Shmooganography 5

How we did it

And how most of you didn’t

What **wasn't** involved

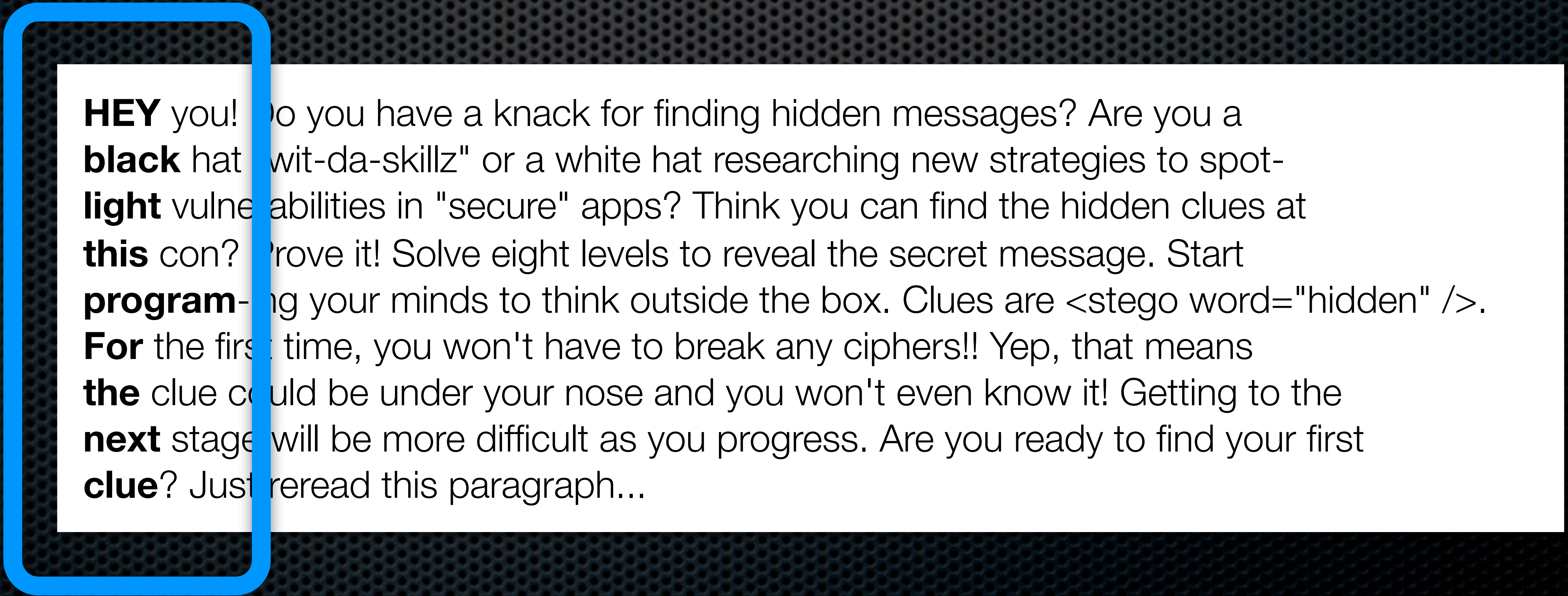
- We did not do the badges
- We did not leave ciphers in the program
- We did not hide messages on the program cover
- We did not hide anything in the pens, this year
- Ended late night phone calls to Bruce/Heidi

Who got the most right?

The Mobile Disco

Stage One:
HEY

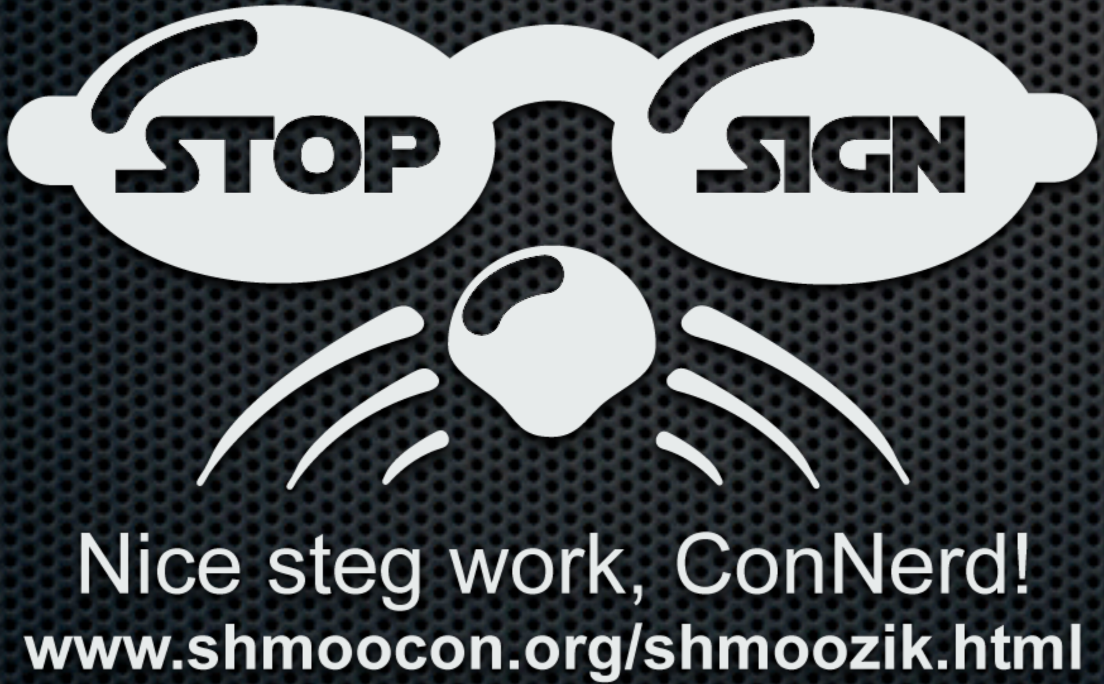
- Just needed to read the contest description vertically to reveal clue
- Requires literacy and ability to follow directions

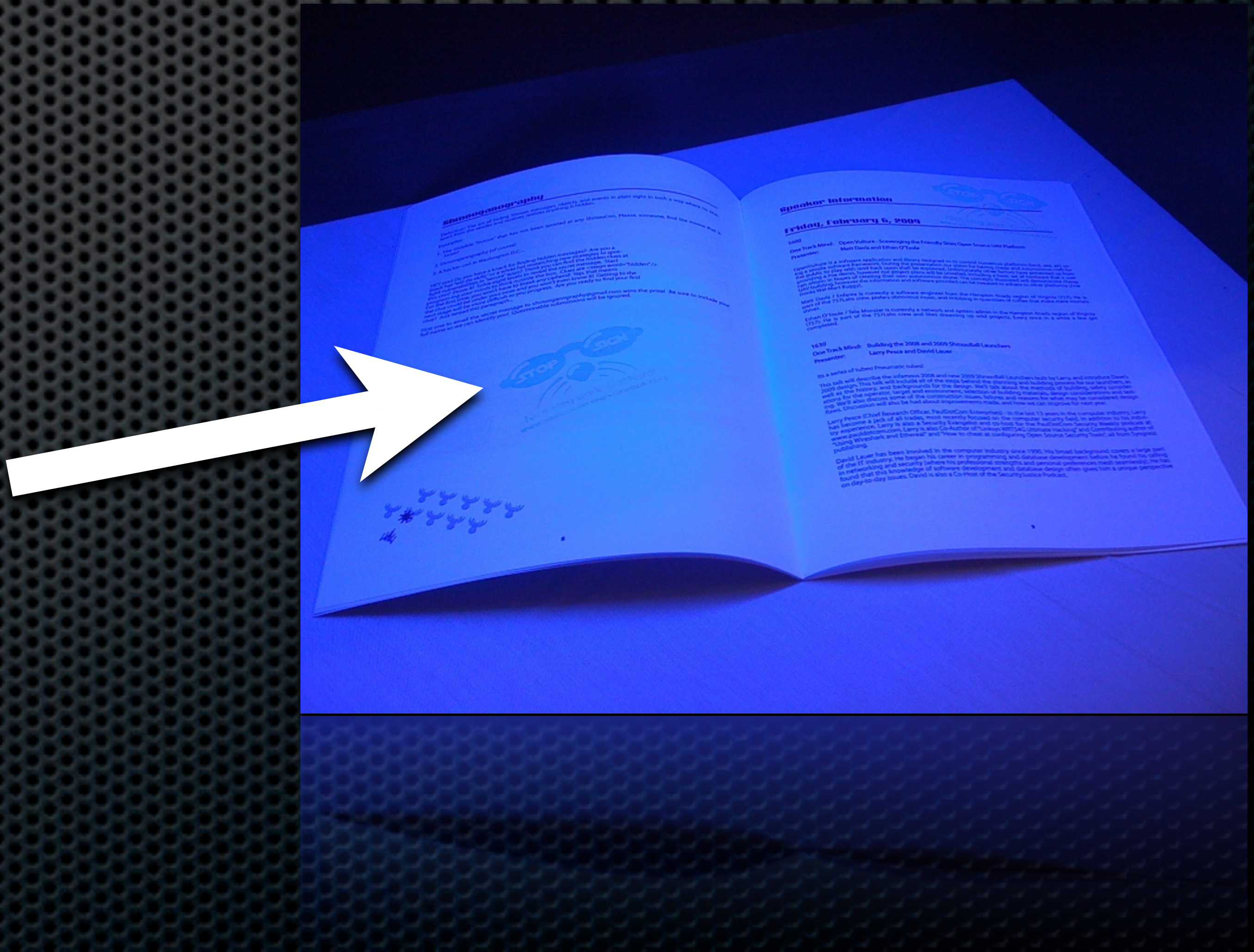


HEY you! Do you have a knack for finding hidden messages? Are you a
black hat "wit-da-skillz" or a white hat researching new strategies to spot-
light vulnerabilities in "secure" apps? Think you can find the hidden clues at
this con? Prove it! Solve eight levels to reveal the secret message. Start
program-ming your minds to think outside the box. Clues are <stego word="hidden" />.
For the first time, you won't have to break any ciphers!! Yep, that means
the clue could be under your nose and you won't even know it! Getting to the
next stage will be more difficult as you progress. Are you ready to find your first
clue? Just reread this paragraph...

Stage Two:
STOP SIGN

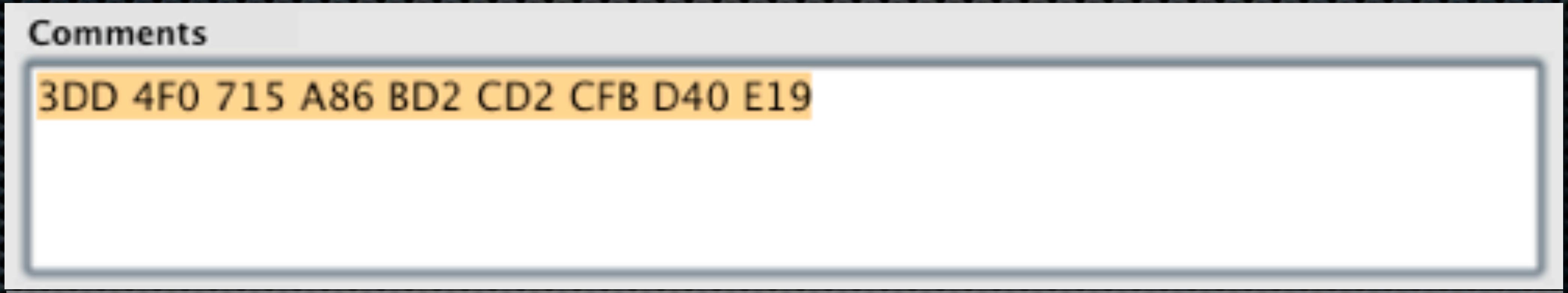
- Revealed only under blacklight/UV
- Used alcohol based ink and rubber stamps, applied by hand





Stage Three: **THANK YOU**

- Nugget was in the MP3 comment field, which were hex byte offsets into the file (see, nothing fancy)

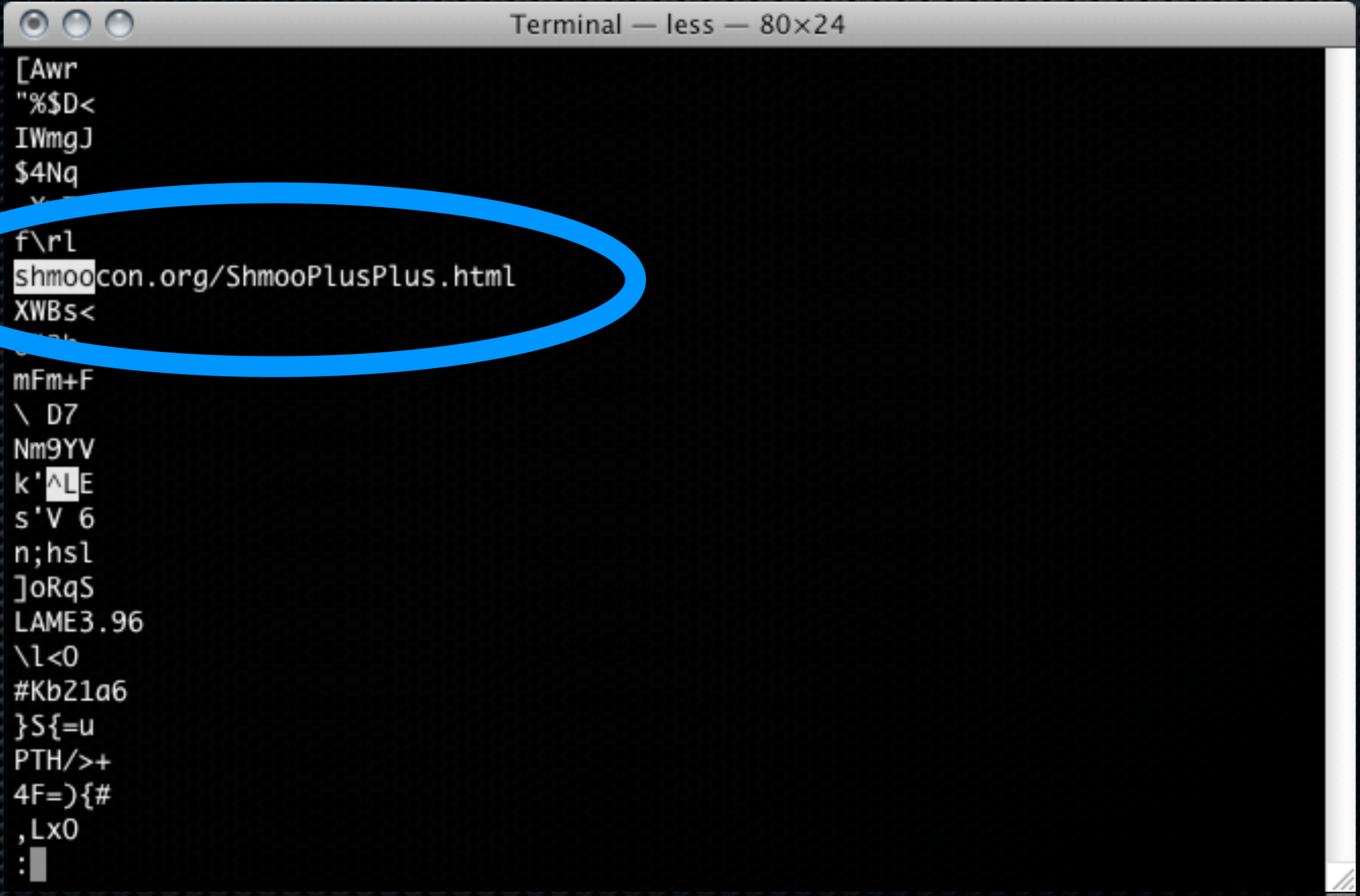


Comments

3DD 4F0 715 A86 BD2 CD2 CFB D40 E19

- The clue was just a web address hidden in some a random padding field
  - Easily found using `strings` or a hex editor

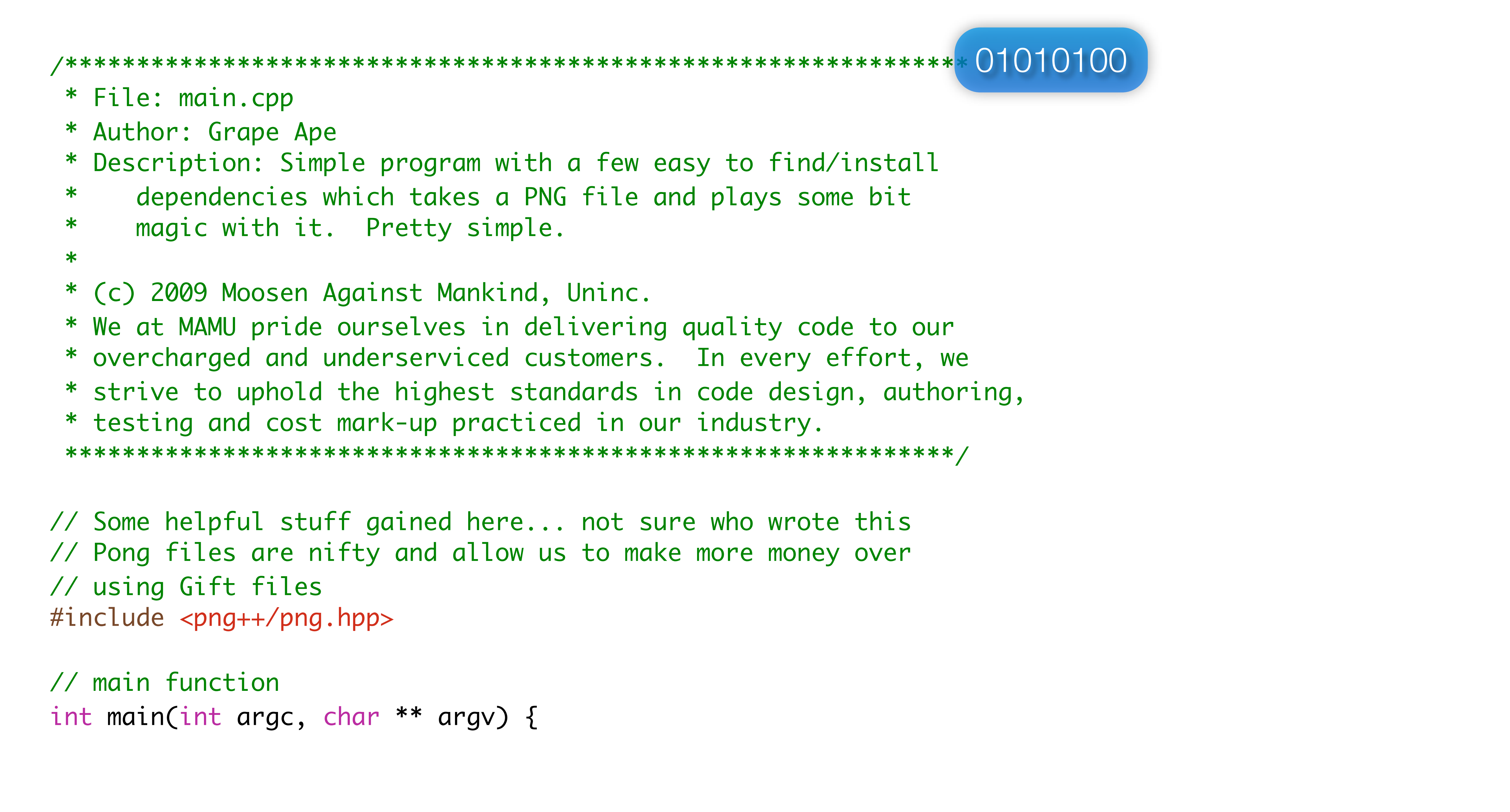
strings Inkarnit_WatchMeFade.mp3 | less



```
[Awr
"%$D<
IWmgJ
$4Nq
[illegible]
f\rl
shmoocon.org/ShmooPlusPlus.html
XWBs<
[illegible]
mFm+F
\ D7
Nm9YV
k'^LE
s'V 6
n;hsl
]oRqS
LAME3.96
\l<0
#Kb21a6
}S{=u
PTH/>+
4F=){#
,Lx0
:
```

Stage Four:
TURN AROUND

- Nugget and clue both encoded as ASCII binary hidden as tabs/spaces at the end of each line
- Could be hand solved, but Python is sexier
- Says “TURN AROUND, Smoke is filling the Con! Our advice: stay close to the floor.”
  - Just a PC blasting 802.11 frames with SSID “~smoke~” — when it was online
  - That’s why you couldn’t connect, Mobile Disco



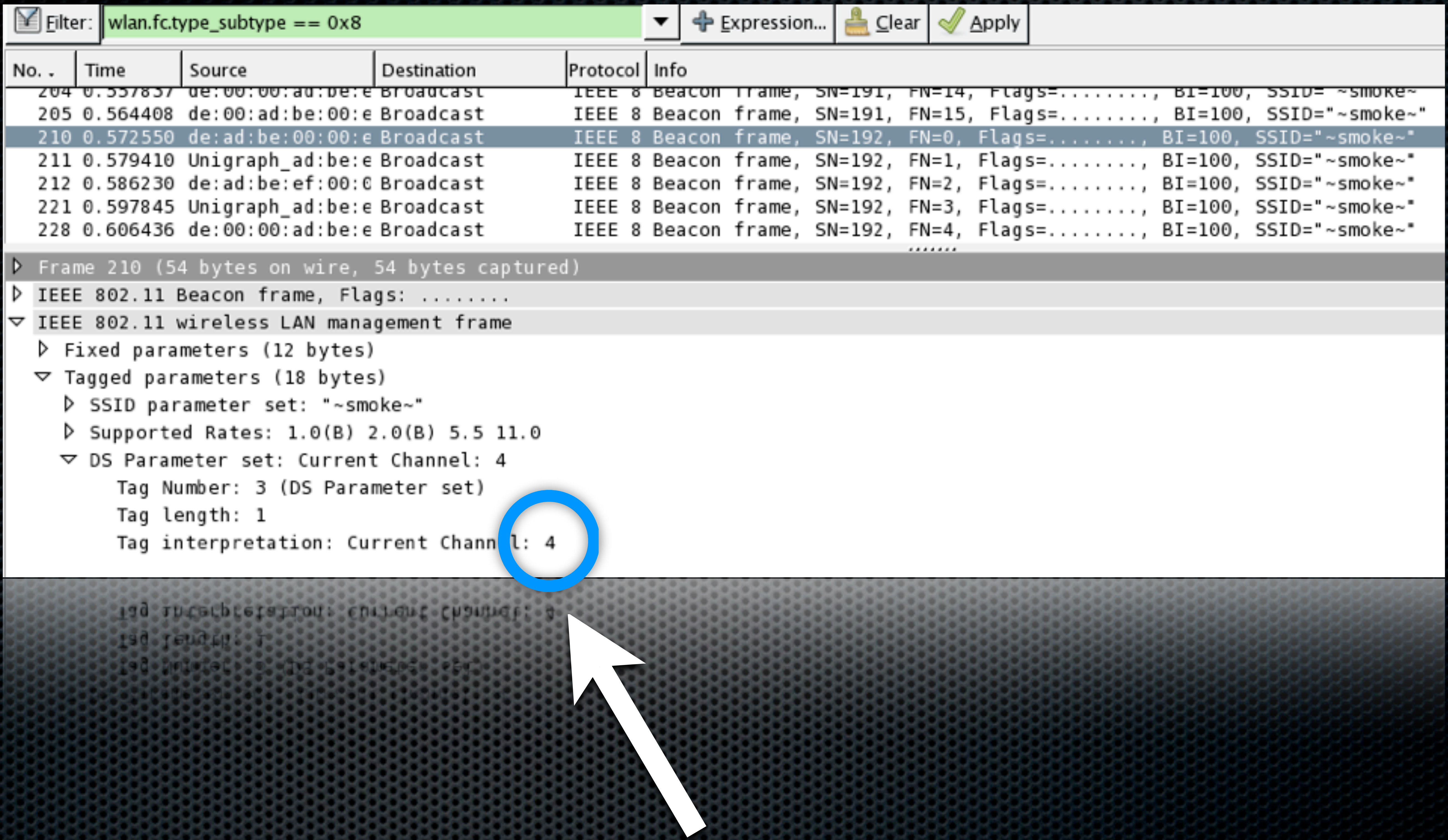
```
/***************************************************************
 * File: main.cpp
 * Author: Grape Ape
 * Description: Simple program with a few easy to find/install
 *    dependencies which takes a PNG file and plays some bit
 *    magic with it.  Pretty simple.
 *
 * (c) 2009 Moosen Against Mankind, Uninc.
 * We at MAMU pride ourselves in delivering quality code to our
 * overcharged and underserviced customers.  In every effort, we
 * strive to uphold the highest standards in code design, authoring,
 * testing and cost mark-up practiced in our industry.
 **************************************************************/

// Some helpful stuff gained here... not sure who wrote this
// Pong files are nifty and allow us to make more money over
// using Gift files
#include <png++/png.hpp>

// main function
int main(int argc, char ** argv) {
```

spaces — 0

tabs — 1

Stage Five:
DOING DOING

- Nugget and clue encoded as octal ASCII in the channel number of each Beacon frame.
  - Offset by one: there’s no such thing as Channel 0
- All packets transmitted on 2.437Mhz, not jumping
- Clue references “smoke rising,” meaning “look at a higher layer”
  - Same packets, but next stage at a higher Layer



Filter: wlan.fc.type_subtype == 0x8

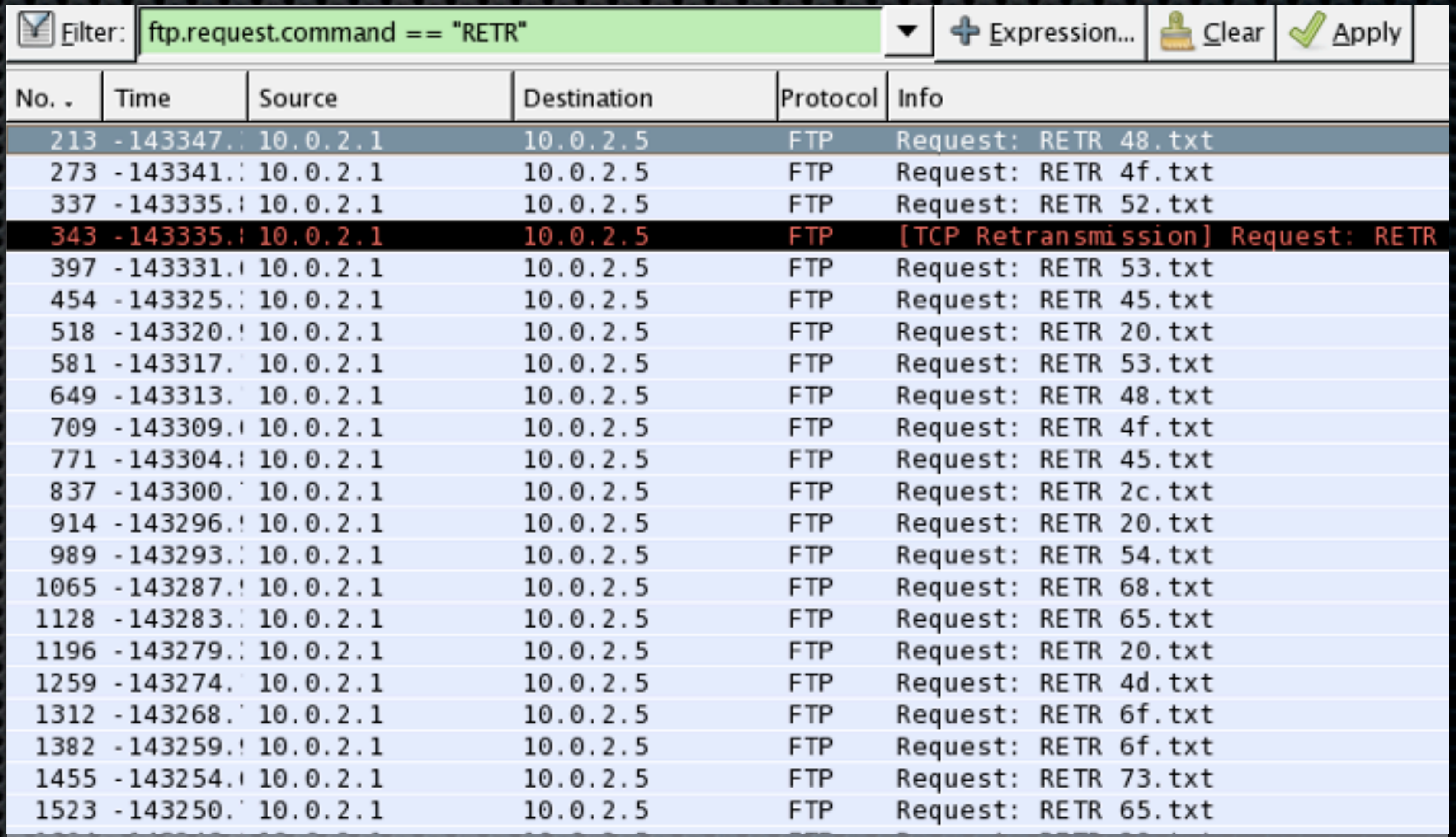
```
No. .  Time      Source           Destination     Protocol  Info
204 0.557857 de:00:00:ad:be:e Broadcast  IEEE 8 Beacon frame, SN=191, FN=14, Flags=........, BI=100, SSID="~smoke~"
205 0.564408 de:00:ad:be:00:e Broadcast  IEEE 8 Beacon frame, SN=191, FN=15, Flags=........, BI=100, SSID="~smoke~"
210 0.572550 de:ad:be:00:00:e Broadcast  IEEE 8 Beacon frame, SN=192, FN=0, Flags=........, BI=100, SSID="~smoke~"
211 0.579410 Unigraph_ad:be:e Broadcast  IEEE 8 Beacon frame, SN=192, FN=1, Flags=........, BI=100, SSID="~smoke~"
212 0.586230 de:ad:be:ef:00:0 Broadcast  IEEE 8 Beacon frame, SN=192, FN=2, Flags=........, BI=100, SSID="~smoke~"
221 0.597845 Unigraph_ad:be:e Broadcast  IEEE 8 Beacon frame, SN=192, FN=3, Flags=........, BI=100, SSID="~smoke~"
228 0.606436 de:00:00:ad:be:e Broadcast  IEEE 8 Beacon frame, SN=192, FN=4, Flags=........, BI=100, SSID="~smoke~"
```

```
▷ Frame 210 (54 bytes on wire, 54 bytes captured)
▷ IEEE 802.11 Beacon frame, Flags: ........
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▽ Tagged parameters (18 bytes)
    ▷ SSID parameter set: "~smoke~"
    ▷ Supported Rates: 1.0(B) 2.0(B) 5.5 11.0
    ▽ DS Parameter set: Current Channel: 4
        Tag Number: 3 (DS Parameter set)
        Tag length: 1
        Tag interpretation: Current Channel: 4
```

Read Channel Number in order from “~smoke~”

Stage Six:
HORSE SHOE

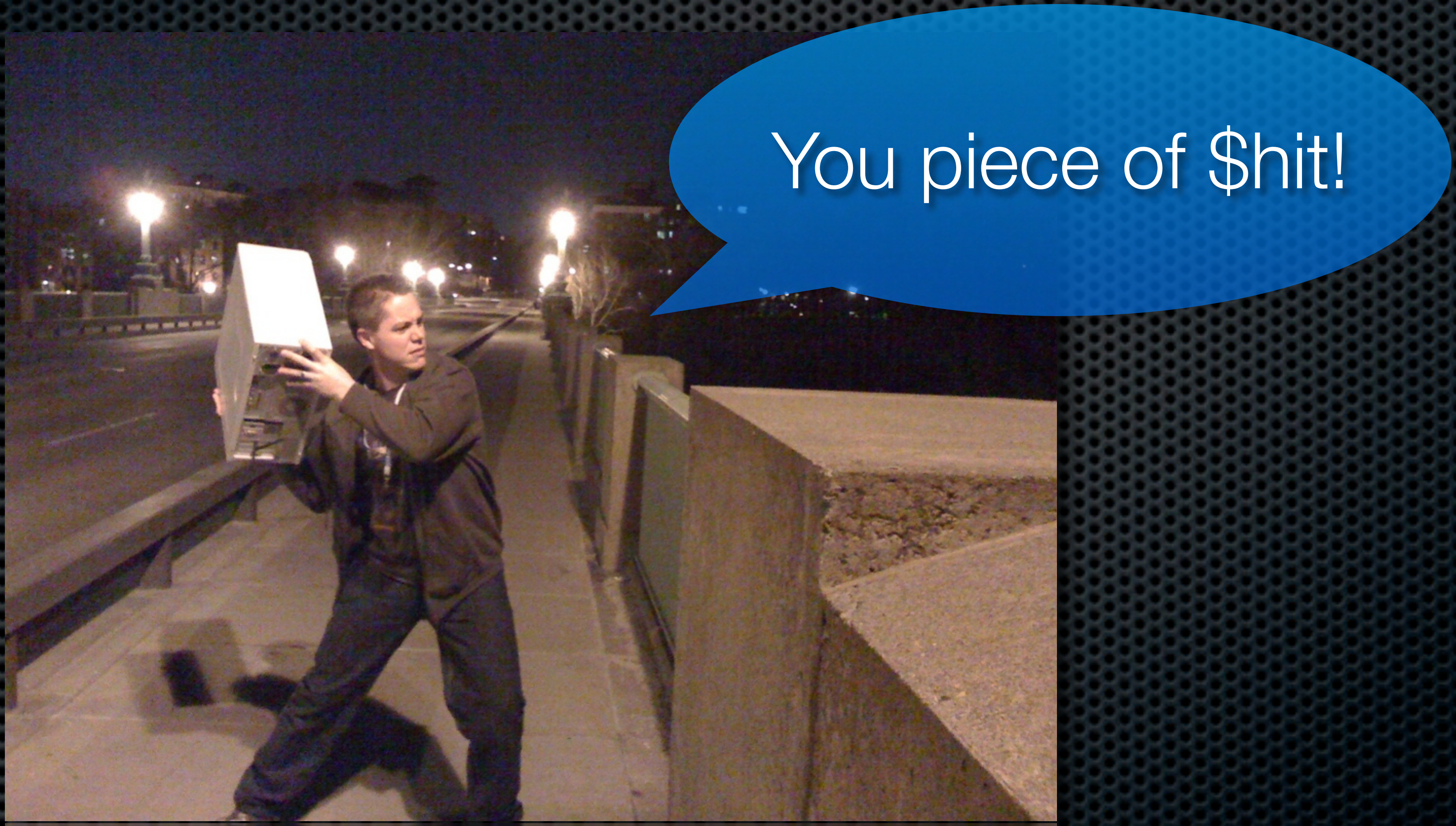
- Nugget and clue hidden as FTP’d files
- File names were ASCII hex
- “The Moose is feeling lucky. Perhaps CL can help with a DC hookup?”



Filter: ftp.request.command == "RETR"

No.	Time	Source	Destination	Protocol	Info
213	-143347.	10.0.2.1	10.0.2.5	FTP	Request: RETR 48.txt
273	-143341.	10.0.2.1	10.0.2.5	FTP	Request: RETR 4f.txt
337	-143335.	10.0.2.1	10.0.2.5	FTP	Request: RETR 52.txt
343	-143335.	10.0.2.1	10.0.2.5	FTP	[TCP Retransmission] Request: RETR
397	-143331.	10.0.2.1	10.0.2.5	FTP	Request: RETR 53.txt
454	-143325.	10.0.2.1	10.0.2.5	FTP	Request: RETR 45.txt
518	-143320.	10.0.2.1	10.0.2.5	FTP	Request: RETR 20.txt
581	-143317.	10.0.2.1	10.0.2.5	FTP	Request: RETR 53.txt
649	-143313.	10.0.2.1	10.0.2.5	FTP	Request: RETR 48.txt
709	-143309.	10.0.2.1	10.0.2.5	FTP	Request: RETR 4f.txt
771	-143304.	10.0.2.1	10.0.2.5	FTP	Request: RETR 45.txt
837	-143300.	10.0.2.1	10.0.2.5	FTP	Request: RETR 2c.txt
914	-143296.	10.0.2.1	10.0.2.5	FTP	Request: RETR 20.txt
989	-143293.	10.0.2.1	10.0.2.5	FTP	Request: RETR 54.txt
1065	-143287.	10.0.2.1	10.0.2.5	FTP	Request: RETR 68.txt
1128	-143283.	10.0.2.1	10.0.2.5	FTP	Request: RETR 65.txt
1196	-143279.	10.0.2.1	10.0.2.5	FTP	Request: RETR 20.txt
1259	-143274.	10.0.2.1	10.0.2.5	FTP	Request: RETR 4d.txt
1312	-143268.	10.0.2.1	10.0.2.5	FTP	Request: RETR 6f.txt
1382	-143259.	10.0.2.1	10.0.2.5	FTP	Request: RETR 6f.txt
1455	-143254.	10.0.2.1	10.0.2.5	FTP	Request: RETR 73.txt
1523	-143250.	10.0.2.1	10.0.2.5	FTP	Request: RETR 65.txt

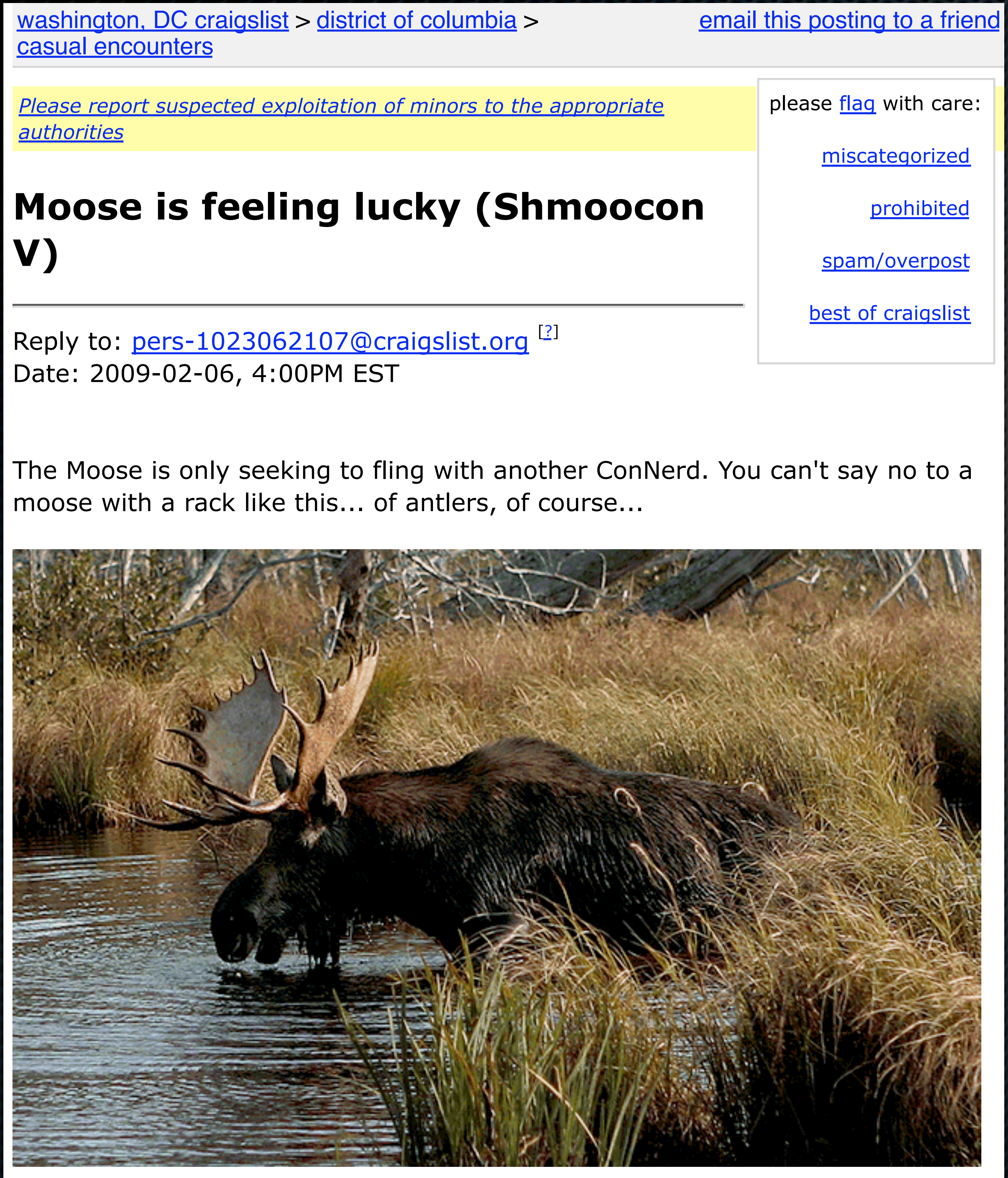
Time for Plan B...



- Don’t tell the hotel we borrowed their computer.

Stage Seven: **TURTLE**

- CL == Craig's List
- Searching for "moose" or "shmoocon" reveals some tickets for sale, and a horny moose
- Image has an embedded image not visible.
- Use GrapeApe's code to decode image
- Clue tells you to make sure you're in the right room



washington, DC craigslist > district of columbia > casual encounters

email this posting to a friend

Please report suspected exploitation of minors to the appropriate authorities

please flag with care:

miscategorized

prohibited

spam/overpost

best of craigslist

Moose is feeling lucky (Shmoocon V)

Reply to: pers-1023062107@craigslist.org [?]
Date: 2009-02-06, 4:00PM EST

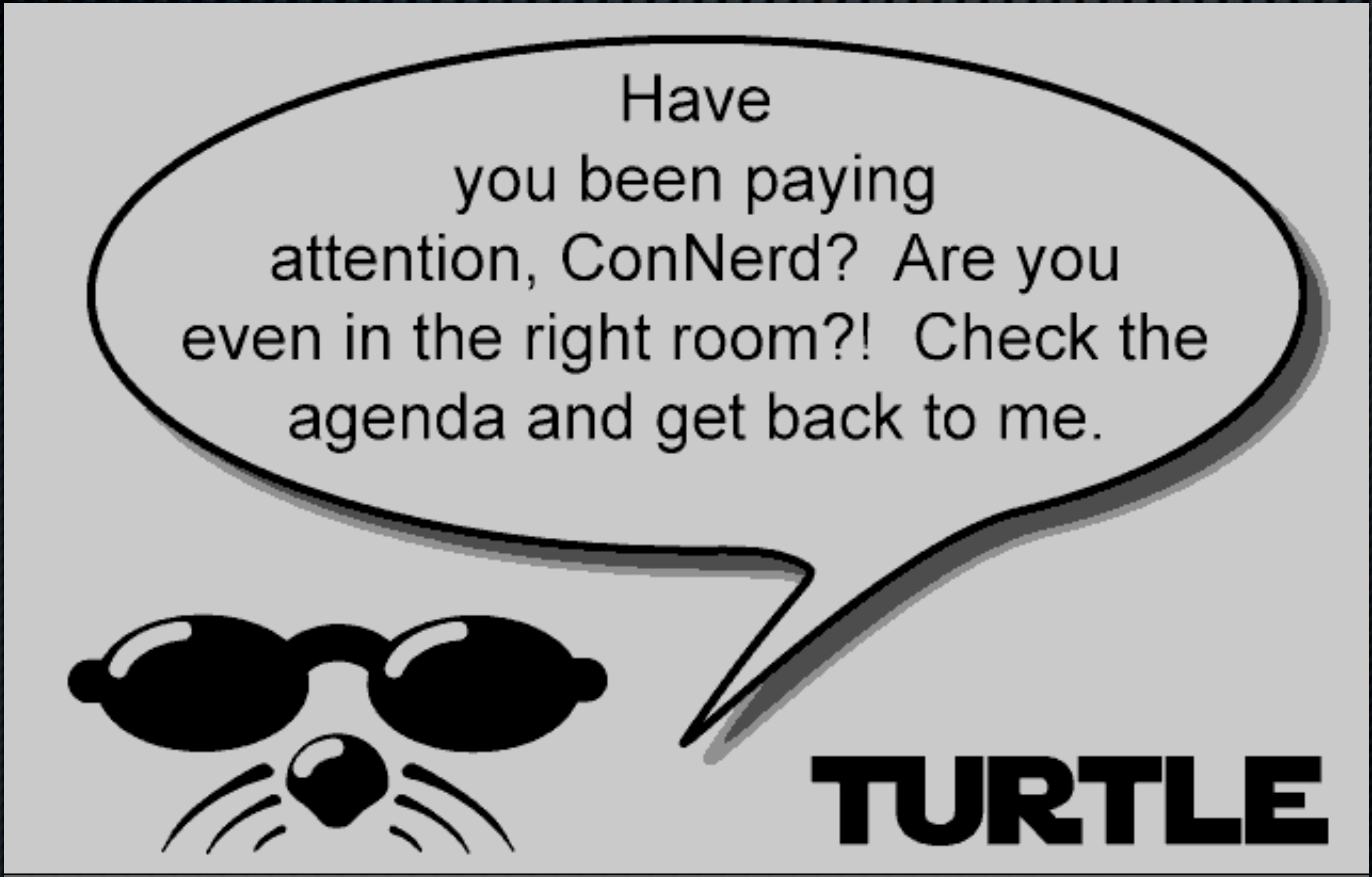
The Moose is only seeking to fling with another ConNerd. You can't say no to a moose with a rack like this... of antlers, of course...

"Nice rack."

Matthew

+

Have you been paying attention, ConNerd? Are you even in the right room?! Check the agenda and get back to me.
TURTLE


Have you been paying attention, ConNerd? Are you even in the right room?! Check the agenda and get back to me.
TURTLE

Stage Eight:
UGGA DIGGA DIGGA DIGGA

- Bottom of each room agenda sign has binary with ASCII hex behind it
  - Binary says “ShMoGaNoGrApHy”
  - Hex reveals no clue, just the last nugget

ShmooCon 2009

Break It!

Saturday February 7th, 2009

1000	Exploring Novel Ways in Building Botnets	Rey / Mende
1100	Pulling a John Connor: Defeating Android	Charlie Miller
1200	Hack the Genome! The Age of Bimolecular Cryptology	R. Mark Adams
1300	Lunch (on your 0wn)	
1400	Blinded by Flash: Widespread Security Risks Flash Developers Don't See	Prajakta Jagdale
1500	802.11 ObgYn or "Spread Your Spectrum"	Rick Farina
1600	All Your Packets Are Belong To Us: Attacking Backbone Technologies	Rey / Mende
1700	The Fast-Track Suite: Advanced Penetration Techniques Made Easy	David Kennedy

Sunday February 8th, 2009

1000	Re-Playing with (Blind) SQL Injection	Alonso / Palako
1100	RFID Unplugged	3ric Johanson
1200	0wn the Con	The Shmoo Group

596F7520666F756E6420697421
4765742074686656D20616C6C21

You found it!   Get them all!

4865726527732074686520317374
55474741204449474741

Here's the 1st   UGGA DIGGA

416E6420746865206C617374
4449474741204449474741

And the last   DIGGA DIGGA

So, the full message was:

HEY, STOP SIGN, THANK YOU, TURN AROUND, DOING DOING, HORSE SHOE, TURTLE, UGGA DIGGA DIGGA DIGGA

WTF?

Special Thanks

- **Bruce, Heidi & Pete**, for building the blacklight boxes and coordinating the programs and signs
- **John & Tamzen**, for helping stamp 1600 programs
- **Inkarnit**, for some free MP3 music
- **BillBarrettsGuideService.com**, for a random moose picture found with Google Images
- **Craig's List**, for giving a moose a chance for love
- **Jeff Dunham & Peanut**, for inspiring this year's message

“I'm not sure that the horse shoe from a lucky feeling moose fits on the foot of a seahorse semen volt, but I am willing to bet they won't get past the stop sign.”

- Justin

WARNING: Do not operate Gmail when drinking on an open tab.

shmooganography@gmail.com