0x0000

there are ghosts from my past that pwn more of my soul than i thought i had given away.
they linger in closets and under my bed and in pictures less proudly displayed
– j. knapp

GROK

grokking all the shizzle — a passionate way to be excellent at binary and computer systems

s/mistak\(.\)s/correction\1/g

regex substitution with field carry

s/mistak\(.\)s/correction\1/g

```
gawk -F: '{ print $1 }' /etc/passwd
```

awk command to print userid's from /etc/passwd

```
gawk -F: '{ print $1 }' /etc/passwd
```

```
for x in xrange(100,1,-1):
```

python ***for*** loop counting down from 100 to 1

```
for x in xrange(100,0,-1):
```

```
for (int a=1, b=1, c; a<100;
          c=b,b+=a,a=c)
     printf(“%d “,a);
```

c language: prints Fibonacci sequence through 89

```
for (int a=1, b=1, c; a<100;
        c=b,b+=a,a=c)
    printf("%d ",a);
```

0 1 1 2 3 5 8 13 21 34 55 89

21686148-6449-6E6F-744E-656564454649

GUID for GPT BIOS Boot Partitions

21686148-6449-6E6F-744E-656564454649

“Hah!IdontNeedEFI”

aGVsbG8gd29ybGQhCg==

base64 encoding of “hello world!\n”

$ echo 'hello world!' | en64

aGVsbG8gd29ybGQhCg==

aad3b435b51404eeaad3b435b51404ee

LM Hash for empty password

aad3b435b51404eeaad3b435b51404ee

NBSWY3DPEB3W64TMMQQQ====

`base32 encoding of 'hello world!\n'`

$ echo 'hello world!"|en32

NBSWY3DPEB3W64TMMQQQ====

ebfe
ebff
eb80

x86 machine language (hex representation)
specifically: relative jmp's

```
ebfe – jmp -2 ;infinite loop
ebff – jmp -1 ; obfuscation
eb80 – jmp -127 ; jmp back 125 bytes
                ; prior to this location
```

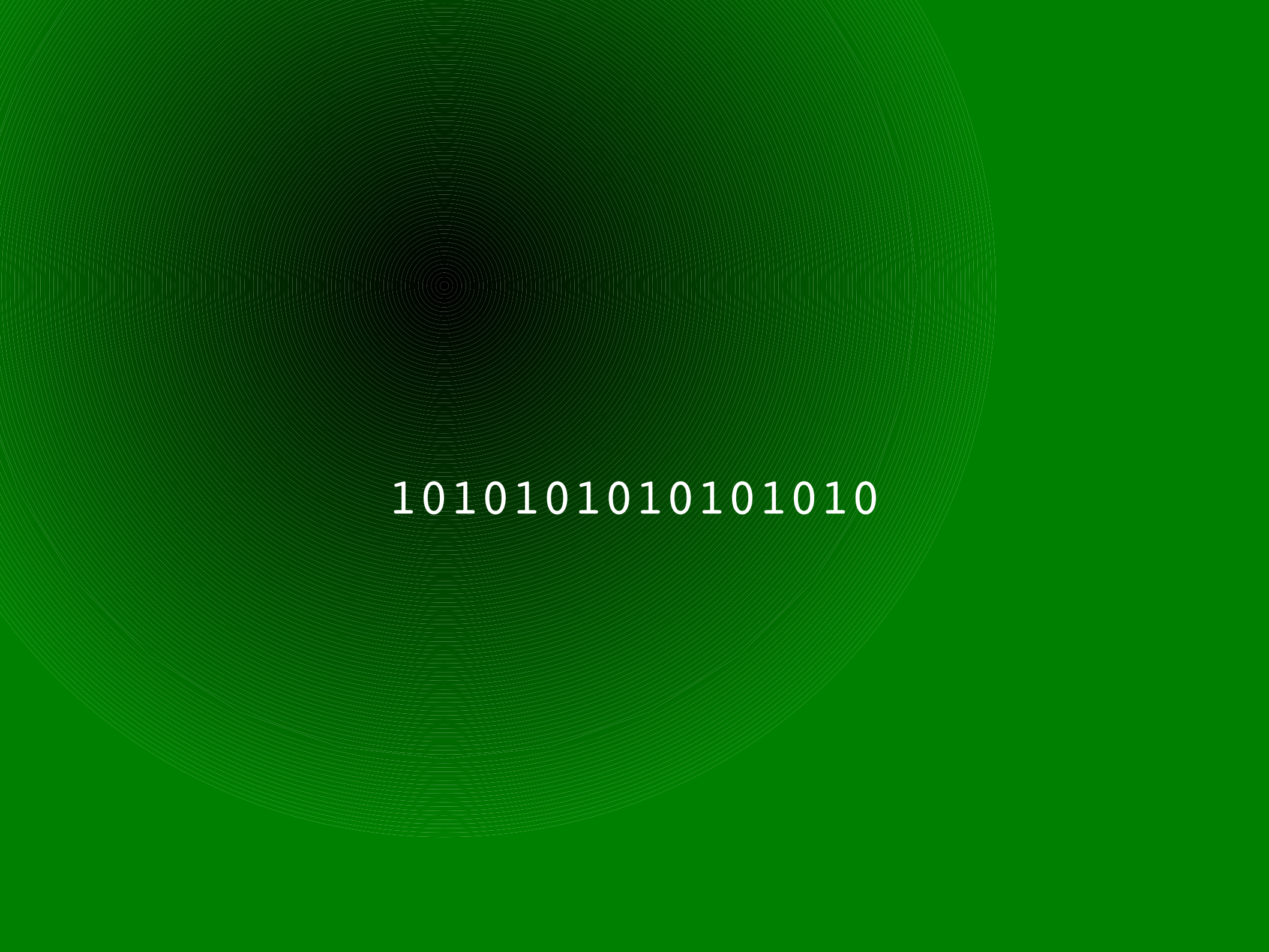
0xED

1) x86 “IN” instruction
2) favorite nickname for Ed Skoudis

0xED – ***in ax,dx***

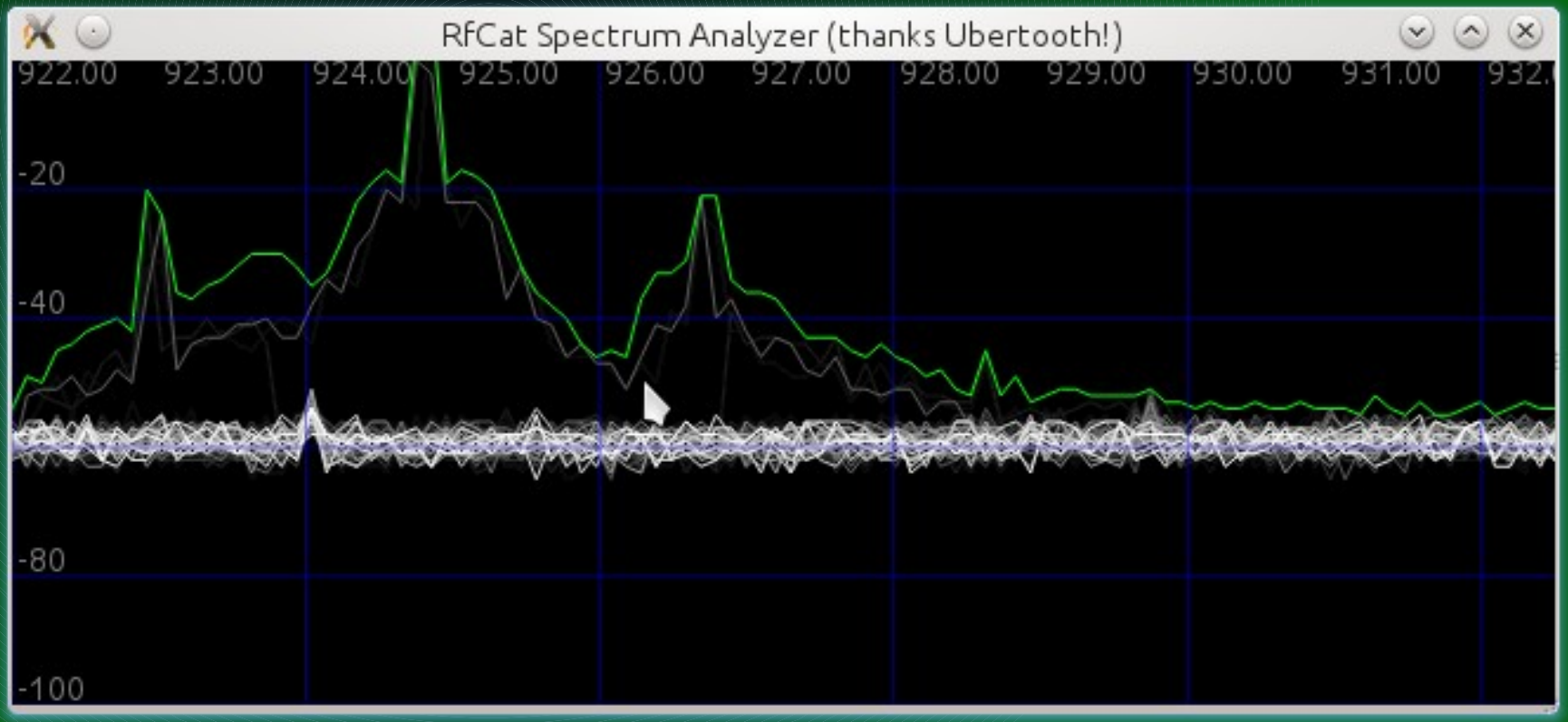
- kernel talks to hardware using this instruction
- Guest talks to VMware Host with it as well
- i talk to sk0d0 with it

sorry, when you see patterns, you see patterns...

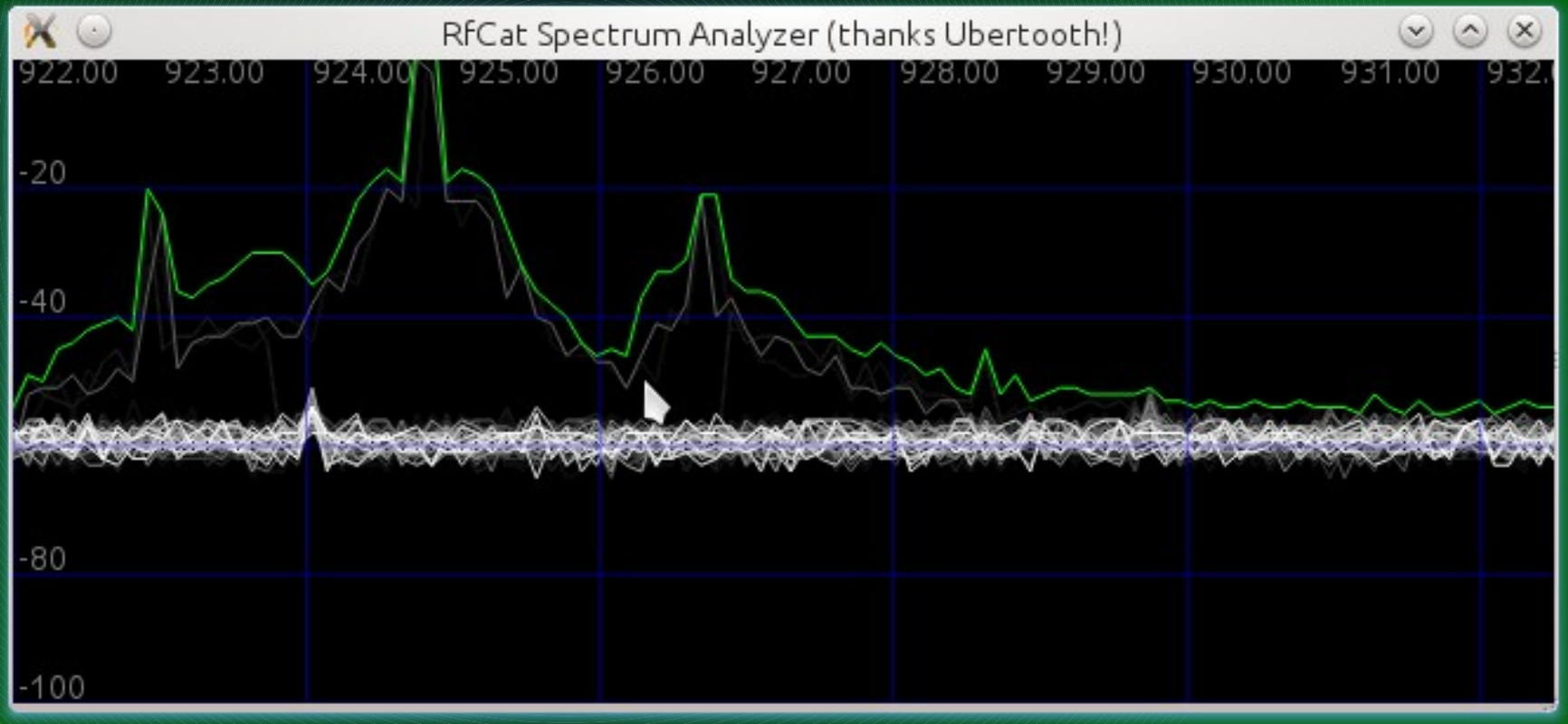

1010101010101010

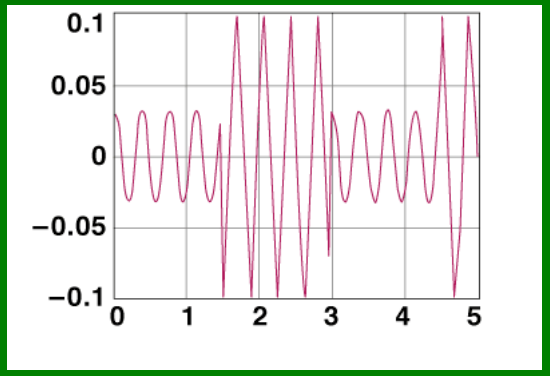
RF Preamble (alternating pattern of 1/0) also specified in 802.* comms protocols. turns out, wired and wireless are not too different!

1010101010101010

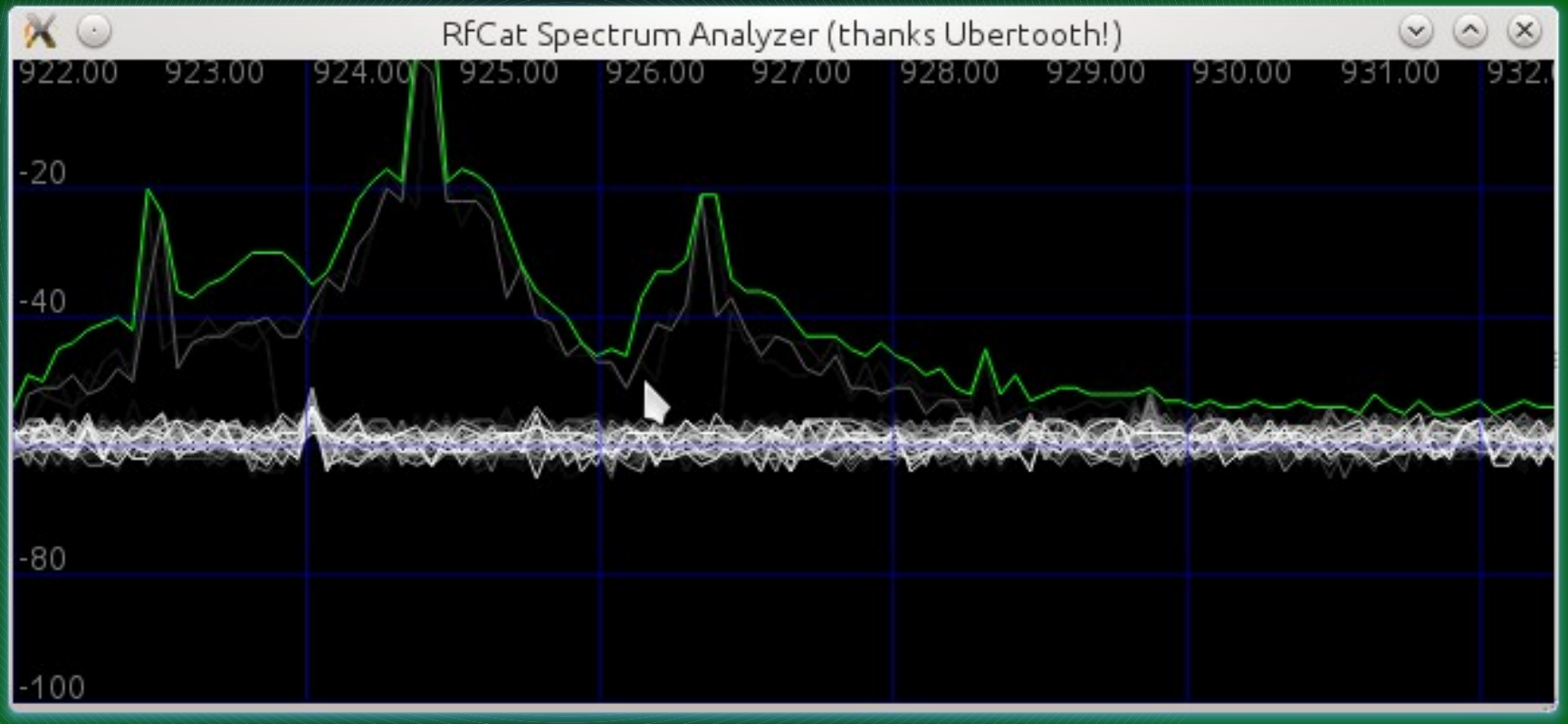

RfCat Spectrum Analyzer (thanks Ubertooth!)
922.00
923.00
924.00
925.00
926.00
927.00
928.00
929.00
930.00
931.00
-20
-40
-80
-100

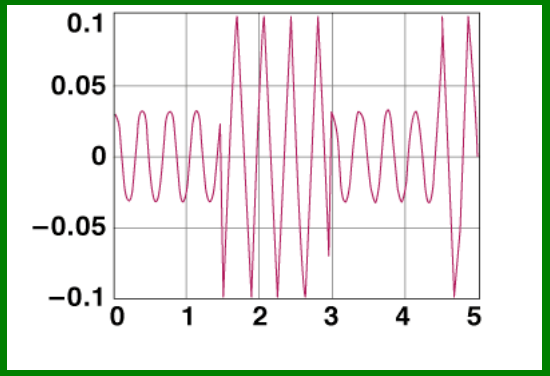
nudge further...





Spectrum Analysis of an Amplitude Shift Key (**ASK**) signal centered at **924.850MHz**





3 different byte-combinations...

03002de9
10b5
4df804dd

ARM, Thumb, and Thumb2 instructions

```
03002de9   stmdb sp!,{r0, r1, }
    10b5   push {r4, sp, }
4df804dd   push.W {lr}
```

```
.text:0x000182ac  8bff                mov edi,edi
.text:0x000182ae  55                  push ebp
.text:0x000182af  8bec                mov ebp,esp
.text:0x000182b1  51                  push ecx
```

x86 function prolog instructions (microsoft-style)

```
.text:0x000182ac  8bff          mov edi,edi
.text:0x000182ae  55            push ebp
.text:0x000182af  8bec          mov ebp,esp
.text:0x000182b1  51            push ecx
```

Never use gets(). Because it is impossible to tell without knowing the data in advance how many characters gets() will read, and because gets() will continue to store characters past the end of the buffer, it is extremely dangerous to use. It has been used to break computer security. Use fgets() instead.

MAN page for gets (man 3 gets)

Never use gets(). Because it is impossible to tell without knowing the data in advance how many characters gets() will read, and because gets() will continue to store characters past the end of the buffer, it is extremely dangerous to use. It has been used to break computer security. Use fgets() instead.

PK\003\004

ZIP header (thanks Phil Katz! R.I.P.)

PK\003\004


\x7fELF

you guessed it, Header for the ELF executable file format

\x7fELF

there will be a test

01000000

binary representation of “@” best char EVAR!

01000000

0xdebb20e3

CRC magic number for ZIP

0xdebb20e3

d41d8cd98f00b204e9800998ecf8427e

md5 of nothing

d41d8cd98f00b204e9800998ecf8427e

da39a3ee5e6b4b0d3255bfef95601890afd80709

sha1 of nothing

da39a3ee5e6b4b0d3255bfef95601890afd80709

- 0x67452301
- 0xefcdab89
- 0x98badcfe
- 0x10325476

md5 magic numbers

- 0x67452301
- 0xefcdab89
- 0x98badcfe
- 0x10325476

TDI, TDO, TMS, TCK

jtag pins for debugging embedded systems

TDI, TDO, TMS, TCK

MZ

PE File Format (DOS/Windows .EXE/.COM/.DLL/.SYS

MZ

'\x89PNG\r\n\x1a\n'

file header for PNG file format

'\x89PNG\r\n\x1a\n'

25504446

Portable Document Format (PDF) file header

%PDF 25504446

55AA

MBR sector terminator

```
root@ironman:/home/atlas/hacking/Presentations/Grok# dd if=/dev/sda count=1 2>
00000000  eb 63 90 10 8e d0 bc 00  b0 b8 00 00 8e d8 8e c0  |.c..............|
00000010  fb be 00 7c bf 00 06 b9  00 02 f3 a4 ea 21 06 00  |...|.........!..|
00000020  00 be be 07 38 04 75 0b  83 c6 10 81 fe fe 07 75  |....8.u........u|
00000030  f3 eb 16 b4 02 b0 01 bb  00 7c b2 80 8a 74 01 8b  |.........|...t..|
00000040  4c 02 cd 13 ea 00 7c 00  00 eb fe 00 00 00 00 00  |L.....|.........|
00000050  00 00 00 00 00 00 00 00  00 00 00 80 01 00 00 00  |................|
00000060  00 00 00 00 ff fa 90 90  f6 c2 80 74 05 f6 c2 70  |...........t...p|
00000070  74 02 b2 80 ea 79 7c 00  00 31 c0 8e d8 8e d0 bc  |t....y|..1......|
00000080  00 20 fb a0 64 7c 3c ff  74 02 88 c2 52 bb 17 04  |. ..d|<.t...R...|
00000090  80 27 03 74 06 be 88 7d  e8 17 01 be 05 7c b4 41  |.'.t...}.....|.A|
000000a0  bb aa 55 cd 13 5a 52 72  3d 81 fb 55 aa 75 37 83  |..U..ZRr=..U.u7.|
000000b0  e1 01 74 32 31 c0 89 44  04 40 88 44 ff 89 44 02  |..t21..D.@.D..D.|
000000c0  c7 04 10 00 66 8b 1e 5c  7c 66 89 5c 08 66 8b 1e  |....f..\|f.\.f..|
000000d0  60 7c 66 89 5c 0c c7 44  06 00 70 b4 42 cd 13 72  |`|f.\..D..p.B..r|
000000e0  05 bb 00 70 eb 76 b4 08  cd 13 73 0d f6 c2 80 0f  |...p.v....s.....|
000000f0  84 d0 00 be 93 7d e9 82  00 66 0f b6 c6 88 64 ff  |.....}...f....d.|
00000100  40 66 89 44 04 0f b6 d1  c1 e2 02 88 e8 88 f4 40  |@f.D...........@|
00000110  89 44 08 0f b6 c2 c0 e8  02 66 89 04 66 a1 60 7c  |.D.......f..f.`||
00000120  66 09 c0 75 4e 66 a1 5c  7c 66 31 d2 66 f7 34 88  |f..uNf.\|f1.f.4.|
00000130  d1 31 d2 66 f7 74 04 3b  44 08 7d 37 fe c1 88 c5  |.1.f.t.;D.}7....|
00000140  30 c0 c1 e8 02 08 c1 88  d0 5a 88 c6 bb 00 70 8e  |0........Z....p.|
00000150  c3 31 db b8 01 02 cd 13  72 1e 8c c3 60 1e b9 00  |.1......r...`...|
00000160  01 8e db 31 f6 bf 00 80  8e c6 fc f3 a5 1f 61 ff  |...1..........a.|
00000170  26 5a 7c be 8e 7d eb 03  be 9d 7d e8 34 00 be a2  |&Z|..}....}.4...|
00000180  7d e8 2e 00 cd 18 eb fe  47 52 55 42 20 00 47 65  |}.......GRUB .Ge|
00000190  6f 6d 00 48 61 72 64 20  44 69 73 6b 00 52 65 61  |om.Hard Disk.Rea|
000001a0  64 00 20 45 72 72 6f 72  0d 0a 00 bb 01 00 b4 0e  |d. Error........|
000001b0  cd 10 ac 3c 00 75 f4 c3  da 8e 01 00 00 00 80 20  |...<.u......... |
000001c0  21 00 83 1a 3b 1f 00 08  00 00 00 98 07 00 00 3b  |!...;..........;|
000001d0  1b 1f 05 fe ff ff fe a7  07 00 02 68 96 3b 00 00  |...........h.;..|
000001e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
```


D0CF11E0

Microsoft Office files

D0CF11E0

aka “DocFile0” :)

```
atlas@ironman:~/hacking/Presentations/Grok$ hexdump -C test.doc |head
00000000  d0 cf 11 e0 a1 b1 1a e1  00 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  3b 00 03 00 fe ff 09 00  |........;.......|
00000020  06 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00  |................|
00000030  01 00 00 00 00 00 00 00  00 10 00 00 0d 00 00 00  |................|
00000040  01 00 00 00 fe ff ff ff  00 00 00 00 00 00 00 00  |................|
00000050  ff ff ff ff ff ff ff ff  ff ff ff ff ff ff ff ff  |................|
*
00000200  fd ff ff ff 1b 00 00 00  03 00 00 00 04 00 00 00  |................|
00000210  05 00 00 00 06 00 00 00  07 00 00 00 08 00 00 00  |................|
00000220  09 00 00 00 0a 00 00 00  0b 00 00 00 0c 00 00 00  |................|
```

63825363

DHCP magic cookie

63825363

start of options section...

in every DHCP packet!

CAFEBABE
CAFED00D

Java / Mach-O / Pack200 compression

CAFEBABE — Java classes / Mach-O
CAFED00D — compressed with Pack200

0x9900

0x9501

0x9500

0xa600

from “file” magic for PGP:

```
0       beshort         0x9900                  PGP key public ring
!:mime     application/x-pgp-keyring
0       beshort         0x9501                  PGP key security ring
!:mime     application/x-pgp-keyring
0       beshort         0x9500                  PGP key security ring
!:mime     application/x-pgp-keyring
0    beshort            0xa600                PGP encrypted data
!:mime     text/PGP # encoding: armored data
```

SCLK, MISO, MOSI, SS

serial peripheral interface (spi) bus pins for embedded communication

SCLK, MISO, MOSI, SS

SCL, SDA

inter-integrated circuit(i2c) bus pins for lower-speed embedded communications

SCL, SDA

all that men know about women

```
CallFunction( 0x08049824, Const(0x08048bb8,4), [Var("arg0", width=4),
    Const(0x0804a200,4), Const(0x000007ff,4)] )

CallFunction( 0x08049843, Const(0x08048c18,4), [Const(0x0804a200,4),
    Const(0x08049c0e,4), o_sub(Var("esp", width=4),Const(0x0000041c,4),4),
```

Symboliks view: STAGE3 CTF Quals vuln (2005)

```
.text:0x080497c4
.text:0x080497c4  FUNC: int cdecl stage3.chldrqst( int arg0, ) [1 XREFS]
.text:0x080497c4
.text:0x080497c4  Stack Variables:
.text:0x080497c4            4: int arg0
.text:0x080497c4          -16: int local16
.text:0x080497c4        -1056: int local1056
.text:0x080497c4        -1060: int local1060
.text:0x080497c4        -1064: int local1064
.text:0x080497c4
.text:0x080497c4  55              push ebp
.text:0x080497c5  89e5            mov ebp,esp
.text:0x080497c7  81ec28040000    sub esp,1064
.text:0x080497cd  8d95e8fbffff    lea edx,dword [ebp - 1048]
.text:0x080497d3  b800040000      mov eax,1024
.text:0x080497d8  83ec04          sub esp,4
.text:0x080497db  50              push eax
.text:0x080497dc  6a00            push 0
.text:0x080497de  52              push edx
.text:0x080497df  e864f4ffff      call memset_08048c48    ;memset_08048c48()
.text:0x080497e4  83c410          add esp,16
.text:0x080497e7  c785e4fbffff0000 mov dword [ebp + local1056],0
.text:0x080497f1  83ec0c          sub esp,12
.text:0x080497f4  ff7508          push dword [ebp + arg0]
.text:0x080497f7  e850feffff      call stage3.authenticate    ;stage3.authenticate(0x41571000)
.text:0x080497fc  83c410          add esp,16
.text:0x080497ff  83ec04          sub esp,4
.text:0x08049802  6a03            push 3
.text:0x08049804  680a9c0408      push loc_08049c0a
.text:0x08049809  ff7508          push dword [ebp + arg0]
.text:0x0804980c  e827f3ffff      call write_08048b38    ;write_08048b38()
.text:0x08049811  83c410          add esp,16
.text:0x08049814  83ec04          sub esp,4
.text:0x08049817  68ff070000      push 2047
.text:0x0804981c  6800a20408      push stage3.input_buffer
.text:0x08049821  ff7508          push dword [ebp + arg0]
.text:0x08049824  e88ff3ffff      call read_08048bb8    ;read_08048bb8()
.text:0x08049829  83c410          add esp,16
.text:0x0804982c  8945f4          mov dword [ebp + local16],eax
.text:0x0804982f  83ec04          sub esp,4
.text:0x08049832  8d85e8fbffff    lea eax,dword [ebp - 1048]
.text:0x08049838  50              push eax
.text:0x08049839  680e9c0408      push str_bacon:%s_08049c0e
.text:0x0804983e  6800a20408      push stage3.input_buffer
.text:0x08049843  e8d0f3ffff      call sscanf_08048c18    ;sscanf_08048c18()
```

Symboliks view of the STAGE3 CTF Quals vuln from 2005

```
(read == 0x8048bb8)
CallFunction( 0x08049824, Const(0x08048bb8,4), [Var("arg0", width=4),
    Const(0x0804a200,4), Const(0x000007ff,4)] )

(sscanf == 0x8048c18)
CallFunction( 0x08049843, Const(0x08048c18,4), [Const(0x0804a200,4),
    Const(0x08049c0e,4), o_sub(Var("esp", width=4),Const(0x0000041c,4),4),
```

def grok():

- GROK: to understand profoundly and intuitively (Merriam Webster)
- GROK: low-level, deep, intimate understanding (atlas)
- _____ the planet

  a)grok

  b)grok

  c)grok

levels of understanding

- buzzword bingo
- conversant but untested
- done it once (powerful step, this...)
- veteran
- master

grok all the things

- sometimes being able to identify one arbitrary pattern can be key to solving a major problem
  - pen-testing
  - forensics
  - reverse engineering
  - new areas of research / combined attacks

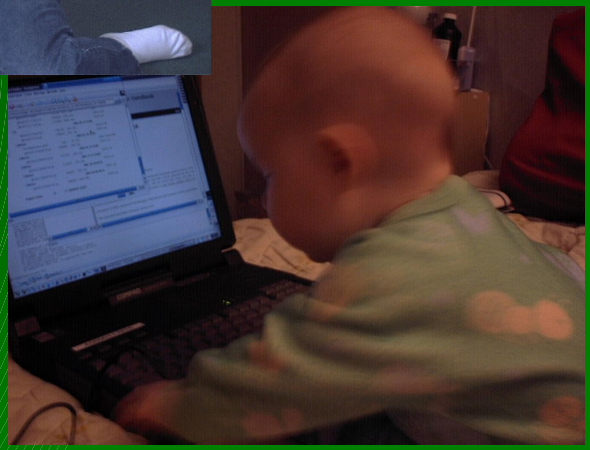
Joint Pen Testing Projects

- maturing of the field:
  - hardware / software reversing
  - cyber / physical / social
  - IT / control systems

- just learning how to think about the combined, complex world we live in is an art form to be mastered

TOO MANY THINGS!

- yeah...
  - father of 3 daughters
  - husband of but one wife
  - farm life



- i work average about 50 hours a week
  - i work with what doesn't cost me too much

TOO MANY THINGS!!!

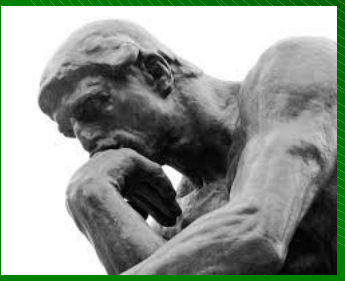
- too many things to grok, so little time!
  - impromptu expertise – what the job needs
    - tom liston
  - play, learn, teach, mentor
    - regularly
    - put together puzzles for your team/SANS class/etc.
    - or just make a neato script for your signature
    - reading and typing... in concert
- must... focus... energy... and... time....
- yeah, but how!

protips for grokking all the … and living to tell about it

- do what you love! and limit scope
- self-inspection
  - identify your own weak areas
    - sober self-assessment
- sharpening the saw
  - spend 4+ hours a week playing... for pay... at your day job...
  - tell your boss i said it was ok. it is mandatory for this field (attempt to get their buy-in)
  - not just at work. hobbify!
  - balance^H^H^H^H^H^H^Htension

sharpening the saw

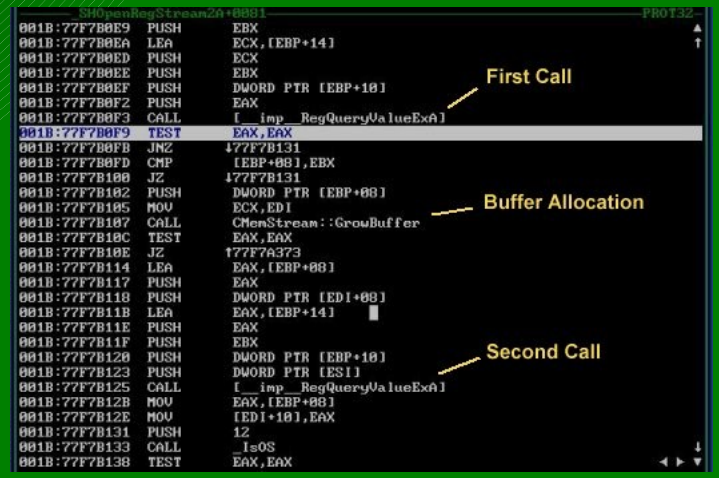
- allow yourself to **believe** in you
- allow yourself to **revel** in the growth process
- allow your **curiosity** to get the better of you for a while, on a **regular** basis
- **envision** the *hacker* - and *person* - you wish to become.



  - what do i want to be when i grow up?
    - i'm 40 and i still ask myself this Q
  - where am i weak? how can i fix? (**play**)
- then, **make** it so.
  - using your regular play-time

pen testing suggestions - bin

- vulnerability info flow
  - how to learn about new vulns
- vuln types
  - some require tools
  - some only require creativity (and netcat or equivalent level of power)
- how vulns work
- exploit toolkits
  - metasploit, of course
  - core impact?
  - canvas?



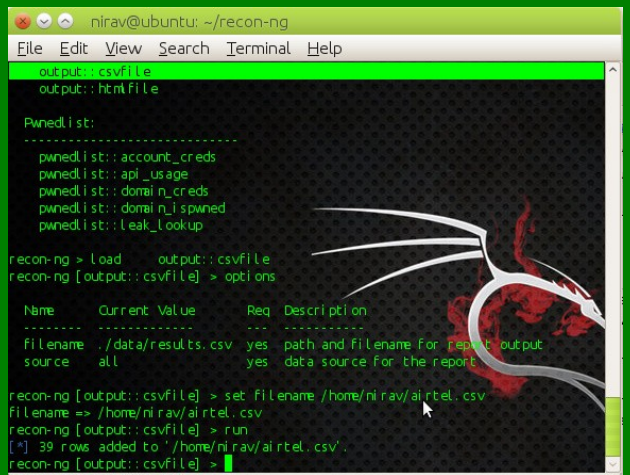
pen testing suggestions – bin (2)

- exploit underground
  - use a throw-away computer
- post-exploitation
  - meterpreter or other like payload
    - or write your own!
  - what is interesting to us?
    - data collection and interpretation
- Netcat Gender-Benders!
- powershell and other target-power
- SANS 560 and 504 ;)

pen testing suggestions – web

- http – it's the carrier of our stuff
- tools: burp, reconNG, soapUI
- vuln types: sql^H^H^Hanything injection, XSRF, XSS, auth-bypass
- tech: Browsers, Flash, Acrobat, JRE, ActiveX, HTML5, video players, etc...

  – whatever attack surface comes up
- crypto
- effective MITM
- SANS 542 and 642



hardware testing suggestions

- reading chip data sheets — master this!
- heck, **finding** datasheets
- SPI / I2C / USB / PCI / Ethernet
- electricity
- rf
- tools: bus-sniffers/injectors, RfCat, HackRF, GoodFET, Arduino or other ad-hoc tool of choice

tech summary

- get in the middle of things, where you can manipulate/interpret

  <snip - removed disturbing vivisection image>

- get to know the lay of the land, break it down... prove your own understandings.
- hunting... the prey is out there... are you ready to predate?
- balance new and existing skillset development

  - measure by weeks/months (ie. avoid THRASHING)

IT sec / pen testing suggestions

- spend time being a normal person (perhaps, 1h/week?)
- communication skills
  - making “contracts” like programming

- scoping
  - SANS 560! set expectations and over-deliver!
- project management
  - companies will often pay for courses!
- 0-day — strategy, where it fits...
- binary/hex/encodings/magic numbers

gratuitous hackers quote

"My son happens to be a genius. He GROKs something happening today that you won't GROK if you live to be a hundred, and he would never use what he knows to harm a living soul."

how to sharpen the saw - environment

- sometimes it's music
  - sometimes familiar, other times new
- sometimes quiet
- limit distractions
- sometimes long periods of time
- sometimes every spare second... in the midst of other things

getting the idea that there is no perfect environment? but you can get to know what you need... and for what part of the work.

how to sharpen the saw - you

- think and process. play with concepts in your mind... make the connections
  - menial tasks: do the dishes, mow the lawn, rototilling is one of my favs
- get to know what your mind/heart needs and what your circumstances allow
- IMPORTANT: make boundaries
  - prioritize, schedule, breathe.
  - believe it or not, you will not be a very satisfied hacker if you lose everything in the process.
  - diligence is **more powerful** than flash-burn.

`the slide that doesn't exist`

- psssst... just between friends
  - i'll deny it if you say that i wrote this slide...

- **caffeine is a terrible substitute for sleep**

john cleese on creativity

- half hour video
- google it
- watch it
- that is all.

https://www.youtube.com/watch?v=08FCXGDtZoU

oh, but humor helps

- and hot chicks? too!
- enjoying the people you work with helps too.
- not that way, ew...

practicing your light saber foo too...

or truly enjoying your bling (bingo!)

knowing you're crazy, and still going for it...

6 Keys to Being Excellent At Anything — Tony Schwartz

http://blogs.hbr.org/2010/08/six-keys-to-being-excellent-at/

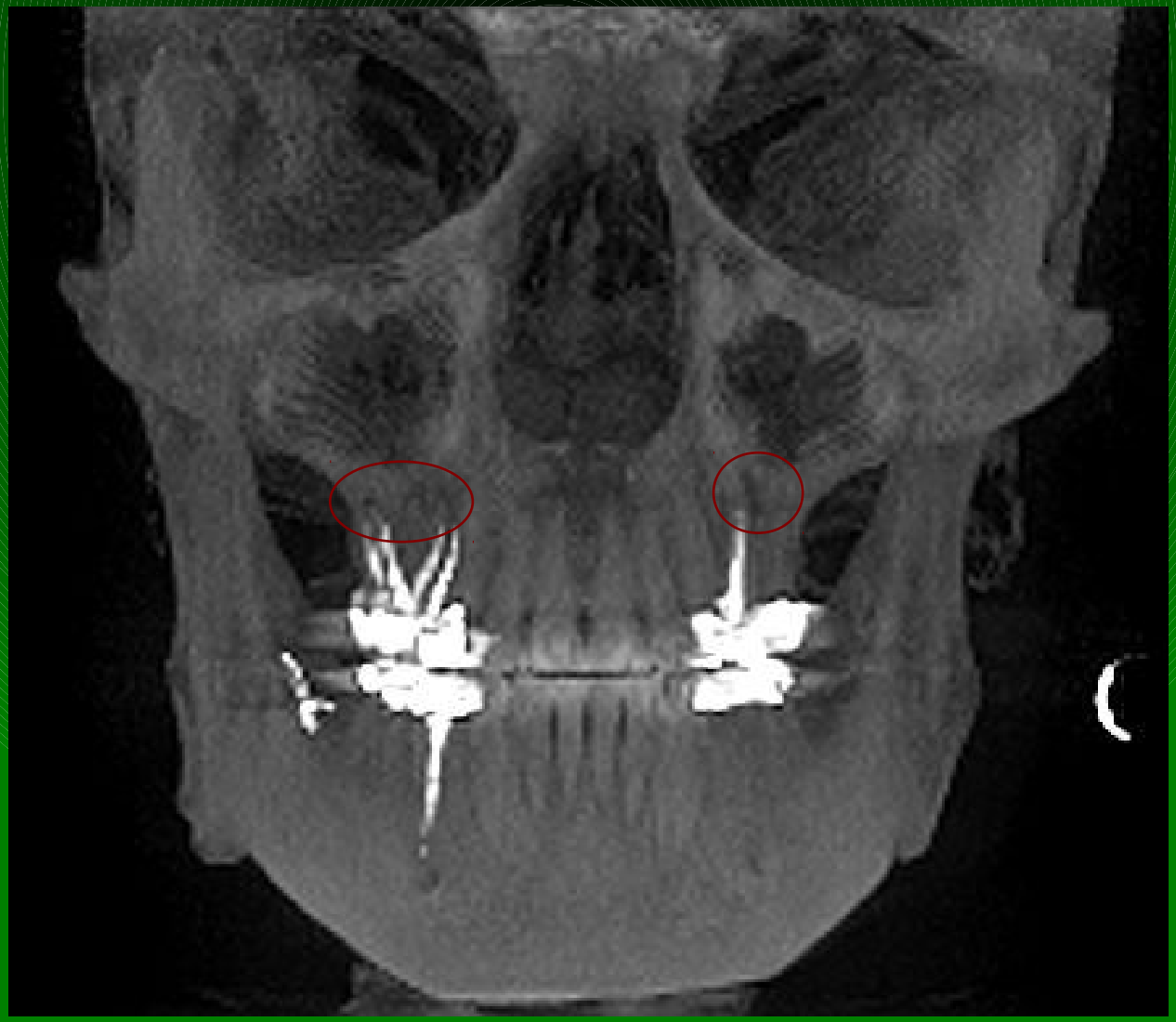
- Pursue What You Love
- Do the Hardest Work First
- Practice intensely: 90min, <5hours/day
- Seek Expert Feedback, Intermittently
- Take Regular Renewal Breaks
- Ritualize Practice

10000 hours to expertise

10000 / 25 hrs:week / 50 weeks:year = 8 yrs

mental health

physical health



holy crap, dental health?

tech ninjas, a word...

- become experienced at the breadth
- be excellent at some...
  - what you love or what is required - sometimes needs dictate your focus. **this is ok.**
- communicate well — in terms of others
- set expectations
- commit... and over-deliver.
- think and speak in terms of mission, goals, team, business
- expect to **respectfully** educate your boss
- expect to be educated by them as well...

corporate phb's

- building a team of cyber-ninjas is not easy
- keeping them happy is it's own game altogether
- keeping them growing and enjoying is where to focus
- “care and feeding of your cyberninja” - not written yet
- push for respectful behavior...
- set an environment of team identity
- you are the business ninja... your cyberninja's **need** you. make it easy for them to succeed!
  - they need your protection and <3
- “you'll never get as much from a team long term, than if they love you. this **requires** that you love them first.” -me

summary

- grok all the shizzle... that you can - never stop growing
- when in doubt, focus on what you love
- soberly assess your weak areas
- treat them as challenges, not as suckages
  - sharpen the saw... while keeping the wheels on.
- communicate well
- learn the tech and the business savvy...
  - it's about what other people need and value
- PLAYPLAYPLAYPLAYPLAYPLAYPLAYPLAYPLAYPLAY

references

- http://en.wikipedia.org/wiki/Magic_number_(programming)
- http://en.wikipedia.org/wiki/List_of_file_signatures
- http://svnweb.freebsd.org/base/head/contrib/file/Magdir/
- http://blogs.hbr.org/2010/08/six-keys-to-being-excellent-at/
- http://www.itburnout.org/tag/jack-daniel
- http://sans.org