



20 teams this year!

As of 1300

Team	Codes Found	Discovered Relationship between Codewords
Team FDG	1 2 3 4 5	NO
pwnEIP	1 2 3 4 5	NO
Avengers	1 2 3 4 5	NO
Flowers By Irene	1 2 3 4 5	NO
Three blind mice	1 2 3 4 5	NO
Too Many Hobbies	1 2 3 4 5	NO
Krusty Krabs	1 2 3 4 5	NO
Team Memeware	1 2 3 4 5	NO
Moose&Penguin	1 2 3 4 5	NO
SuperDuper	1 2 3 4 5	NO
stormflight	1 2 3 4 5	NO

11 Passed Stage 1!

7 Passed Stage 2!

5 Passed Stage 3!

Stage Prizes:

1: pwnEIP

2: pwnEIP

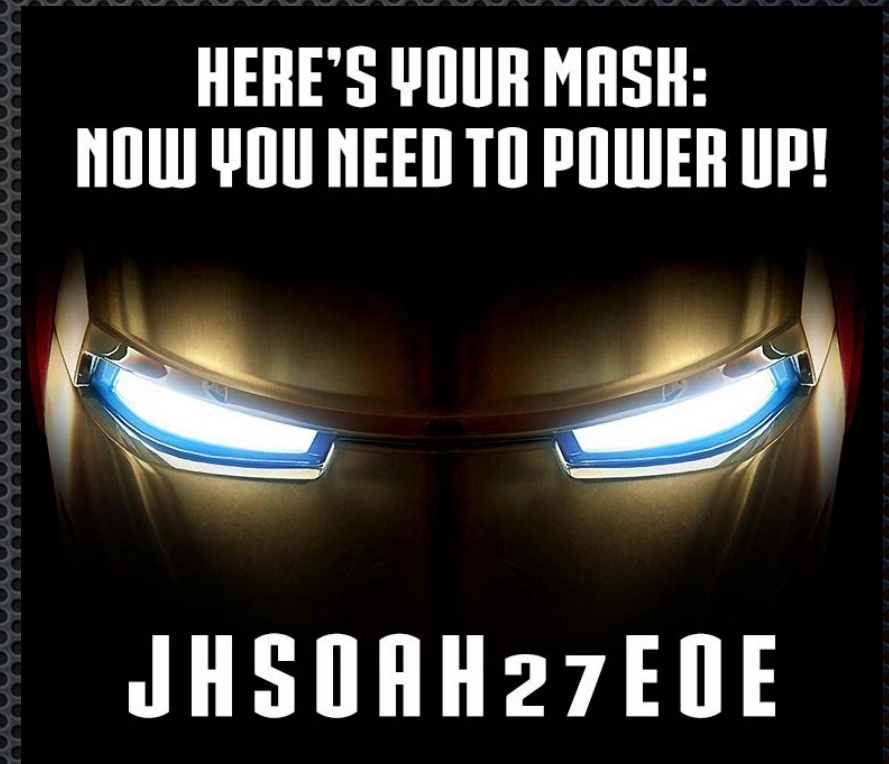
3: Team FDG

4: pwnEIP

No one figured out the codeword relationship!

Stage One: JHSOAH27EOE iPad-enabled Mirror (Smile!) & Mask

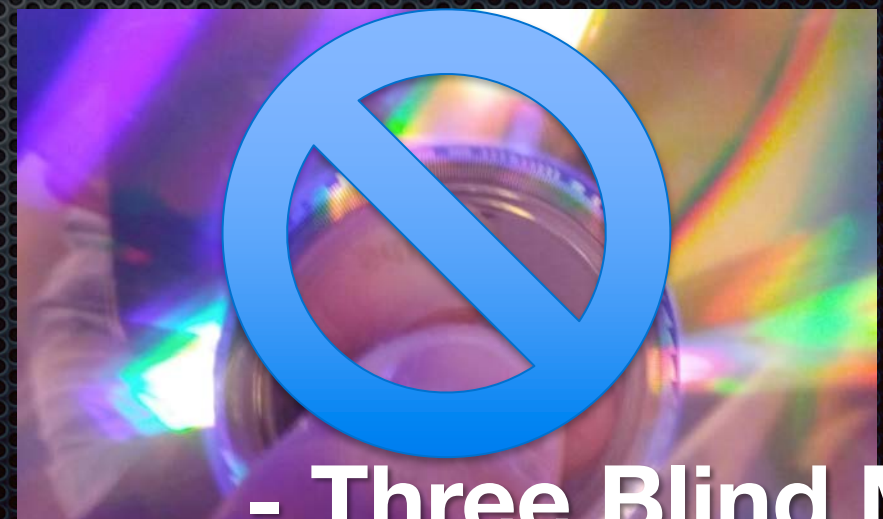
- Overtly, just a part of the hotel furnishing (but plugged in)
- Repurposed SquareCam-Swift to recognize faces and present mask graphic through mirror
- Must *smile* to trigger display of mask and code
- Thanks for not stealing our iPad (before we tethered it)



Stage Two: E0INNU0HCST

Arc Reactor Light (Under) Scribe CD-R

- Used crappy LightScribe drive on over-priced discs to etch the top
- Simply peel the label (in shreds) to reveal the message
- It was not the encoded marks on the central ring of the disk (our budget isn't that big)



- Three Blind Mice

Stage Three: RMLINDEAHKO

Font Corruption in Threat Letter PDF

- Disc contained a number of random Iron Man and contest references (remember the Stargate?)
- PDF had various fonts used, but some were modified in the PDF markup
- Codeword was part of the erroneous tags

t0 th3 LOser – (yea shmarK, this is for you)

I have intercepted your communications and monitoring all your moves. You can't hide behind your mask anymore. The hackers you deploy are just pathetic recruits allying to pad their wallets with bug bounties. Most of them still live in their mom's basement! You are so far behind my technology regime that it is laughable. Quit now. Stop embarrassing yourself.

Do **NOT** get in **MY** way.

hydrA

Copy & Paste

!0 t"3 los#r – (yea shmark, this is \$or you)

I have intercepted your communications and (monitoring all your moves. You can't hide behind your mas) anymore#. The hackers *ou +employ are just pathetic, #cruits all -ying to pad th#ir w&.le!s wit" bug bounty#s. /o0t of th#m sti.l li-# in their mom'0 basement! You are so \$a, behind my techn1logy regi(e !hat it is laugh"able. Qu2t 'ow. Stop emb&rrass2ng you, self.

Do NOT get in my way.

hydra

Inspect PDF Markup

```

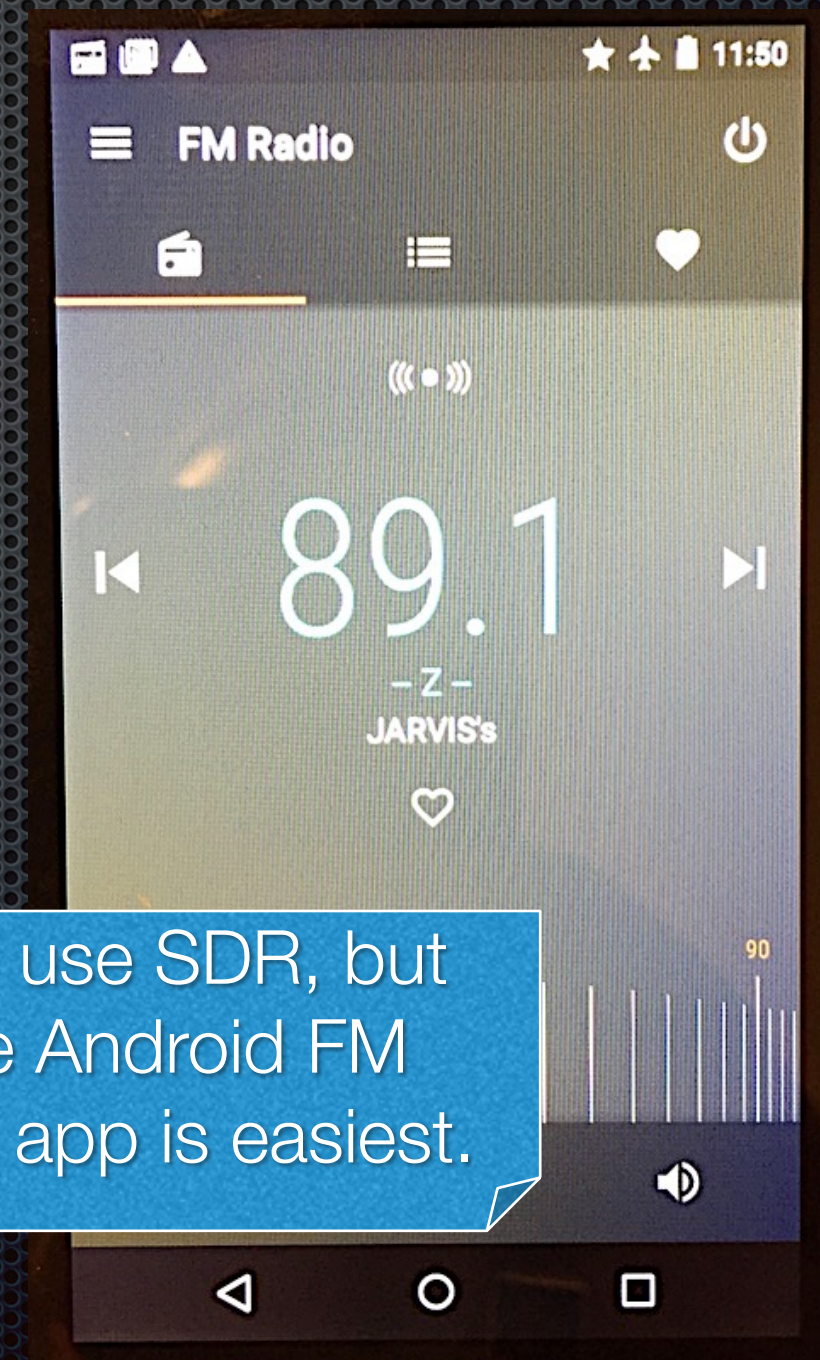
9 0 obj
<< /Type /Font /Subtype /TrueType /BaseFont /TLZLOH+Cambria-Bold /FontDescriptor
212 0 R /ToUnicode 213 0 R /FirstChar 33 /LastChar 50 /Widths [ 365 597 531
326 469 535 604 890 592 531 597 461 531 308 846 459 569 314 ] >>
endobj
213 0 obj
<< /Length 214 0 R /RMLINDEAHK0 /FlateDecode >>
stream
x^A]<92>Ën<83>0^PE÷p
/ÛE<84>×<81>×%<84>T¥<8a>Ä¢^0<95>ö^CÀ^^"KAXÆYÖ÷½a□00ÄY^\\_I^L^I<90>^]<9b>çÆÙ(³÷0é<96>
^<84>×<94>Û^GJæ^X^Vùöð!<9e>^^ùì-^X
ñ_ö_d_äq_v+M!íÄûö^7ÉÉÖD7KÇÇ_..òùvñ$_00_vòUç^D_çV:Ä/äçö$M^0*äLkz?24ûNÇäI_00_0vT7_0_d_Mu

```


Stage Four: IIECO2XZEEN

Raspberry Pi Broadcasting FM RDS

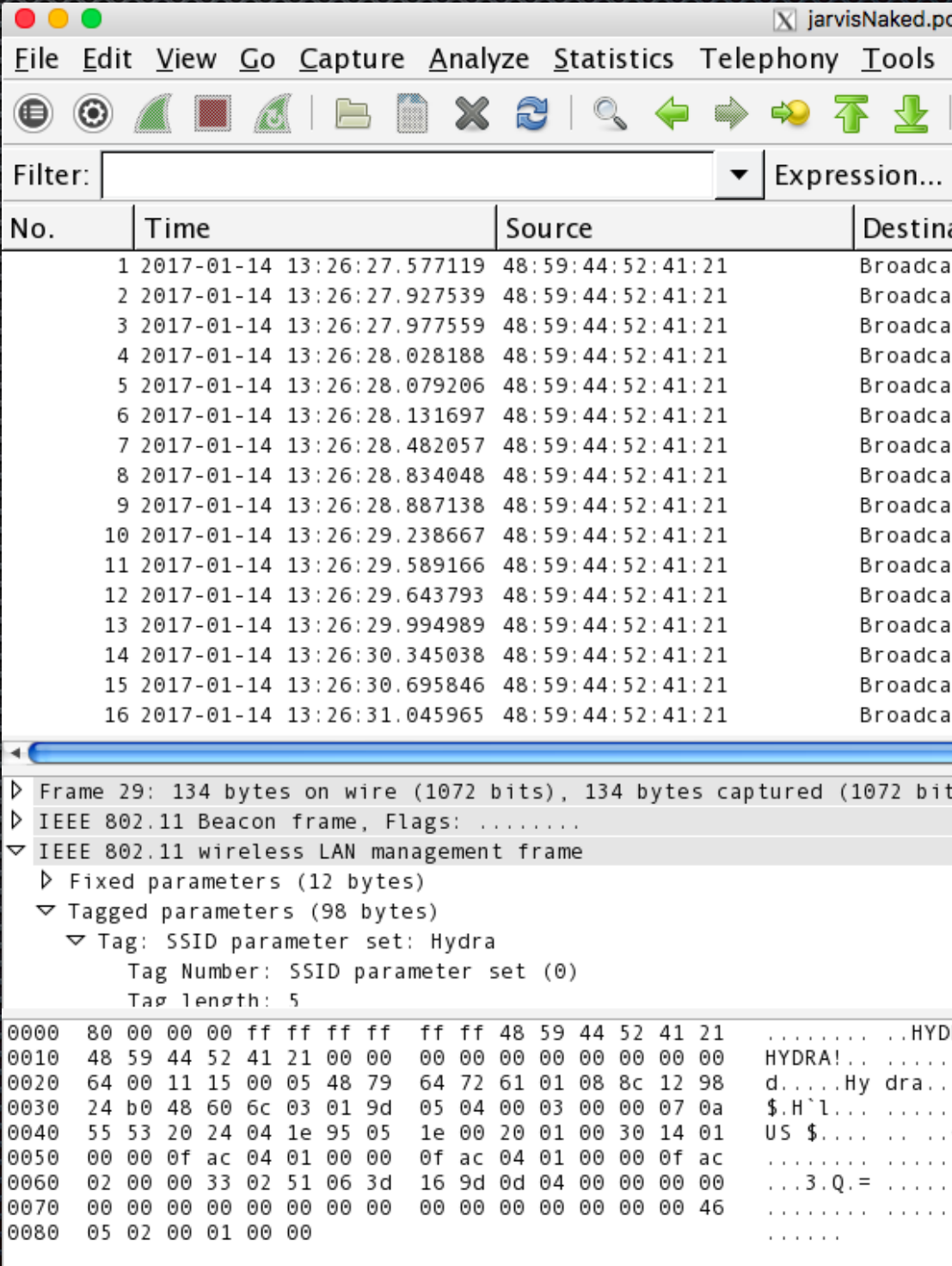
- Used PiFmRds project to emit FM signal on GPIO 4 on Raspberry Pi 2 @ 89.1Mhz
- Audio is just Whiplash (Ivan) clip from Iron Man 2 on loop
- RDS Text contains codeword and clue in 10 second increments
- Don't tell the FCC



Stage Five: CSSCNOOTXL!

Curious WiFi Traffic

- Inspired by packet timing steg research by *anfractuusus*
- Applied time delay routine to “broadcast” of WiFi beacon packets to encode binary
- 0 was ~50ms
- 1 was ~350ms
- 816 beacon packets total



jarvisNaked.pc

File Edit View Go Capture Analyze Statistics Telephony Tools

Filter: Expression...

No.	Time	Source	Destination
1	2017-01-14 13:26:27.577119	48:59:44:52:41:21	Broadcast
2	2017-01-14 13:26:27.927539	48:59:44:52:41:21	Broadcast
3	2017-01-14 13:26:27.977559	48:59:44:52:41:21	Broadcast
4	2017-01-14 13:26:28.028188	48:59:44:52:41:21	Broadcast
5	2017-01-14 13:26:28.079206	48:59:44:52:41:21	Broadcast
6	2017-01-14 13:26:28.131697	48:59:44:52:41:21	Broadcast
7	2017-01-14 13:26:28.482057	48:59:44:52:41:21	Broadcast
8	2017-01-14 13:26:28.834048	48:59:44:52:41:21	Broadcast
9	2017-01-14 13:26:28.887138	48:59:44:52:41:21	Broadcast
10	2017-01-14 13:26:29.238667	48:59:44:52:41:21	Broadcast
11	2017-01-14 13:26:29.589166	48:59:44:52:41:21	Broadcast
12	2017-01-14 13:26:29.643793	48:59:44:52:41:21	Broadcast
13	2017-01-14 13:26:29.994989	48:59:44:52:41:21	Broadcast
14	2017-01-14 13:26:30.345038	48:59:44:52:41:21	Broadcast
15	2017-01-14 13:26:30.695846	48:59:44:52:41:21	Broadcast
16	2017-01-14 13:26:31.045965	48:59:44:52:41:21	Broadcast

Frame 29: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0

IEEE 802.11 Beacon frame, Flags:

IEEE 802.11 wireless LAN management frame

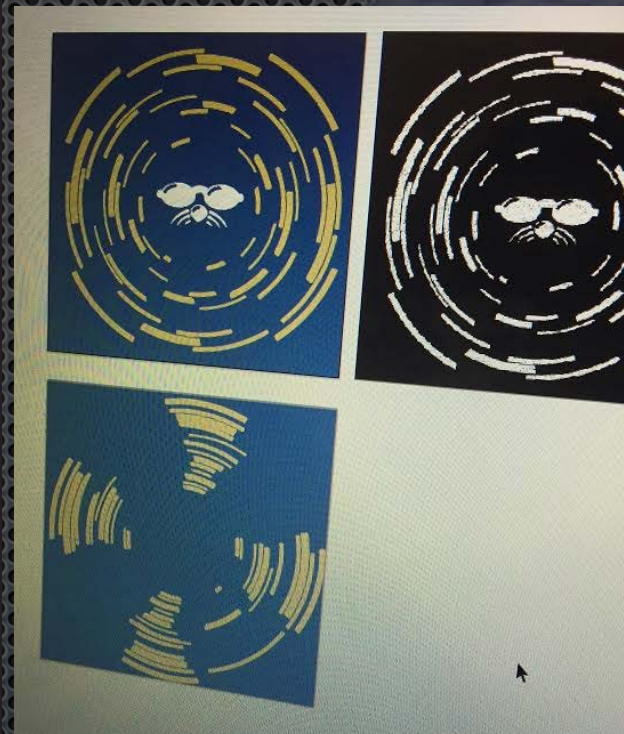
- Fixed parameters (12 bytes)
- Tagged parameters (98 bytes)
 - Tag: SSID parameter set: Hydra
 - Tag Number: SSID parameter set (0)
 - Tag length: 5

Offset	Hex	ASCII
0000	80 00 00 00 ff ff ff ff ff ff 48 59 44 52 41 21HYD
0010	48 59 44 52 41 21 00 00 00 00 00 00 00 00 00 00	HYDRA!..
0020	64 00 11 15 00 05 48 79 64 72 61 01 08 8c 12 98	d....Hy dra..
0030	24 b0 48 60 6c 03 01 9d 05 04 00 03 00 00 07 0a	\$.H`l...
0040	55 53 20 24 04 1e 95 05 1e 00 20 01 00 30 14 01	US \$....
0050	00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac
0060	02 00 00 33 02 51 06 3d 16 9d 0d 04 00 00 00 00	...3.Q.=
0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 46
0080	05 02 00 01 00 00

Bonus Stage: Our shirts

Code 128 Barcode Made Circular

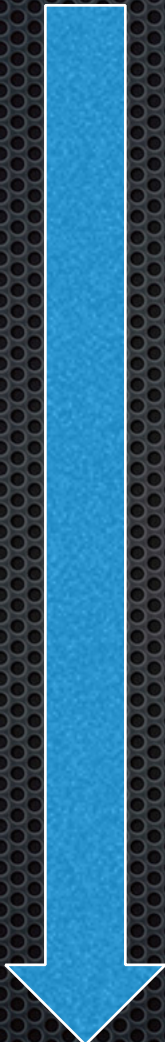
- Modeled after JARVIS graphics in Iron Man films



PwnEIP was
so close!



How were the codewords related?



JH SOAH27EOE
EO INNU0HCST
RM LINDEAHKO
IE CO2XZEEN
CS SCN00TXL!

Reorder the letters to reveal
Stark Industries Weapons:

JERICH0 MISSILE

SONIC CANNON

HUD 2020 EX07

HAZTECH

EXOSKELETON!

Very Special Thanks



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

Special Thanks

- **Marvel Comics**, for not suing our pants off
- **NicBow Design Works**, for our cool shirt graphics
- **No Starch Press**, for coordinating gift certificates
- **King & Union**, for Aaron and Matt watching our mirror
- **UberShirts**, for another great last minute turnaround
- **Not Just Signs**, for super last-minute sign-printing
- **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. No... really this time.