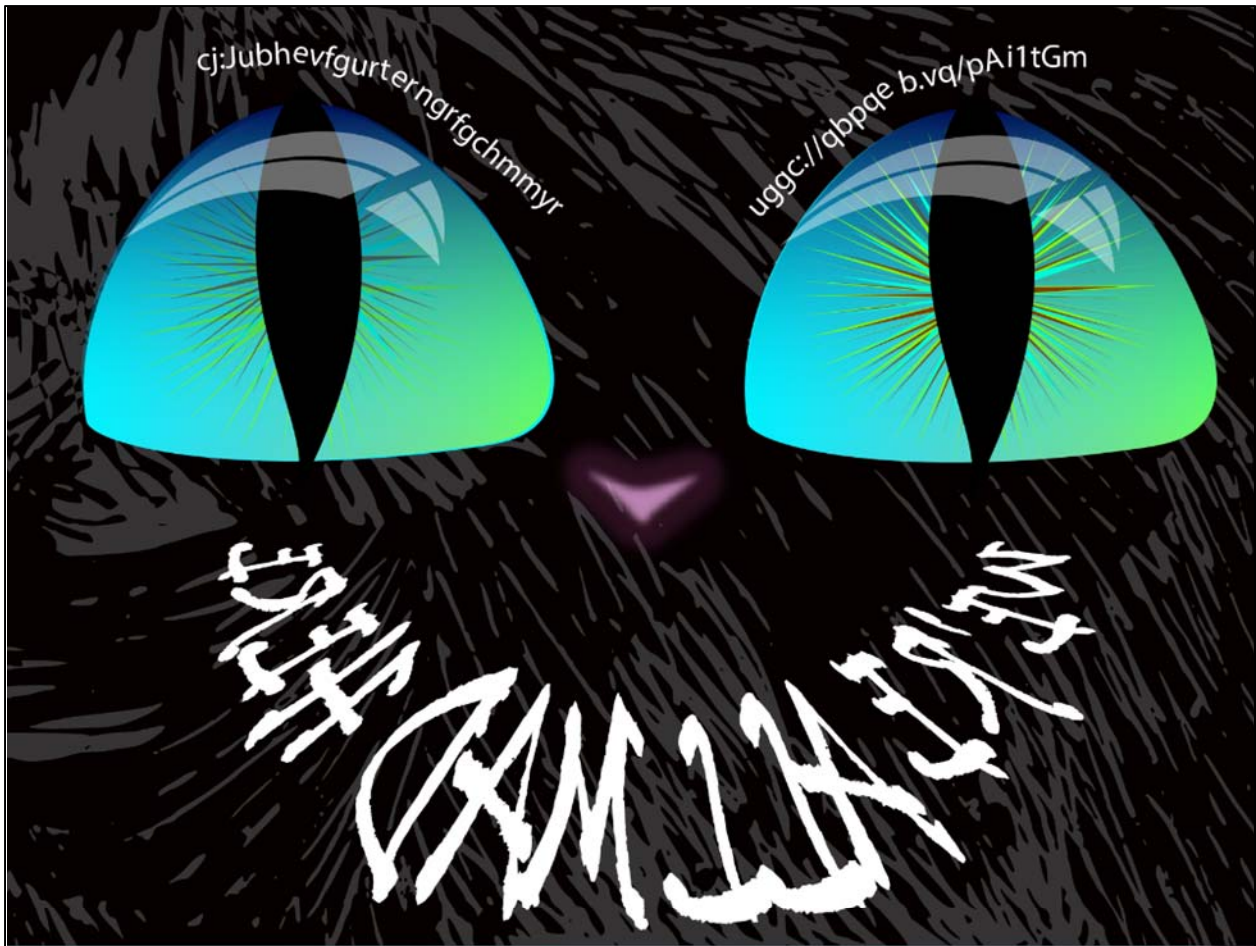
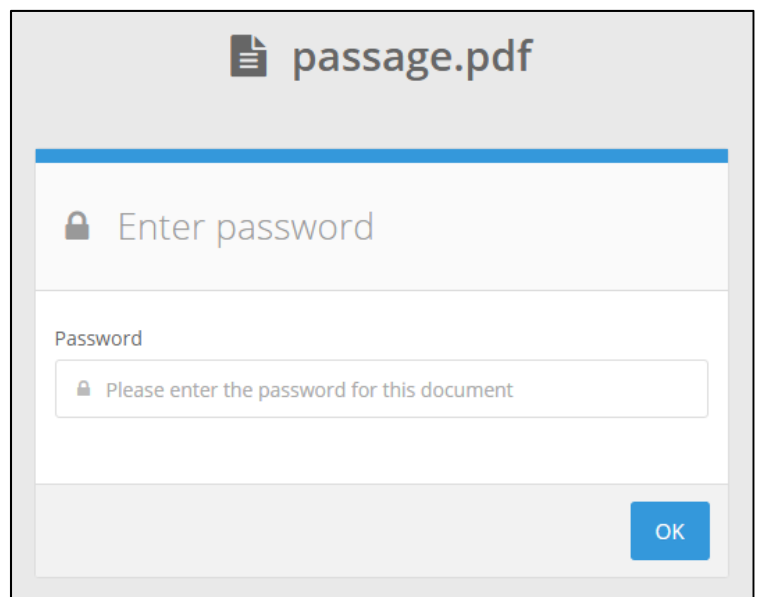


FIGURE 11 – REVERSING THE CHESHIRE CIPHER

The user can now properly see the strings, and decrypt the ROT13 cipher. The properly decrypted strings contain the following:

`http://docdro.id/cNv1gTz`
`pw:Whouristhegreatestpuzzle`



What do you know?

Once the user follows the docdroid link and enters in the password of "Whouareisthegreatestpuzzle", the following pdf will be revealed:

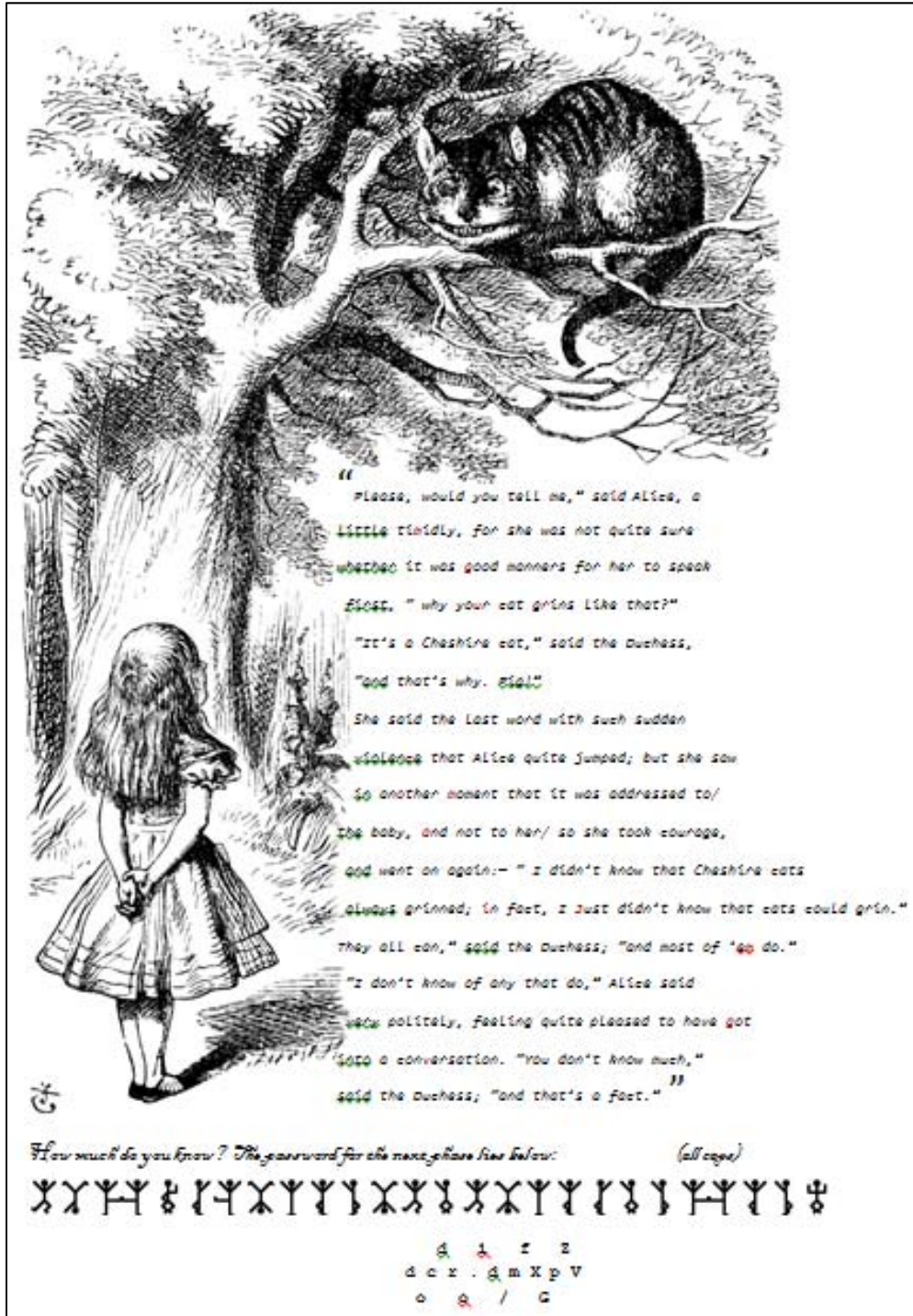


FIGURE 12 – WHAT DO YOU KNOW

This pdf contains several layers that the user will have to uncover.

First, the PDF contains a passage from Lewis Carrol's "Alice's Adventures in Wonderland."

There is also enciphered text at the bottom of the page. The text tells the user that the following enciphered text is the password to the next phase:

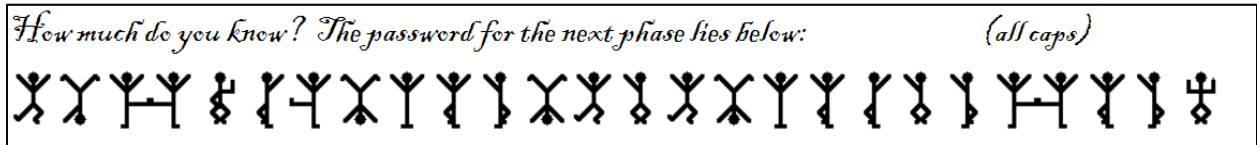


FIGURE 13 – DANCING MEN CIPHER

This enciphered text is actually a substitution cipher. The following is a cipher called Dancing Men, and is based on the Sherlock Holmes story of "The Dancing Men" by Sir Arthur Conan Doyle. When the user decodes this text, it will reveal the following password:

AGRINWITHOUTACATHOWCURIOUS

The user will then need to decode the next cipher, which is actually a railfence cipher. Since the Puzzlemaster was being nice, the railfence cipher is somewhat laid out for the user to read, and not in the one string encipherment typically used in railfence ciphers ☺

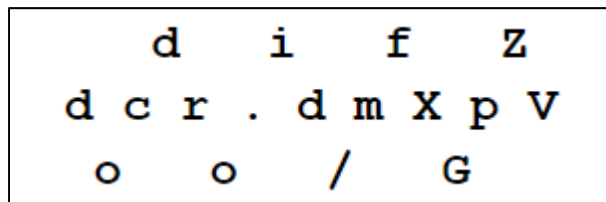


FIGURE 14 – RAILFENCE CIPHER

The user should read the aforementioned figure in a zig-zag fashion:

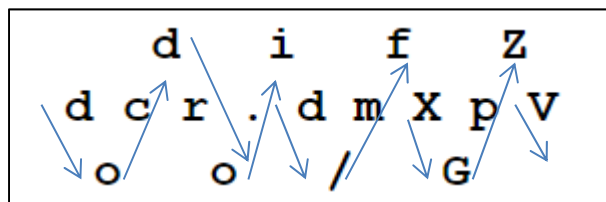


FIGURE 15 – DECODING THE RAILFENCE CIPHER

The railfence cipher decrypted is as follows:

docdro.id/mfXGpZV

Finding the Key

The user now has the passphrase to the PDF, but not the key. If the user closely inspects the PDF, they will see that some letters within the pdf are colored in burgundy, as shown in the figure below:

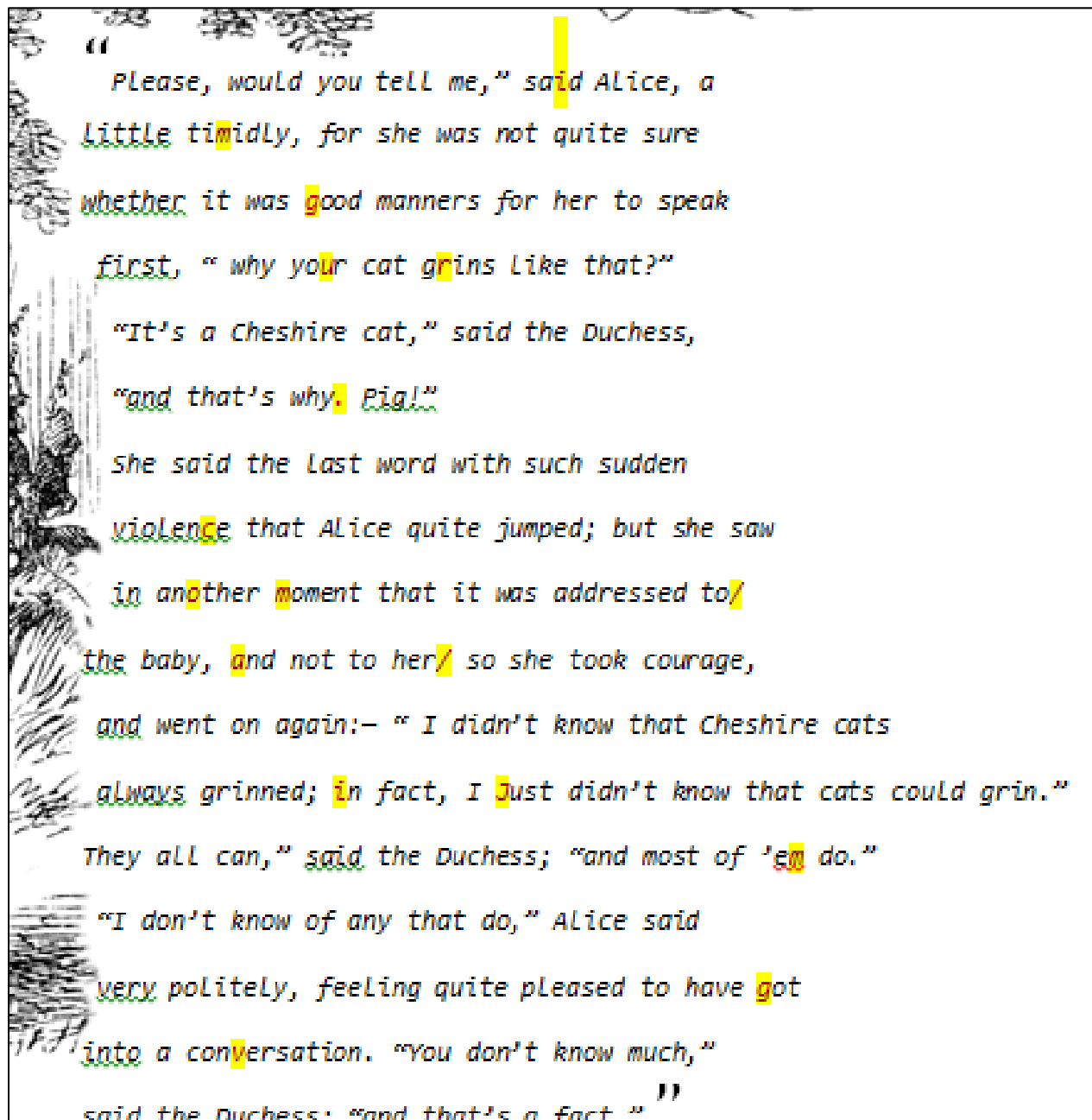


FIGURE 16 – DEDUCING THE KEY

If the user combines these letters all together, they will be able to see a URL that leads to the following imgur link, which is the key to reading the Queen’s letter:

imgur.com/a/iJmgv

Grabbing the Key

The imgur link will lead them to this png. As the hint states, the user will have to download the png to see its true value.

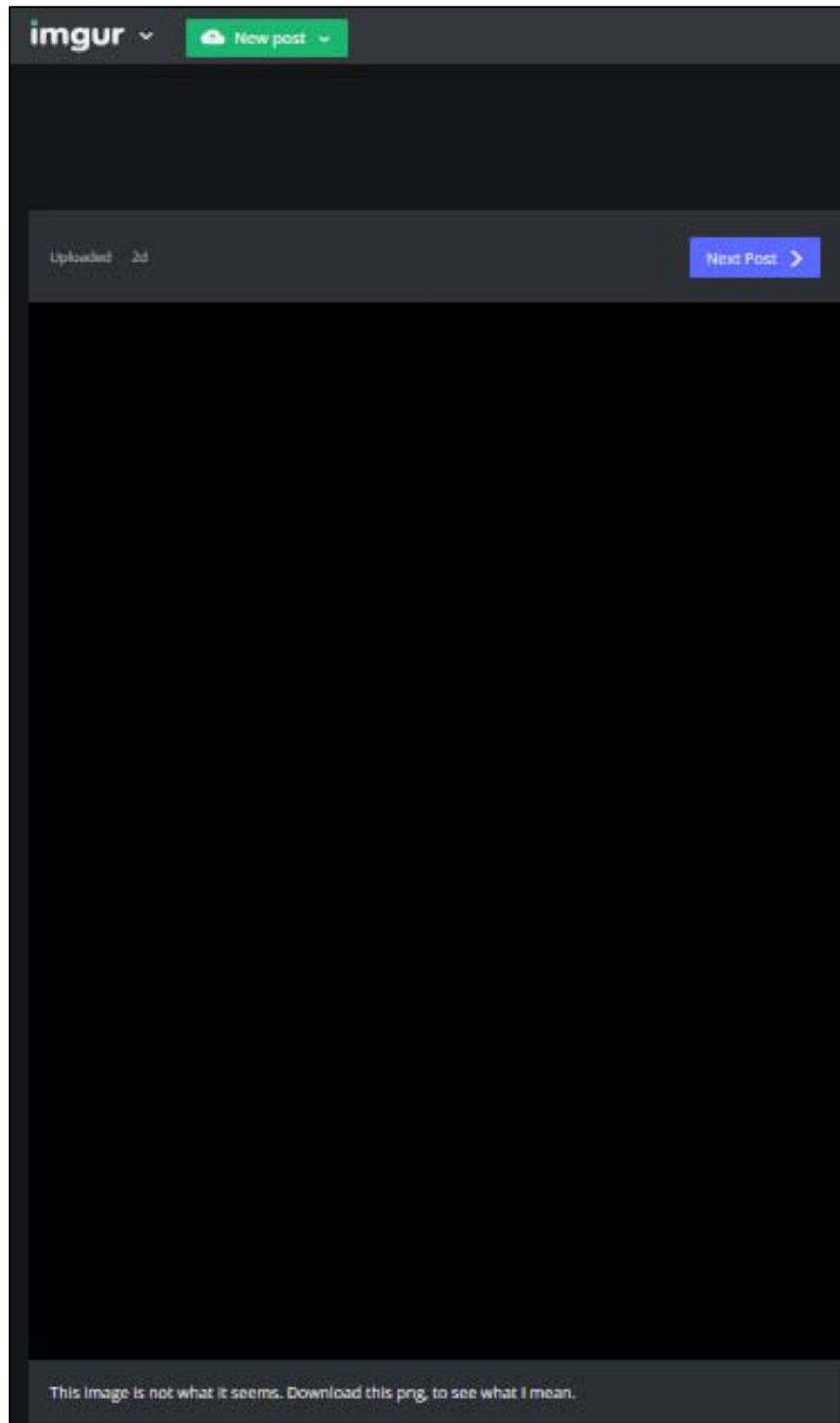


FIGURE 17 – THE KEY

Decoding the Queen's Letter-(It's about more than just Croquet)

If the user follows the decrypted docdroid link obtained from the railfence cipher, the user will find the following password protected PDF. The user will have to enter the passphrase: "AGRINWITHOUTACATHOWCURIOUS" to successfully unlock the pdf.

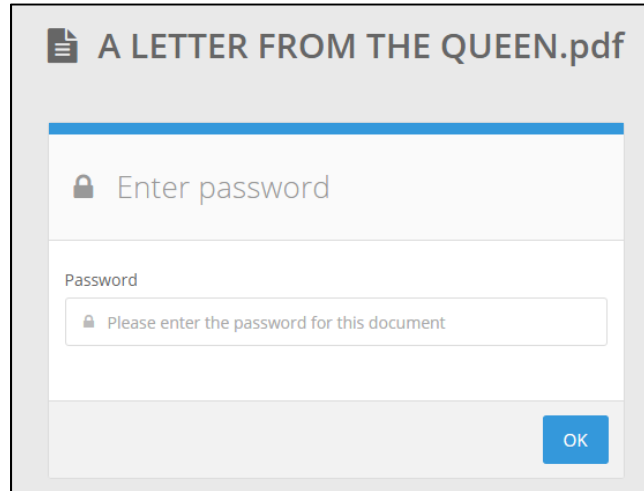


FIGURE 18 – UNLOCKING “A LETTER FROM THE QUEEN”

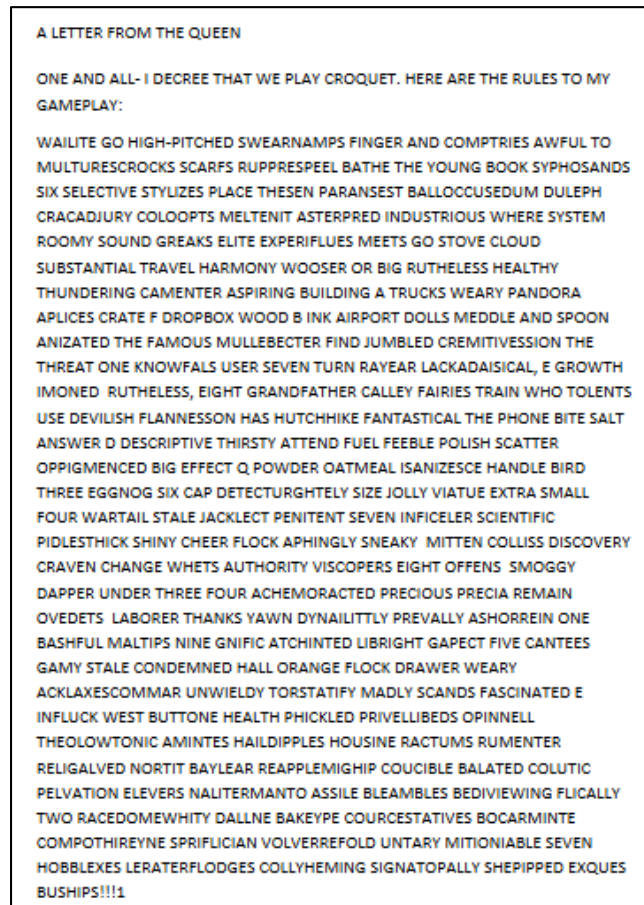


FIGURE 19 – THE LETTER FROM THE QUEEN

After the user downloads the aforementioned png key, they can copy the key directly into the PDF:



FIGURE 20 – COPYING THE KEY TO THE LETTER

Once expanded to full sheet size, true meaning of the letter will be revealed:

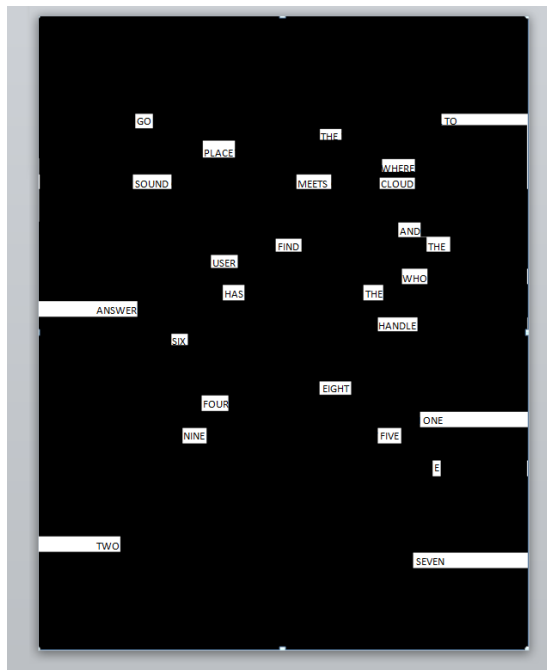


FIGURE 21 – EXPANDING THE KEY

The text reads:

“GO TO THE PLACE WHERE SOUND MEETS CLOUD AND FIND THE USER WHO HAS THE ANSWER. HANDLE SIX EIGHT FOUR ONE NINE FIVE E TWO SEVEN.”

This should translate to the username/handle: 684195e27 on SoundCloud.

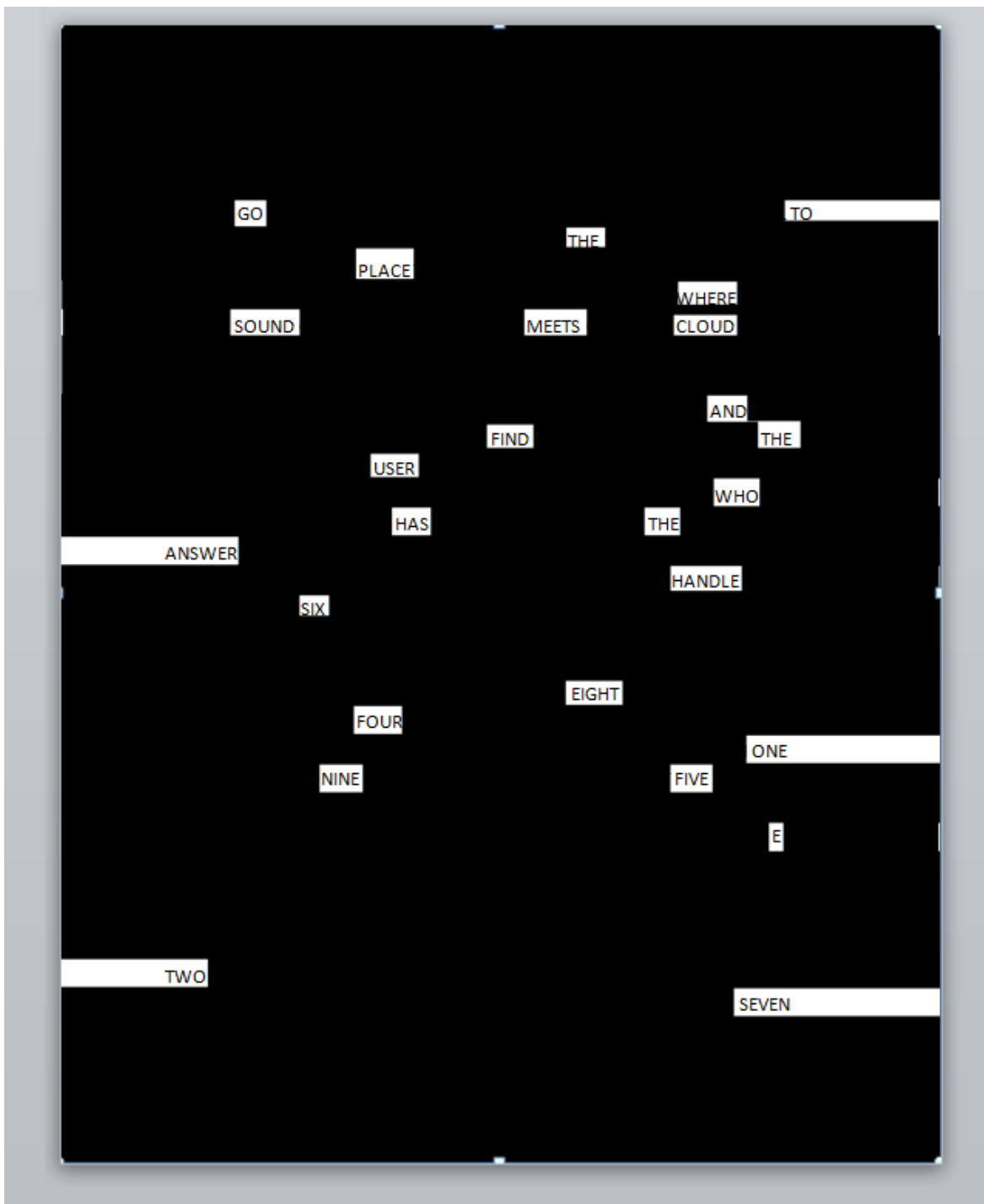


FIGURE 22 – HANDLE 684195E27

Upon searching "684195e27", the following user will pop up on SoundCloud:

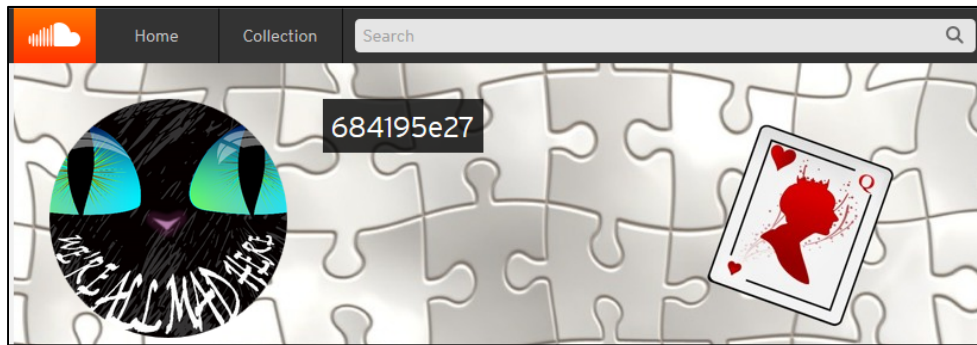


FIGURE 23 – USER 684195E27

Here the user will find an audio file that is available for download.

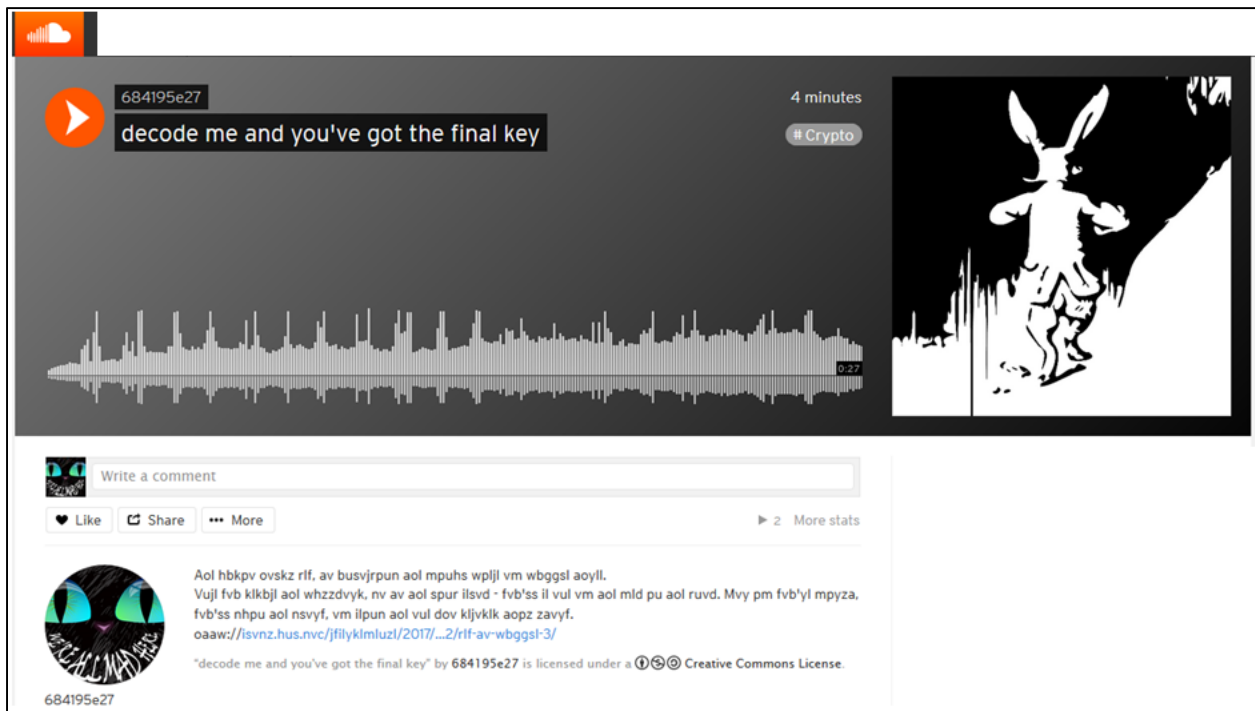


FIGURE 24 – DEDUCING THE ENCIPHERED TEXT

The user may also see some enciphered data, which reads:

“Aol hbkpov ovskz rlf, av busvjrpun aol mpuhs wpljl vm wbggs1
aoyll.

Vujl fvb klkbjl aol whzzdvyk, nv av aol spur ilsud - fvb'ss
il vul vm aol mld pu aol ruvd. Dolu lualypun pu aol
whzzdvyk, wslhzi bzl hss jhwz, vaolydpzl aol whzzdvyk dpss
tvza klmpupalsf mhss msha. Uvd nv dpao hss kbl ohzal! Pm
fvb'yl mpyza, fvb'ss nhpu aol nsvyf, vm ilpun aol vul dov
kljvklk aopz zavyf.

oaaw://isvz.hus.nvc/jfilyklmluzl/2017/01/02/rlf-av-wbggs1-
3/”

This is a simple Cesar cipher with a n shift of 7. Upon deciphering the text, the user will see:

“The audio holds key, to unlocking the final piece of puzzle
three.

Once you deduce the password, go to the link below - you'll
be one of the few in the know. When entering in the
password, please use all caps, otherwise the password will
most definitely fall flat. Now go with all due haste! If
you're first, you'll gain the glory, of being the one who
decoded this story.

[http://blogs.anl.gov/cyberdefense/2017/01/02/key-to-puzzle-
3/](http://blogs.anl.gov/cyberdefense/2017/01/02/key-to-puzzle-3/)”

This is also a hint to the user to take a closer look at the audio.

Upon listening to this audio file, the user should be prompted to do some audio analysis since the audio sounds nonsensical.

Once the file is downloaded, the user can perform any number of audio analysis techniques. It is likely that the user will download audacity, since is free and easy to use.

In order to decipher the audio, the user will have to reverse the audio. In Audacity, the user can click on “effects” and select “reverse,” as shown in the figure below:

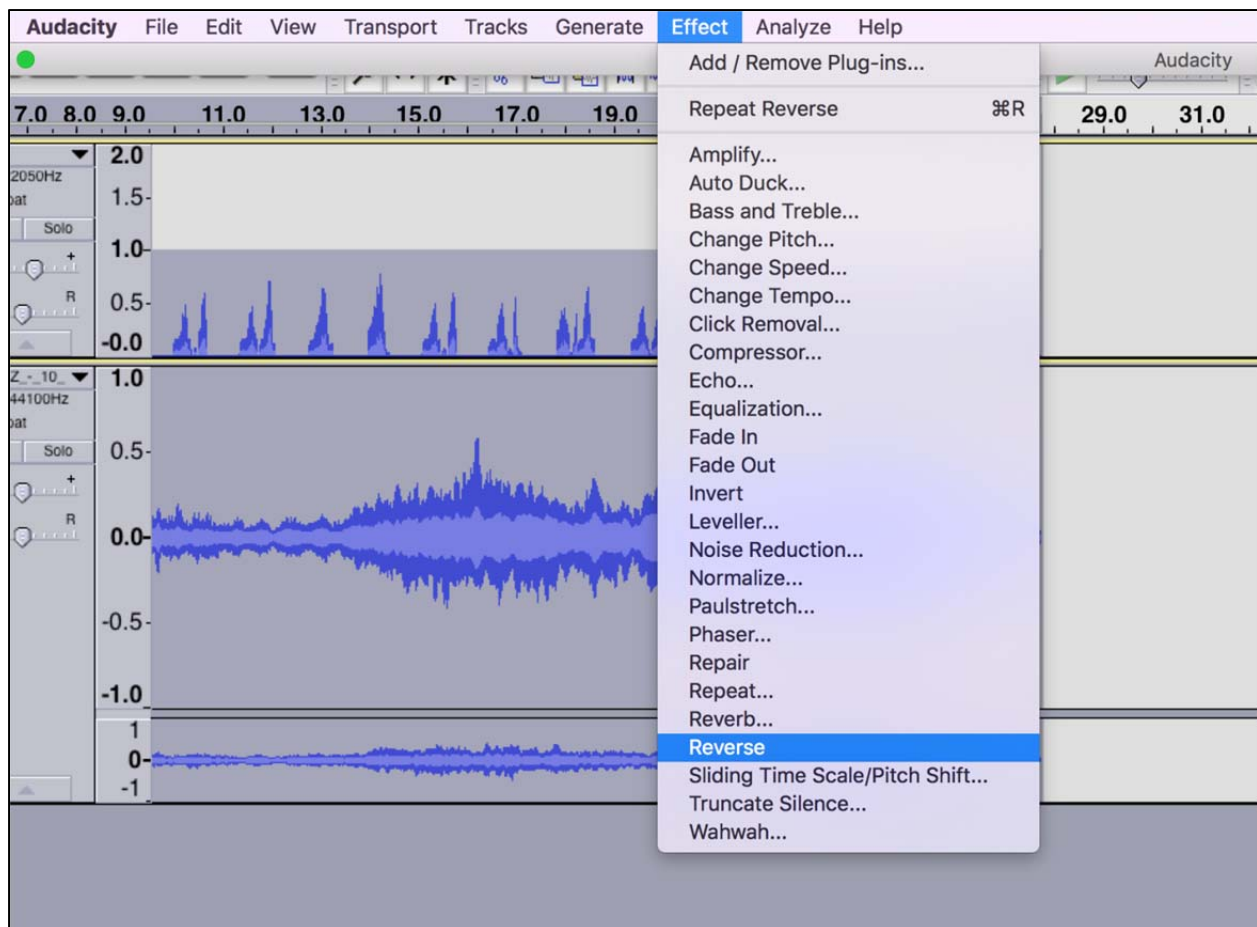


FIGURE 25 – REVERSING THE AUDIO IN AUDACITY

Once the audio is reversed, the user will hear the following sequence:

20-8-5-16-1-19-19-23-15-18-4-9-19-18-5-4-16-1-9-14-20.

This is a simple "letter number" cipher. To encrypt using this cipher, the user would replace letters with a number: A=1, B=2, C=3, etc. Upon further analysis, the user will deduce that the numerical string decodes to the following:

“THE PASSWORD IS RED PAINT”

The user now knows the password to the ciphered link:

<http://blogs.anl.gov/cyberdefense/2017/01/02/key-to-puzzle-3/>

The user should go to the link and see the following:

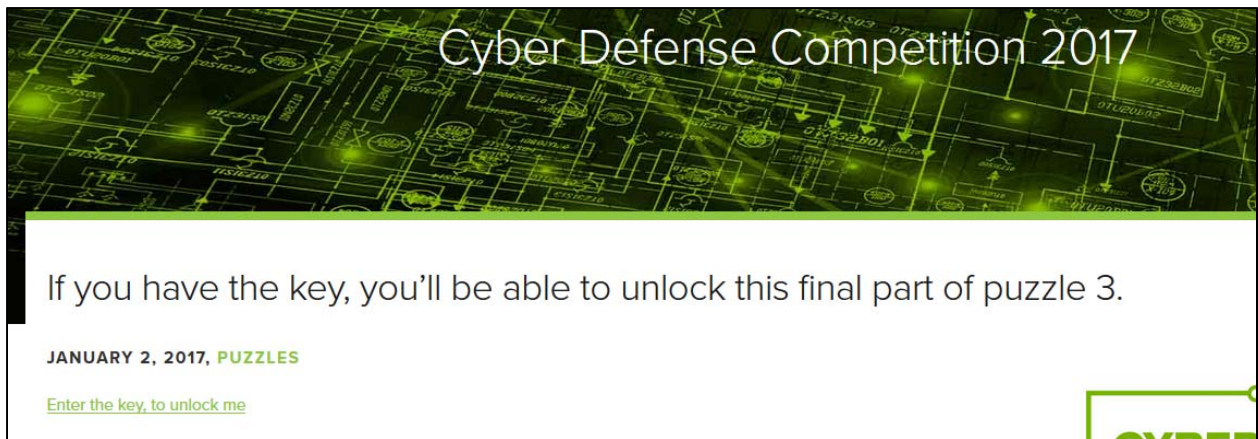


FIGURE 26 –FOLLOWING THE HYPERLINK

Once the user clicks on the hyperlink, they will see a password protected zipfile.

The password to open the zip file is “REDPAINT”

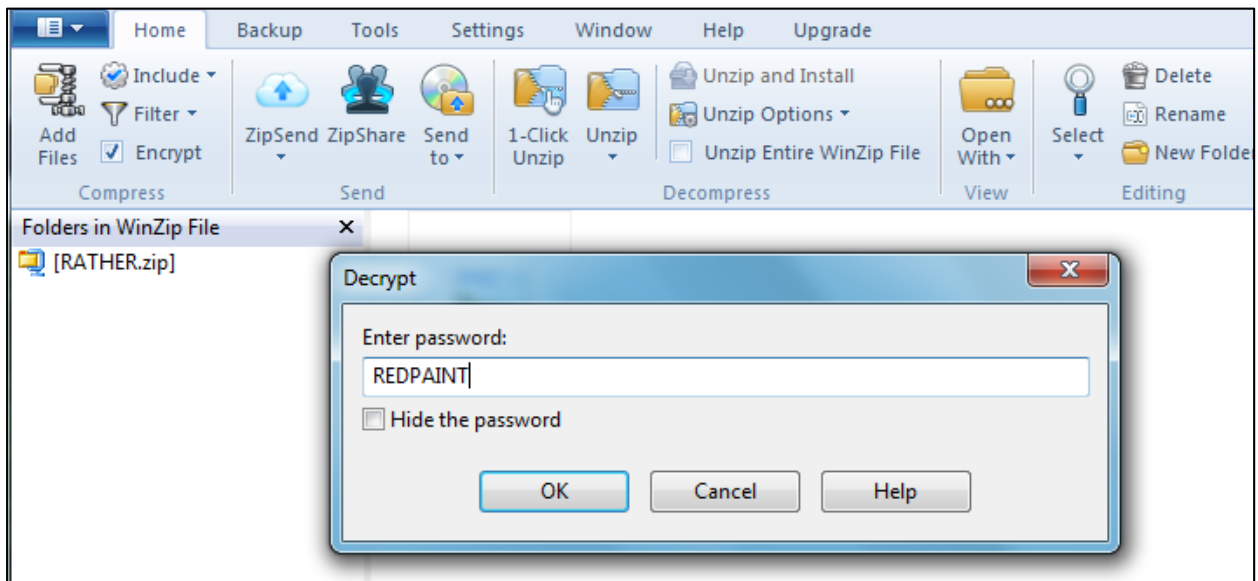


FIGURE 27 –DECRYPTING THE ZIP FILE

Once the password “REDPAINT” has been entered into the password box correctly, the user will see the decrypted zipfile:



FIGURE 28 –THE DECRYPTED ZIP FILE

A Mad Tea Party, and a Password somewhere in the Chaos

When the user opens the file, they will need to look for the password hidden in plain sight. For Meditullium, the password is hidden in the Hatter's tag on his hat.



FIGURE 29 – A MAD TEA PARTY, AND A PASSWORD SOMEWHERE IN THE CHAOS



FIGURE 30 – FINDING THE STEGO PASSWORD

The password to decrypt the steganography is 10/6.

Steganalysis and Decryption

Similar to Genesis and Patronizare, the user can deduce that there is more to this image that utilizes a key. Using steganalysis techniques such as histogram analysis or steganography tools such as StegSecret, Digital Invisible Ink Toolkit, or Virtual Steganographic Laboratory (VSL), will illuminate the usage of steganography in the puzzle.

The user will have to figure out which software was used to complete the steganography or use an online cracker that cycles through all known steganography tools to decrypt the steganography. To retrieve the file hidden in this picture, the user will have to either use the aforementioned method or download a program called steghide (which was also needed for Genesis and Patronizare).

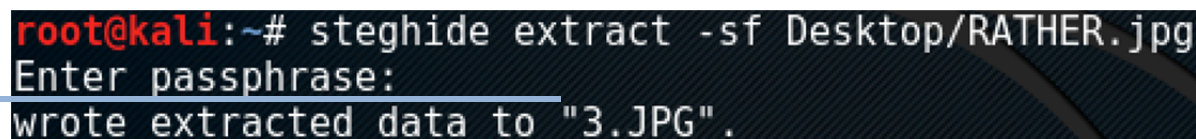
To install steghide, the user will need to install the dependencies, including libmcrypt, libmhash, and libjpeg62, and compile the program or install it from a package in order to use the software in Linux.

Once the user successfully downloads and configures steghide correctly, they will have to run it from the terminal and figure out what commands to type in, in order to extract the text file.

Similar to Genesis, the user will need to run steghide to receive the third piece of four.

The command to extract the text file is as follows:

```
steghide extract -sf /"picture location goes here"/RATHER.jpg
```



```
root@kali:~# steghide extract -sf Desktop/RATHER.jpg
Enter passphrase:
wrote extracted data to "3.JPG".
```

FIGURE 31 – DECRYPTING THE ZIP FILE

→ This is where the user will enter in the passphrase "10/6"

→ The extracted data will then be written to their pre-designated location, and the user will be able to open the 3.jpg file.

The Third Piece of Four

Upon opening the 3.jpg file, the user will notice that there is only part of an image available for viewing. This is part of a larger puzzle that will be revealed later.

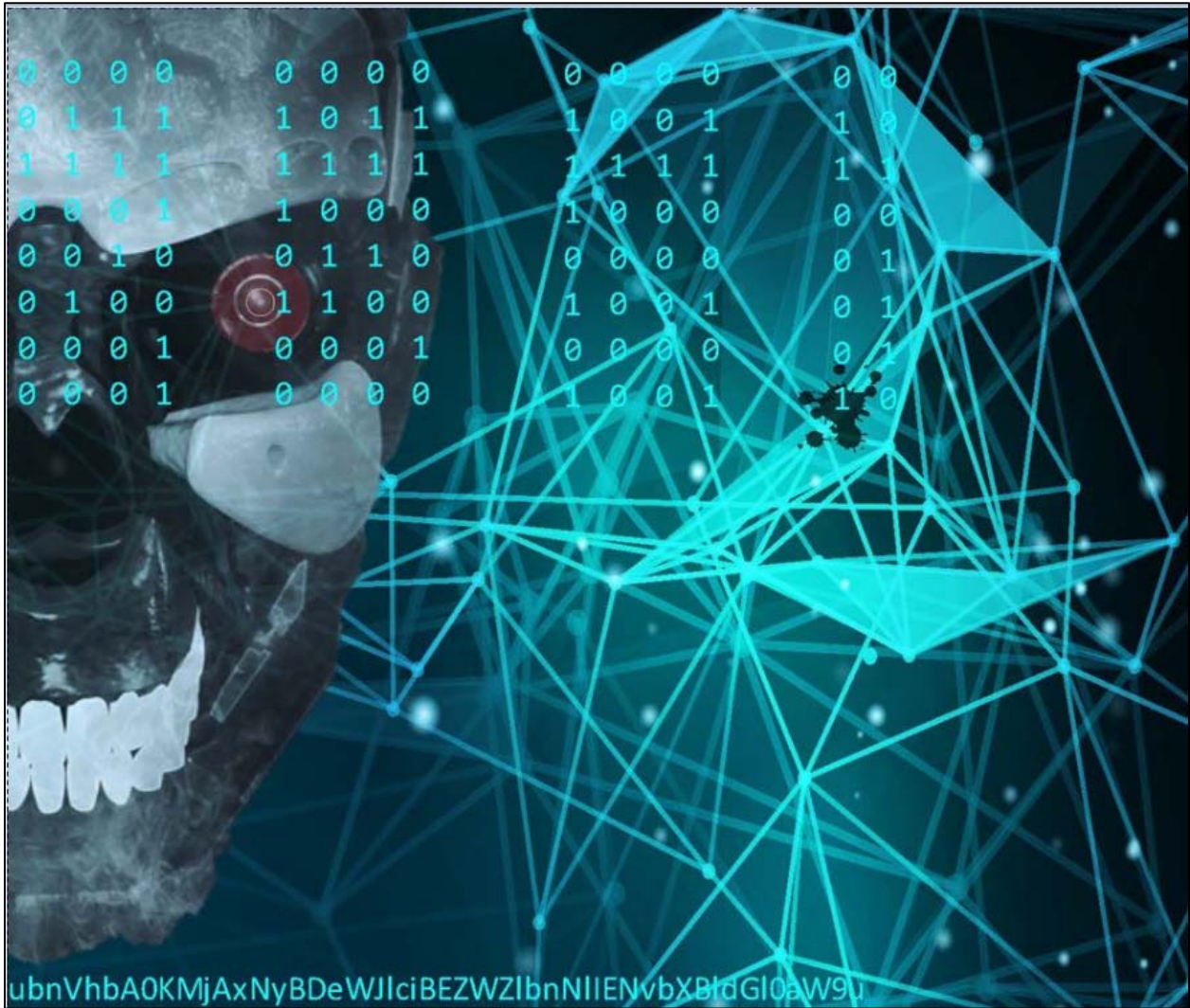


FIGURE 32 –THE THIRD PIECE OF FOUR