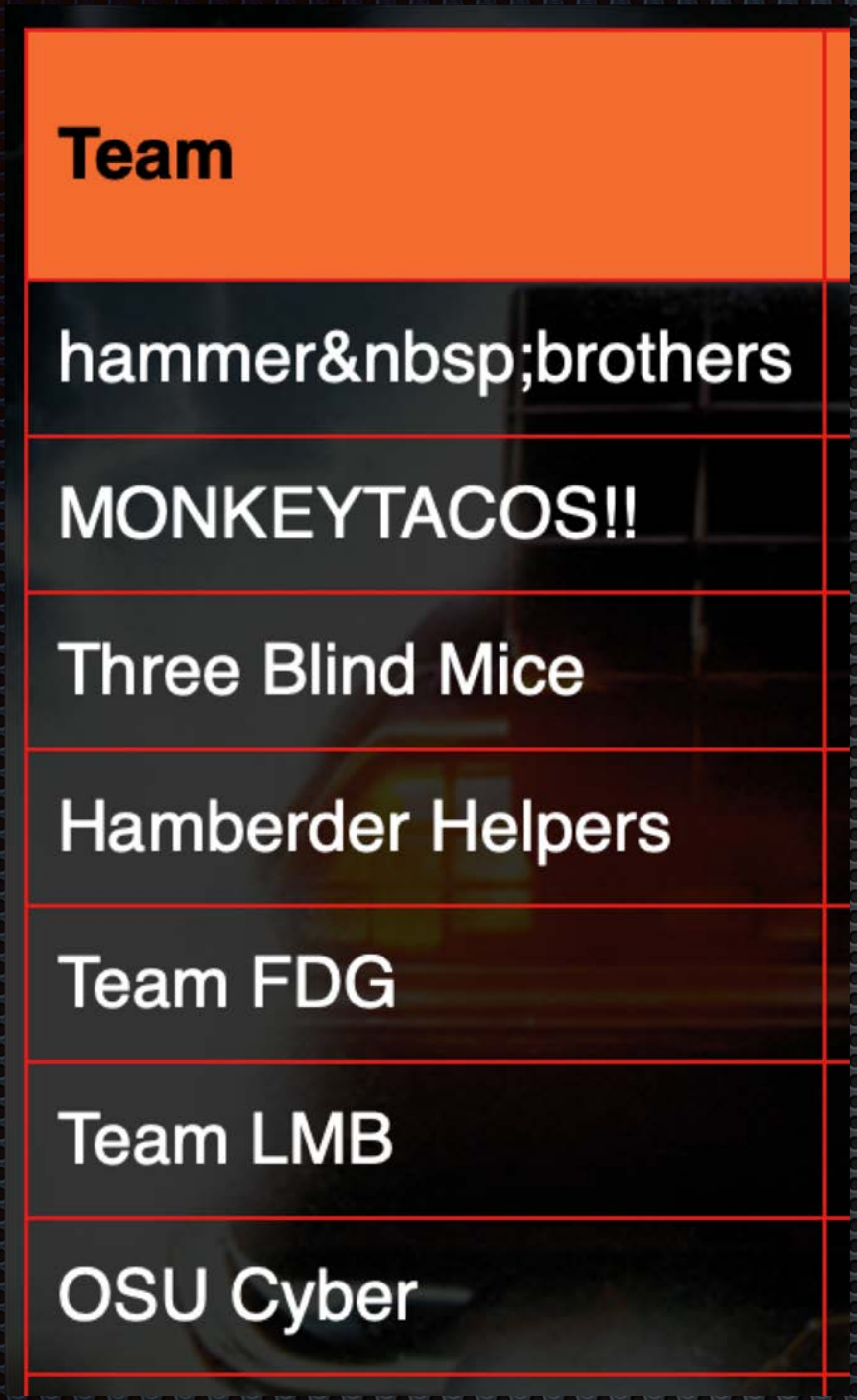
SHMOO
GANOGRAPHY
2019

#shmoocow

24 teams this year!

As of Noon



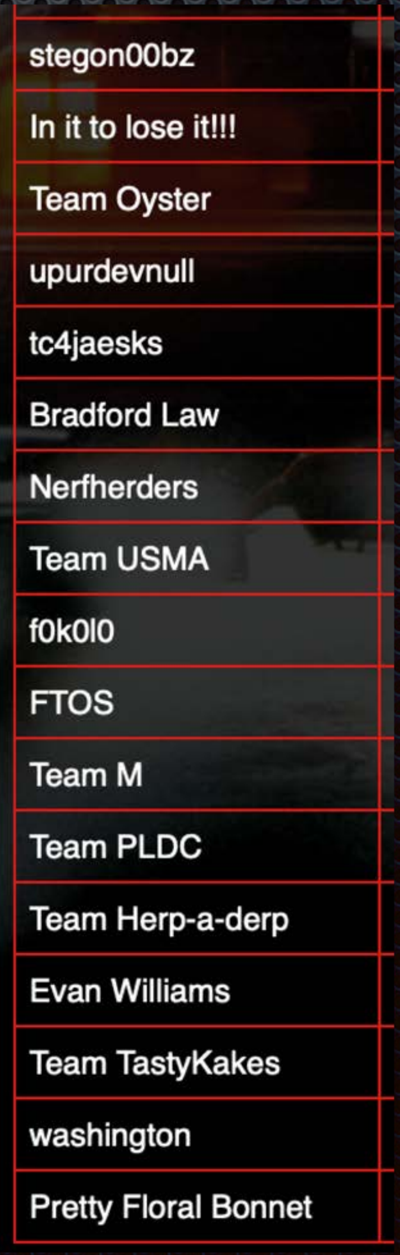
Team
hammer brothers
MONKEYTACOS!!
Three Blind Mice
Hamberder Helpers
Team FDG
Team LMB
OSU Cyber

<u>Stage Prizes:</u>

1: Hammer&nbsp;Brothers
2: Three Blind Mice
3: Hammer&nbsp;Brothers
4:
5:

Actively played

Thanks for registering!

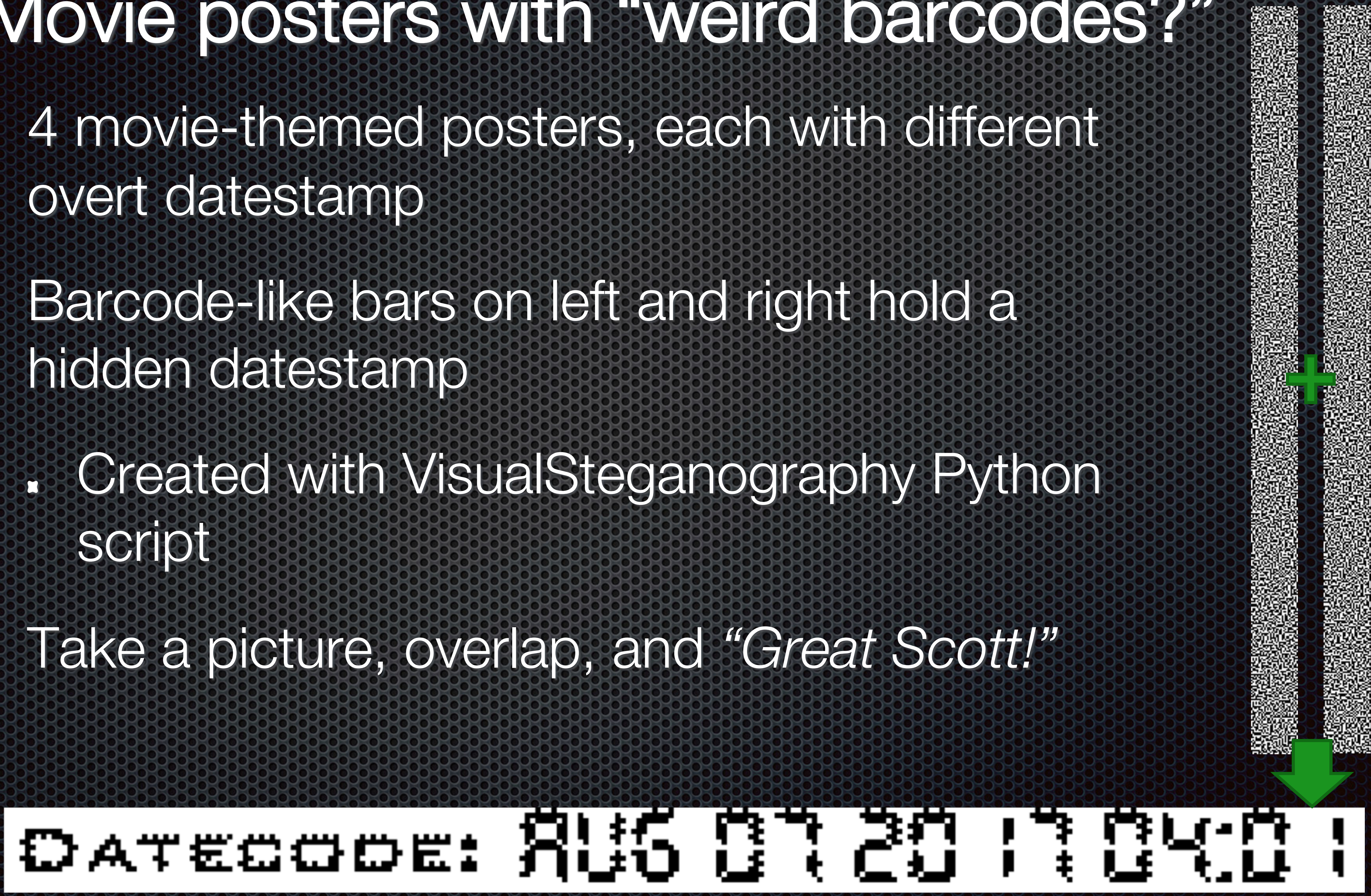


stegon00bz
In it to lose it!!!
Team Oyster
upurdevnull
tc4jaesks
Bradford Law
Nerfherders
Team USMA
f0k0l0
FTOS
Team M
Team PLDC
Team Herp-a-derp
Evan Williams
Team TastyKakes
washington
Pretty Floral Bonnet

Stage 1: AUG0720170401

Movie posters with "weird barcodes?"

- 4 movie-themed posters, each with different overt datestamp
- Barcode-like bars on left and right hold a hidden datestamp
  - Created with VisualSteganography Python script
- Take a picture, overlap, and *"Great Scott!"*

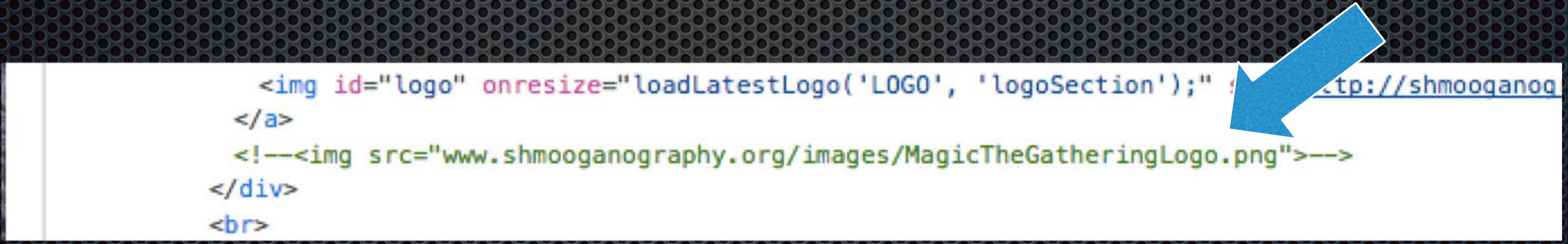


Stage 2: FEB0320130204

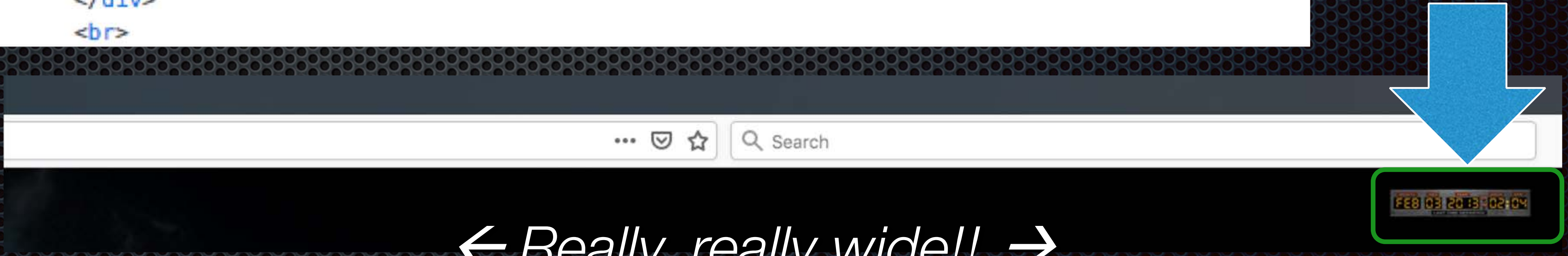
Ajax-powered website resizing/re-rendering

- Visit any page of contest website
- Resize browser window to past 3500 pixels wide, and new graphic appears containing the datestamp

PNG for Stage 3



```
        <img id="logo" onresize="loadLatestLogo('LOGO', 'logoSection');" s     tp://shmooganog
      </a>
      <!--<img src="www.shmooganography.org/images/MagicTheGatheringLogo.png">-->
    </div>
    <br>
```



← Really, really wide!! →

Stage 3: APR0220110700

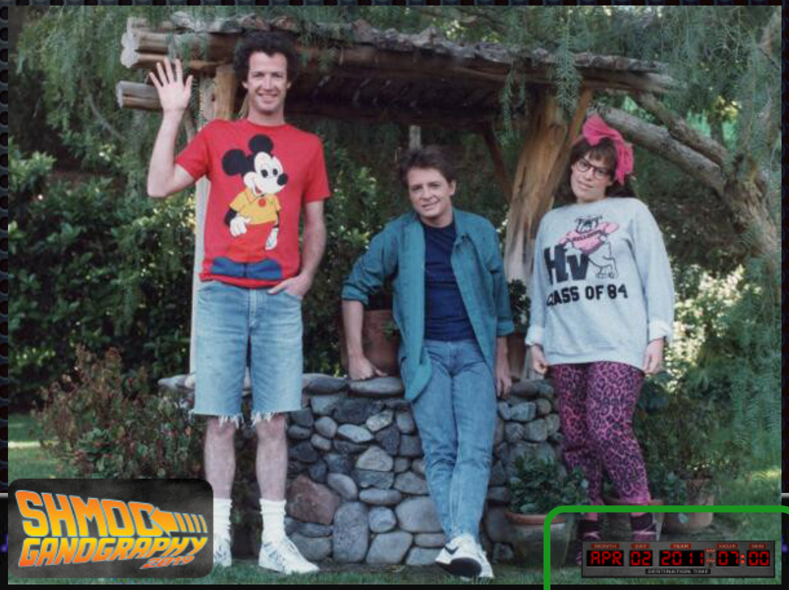
Embedded PNG with mysterious payload

- Using photos from the movie, start with mostly faded version
- Inner JPEG contained within Middle PNG
- Outer PNG contained Middle PNG XOR'd with 0xFF

Outer

Middle

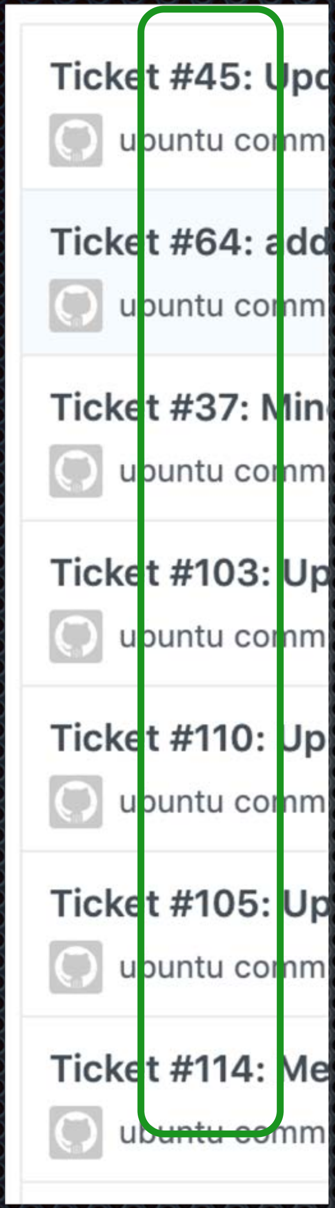
Inner



```
^@6Traversing the /timeplane reveals an assembled truthÿ0                                    C^D
```

Stage 4: OCT0720140105

Travel through time with GitHub



Ticket #45: Upc
ubuntu comm

Ticket #64: add
ubuntu comm

Ticket #37: Min
ubuntu comm

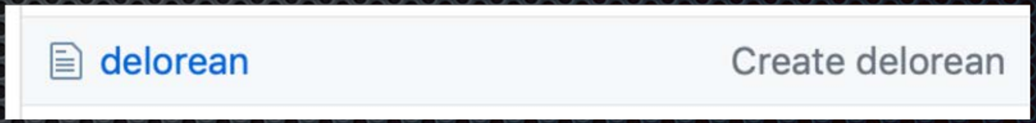
Ticket #103: Up
ubuntu comm

Ticket #110: Up
ubuntu comm

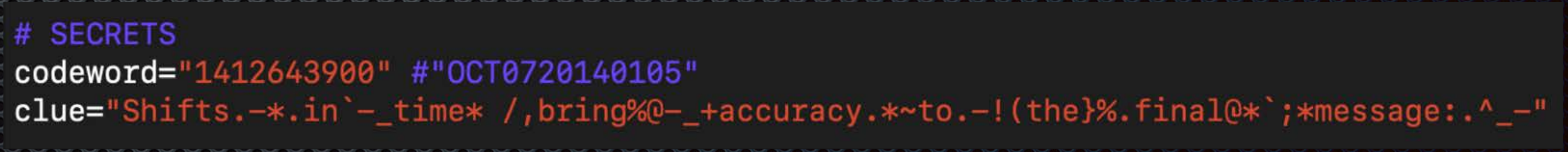
Ticket #105: Up
ubuntu comm

Ticket #114: Me
ubuntu comm

- Retraced all 343 commits from Cédric Bonhomme's *Stegano* Python GitHub project as source, checked into misterfusion's repo
- Ticket numbers with numeral ASCII to hold the clue; space/tab-encoded ASCII at end of *all* Python files for datestamp, just grab one
- Stage 5 FQDN in:

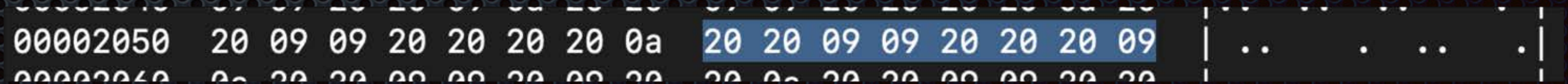


delorean   Create delorean



```
# SECRETS
codeword="1412643900" #"OCT0720140105"
clue="Shifts.-*.in`-_time* /,bring%@-_+accuracy.*~to.-!(the}%.final@*`;*message:.^_-"
```

0 = space
1 = tab

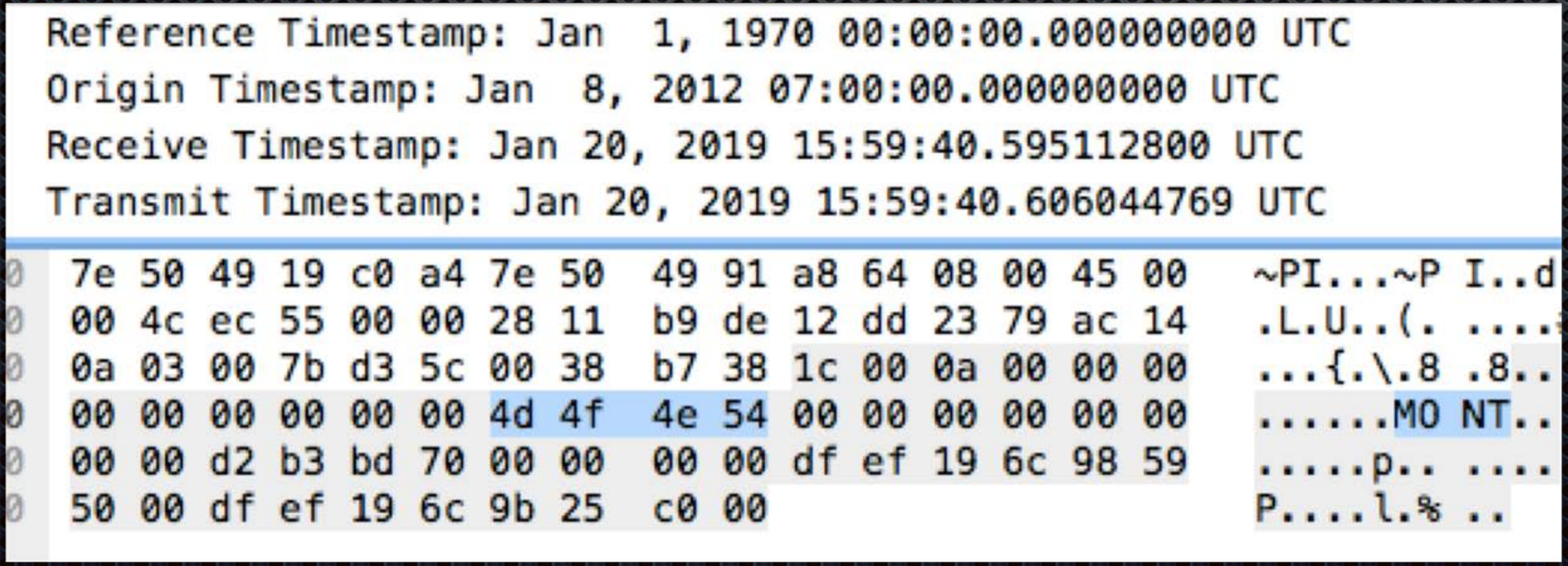


```
00002050  20 09 09 20 20 20 20 0a  20 20 09 09 20 20 20 09  | ..     .  ..   .|
```

Stage 5: JAN0820120700

Special NTP service exfil'ing secrets

- AWS-hosted Python NTP server at *delorean.us.to*
- Acts like a normal NTPD dishing overt time updates
- Attempt to DoS it, and it responds with a Kiss of Death response with datestamp & fragment of clue
  - Hit 7 times total to get full clue



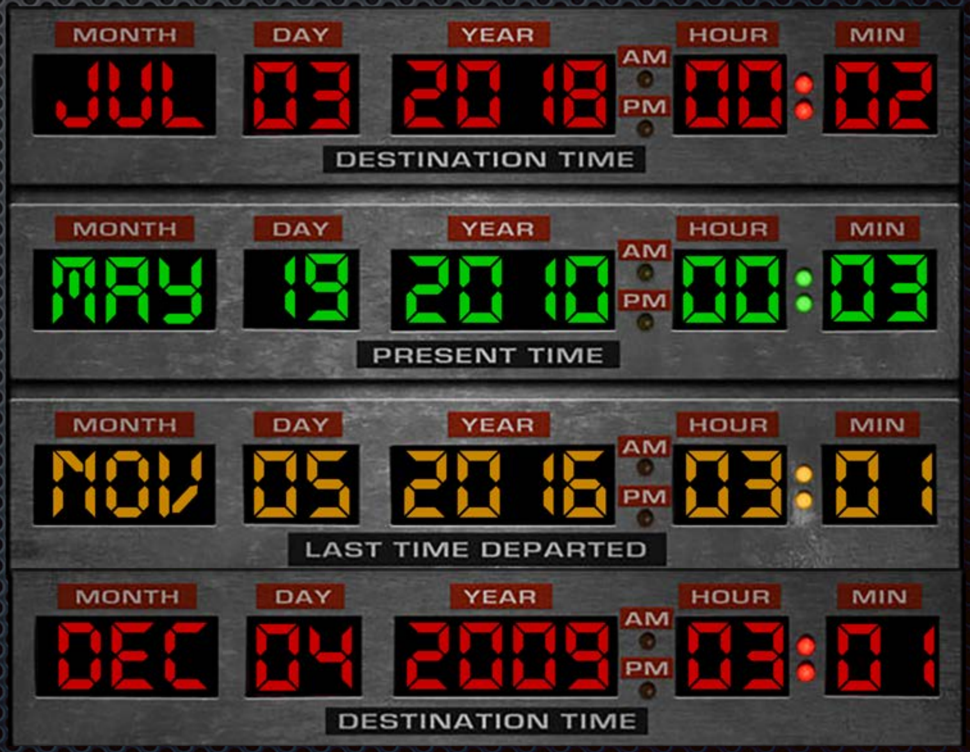
```
Reference Timestamp: Jan  1, 1970 00:00:00.000000000 UTC
Origin Timestamp: Jan  8, 2012 07:00:00.000000000 UTC
Receive Timestamp: Jan 20, 2019 15:59:40.595112800 UTC
Transmit Timestamp: Jan 20, 2019 15:59:40.606044769 UTC

0  7e 50 49 19 c0 a4 7e 50  49 91 a8 64 08 00 45 00   ~PI...~P I..d
0  00 4c ec 55 00 00 28 11  b9 de 12 dd 23 79 ac 14   .L.U..(. ....
0  0a 03 00 7b d3 5c 00 38  b7 38 1c 00 0a 00 00 00   ...{.\.8 .8..
0  00 00 00 00 00 00 4d 4f  4e 54 00 00 00 00 00 00   ......MO NT..
0  00 00 d2 b3 bd 70 00 00  00 00 df ef 19 6c 98 59   .....p.. ....
0  50 00 df ef 19 6c 9b 25  c0 00                     P....l.% ..
```

*"MONT", "HS B",
"RING", " ORD", "ER, ",
"INDE", "XED ", "BY S",
"LIDE", "S, L", "INES", ",
AN", "D WOR", "DS--"*

Code words are all cleverly selected datestamps

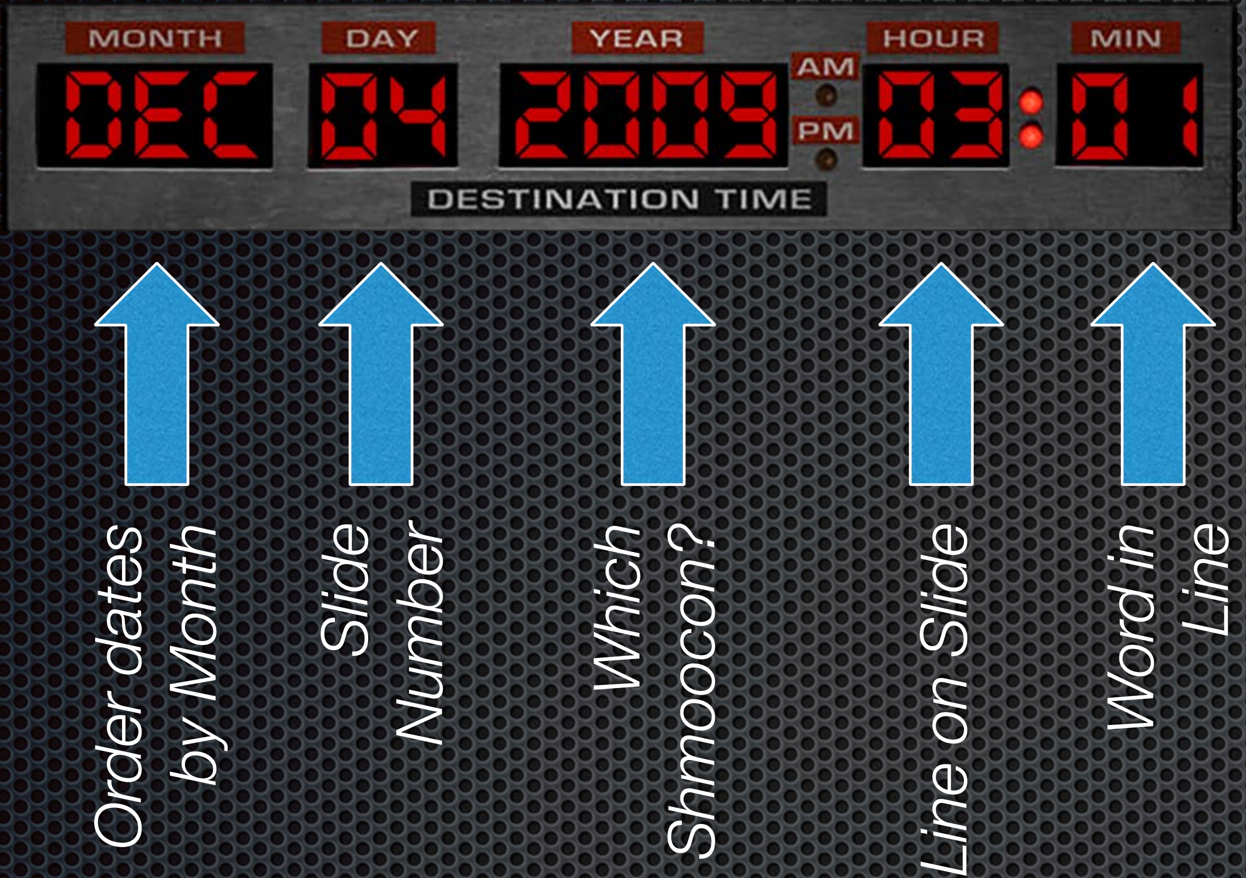
AUG07201704O1
FEB03201302O4
APR02201107OO
OCT07201401O5
JAN08201207OO

Plus the overt ones on the posters…



Datestamps → Slide Pointers

“Months bring order…”



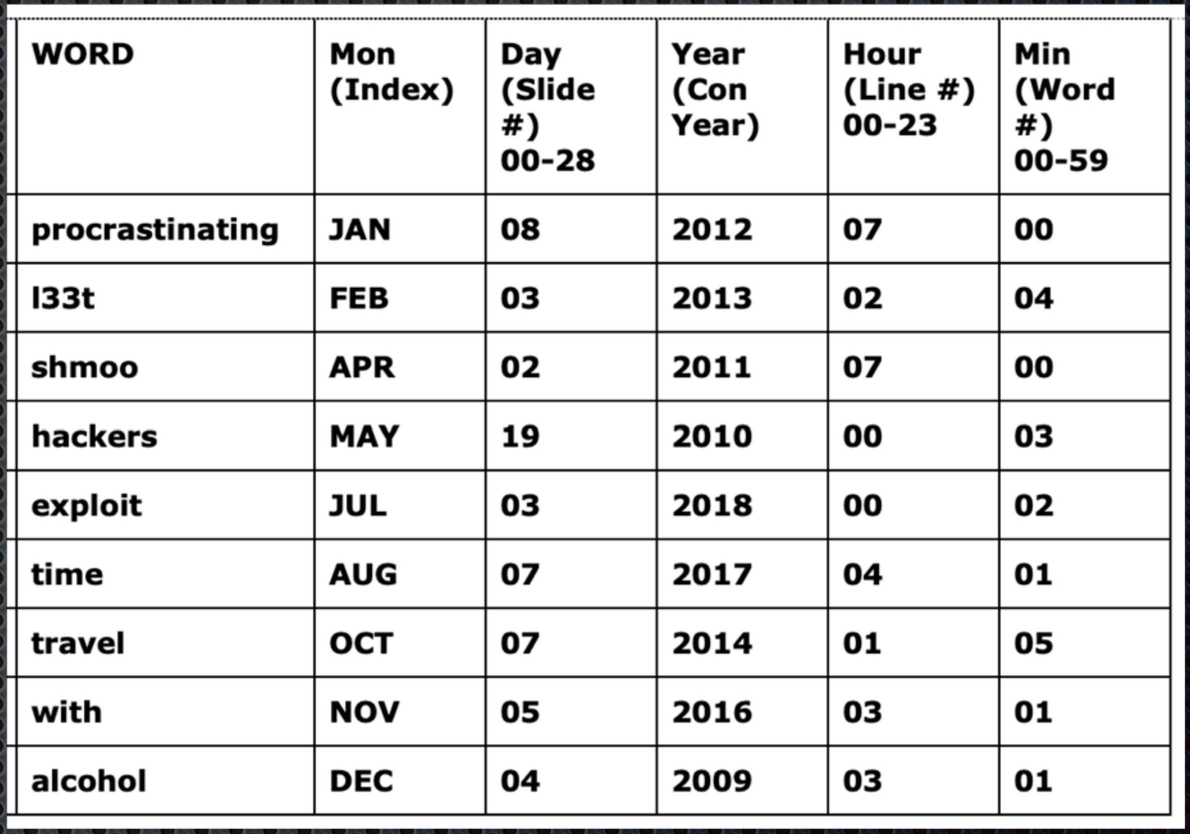
Order dates by Month

Slide Number

Which Shmoocon?

Line on Slide

Word in Line



WORD	Mon (Index)	Day (Slide #) 00-28	Year (Con Year)	Hour (Line #) 00-23	Min (Word #) 00-59
procrastinating	JAN	08	2012	07	00
l33t	FEB	03	2013	02	04
shmoo	APR	02	2011	07	00
hackers	MAY	19	2010	00	03
exploit	JUL	03	2018	00	02
time	AUG	07	2017	04	01
travel	OCT	07	2014	01	05
with	NOV	05	2016	03	01
alcohol	DEC	04	2009	03	01

“procrastinating l33t shmoo hackers exploit time travel with alcohol”

Very Special Thanks

PRAXIS
ENGINEERING

for their continued sponsorship,
covering our expenses, materials,
shirts, and prize!

Special Thanks

- **Steven Speilburg & Universal,** for not suing us (yet)
- **No Starch Press,** for coordinating gift certificates
- **Not Just Signs,** for super last-minute sign-printing
- **FOSS Projects,** like VisualSteganography, Stegano, LimiFly NtpServer & Brian de Heus' PNG technique
- **Our Wives & Bosses,** for permitting our annual hiatus
- **Bruce & Heidi,** for tolerating our endless shenanigans

The struggle is real
#hotelfail

shmooganography@gmail.com

Presentation will be available on the contest website soon.

You gotta spread positivity around the con'…

Adam Reinhard

Let's keep being awesome to each other.

Two Shmoo HAMs