

Cicada 3301

The Mystery



@iBotPeaches
sourcetoad



Story Time

- Cicada 3301
- 3 Puzzles
- Worldwide Hunt
- Largely Unknown in Public
- Scary



Who?

- **Connor Tumbleson**
- @iBotPeaches
- Apktool



January 5, 2012 - 4chan

- Weird part of Internet
- No Description
- “hidden in this image”
- Hex Editor Time?

Hello. We are looking for highly intelligent individuals. To find them, we have devised a test.

There is a message hidden in this image.

Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through.

Good luck.

3301

Puzzle #1 - Text Editor

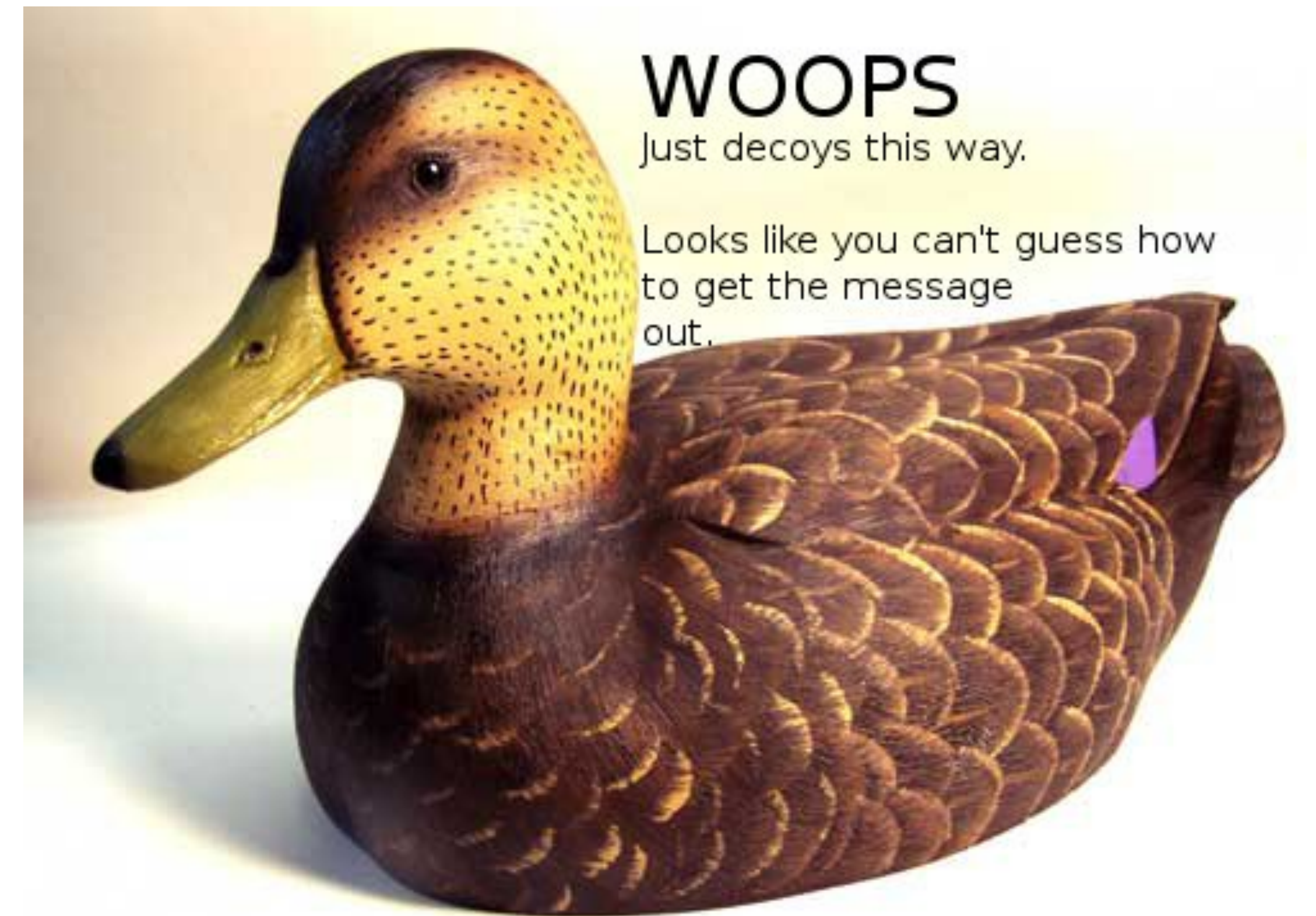
```
\9C\E7\DB\DF"\AF\EA\9E+\D2\F4\AF\8E\EB\AE\C3,W[00]QJ\91^M \CAHLB9\DD@
\DB\CA.[00]W3)\86K`r \E4\B1P[00]\A8[00]\E4\FAs\ [00]\8B\B5\B1\E2?[00]\EA\BA@T\
\C7\F3[00]\CB\F2\F7\B7\97\9C\ED\C9\C6~\95 \00w[00][00][00]\E3\CF\C1_\F6-\DB[
\00QKI@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]R\D0[00]QE[00]\00QE[00]\00QE-\00%[00]
\00QE[00]\00QE[00]\00QE[00]\00R\D2Q@[00][00]Q@[00]-%[00]\00R\D2Q@[00][00]Q@[00][00]\B4\94\
\00%[00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00]IE[00]\00QKI@[00][00]Q@[00][00]Q@[00][00]R\
\94Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]\B4\94\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\
\00%[00]Q@[00][00]R\D0[00]QE[00]\00QE[00]\00QE[00]\00QKI@[00][00]Q@[00][00]R\D0[00]R\D2Q@[00][00]
\00%[00]R\D0[00]R\D2Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00]IE[00]\00QE[00]\00QKI@[00]IE[00]\00QE[00]
\00QE[00]\00QE[00]\00QKI@[00][00]Q@[00]IE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\
\00QE-\00%[00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]Q@[00][00]R\D0[00]R\D2Q@[00]-%[00]\00\B4\94Q@[00][00]
\00QE[00]\00QE[00]\00\B4\94Q@[00][00]Q@[00][00]Q@[00][00]Q@[00]-%[00]\00QE[00]\00QE[00]\00QE[
\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE[00]\00QE
\D9TIBERIVS CLAUDIVS CAESAR says "lxx>33m2mqkyv2gsq3q=w]02ntk"
```


Puzzle #1 - Caesar Cipher

- *lxxxt> 33m2mqkyv2gsq3q = w] 02ntk*
- Caesar Cipher is part of ROT family
- ROT0 - ROT26 - “rotates” text
- +4 - [http://{i.imgur.com/m{9{sY{K.jpg](http://i.imgur.com/m{9{sY{K.jpg)

Puzzle #1 - The Decoy

- Image loaded
- “can’t guess how”
- “to get image out”
- **outguess** (tool)



Puzzle #1 - Original Outguess

```
→ cicada outguess -r 3301orig2012cesarincluded.jpg out2.txt
```

```
Reading 3301orig2012cesarincluded.jpg....
```

```
Extracting usable bits: 29049 bits
```

```
Steg retrieve: seed: 228, len: 535
```

```
→ cicada cat out2.txt
```

```
Here is a book code. To find the book, and more information, go to http://www.reddit.com/r/a2e7j6ic78h0j/
```

1:20

2:3

3:5

4:20

5:5

6:53

Puzzle #1 - The sub Reddit


A2E7J6IC78H0J
hot
new
rising
controversial
top
gilded
Want to join? [Log in](#) or [sign up](#) in seconds. | [English](#)

Welcome to Reddit.

Come for the cats, stay for the empathy.

BECOME A REDDITOR

and start exploring.



search

username

password

☐ remember me [reset password](#)

login

Submissions restricted

Only approved users may post in this community.



Get an ad-free experience with special benefits, and directly support Reddit.

Get Reddit Premium

a2e7j6ic78h0j

join 1,341 readers

6 users here now

a2e7j6ic78h0j7eiejd0120

Verify: 7A35090F

created by [CageThrottleUs](#)

a community for 7 years

MODERATORS

message the moderators

Pixelated_Fudge

[about moderation team »](#)

source**toad**

Puzzle #1 - The sub Reddit

- 2 image posts
- Too many lines of gibberish
- No comments. No descriptions.
- Just titles.
- The puzzle continues...

Puzzle #1 - Image 1 - Reddit



Puzzle #1 - Image 2 - Reddit



Puzzle #1 - Outguess time

```
→ cicada cat welcome.txt
```

```
-----BEGIN PGP SIGNED MESSAGE-----
```

```
Hash: SHA1
```

- From here on out, we will cryptographically sign all messages with this key.

It is available on the mit keyserver. Key ID 7A35090F, as posted in a2e7j6ic78h0j.

Patience is a virtue.

Good luck.

```
3301
```

```
-----BEGIN PGP SIGNATURE-----
```

```
Version: GnuPG v1.4.11 (GNU/Linux)
```

```
iQIcBAEBAgAGBQJJPBRz7AAoJEBgfAeV6NQkP1UIQALFc08DyZkecTK5pAIcGez7k  
ewjGBoCfjf02NlRR0uQm5CteXiH3Te5G+5ebsdRmGWVcah8QzN4UjxpKcTQRPB9e  
/ehVI5BiBJq8Gl0naSRZpzsYobwKH6Jy6haAr3kPFK1l0XXyHSiNnQbydGw9BFRI  
fSr//DY86BUILE8sGJR6FA8Vzjiifcv6mmXkk3ICrT8z0qY7m/wF0YjgiSohvYpg  
x5biG6TBwxfmXQ0aITd05r08+4mtLnP//qN7E9zjTYj4Z4gBhdf6hPSu0qjh1s+6  
/C6IehRChpx8gwpdhIlNf1coz/ZiggPiqdj75Tyqg88lEr66fVVB2d7PG0bSyYSp  
HJl8llrt8Gnk1UaZUS6/eCjnBniV/BLfZPVD2VFKH2VvvtY8sL+S8hCxsuLCjydh  
skpshcjMVV9xPIEYzwSEaqBq0ZMdNFEPxJzC0XISlWSfxR0m85r3NYvbrx9lwVbP  
mUpLKF8ZcMbf7UX18frg0tUjmqQUvDQ2dQhmCUywPdtSKHFLc1xIqdrnRWUS3CD  
eejUzGYDB5lSflujTjLPgGvtlCBW5ap00cfIHUZPOzmJWoEzgFgdNc9iIkcUulke  
e2WbYwCCuwSlLsdQRMA//PJN+a1h2ZMSzzMbZsr/YXQDUWvEaYI8MckmXEkZmDoA  
RL0xkbHEFVGBmoMPVzeC
```

```
=fRcg
```

```
-----END PGP SIGNATURE-----
```

```
→ cicada █
```

Puzzle #1 - Outguess time

```
→ cicada cat problems.txt
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

The key has always been right in front of your eyes.

This isn't the quest for the Holy Grail. Stop making it more difficult than it is.

Good luck.

```
3301
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)
```

```
iQIcBAEBAGAGBQJPCBl3AAoJEBgfAeV6NQkPo6EQAkghp7ZKYxmsYM96iNQu5GZV
fbjUHsEL164ZLctGkgZx2H1HyYFEc6FGvcfzqs43vV/IzN4mK0SMY2qFPfjuG2JJ
tv3x2QfHMM3M2+dwX30bUD12UorMZNrLo8HjTpanYD9hL8WglbSIBJhnLE5CPUS
BZRSx0yh1U+wbnlTQBxQI0xLkPIz+xCMBwSKl5BaCb006z43/HJt7NwynqWXJmVV
KScmkpFC3ISEBcYKhHHWv1IPQnFqMdW4dExXdRqWuwCshXpGXwDo0XfKVp5NW7Ix
9kCyfC7XC4iWxymGgd+/h4ccFFVm+WW0cz0q/zeME+0vJhJqvj+fN2MZtvckpZbc
CMfLjn1z4w4d7mkbEpVjgVIU8/+KClnFPSf4asqjBKdrcCEMA180vZorElG60VIH
aLV4XwqiSu0LEF1ESCqbxkEmqp7U7CHl2VW6qv0h0Gxy+/UT0W1NoLJTzLBFiOzy
QIqqpgVg0dAFs74SlIf3oUTxt6IUpQX5+uo8kszMHTJQRP7K22/A3cc/VS/2Ydg4
o60fN54Wcq+8IMZxEx+vxtmRJCUR0VpHTTQ5unmyG9zQATxn8byD9Us070FAg6/v
jGjo1VVUxn6HX9HKxdx4wYGMP5grmD8k4jQdF1Z7GtbcqzDsXP65XCa0Ymray1Jy
FG50lgFyOfImjBXHsNad
=SqLP
-----END PGP SIGNATURE-----
→ cicada █
```

Puzzle #1 - The Sidebar

- Reddit Sidebar
- What is that?
- Longer version of subreddit name

a2e7j6ic78h0j

join 1,352 readers

4 users here now



a2e7j6ic78h0j7eiej0120

Verify: 7A35090F

















Puzzle #1 - The Header

- Reddit Header
- What is that?



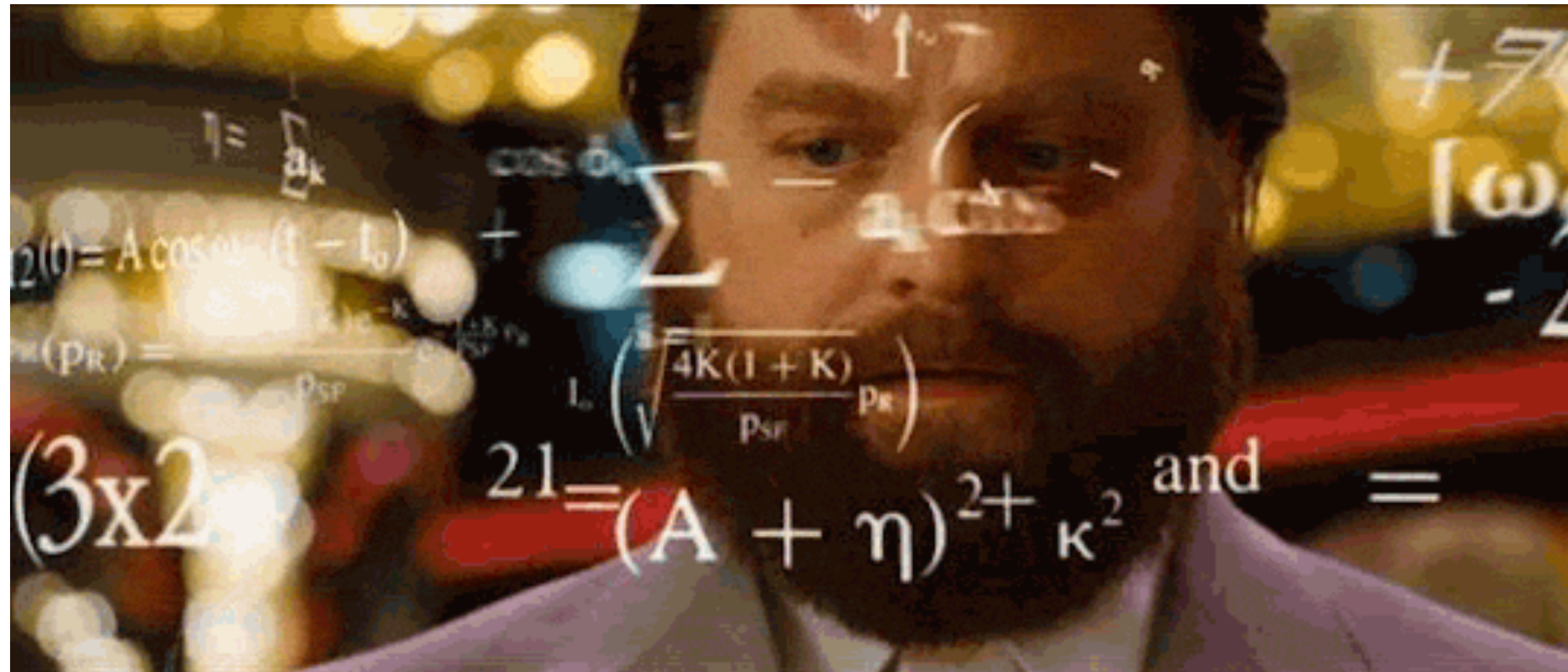
Puzzle #1 - The Mayans

- Mayan Numbering
- There is our key :)
- So decode header

0	1	2	3	4
	•	••	•••	••••
5	6	7	8	9
				
10	11	12	13	14
				
15	16	17	18	19
				

Puzzle #1 - The Number

- 10 2 14 7 19 6 18 12 7 8 17 0 19 7 14 18 14 19 13 0 1 2 0



Puzzle #1 - The Number Serious

- 10 2 14 7 19 6 18 12 7 8 17 0 19 7 14 18 14 19 13 0 1 2 0
- Pattern of this puzzle has been shifts/rotates
- djsl aoltlz? Nhta snwe uawg I nqbl mu ltlm, khta hzcn fhpwlnuh hvz
- Shift backwards...
- d = shift 10 = t
- j = shift 2 = h
- s = shift 14 = e
- l = shift 7 = e

We spelled "THEE"

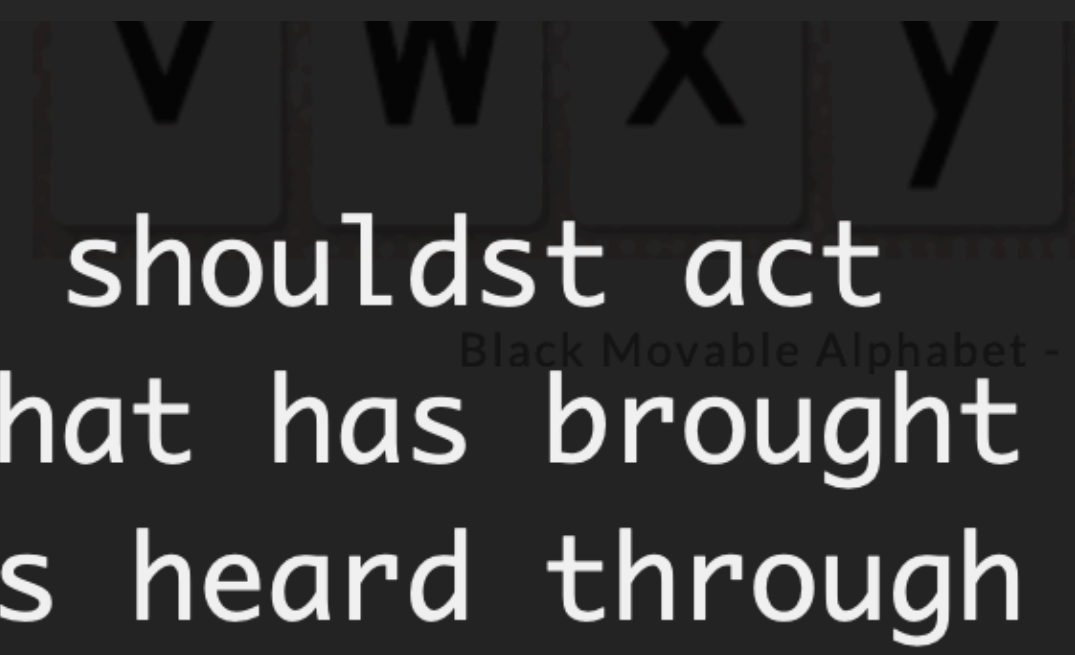
Puzzle #1 - The Batch

- We aren't savages. Let's script this.

-

→ **BarCamp2019** `./decipher < reddit.txt`

thee hither? What evil have I done to thee, that thou shouldst act
the valley, approaching me and saying, 'Oh, Knight, what has brought
with listening to the birds, lo, a murmuring voice was heard through



Puzzle #1 - The Story

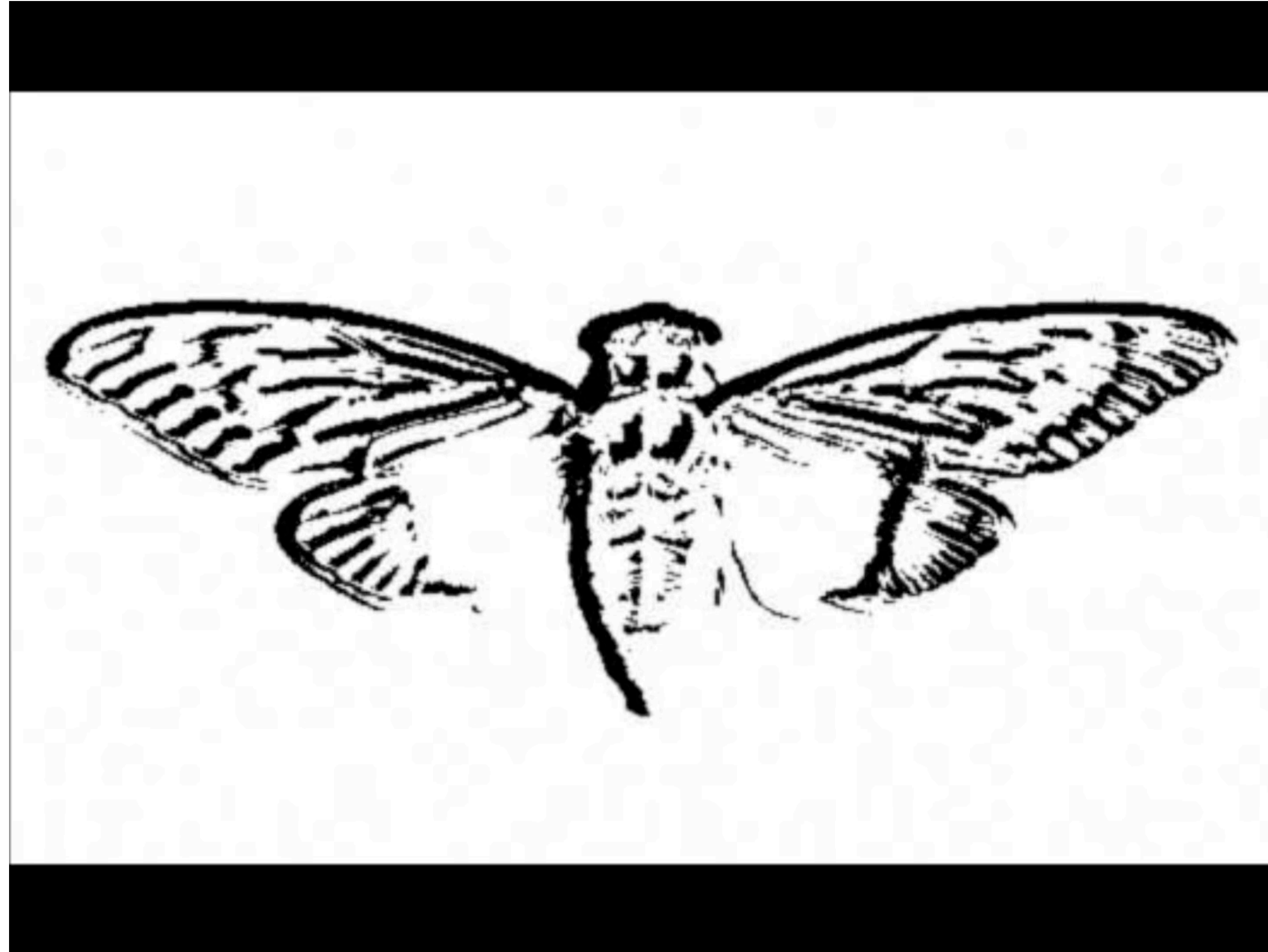
- Story about King Arthur
- We had a book!
- Our book code is useful!
- Line 2, character 20.
- Line 3, character 11...etc

Puzzle #1 - The Message

- Call us at us tele phone numBer two one four three nine oh nine six oh eight
- WOW.
- Into the phone world we go.

Puzzle #1 - The Recording

- Video



Puzzle #1 - Backup: Audio

- Very good. You have done well.

There are **three** prime numbers associated with the original *final.jpg* image. **3301** is one of them.


You will have to **find** the other two.

Multiply all three of these numbers together and add a .com to find the next step.

Good luck. Goodbye.

Puzzle #1 - Prime Hunt

- Take the original image from 4chan
- 509px by 503px (both prime)
- $3301 \times 509 \times 503 = ??$
- **845145127.com**



Hello. We are looking for highly intelligent individuals. To find them, we have devised a test.

There is a message hidden in this image.

Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through.

Good luck.

3301

Puzzle #1 - The Website

- Countdown first
- Then lat/long
- Embedded in image



Find our symbol at the location nearest you:

52.216802,	21.018334
48.85057059876962,	2.406892329454422
48.85030144151387,	2.407538741827011
47.664196,	-122.313301
47.637520,	-122.346277
47.622993,	-122.312576
37.577070,	126.813122

Puzzle #1 - The Locations

- Chino, California
- Erskineville, Australia
- Fayetteville, Arkansas
- Haleiwa, Hawaii
- Miami, Florida
- New Orleans, Louisiana
- Paris, France (2)
- Seattle, Washington (3)
- Seoul, South Korea
- Warsaw, Poland

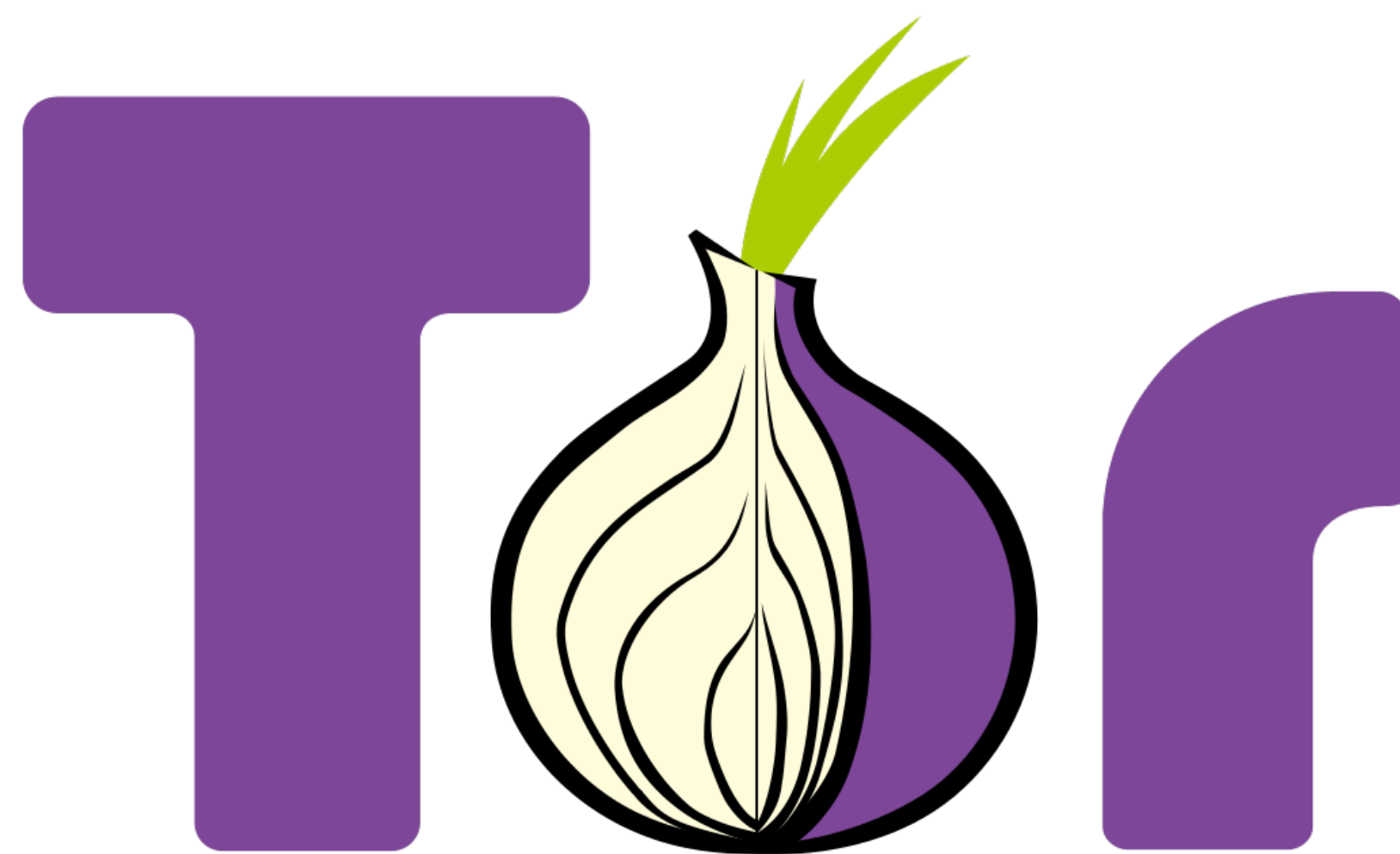
Puzzle #1 - Real World

- Find the lat/long
- Find the symbol
- Scan the QR



Puzzle #1 - The Onion

- TOR Browser Required
- This story gets unverified.
- Private tests with Cicada



Puzzle #1 - Ended

- Released on the subreddit
- End of the 2012 Puzzle
- Started a movement

Hello.

We have now found the individuals we sought.
Thus our month-long journey ends.

For now.

Thank you for your dedication and effort. If you
were unable to complete the test, or did not receive
an email, do not despair.

There will be more opportunities like this one.

Thank you all.

3301

P.S. 1041279065891998535982789873959431895640\
442510695567564373922695237268242385295908173\
9834390370374475764863415203423499357108713631

Puzzle #2 - Began

- January 5, 2013
- Released on subreddit

Hello again. Our search for intelligent individuals now continues.

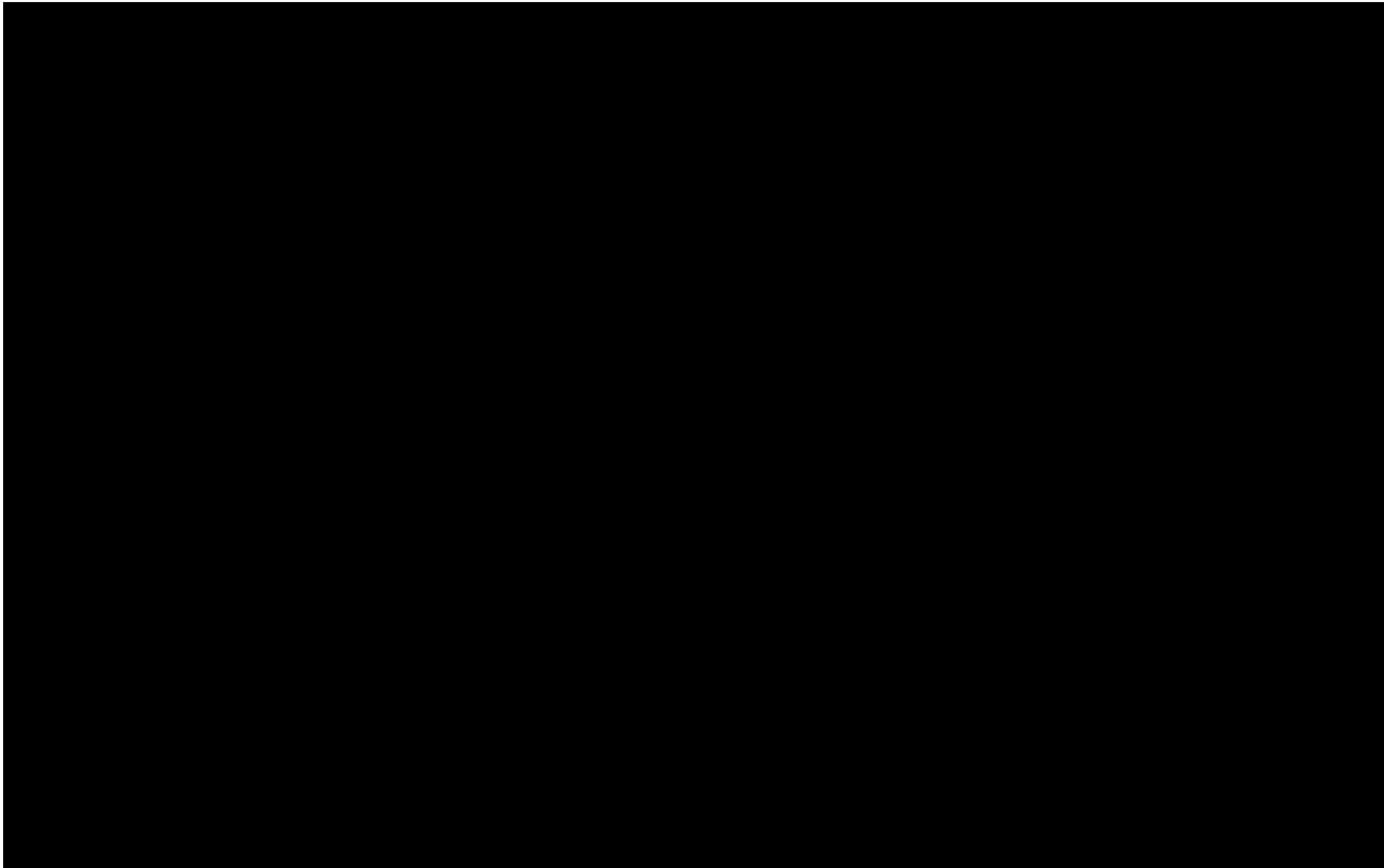
The first clue is hidden within this image.

Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through.

Good luck.

3301

Puzzle #2 - ISO

- Riddle, Book Code, Book
 - Led to a dropbox file.
 - File was an ISO
 - Strange boot
 - Random files
- 

Puzzle #2 - The Song

- The Instar Emergence
- 167 seconds
- 761.mp3



Puzzle #2 - ISO Ending

- OS Boot ended w/ message

- @1231507051321

The key is all around you.

Good luck.

3301



Puzzle #2 - Tweets

- Each tweet, offset and data
- File is gibberish - useless
- XOR this with 761.mp3 from ISO.

```
0000000: b69ccce300104a464802545959580001008d0000ff8b6131616a6a632737293d3e322b3b3e3
0000041: 404a727b0843460c44595114476a555f5c5b57604064511292ae7337217a616c682b636d7f2
0000082: 5a5712565b445b5c5b464b12455b465a5b5c12535c5612575f5740559aee54585c314a02561
00000c3: 0000000501020337363636f7f2ba6fffc400b5100002010303020403050504040000017d010
0000104: 57d6fa283c736695101608363b3f320e08171b1c120e0876757d7e700f0b141210111514323
0000145: 23273a21262c2f2b575a5c5d686f6b7772707175745350525c5d59484a4f3a3839c5c6c7f18
0000186: f8c4c8e1e50c2cae000301010101010101010100000000000000102030405060708090a0bffc
00001c7: 31061241510761711322328108144291a1b1c109233352f0156272d10a162434e125f117181
```

Puzzle #2 - The Image

- Lead to an alphabet
- Runes (?)
- Plays an important part.
- Can you outguess this?

Gematria Primus					
an order and a value as revealed through 3301					
Rune	Letter	Value	Rune	Letter	Value
ƒ	F	2	ᚱ	S/Z	53
ᚢ	U	3	ᚦ	T	59
ᚦ	TH	5	ᚷ	B	61
ƒ	O	7	ᚱ	E	67
ᚱ	R	11	ᚱ	M	71
ᚠ	C/K	13	ᚦ	L	73
ᚨ	G	17	ᚨ	NG/ING	79
ᚦ	W	19	ᚨ	OE	83
ᚱ	H	23	ᚱ	D	89
ᚦ	N	29	ᚦ	A	97
ᚠ	I	31	ᚦ	AE	101
ᚦ	J	37	ᚢ	Y	103
ᚦ	EO	41	ᚨ	IA/IO	107
ᚠ	P	43	ᚦ	EA	109
ᚦ	X	47			



Puzzle #2 - The Image

- A new image
- Blank (?)
- Tabs vs Spaces

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.11 (GNU/Linux)

iQIcBAEBAgAGBQJQ5lDTAAoJEBgfAeV6NQkP7nMQAJVg7DQilA7NpkacR0RA4eBs
NZHJBQNHO2P22h+aFfP/r11gjGaV3hMWaa2sQ4Vbi/W8eZuH40AsmZUy3EOb+4j0
3cJRJgAJI99ZjDcVXI7m5VyUv+WlqCzBr+bHMK7pkMYQ/rEzeWD56tIsrDgFdimh
PA/b7XrDcofd9JfBNFI7D/sF84HL2ig5baNo+MGjYl4Dq2cHX+SAafXmIN9PXFjx
HRBbuoMLlviKywQ8MnePBPYG6V8sIMmrJIHS5ZcNEaSJ9nGL4X0XbECqV79ermye
1EeNKcckoeZMU86SabfMeyZozG04Vkbemn8JH5cssbuF8hf4fdN/LSP4NG0r5y9
jfRv7z59pL577ZpGAju5zBtCBUvmxxNYR5lGLg+Fi/ICqcRC98mzesFnQ7wbDLS
HKyV95SBQK82bbqSREBflrrNb+MjVtJwlvOY5OPTBViHPqrluMw8KDGfSvw9ncCt
dase7vUjXxlrn36xDSRN6cMzTmFZ9lkQYkRAYq5ApERud+JfKCwszG/UxRwo1WOU
0ALaWXq5VMp+w5pvQkqg9eHpOriG9Z11VLdb53eTmxKrwYX/2eaiybsnMrRNuxv1
iE8PVRkifCcJccw1bGq8TyCQF3a5ozeiBRngAUT7BwZhLa4bShtki7amR0ZZgbKk
8JRMGvoSA5NNTEwvUhwI
=ZeNf
-----END PGP SIGNATURE-----

Puzzle #2 - Another Onion

"Come to emiwp4muu2ktwknf.onion"

"We shall await you there."

"Good luck."

"3301"

Web browsers are useless here.

```

      ,+++77777++=:,
      7~?7      +7I77 : ,I777 I
=7I7I~7      ,77: ++:~+7 77=7777 7
77+7I 777~,,=7~      ,::7=7: 7 77
= 7 ?7 , 7~,~ + 77 ?: :?777 +~77 77? I7777I7I7 777+77
77 ~I == ~77= +777 777~: I,+77? 7 7:~?7? ?7 7 7 77 ~I 7I,,?7 I77~
I 7=77~+77+?= :I+~77? , I 7? 77 7 777~ +7 I+?7 +7~?777,77I
=77 77= +7 7777 ,7 7?7:,??7 +7 7 77??+ 7777,
      =I, I 7+:77?
      7I7I?77 ~
      ,7~77?7? ?:
      ?77 +I7+,7
      I777=7777 ~
      + ~?
      +=
      77 7+77 7:
      +77=7 =7I7
      ,I777= 77,:~7 +?7, ~7 ~ 777?
      ,?777777??~,+=~I7?,=77 I
      ,I777= 77,:~7 +?7, ~7 ~ 777?
      =:,77,77 77 7,777,
      =:, ?7 +7 777?
      7I,,?7 I77~
      , I 7? 77 7 777~ +7 I+?7 +7~?777,77I
      ,7 7?7:,??7 +7 7 77??+ 7777,
      +7I7?7777 :
      +7:77, ~
      7+:77777,
      7~ 7,+7 ,?
      77 : 77 =7+, I77 777
      , + 7 , , ~I, = ? ,
      77:I+
      ,7
      :77
      :

```

Welcome.

Puzzle #2 - Telnet

- Telnet to the onion.
- Tons of commands - *hello/count/quit/#*
- “*hello*” dumped out another file

```
hello
A message for you:
```

```
0000000:2d2d2d2d2d424547494e20504750205349474e4544204d45535341147452d2d2d2d2d0a486173683
0000041:20200a596f75206861766520646f6e652077656c6c20746f20636f6d652074686973206661722e0
0000082:0a20200a476f6f64206c75636b2e0a2020200a333330310a2020202020200a2d2d2d2d2d424547494
00000c3:6f6e3a20476e7550472076312e342e31312028474e552f4c696e7578290a0a69514963424145424
0000104:6b502f4a3051414c44716133564a7939784c4c6c6749356a5068524970340a66786562624e68744
0000145:4d536e636949593035394b4969354e53545637493937734a626f473377740a6b6848745a674e527
0000186:6d456c784f427a57723638646c5159743271664251786b327a522f6654490a544c43454776465a7
00001c7:5039764f45586c42312b506d30433775505042504e3761716b665550476c0a6f3166326873634a6
0000208:414e41642f557046567a542f3835325867363367745a72492b536d66335a0a4256636a70437a794
0000249:51476d584c325358424234337a565a414a716c355564584c5447586b62640a6e504d64332f43624
000028a:3277484b4c4f76666a5176455758495931434d68493638426a30725a6f2f0a4d2f6669333133464
00002cb:6e45385878685273793734415a35477141326f484d6566544171335975570a35505838733638324
000030c:414c4a4762777a366d7461754251716c53364152735166656b446e336f5a0a796f73532b6757433
000034d:35635439526e367058324e564e585378677a585842346e493258727259610a346b5172356157423
000038e:2f554633515437354d6978514d75344d2b3577436e4e656b676675794f360a5a7679627a7034733
00003cf:4420504750205349474e41545552452d2d2d2d2d0a
Offset: 3201 Skip: 0 Col: 65 Line: 16
```


Puzzle #2 - Another Onion

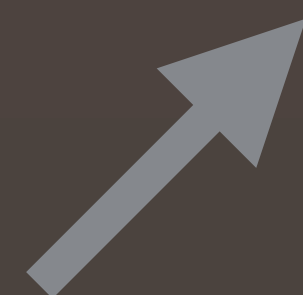
- Read file - points to another.

```
<html>
  <head><title>3301</title></head>
  <body>
    Patience is a virtue.
    <!-- which means, come back soon. -->
  </body>
</html>
```

Puzzle #2 - Waiting Over

- Tron?
- No, a Zen proverb
- Knock = ping?

You already have everything you need to continue.
Sometimes one must "knock on the sky and listen to the sound."
Good luck.



Puzzle #2 - Ping Pong Data

- Each ping returned data
- Slowly build a file

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1
```

```
Well done.  You have come far.
```

```
pklmx2eeh6fjt7zf.onion
```

```
Good luck.
```

```
3301
```

```
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.4.11 (GNU/Linux)
```

```
iQIcBAEBAGAGBQJQ7vVDAAoJEBgfAeV6NQkP9x4P/31A5LPzIhkii8sBjuVxIcOn  
4KFQO+uVVSR53zImSqlhq6iVAE9+Ko7vIqjD2whTIUFVYZNBq/92wEZJuCSonovH  
HqYZTQihIS9d+QDuwUNvXr4ilrRmITKMrWw3D23rpWs6ZlnehuUDVI8unbN9Zi3h  
3hvok3/+FofLia9Kvbo+FIDi7T9NNRpgpgXd/6dQIP4kn63kKCP20QMdrf2fXF  
ZLx5ADS14OvaNFNUAHTJlqdkPYcdTiNDJkxqk1s82y2doGoEP0ChBUJxlyMiUVXn  
1iLOwm2KNrf6If64KxEoetOraWqg9P6l3BjGVPCkrotB608SSs2Lihsa4B0ifI33  
ABlpvSDIgpBu/zIO/WFYOfnnrtdvDpVP/Wy+pgqZJ/wOUuhJZhzi5vppjVCm/q9H  
C/aXQxa+XXe7his4f9tuIBD1wIYAtnE8M0uDCsfizjBaZNMn007/hOwnNQSBAMcr  
KqL5yHSnpI50CtoA+6ycWZURBkrt1rt4eNxsCqQ1XWed/hWbqb6SlJJemJOPbbmt  
V5D7iDUO+r2OIUEZTfCSjdZrXcJ8FLtqCGVaLJhCdsyirRHmURwkYLw/B8TpcJQz  
qbY6oeDxDosIbE6uhDNV2RVKmpWqLDMhLGHVjkDjJpode5L3ObbylWuRnHfFqfKH  
lmubvMAGo03rxxlY+9XG  
=6Sgs  
-----END PGP SIGNATURE-----
```

Puzzle #2 - The Locations

- Annapolis, Maryland
- Columbus, Georgia
- Dallas, Texas
- Little Rock, Arkansas
- Moscow, Russia
- Okinawa, Japan
- Portland, Oregon



Puzzle #2 - Calling Again

- Call number on poster. It asks for code.
- Enter code “L (5) M (6)” and **failed**.
- Lets look at the Primus
 - L - 73
 - M - 71
- Password **Accepted**.

Gematria Primus					
an order and a value as revealed through 3301					
Runo	Letter	Value	Runo	Letter	Value
ƿ	F	2	ᚠ	S/Z	53
ᚢ	U	3	ᚦ	T	59
ᚦ	TH	5	ᚧ	B	61
ƿ	O	7	ᚩ	E	67
ᚱ	R	11	ᚪ	M	71
ᚲ	C/K	13	ᚫ	L	73
ᚨ	G	17	ᚨ	NG/ING	79
ᚦ	W	19	ᚦ	OE	83
ᚱ	H	23	ᚪ	D	89
ᚦ	N	29	ᚦ	A	97
ᚫ	I	31	ᚦ	AE	101
ᚦ	J	37	ᚢ	Y	103
ᚦ	EO	41	ᚨ	IA/IO	107
ᚱ	P	43	ᚦ	EA	109
ᚦ	X	47			

Puzzle #2 - Onion Hunt

- Dataset 13? - From the ISO
- XOR it again. Another onion....

Dataset:13
Offset:12821

Data:28C07E1B102D4D5C4C1A376E064477E1416FCC94928765

Puzzle #2 - SSSS

- 02-41cc481a51fe77f91600f593c1db2ce9babd2626ea6e
- 03-7678a5f6b72042d839151b34b02ffe161cf997fed484
- 05-fcd82965b6632ea25d80edc3e58baafb4b2938895cbd
- 08-b970e507dbc4ac115a273126f62671654c480fce32e5
- 09-82a98a7fe06014f783b752506cf6cd1fabaa3d8b3750
- 10-1668a611ba9fccdde2a0d8fd7e05df4d01c6d42a26d

Output from the **SSSS-COMBINE** invocation:

```
p7amjopgric7dfdi.onion
```

Puzzle #2 - The Test

- 20 Questions. 5 Minutes.
- No retry.

Question:

You cannot step into the same river twice.

Answer:

- ☐ True
- ☐ False
- ☐ Indeterminate
- ☐ Meaningless
- ☐ Self-Referential
- ☐ Game Rule
- ☐ Strange Loop
- ☐ None of the Above

Post Answer

01 min and 58 sec

Question:

Two people are standing by a lake. One says, "that's a lovely reflection in the water." The other says "I see no reflection, but it's a fascinating assortment of fish, plants, and rocks within the water."

Which one is lying?

Answer:

- ☐ The person who sees the reflection
- ☐ The person who sees the fish
- ☐ Both
- ☐ Neither

Post Answer

01 min and 56 sec

Puzzle #2 - Goes Unverified

- Email sent to solvers
- Cookies set
- Goal: Build a TCP Server in any language
 - Respond to this protocol
- Deadline: Feb 3, 2013

```
2013/02/25 14:32:01 server is running under address [::]:3307
2013/03/03 10:57:48 got connection from 127.0.0.1:42483
2013/03/03 10:58:05 executing 'rand 3' for 127.0.0.1:42483
2013/03/03 10:58:09 executing 'rand 3' for 127.0.0.1:42483
2013/03/03 10:58:18 executing 'rand 0' for 127.0.0.1:42483
2013/03/03 10:58:29 executing 'rand 1' for 127.0.0.1:42483
2013/03/03 10:58:56 executing 'quine' for 127.0.0.1:42483
2013/03/03 10:59:10 executing 'base29 1033' for 127.0.0.1:42483
2013/03/03 10:59:14 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:16 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:18 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:21 executing 'koan' for 127.0.0.1:42483
2013/03/03 10:59:28 executing 'dh 3301' for 127.0.0.1:42483
2013/03/03 10:59:56 executing 'dh 3301' for 127.0.0.1:42483
2013/03/03 11:00:29 executing 'dh 3301' for 127.0.0.1:42483
2013/03/03 11:00:58 executing 'next' for 127.0.0.1:42483
2013/03/03 11:01:11 executing 'dh' for 127.0.0.1:42483
2013/03/03 11:01:18 executing 'goodbye' for 127.0.0.1:42483
2013/03/03 11:01:18 closing connection to 127.0.0.1:42483
```

Puzzle #3 - Began

- January 6, 2014
- Tweeted

Hello.

Epiphany is upon you. Your pilgrimage has begun. Enlightenment awaits.

Good luck.

3301

Puzzle #3 - A Book Code

- Paragraph
- Sentence
- Word
- Letter

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

The work of a private man
who wished to transcend,
He trusted himself,
to produce from within.

1:2:3:1
3:3:13:5
45:5:2:3
20:3:20:5
8:3:8:6
48:5:14:2
21:13:4:1
25:1:7:4
15:9:3:4
1:1:16:3
4:3:3:1
8:3:26:4
47:3:3:5
3
13:2:5:4
1:4:16:4

.
o
n
i
o
n

Good luck.

3301

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

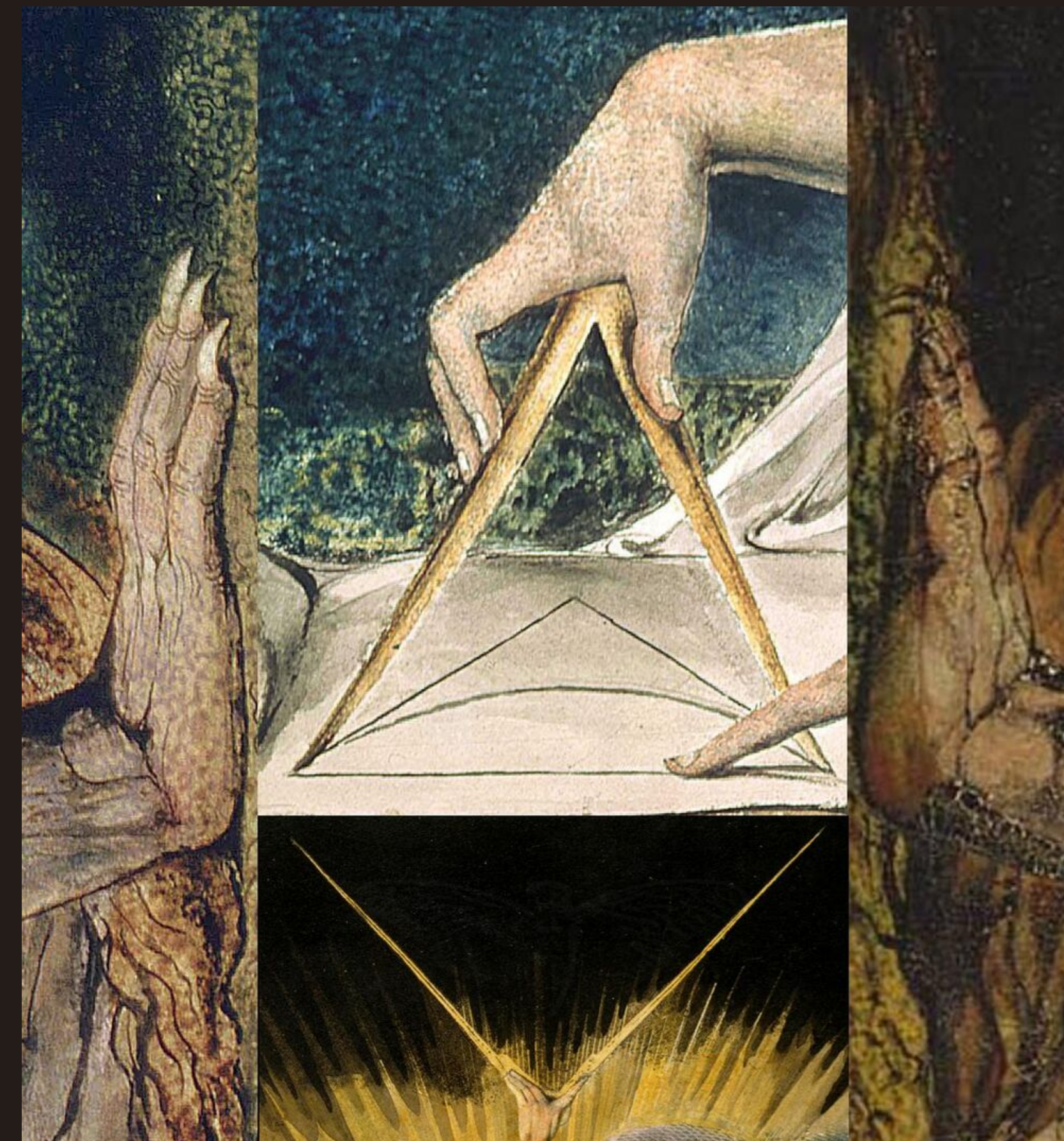
Puzzle #3 - Another Image

- Outguess again.
- An RSA Key


```
e = 65537
n = 75579125746085351644267182920580212556413102071876330957950694457000592\
10248050757270234679993673844203148013173091173786572116639

- -----BEGIN COMPRESSED RSA ENCRYPTED MESSAGE-----
Version: 1.99
Scheme: Crypt::RSA::ES::OAEP

eJwBswBM/zEwADE2MgBDeXBoZXJ0ZXh0LE2jxJS1EzMc80kOK+hra1GKnXgQKQgVitIy8NgA7kxn
2u8jNQDvlu0uymNNiu6XVCCn66axGH0IZ9w4Af3K/yRgjObsfAlQ7QqpXNALJ9FFPgYl5rh07cBP
M9kbSH6DynU/5cYgQod2KymjWcIvKx3FkjV4UOGakDnBfleQpluwvn3KxDVwTyzPqbMnZvOA06Ec
AfKtyzlhEK/UBXkeMeVrnV5SQQ==
=yTUshDMKN65aPaKAR0OU8g==
- -----END COMPRESSED RSA ENCRYPTED MESSAGE-----
```



Puzzle #3 - RSA Catch Up

- Given **e** & **n**
- $N = p * q$ (secret )
- **e** = encryption exponent
- **n** length = 130 digits (430 bits)

Puzzle #3 - RSA Factorization

- 2019 Laptop
- 7h 20min
- Key obtained.

```
ibotpeaches@foundation$ time docker run -it b4den/rsacrack 755791257460853516442671829205802125564131020718763309579506944570005921024805075727023467999367384420314801317309117378657211663
[] pubkey.e: 6553
[] pubkey.n: 755791257460853516442671829205802125564131020718763309579506944570005921024805075727023467999367384420314801317309117378657211663
[] Key looks like 432 bit
[] Using cadonfs to compute prime
[] results are: [u'97513779050322159297664671238670850085661086043266591739338007321', u'77506098606928780021829964781695212837195959082370473820509360759', 65537L
[] Key extraction done
-----BEGIN RSA PRIVATE KEY-----
MIIBDAIBAAI3AK50gkj06lhiMbT/iIsA+l1l517rg0iDK25eRHiXDlGp00NuKFH03U/5YHNaIjM
YqZZ4ilSnwIDAQABAjZtP5cL0xy6RpvPh3y9qTS8mrnHVVH3yZTcI/lwoIubRaCJaifErsBrjIv
e7LQ1fgyRo+c8hECHADtCvLDTZS6NNntQIAKTebM9nwGSpu4imfXoxkCHAC8aCngGxUhK0bNdTn
h4An2V1NmuWt2dhy0ncCGwcXfSAie0KBt851ZR3Jj1gA/Yd59zPLwxw4uAIbNs0R69rhfdX5eVH
4QFynOdXzrhchHs13IjkAhsmGCSA2T0fTd6T+mJ7XHMpxqj9oFdZ93zmJLk=
-----END RSA PRIVATE KEY-----

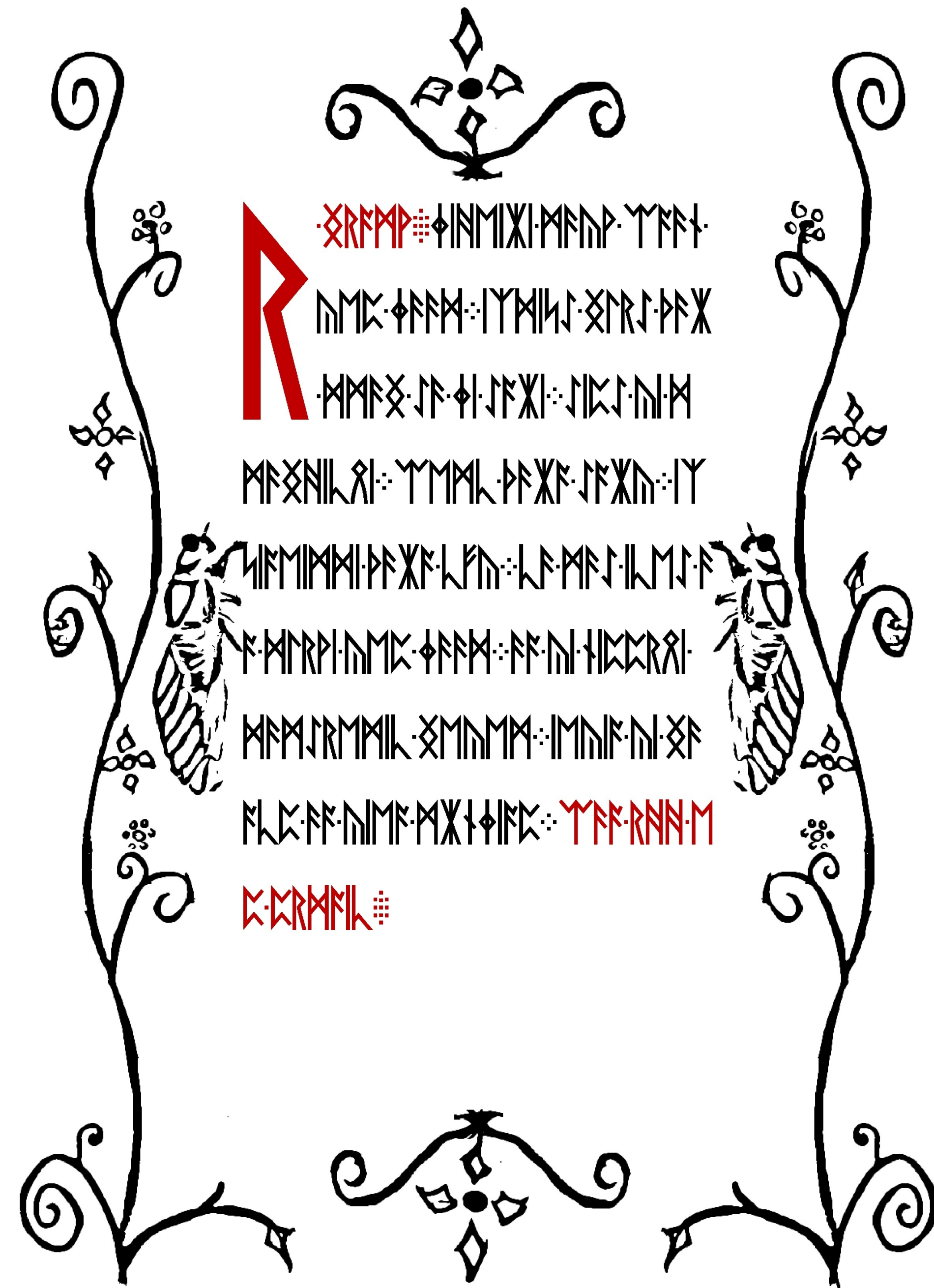
real    717m2.977
user    0m1.752
sys     0m0.245
```


Puzzle #3 - Quick Hits - 1

- Page growing with bytes
- Tons of characters - 3,641,299
- Convert to binary (xxd)
- Flipped bits (perl)
- Detect magic values for JPEG (binwalk)

Puzzle #3 - Quick Hits - 3

- 3 images. A book (?)
- Decode to hexadecimal
- Complicated decode
- Transposition cipher
- Decode to another msg
- Goal: Onion URL

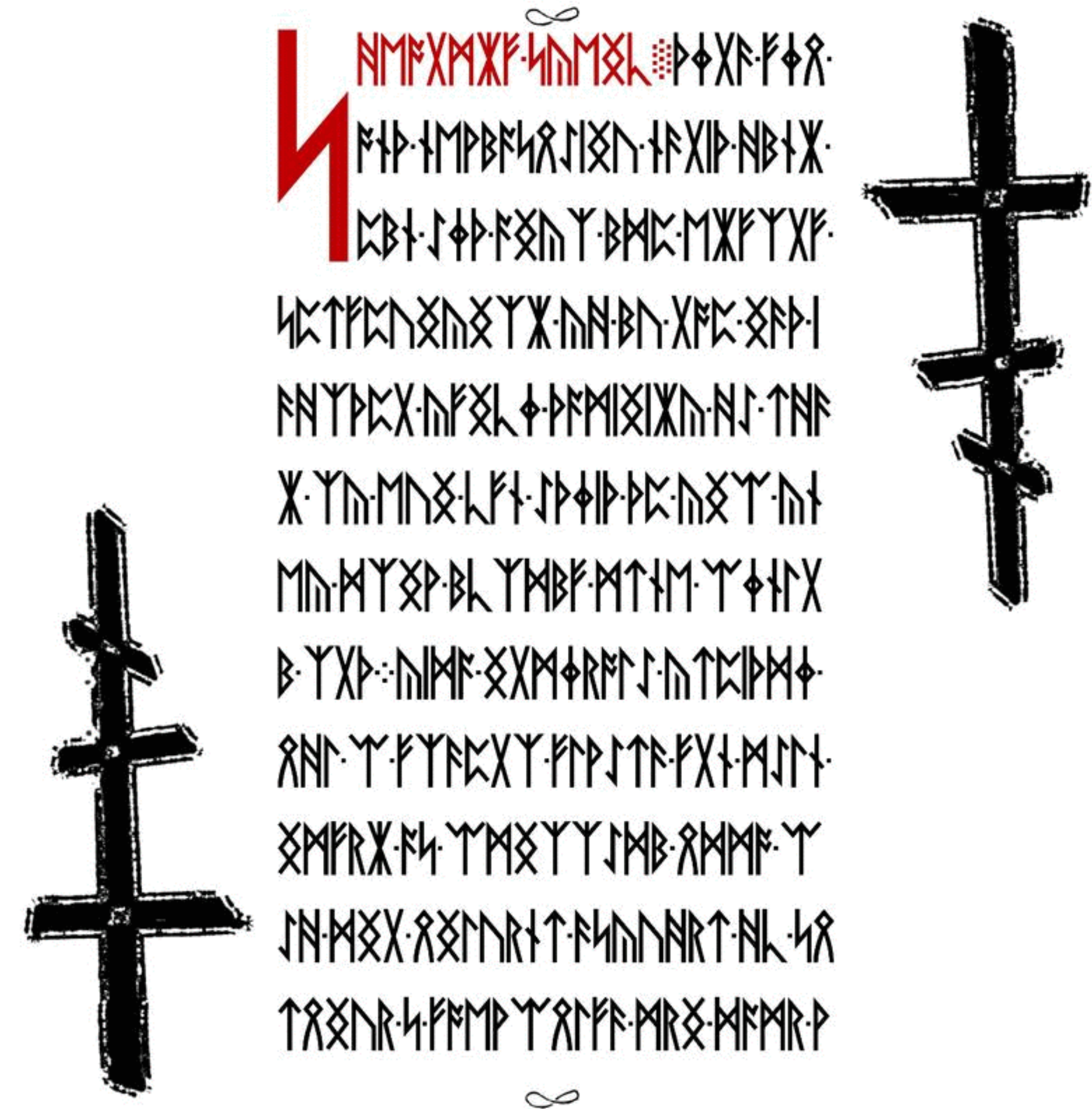


Puzzle #3 - The slowdown

- Progress was tough, or hidden
- Onions started going offline
- Only had a few select pages
- Then May 2, 2014
 - Cicada returned...

Puzzle #3 - Liber Primus

- Released at once
- 76 pages.
- Only 19 solved (public)



Cicada Update - Jan 2016

- Stick to the Book
- No new puzzle

Hello.

The path lies empty; epiphany seeks the devoted.

Liber Primus is the way. Its words are the map, their meaning is the road, and their numbers are the direction.

Seek and you will be found.

Good luck.

3301

Beware false paths. Verify OpenPGP 7A35090F.

Cicada Update - April 2017

- No image
- Verified message.
- *Beware false paths. Always verify PGP signature from 7A35090F.*

"Question all things."

- Cicada 3301

@iBotPeaches
Connor Tumblson
connortumblson.com



source**toad**