ShmooCon 8 Badge Puzzle

Darth Null, January 2012

I like crypto puzzles

ShmooCon Hall Pass

Date: JAN 28–30, 2011

Name: SPEAKER

0 One track mind 0 Build it

0 Break it 0 Bring it on

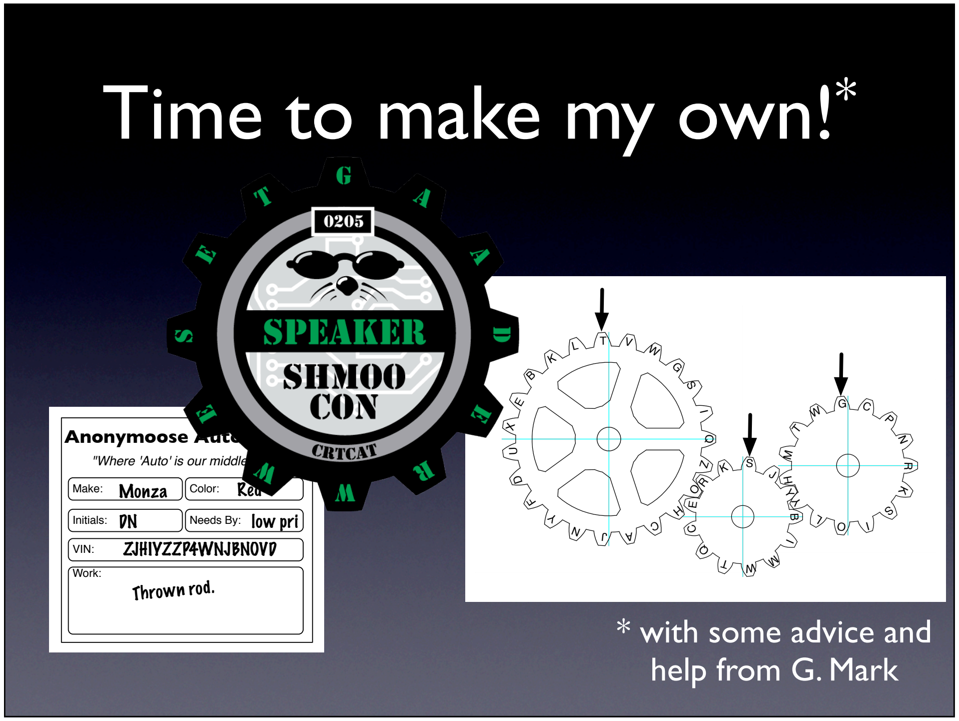
Reason: LOST VOICE ON ALCAN

Signature: A. NOONY MOOSE

I've always liked puzzles. I used to do a lot of GeoCaching, and always enjoyed the puzzle caches where I had to decrypt something or do some other crazy math or magic to find the final coordinates.

In 2009, I got sucked into a rabbit hole for days trying to solve G. Mark Hardy's ShmooCon V badge puzzle, and after that I've solved a whole bunch, including "playing from home" for at least four conferences.

I've tried to document most of my successes at www.darthnull.org. (I'm a little slower at writing up the failures, but I'll get to them, too, eventually).



Time to make my own!*

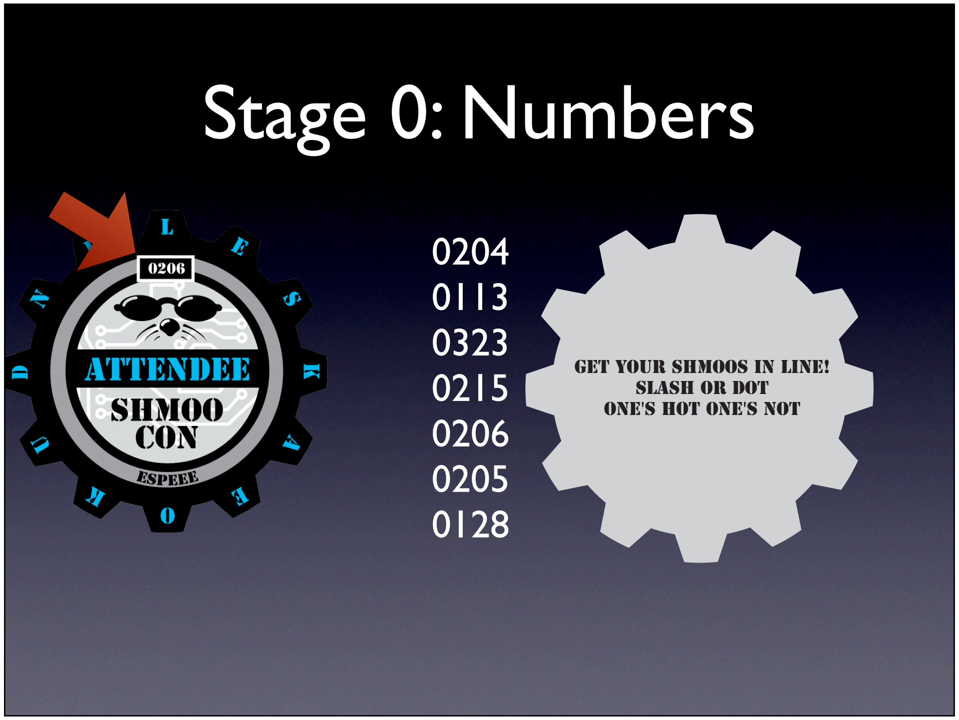
Anonymoose Auto

"Where 'Auto' is our middle

Make: Monza	Color: Red
Initials: DN	Needs By: low pri
VIN: ZJHIYZZP4WNJBNOVD	
Work: Thrown rod.	

* with some advice and help from G. Mark

So after winning three ShmooCons in a row (I'd swear I heard someone say "Again!?!" when my name was announced last year), I asked Heidi if I could do the contest this year. She agreed to take a look at what I come up with, and after a lot of back and forth with her, and a lot of good advice and suggested changes from G. Mark, I had my first puzzle published!



Stage 0: Numbers

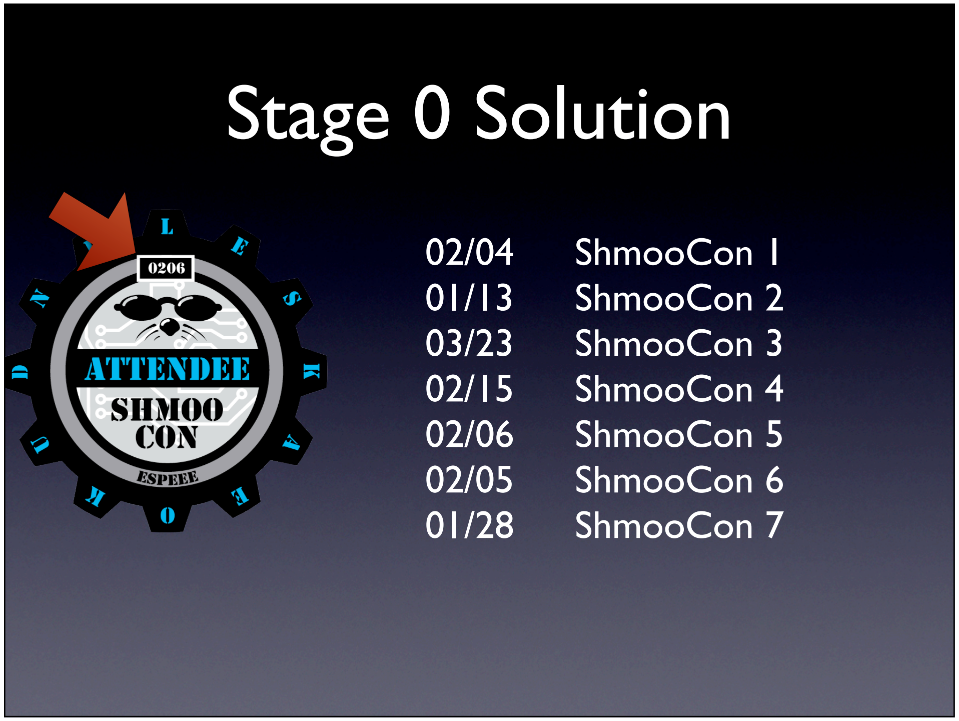
0204
0113
0323
0215
0206
0205
0128

GET YOUR SHMOOS IN LINE!
SLASH OR DOT
ONE'S HOT ONE'S NOT

So the puzzle included five different stages, with information on badges and in several locations within the program. The first stage isn't strictly necessary, but once suggested kind of stuck 'cause it was so much fun.

Originally, I'd considered a stick-shift motif to number the badges, or pips on fuzzy dice, but G. Mark came up with a crazy four-digit index system.

To help people get started, the hint "Slash or Dot" was included in the program. The idea here was to get people to think "hm..what if I add a slash to these numbers?...."



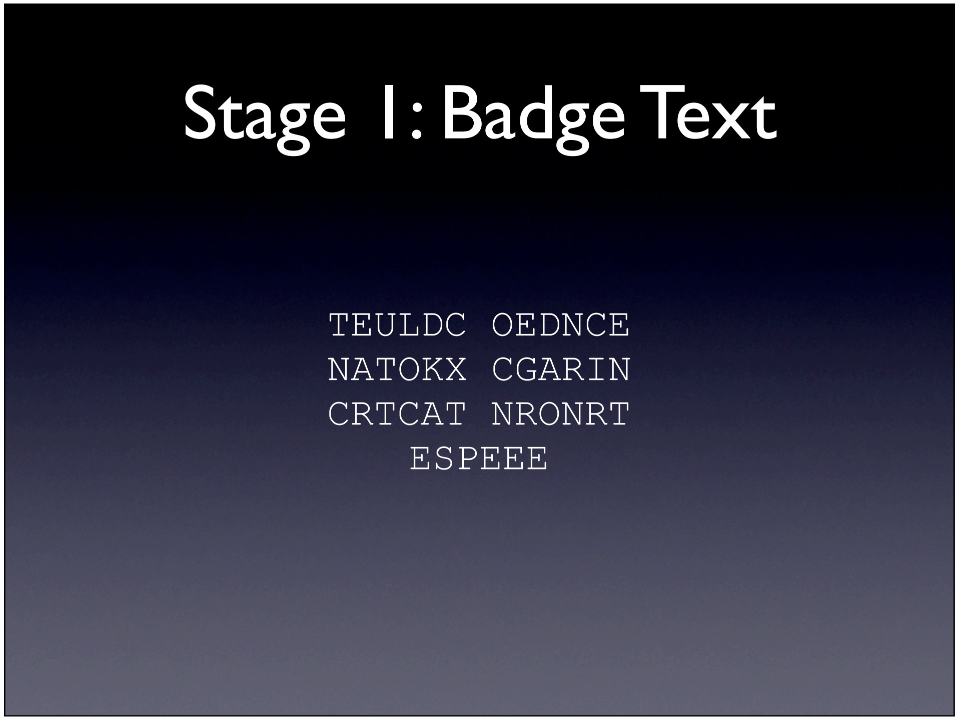
Stage 0 Solution

0206
ATTENDEE
SHMOO
CON
ESPEEE
L E S K A E O K U D N

02/04	ShmooCon 1
01/13	ShmooCon 2
03/23	ShmooCon 3
02/15	ShmooCon 4
02/06	ShmooCon 5
02/05	ShmooCon 6
01/28	ShmooCon 7

If you include a slash, then the numbers look a lot like dates. If you realize that this con started on 1/27...then you might recognize that one of these numbers was pretty close to that date. Which, hopefully, would get you searching for past ShmooCon dates...

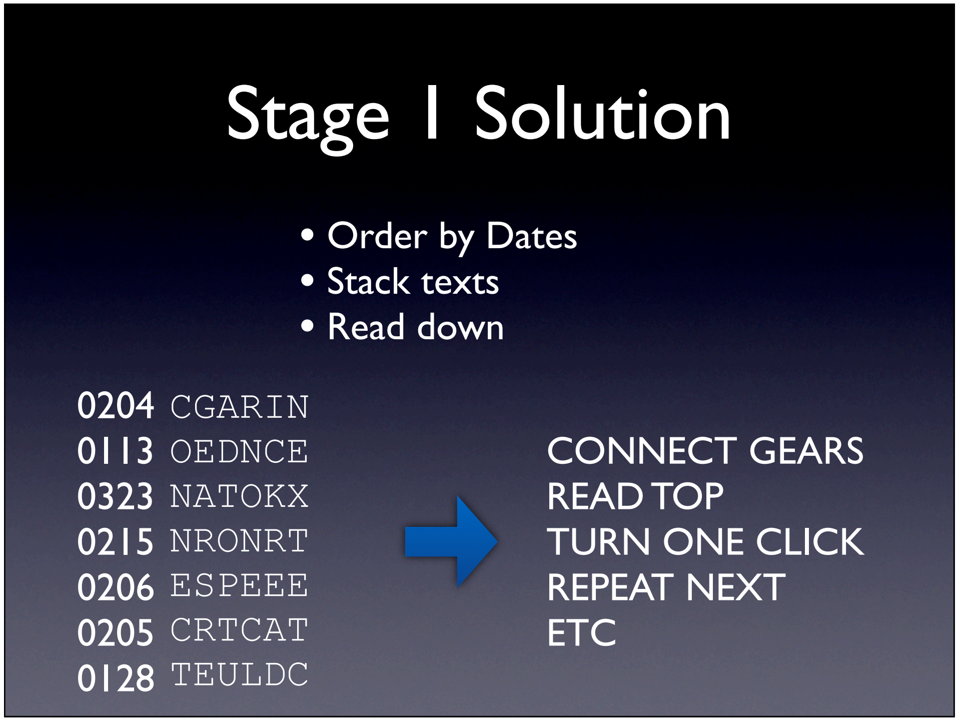
Once you've put years with all the dates, you have the proper order for the badges. But what does that do for you?



Stage 1: Badge Text

```
TEULDC OEDNCE
NATOKX CGARIN
CRTCAT NRONRT
    ESPEEE
```

Here's the text from the bottom of all seven badges. It's actually encrypted with a Columnar Transposition Cipher, but since the "delivery order" of the badges isn't really set, it's more like a random scramble. Anyway, you take these text strings....



Stage 1 Solution

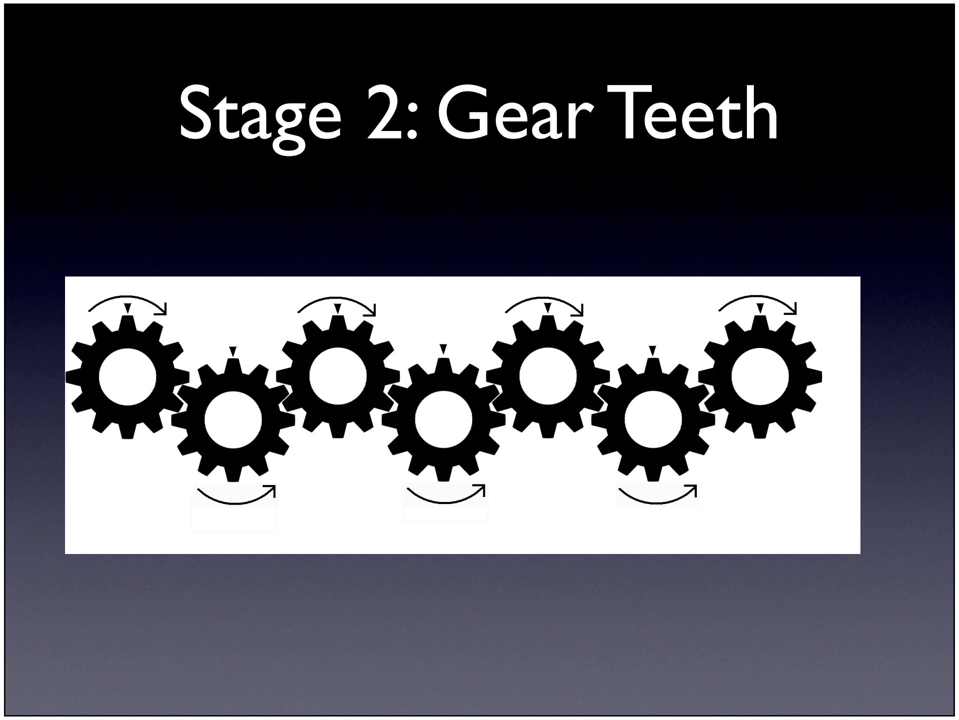
- Order by Dates
- Stack texts
- Read down

0204	CGARIN
0113	OEDNCE
0323	NATOKX
0215	NRONRT
0206	ESPEEE
0205	CRTCAT
0128	TEULDC

CONNECT GEARS
READ TOP
TURN ONE CLICK
REPEAT NEXT
ETC

...and stack them one on top of the other, in the same order as the badge dates. Read down each column, to get the message. This tells you what to do for the next stage, as the mechanics of stage 2 are arbitrary and specific to this puzzle (any idea you could come up with would be just as valid as the one we used).

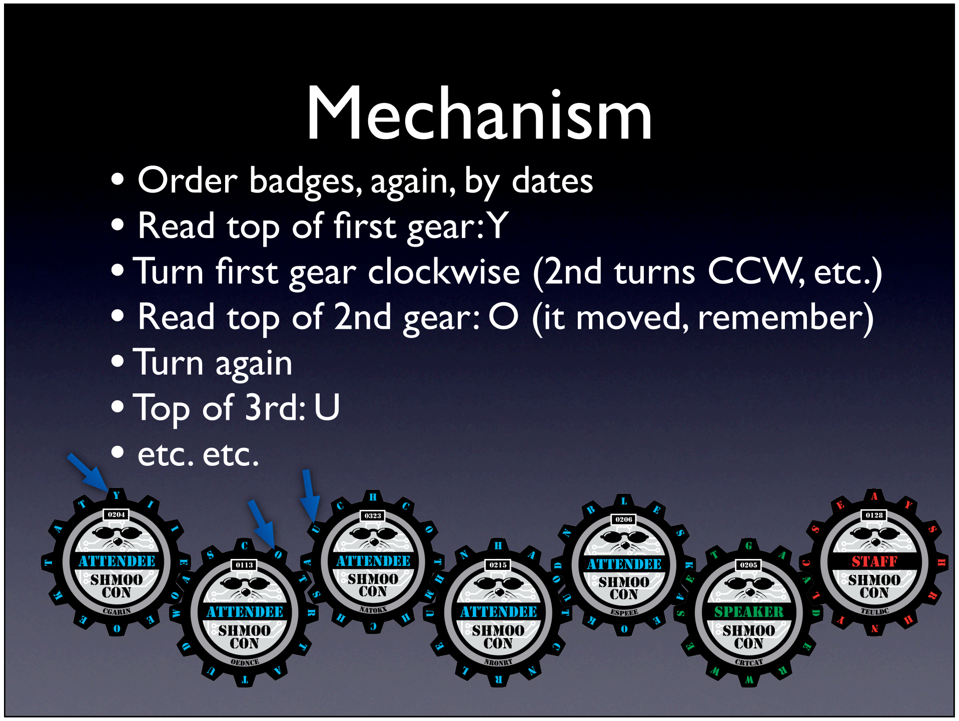
I don't think anyone simply stacked the strings and tried to form words. If they had, they could've skipped the index numbers altogether. Looking at the last column, E and T are repeated, so you'd just have to anagram "C, E, N, T, and X" -- which should have quickly given NEXT", and "GEAR" or "GSAR" in the 2nd column (depending on which rows they use). This might've actually saved people a LOT of time. Sorry, guys. :)



Stage 2: Gear Teeth

In the program was this image, intended to help people figure out how to line up the badges (if you put them in a straight line, then the three middle badges would be rotated by a half-tooth and the machine wouldn't work right). It also had the side effect of revealing just how many badges there were.

Heidi and I had brainstormed that this might be a neat way to work with badges, if they chose badges with teeth on them (it wasn't decided at the time). I even said it'd be great to see people cutting out paper badges, tacking them to cardboard, and spinning them, but didn't really expect it to happen. G. Mark revived the idea, and came up with the read/turn/move & read/turn/etc. method of using this particular machine.

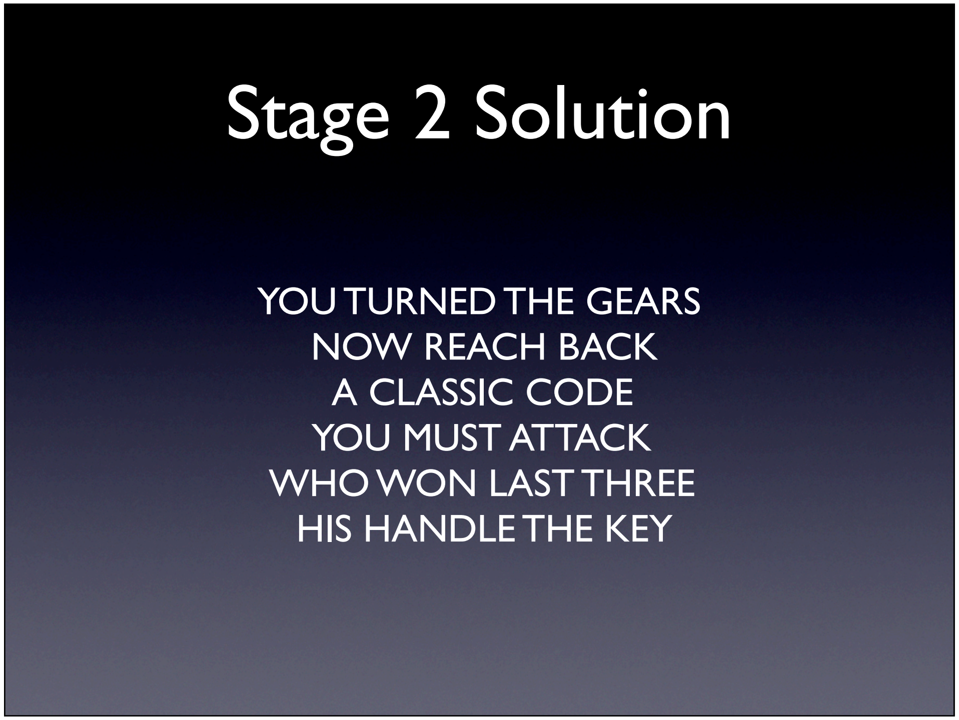


Mechanism

- Order badges, again, by dates
- Read top of first gear: Y
- Turn first gear clockwise (2nd turns CCW, etc.)
- Read top of 2nd gear: O (it moved, remember)
- Turn again
- Top of 3rd: U
- etc. etc.

Line all the badges up like in the picture in the program. There were some questions as to whether badges should start “up” or rotated by one or more notches, my typical response was “You should always try the easy approach first.” Then, read the first letter off the first badge, then turn the entire system one click. Read the top letter off the next badge, turn again.

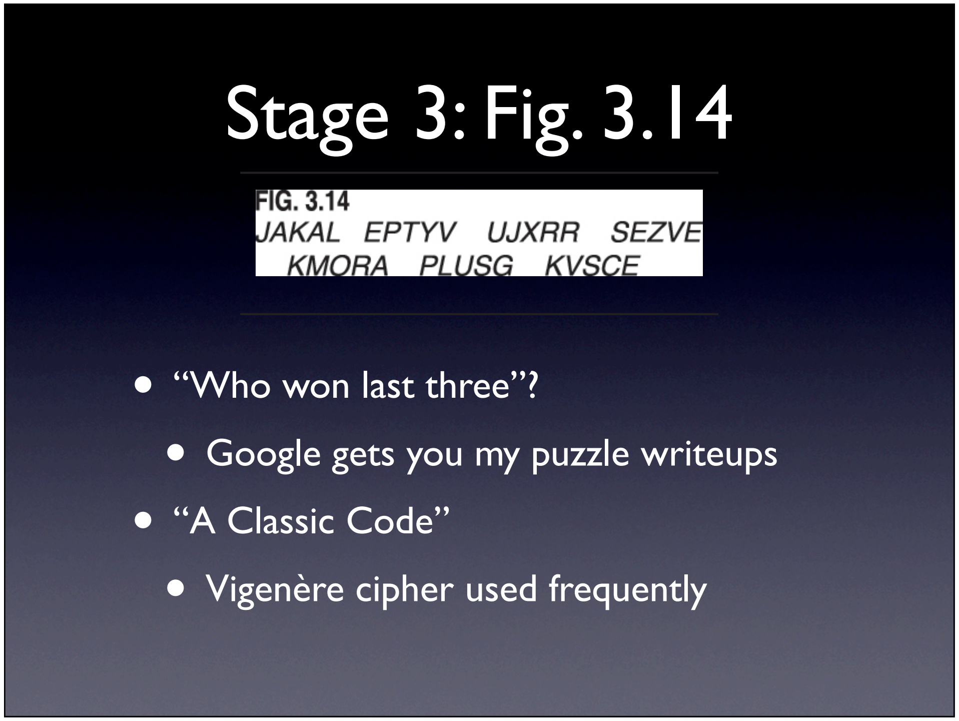
It’s actually easier to just draw the whole thing out on paper, and count teeth. Tooth 0 (top) on first badge, then clockwise 1, then counterclockwise 2, then cw 3, etc., etc. Scratch off each letter as you use it just to help keep yourself on track, and go through the whole thing that way until every letter is used.



Stage 2 Solution

YOU TURNED THE GEARS
NOW REACH BACK
A CLASSIC CODE
YOU MUST ATTACK
WHO WON LAST THREE
HIS HANDLE THE KEY

This is the result of Stage 2. A hint about the next stage’s cipher, and key.



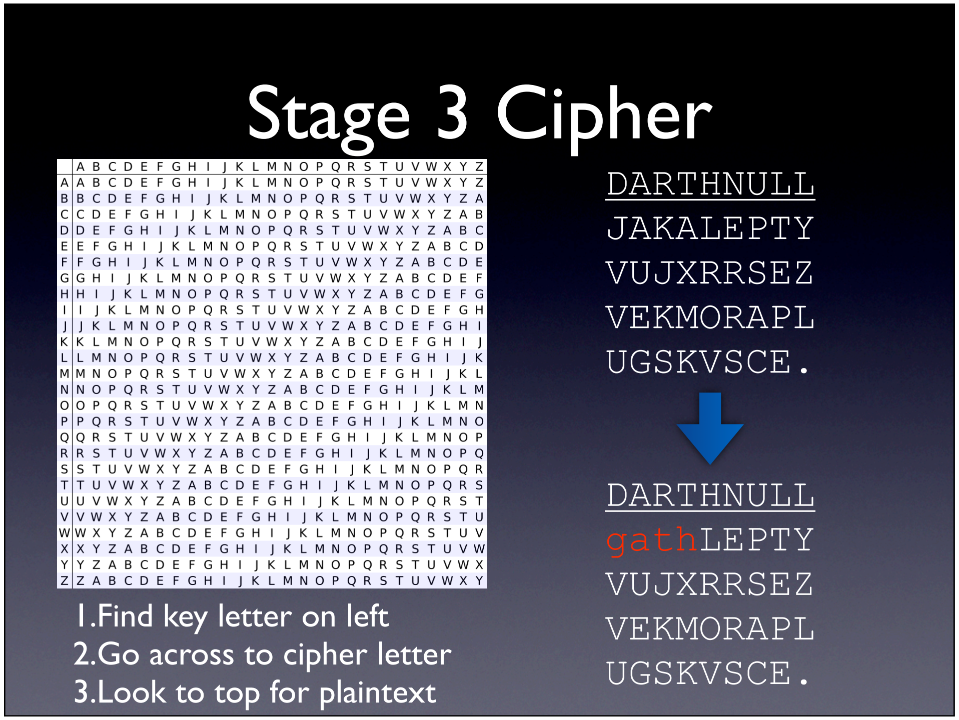
Stage 3: Fig. 3.14

FIG. 3.14
JAKAL EPTYV UJXRR SEZVE
KMORA PLUSG KVSCE

- “Who won last three”?
  - Google gets you my puzzle writeups
- “A Classic Code”
  - Vigenère cipher used frequently

One amusing bit -- one group found “sevens” all over the program, and puzzle. I can’t even remember where they found them, but apparently they occurred multiple times (not just that there were seven badges). And this stage had seven blocks of five letters. Pure chance, really.

Anyway, the “reach back” and “classic code” should have helped people look for older, classical ciphers. The “Who won last three” hopefully would have gotten players to find my website, where I wrote up many puzzles using the Vigenère cipher, which is a good example of such a cipher (and the one used here). Also, obviously, that’d get them my handle, which was the key for this stage.



Stage 3 Cipher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

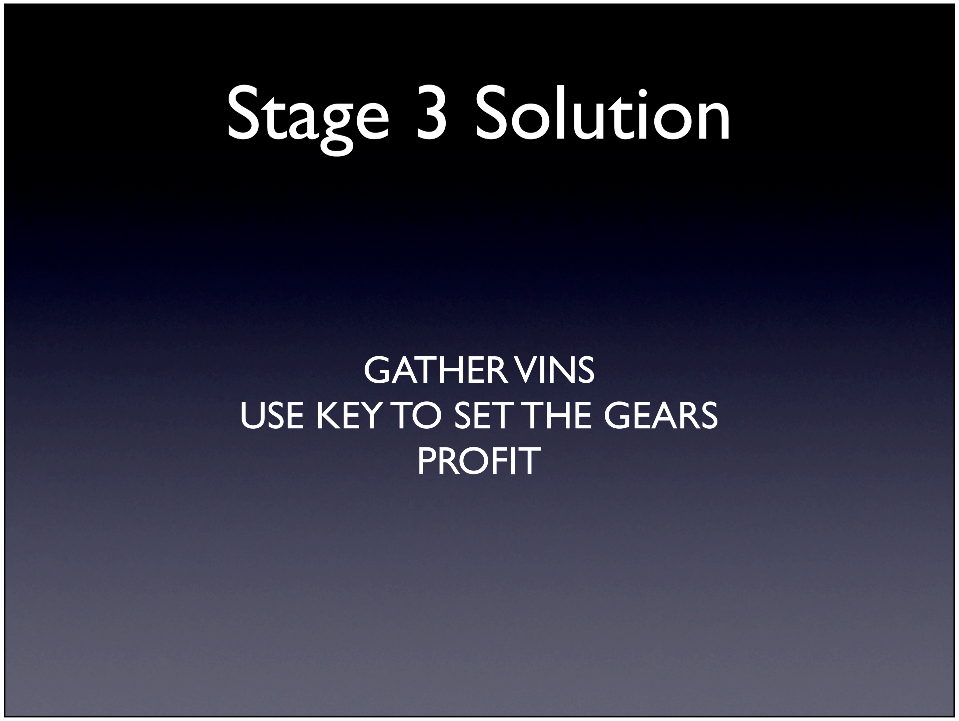
1. Find key letter on left
2. Go across to cipher letter
3. Look to top for plaintext

```
DARTHNULL
JAKALEPTY
VUJXRRSEZ
VEKMORAPL
UGSKVSCE.
```

```
DARTHNULL
gathLEPTY
VUJXRRSEZ
VEKMORAPL
UGSKVSCE.
```

To solve, you write out the key, and then write the message under it (writing across in 9-letter blocks). Then everything under each key letter is encrypted using the cipher alphabet for that letter.

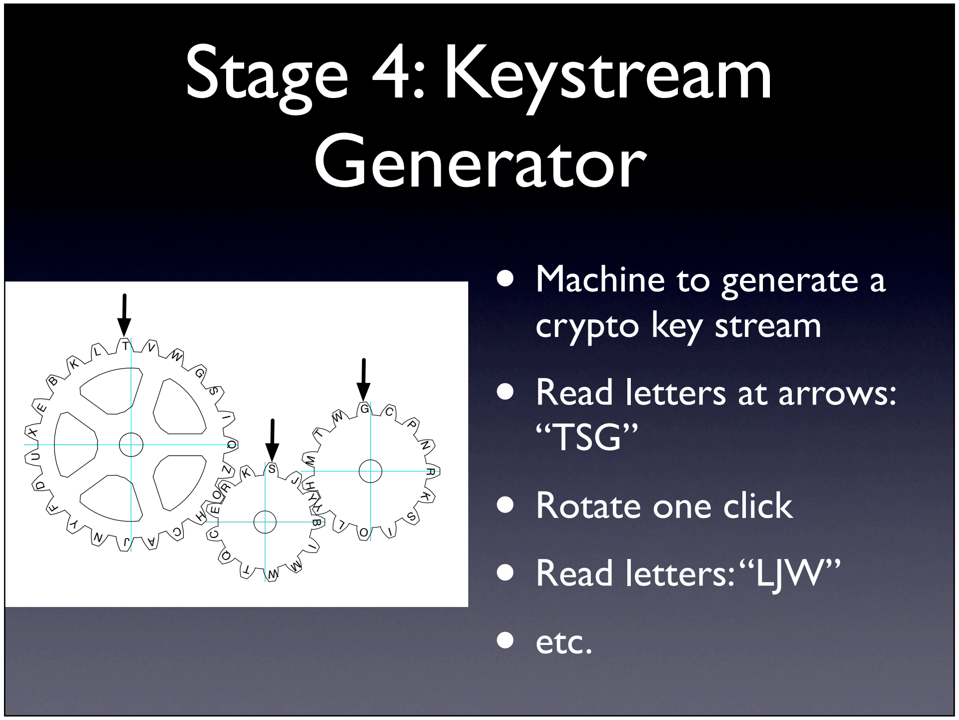
It’s easy to solve using the Vigenère tableau. Just look for the key letter on the left edge (D, for example), then move over in that row until you find the ciphertext letter you want to decrypt (J). Then look up to the top to find what letter is on the top row (G) and you have your first plaintext letter. Do this over and over and you decode the message.



Stage 3 Solution

GATHER VINS
USE KEY TO SET THE GEARS
PROFIT

“Use key to set the gears.” What does that mean? What key? Where do I find it?



Stage 4: Keystream Generator

- Machine to generate a crypto key stream
- Read letters at arrows: “TSG”
- Rotate one click
- Read letters: “LJW”
- etc.

This was actually the inspiration for the entire puzzle. Heidi had told me they’d be using a “gearhead” theme for the con, and I thought, hm...how about a keystream generator?

The idea is that you set the gears to a starting position (here I chose “TSG”), and as you turn the gears they produce a random-looking string of letters that you can use to encrypt a message. It’s a greatly over-simplified implementation of a basic approach used in many cipher machines, especially before and during World War II. (look at me trying to teach!)

Stage 4 Key

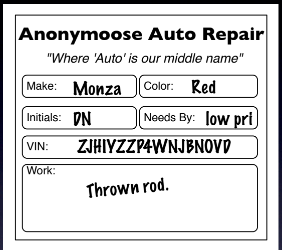
- “USE KEY TO SET GEARS”
- Set gears so top teeth read:
  - Left gear: K
  - Middle gear: E
  - Right gear: Y

I’ve no idea whether this little trick stumped anyone, or if it was just a minor inconvenience. But it at least got a chuckle out of the crowd when I announced it....

Turn the gears in the 3-gear diagram to match the starting key of “KEY” and your keystream machine is set.

Stage 4 Ciphertext

- VINs from the repair slips
- In a real VIN, middle char is a check digit
- In this puzzle, that gives you the proper order


Anonymoose Auto Repair

"Where 'Auto' is our middle name"

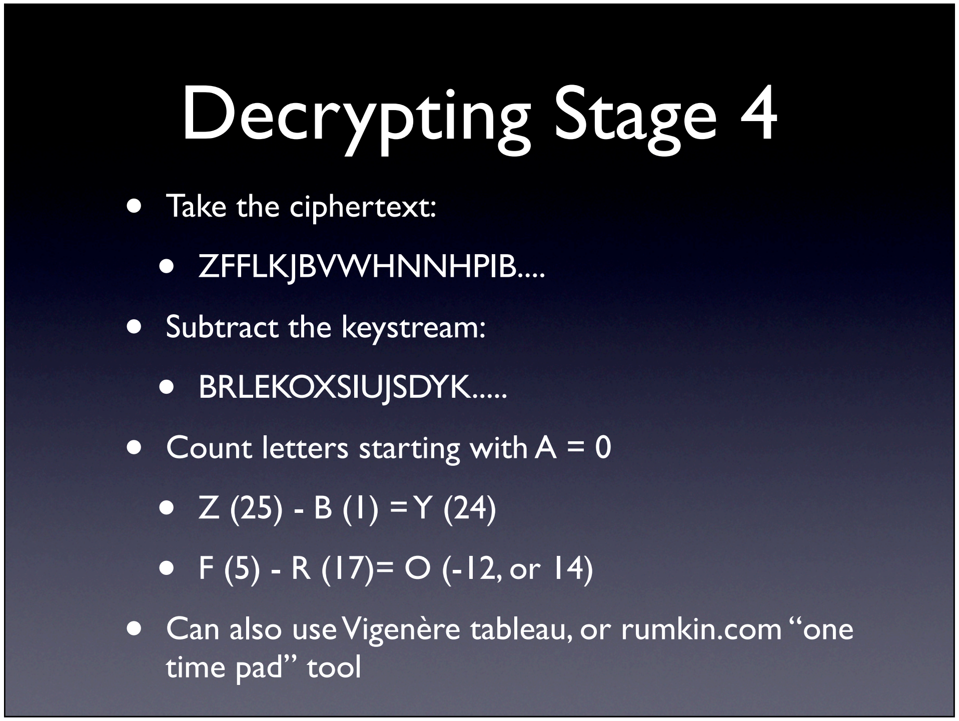
Make: Monza	Color: Red
Initials: DN	Needs By: low pri
VIN: ZJHIYZZP4WNJBNOVD	
Work: Thrown rod.	

```
ZFFLKJBV1WHNNHPIB
FCJVBJRD2APJEYOPQ
HJJTZPQM3XLJYUQFH
ZJHIYZZP4WNJBNOVD
PVVEWBLG5SPHISYEJ
```

The last hint said to “Gather VINs.” I scattered 5 little repair slips through the program... The VIN on each slip wasn’t a real number, but was the cipher text. The middle digit gave the ordering for the ciphertext.

Though the slips were provided in a random order, somehow when they got into the program they actually were printed in the proper order, so this middle digit was sort of unnecessary.

I saw at least one team looking for deep significance in the rest of the text on the slips -- including the fact that one slip had a “/” on it, and one had a “.” Ah...rabbit holes...so much fun to see someone ELSE get stuck in one for a change....

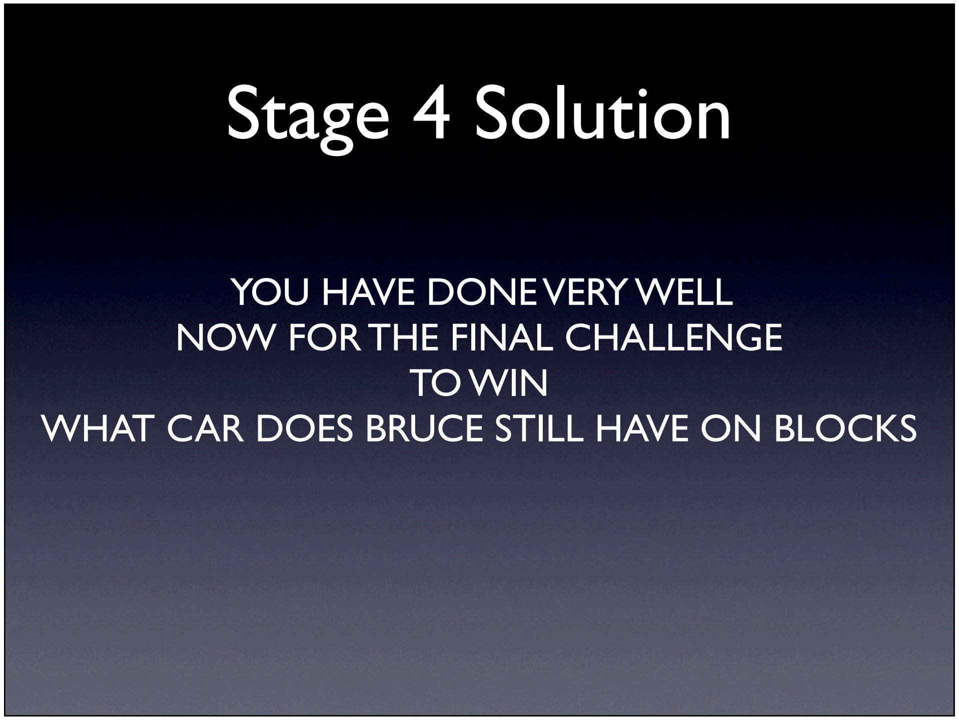


Decrypting Stage 4

- Take the ciphertext:
  - ZFFLKJBVWHNNHPIB....
- Subtract the keystream:
  - BRLEKOXSIUJSDYK.....
- Count letters starting with A = 0
  - Z (25) - B (1) = Y (24)
  - F (5) - R (17)= O (-12, or 14)
- Can also use Vigenère tableau, or rumkin.com "one time pad" tool

Take the keystream generated by setting the gears to KEY, and subtract that from the ciphertext. In this case, we assign numbers 0-25 to the alphabet, and use modulo 26 arithmetic (so 5 - 17 = -12, or 26-12, or 14).

It's also the same method, mathematically, that the Vigenère tableau uses, so you can use that grid to solve this stage as well. Finally, it's kind of how many One Time Pads work, and a popular online cipher tools site (rumkin.com) has a tool that'd work perfectly with this code as well.



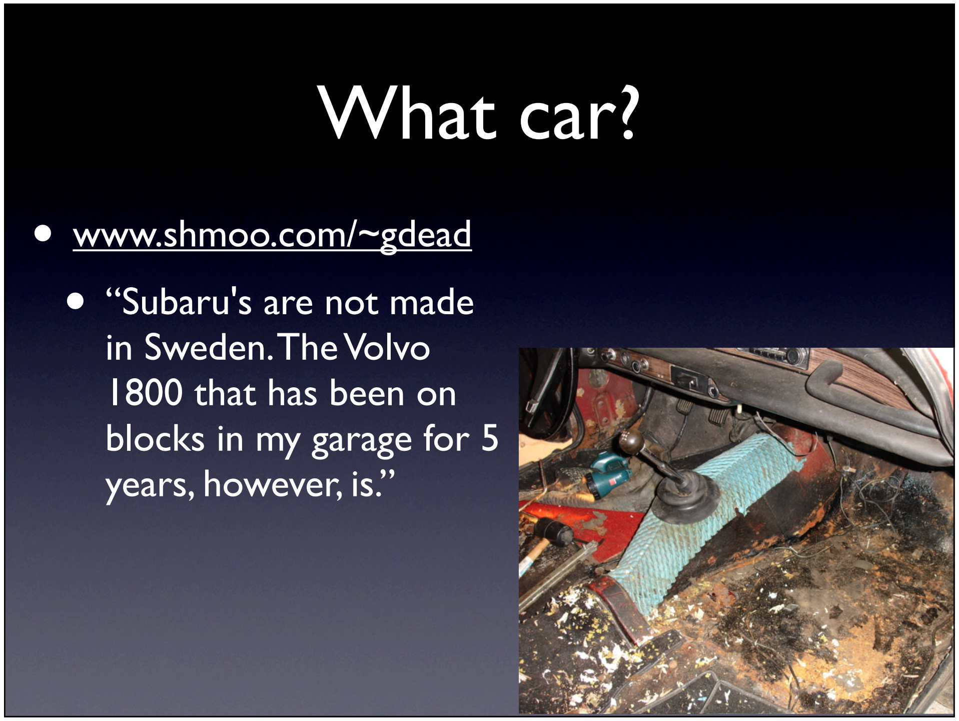
Stage 4 Solution

YOU HAVE DONE VERY WELL
NOW FOR THE FINAL CHALLENGE
TO WIN
WHAT CAR DOES BRUCE STILL HAVE ON BLOCKS

And this is what the VINs decode to.

This wasn't an easy bit of trivia to figure out, but it WAS recoverable using a certain amount of Google Fu. However, a little while before the con Bruce actually added the answer to his long-neglected page on shmoo.com, so it was a little easier.

The team that won the contest actually asked Bruce what the answer was, but he was (correctly) instructed by Heidi to NOT answer. So they went into a corner and started poring through the program, hoping they'd just missed it. After a few minutes, Heidi told them it wasn't in there, and they decided to "ask the internet" instead.

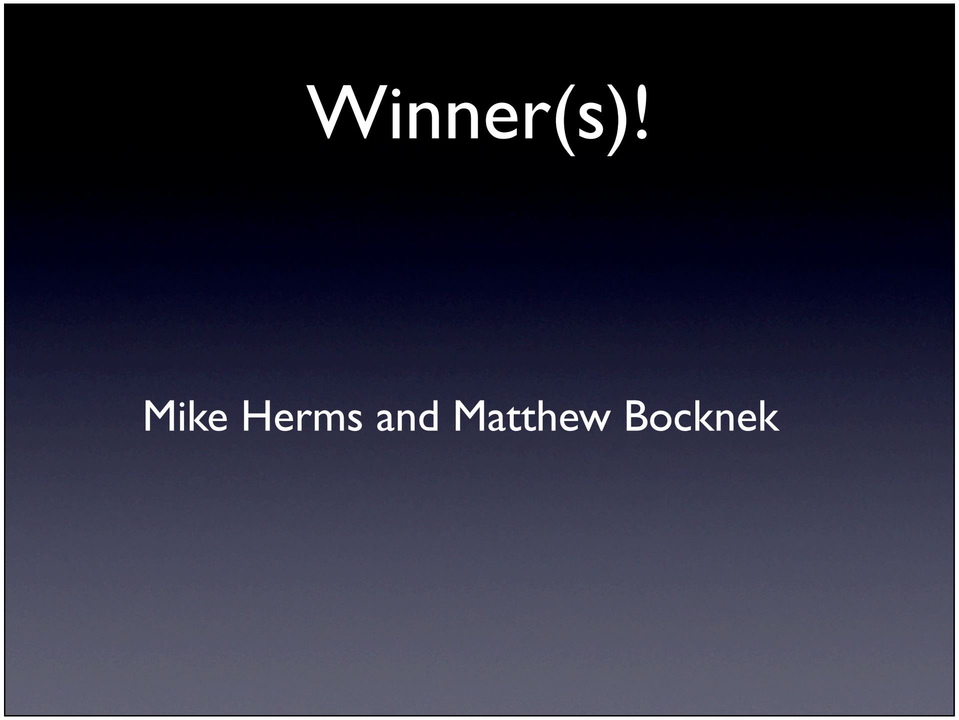


What car?

- www.shmoo.com/~gdead
  - “Subaru's are not made in Sweden. The Volvo 1800 that has been on blocks in my garage for 5 years, however, is.”

And apparently “asking the internet” worked, because 10 minutes later they came back and gave Heidi the correct answer, winning the contest at about 12:45 on Saturday!

(and, yes, that’s actually the interior of Bruce’s Volvo 1800.)



Winner(s)!

Mike Herms and Matthew Bocknek

Congratulations to Mike and Matthew, who both won free tickets to ShmooCon 9!