Filename: anime.7z
Size: 2.6 MB
Type: 7-zip archive data
MD5: 9bb8ac526d789fc811beba9067b25b64
SHA1: c6f41818db02eb995a1f1acbce5e6a9a63207c92
SHA256: a113ac59d3b1c8856a0afd2dee94be1d7669fcf0bf1f819633a980084cddcc72
First submission to VT: 2018-11-02 03:29:20

Extracted File:

- **Filename:** findme
- **Size:** 2.7 MB
- **Type:** SQLite 3.x database
- **MD5:** ac36baf8bf43fde58498ddc2161b0213
- **SHA1:** 5db2cc25513a3f771f1595b287f151fe15c95aeb
- **SHA256:** a13ba0c4c6b8a8c8eeec06ef3a8b458003577c8f3cfc36d7a2482be68bf08316
- **Header:** *53 51 4C 69 74 65 20 66 6F 72 6D 61 74 20 33 00* (16 bytes, SQLite)

Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Create Table | Create Index | Modify Table | Delete Table

Name	Type	Schema
Tables (3)		
Files		CREATE TABLE `Files` (`Uploads` BLOB NOT NULL)
Uploads	BLOB	`Uploads` BLOB NOT NULL
Users		CREATE TABLE `Users` (`Name` TEXT NOT NULL, `Email Address` TEXT NOT NULL, `Password` TEXT NOT NULL)
Name	TEXT	`Name` TEXT NOT NULL
Email Address	TEXT	`Email Address` TEXT NOT NULL
Password	TEXT	`Password` TEXT NOT NULL
admin_area		CREATE TABLE "admin_area" (`флаги` TEXT)
флаги	TEXT	`флаги` TEXT
Indices (0)		
Views (0)		
Triggers (0)		

Database Structure

Database Structure | Browse Data | Edit Pragmas | Execute SQL

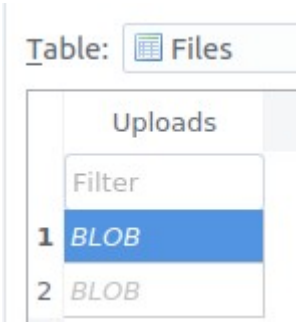
Table: Users | New Record | Delete Record

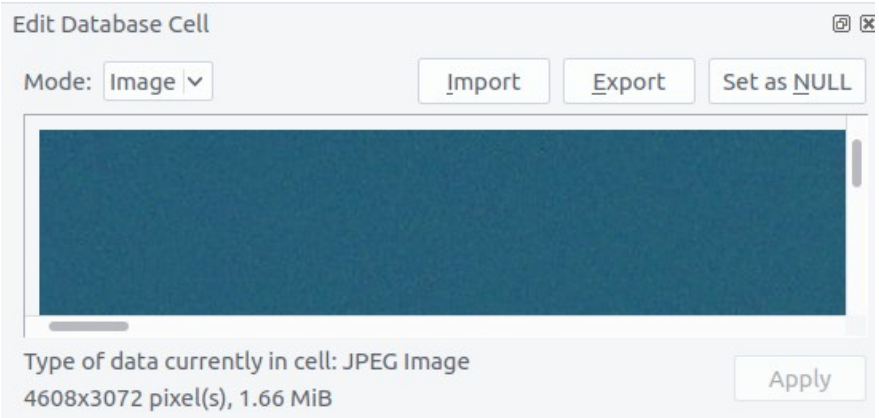
	Name	Email Address	Password
	Filter	Filter	Filter
1	Margaret Russell	redacted	/-K7Dx[z8c
2	Sam Murach	redacted	`UR3"LS
3	Laura	redacted	Eme(of3
4	Arch Cummings	redacted	@sqve:{L
5	Bill Sullivan	redacted	BT3b/Z
6	John Russell, Sr.	redacted	yellow-red
7	Hanna Schiller	redacted	brown-orange
8	Joseph Palmi	redacted	m0lly$
9	John Russell, Jr.	redacted	uti5Ekyv
10	Edward Wilson	redacted	%saumyb1m/%$

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: admin_area | New Record | Delete Record

	флаги
	Filter
1	forwards == backwards
2	it's all in the past
3	sometimes gifs taste better with hash, tumble dry
4	steam dry, hmmmm pastie





Exported Image:

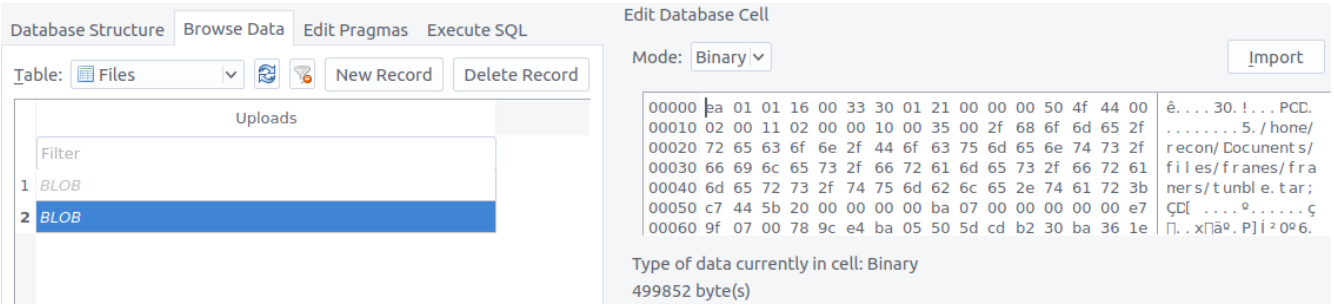
EXIF Data

- *File Type: JPEG*
- *File Type Extension: jpg*
- *MIME Type: image/jpeg*
- *Processing Software:* ***pyExifToolGui 0.5***
- *Copyright:* ***reconctf2018***
- ***ELA (Error Level Analysis)* Max difference: 17 *!!! (Possible Steganography)***

Difference hashing	349b93f586a6f1cf
Average hashing	00005910777f3f2f

Perception hashing 80781bd4368ae7f9

Second File



MD5: 12f895c210b4772b7811d088df64a142
SHA1: 15dc5b6b8cc424e907907c4bc6c2d760de5b8e82
SHA256: 1fa1f3e9b4fcb940323545925611de3b2f178e383a19a70df8b5b94b63c90eb3
Size: 489K
First Submission to VT: 2018-11-02 06:24:53
Type: Data (File Magic Fails Us)
TrID: PEA compressed archive (v1.x)*

- * Requires PeaZip to extract

Extracted File

Filename: tumble.tar
MD5: 6b92a7b4e8c185275cd2e96da1755a19
SHA1: a9a860683cbeff1317c70e82053ca5ab4265d5d3
SHA256: e92dbdcf88b9493d8005dae89a6ccdf41511479eb9625b5d14d2533ca3d353dc
Size: 495K

Extracted File(s)

Filename: recon.jpg
MD5: 41ae8937a9529905db209e486c06f9fd
SHA1: e0663d48ace1c8cba05098db00dc7cea6e67a94f
SHA256: 5d78a3055aa3d37311b2e485e2759083ba484158e3944243761102a9e1c160d7
First Submission to VT: 2018-11-04 22:28:21
Size: 18K

Filename: tumble.gif
MD5: 495695b3b9dc7949ac972687d0b9ee84
SHA1: 4c2bc05657fd0426c54133573ced12324958b3e4
SHA256: e0d5b477844fbc50b35b3efb9e87c5aeb0df8eaa424916ab1562a12954d9fec8

First Submission to VT: 2018-11-04 22:08:27
Size: 474K

recon.jpg

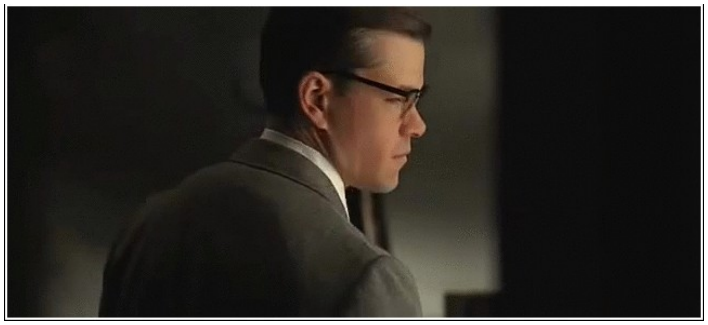
EXIF Data:

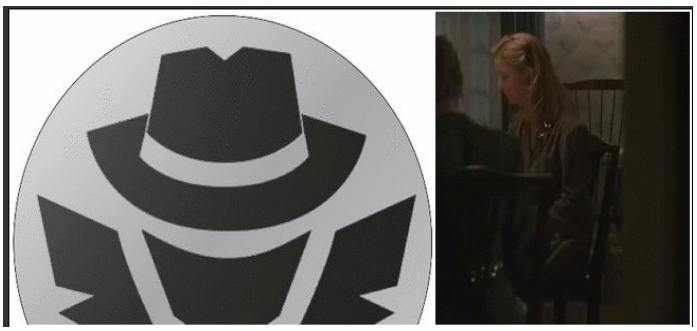
- *File Type: JPEG*
- *File Type Extension: jpg*
- *MIME Type: image/jpeg*
- *Processing Software:* ***pyExifToolGui 0.5***
- *Artist:* ***sparkly - sheep – chaos***

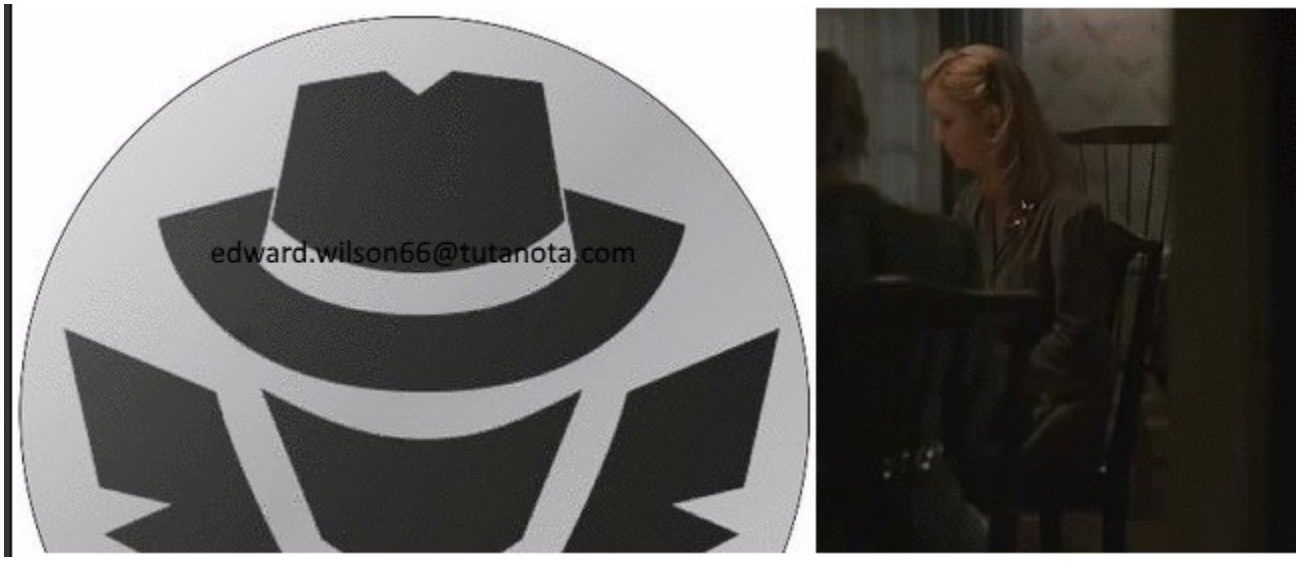
tumble.gif

File is an animated gif, here are the extracted frames:

- (extract frames with: *convert -coalesce tumble.gif tumble_%d.png)*



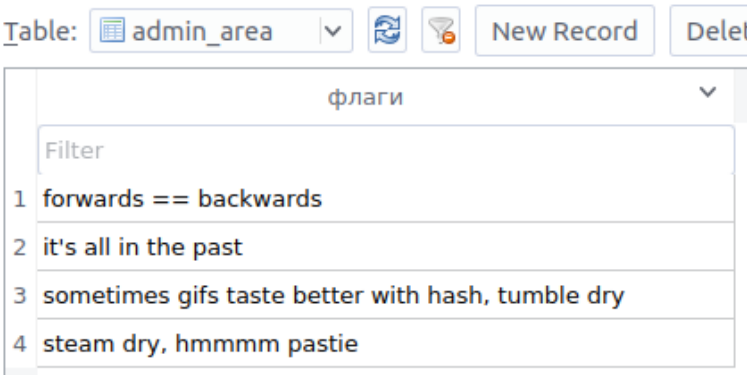




Let’s solve this ish…

Looking at the database within the initial archive, we see an interesting table “admin_area”

флаги (Russian) == flags (English)



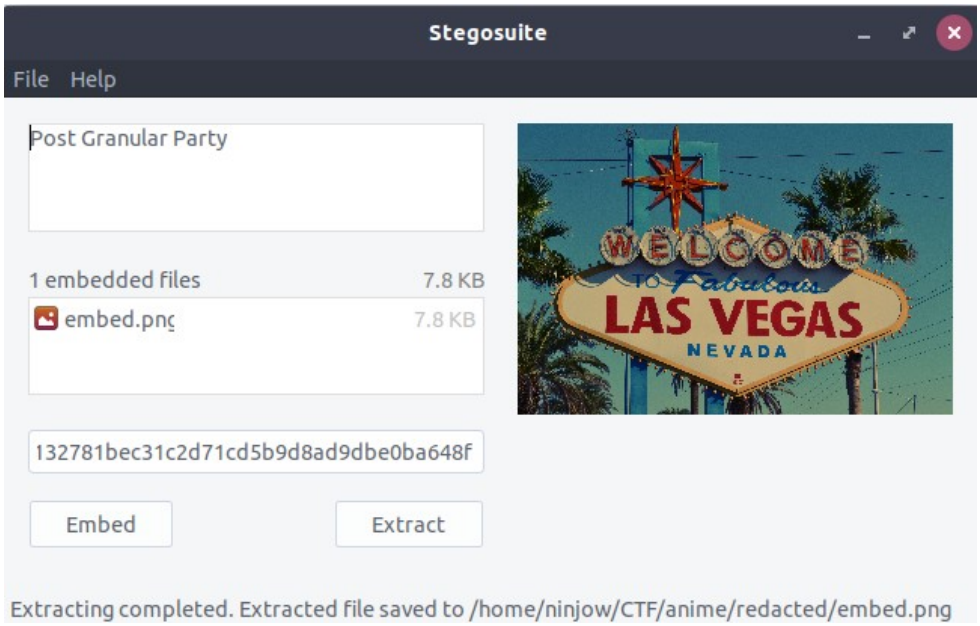
Judging by the name of the table, it’s possible these are clues related to the flags. (protip: they are)

Flag #1 : *"forwards == backwards"*
When we initially looked at the image exported from the database, it was apparent there was possible steganography at play (*ELA (Error Level Analysis)* Max difference: 17). If we look at the EXIF, we can see it was more than likely modified (who would do that?), "Processing Software: pyExifToolGui 0.5".; we can assume something useful has been added. Oh look, "*Copyright: reconctf2018*"...

Hmm, what could one do to manipulate that string? Let's try SHA256!

```
➜  ~ echo -n reconctf2018 | sha256sum
9f037becae938906c301b05672a8132781bec31c2d71cd5b9d8ad9dbe0ba648f  -
```

Using stegosuite (https://stegosuite.org/), we can see if our hunch is correct:



Hooray!

Embedded file:

Filename: embed.png
MD5: 6a9eb1b1d958578cc011289a681fd5f6
SHA1: fc0df19e88e4506253c35293c8915ca6c4f5c104
SHA256: 75fda198429097f615753eca8a1890a749a874b60433d1642ef82a799ae95cdb
Type: PNG image data

```
0x3d 0x3d 0x51 0x5a 0x6b
0x35 0x53 0x59 0x30 0x39
0x6d 0x62 0x68 0x52 0x58
0x64 0x30 0x42 0x45 0x62
0x73 0x56 0x32 0x63 0x7a
0x56 0x6e 0x63 0x75 0x51
0x58 0x5a 0x79 0x46 0x32
0x5a 0x79 0x46 0x57 0x62
```

The HEX string (minus 0x) from the image (yes I made you type it manually) is:

3d3d515a6b35535930396d626852586430424562735632637a566e637551585a7946325a79465762

Since we already used hash sum string manipulation, guessing someone chose to use base64 next:

echo -n 3d3d515a6b35535930396d626852586430424562735632637a566e637551585a7946325a79465762 | xxd -r -p | grep -v %

And the hint is something something reverse:

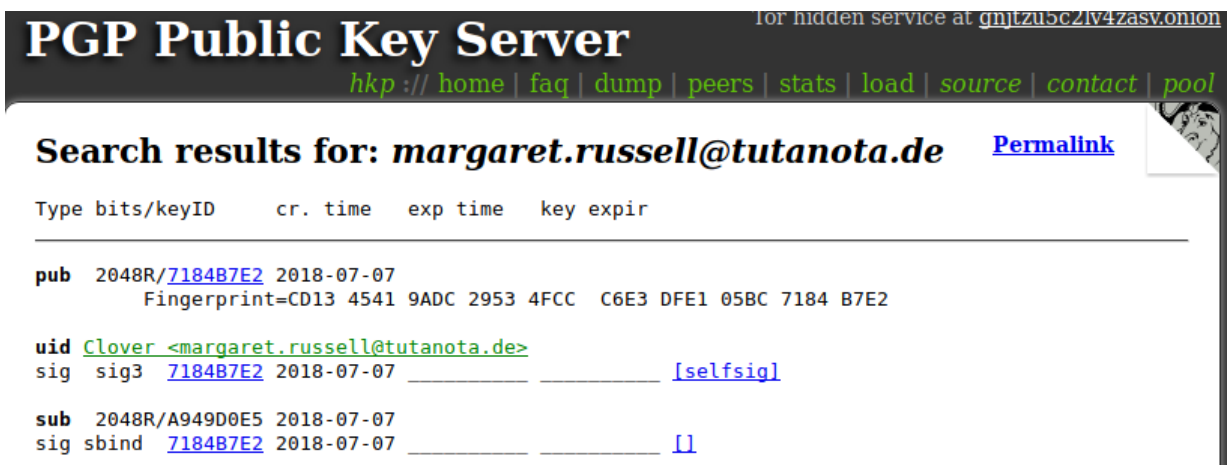
echo -n '==QZk5SY09mbhRXd0BEbsV2czVncuQXZyF2ZyFWb' | rev | grep -v % | base64 –decode

```
→ redacted echo -n '==QZk5SY09mbhRXd0BEbsV2czVncuQXZyF2ZyFWb' | rev | grep -v % | base64 --decode
margaret.russell@tutanota.de%
```

Oooh an email address: **margaret.russell@tutanota.de**

I wonder if they use PGP? If we look at the message from the stegosuite export, we saw:

- "**P**ost **G**ranular **P**arty" == PGP



https://pgp.key-server.io/search/margaret.russell@tutanota.de

Get: *0xDFE105BC7184B7E2*

Download | **Permalink**


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.6+
Comment: Hostname: pgp.key-server.io

mQENBFtBNl4BCACUXvHyF7GbpVD7kzFm/egmNxucuw2Rc5rvoYFPPuoZidqfhk8vQQl3rP4t
p7Q/wxQCl+FHvy9iXEHgpe8q6kv4McykMwZhNONkEJpPm26/LbSP/72NO/F08sKflusZvnJL
EMzFeAtwmw3z9BVdRt5BW2bMzL49tCvduQY7LOd3QgsesbjeUGGR9FCCBt3NlwHAQNi2PzYD
NsfGqU19JP07CaOVc+DN87aBa2uo28WU6kFfco2bqagj08grPvVsUiCHIYMb1QjyU10m8aGB
5G656APJ6pLLcvkTZz7IRtzPbob2rSHtTq7SPcjBTLr4Pr0R8KInpJbEy/y31u2toCqnABEB
AAG0JUNsb3ZlciA8bWFyZ2FyZXQucnVzc2VsbEB0dXRhbm90YS5kZT6JAU0EEwEIADcWIQTN
E0VBmtwpU0/MxuPf4QW8cYS34gUCW0E2XgIbAwULCQgHAgYVCgkICwIDFgIBAh4BAheAAAoJ
EN/hBbxxhLfiEGUH/26qxQ8hai0V4g4o4GPvlmF/hgB8sCWHl7tk2/uPtFnYh0D7lrswLpBE
Gq+jFp3O/yO3TTSc2p30DvuI+zedT69qc77+rYUefwNvCeDUWQ9uNrGnH2idOCNgIGBZSZ4c
vwwqV3BUaN0AM82udvb5QJvo0UsDyY2KQSNR0DdXJ/99EvBSg2dGd+/4uOL+u7hGnrxVR3oI
YvCx4u2lVUvKswn8X3z4nYroS2SxzPIPDpcgdAxtVH1VPQGKmxArR//nhyGfETvoenLPK28M
gMtETR/u2DVnm2Q8EuG9IL5lvUI/Ti11wUfXphBxisGDeZlrHQeT6OUcIxJk6UFe43IF+Pi5
AQ0EW0E2XgEIAMpX5a1uqve1ncdIYO39Mn9HjwY/BFL+cIo+xZYE/VtryIxXgjy930G0031a
FpGGvQLGxcLKXnj7/RGNkUqXNT50nKN/okva4DEwMnAkel6YbNqKpJdeXiGf+77BxoL8++gg
/3gp9YHctoV5Mb/mGouujuigOLAe2WW1emMuW70nS7F8vbbEB1Mij+rU3+A8ktPAKVlMEeXH
nB6vMgKY//b+iR8I+0YCKNw8G4HTRQcuA572inD3X70M6NeMpo768HYnzdwUWR0W076AYQi1
tRWGJDBapOnwh3oPg7ee+hQUNgvsdjBaDdVuZRvLJJbHwGxc/Oa4LOAaSB56GtQta4EAEQEA
AYkBNgQYAQgAIBYhBM0TRUGa3ClTT8zG49/hBbxxhLfiBQJbQTZeAhsMAAoJEN/hBbxxhLfi
n28IAI5vaQgx6+AM89g1hoJX/Jrfjtji/LaiNLj+GEPMkNxgeCTQo7IJexswieoNoj5g/UnF
/AKIRmiPlYIrr8rF/7mh8+G7Nnfi4+p/ldU3850t9zaRmQty7g4A3bzTRdtwxCT8C4dAu6tj
5KblJM4BOiWih+1JcRmFiZKmK6Iri+zBVuUs8WgSL5ImP5ZyrSpJ/dqWB406RgMAbNMcnxmc
42hf7vczkWwt17+Svp0STNSOdz5TH/NvC6fGmc+SR5xBULYrKHNKd+BMjRqRwIHoNJCehDta
4vmQnQ3+19Z30DVFbEtEVkqHEBjIS5PIAHv3nxc7viyAF57CakEdwzPAnfs=
=xYdy
-----END PGP PUBLIC KEY BLOCK-----
```


https://pgp.key-server.io/pks/lookup?op=get&search=0xDFE105BC7184B7E2

If you search for the key ID, you would have found flag #1:

flag:{1} - Pastebin.com

0xdfe105bc7184b7e2. RAW Paste Data. We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy. OK, I Understand . create new paste / deals new! / api ...

pastebin.com/xGK9c2YX

flag:{1}

A GUEST AUG 1ST, 2018 281 NEVER

Flag #2 : *"it's all in the past"*

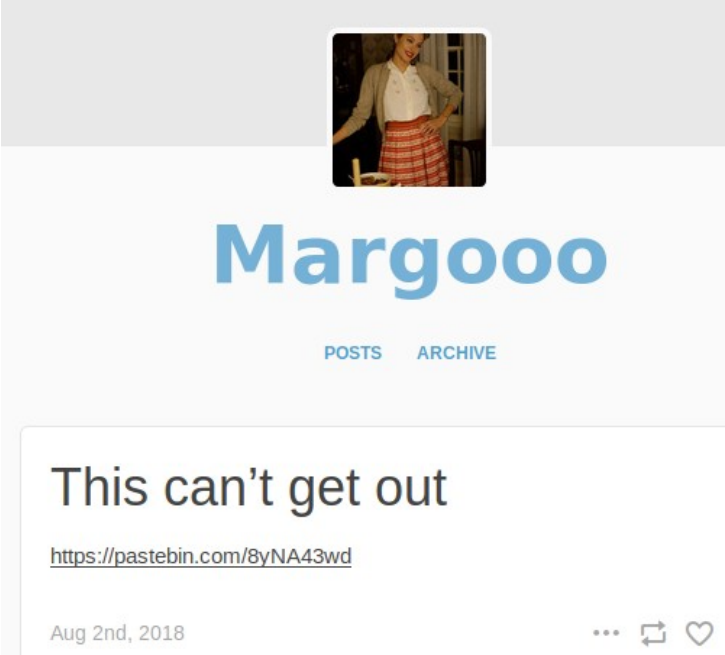
Using the email address from flag #1, you would have come across a Tumblr account (protip: flag #3 would have also given you the pivot to Tumblr)

Looking the Tumblr account up by email address (requires an account) would have led you to:

- margaretclover.tumblr.com

The hint we were given was related to the paste…Now what web service keeps track of pages from the past?

Looks like someone may have deleted a post (flag #2):



https://web.archive.org/web/20180802134854/https://margaretclover.tumblr.com/post/176553424626/this-cant-get-out

https://pastebin.com/8yNA43wd

"How_can_you_have_a_covert_organization_if_you_have_people_looking_over_your_shoulder"

Flag #3 : "*sometimes gifs taste better with hash, tumble dry*"

There are two ways to solve Flag #3

#1
One of the passwords in the table is not like the others:

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: Users | New Record

	Name	Email Address	Password
	Filter	Filter	Filter
1	Margaret Russell	redacted	/-K7Dx[z8c
2	Sam Murach	redacted	`UR3"LS
3	Laura	redacted	Eme(of3
4	Arch Cummings	redacted	@sqve:{L
5	Bill Sullivan	redacted	BT3b/Z
6	John Russell, Sr.	redacted	yellow-red
7	Hanna Schiller	redacted	brown-orange
8	Joseph Palmi	redacted	m0lly$
9	John Russell, Jr.	redacted	uti5Ekyv
10	Edward Wilson	redacted	%saumyb1m/%$

- saumyb1m
- inurl:pastebin "saumyb1m"
- "Thepriceofgreatnessisresponsibility"

flag:{3} - Pastebin.com
https://pastebin.com/saumyb1m
a guest Aug 2nd, 2018 118 Never. Not a member of Pastebin yet? Sign Up, it unlocks many cool features! rawdownloadcloneembedreportprint text 0.16 KB.

#2

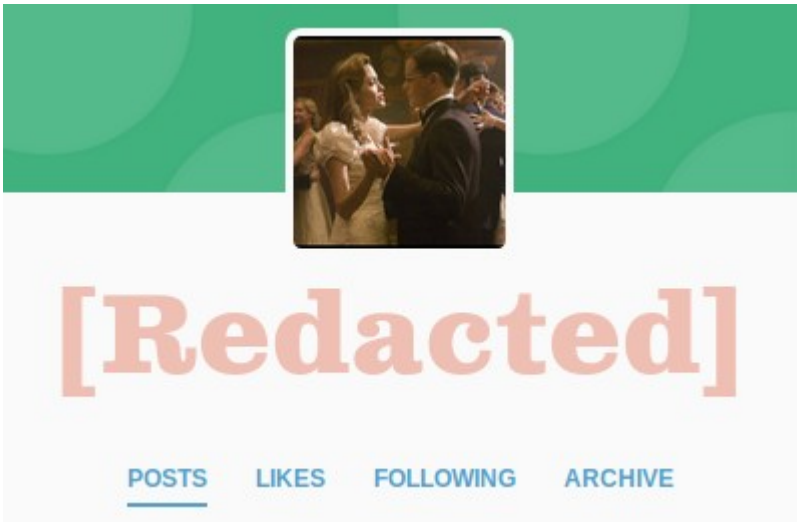
If we take each frame out of the gif, we find an email address in the last image:

- edward.wilson66@tutanota.com

There's also a hint in the EXIF: "*Artist:* ***sparkly - sheep – chaos***"

If we reference the hint "tumble dry" we can assume it's related to a Tumblr account; it is!

sparklysheepchaos.tumblr.com (this will be useful later)



Taking the email address, let's apply a SHA512:

```
→ redacted echo -n edward.wilson66@tutanota.com | sha512sum
3af869dcea82d29cb6f1c37df14e46d892cd8316bb37f1aa44990da2f03b6ad64ab9d2119a775a2d746599c4d237e9924a9106
d11b8c110b838c99615fe24083  -
```

Searching for the string, we also find the flag:

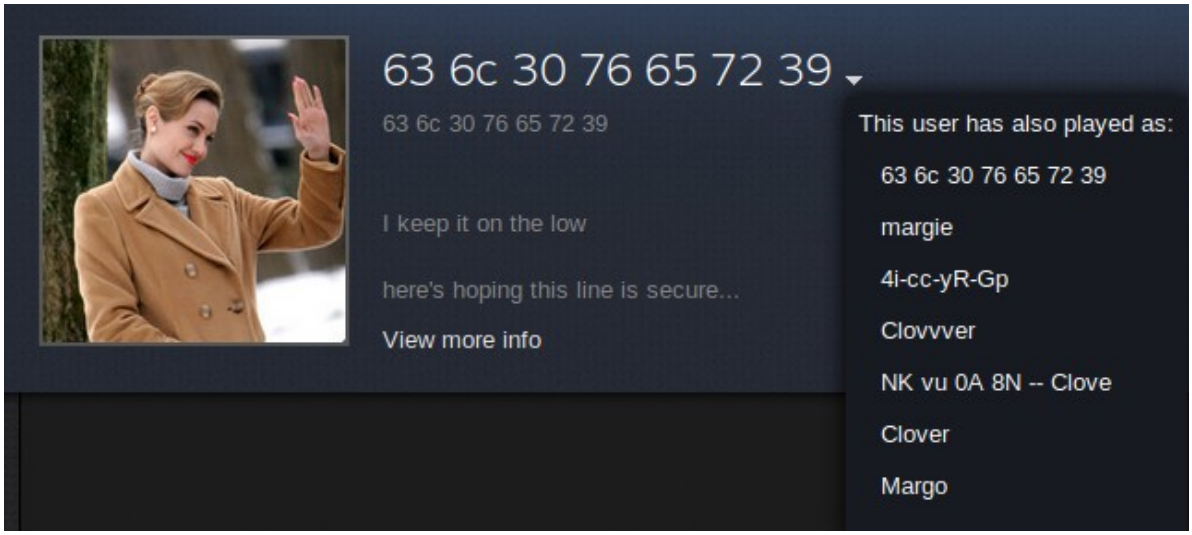
https://pastebin.com/GpRrcvq9 "The price of greatness is responsibility."

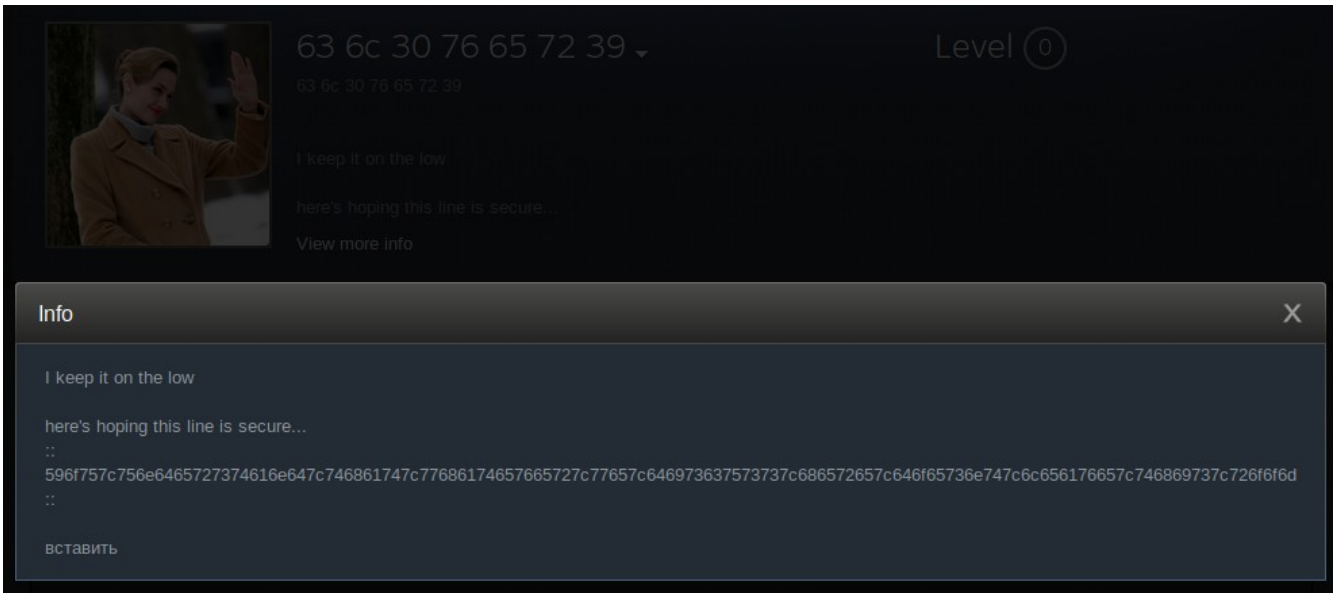
Flag #4 : *“steam dry, hmmmm pastie”*

Going back to the Tumblr account discovered previously, we get a hint related to a Steam account:

https://margaretclover.tumblr.com/ (cl0ver9)

https://steamcommunity.com/id/cl0ver9/





I keep it on the low

here's hoping this line is secure...
::
596f757c756e6465727374616e647c746861747c77686174657665727c77657c646973637573737c686572657c646f65736e747c6c656176657c746869737c726f6f6d
::

вставить

596f757c756e6465727374616e647c746861747c77686174657665727c77657c646973637573737c686572657c646f65736e747c6c656176657c746869737c726f6f6d

==

‘You|understand|that|whatever|we|discuss|here|doesnt|leave|this|room’

Created using:
echo -n 'You|understand|that|whatever|we|discuss|here|doesnt|leave|this|room' | od -A n -t x1

https://pastebin.com/4iccyRGp

flag:{4}

A GUEST AUG 2ND, 2018 46 NEVER

text 0.72 KB raw download clone emb

```
you have completed your assignment

  ___                                       ___    _____     ___           ___      __      _      ___
 | _ \    ___     __      ___    _ _      o O O  / __|  |_   _|   | __|    o O O  |_  )    /  \    / |    ( _ )
 |   /   / -_)   / _|    / _ \  | ' \     o      | (__     | |     | _|    o        / /    | () |   | |    / _ \
 |_|_\   \___|   \__|_   \___/  |_||_|   TS__[O]  \___|   _|_|_   _|_|_   TS__[O]  /___|   _\__/   _|_|_   \___/
_|""""|_|""""|_|""""|_|""""|_|""""| {======|_|""""|_|""""|_| """ | {======|_|""""|_|""""|_|""""|_|""""|
"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'"`-0-0-'./o--000'"`-0-0-'"`-0-0-'"`-0-0-'./o--000'"`-0-0-'"`-0-0-'"`-0-0-'
```