



*“Never Steg a Sleeping Moose”*

# 20 teams this year!

*As of Noon*

Team FDG
Three Blind Mice
uhthatone
hammer&nbsp;brothers
Dark Arts of Data Concealment
flippers.jpg

## Stage Prizes:

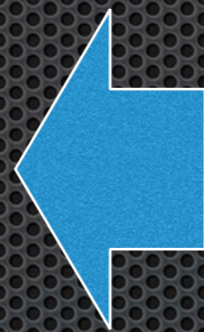
1: Hammer&nbsp;Brothers

2: Three Blind Mice

3:

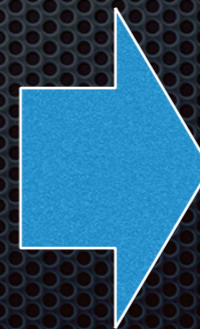
4: uhthatone

5:



*Actively  
played*

*Thanks for  
registering!*



Hit It And Quidditch
Definitely Not Two Raccoons In A Trenchcoat
Babint_is_best
Slyther-out
PS1 Hagrid
Psyberducks
Grace & Alan
That Guy D4ve
SecSeaMussels
YourMomsAHorcrux
NoodleBowl
scriptohio
ThiefD&Z
Casual Puzzle Solvers

# Stage 1: STONE

## Layered QR Codes, with GeolP foo

- Each contest poster has a different QR code, overtly pointing to a dynamic URL to a LufCo site
- By changing light gray to black and dark gray to white, covert QR and URL are uncovered
- When attempted from a US IP, points to LufCo's website; use a VPN outside the US points to the next contest page

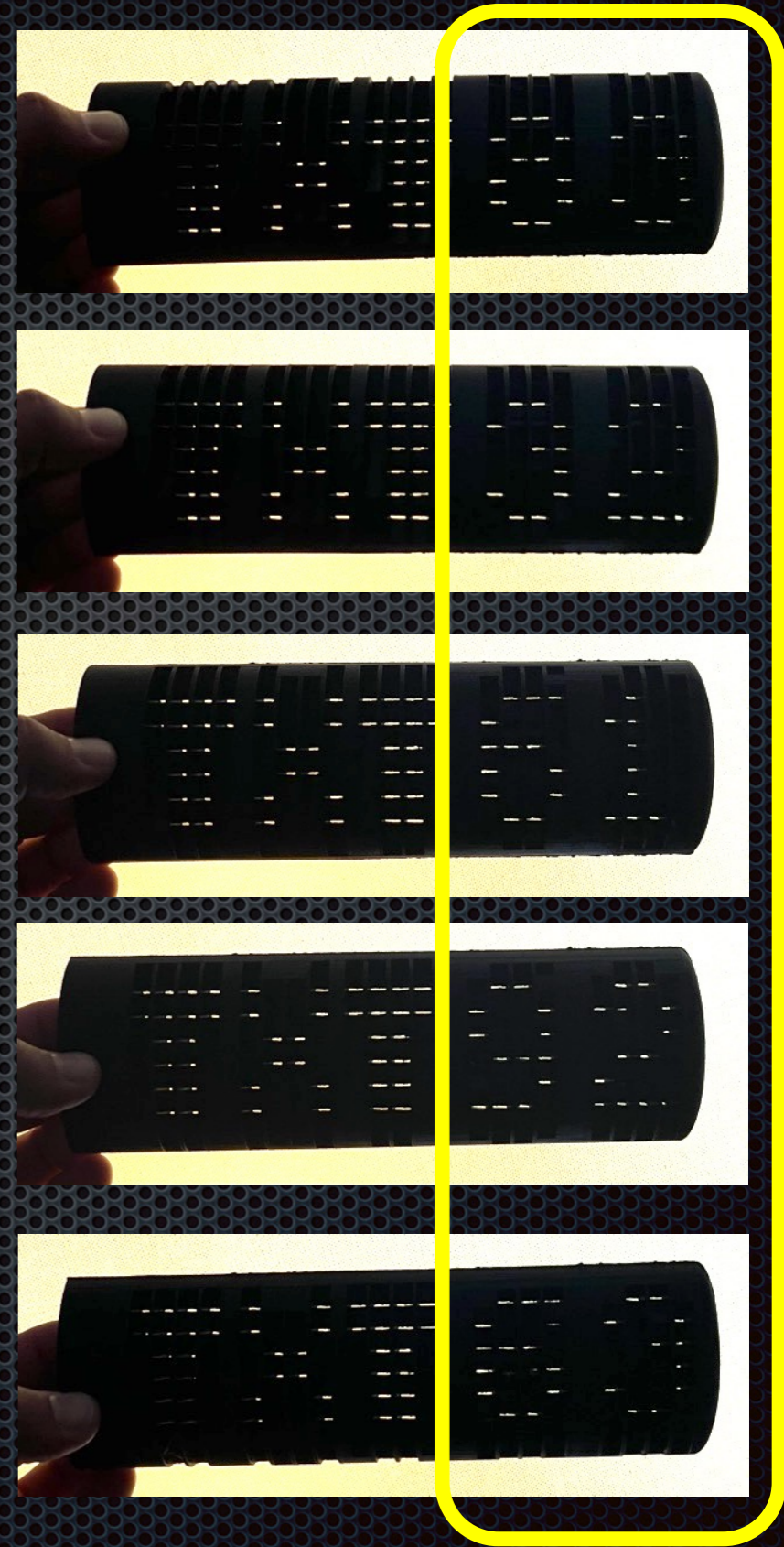


# Stage 2: WAND

Container is your wand, but hosts an STL

- Website points to DockerHub-hosted “wand” container, with script on the GitHub site to use it
- Wand shell script activates functions in the container, though the container has the payload needed for this stage
- Shmoo.stl, found after some directory crawling, has embedded “sun dial” stating TXT 83 32 61 92 63


*Also, “WAND” on a dial pad...*



# Stage 3: CLOAK

## Most unreliable AWS stack

*ASCII characters  
emerge from  
each (ordered)  
state – on or off*



- 8 AWS instances carefully starting and stopping over the course of 15 minutes
- Instances are managed by Lambdas, executed by CloudWatch every minute
  - 1 “all-on” state
  - 8 “ASCII” states: spelling *WANDS0ul*
  - 1 “all-off” state
- GrandStaircase tag is used to order the instances, keyed by the book/movie names

Instances (1/40) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state
sUoxljpDwq	i-0e0061a3abf92fb67	Running
jfLrUHHByB	i-0d741c073485c9d6a	Running
zneptvBxBb	i-026db632eeac9730b	Running
HcOfFxspLC	i-02a91a1da741dfc53	Running
yUJlSZNqN	i-06590c66f9e4534a3	Running
LMMKZyrzDj	i-0a461929ede1accd3	Stopped
VMIIFBprls	i-0bd8d0fa884289ebf	Stopped
oecOiWDoWX	i-078e300eb48a05cd2	Stopped

Instance: i-0e0061a3abf92fb67 (sUoxljpDwq)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Tags

Key | Value

Wizards	526F77656E61
Name	sUoxljpDwq
Muggles	KovvYfonAN
GrandStaircase	4368616D626572206F662053656372657473
Tarantallegra	1001110110100000101010011111100001100001

# Stage 4: ELDER

RTP stream of Hedwig's Theme, with magical option data

No.	Time	Source	Destination	Protocol	Length	Info
2	0.011998	172.20.10.3	224.2.127.254	SAP/SDP	296	Announcement (v1)
3	0.011998	127.0.0.1	127.0.0.1	RTCP	88	Sender Report Source description
4	0.012998	127.0.0.1	127.0.0.1	MPEG TS	1364	PT=MPEG-II transport streams, SSRC=0xEA8028
5	0.014997	127.0.0.1	127.0.0.1	MPEG TS	1364	Audio Layer 3, 160 kb/s, 44.1 kHz [MP2T fra

- Music is streamed, but not hiding any information (this year)
- Inspecting the often-overlooked Overflow field in the IP header reveals a GIF, one nibble at a time

Pointer: 5

0011 .... = Overflow: 3

# ELDER

*Being made from wood,  
your wand has many rings.  
Voldemort doesn't want  
us to tell you more.*

# Stage 5: RESURRECTION

## Docker layering

- Take container received in Stage 2, unpacking it to reveal internal layers

```
docker pull ${IMAGE}:${PHASE12TAG}

mkdir validate
docker save -o validate/phase12-4A4B.mod.tar ${IMAGE}:${PHASE12TAG}
tar -xvf phase12-4A4B.mod.tar
```

```
/opt/dev/workspaces/github/hckeyguy33/shmooganography/2023/docker/shmooganography2023/validate$ docker save -o test.tar hckeyguy33
hy2023:wand
/opt/dev/workspaces/github/hckeyguy33/shmooganography/2023/docker/shmooganography2023/validate$ tar -xvf test.tar | grep 538.json
9fdd6c648b3ded296325ae7f6a83534b84afe0b4f57d56f538.json
```

*Space after comma  
is 1, no space is 0.*

```
ead5a1990f9bf86eadafcb463920", "sha256:6c72ac497917fc261
b4cd9b1f7ec9003405fbc70e5f3bf33ac", "sha256:17ef1685390e
cb7943eedb67d753ab6c7492769b9706117885", "sha256:712a7a87
63188b5bfb68e2db29978b4220bcc19bf60b3a59df", "sha256:ad65
b013ecba06a381d0dd300e54eef22179495af6c40677e6c", "sha25
4d4d3b62c882944c06290fe5fc67388cf9960dede89d60711a9a", "
```

# **Code words are The Deathly Hallows!**

*STONE*

*WAND*

*CLOAK*

*ELDER*

*RESURRECTION*



Very Special Thanks



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

# Special Thanks

- Warner Brothers overlords, for not suing us (yet)
- No Starch Press, for donating ebook gift certificates
- Not Just Signs, for super last-minute sign-printing
- Rob, for swooping in to bring fresh steg ideas for 2023
- Linkly, ClickSend, AWS, and ScaPy tools & services
- Our Wives & Bosses, for permitting our annual hiatus
- Heidi & Bruce, for tolerating our endless shenanigans
  - *And all of the Shmoo staff who play and help us*
- You, for playing and providing feedback for 16 years!

[shmooganography@gmail.com](mailto:shmooganography@gmail.com)

Presentation will be available on the  
contest website soon.

T-Shirts *may* available for sale,  
so email us if interested!