

Decrypting Achévere

Thank you for reading the fourth and final installment of my puzzle series. This document will entail how to solve Achévere. Users are introduced to Puzzle #4 with this beginning image:

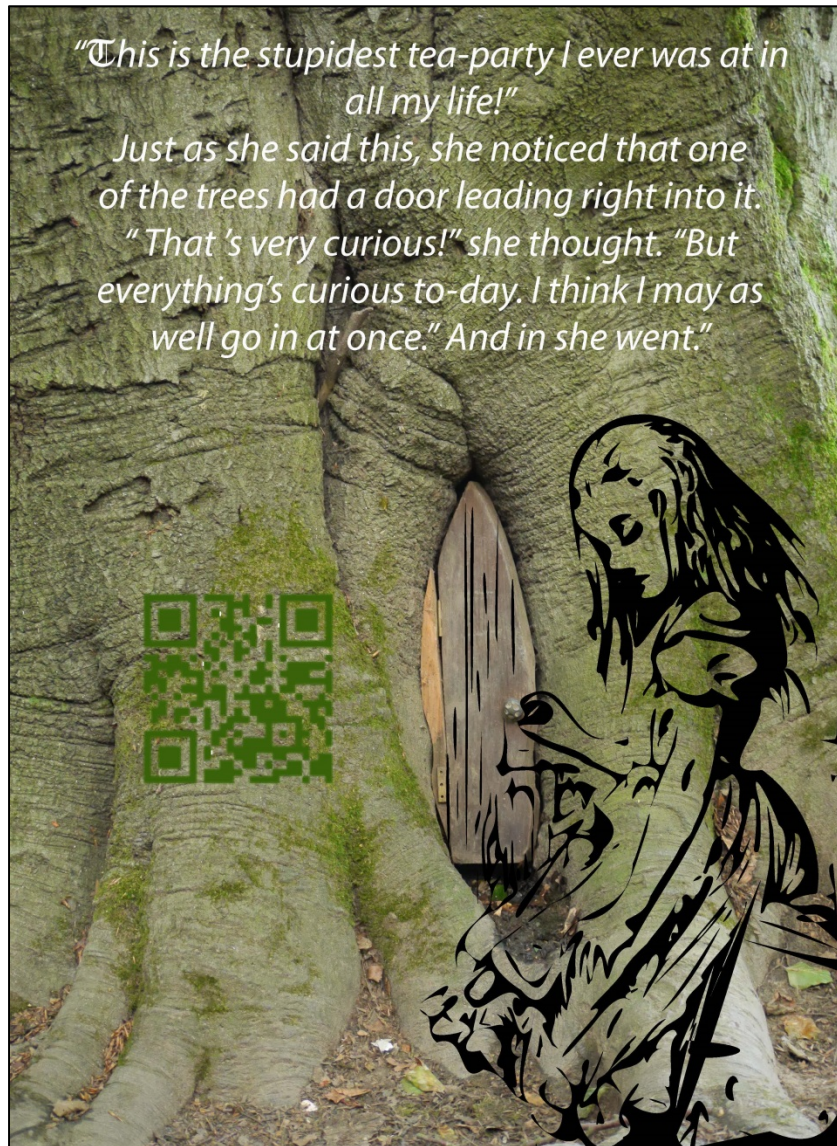


FIGURE 1 – THE KEY TO THE GARDEN¹

The user must scan the QR code to continue with the puzzle. The QR code will lead to another imgur link, which contains the first cipher.

¹ <http://imgur.com/4G1FfJ1>

POLYBIUS CIPHER

After scanning the first QR code, users will see this image:



FIGURE 2 – THE KEY TO THE GARDEN

The first chunk of text is a passage from Lewis Carroll’s *Alice’s Adventures in Wonderland*, which is supposed to allude to the reader that they are supposed to “enter” into the garden. They can accomplish this by cracking the numerical-based cipher to the right of the keyhole.

The next part of this puzzle uses a Polybius Cipher. The Polybius square, also known as the Polybius

checkerboard, was a device invented by the Ancient Greek scholar Polybius. This cipher can be used to fraction plaintext characters so that they can be represented by a smaller set of symbols, or numbers.

Each letter is then represented by its coordinates in the grid, starting with the row and then following the column. For example, "BAT" becomes "12 11 44". Because 26 characters do not quite fit in a square, it is rounded down to the next lowest square number by combining two letters (usually C and K or I and J). For this particular puzzle, the user is alerted that the square is supposed to be composed with a i/j fractioning.

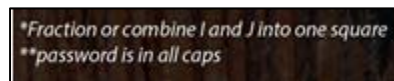


FIGURE 3 – FRACTIONING POLYBIUS SQUARE

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

FIGURE 4 – POLYBIUS CHECKERBOARD

TABLE 1 - DECRYPTING THE POLYBIUS CIPHER

T	H	E	Q	U	E	E	N	S	C	R	O	Q	U	E	T	G	R	O	U	N	D
44	23	15	41	45	15	15	33	43	13	42	34	41	45	15	44	22	42	34	45	33	14


The decoded message outputs to:

THEQUEENSCROQUETGROUND


The QR code will lead the reader to the "Trouble in the Garden" PDF.




FIGURE 5 – QR CODE TO THE “TROUBLE IN THE GARDEN”


 Trouble in the Garden


Type


☒  **Document:** Default view.

☐  **Presentation:** View optimized for slides.

Visibility

☐  **Public:** Everyone who knows the link can view and download this document.

☐  **Private:** Only you can view and download this document.

☒  **Password Protected:** Set a password for vieweing or downloading the document.

Password


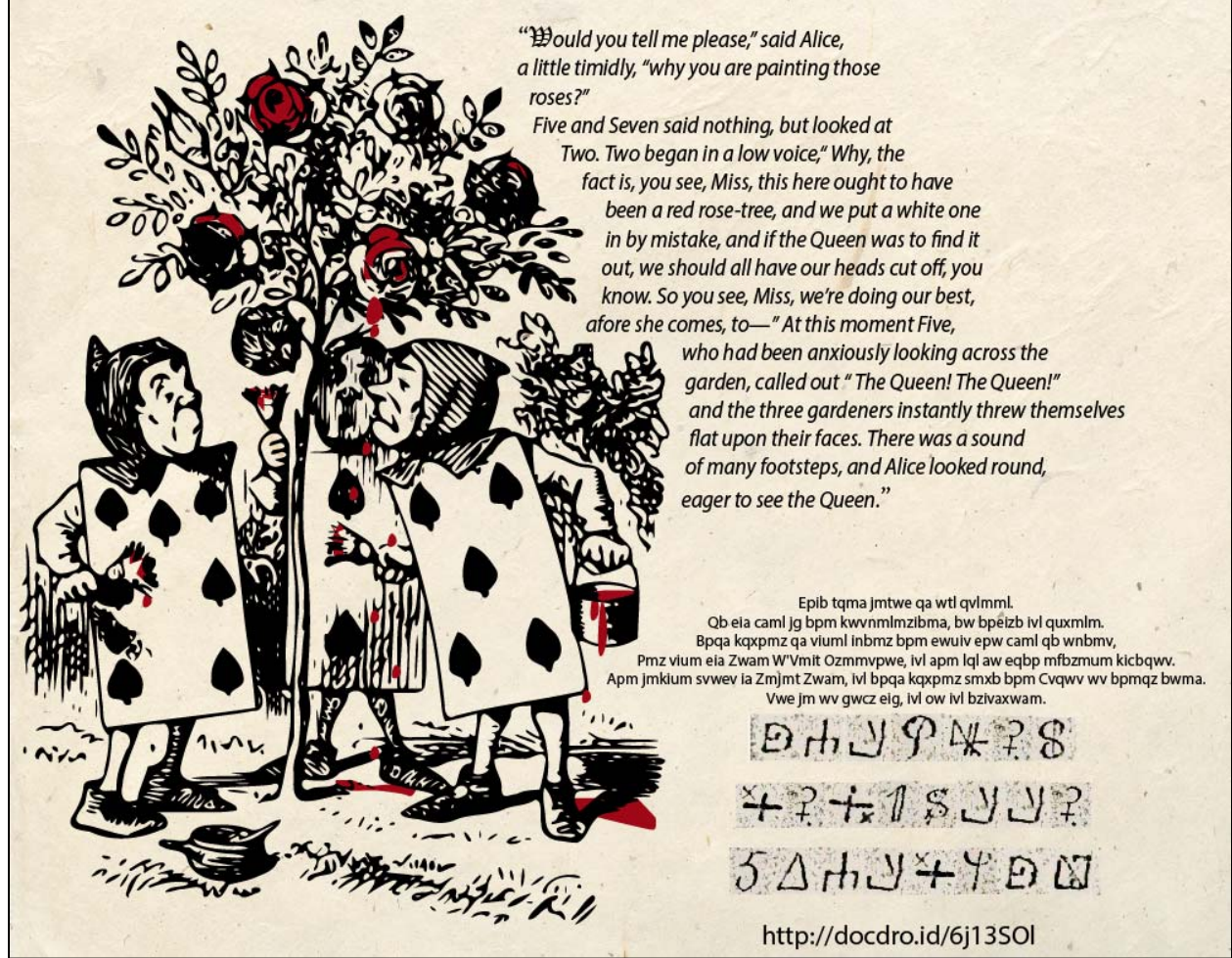
 THEQUEENSCROQUETGROUND

FIGURE 6 – UNLOCKING TROUBLE IN THE GARDEN

The user will utilize the password obtained from the Polybius to unlock the next pdf: “Trouble in the Garden.”



The middle paragraph utilizes a simple Caesarian Shift, with a N value of 8:

“Epib tqma jmtwe qa wtl qvlmml.
Qb eia caml jg bpm kwvnmlmzibma, bw bpeizb ivl quxlm.
Bpqa kqxpmz qa viuml inbmz bpm ewuiv epw caml qb wnbmv,
Pmz vium eia Zwam W'Vmit Ozmmvpwe, ivl apm lql aw eqbp
mfbzmum kicbqv.
Apm jmkium svwev ia Zmjmt Zwam, ivl bpqa kqxpmz smxb bpm
Cvqv wv bpmqz bwma.
Vwe jm wv gwcz eig, ivl ow ivl bzivaxwam bpm xiaaewzl bw bpm
vmfb xpia jmtwe:.”

When the N value is applied, the text outputs to the following:

“What lies below is old indeed.
It was used by the confederates, to thwart and impede.
This cipher is named after the woman who used it often,
Her name was Rose O'Neal Greenhow, and she did so with
extreme caution.
She became known as Rebel Rose, and this cipher kept the
Union on their toes.
Now be on your way, and go and transpose the password to the
next phase below:”

The next goal of this puzzle is to actually decode the symbols at the bottom of the PDF.

Users can obtain the original key from Greenhow, so we can decode the message in the “Trouble in the Garden” PDF

+	A	☐	S	tr. ph. sh. st. oo. ie
7	B	⊖	T	7. H. 4. 2. H. 7.
3	C	8	U	ch. au. ou. ei ss
+	D	8	V	☐. 7. 2. 8. 100
∟	E	⊖	W	Thousand. Hundred. House
Δ	F	7	X	7. 7. 7.
8	G	7	Y	Horses. Men. Officers.
h	H	R	Z	X. Lions. 4.
4	I			Capitol. Street. Cannon
⊖	J			7. 7. 7.
9	K			Lincoln. Infantry. Pen. Avenue
8	L	7		7. 7. 7.
◇	M			Regiment 1. 2. 3. 4. 5. 6. 7. 8. 9.
7	N			7. a. d. 7. 7. 7. b. 7. c. c.
5	O	10		{ Washington } Richmond
⊕	P	☐		{ K- } Z.
1	Q			Virginia. S. Carolina. Soldiers
4	R	7		7. 7. 7.
Double letters. 2 nd letter itself inverted.				

FIGURE 8 — GREENHOW ROSE CIPHER SYMBOL KEY

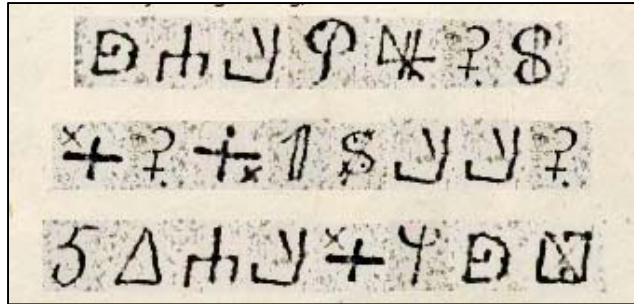


FIGURE 9 – ROSE CIPHER SYMBOLS

TABLE 2 - DECRYPTING THE ROSE CIPHER

T	H	E	K	I	N	G	
A	N	D	Q	U	E	E	N
O	F	H	E	A	R	T	S

The full phrase is as follows:

THEKINGANDQUEENOFHEARTS

This password will decrypt the next part of the puzzle, the docdroid link at the bottom of the page:

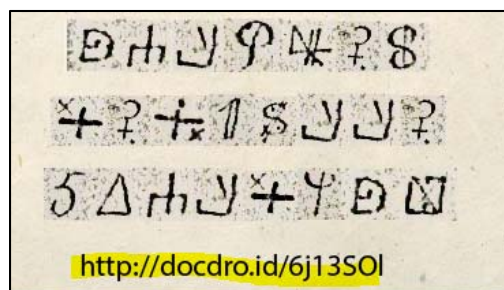


FIGURE 10 – ROSE CIPHER SYMBOLS

Password Protected: Set a password for vieweing or downloading the document.

Password

THEKINGANDQUEENOFHEARTS

FIGURE 11 – UNLOCKING “SAVE THEM.PDF”

Save Them: Their Fate is in Your Hands

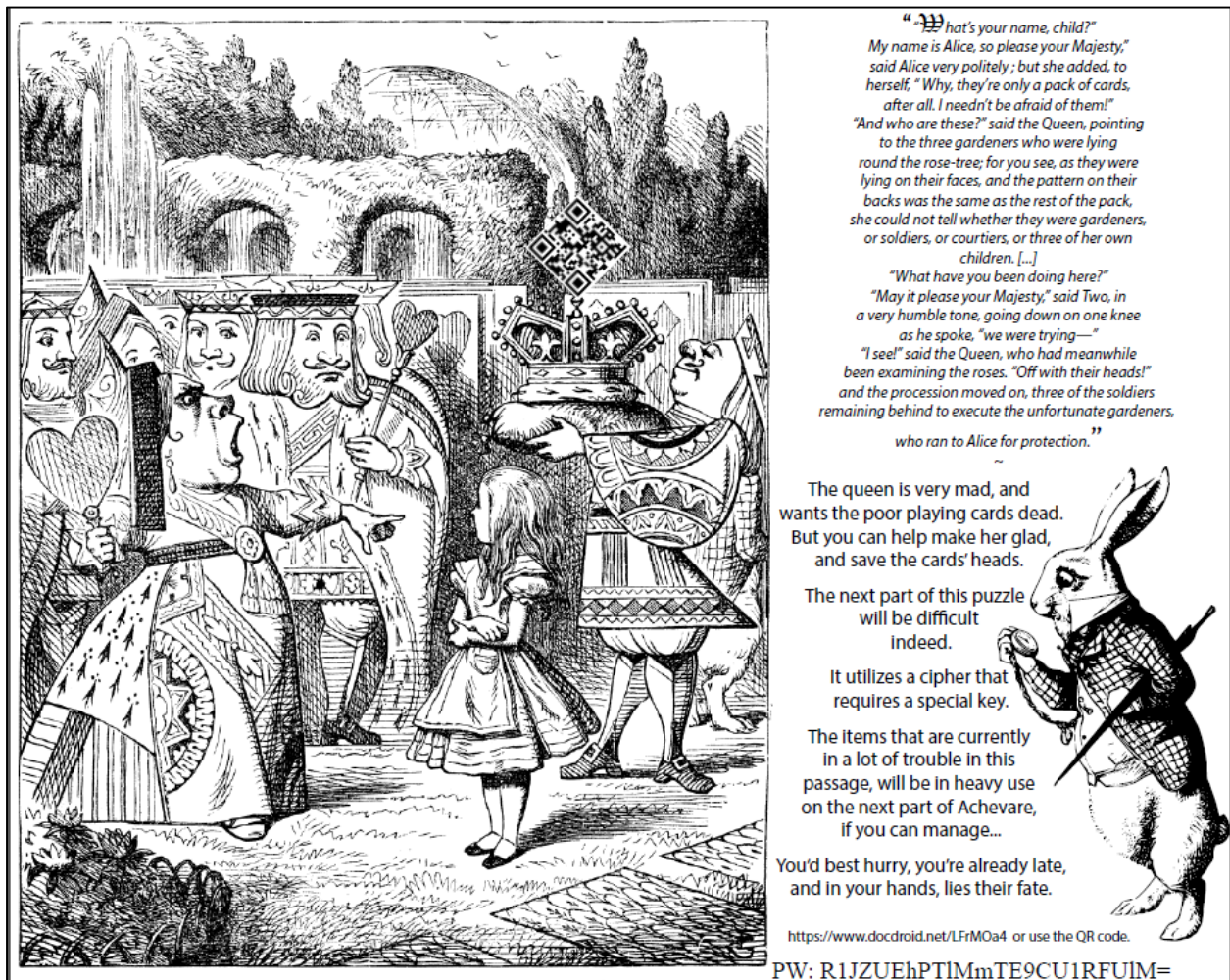


FIGURE 12 – UNLOCKING "SAVE THEM"

The first part of this PDF is an abridged passage from Alice's Adventures in Wonderland.

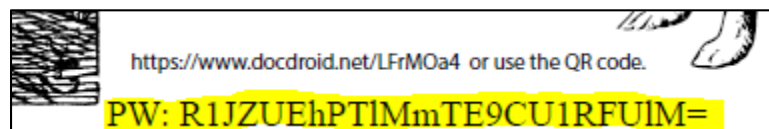
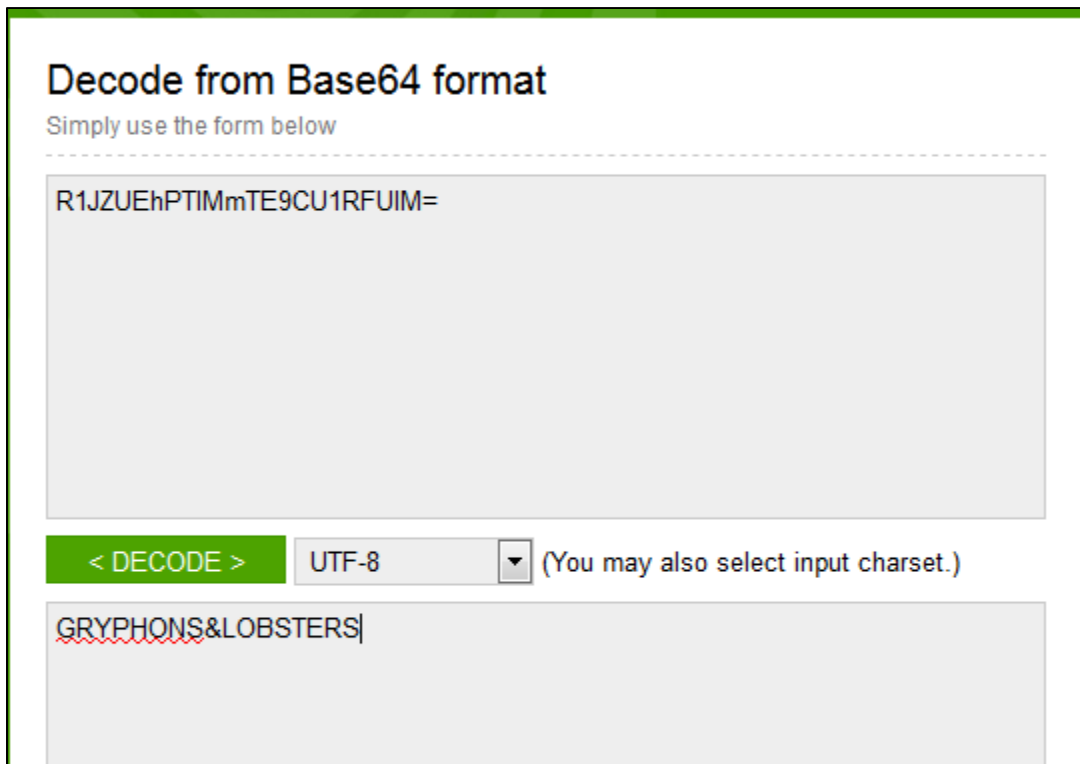


FIGURE 13 – UNLOCKING "SAVE THEM.PDF"

The second paragraph informs the user that the next challenge will be to "save" the playing cards currently in trouble in the aforementioned paragraph.

The password is at the bottom of the page and is in base 64. To decode, simply pop the string into a base 64 decoder.²

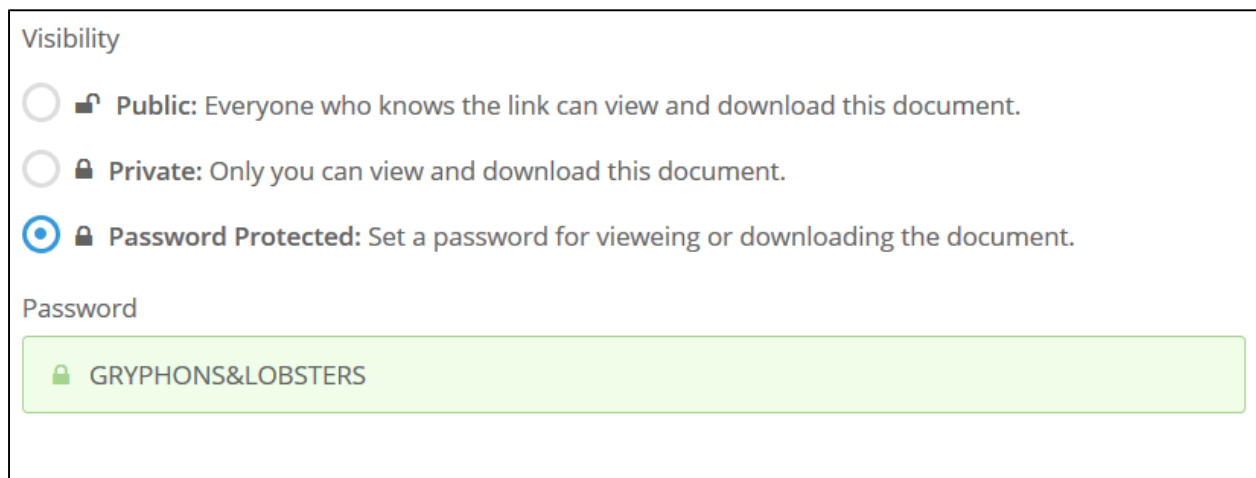
² <https://www.base64decode.org/>



The screenshot shows a web interface for decoding Base64 strings. At the top, the title "Decode from Base64 format" is displayed in a bold, black font. Below the title, a subtitle "Simply use the form below" is shown in a smaller, regular font. A dashed horizontal line separates the header from the input area. The input area is a large, light gray rectangular box containing the Base64 string "R1JZUEhPTIMmTE9CU1RFUIM=". Below the input box, there is a green button with the text "< DECODE >". To the right of the button is a dropdown menu currently set to "UTF-8", followed by the text "(You may also select input charset.)". Below these controls is another light gray rectangular box showing the decoded output "GRYPHONS&LOBSTERS|". The first few characters of the output, "GRYPHONS", are underlined with a red, wavy line.

FIGURE 14 – DECODING THE BASE64 STRING

The user will then have to go to the docdroid link listed at the bottom of the document and the password to unlock it is the aforementioned Base64 encoded string “GRYPHONS&LOBSTERS”:



The screenshot displays a settings panel for document visibility and password protection. The "Visibility" section has three radio button options: "Public: Everyone who knows the link can view and download this document.", "Private: Only you can view and download this document.", and "Password Protected: Set a password for vieweing or downloading the document." The "Password Protected" option is selected, indicated by a blue dot. Below this, the "Password" section features a light green rectangular input field containing the text "GRYPHONS&LOBSTERS" preceded by a small lock icon.

FIGURE 15 – DECODING THE BASE64 STRING

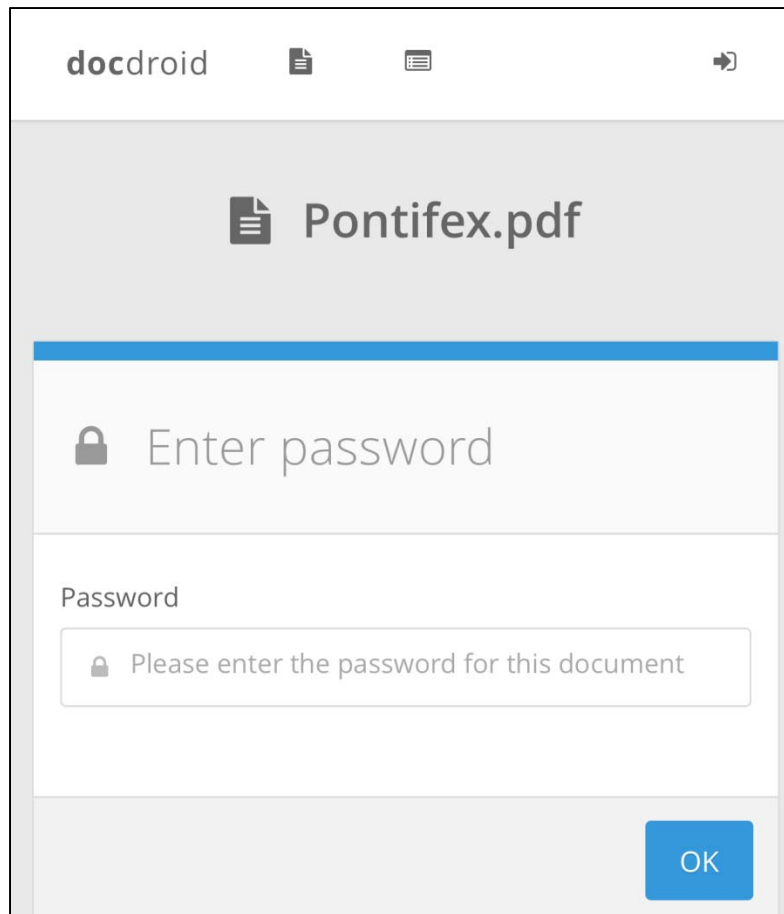


FIGURE 16 – UNLOCKING PONTIFEX

Once the user has unlocked the Pontifex PDF , they will then be confronted with the next part of the puzzle.

Pontifex ...This Will Probably Cause Codebreakers to Vex

The next part of this puzzle uses the Pontifex Cipher.

Pontifex Cipher

Key:

♦7	♥K	♥10	♠10	♦Q	♠6	♥2	♠K	♠J	♦4	♣9	♣7	♣K
♦3	♦10	♠8	♥J	♦5	♠2	♣A	♦9	♣J	♠3	♥4	♠5	♦A
♠7	♦K	♣Q	♠J	♥Q	♦2	♣2	♦J	♥7	♥5	♠J	♥6	♠3
♦8	♦6	♣6	♥3	♠4	♠10	♣5	♠9	♠Q	♠A	♣4	♥A	♥8

♥9 ♣8

Stack your deck, exactly as shown, in order to decrypt the cipher that lies below:

B F M G C R J M T K

uggc://pl0re4srafr4.nay.tbi/2017/02/01/npuriner-ybpx-naq-xrl/

"To decrypt a ciphertext message, we must start with the same deck key order that was used to encrypt the message, otherwise the plaintext message may not be recovered. We work through the algorithm, unchanged. If we started with the same deck key order as the sender, and we executed the algorithm exactly with no mistakes, then we should be able to get the same keystream output values that were used to encrypt the plaintext." ->

Require some assistance? Try this:




FIGURE 17 – PONTIFEX

This cipher was created by Bruce Schneier for the book *Cryptonomicon*, by Neal Stephenson. Also known as the Solitaire Cipher, this cryptographic algorithm was designed to allow field agents to communicate securely without having to rely on electronics or carry incriminating tools. The Pontifex cipher was designed to be a manual cryptosystem calculated with an ordinary deck of playing cards. In *Cryptonomicon*, this algorithm was originally called Pontifex to hide the fact that it involved playing cards.

Solitaire gets its security from the inherent randomness in a shuffled deck of cards. By manipulating this deck, a communicant can create a string of "random" letters that the user then combines with their message. Of course Solitaire can be simulated on a computer, but it is designed to be implemented by hand.

Encrypting with Solitaire:

Solitaire is an output-feedback mode stream cipher. Sometimes this is called key-generator. The basic idea

is that Solitaire generates a stream, often called a “keystream” of numbers between 1 and 26. To encrypt, generate the same number of keystream letters as plaintext letters. Then add them modulo 26 to plaintext letters, one at a time, to create the ciphertext. To decrypt, generate the same keystream and subtract, modulo 26 from the ciphertext to recover the plaintext.³

This table below will help with card conversions:

TABLE 3 - ALPHABETIC TO NUMERIC CONVERSION TABLE

Clubs ♣													Diamonds ♦												
Ace	2	3	4	5	6	7	8	9	10	J	Q	K	Ace	2	3	4	5	6	7	8	9	10	J	Q	K
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Hearts ♥													Spades ♠												
Ace	2	3	4	5	6	7	8	9	10	J	Q	K	Ace	2	3	4	5	6	7	8	9	10	J	Q	K
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

This table will be important as the user counts the cards and starts to develop their key stream.

The next section will go through how to encrypt and decrypt Schneier’s Solitaire cipher. The following resources may also prove to be helpful in understanding how this cipher works.

- Helpful writeup: <http://aarontoponce.org/wiki/card-ciphers/solitaire>
- Schneier writeup: <https://www.schneier.com/academic/solitaire/>

³ <https://www.schneier.com/academic/solitaire/>

Schenier's Solitaire cryptosystem first dictates to shuffle the deck around six times, which I have done.

- Shuffle the deck multiple times in order to achieve complete randomness
- Identify the first and second joker, which I did by labeling them joker A (yellow post-it) at position 9 in the 54 card deck, and
- Joker B (orange post-it) at position 37 out of the 54 card deck
- I then move Joker A down one place in the deck, and Joker B down two places in the deck.
- I then perform a triple cut, where I take all of the cards above Joker A, and all of the cards below Joker B and separate them into three separate piles. I move the cards that were below Joker B to the top of the deck, and the cards that were above Joker A to the bottom of the deck.
- I now perform a count cut, where I identify the numerical value of the bottom most card in the deck. Bottom card of count cut is the Four of Diamonds (Bridge value of 17) This means that I will count 17 cards from the top of the deck and place it just before the bottom card (which is still the Four of Diamonds)

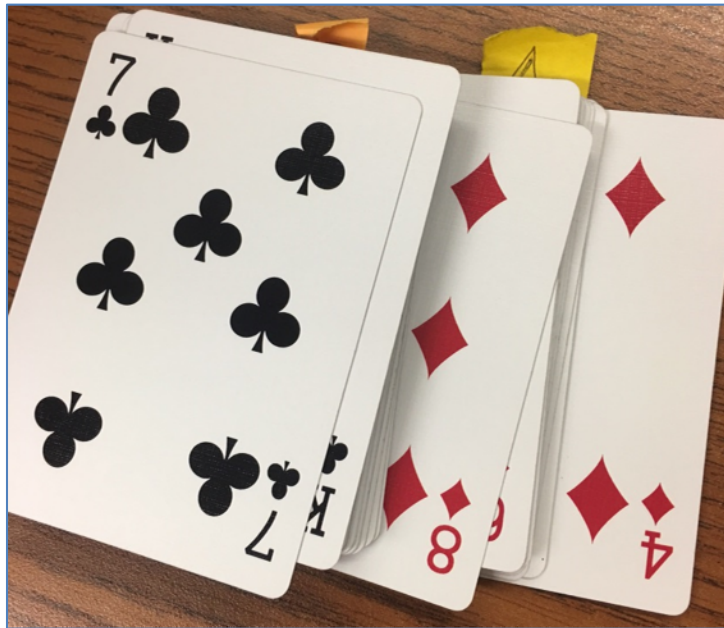


FIGURE 18 – PERFORMING A COUNT CUT

- The last step is to find the output card, by identifying the top most card in the deck, and using the bridge order to identify value (Seven of Clubs=7). I will count 7 cards and use the next card as my keystream (the 8th card), which is the Two of Spades (41)
- **Keystream Output: 41**

I'll now repeat this for the entirety of my keys:

- Bottom most card: King of Hearts (39)
Output card (top card): Ace of Diamonds (14)
Next output value: Four of Diamonds (17)
Key stream value = 17

- Bottom most card: Ten of Spades (49)
 Output card (top card): Three of Clubs (3)
 Next output value: Ten of Hearts (36)
Key stream value = 36
- Bottom most card: Six of Spades (45)
 Output card (top card): Ace of Clubs (1)
 Next output value: Nine of Diamonds (22)
Key stream value = 22
- Bottom most card: King of Spades (52)
 Output card (top card): Two of Hearts (28)
 Next output value: Nine of Clubs (9)
Key stream value = 9
- Bottom most card: Six of Diamonds (19)
 Output card (top card): King of Spades (52)
 Next output value: Ten of Spades (49)
Key stream value = 49
- Bottom most card: Three of Hearts (29)
 Output card (top card): Six of Hearts (32)
 Next output value: Five of Diamonds (18)
Key stream value = 18
- Bottom most card: Ten of Clubs (10)
 Output card (top card): 2 of Spades (41)
 Next output value: Six of Diamonds (19)
Key stream value = 19
- Bottom most card: Nine of Spades (48)
 Output card (top card): Jack of Diamonds (24)
 Next output value: eight of Hearts (34)
Key stream value = 34
- Bottom most card: Ace of Spades (40)
 Output card (top card): Four of Spades (43)
 Next output value: Six of Hearts (32)
Key stream value = 32

Encrypting my plaintext MOCKTURTLE with the Solitaire Cipher:

Plaintext:	M	O	C	K	T	U	R	T	L	E
Numerical Representation of Plaintext	13	15	3	11	20	21	18	20	12	5
Key Stream: (Calculation shown above:)	41	17	36	22	9	49	18	19	34	32
Addition of Plaintext + Keystream:	54	32	39	33	29	70	36	39	46	37
Mod 26 for # > than 26:	28	6	13	7	3	44	10	13	20	11
Mod 26 again for # still > than 26:	2					18				
Final Numbers:	2	6	13	7	3	18	10	13	20	11
Ciphertext	B	F	M	G	C	R	J	M	T	K

FIGURE 4 - ALPHABETIC TO NUMERIC CONVERSION TABLE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

To *decrypt* this ciphertext, I will reverse what I did in the above table:

Starting with my ciphertext BFMGCRJMTK:

Ciphertext	B	F	M	G	C	R	J	M	T	K
Numerical representation of ciphertext:	2	6	13	7	3	18	10	13	20	11
Key Stream, derived from cipher in deck:	41	17	36	22	9	49	18	19	34	32
Subtracting the numerical representation from the keystream:	-39	-11	-23	-15	-6	-31	-8	-6	-14	-21
We now mod (add 26) any number less than zero:	26	26	26	26	26	26	26	26	26	26
Result of mod 26:	-13	15	3	11	20	-5	18	20	12	5
Mod 26 again to any number less than 1	26					26				
Result of the second Mod 26:	13					21				
Final output:	13	15	3	11	20	21	18	20	12	5
Alphabetic representation of numerical output:	M	O	C	K	T	U	R	T	L	E

This passphrase “MOCKTURTLE” will be used to unlock the final piece of the puzzle, which is a zip file back on the cyberdefense.anl.gov website, as shown in yellow in Figure 18 below. The URL is just enciphered with a simple Caesar cipher (ROT13) with an n shift of 13.



FIGURE 19 – ROT 13 CIPHER

Once decrypted, this cipher leads back to:

<http://cyberdefense.anl.gov/2017/02/01/achieve-lock-and-key/>

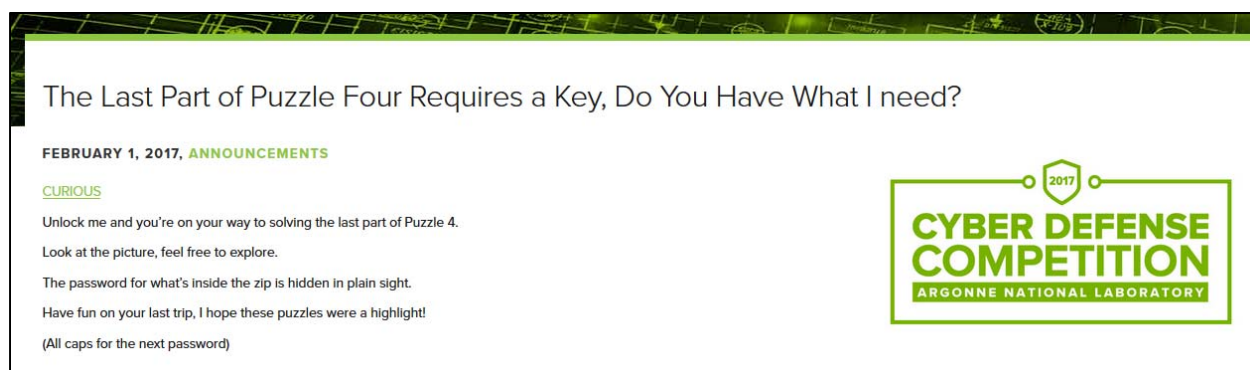


FIGURE 20 – LOCKED ZIP

Once the user has navigated to the CDC website, they will see that there is an encrypted zip file. The user must use the passphrase “MOCKTURTLE” which was gleaned via the Pontifex cipher to unlock to the zip file.

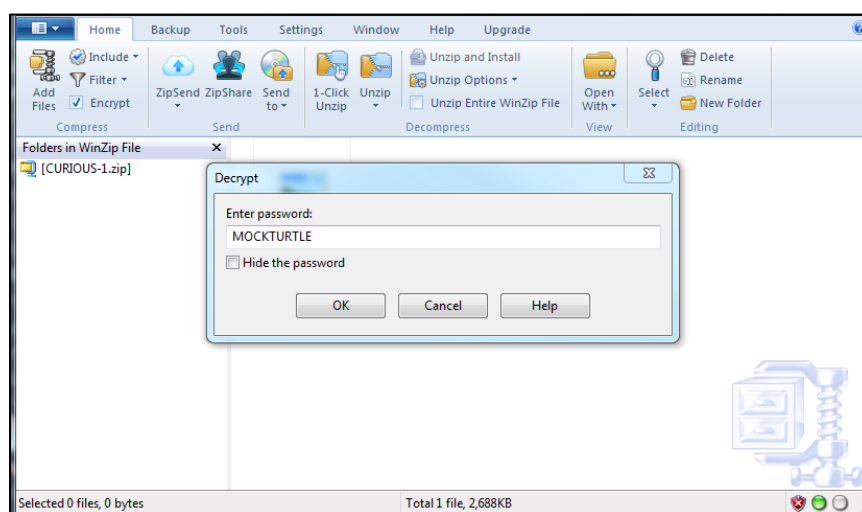


FIGURE 21 – UNLOCKING THE ZIP

A Password Hidden in way more than a game of 52 Card Pickup

Once the user has entered the correct password, the following image will be revealed:

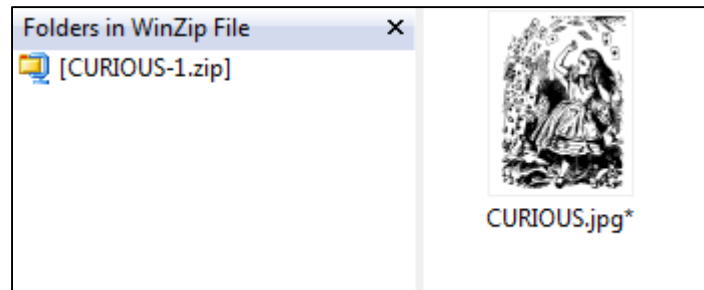


FIGURE 22 – CURIOUS



FIGURE 23 – A WONDERLAND PICKUP

When the user opens the file, they will need to look for the password hidden in plain sight. For Achevare, the password is hidden in the deck of cards:



FIGURE 24 – UNCOVERING THE PASSWORD

The cards spell out the word:

WONDERLAND

This is the passphrase needed to unlock the steganography.

Steganalysis and Decryption

Similar to Genesis, Patronizare, and Meditullium, 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, Patronizare, and Meditullium).

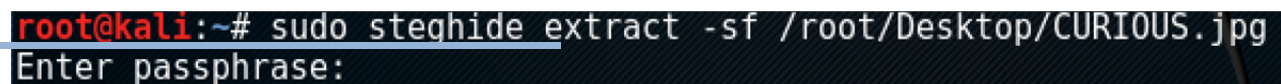
To install steghide, the user will need to install the dependencies, including libmcrypt, libmhash, and libjpeg62, and compile the program or install it from a package in order to use the software in Linux.

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
```

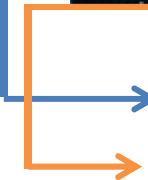


```
root@kali:~# sudo steghide extract -sf /root/Desktop/CURIOUS.jpg
Enter passphrase:
```

FIGURE 25 – DECRYPTING THE ZIP FILE



This is where the user will enter in the passphrase "WONDERLAND"



The extracted data will then be written to their pre-designated location, and the user will be able to open the 4.jpg file.

The Final Piece of Four

Upon opening the 4.jpg file, the user will notice that this is the final image needed to decode the binary. There is also a QR code for the user to view at their leisure.



FIGURE 26 – THE FINAL PIECE OF FOUR

The user can now piece together all of the pieces of four, to reveal the following:

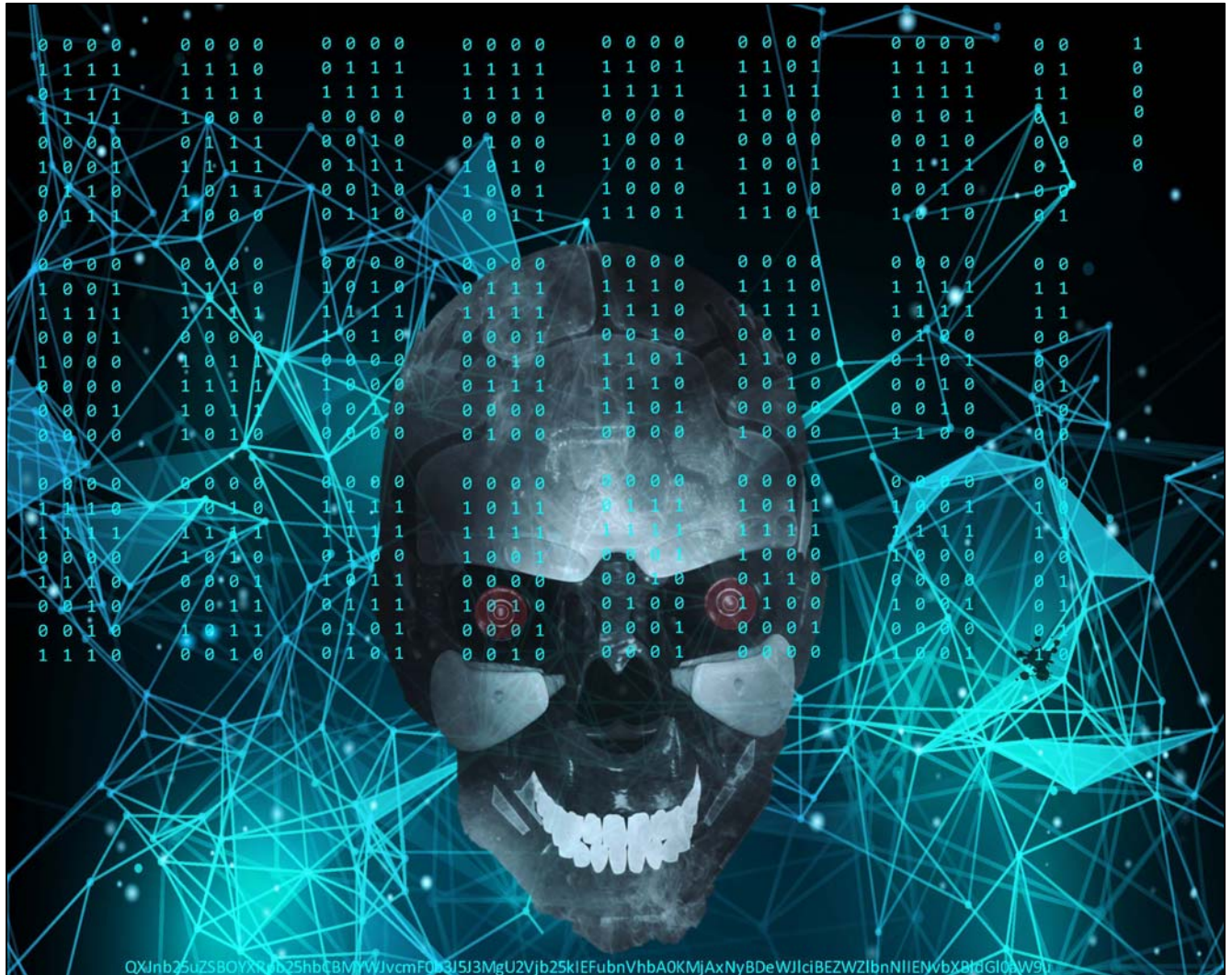


FIGURE 27 – ALL PIECES OF FOUR

Once the user decodes the binary, they will see that it resolves to:

Binary decrypts to:

“This is our world now... the world of the electron and the switch, the beauty of the baud.”

(From the hacker’s manifesto: <https://www.usc.edu/~douglast/202/lecture23/manifesto.html>)

Base64 decrypts to:

Argonne National Laboratory's Second Annual 2017 Cyber Defense Competition

Puzzlemaster's Thoughts

The user will also notice a QR code. This resolves to the following image posted on Imgur:

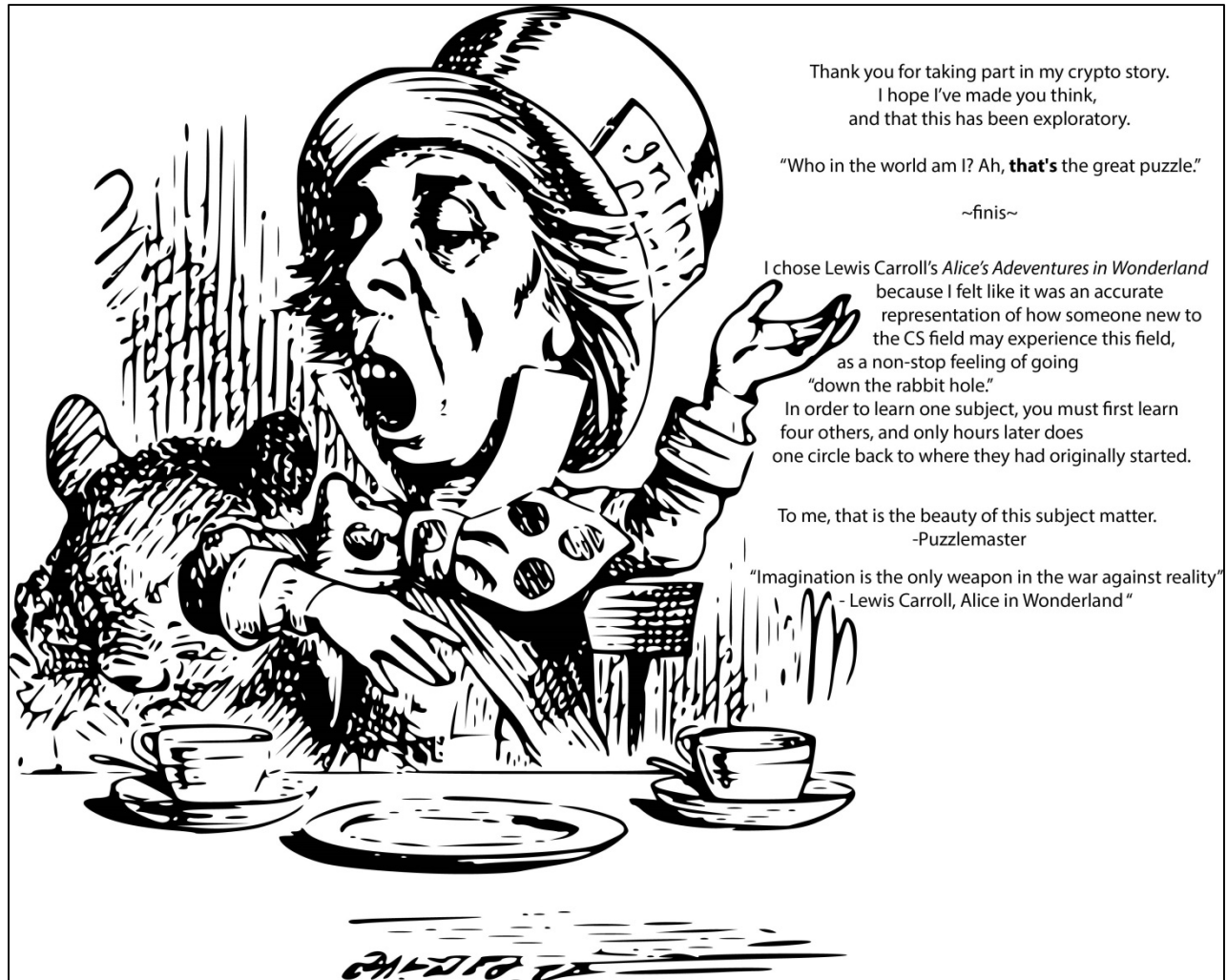


FIGURE 28 – IMGUR EXPLANATION⁴

I wanted to leave the user with my thoughts on how I built the puzzles and leave them with the following quotes for introspection:

"Who in the world am I? Ah, that's the greatest puzzle."

and

"Imagination is the only weapon in the war against reality"

Both quotes from Alice's Adventures in Wonderland.

⁴ <http://imgur.com/yRcHEKz>