PROJECT

SMASHING THE SLACK

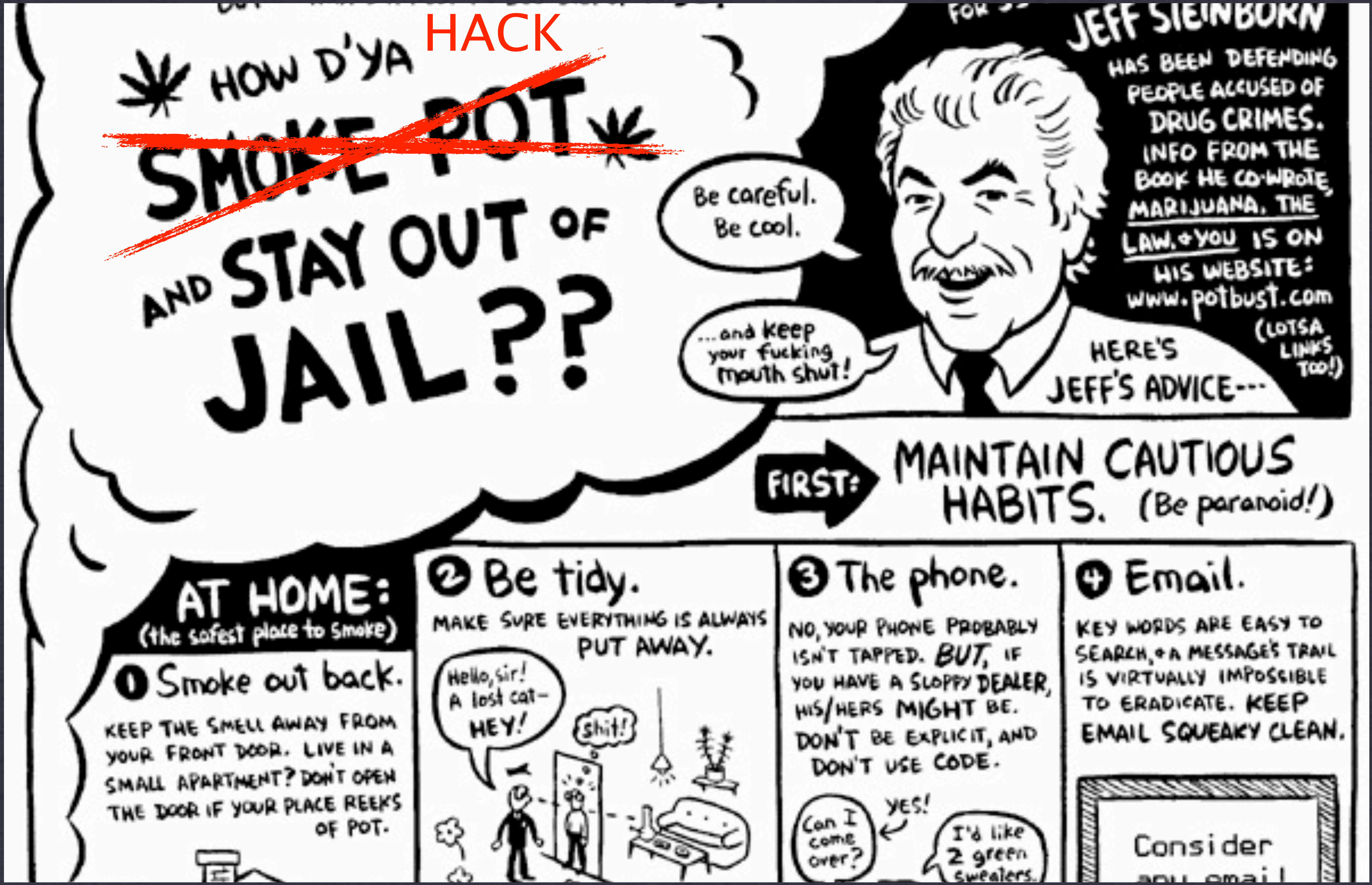
FOR FUN AND PROFIT

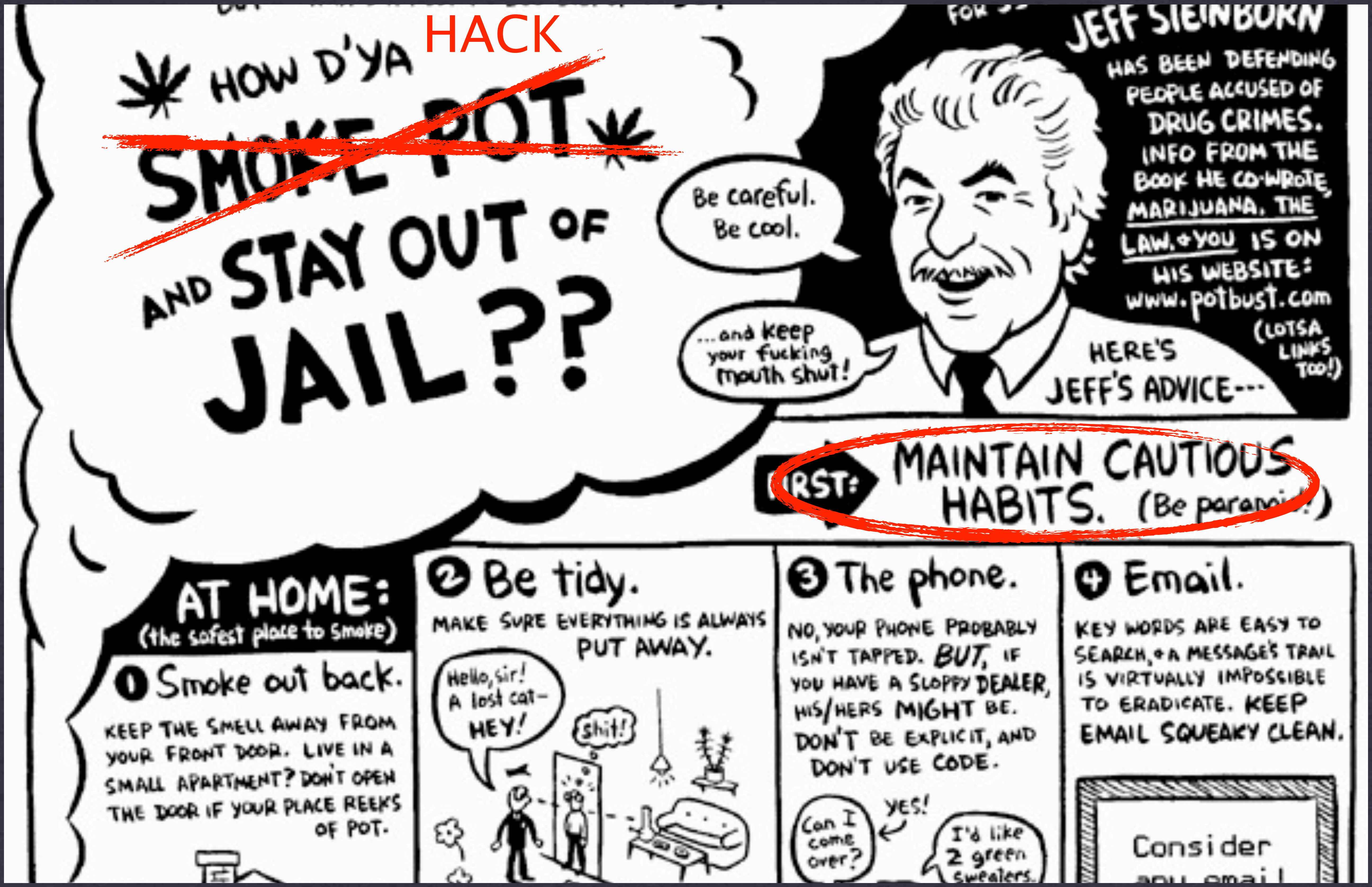
DATE **HITB2011KUL**

CLIENT **THE GRUGQ**

A Talk in Three Parts

- Anti Forensics, the lightening talk
  - Data Hiding is hard ...lets go shopping!
  - Yo’ TTY so dumb, it got you 5-7 in federal.
  - Leveraging cloud synergies for exfiltration solutions
- Happy Ending


HOW D'YA HACK ~~SMOKE POT~~ AND STAY OUT OF JAIL??
Be careful. Be cool.
...and keep your fucking mouth shut!
JEFF STEINBORN HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)
HERE'S JEFF'S ADVICE---
FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)
AT HOME: (the safest place to smoke)
1 Smoke out back.
KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.
2 Be tidy.
MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.
Hello, sir! A lost cat— HEY!
Shit!
3 The phone.
NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.
Can I come over?
YES!
I'd like 2 green sweaters.
4 Email.
KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.
Consider any email


HACK
HOW D'YA ~~SMOKE POT~~ AND STAY OUT OF JAIL??
Be careful. Be cool.
...and keep your fucking mouth shut!
JEFF STEINBORN HAS BEEN DEFENDING PEOPLE ACCUSED OF DRUG CRIMES. INFO FROM THE BOOK HE CO-WROTE, MARIJUANA, THE LAW, & YOU IS ON HIS WEBSITE: www.potbust.com (LOTSA LINKS TOO!)
HERE'S JEFF'S ADVICE---
FIRST: MAINTAIN CAUTIOUS HABITS. (Be paranoid!)
AT HOME: (the safest place to smoke)
1 Smoke out back.
KEEP THE SMELL AWAY FROM YOUR FRONT DOOR. LIVE IN A SMALL APARTMENT? DON'T OPEN THE DOOR IF YOUR PLACE REEKS OF POT.
2 Be tidy.
MAKE SURE EVERYTHING IS ALWAYS PUT AWAY.
Hello, sir! A lost cat- HEY!
Shit!
3 The phone.
NO, YOUR PHONE PROBABLY ISN'T TAPPED. BUT, IF YOU HAVE A SLOPPY DEALER, HIS/HERS MIGHT BE. DON'T BE EXPLICIT, AND DON'T USE CODE.
Can I come over?
yes!
I'd like 2 green sweaters.
4 Email.
KEY WORDS ARE EASY TO SEARCH, & A MESSAGE'S TRAIL IS VIRTUALLY IMPOSSIBLE TO ERADICATE. KEEP EMAIL SQUEAKY CLEAN.
Consider you email

Forensic Analysis

A digital forensic analyst conducts an investigation by searching for artefacts and attempting to assemble into them a complete, factually correct, re-enactment of the incident.

Forensic Analysis

- Digital forensic analyst performs the following to assist the investigation
  - Searching for artefacts
  - Combining artefacts to develop timelines
  - Develops a factually correct history of the incident

Artefacts

Residual traces of activity on a system which can contain information indicating

who what when where how

Anti Forensics

The practise of deliberately reducing the quantity and quality of evidentiary artefacts

Anti Forensic Strategies

Data Destruction

Completely removing artefacts from the system

Anti Forensic Strategies

Data Hiding

- Obscure the location of artefacts

Anti Forensic Strategies

Data Contraception

- Avoid generating artefacts (* whenever possible)

Anti Forensic Strategies

Data Blurring

Obscure factual artefacts with spurious ones

History = Narrative

- Fundamentally predisposed to developing an early hypothesis and then cherry picking the supporting evidence
- Human brain has a cognitive bias towards narrative
    - Create a compelling, believable narrative early in the investigation and direct its path.

Core Strategies

- Data Destruction
- Data Hiding
- Data Contraception
- Data Blurring

Guiding Principle

The earlier you subvert the investigation process, the better your long term survival

The forensic analyst is not your enemy.

The sysadmin is your enemy. He is the first line of defence, avoid arousing his suspicion.

BDSM FOR THE MASSES

GENERIC STRUCTURED FORMAT EXPLOITATION

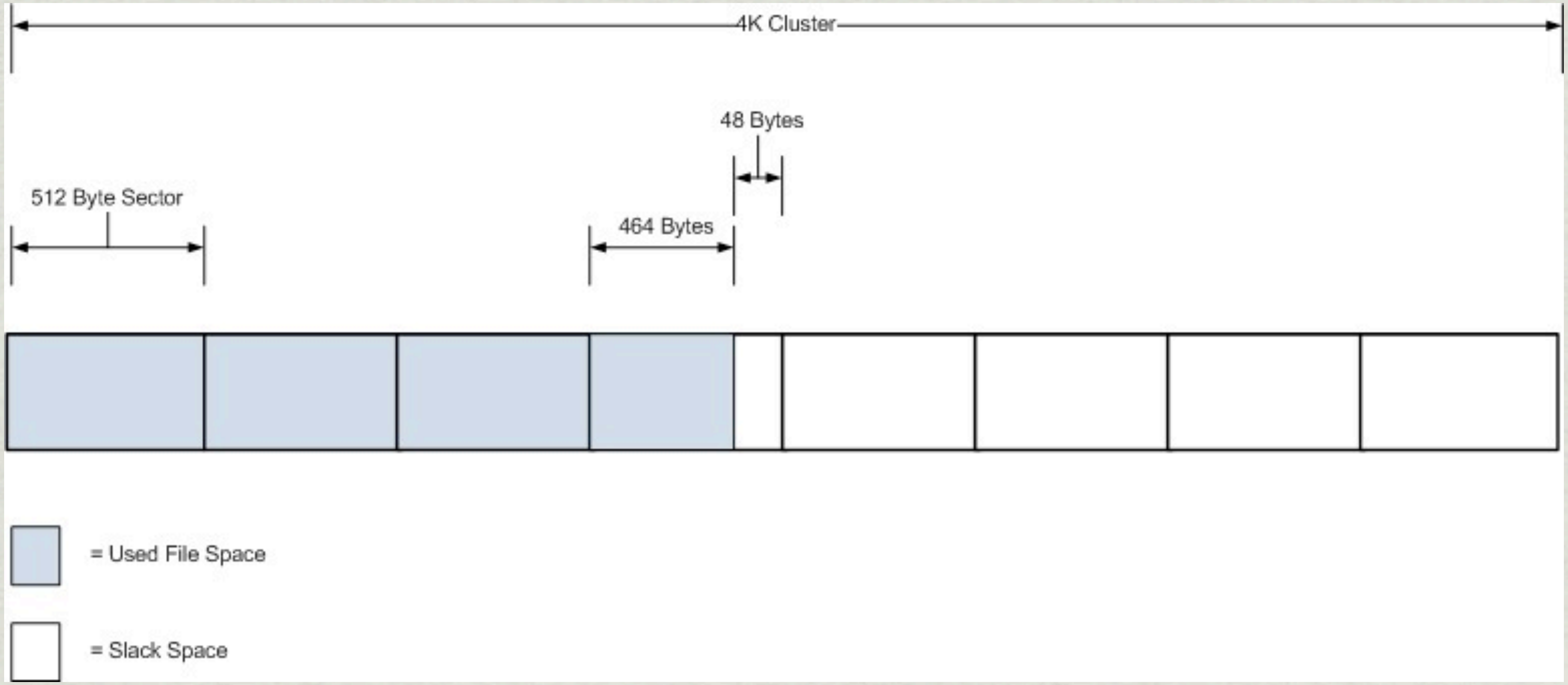
Computer Truths

- Everything is either
  - Data
  - Meta Data
  - Free Space

Data Hiding for Dummies

- All data is stored in a structured format
  - Most data has associated meta data
- Data allocation is imperfect, inefficient
  - The difference: Slack Space

Original Slack Space Gangsta



Slack space

is ubiquitous

- Office documents
- Databases
- File Systems
- Multi media
- ... pretty much anything that is used by computers

Smash the Slack

Introducing BDSM

BDSM: this is plan

- Encapsulate the slack space location specific code into a plugin
- Expose that plugin via an generic API
- Provide common utilities and features on top of that API

BDSM:zip

- ZIP file format is an array of compressed files
  - header, compressed data
- ZIP file header is in the footer (!)
  - It is at the end of the file

BDSM:zip

- Uses data at the beginning of the file as the slack storage space.
- Trivial to put together

BDSM:sqlite3

- Multiple techniques for storing data inside SQLite format files
  - Create a new table, use each row as a block
  - Parasitic insertions into existing tables
  - Free space within the file format

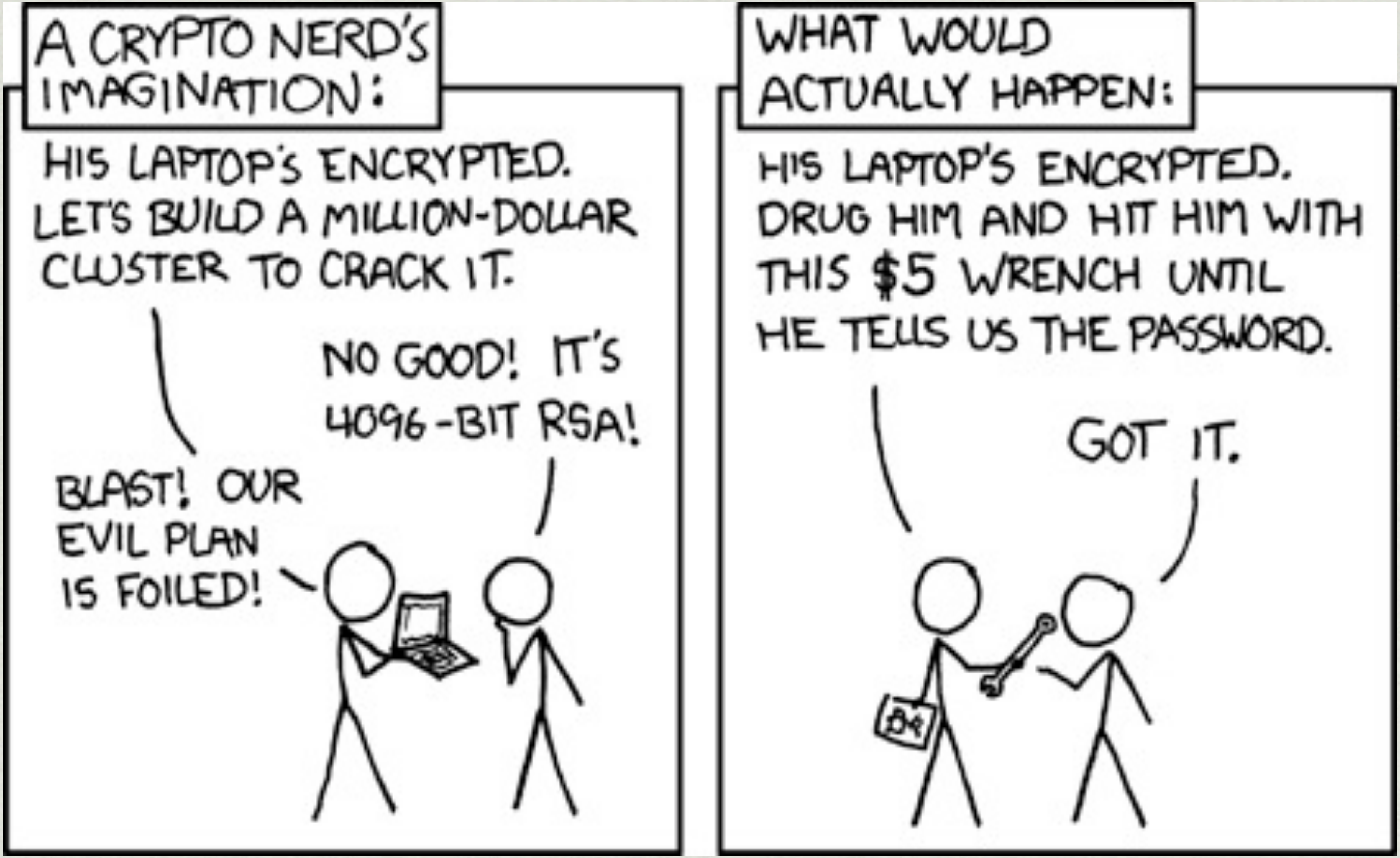
BDSM data I/O

- Linux’s Network Block Device, reinvented (ooops)
    - read(): { offset, count } resp:{ count, <data> }
    - write(): { offset, <data> } resp:{ count }
- Abstraction layer is trivial to implement,
    - the devil is in the details...

Problems with slack

- Forensic analysts are trained to look at slack space first
  - Fortunately, there is so much of it we have good odds
- Space is tight
  - typically only interesting in aggregate

- “Normal” slack space will typically contain non-random data
  - Naked encryption or compression can draw attention
-


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

An ACCESS_VIOLATION exception occurred ...
/msg #busticati I busticated all up on this Chrome piece!
50 hours later
EIP 0x41414141
2 months later
EIP 0x41414141
Fuck it. Good enough for ~~BlackHat.~~
HITB

TRY HARDER

```
at the east end of the passage.

There is a small wicker cage discarded nearby.
light lamp

Your lamp is now on.
look

You are crawling over cobbles in a low passage.  There is a dim light
at the east end of the passage.

There is a small wicker cage discarded nearby.
take cage

OK
w

You are in a debris room filled with stuff washed in from the surface.
A low wide passage with cobbles becomes plugged with mud and debris
here, but an awkward canyon leads upward and west.  A note on the wall
says "Magic word XYZZY".

A three foot black rod with a rusty star on an end lies nearby.
```

HACKING (STILL) SUCKS

1972 WANTS ITS UI BACK

Hacking Sucks

- Awesome tools that automate tedious, repetitive, error prone parts of a penetration test
  - Scanning, exploiting, maintaining access
- But nothing for penetration assistance.

  - At every step of the way, from surveying to exploiting -- there is help.
  - CANVAS, MetaSpoit nmap, hydra, etc. etc.
- Awesome

LEVERAGING CLOUD SYNERGIES FOR EXFILTRATION SOLUTIONS

Covert channels

Covert channels

in The Cloud

Abusing online storage

- Online storage is more common on the Internet these days
  - Dropbox
  - UbuntuOne
  - MegaUpload

Data Stores, obviously

- Using online storage capacity as a covert channel is old news
    - Technique such as shared web-mail and unsent drafts

Lets go subtle

- Bookmark and profile syncing from browser vendors and third parties
  - Firefox and Chrome
  - clear text

Chrome Sync

- Chrome syncs everything. Everything.
    - Filled in form details, cookies, passwords, bookmarks, history...
    - ... in plain text.
- Loads of storage capacity via the cookies

Firefox Sync

- Mozilla Weave
  - Syncs base64 encoded JSON serialized blobs of data up to 250k in size each.
  - Why, thank you, yes. I would like an anonymous, encrypted, online storage file system.

HAPPY ENDING

GOOD NEWS EVERYONE, WE’RE WINNING

Concluding Thoughts

Aspire to subtlety

Questions?

grugq@coseinc.com

http://github.com/thegrugq/dtk

src code is available. at your own risk.