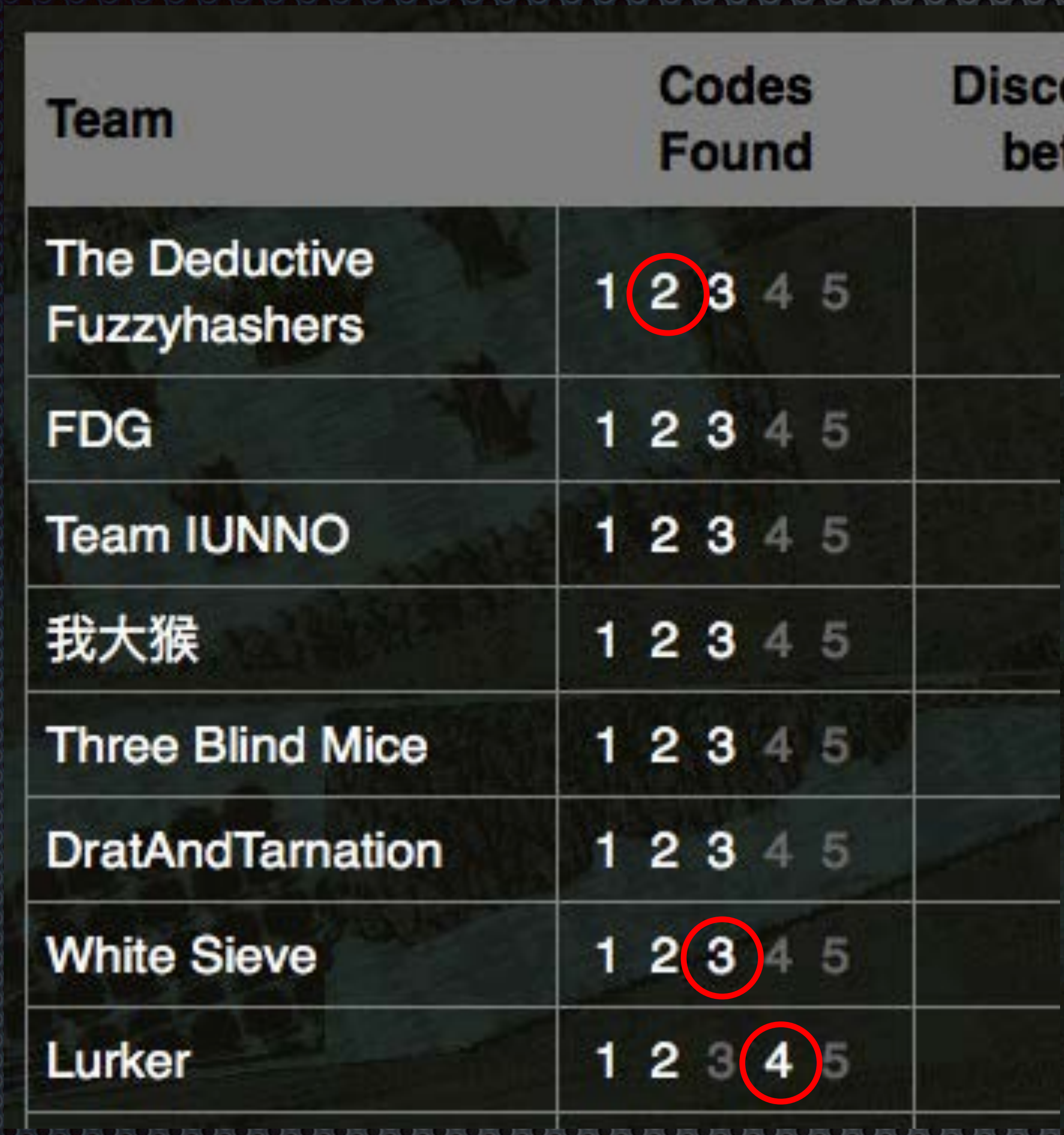
2016

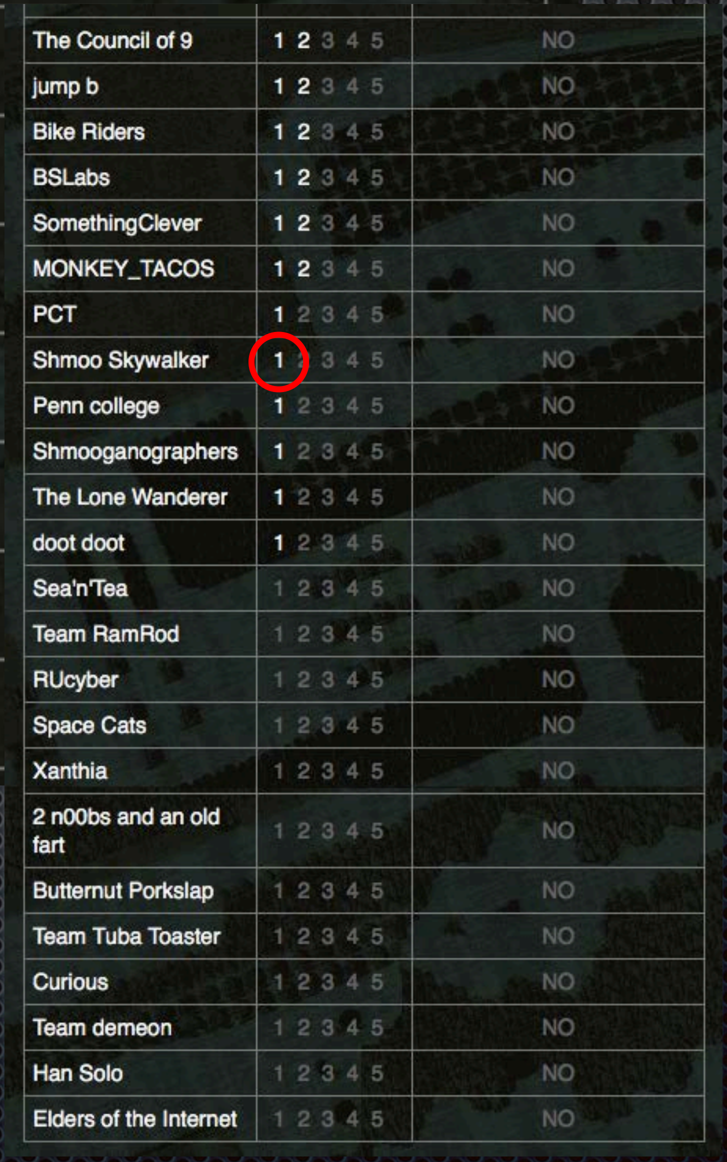
SHMOO GANOGRAPHY

32 teams this year!

As of 1330



Team	Codes Found	Discovered Relationship between Codewords
The Deductive Fuzzyhashers	1 2 3 4 5	NO
FDG	1 2 3 4 5	
Team IUNNO	1 2 3 4 5	
我大猴	1 2 3 4 5	
Three Blind Mice	1 2 3 4 5	
DratAndTarnation	1 2 3 4 5	
White Sieve	1 2 3 4 5	
Lurker	1 2 3 4 5	



The Council of 9	1 2 3 4 5	NO
jump b	1 2 3 4 5	NO
Bike Riders	1 2 3 4 5	NO
BSLabs	1 2 3 4 5	NO
SomethingClever	1 2 3 4 5	NO
MONKEY_TACOS	1 2 3 4 5	NO
PCT	1 2 3 4 5	NO
Shmoo Skywalker	1 2 3 4 5	NO
Penn college	1 2 3 4 5	NO
Shmooganographers	1 2 3 4 5	NO
The Lone Wanderer	1 2 3 4 5	NO
doot doot	1 2 3 4 5	NO
Sea'n'Tea	1 2 3 4 5	NO
Team RamRod	1 2 3 4 5	NO
RUcyber	1 2 3 4 5	NO
Space Cats	1 2 3 4 5	NO
Xanthia	1 2 3 4 5	NO
2 n00bs and an old fart	1 2 3 4 5	NO
Butternut Porkslap	1 2 3 4 5	NO
Team Tuba Toaster	1 2 3 4 5	NO
Curious	1 2 3 4 5	NO
Team demeon	1 2 3 4 5	NO
Han Solo	1 2 3 4 5	NO
Elders of the Internet	1 2 3 4 5	NO

No one figured out the codeword relationship!

***20** Passed Stage 1!*

***14** Passed Stage 2!*

***7** Passed Stage 3!*

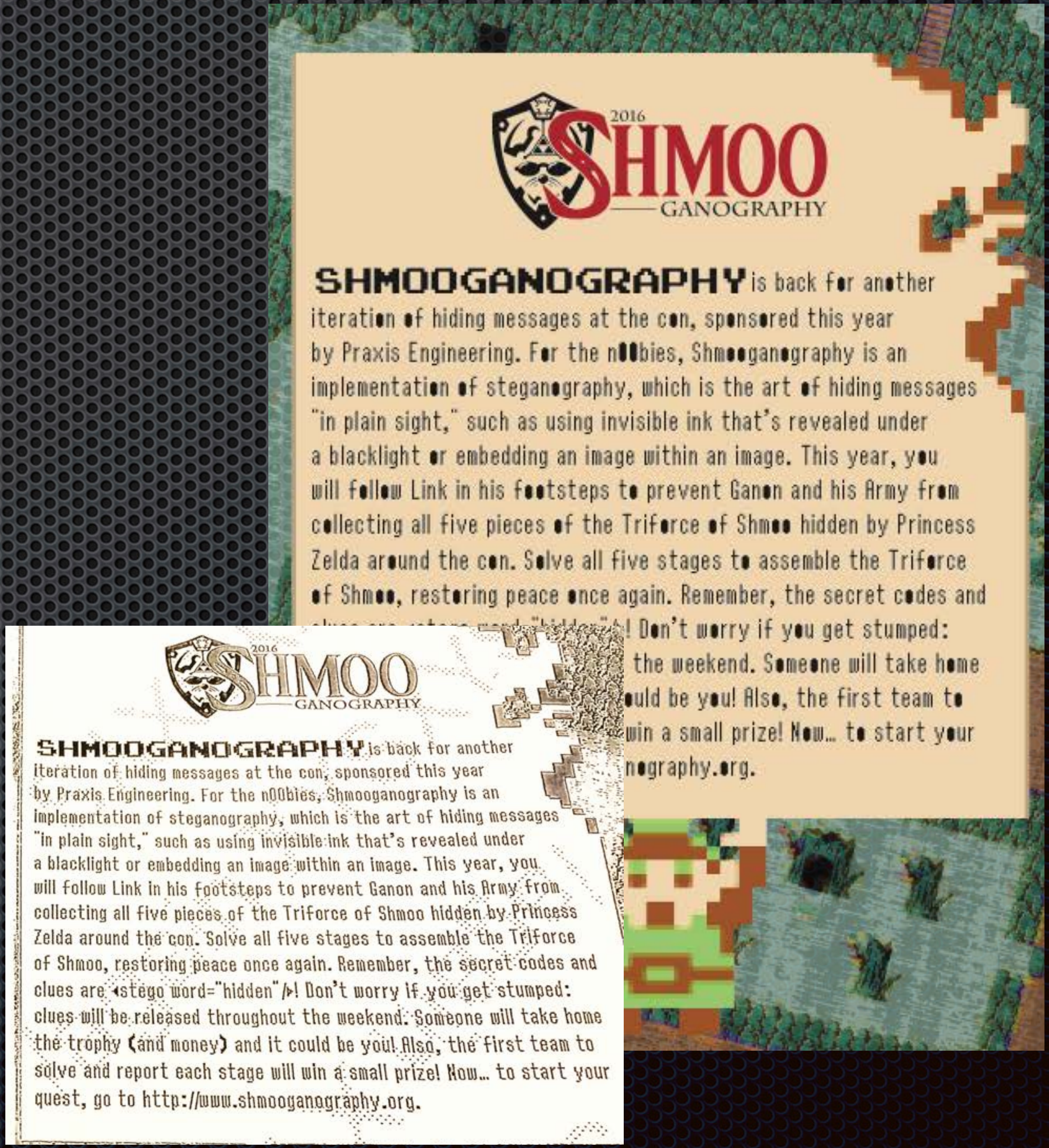
Stage Prizes:

1: Penn college
2: Fuzzyhashers
3: White Sieve
4: Lurker

Stage One: AVVLAUSZ

Anti-copy pattern on ad slips

- Overtly, just a description of the contest
- Code word was embedded using a Ricoh/Lanier color laser printer
- Uncovered using photocopies or editing software



2016
SHMOO
GANOGRAPHY

SHMOOGANOGRAPHY is back for another iteration of hiding messages at the con, sponsored this year by Praxis Engineering. For the n00bies, Shmooganography is an implementation of steganography, which is the art of hiding messages "in plain sight," such as using invisible ink that's revealed under a blacklight or embedding an image within an image. This year, you will follow Link in his footsteps to prevent Ganon and his Army from collecting all five pieces of the Triforce of Shmoo hidden by Princess Zelda around the con. Solve all five stages to assemble the Triforce of Shmoo, restoring peace once again. Remember, the secret codes and clues are <stego word="hidden"/>! Don't worry if you get stumped: clues will be released throughout the weekend. Someone will take home the trophy (and money) and it could be you! Also, the first team to solve and report each stage will win a small prize! Now… to start your quest, go to http://www.shmooganography.org.

SHMOOGANOGRAPHY is back for another iteration of hiding messages at the con, sponsored this year by Praxis Engineering. For the n00bies, Shmooganography is an implementation of steganography, which is the art of hiding messages "in plain sight," such as using invisible ink that's revealed under a blacklight or embedding an image within an image. This year, you will follow Link in his footsteps to prevent Ganon and his Army from collecting all five pieces of the Triforce of Shmoo hidden by Princess Zelda around the con. Solve all five stages to assemble the Triforce of Shmoo, restoring peace once again. Remember, the secret codes and
! Don't worry if you get stumped:
the weekend. Someone will take home
ould be you! Also, the first team to
win a small prize! Now… to start your
nography.org.

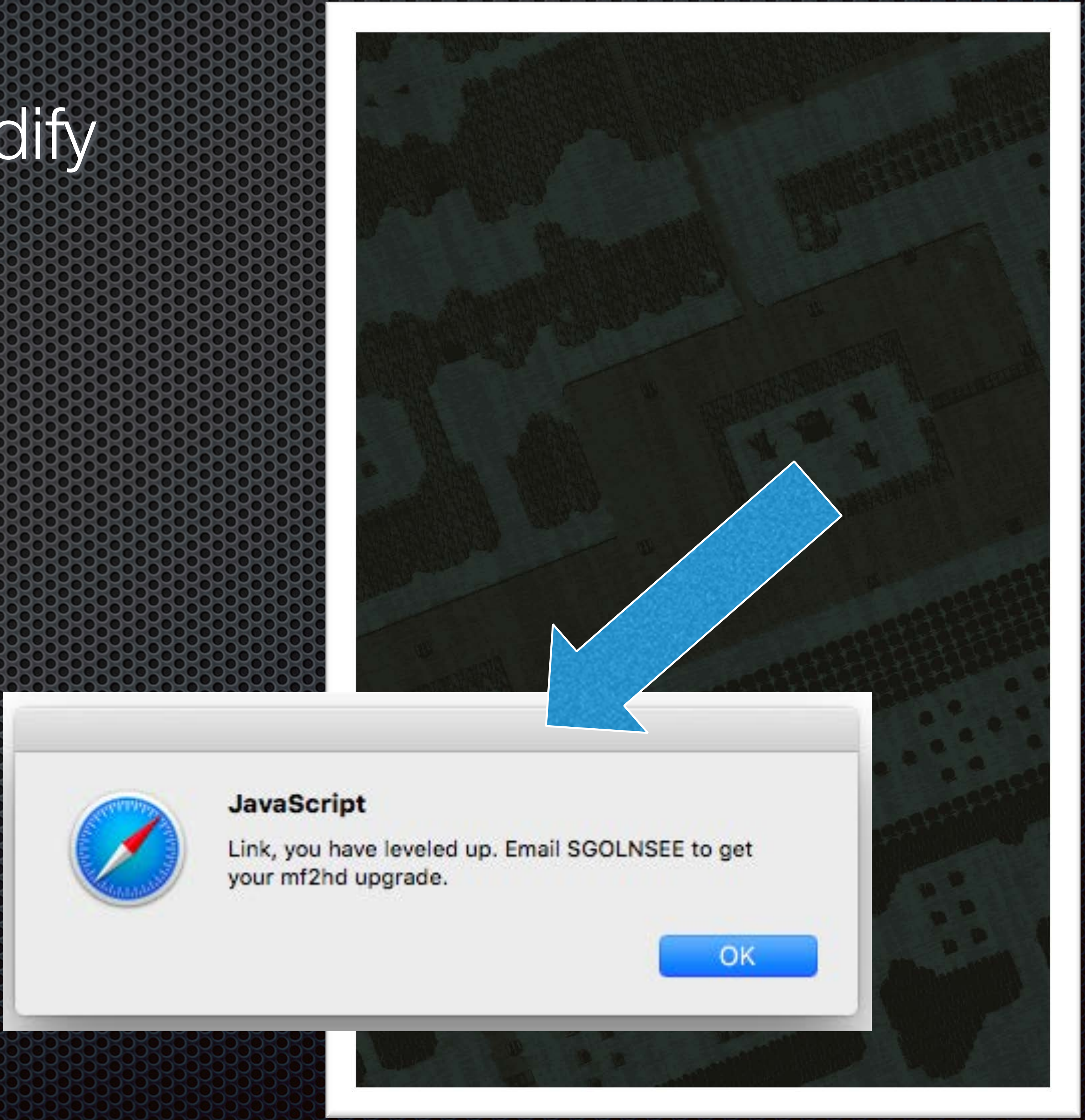
Stage Two: SGOLNSEE

Embedded Javascript in GIF

- Used online tool to modify the map used as background for the contest website
- Reload as a script and dialog appears.

“PBR + Actual Laptop
+ GIF Magic Numbers
+ Shittly looking
Javascript =
SGOLNSEE”

- FDG



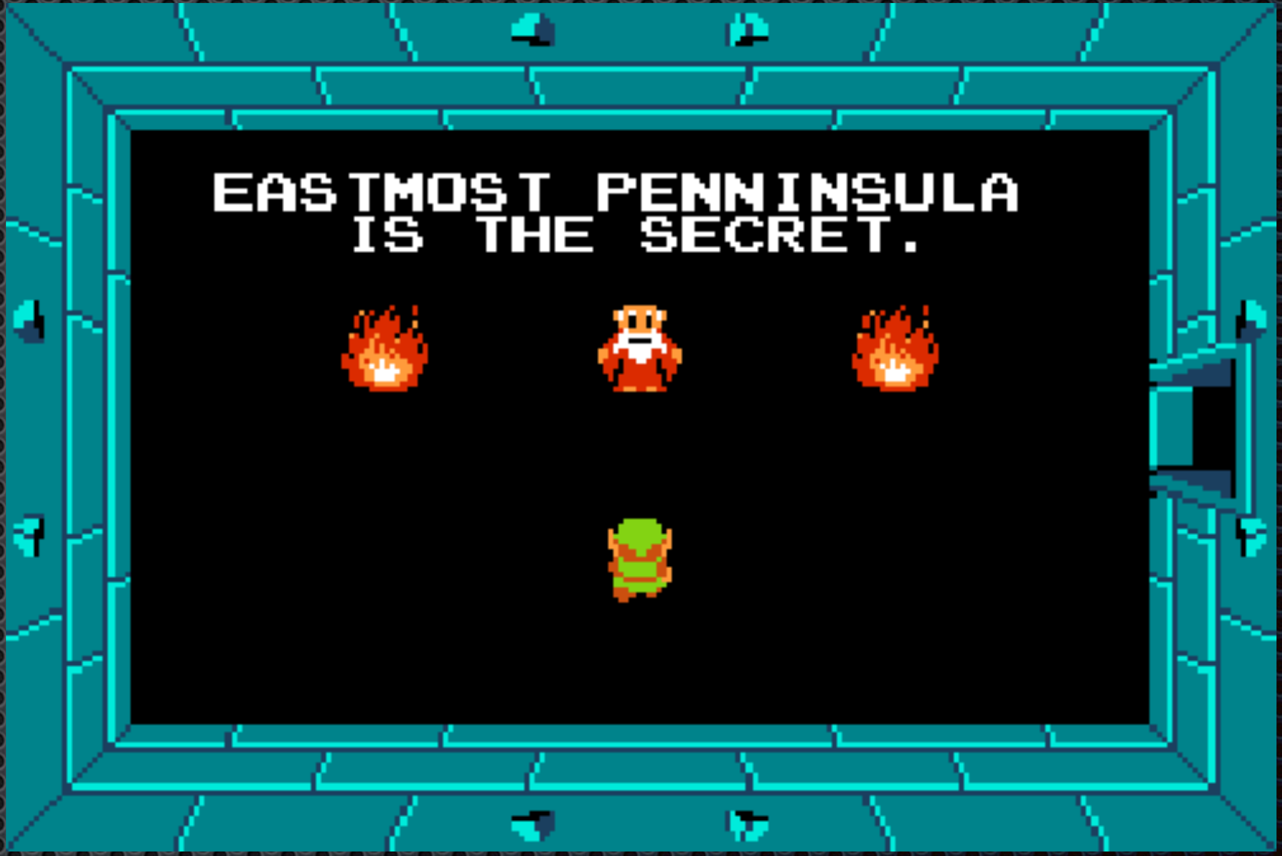
JavaScript

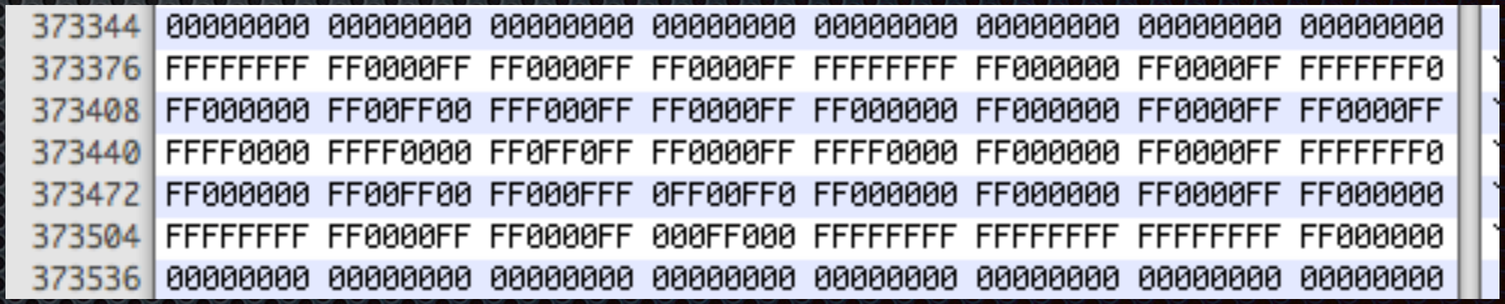
Link, you have leveled up. Email SGOLNSEE to get your mf2hd upgrade.

Stage Three: EKNVELUP

MF2HD upgrade “Game cartridge” with hidden files

- Throwback to 1.44MB floppy diskette
- Can’t just copy the overt files (an LoZ ROM)
- Disk has deleted PNG of LoZ screenshot
- Code hidden as bytes at 0x373376



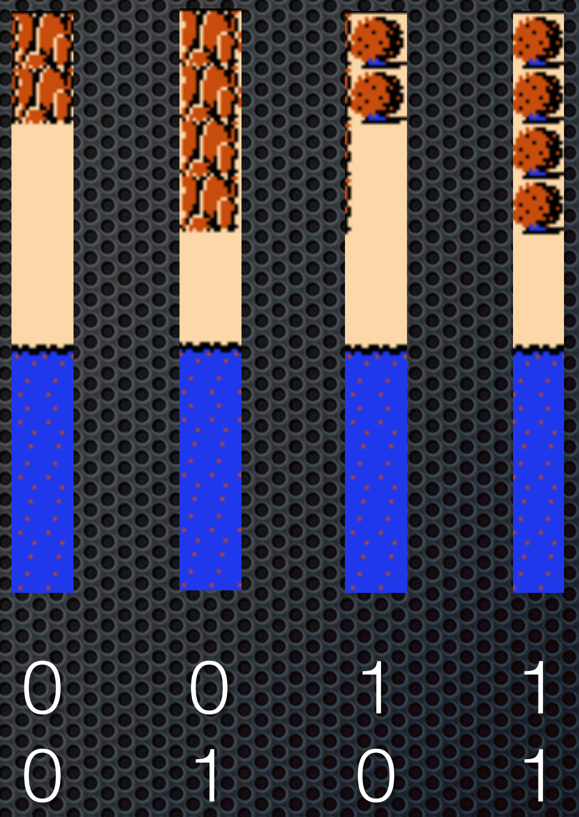


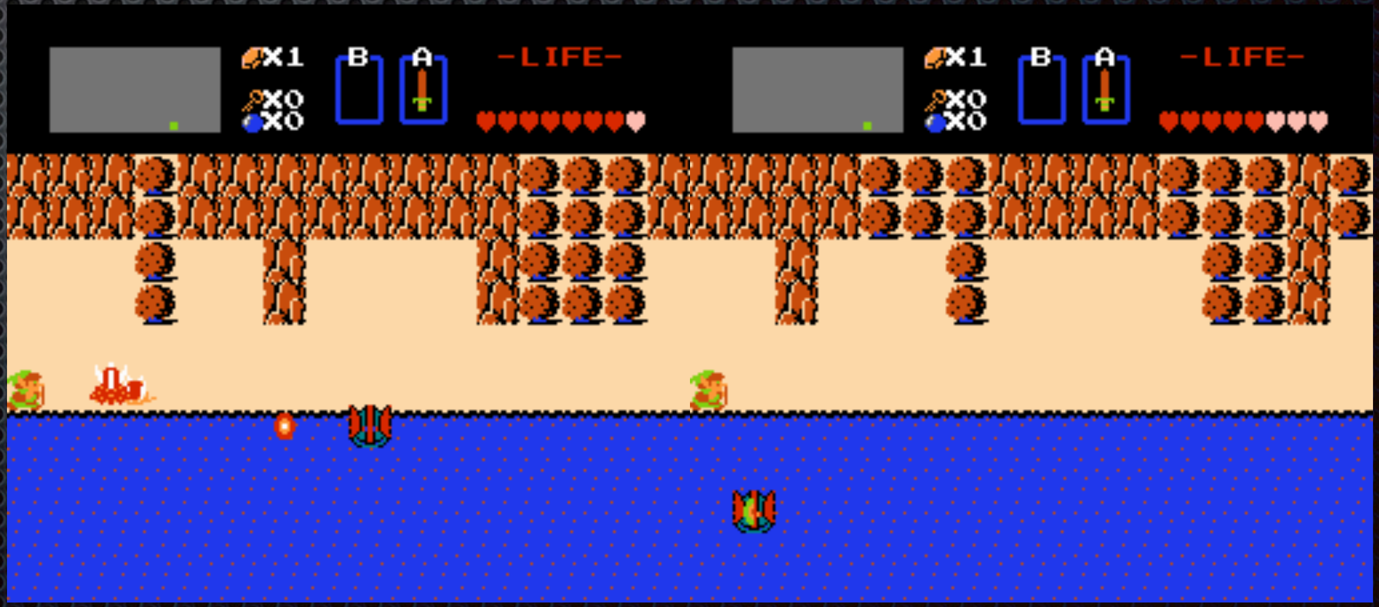
```
373344  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
373376  FFFFFFFF FF0000FF FF0000FF FF0000FF FFFFFFFF FF000000 FF0000FF FFFFFFF0
373408  FF000000 FF00FF00 FFF000FF FF0000FF FF000000 FF000000 FF0000FF FF0000FF
373440  FFFF0000 FFFF0000 FF0FF0FF FF0000FF FFFF0000 FF000000 FF0000FF FFFFFFF0
373472  FF000000 FF00FF00 FF000FFF 0FF00FF0 FF000000 FF000000 FF0000FF FF000000
373504  FFFFFFFF FF0000FF FF0000FF 000FF000 FFFFFFFF FFFFFFFF FFFFFFFF FF000000
373536  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

Stage Four: GEETIUYE

Game console hosting altered LoZ

- Hosted RetroPie v3.3.1 with ROM with modified maps in Southeastern corner and clue to the next stage
- Encoded using rock & cacti pattern using LoZ hex for alphabet, doubled up

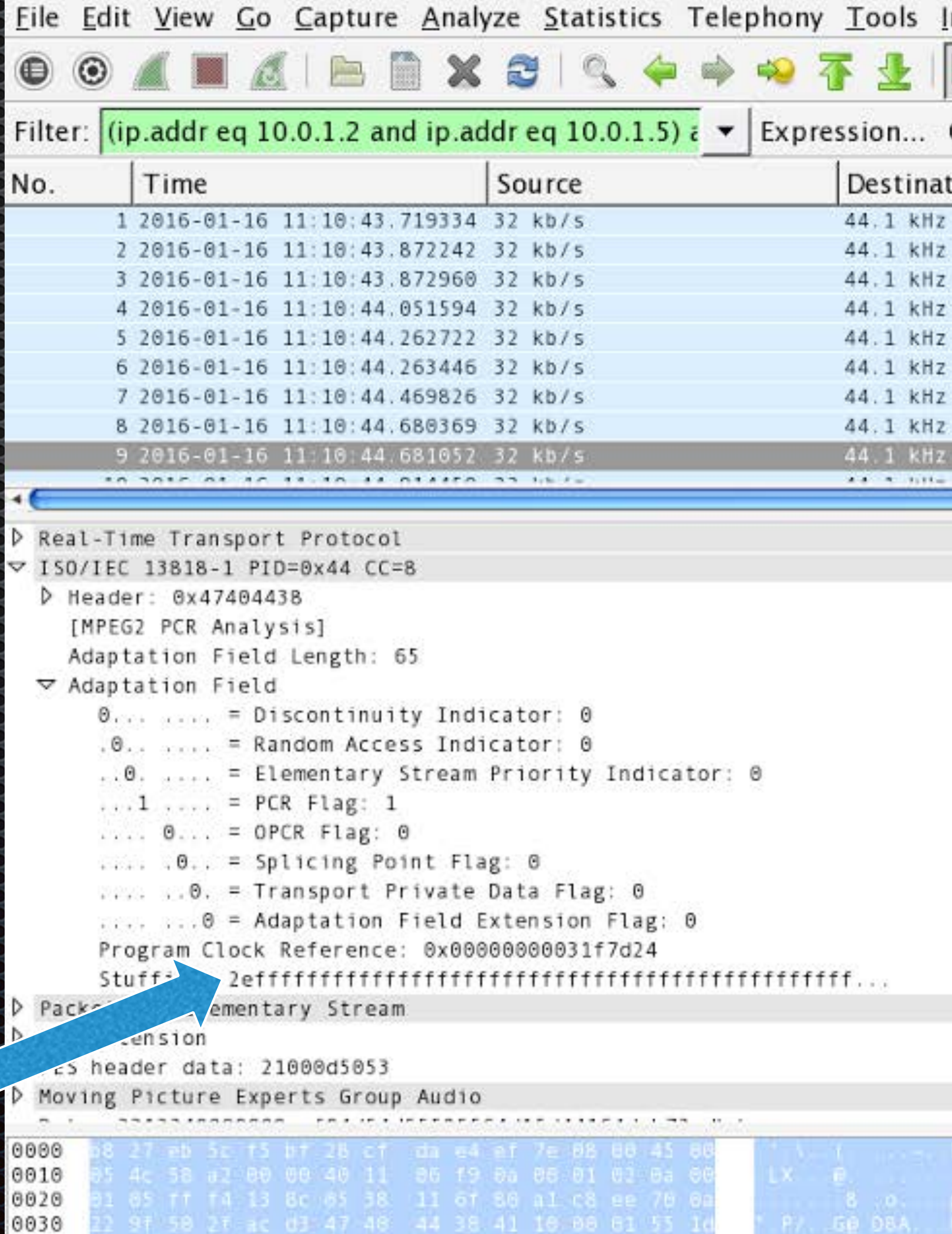




Stage Five: TZOLESEL

RTP stream with mod'd MPEG audio

- Adaptive "FF" stuffing in ISO header, spread over series of packets
- Used VLC to create stream, then scapy to alter it
    - Thanks ZEDD for LoZ music
- "Good job. Did you figure out how the codewords are **'NETDCCOEN'**?


File Edit View Go Capture Analyze Statistics Telephony Tools

Filter: (ip.addr eq 10.0.1.2 and ip.addr eq 10.0.1.5) a

```
No.      Time                          Source        Destinat
       1 2016-01-16 11:10:43.719334    32 kb/s       44.1 kHz
       2 2016-01-16 11:10:43.872242    32 kb/s       44.1 kHz
       3 2016-01-16 11:10:43.872960    32 kb/s       44.1 kHz
       4 2016-01-16 11:10:44.051594    32 kb/s       44.1 kHz
       5 2016-01-16 11:10:44.262722    32 kb/s       44.1 kHz
       6 2016-01-16 11:10:44.263446    32 kb/s       44.1 kHz
       7 2016-01-16 11:10:44.469826    32 kb/s       44.1 kHz
       8 2016-01-16 11:10:44.680369    32 kb/s       44.1 kHz
       9 2016-01-16 11:10:44.681052    32 kb/s       44.1 kHz
```

```
▷ Real-Time Transport Protocol
▽ ISO/IEC 13818-1 PID=0x44 CC=8
  ▷ Header: 0x4740443B
    [MPEG2 PCR Analysis]
    Adaptation Field Length: 65
  ▽ Adaptation Field
      0... .... = Discontinuity Indicator: 0
      .0.. .... = Random Access Indicator: 0
      ..0. .... = Elementary Stream Priority Indicator: 0
      ...1 .... = PCR Flag: 1
      .... 0... = OPCR Flag: 0
      .... .0.. = Splicing Point Flag: 0
      .... ..0. = Transport Private Data Flag: 0
      .... ...0 = Adaptation Field Extension Flag: 0
      Program Clock Reference: 0x00000000031f7d24
      Stuff    2efffffffffffffffffffffffffffffffffffffffffff...
▷ Pack        ementary Stream
▷      ension
   ES header data: 21000d5053
▷ Moving Picture Experts Group Audio
```

```
0000  b8 27 eb 5c f5 bf 2b cf  da e4 ef 7e 08 00 45 00
0010  05 4c 58 a2 00 00 40 11  06 f9 0a 00 01 02 0a 00   .LX...@.
0020  01 05 ff f4 13 8c 05 38  11 6f 80 a1 c8 ee 70 0a   .......8 .o....p.
0030  22 9f 58 2f ac d3 47 40  44 38 41 10 00 01 53 1d   ".X/..G@ D8A...S.
```

What was the theme?

GameGenie codes…

sorta

Codewords are anagrammed!

1: AVVLAUSZ
2: SGOLNSEE
3: EKNVELUP
4: GEETIUYE
5: TZOLESEL

A real GameGenie code for Legend of Zelda

Made-up codes using GameGenie-valid letters (so you can't just guess them!)

stegogeekseventuallysolveanelusivepuzzle

Stego geeks eventually solve an elusive puzzle

Very Special Thanks

PRAXIS
ENGINEERING

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

Special Thanks

- **Nintendo,** for not suing our pants off
- **ROMHacking.net,** for a great collection of NES tools
- **Marco Ramilli**, for an off-the-shelf Javascript steg tool
- **RetroPie,** for making the console easy to set up
- **Python,** for answering our con' scripting prayers
- **UberShirts,** for another great last minute turnaround
- **Not Just Signs,** for sweet sign-printing magic
- **Our Wives,** for tolerating our annual hiatus
- **Bruce & Heidi,** for tolerating our endless shenanigans

shmooganography@gmail.com

Presentation will be available on
the contest website soon.

Shirt orders due by 15 February.
$25/each. Email us.