Following Alice’s QR Code

Users will first be confronted with an ordinary image of Alice that has a QR code placed within the picture.

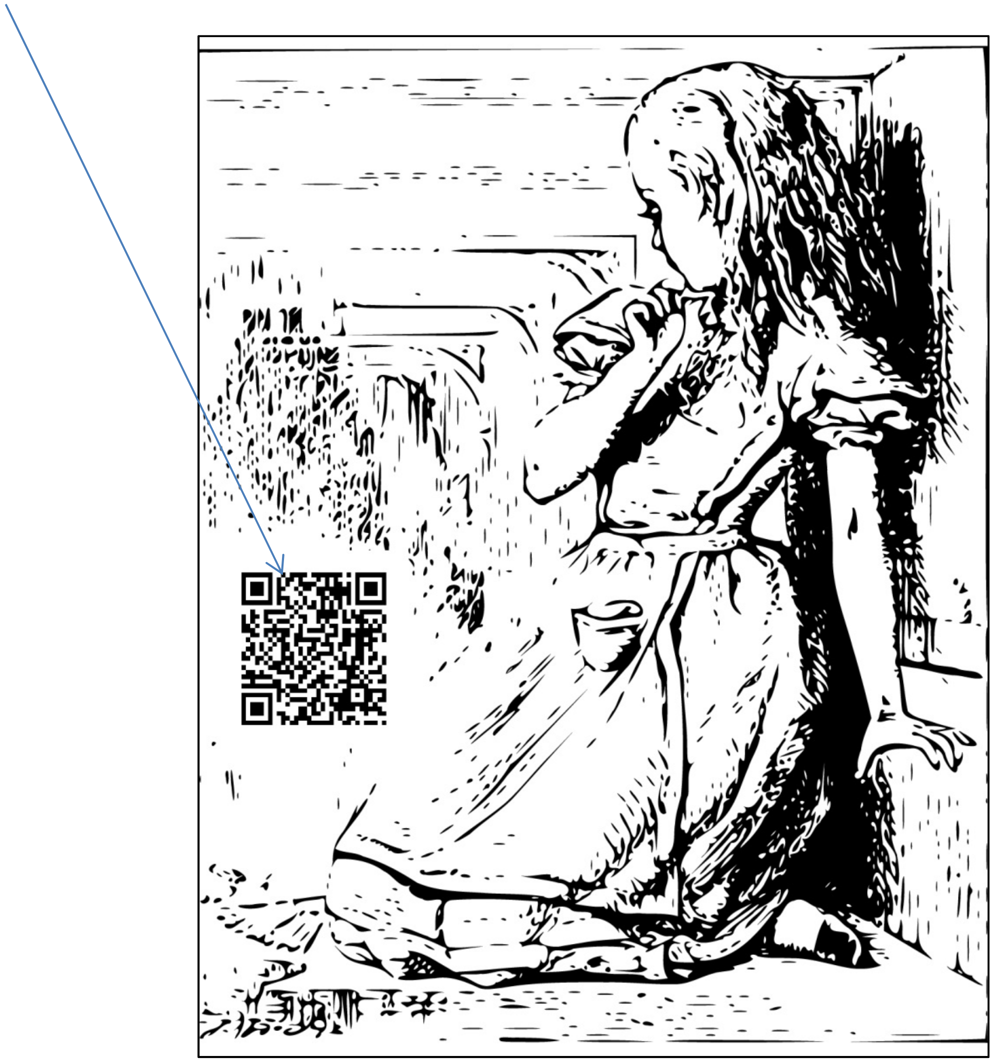
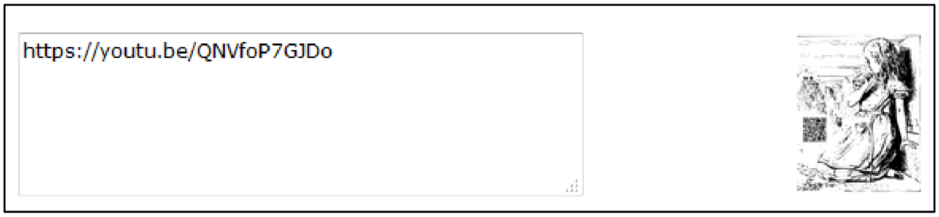


Figure 1 – Image of Alice and her QR Code

Users can either use a QR Reader on their smart device, such as Norton Snap, decode the QR code by hand, or use an online QR code reader, as shown in Figure 2.



https://youtu.be/QNVfoP7GJDo

Figure 2 – QR to URL decoder[1]

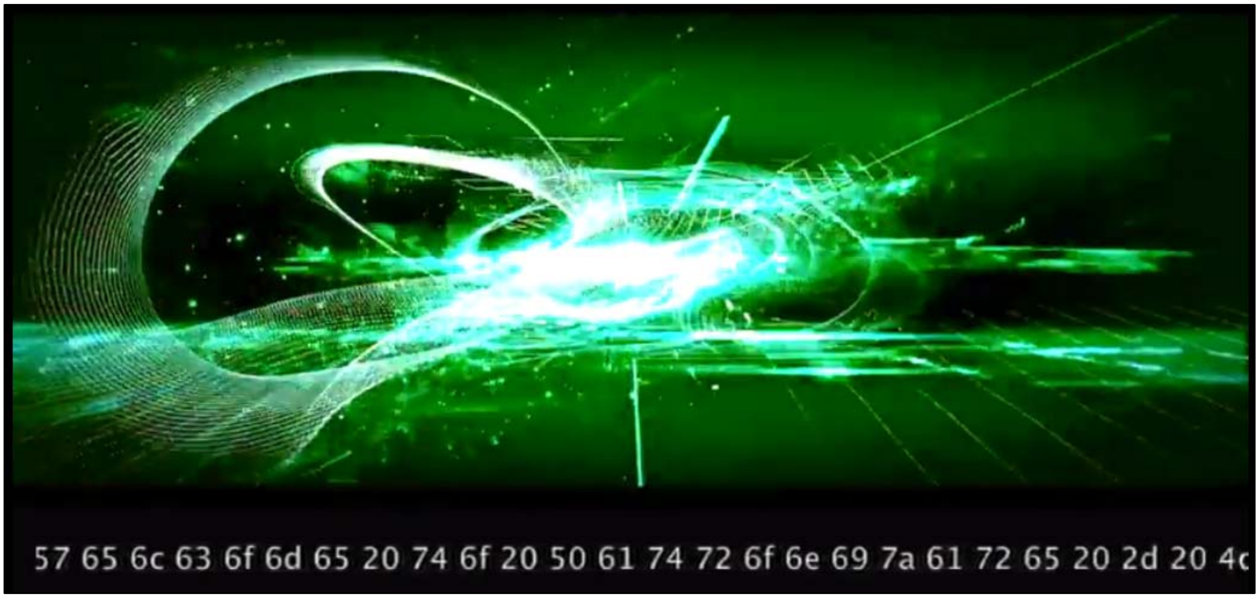
[1] http://blog.qr4.nl/Online-QR-Code_Decoder.aspx

Following the clues on Youtube

The user will be directed to a YouTube link after decoding the QR code.

The user will first watch the video that sets the tone for Puzzle 2. The hexadecimal that rolls across the screen in the first 10 seconds of the video says:

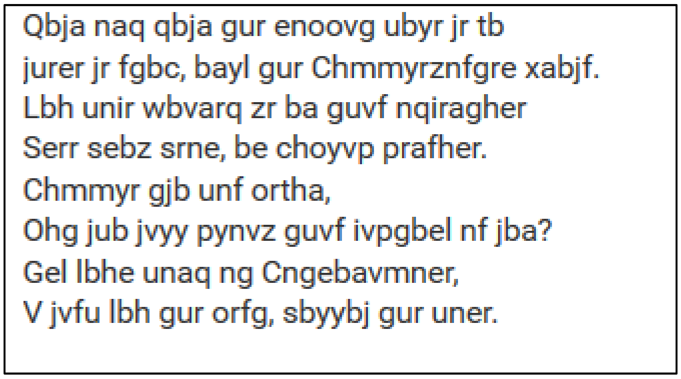
“Welcome to Puzzle 2. Let’s Begin.”



```
57 65 6c 63 6f 6d 65 20 74 6f 20 50 61 74 72 6f 6e 69 7a 61 72 65 20 2d 20 4c
```

Figure 3 – Youtube Video - Hexadecimal

The audio from the video gives the user a hint as to what to do next with this puzzle. If users are hearing impaired, the text in the description will decrypt to show the audio. The cipher used in the description is a simple ROT13 cipher.



Qbja naq qbja gur enoovg ubyr jr tb
jurer jr fgbc, bayl gur Chmmyrznfgre xabjf.
Lbh unir wbvarq zr ba guvf nqiragher
Serr sebz srne, be choyvp prafher.
Chmmyr gjb unf ortha,
Ohg jub jvyy pynvz guvf ivpgbel nf jba?
Gel lbhe unaq ng Cngebavmner,
V jvfu lbh gur orfg, sbyybj gur uner.

Figure 4 – Youtube Description Details – ROT13

Decrypted, the description will read:

“Down and Down the rabbit hole we go.
Where we stop, only the Puzzlemaster knows.

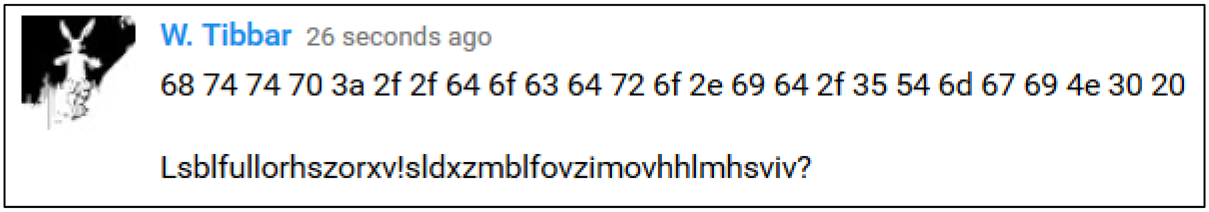
You have joined me on this adventure,
Free from fear and public censure.

Puzzle Two has begun,
But who will claim this victory as won.

Try your hand at Patronizare,
I wish you the best, follow the hare.”

The main clue the user will have to be aware of is the “follow the hare” comment.

If the user scrolls to the comment section of the Patronizare video, they will see a user named “W.Tibbar” which is an inverse of “W. Rabbit”. This is a nod to the white rabbit in “Alice’s Adventures in Wonderland,” by Lewis Carroll.



W. Tibbar 26 seconds ago

68 74 74 70 3a 2f 2f 64 6f 63 64 72 6f 2e 69 64 2f 35 54 6d 67 69 4e 30 20

Lsblfullorhszorxv!sldxzmblfovzimovhhlmhsviv?

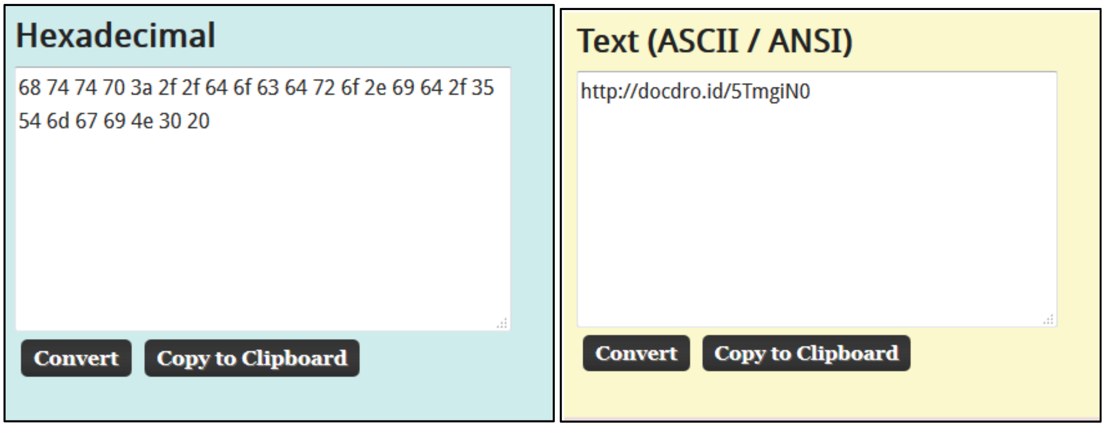
FIGURE 5 – YOUTUBE COMMENTARY BY W. TIBBAR

"W. Tibbar" left a comment that says:

68 74 74 70 3a 2f 2f 64 6f 63 64 72 6f 2e 69 64 2f 35 54 6d 67 69 4e 30 20

This is hex that decodes to: http://docdro.id/5TmgiN0

Users can pump the hex into a Hex to ASCII converter to decode the output:



```
68 74 74 70 3a 2f 2f 64 6f 63 64 72 6f 2e 69 64 2f 35
54 6d 67 69 4e 30 20
```

```
http://docdro.id/5TmgiN0
```

Figure 6 – Hex to ASCII converter[2]

The next string in W. Tibbar's comment is: Lsblfullorhszorxv!sldxzmblfovzimovhhlmhsviv?

This string is enciphered using an Atbash cipher, which is a mono-alphabetic substitution cipher. It works by substituting the first letter of an alphabet for the last letter, the second letter for the second to last and so on, effectively reversing the alphabet.

Successfully cracking this cipher will reveal the following string:

Ohyoufoolishalice!howcanyoulearnlessonshere?

W. Tibbar's comment fully deciphered will lead the user to a password protected pdf on DocDroid, and the passphrase, which is "Ohyoufoolishalice!howcanyoulearnlessonshere?"

[2] http://www.asciitohex.com/

On to DocDroid

Once the user has navigated to DocDroid, they will see that the PDF is password protected. The user will utilize the decrypted atbash cipher as the passphrase to unlocking the “Advice” PDF.

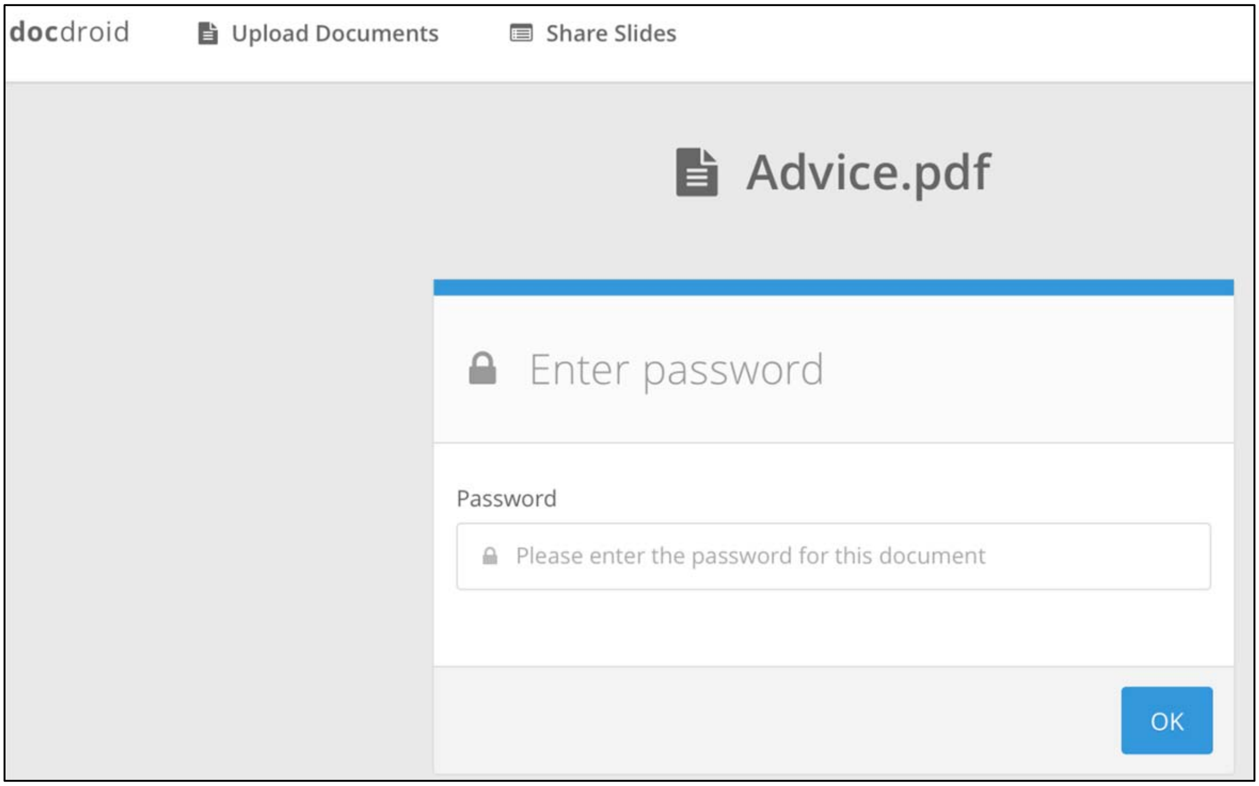


FIGURE 7 – DOCDROID

The user will need to enter the passphrase: “Ohyoufoolishalice!howcanyoulearnlessonshere?”

Decrypting the PDF

After entering in the password "Ohyoufoolishalice!howcanyoulearnlessonshere?" the following PDF will be revealed:

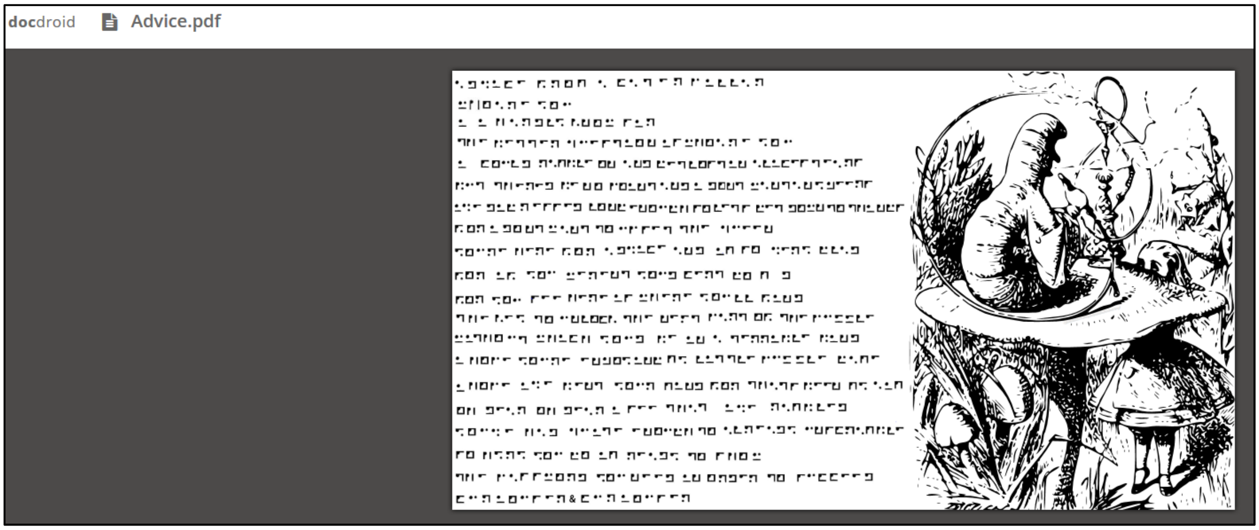


FIGURE 8 – DOCDROID

This PDF utilizes a square alphabet, more commonly known as a Nyctograph. Carroll invented this alphabet as a type of shorthand while writing Alice's Adventures in Wonderland.

"Any one who has tried, as I have often done, the process of getting out of bed at 2 a.m. in a winter night, lighting a candle, and recording some happy thought which would probably be otherwise forgotten, will agree with me it entails much discomfort. All I have now to do, if I wake and think of something I wish to record, is to draw from under the pillow a small memorandum book containing my Nyctograph, write a few lines, or even a few pages, without even putting the hands outside the bed-clothes, replace the book, and go to sleep again. – Lewis Carroll, Letter to The Lady *magazine in October 1891"*[3]

The user will have to decode the PDF using Carroll's Square Nyctograph key:

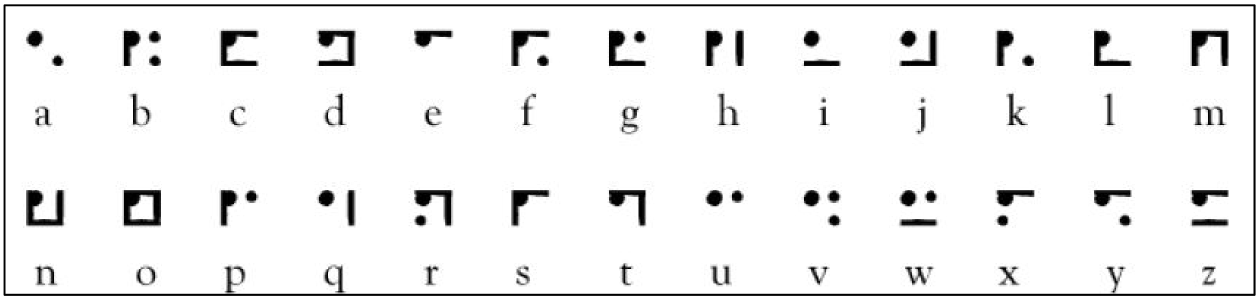
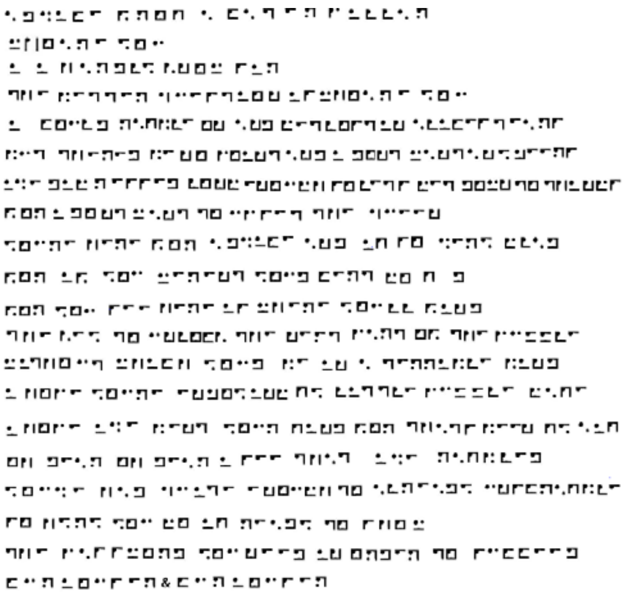


FIGURE 9 – NYCTOGRAPH KEY[4]

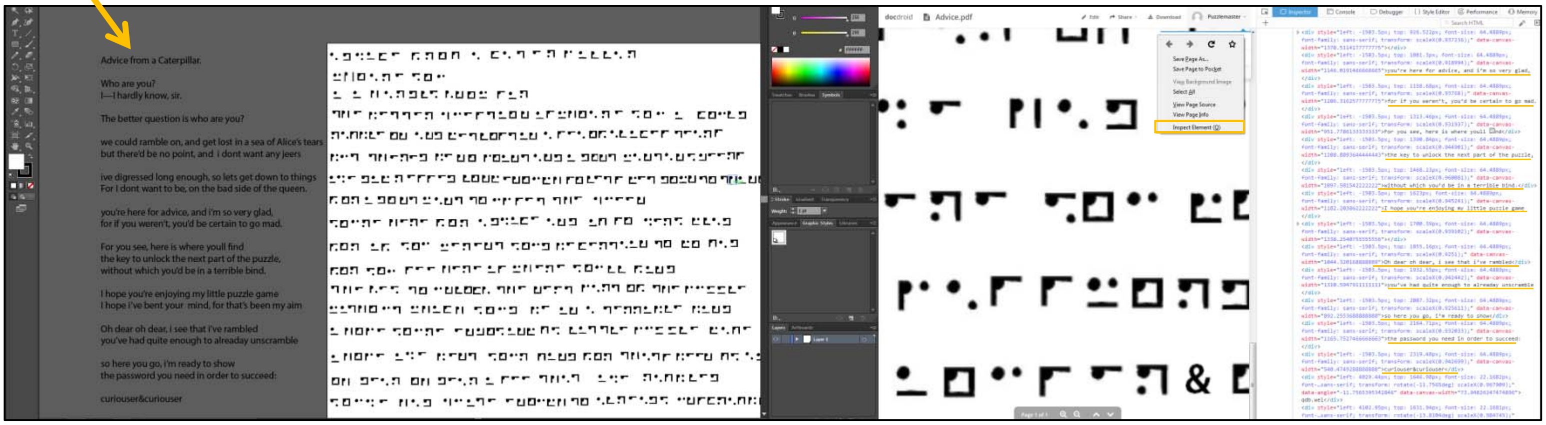
[3] http://www.lewiscarroll.org/tag/nyctograph/

[4] http://www.lewiscarroll.org/wp-content/uploads/2012/02/nyctograph_alphabet.jpg

The decrypted text is as follows:

Nyctograph	Deciphered Text
	Advice from a Caterpillar. Who are you? I—I hardly know, sir. The better question is who are you? we could ramble on, and get lost in a sea of Alice's tears but there'd be no point, and i dont want any jeers ive digressed long enough, so lets get down to things For I dont want to be, on the bad side of the queen. you're here for advice, and i'm so very glad, for if you weren't, you'd be certain to go mad. For you see, here is where youll find the key to unlock the next part of the puzzle, without which you'd be in a terrible bind. I hope you're enjoying my little puzzle game I hope i've bent your mind, for that's been my aim Oh dear oh dear, i see that i've rambled you've had quite enough to already unscramble so here you go, im ready to show the password you need in order to succeed: curiouser&curiouser

The use can also inspect the text that I have embedded in the PDF, by right clicking on "inspect element" and looking at the HTML, which shows the decoded nyctograph:



Advice from a Caterpillar.

Who are you?
I—I hardly know, sir.

The better question is who are you?

we could ramble on, and get lost in a sea of Alice's tears
but there'd be no point, and i dont want any jeers

ive digressed long enough, so lets get down to things
For I dont want to be, on the bad side of the queen.

you're here for advice, and i'm so very glad,
for if you weren't, you'd be certain to go mad.

For you see, here is where youll find
the key to unlock the next part of the puzzle,
without which you'd be in a terrible bind.

I hope you're enjoying my little puzzle game
I hope i've bent your mind, for that's been my aim

Oh dear oh dear, i see that i've rambled
you've had quite enough to alreaday unscramble

so here you go, i'm ready to show
the password you need in order to succeed:

curiouser&curiouser

FIGURE 10 – INSPECTOR ELEMENT, FINDING THE PASSWORD

The user will utilize the password at the bottom "curiouser&curiouser" for the final part of the puzzle.

The user may be wondering where the password they have just decrypted will be used. If the user further inspects the PDF, they will see some writing on the caterpillar image:

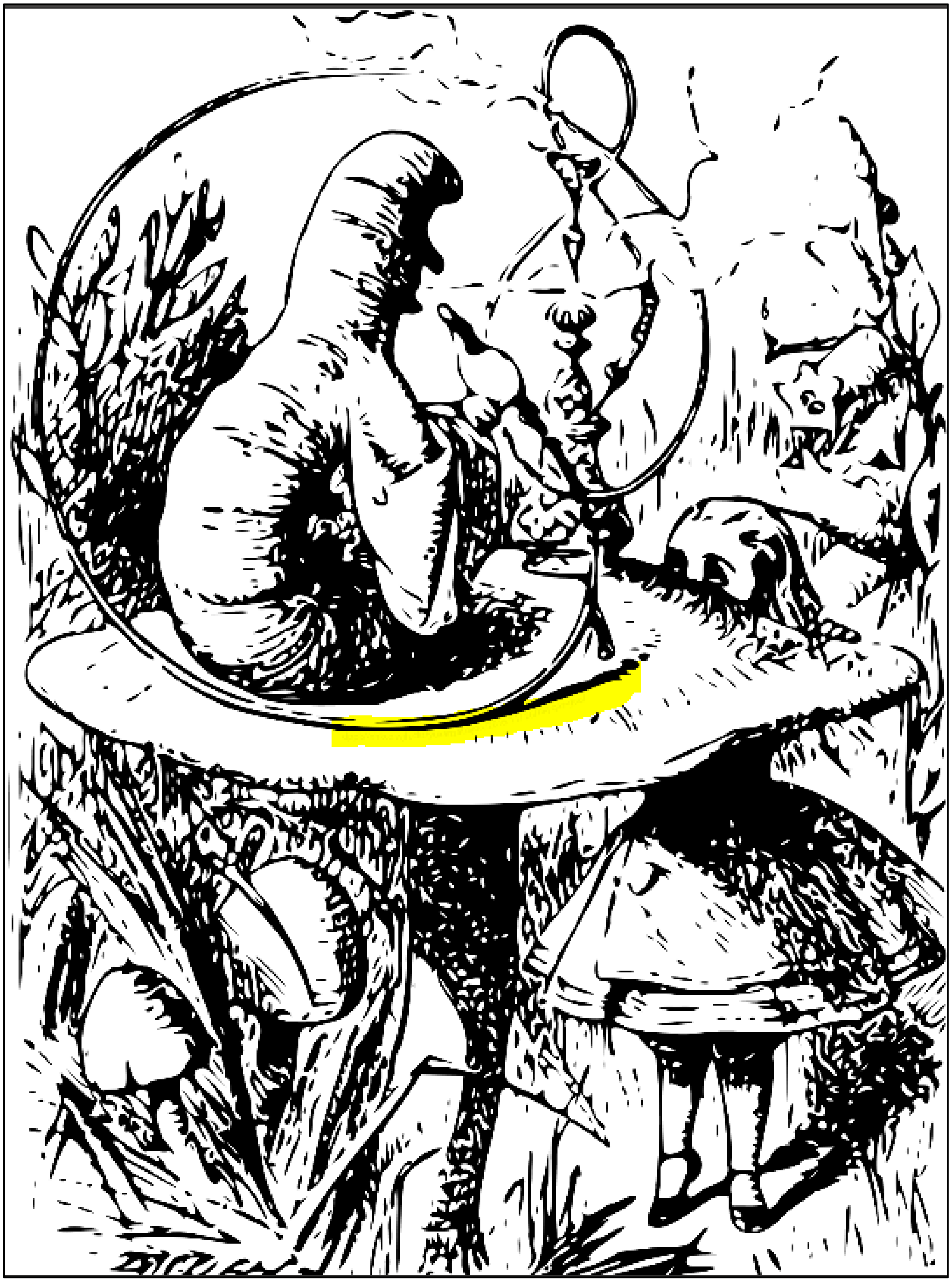


FIGURE 11 – CIPHER HYPERLINK

The user may have to use some photo editing techniques in order to see the string properly.

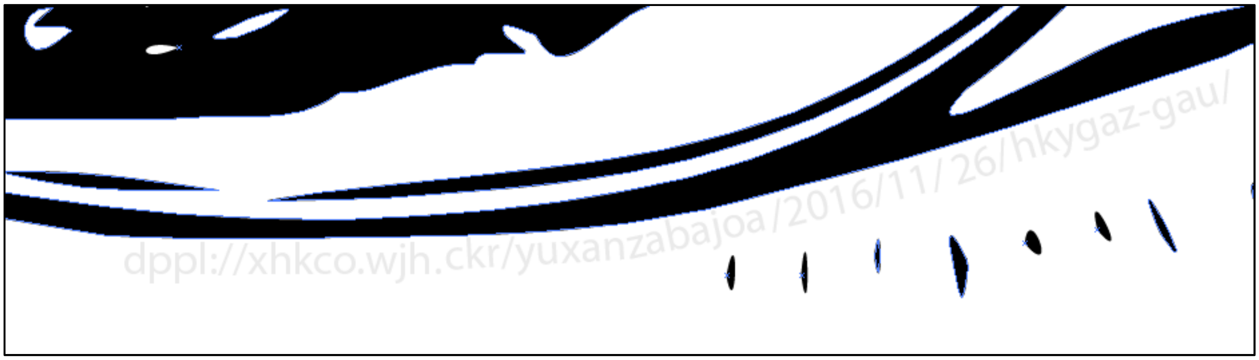


Figure 12 – Cipher hyperlink – zoomed in

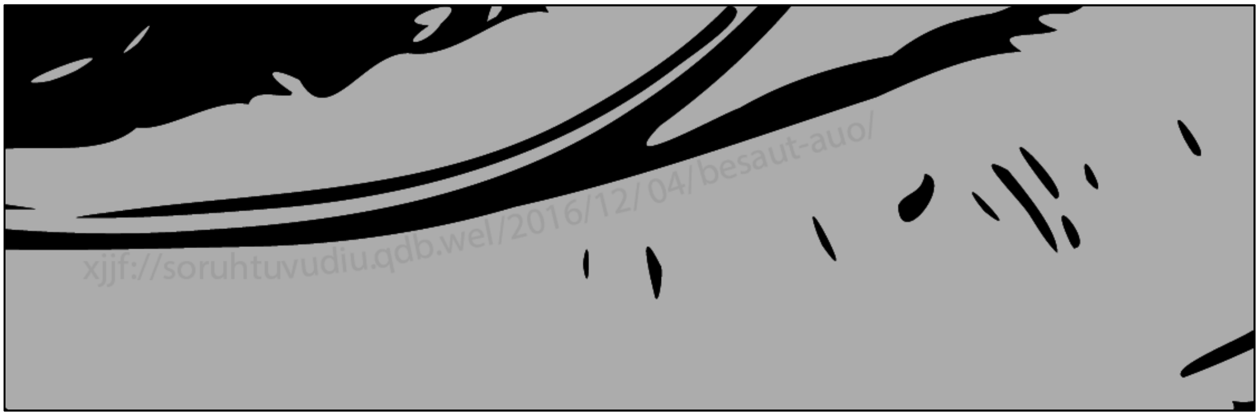


Figure 13 – Cipher Hyperlink with darkening

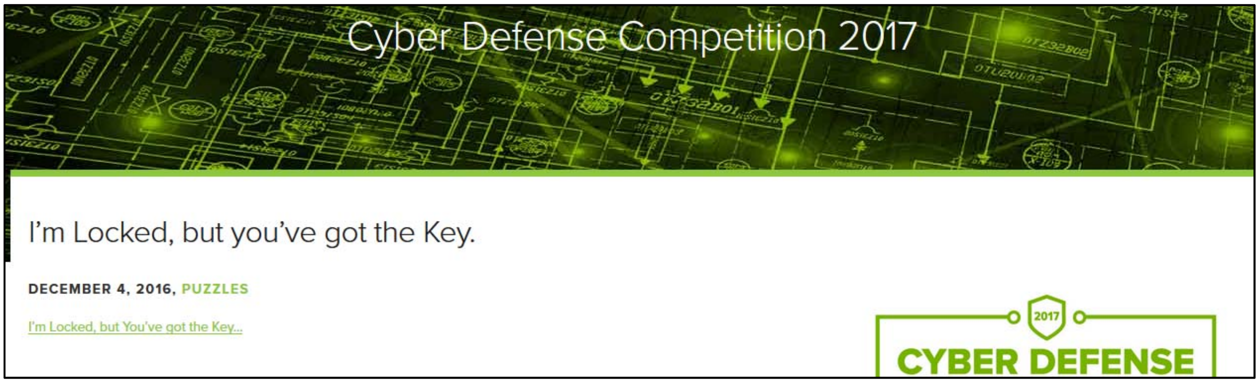
Upon further inspection, the user will see that this string is actually a Caesarian Shift cipher with an n value of 16. Once the user decrypts the string, they will see that it is actually a hyperlink that leads back to the cyberdefense.anl.gov website.

```
http://cyberdefense.anl.gov/2016/12/04/locked-key/
```

Back to the Website we go

After the user has decoded the nyctograph letter and corresponding caesar cipher, it will lead them to the final location of the puzzle, which is back to the cyberdefense.anl.gov website. The user will also have the key needed to unlock the zip file, which is "curiouser&curiouser."

After entering in the decrypted URL, the user will see the locked post:



Cyber Defense Competition 2017

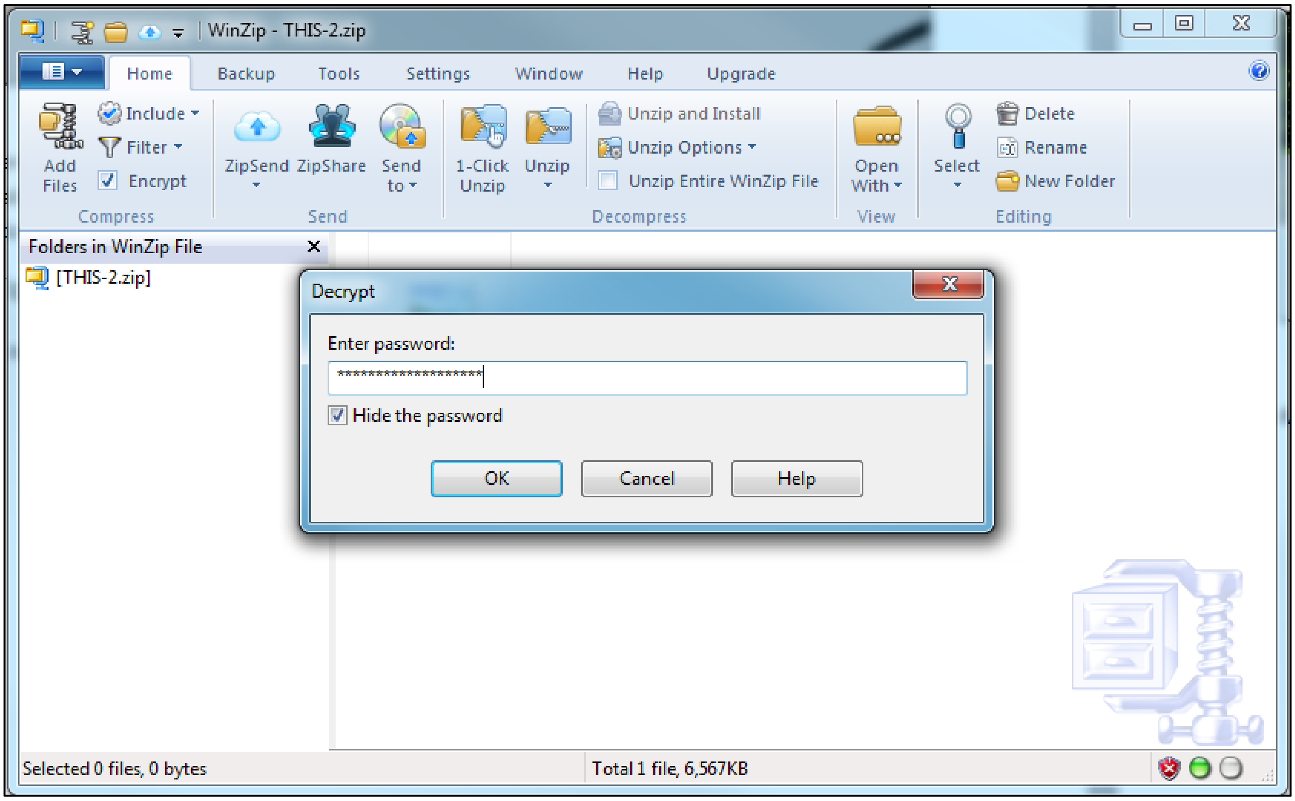
I'm Locked, but you've got the Key.

DECEMBER 4, 2016, PUZZLES

I'm Locked, but You've got the Key...

FIGURE 14 – DECRYPTING PATRONIZARE

The user will need to click on the hyperlink, which will activate the download of the zip file, and enter the correct password.



WinZip - THIS-2.zip

Decrypt

Enter password:

****

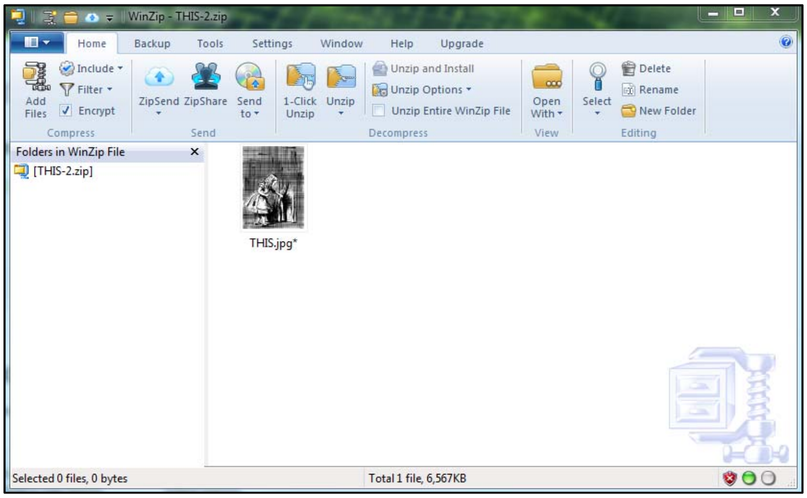
☑ Hide the password

Selected 0 files, 0 bytes

Total 1 file, 6,567KB

FIGURE 15 – DECRYPTING THE ZIPFILE

After entering in the passphrase: curiouser&curiouser, the user will see the final puzzle piece:



Selected 0 files, 0 bytes

Total 1 file, 6,567KB

Figure 16 – Unlocked Zip File

The user can then save the image to their desired file location for further analysis.

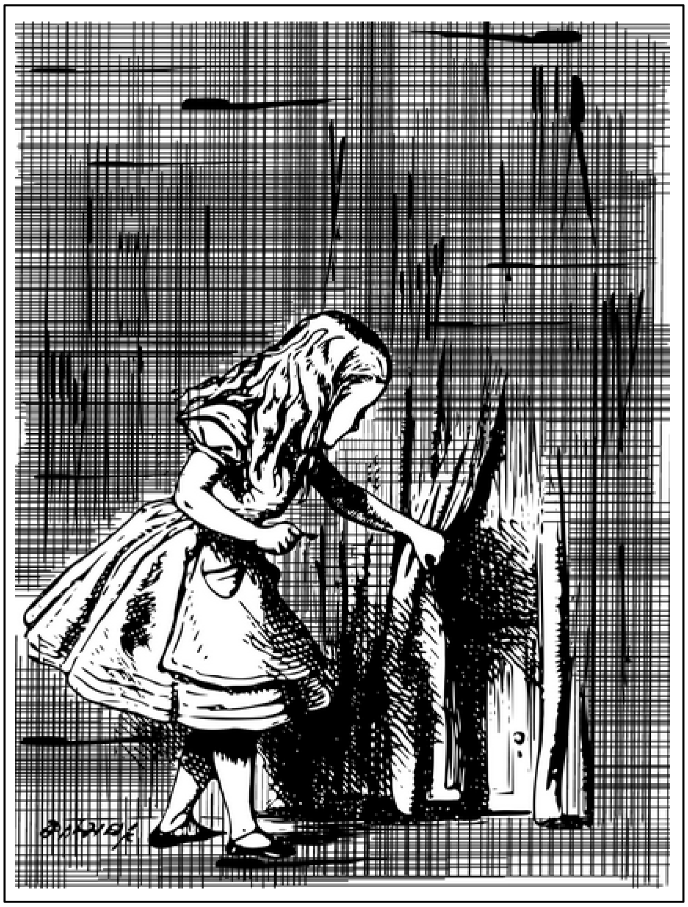


Figure 17 – Decrypting Patronizare

Alice Image Analysis

Similar to Genesis, this picture uses steganography.

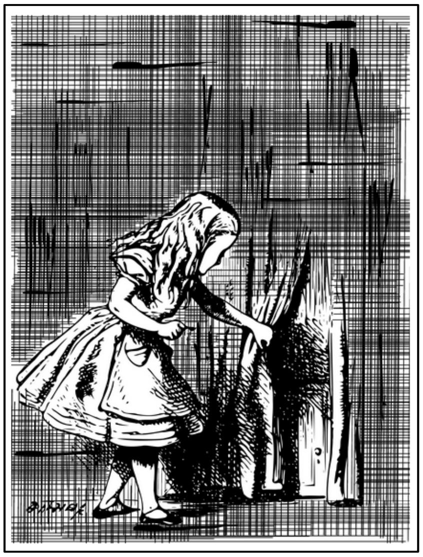


FIGURE 18 – DECRYPTING PATRONIZARE

The passphrase key to the steganography is hidden in the picture using simple obfuscation techniques. If the user tilts the picture horizontally, the word “drink” is revealed in the first quadrant, as shown in figure 16.

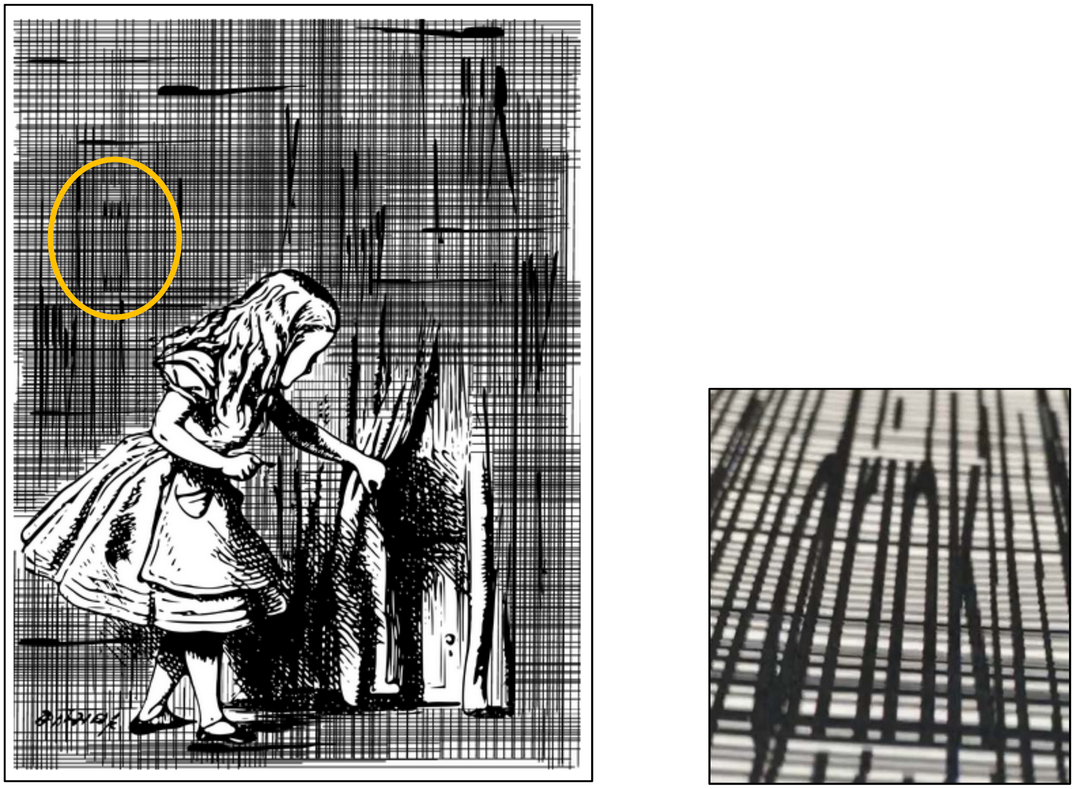


FIGURE 19 – DECRYPTING PATRONIZARE

Steganalysis and Decryption

Similar to Genesis, 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).

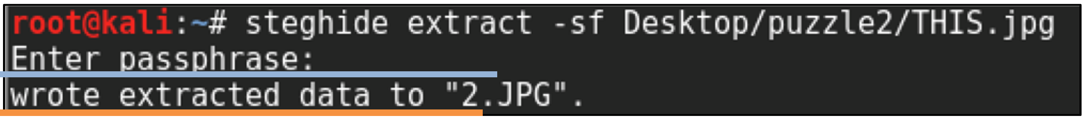
To install steghide, the user will need to install the dependencies, including libmcrypt, libmhash, and libjpeg62, and compile the program or install it from a package in order to use the software in Linux.

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 second piece of four.

The command to extract the text file is as follows:

```
steghide extract –sf /“picture location goes here”/THIS.jpg
```



```
root@kali:~# steghide extract -sf Desktop/puzzle2/THIS.jpg
Enter passphrase:
wrote extracted data to "2.JPG".
```

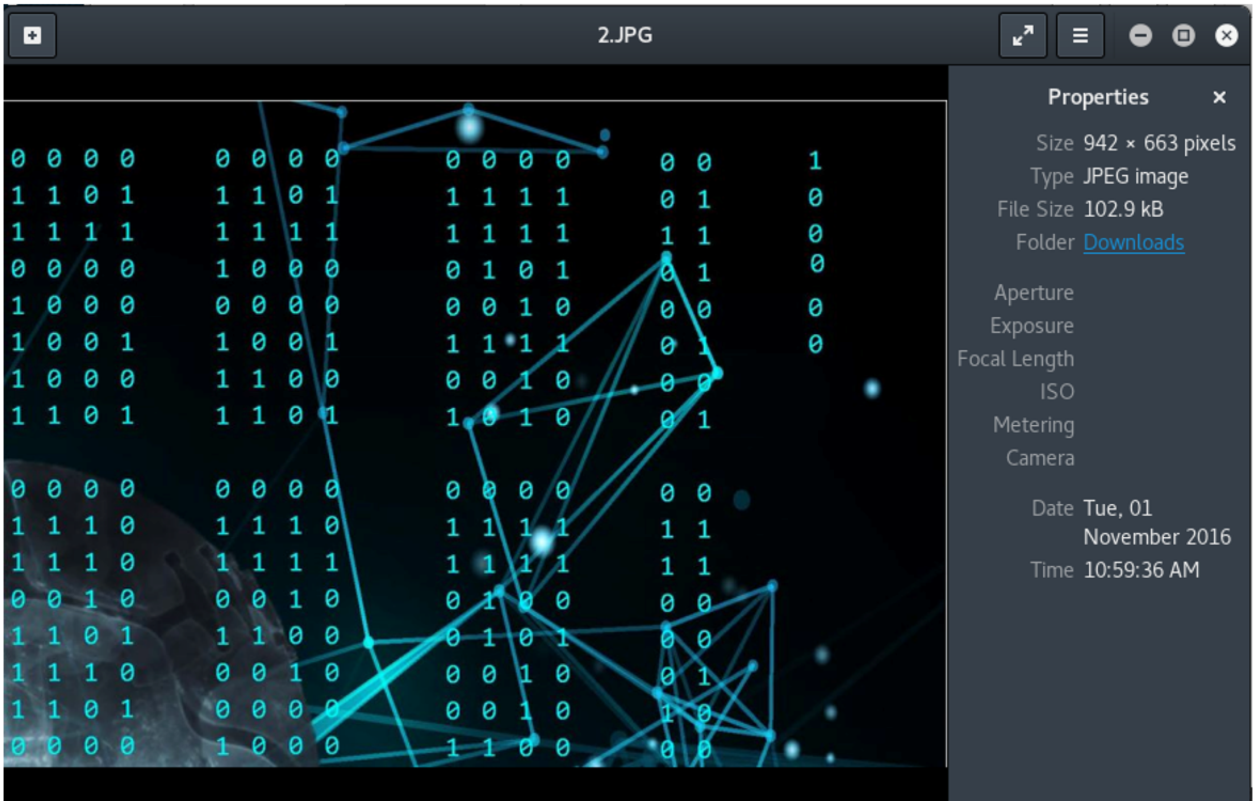
Figure 20 – Decrypting Patronizare

This is where the user will enter in the passphrase “drink”

The extracted data will then be written to their pre-designated location, and the user will be able to open the 2.jpg file.

The Second Piece of Four

Upon opening the 2.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.



Size	942 × 663 pixels
Type	JPEG image
File Size	102.9 kB
Folder	Downloads
Aperture	
Exposure	
Focal Length	
ISO	
Metering	
Camera	
Date	Tue, 01 November 2016
Time	10:59:36 AM

FIGURE 21 – DECRYPTING PATRONIZARE