

Shmooganography 2010

How we did it

And how most of you didn't

Who got the most right?

Umm...

Stage One:

EVIL NOSE PUNK

- ✦ Just needed to read the contest description and index the spelling mistakes.
- ✦ These numbers reveal an ISBN for:



1 **Due** you have a knack for finding hidden messages? Are you a hacker with bits streaming
4 through your veins **oar** some EVIL NOSE PUNK (aka script-kiddie) learning how to use the
2 remote? **We'll** prove it! Find all the hidden clues at this con. There are a total of eight rounds.
5 Each round will reveal **uh** clue embedded with a secret code. Secret codes are identified by
1 **sum** unique representation within each clue. Clues and codes are <stego word="hidden" />.
3 Sounds easy **e'nuff**, right? Getting to the next stage will be more difficult as you progress.
3 Be the **furst** to find the common theme between the codes and you win. Simply email
7 Shmooganography@gmail.com with the secret codes and **thee** connecting theme. One helpful
4 hint: Shmooganography is **knot** connected with the badge contest! Are you ready for your
6 first clue? Sometimes you should **cownt** on mistakes...

Stage Two:

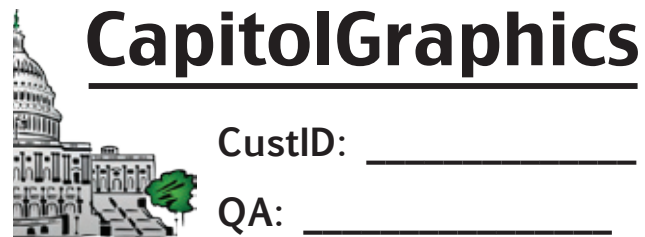
DANG MULE ZONE

- ✦ Barcodes hidden in swag bags
 - ✦ Luggage tag: UPC-A 1D Barcode
 - ✦ Inside bag: QR 2D Barcode



416541856554

- Indexes into 2D barcode text
- Text says “shmoo!” — tricky!



Spiders **are** weaving incognito.
Kismet **u**sing quarterly increments.
Analyze barcodes, glean code.

It doesn't scan with iPhone 3G!

Use RedLaser and i-nigma.

Stage Three:

ANGRY MOCK INN

- ✦ Automated spider trolling through these websites:

- www.**A**pple.com
- www.**N**ascar.com
- groups.**G**oogle.com/group/shmooganography
- www.**R**everseengineering.com
- www.**Y**outube.com
- www.**S**PACE.com
- www.**M**icrosoftsucks.org
- www.**O**penoffice.org
- www.**C**isco.com
- www.**K**ismetwireless.net
- www.**S**PACE.com
- www.**I**ana.org
- www.**N**etgear.com
- www.**N**intendo.com

Clue



- ✦ Connected to “shmoocon” open WiFi Lan
- ✦ Pulled websites every quarter hour
- ✦ Then every tenth hour

Stage Four: IN MILD REVIVAL

- ✦ Windows program which lightly wrapped “ipconfig”
- ✦ Posted to “shmooganography” Google Group
- ✦ Running `strings` reveals **secretmoose** CLI switch
 - ✦ Other strings loosely hidden by XORing function
- ✦ Need to pass code words as argument to secret CLI switch



```
C:\>ipconfig.exe
```

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix .	:	localdomain
IP Address.	:	192.168.39.128
Subnet Mask	:	255.255.255.0
Default Gateway	:	192.168.39.2

```
C:\>ipconfig.exe /secretmoose
```

Nicely played. The codeword is **INMILDREVIVAL**.

If you want your clue... you're going to have to dig deeper...

```
C:\>ipconfig.exe /secretmoose INMILDREVIVAL
```

Come on, ConNerd... You have to try harder than that!

```
C:\>ipconfig.exe /secretmoose INMILDREVIVAL
```

Drat, you found me. Now go talk to Matt. He's probably just laying around here somewhere.

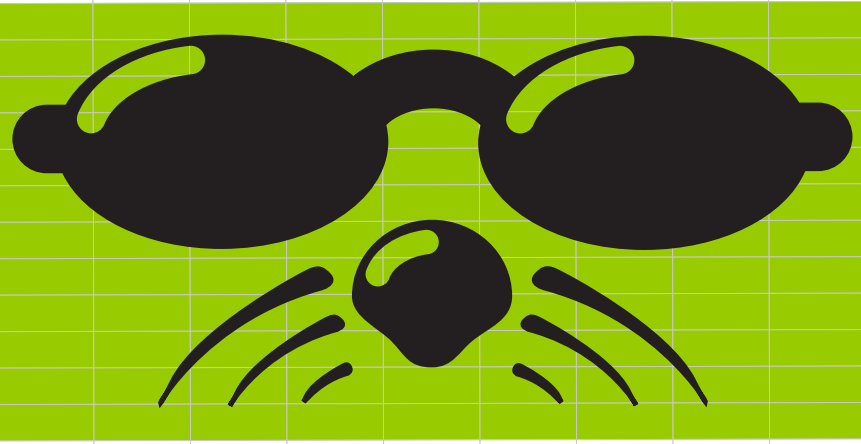
owemrele

Drat, you found me. Now go talk to Matt. He's probably just laying around here somewhere.

```
C:\>ipconfig.exe /secretmoose INMILDREVIVAL
```

Stage Five: ANIMAL ROAD

- ✦ The Shmoocon mat at registration area, using octal

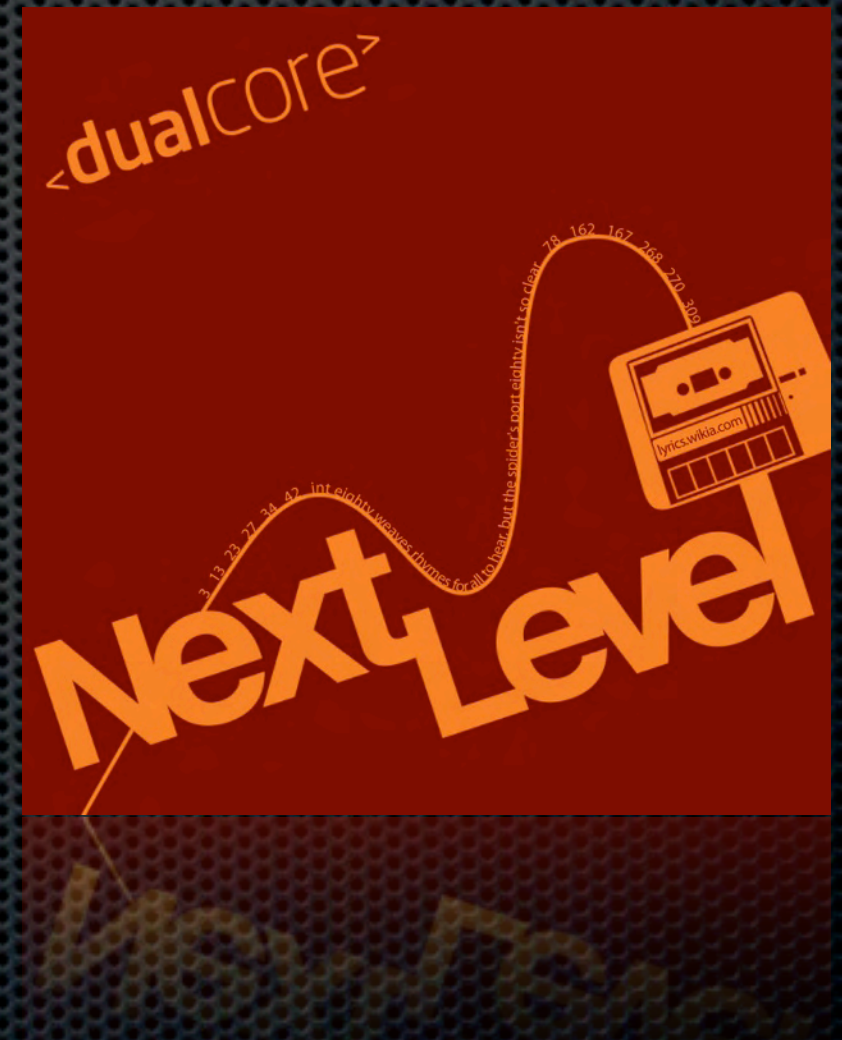
S		W	e	l	c	o	m	e		t	o	
h	S	h	m	o	o	C	o	n		V	l	!
m	H	a	v	e		y	o	u		f	o	u
o	n	d		t	h	e		t	h	e	m	e
o		b	e	h	i	n	d		t	h	e	
g	c	o	d	e	s		y	e	t	?		
a		G	o	t		M	o	o	s	e	?	
n	A										s	/
o	A										h	t
g	N										m	e
r	I										o	g
a	M										c	a
p	A										o	m
h	L										n	e
y											.	.
!	D										o	m
!	A										r	p
e	O										g	3
g	R										e	h
n		u	o	y		t	a	?	d	r	a	
e			u		y		f	h	w		p	r
l		a		e	y	s		u		e	u	c
l			n	e	h	s		,	o	y		d
a			d	n	a	s	u	o	s	d	r	w
h			s	i		c	i	p		a		
C											f	l

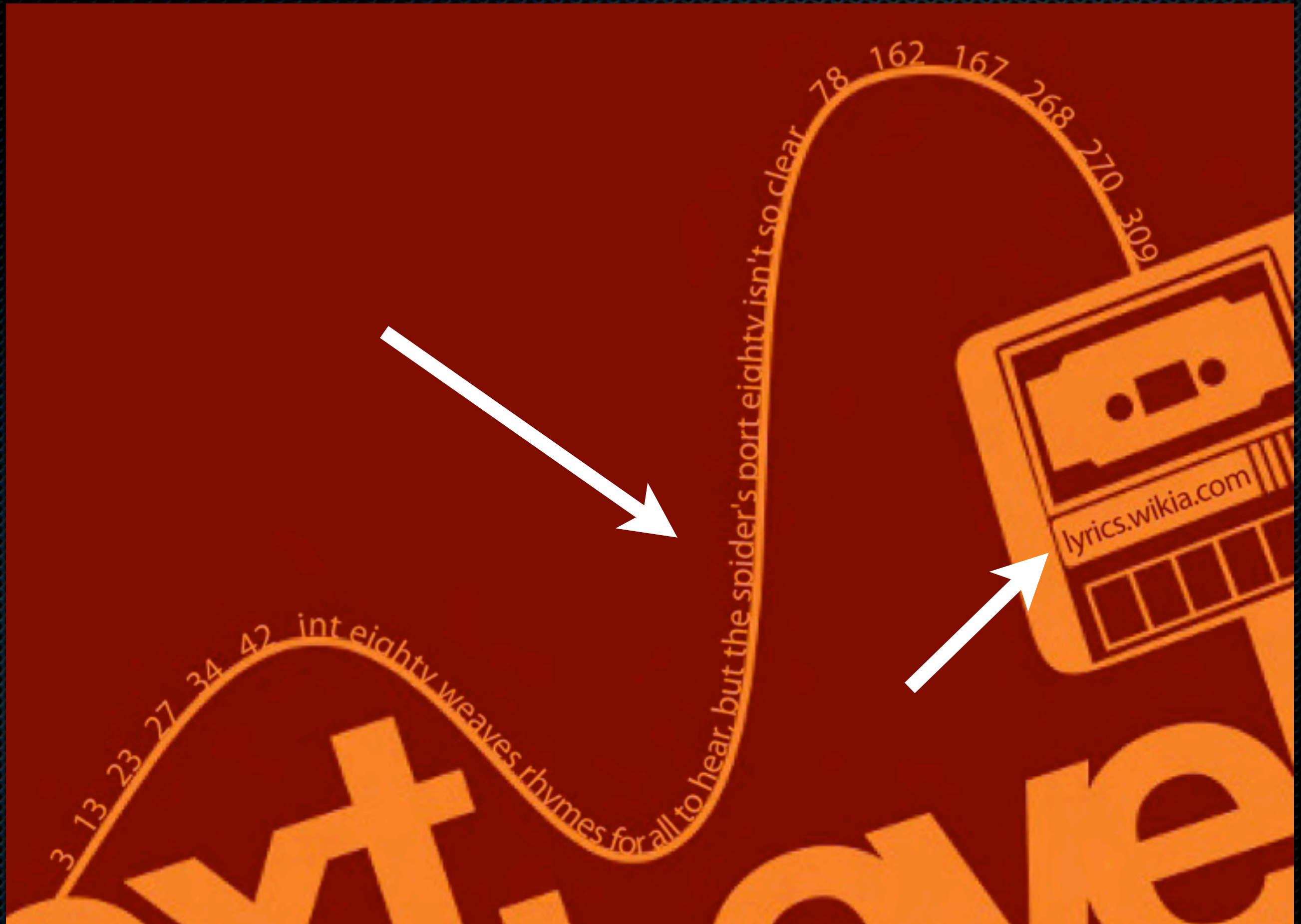


Stage Six:

VICTIM KEN KIN

- ✦ Slightly modified MP3 of “The Game” from Dual Core
- ✦ Embedded album art has indexes and clue on “wire”
- ✦ Indexes are for words in lyrics pulled from lyrics.wikia.com, revealing code word
- ✦ Clue reveals a return to the spider...

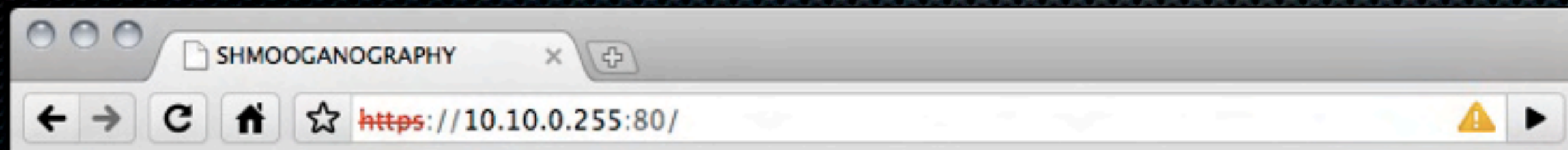




Stage Seven:

ADD THIS VIM

- ✦ If you found the spider, you would know its valid IP address on “shmoocon” WiFi LAN
- ✦ Connecting to port 80 reveals that https should be used
- ✦ Connecting blindly with normal https reveals... well... nothing
- ✦ Need to force https on port 80



Shmooganography

Nice work ConNerd. You have appeased the MOOSE, but your work is not complete. Ah...you want your code and clue...if life can be so simple. Well, we already gave it to you! Listen ConNerd, we think of it this way: You are *now* the KeyMaster and we are the GateKeeper...

SHM  **CON**

**localhost**

Issued by: Shmooganography-CA

Expires: Sunday, February 14, 2010 6:49:19 PM ET

⚠ This certificate was signed by an unknown authority

▼ Details

Issuer Name	
Country	US
State/Province	Washington DC
Locality	Washington DC
Organization	ShmooCon
Organizational Unit	SHMOOGANOGRAPHY
Common Name	Shmooganography-CA
Email Address	ADD.THIS.VIM@code
Serial Number	1
Version	1
Signature Algorithm	SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)
Parameters	none
Subject Name	
Country	US
State/Province	Washington DC
Locality	Washington DC
Organization	ShmooCon
Organizational Unit	SHMOOGANOGRAPHY
Common Name	localhost
Email Address	AdvertisementsCanBeDeceiving-SHMOOGANOGRAPHYisNoException@clue
Not Valid Before	Thursday, February 4, 2010 6:49:19 PM ET
Not Valid After	Sunday, February 14, 2010 6:49:19 PM ET

- ✦ 4 posters hung throughout Con area advertising game
- ✦ Need to take picture of each, then find subtle differences to reveal clue and code word



```

G      w      gm0nz2  Cu      e 9uxKVXb YcZ2jM  vDGqv  n      z LDaVbT3 xHTkzGF
v      2 t      T      S 2 x      u K      m      W A      Q m      9 e      B i      v
M M      T      H      h e M      r R      7      X H      y E      c z      7 b      K
T PpqZBqs OuxsxP  b  a  4 hW7I      5mrZg4  h      l SVGjGcc E      D ANK84TS
C      f 9      H x      n      q P C      K      O e      x v      l w      N c
9k1H0EF G      J E      n      ia z3QlVnI x      C rYRqN  6      d CQsh8bM S

```

The **ehemt** is people,
places, or things.

ANAGRAMS!!!!

So, the code words were:

**EVIL NOSE PUNK
DANG MULE ZONE
ANIMAL ROAD
IN MILD REVIVAL
ANGRY MOCK INN
VICTIM KEN KIN
ADD THIS VIM
JAR NERD HOP**

WTF?

What was the ehemt?

ANAGRAMS!

**EVIL NOSE PUNK
DANG MULE ZONE
ANIMAL ROAD
IN MILD REVIVAL
ANGRY MOCK INN
VICTIM KEN KIN
ADD THIS VIM
JAR NERD HOP**

**Kevin Poulsen
Onel de Guzman
Adrian Lamo
Vladimir Levin
Gary McKinnon
Kevin Mitnick
David Smith
John Draper**

They're all famous hackers!

Special Thanks

- ✦ **Our Understanding Wives**, for helping us stick barcodes on 1600 luggage tags and paint (and repaint) the Shmoo mat
- ✦ **Bruce & Heidi**, for tolerating our endless shenanigans
- ✦ **Dual Core**, for free MP3 music for all to enjoy

shmooganography@gmail.com