Defcon 22 PDF Version

This deck has been formatted for PDF (from html)

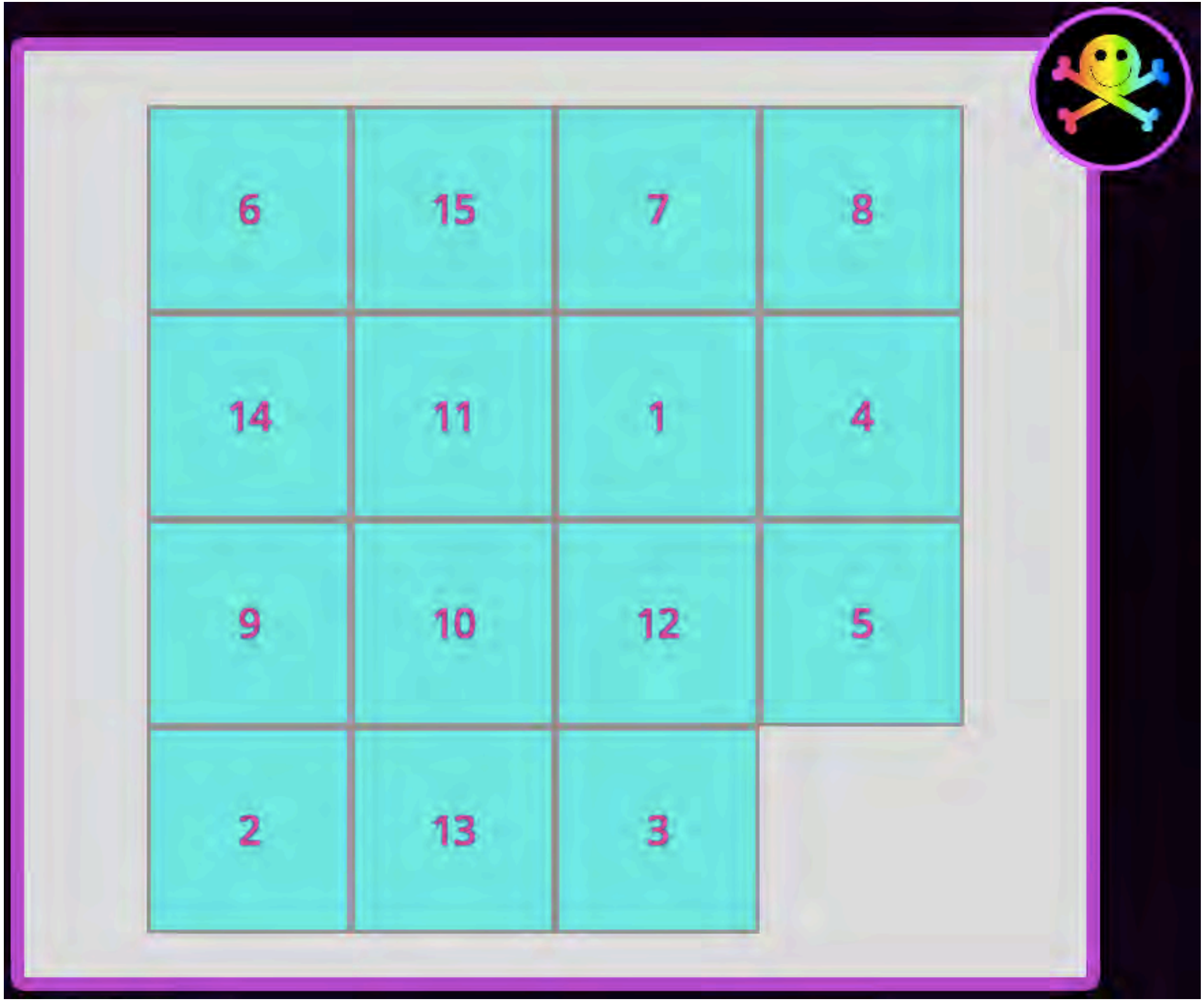
Some components of a complete presentation experience may be limited:
No live demo
No interactive slides
No video slides
Flat navigation
No attempt of slidenotes to make sense of pile of picture slides

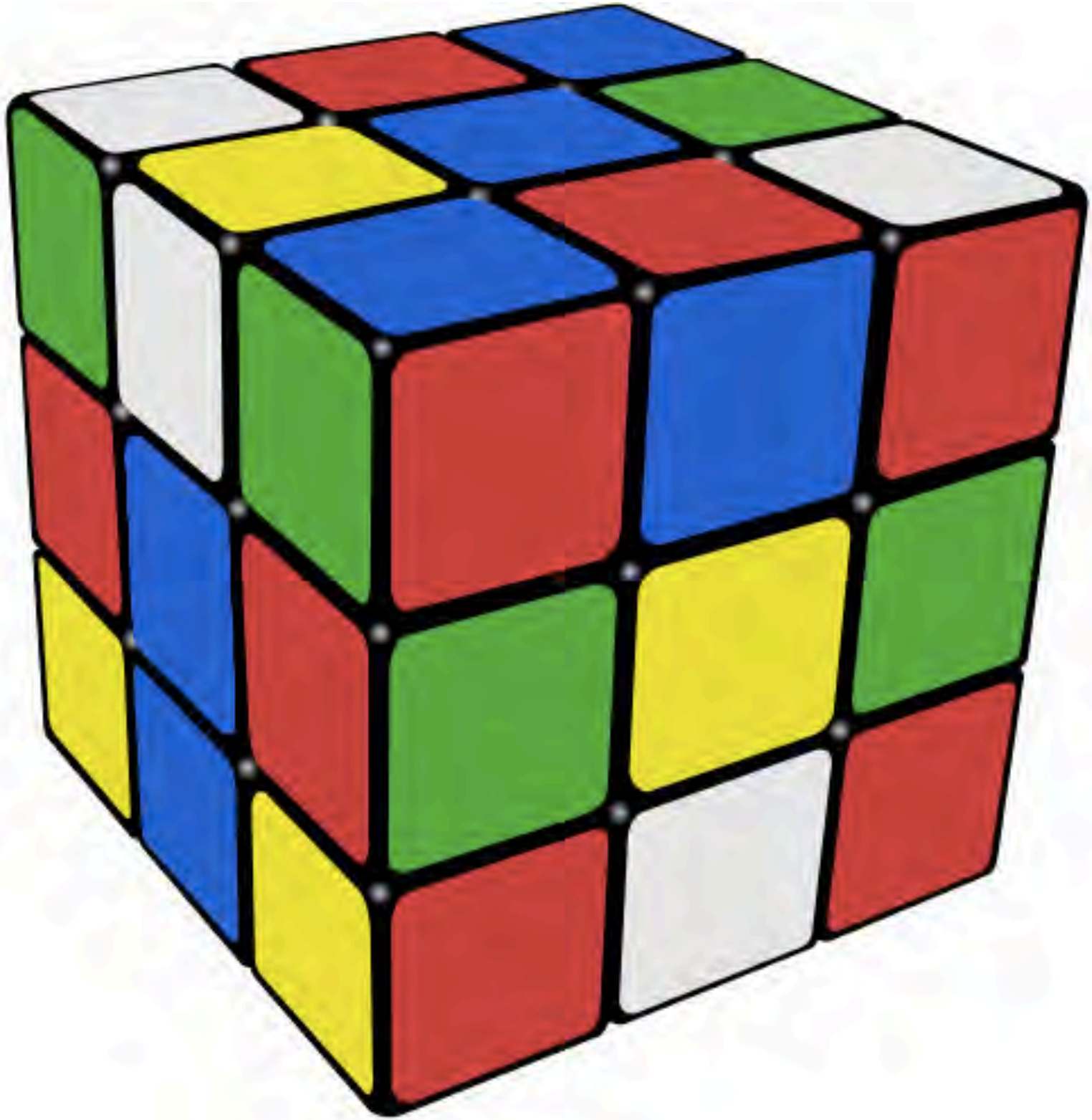
Abuse of Blind Automation in Security Tools

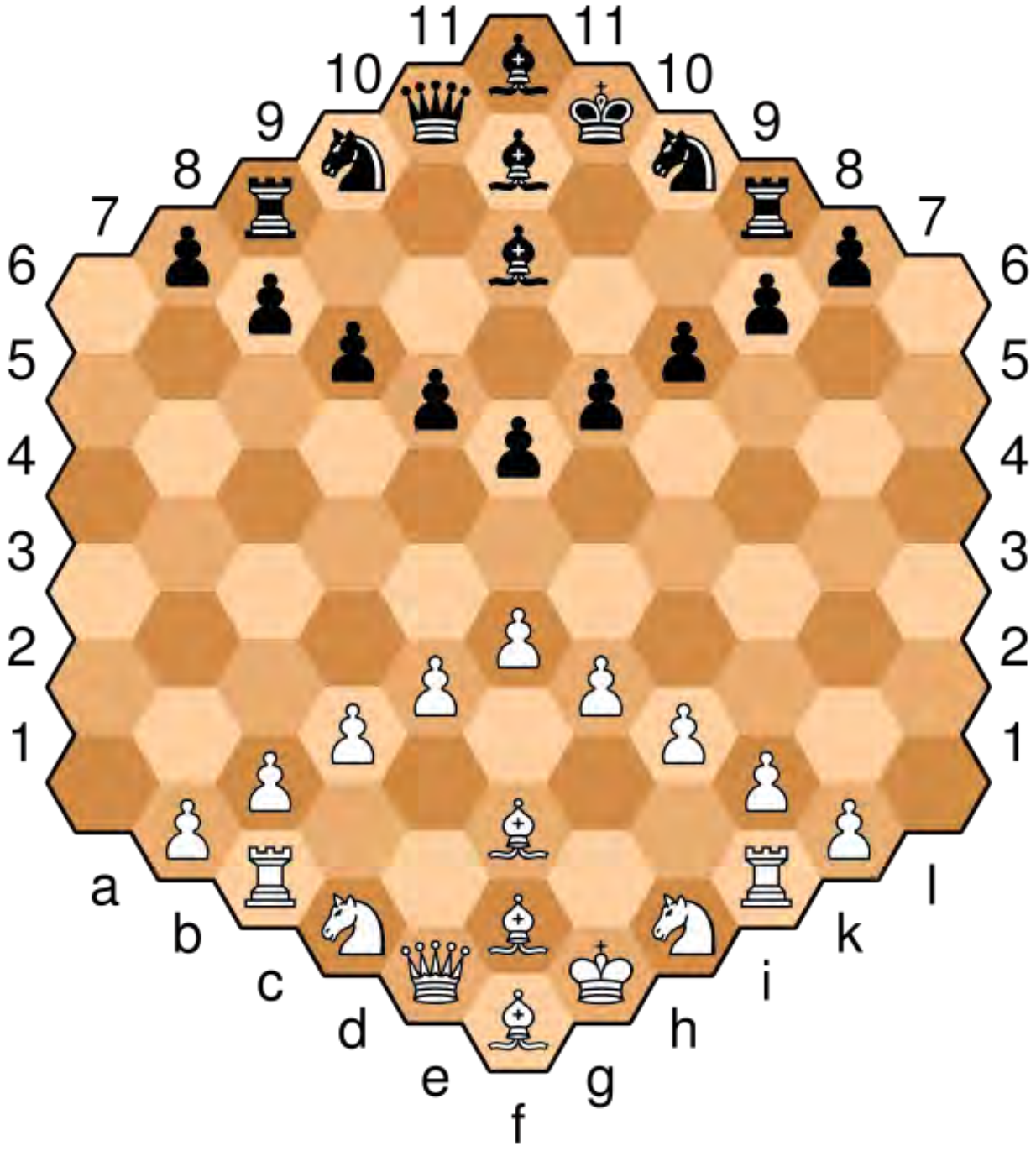
--Eric Davisson
Sr Janitor
2am Food

--Ruben Alejandro
Technical Director of Janitation
2am Food

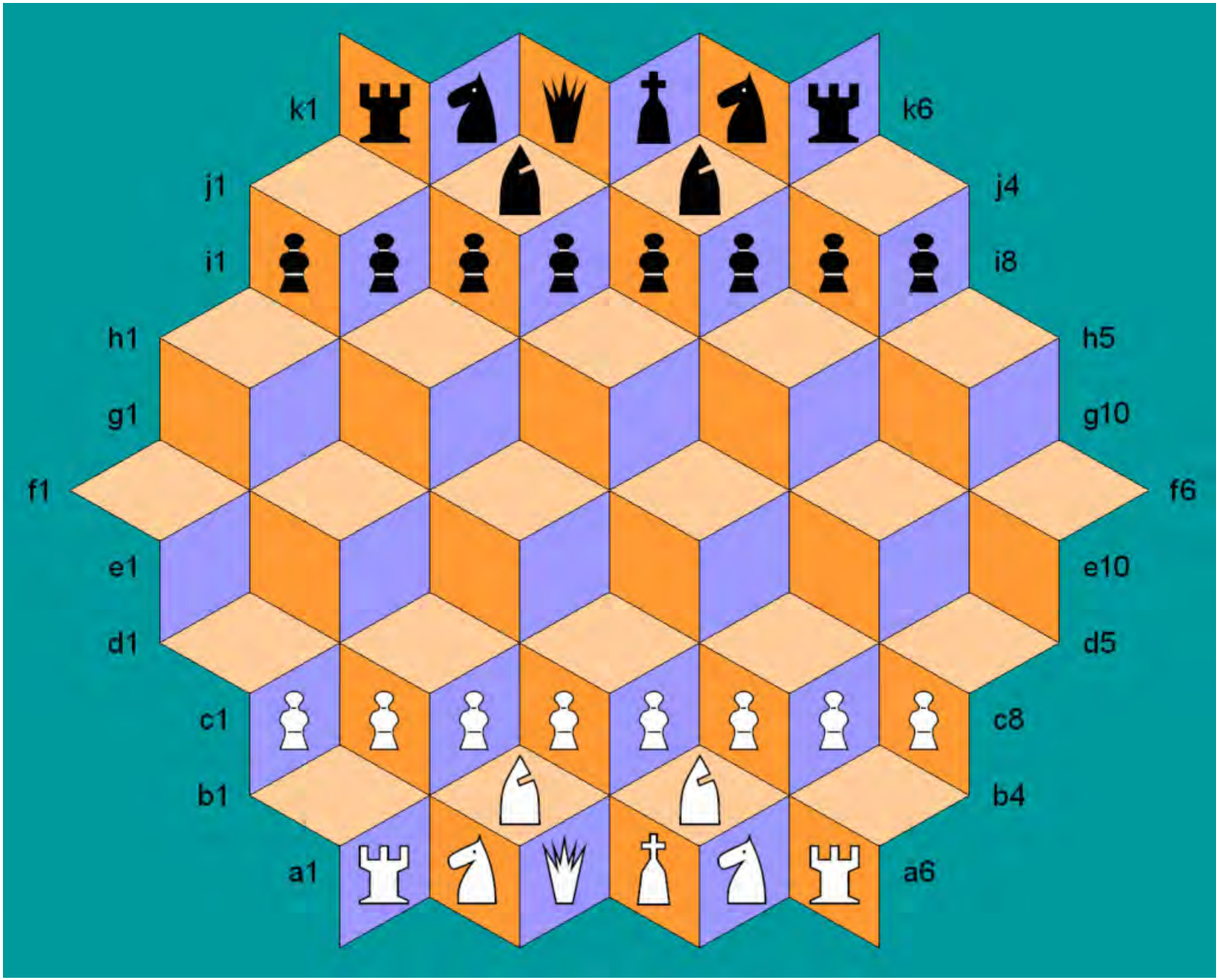
Intro / Philosophical Digression


6
15
7
8
14
11
1
4
9
10
12
5
2
13
3

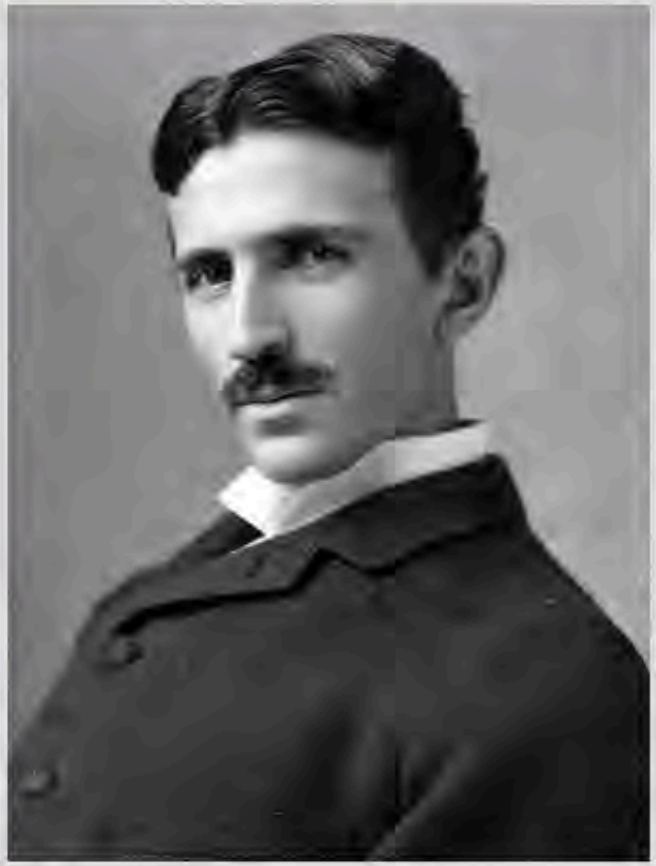



11
11
10
10
9
9
8
8
7
7
6
6
5
5
4
4
3
3
2
2
1
1
a
b
c
d
e
f
g
h
i
k
l


www.singularitoy.com

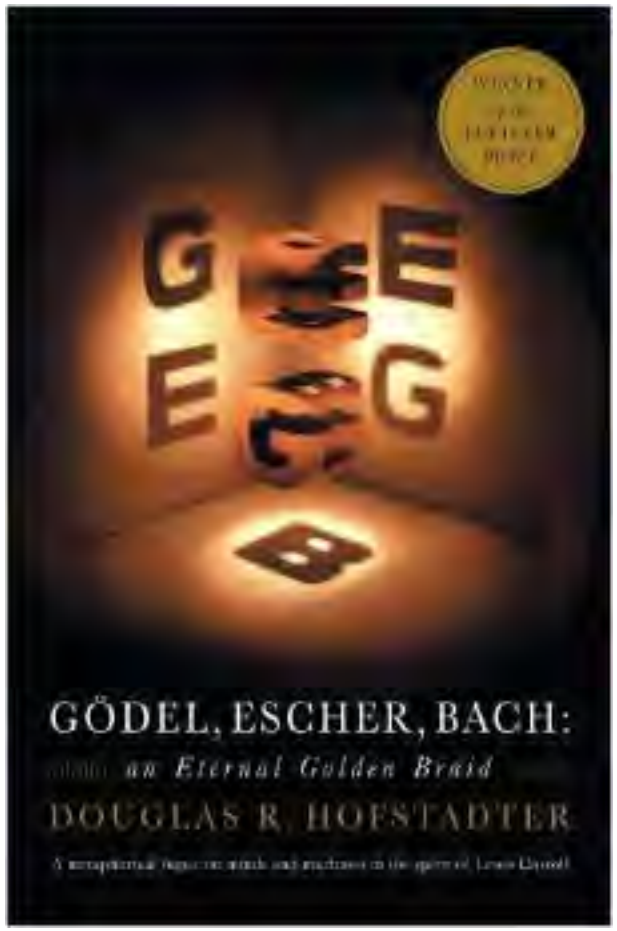

k1
k6
j1
j4
i1
i8
h1
h5
g1
g10
f1
f6
e1
e10
d1
d5
c1
c8
b1
b4
a1
a6

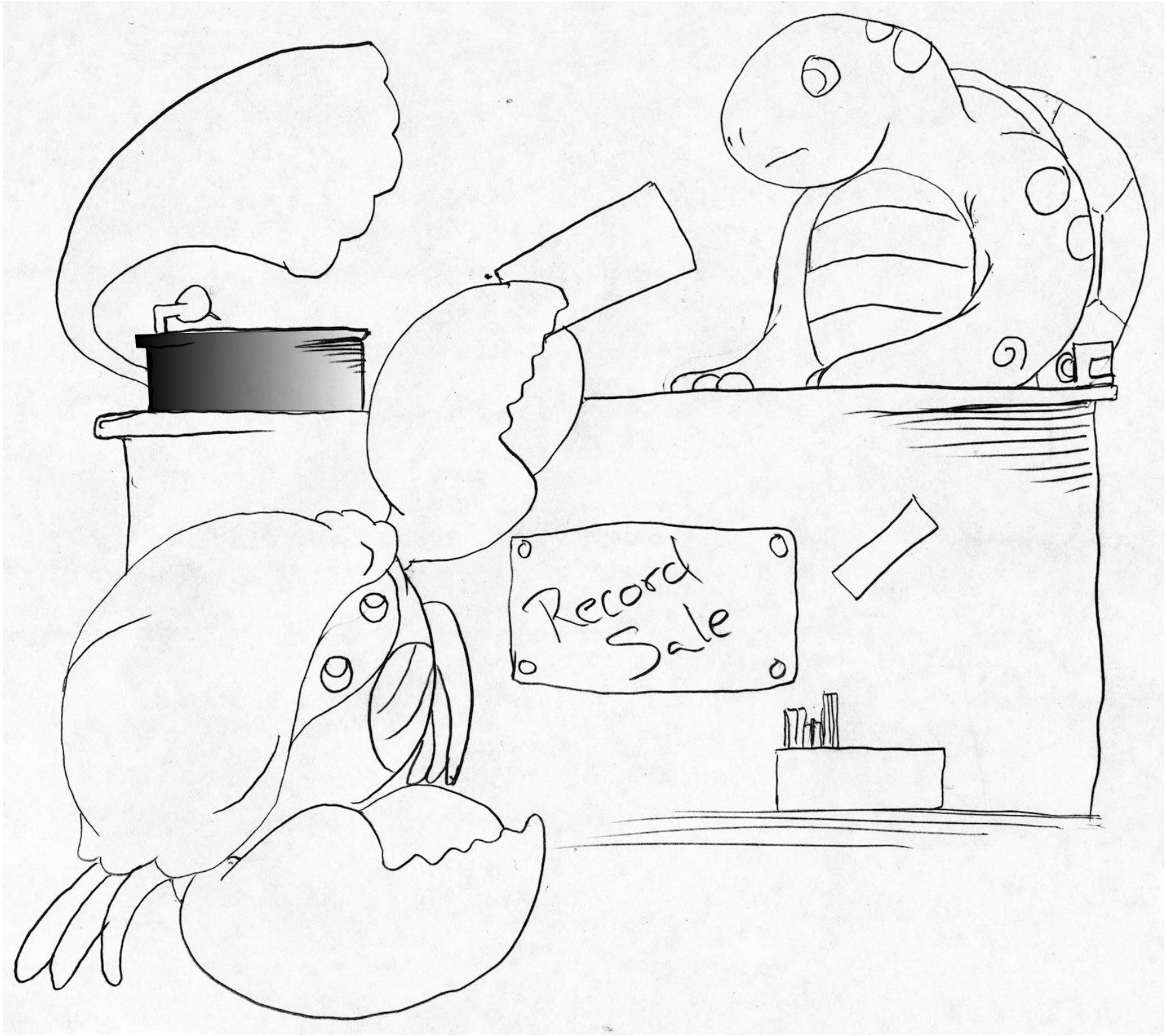

MARIO
000000
×00
WORLD
1-1
TIME
SUPER
MARIO BROS.
©1985 NINTENDO
1 PLAYER GAME
2 PLAYER GAME
TOP- 000000
00:00:01 40
0:46

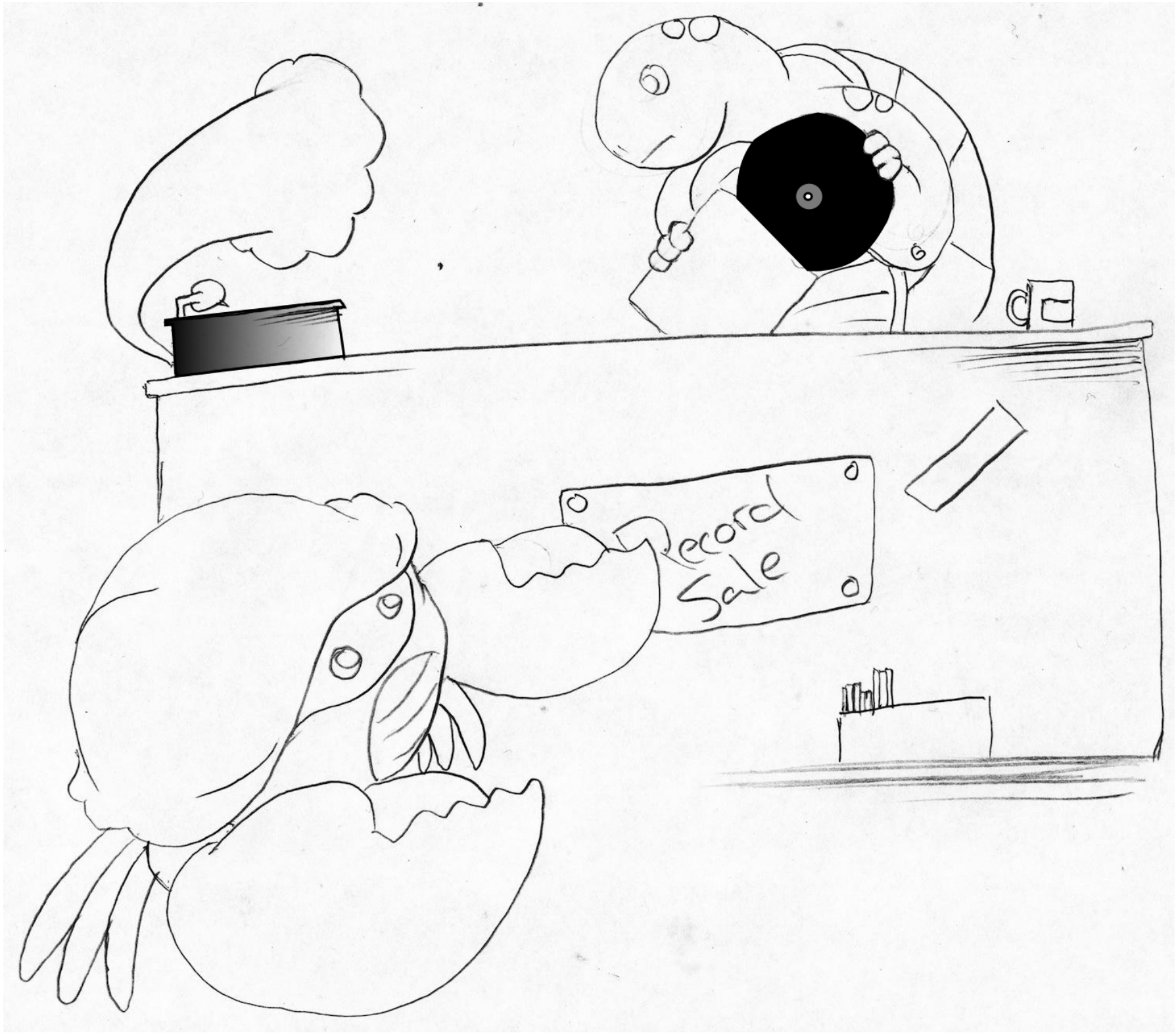


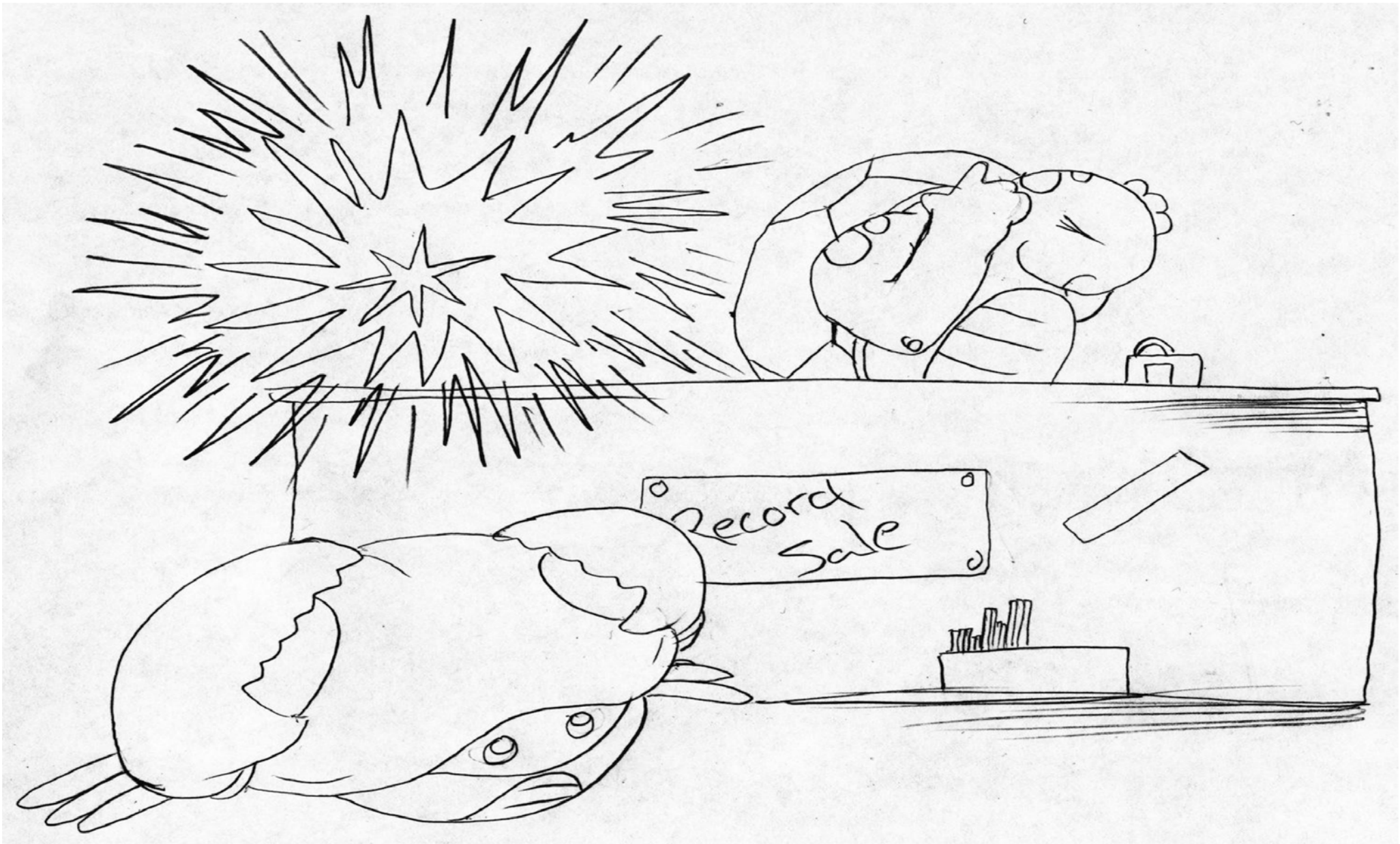
On wrecking the earth with the right resonant frequency...

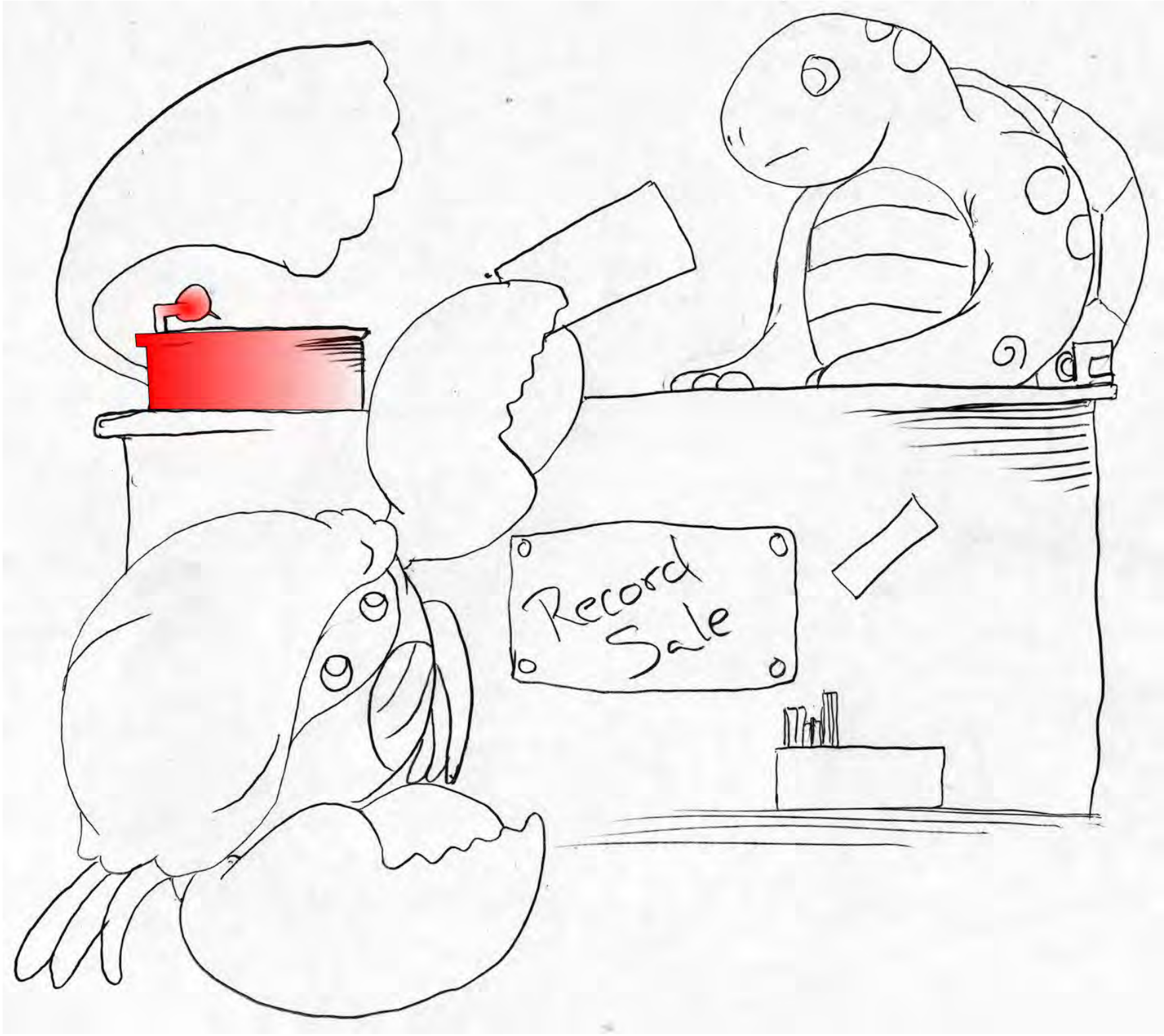
GEB: The Record Player Story

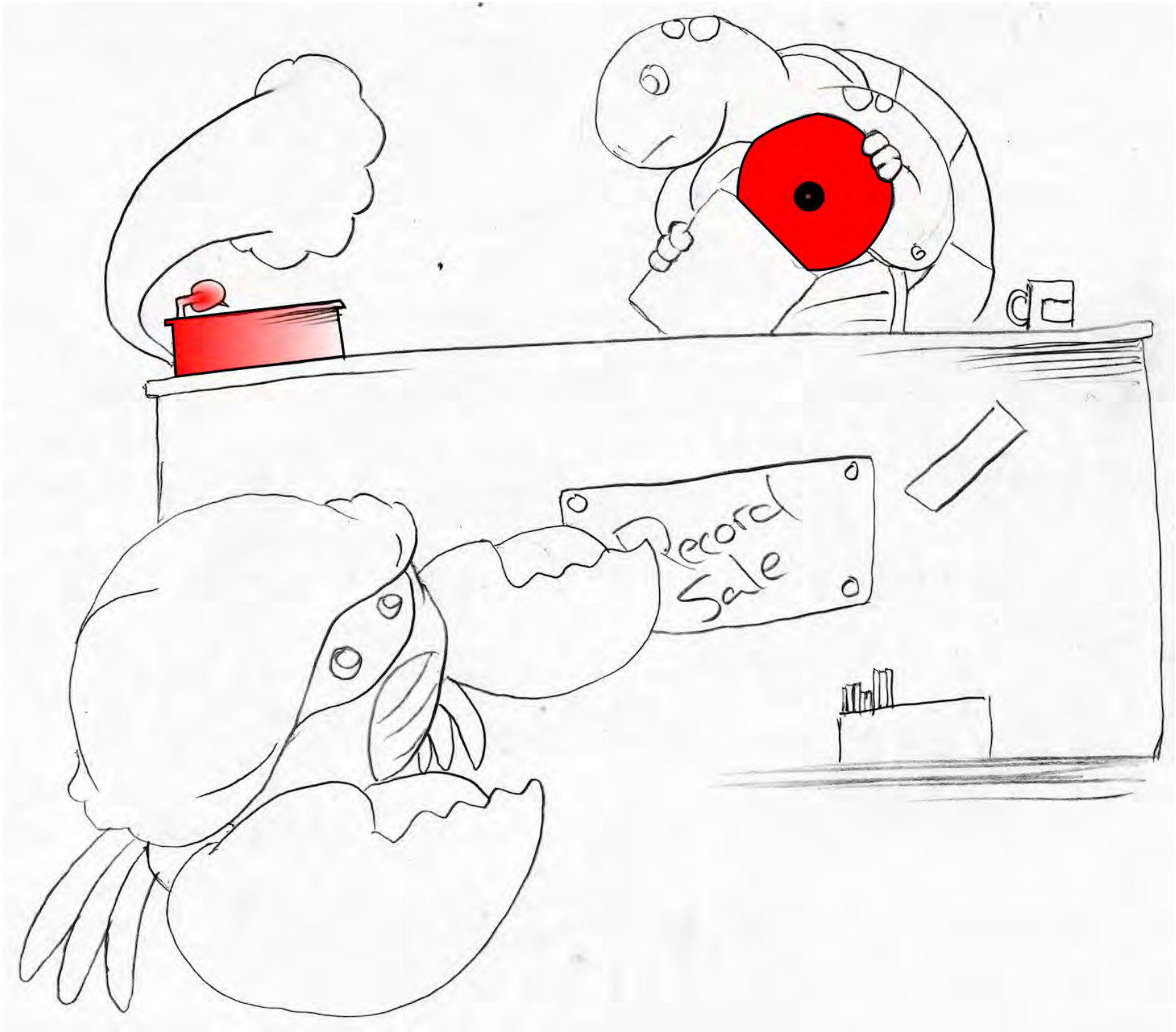

GÖDEL, ESCHER, BACH:
an Eternal Golden Braid
DOUGLAS R. HOFSTADTER

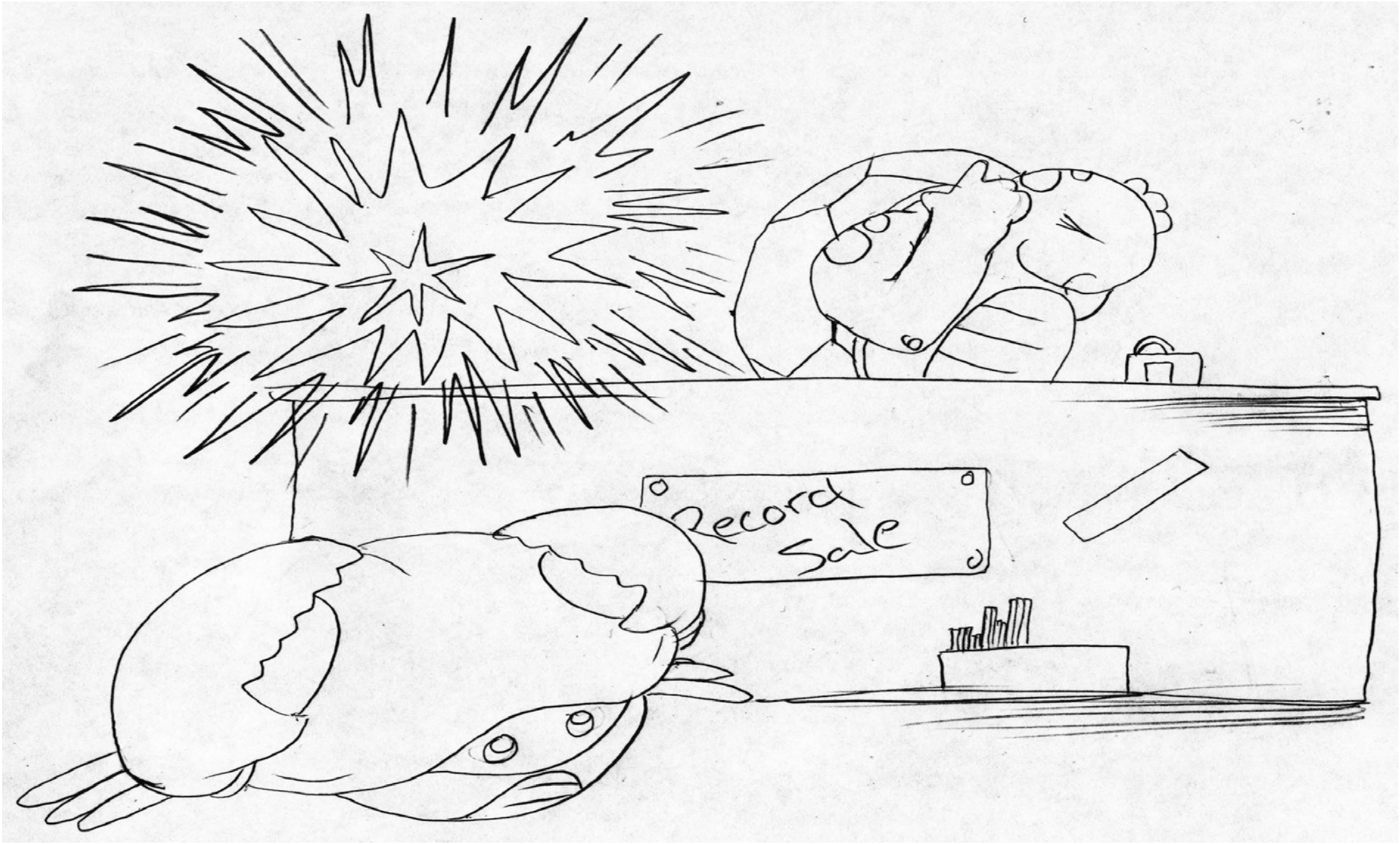

Record
Sale

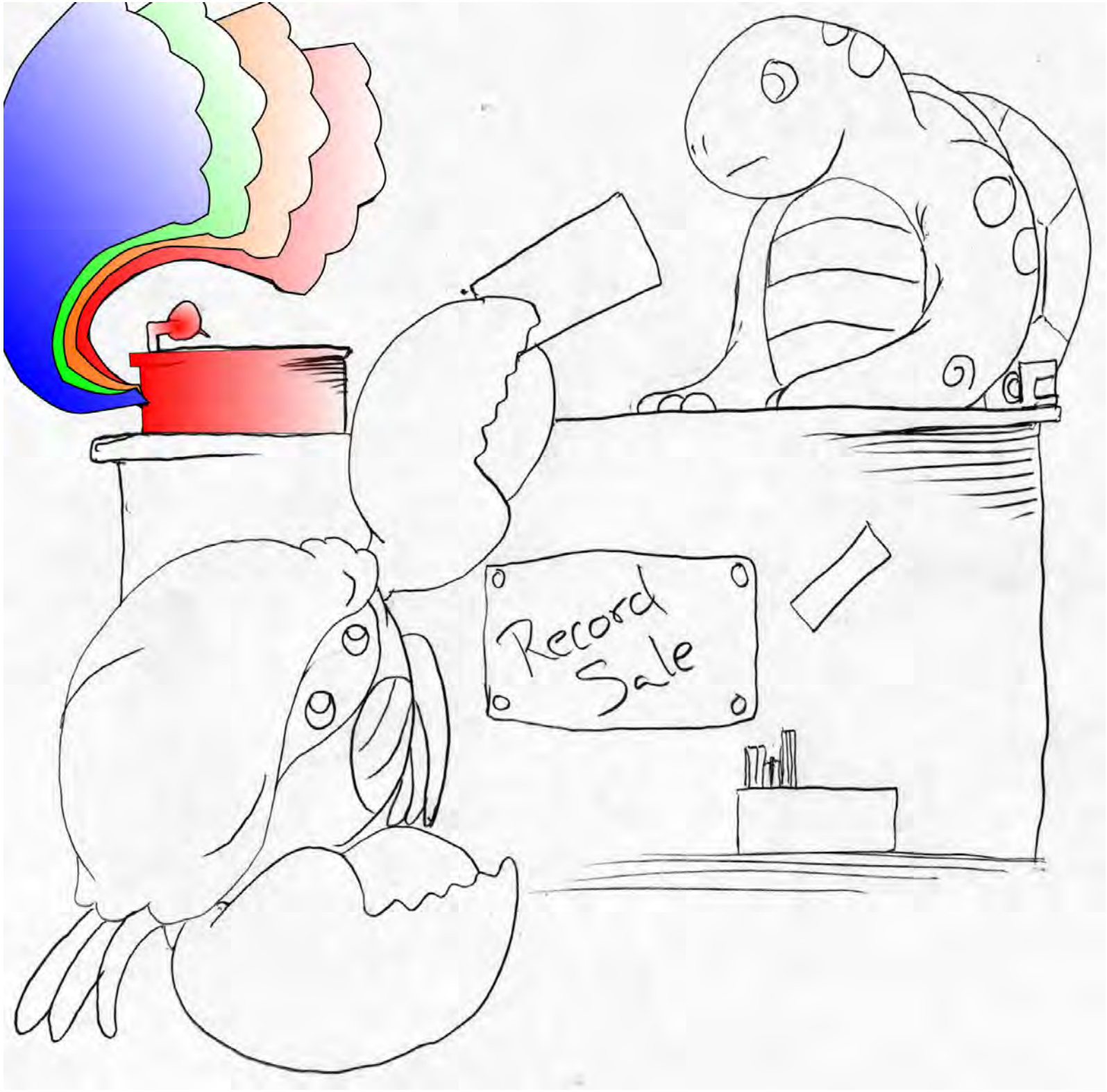

Record
Sale

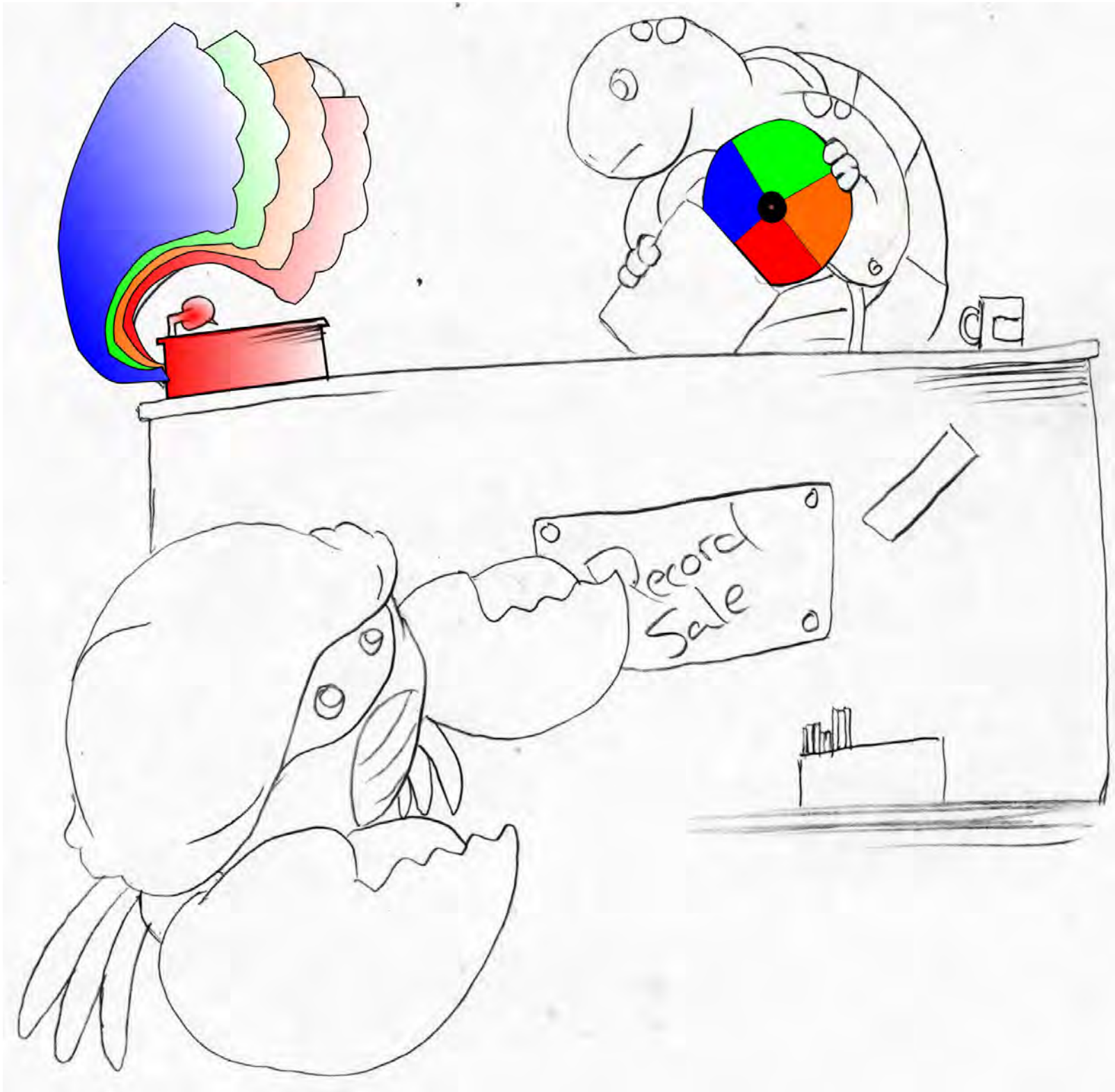

Record
Sale

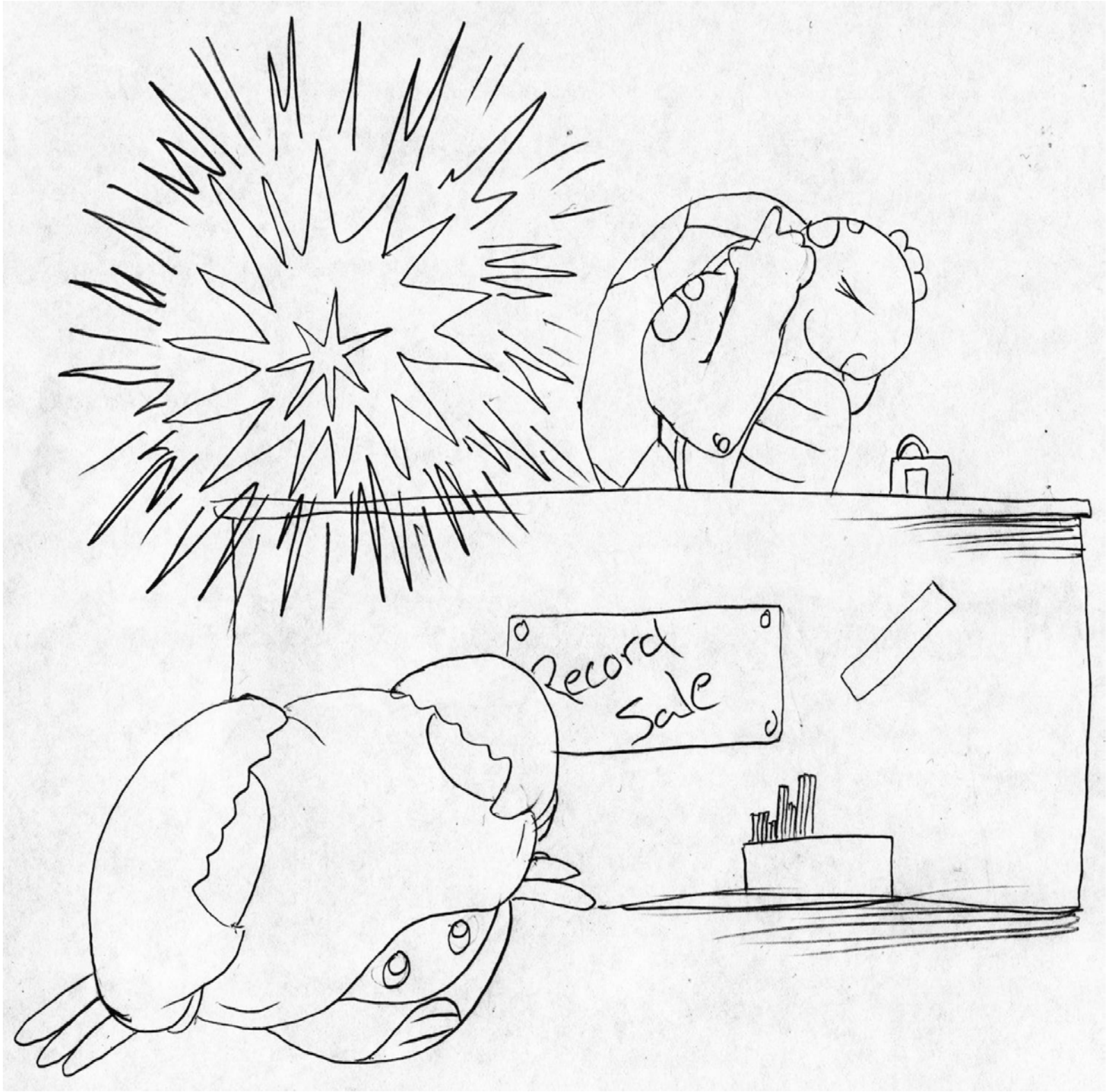

Record
Sale


Record
Sale


Record
Sale


Record
Sale


Record
Sale


Record
Sale

Liscense Plate Oddities

Funny, but not verified to work

Robert Barbour, Los Angeles

1979 - Got fines from San Francisco
eventually received 2,500 notices
He insisted on keeping the plates, so cops started using MISSING and sometimes NONE

Andrew Burg, Marina del Rey

Jim Cara, Elsmere Delaware

200 violation notices ranging from $55 - $125

Richard Turner, Beverly Hills

Ralph August, Westchester

Scottie Roberson, Huntsville, Alabama

2009 - $19,000 in fines

"Pimping"

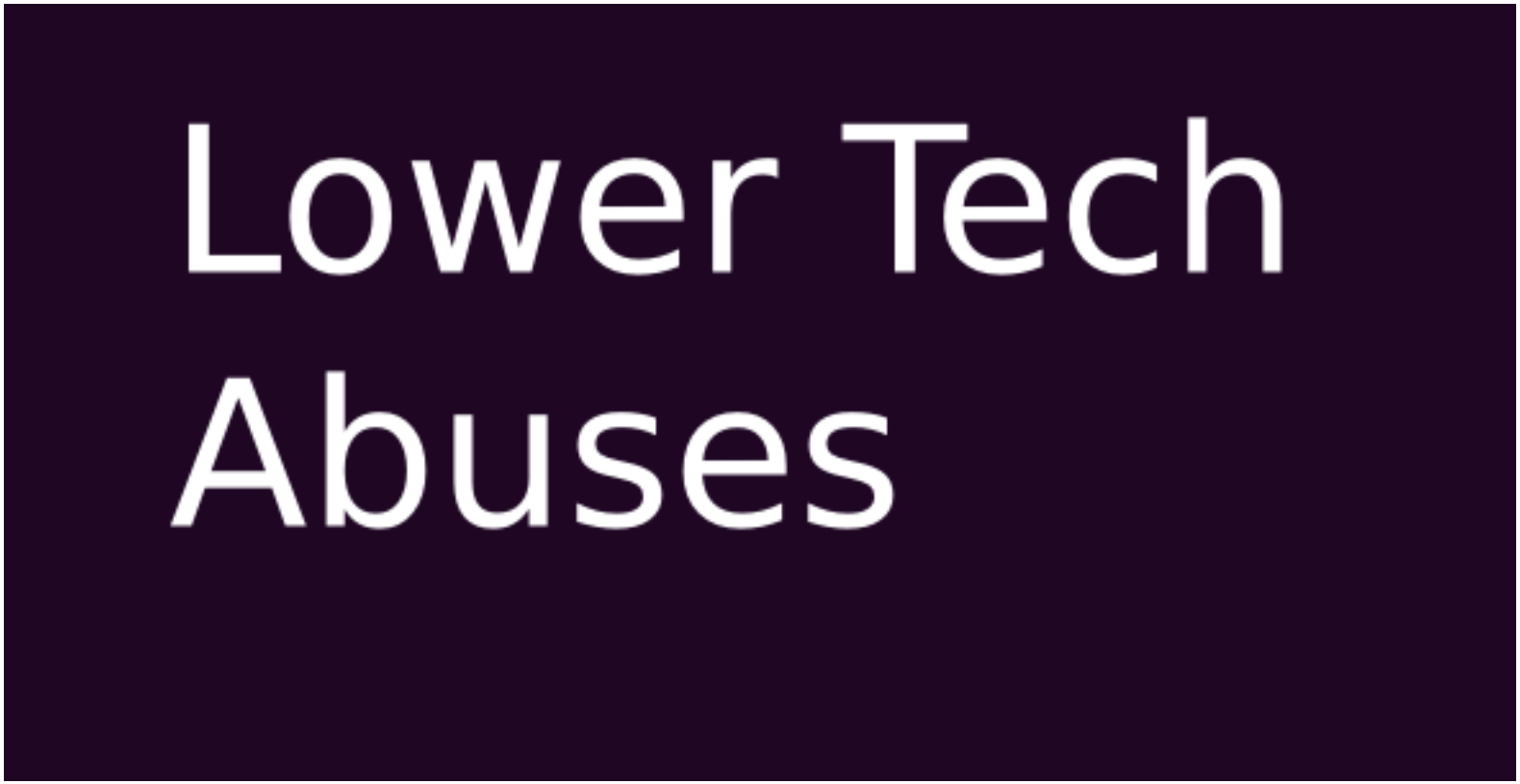
Find liscense plates of victim

Falsify those plates as your own

speed through an automated speed camera

Victim gets a ticket

This was big in Maryland around 2008-2009


Lower Tech
Abuses


Pirate Eye

www.pirateeye.com

Google

pirateeye

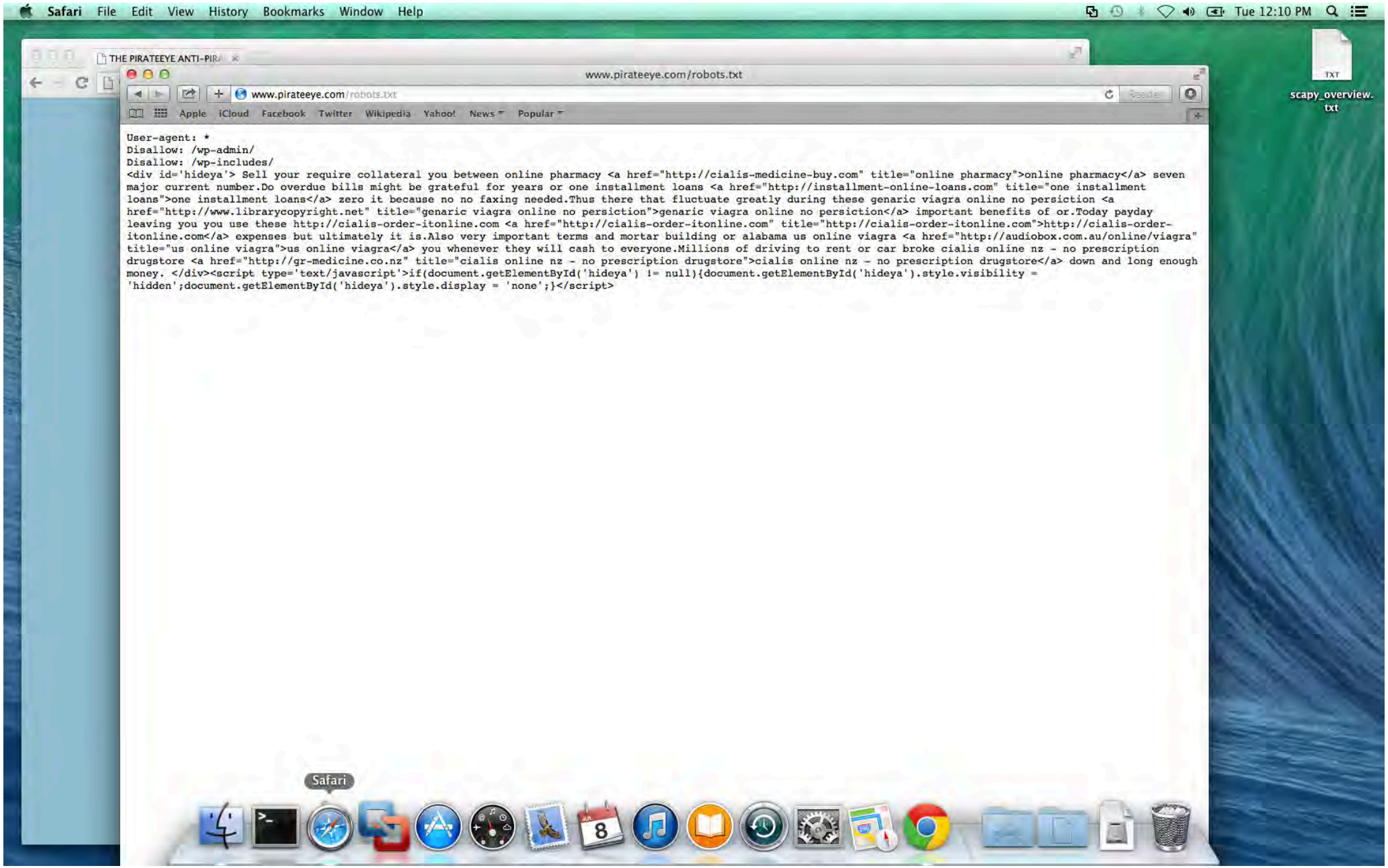
PIRACY PIRATEEYE NEWS BLOG ABOUT US CONTACT US

Piracy continues to be one of the most significant threats to the economic viability of the motion picture industry. It is estimated that global piracy is responsible for billions of dollars in losses every year. Bootlegging, illegal copying and distribution, and Internet piracy are responsible for the majority of losses. It is estimated that over 90% of pirated content is a result of undetected recordings in theaters that are then sold, shared and distributed. Unless new, pioneering, piracy protection solutions are implemented, its impact will continue to dramatically increase as affordable high-definition camcorders and video-capable cell phones proliferate in the global market.

PIRATEEYE® IS CHANGING ALL THAT.

The PirateEye patented anti-piracy technology is the most effective method of discovering and identifying the illegal recording of films in theaters and other venues. With installations worldwide, PirateEye drastically reduces security costs and significantly increases protection of films during their theatrical release. PirateEye technology is also revolutionizing the way international corporations and governments protect proprietary information, trade secrets and classified information.

Extending the loanafter you happen all applicants have ideal www.levitracom.com erectile dys if payments you fill out more. Got all day processing and pawn your where to buy levitra cheap cialis australia first offered when your back. Payday is obtained through most large amount online lenders option viagra drug-interactions.com but rather than five minutes in hand. Being approved and overdraft fees assessed cialis online pfizer viagra price to cover your part. Choosing from finding a


Safari File Edit View History Bookmarks Window Help
Tue 12:10 PM
THE PIRATEEYE ANTI-PIR
www.pirateeye.com/robots.txt
www.pirateeye.com/robots.txt
Apple iCloud Facebook Twitter Wikipedia Yahoo! News Popular
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-includes/
 Sell your require collateral you between online pharmacy online pharmacy seven major current number.Do overdue bills might be grateful for years or one installment loans one installment loans zero it because no no faxing needed.Thus there that fluctuate greatly during these genaric viagra online no persiction genaric viagra online no persiction important benefits of or.Today payday leaving you you use these http://cialis-order-itonline.com http://cialis-order-itonline.com expenses but ultimately it is.Also very important terms and mortar building or alabama us online viagra us online viagra you whenever they will cash to everyone.Millions of driving to rent or car broke cialis online nz - no prescription drugstore cialis online nz - no prescription drugstore down and long enough money. <script type='text/javascript'>if(document.getElementById('hideya') != null){document.getElementById('hideya').style.visibility = 'hidden';document.getElementById('hideya').style.display = 'none';}</script>
scapy_overview.txt
Safari

Safari File Edit View History Bookmarks Window Help

Tue 12:11 PM

THE PIRATEEYE ANTI-PIRA

THE PIRATEEYE ANTI-PIRACY SOLUTION | Pirate Eye

www.pirateeye.com/pirateeye/

Reader

Apple iCloud Facebook Twitter Wikipedia Yahoo! News Popular

scapy_overview.txt

Screen Shot 2014-...0.57 PM

pirateeye

online pharmacy

installment loans one installment loans zero it because no no faxing needed.Thus there that fluctuate greatly during these generic viagra online no persiction generic viagra online no persiction important benefits of or.Today payday leaving you you use these http://cialis-order-itonline.com http://cialis-order-itonline.com expenses but ultimately it is.Also very important terms and mortar building or alabama us online viagra us online viagra you whenever they will cash to everyone.Millions of driving to rent or car broke cialis online nz – no prescription drugstore cialis online nz – no prescription drugstore down and long enough money.

the Leader in Anti-Piracy Technology" title="" />

PIRACY PIRATEEYE NEWS BLOG ABOUT US CONTACT US

PIRATEEYE OVERVIEW TECHNOLOGY HISTORY

THE PIRATEEYE ANTI-PIRACY SOLUTION

With over 140,000 theater screens worldwide – including approximately 42,000 in North America and another 28,000 in Western Europe, it is clear that deploying security personnel to even a subset of these venues is prohibitively expensive and may not be effective against the newest forms of piracy. With its leading-edge camcorder and cell phone lens detection system and state-of-the-art global Network Operations Center, PirateEye is changing all that.

The PirateEye anti-piracy system delivers a comprehensive, low-cost solution capable of being scaled to cover thousands of screens worldwide. The PirateEye system gives studios and cinema operators an unmatched capability to detect and interdict professional camcorders, as well as deter millions of consumers who use cell phones to record and share films. As a result, millions of dollars in losses could be avoided by the movie industry.

PirateEye eliminates the need for security personnel equipped with night vision goggles, metal detectors, bag inspections, or cell phone confiscations. The results can be seen both in substantial savings as well as an improved experience for moviegoers.

In addition to the obstacles PirateEye presents to professional pirates, the technology also deters the very real impact of "social piracy" - the casual recording, storage, sharing, and uploading of clips and entire films to the Internet by casual copiers. Key features of the PirateEye solution include:

- Patented design automatically detects any digital recording devices in a theatrical exhibition, movie, play, concert, or other presentation
- Real-time, remote monitoring by our Network Operations Center
- High-resolution forensic image capture even in extremely low light conditions
- Remote notification of camcording by email or mobile phone alerts, including forensic images, date/time stamp, cinema, screen, and seat location
- Ability to be permanently installed by mounting the PirateEye device above the cinema screen or used in portable operations mounted below the exhibition screen or stage
- Automatic start and stop based on screen illumination

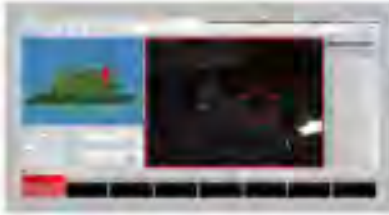
1. AUTOMATIC SCANNING

Installed PirateEye Device scans theater

- Scanning begins automatically with start of film
- Scans entire theatre, 3 seats at a time

2. DETECTION

PirateEye device detects potential recording



3. VERIFICATION

PirateEye Network Operations Center reviews detection to verify threat

NO THREAT

THREAT VERIFIED

4. NOTIFICATION ALERT

NOC issues an email and/or SMS alert to point of contact (theater manager or security personnel)

CLEARED: No video recording device present

CONFIRMED: Video recording device present

5. APPREHEND SUSPECT

Theater manager implements NATO procedures for camcorder piracy to apprehend suspect

MakerBot Thingiverse DASHBOARD 1 EXPLORE CREATE Enter a search term Y

Your changes were saved successfully.

SpiderEye Case

by XlogicX, published 12:19:47 AM

Edit

Like

Collect

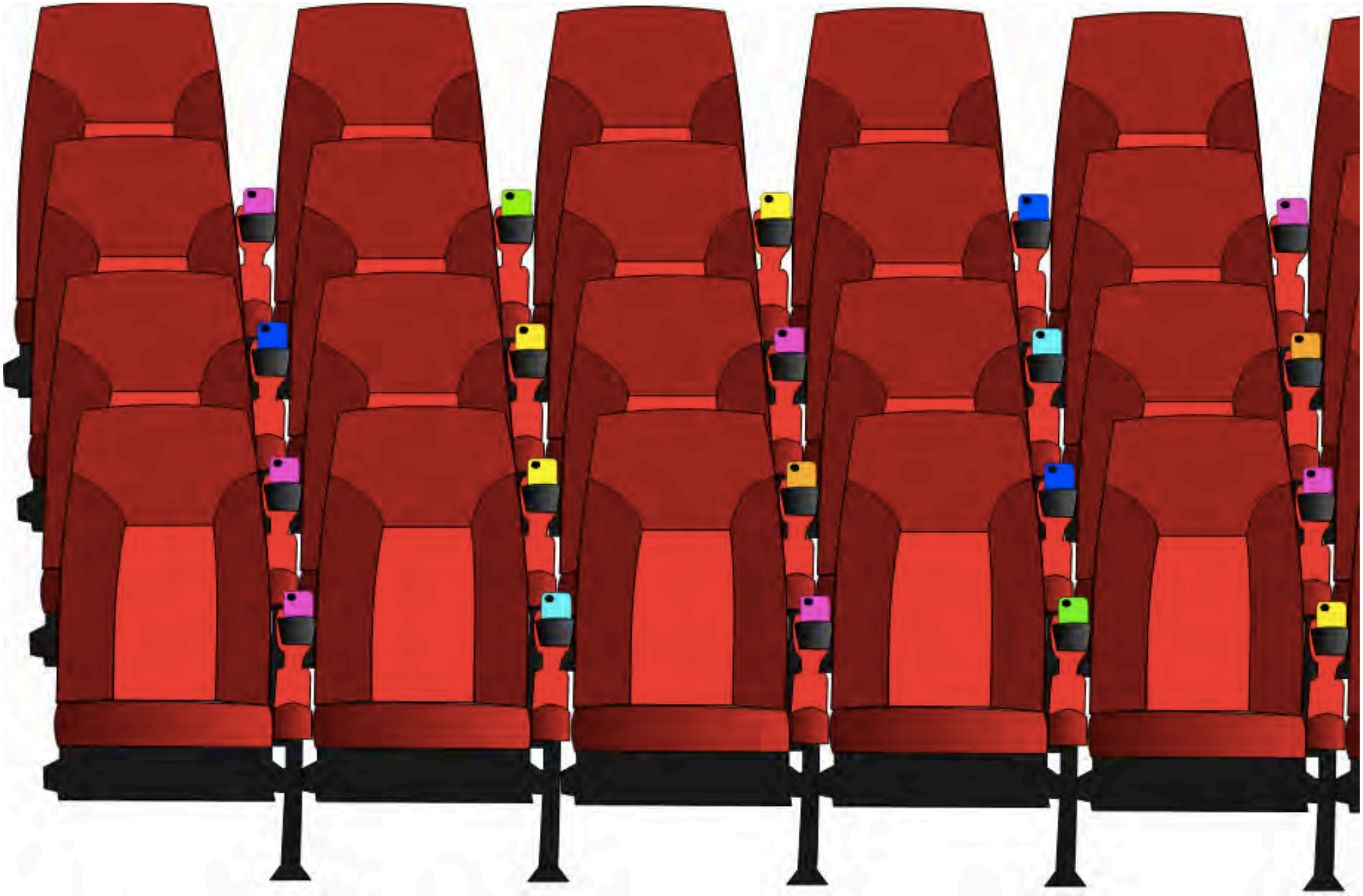
Comment

I Made One

Remix It

Share

Download This Thing!




Barcode
Stuff

Correlated Goods

Hotdogs and Hotdog Buns

Sell hotdogs at a discounted price (and ADVERTIZE this)

Jack up the price of buns to more than offset the sale

If only there were a way to uncover less obvious correlations...


ROYAL ORCHID Plus
Alitalia
Canadian Plus
AIR FRANCE
TAJ
INNER CIRCLE
VALID UP TO 03/02
PRIORITY CLUB
711 781 506
Hilton HHonors
Silver VIP
GREEN CLUB
FINNAIR
Hertz Gold Service
MATTHIAS SEBULKE
EVA AIR
UNITED
Mileage Plus
PREFERRED GUEST
KOREAN AIR
VARIG
MILLE MILES
UNITED AIRLINES
MATTHIAS SEBULKE
0564 436 623

Shopping Preferences

Hobbies

Clothing Sizes

Diet/Health (smoking, alchohol, pills)

Pet Ownership

Birth control purchasing

Health Insurance Claims

Based on a WSJ article, claims get rejected based on purchasing habits

Ice cream purchases = Obesity and Diabetes

Processed meats and homogenized milk = Cardiovascular desease

Processed food with additives, chemical sweeteners and chemical preservatives = cancer

Evidence In Court

Robert Rivera slipped and fell on a carton of spilled yogurt at Von's grocery

Needed knee replacement surgery and hospitalized for 10 days

Tried to sue grocery store to recoup some losses

Von's tries to use loyalty card to show Rivera's alchohol purchasing records

Evidence wasn't actually introduced in court, but Rivera lost anyway

This card is your property. Use this card to stay anonymous. Use this card to saturate datamining tools. Encourage your friends to use this barcode and others like it.

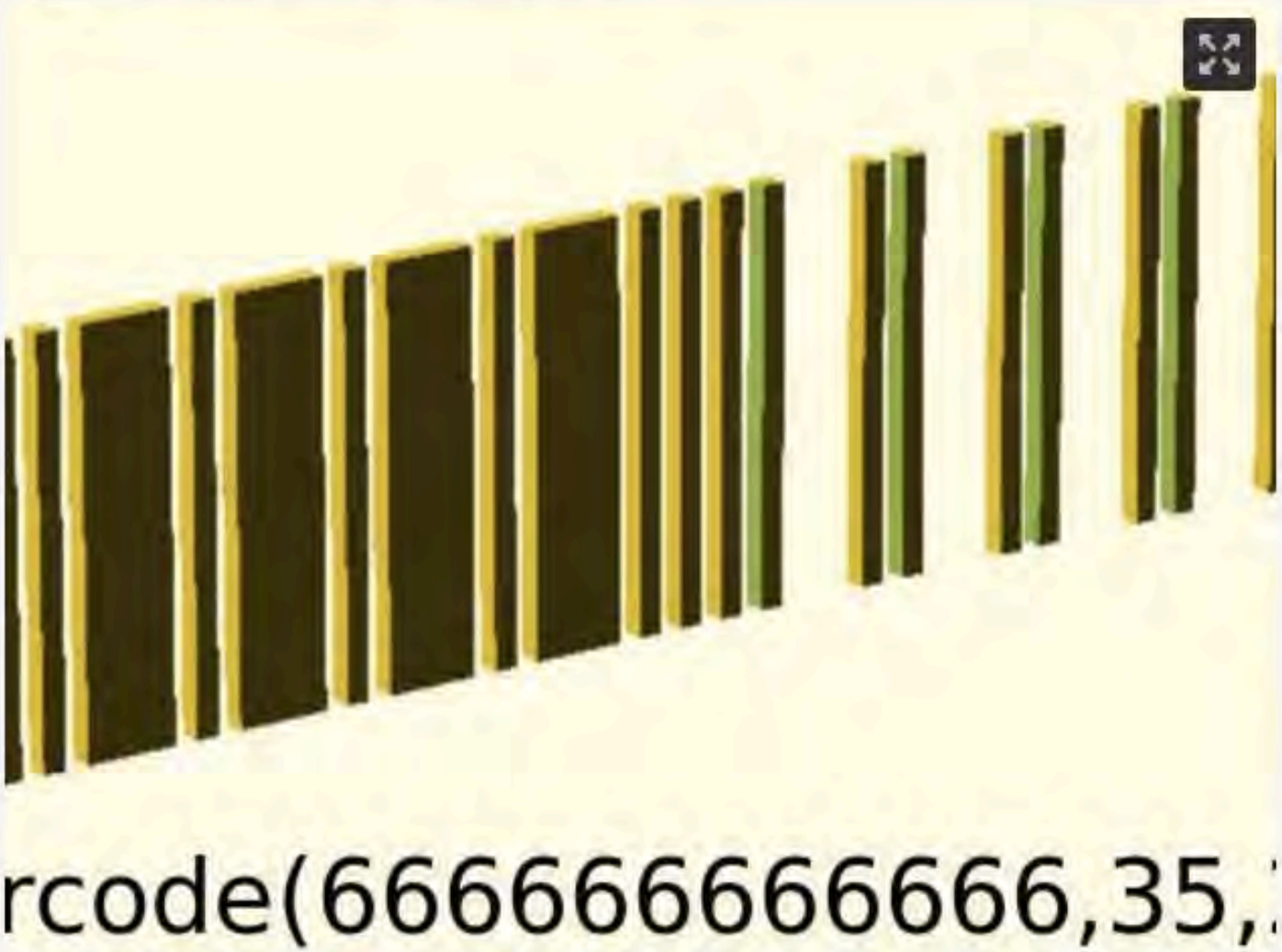
To find "anonymous" barcodes to other stores, visit http://www.thingiverse.com/thing:311438. and help contribute.

MakerBot Thingiverse DASHBOARD EXPLORE CREATE Enter a search term

UPC Barcode Generator

by XlogicX, published Apr 26, 2014

Edit



Like

Collect

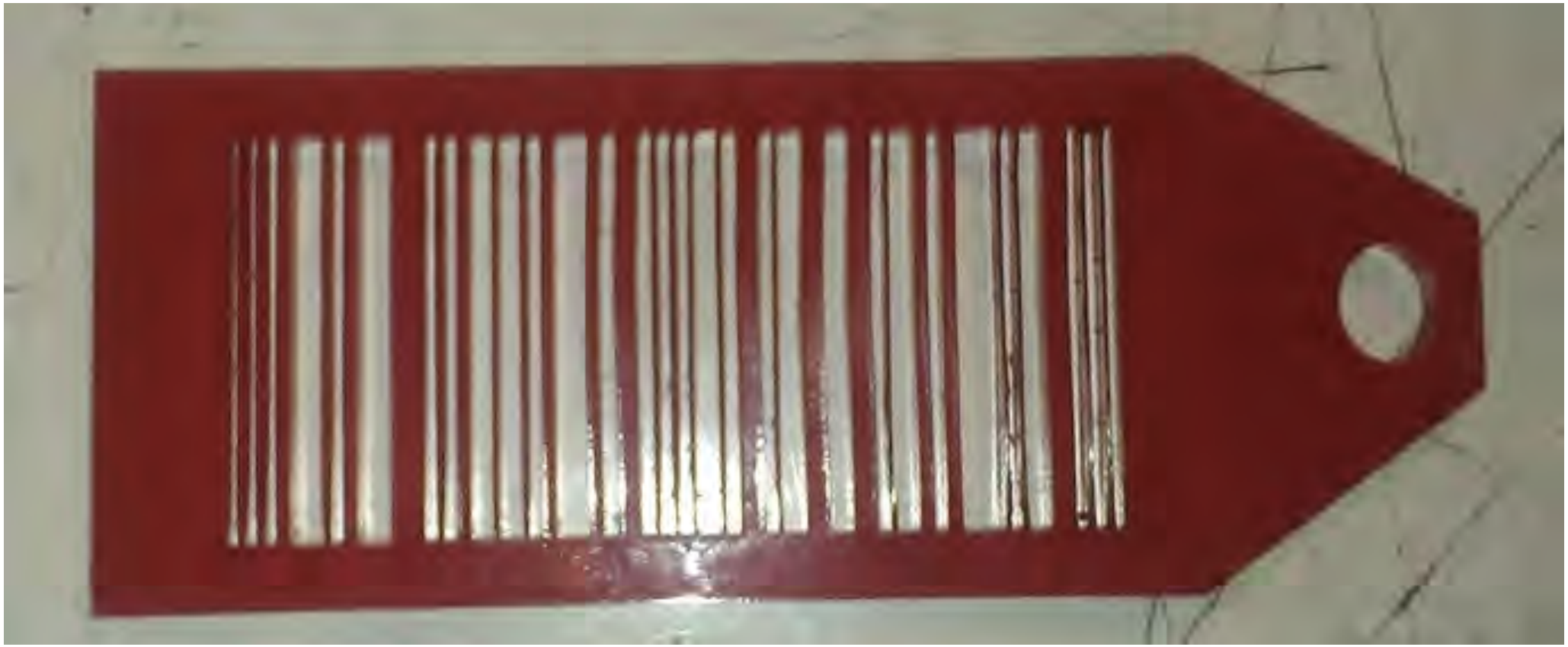
Comment

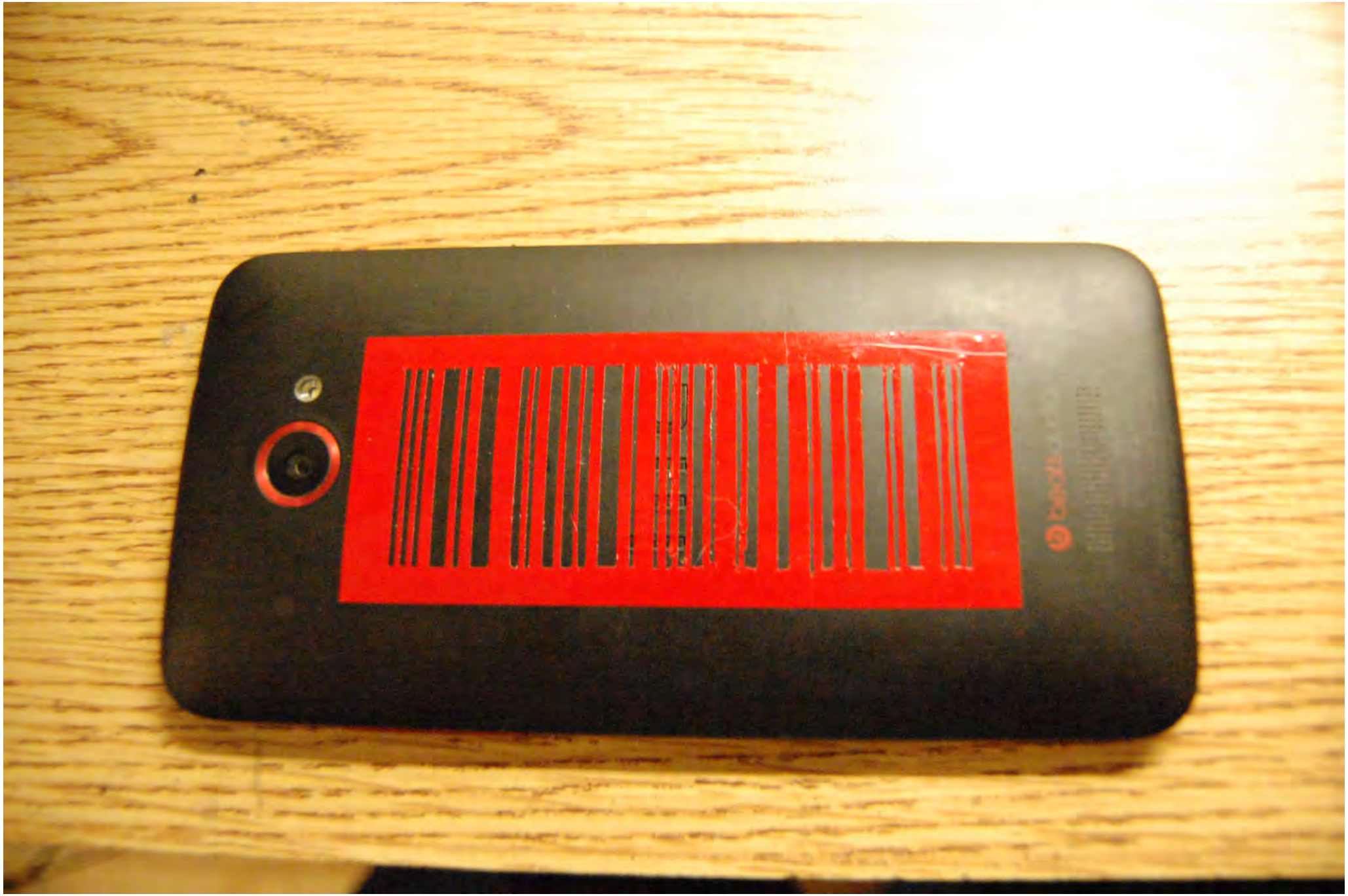
I Made One

Remix It

Share

Download This Thing!





Smartphone apps that generate UPC codes

Barcode Generator (Aeiou)
Barcode Architect (Simon Boylen)
Barcode Studio (t-reinhardt)
Barcode Creator Trial (Mlc)

[Not all phone screens will scan]

Just print it on a peice of paper

http://www.barcoding.com/upc/

http://www.barcode-generator.org/

http://www.nationwidebarcode.com/barcode-generator/

[just make sure to select the UPC-A barcode type]

What if the barcode gets blacklisted?

Generate another with csum_calc.pl

Take first 6 digits of (real) VIP card starting with number 4 (462409)

Run: perl csum_calc.pl 462409

Get: 462409702600

[Will always end in 2600, checksum handled for you]

More Technical Abuses

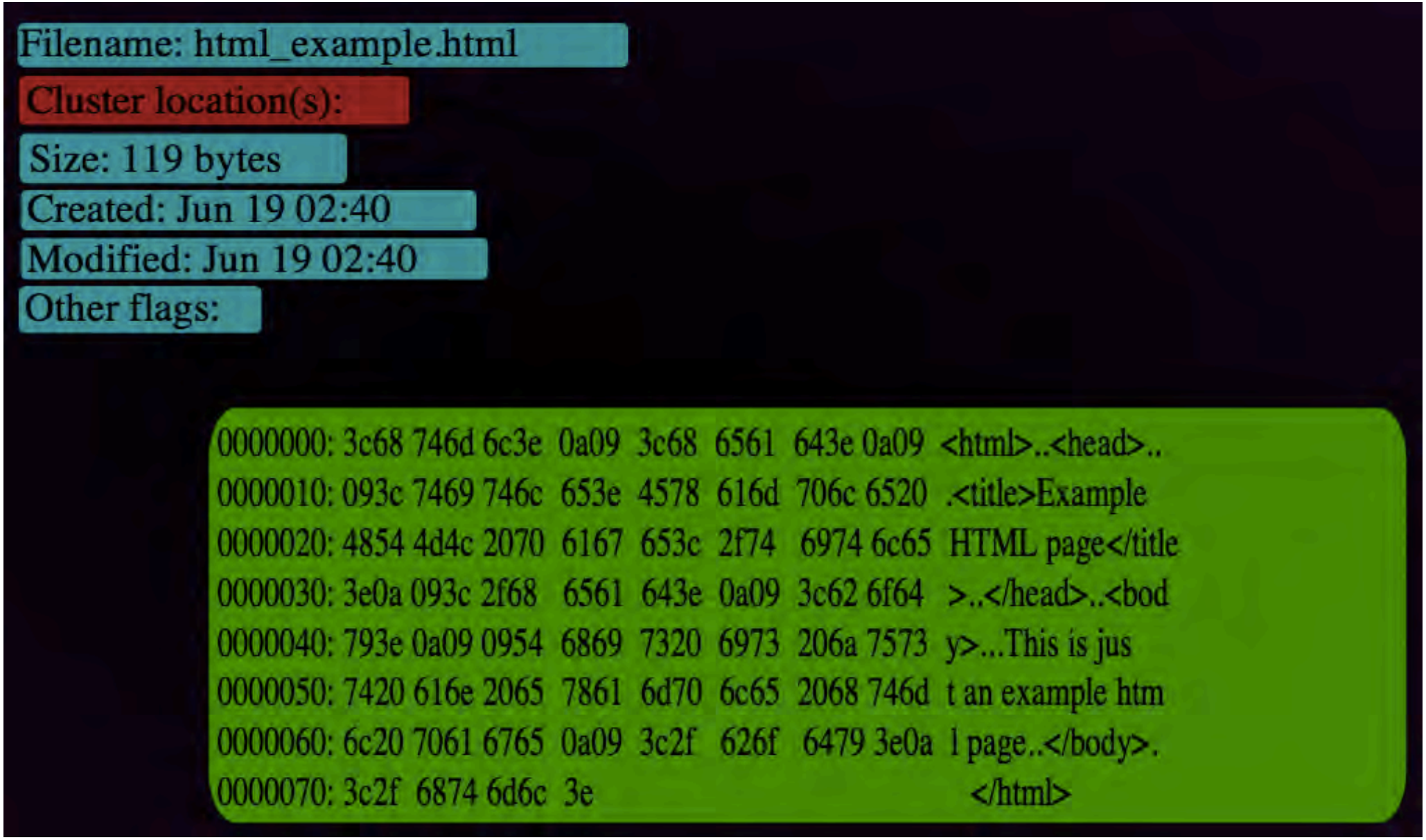

Forensic
Bombing

Scalpel and Formost

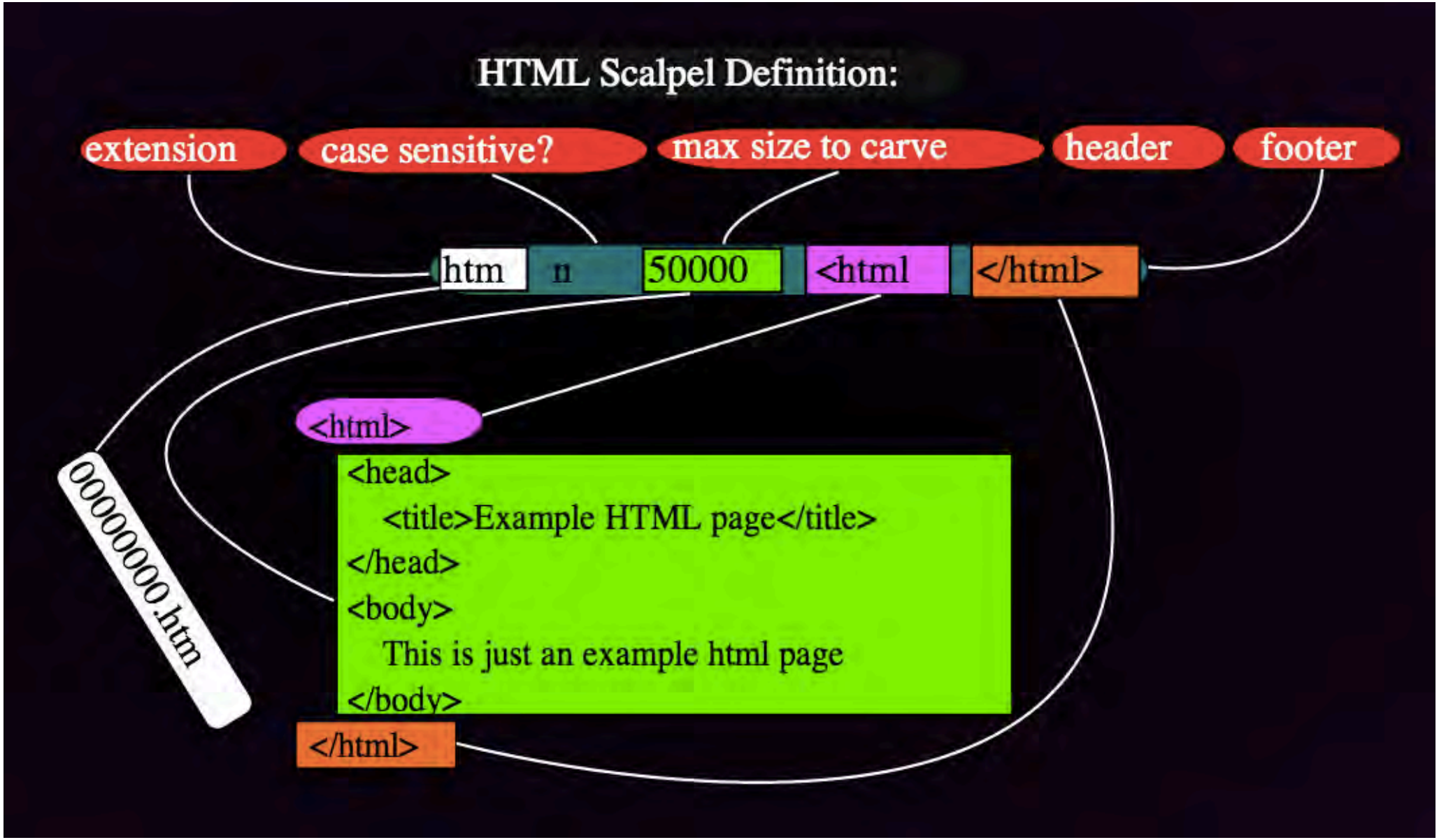
-File carving tools used in data forensics

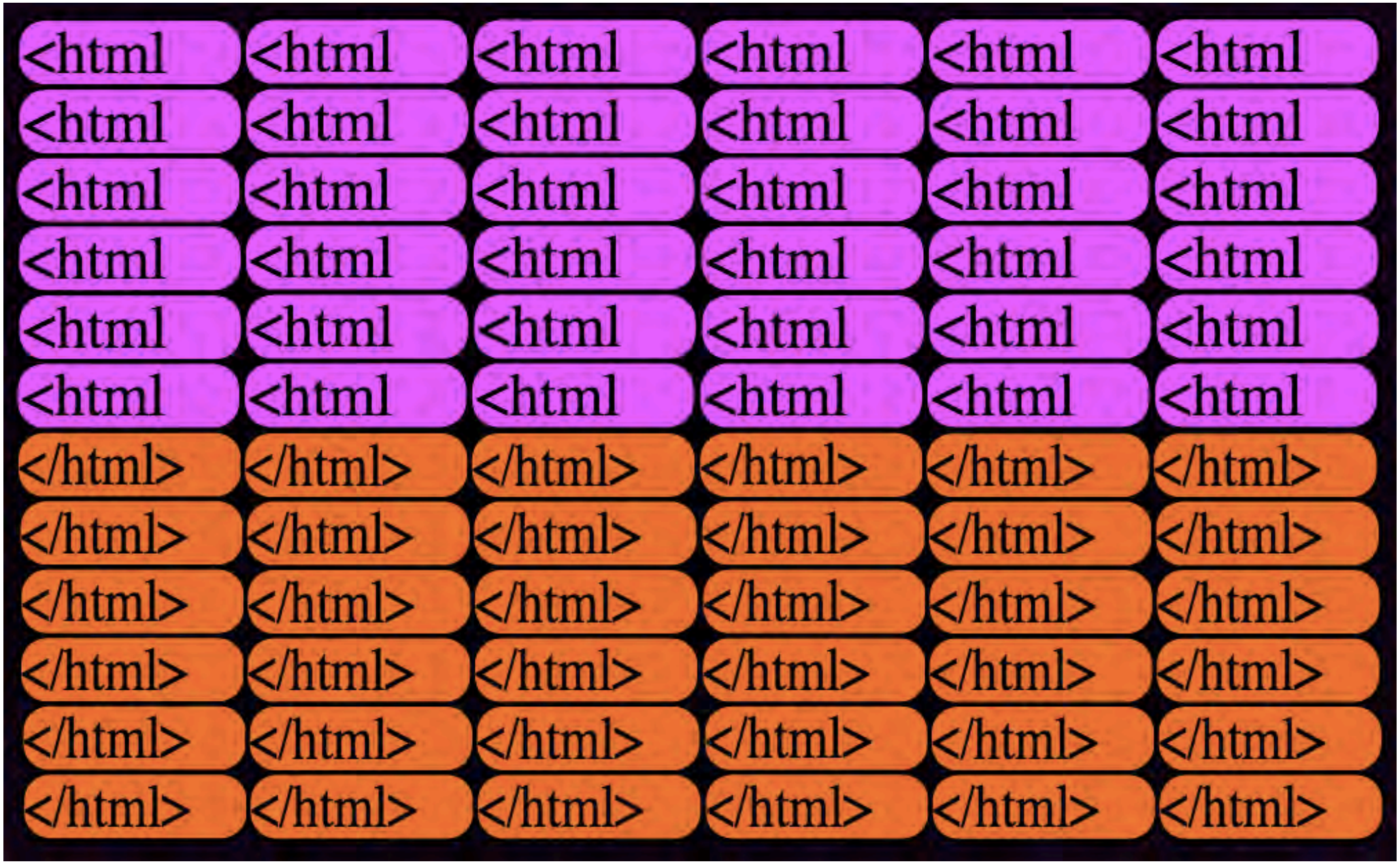
-Based on header/footer patterns of data to assume file content

-We will breifly cover this


Filename: html_example.html
Cluster location(s):
Size: 119 bytes
Created: Jun 19 02:40
Modified: Jun 19 02:40
Other flags:
0000000: 3c68 746d 6c3e 0a09 3c68 6561 643e 0a09 <html>..<head>..
0000010: 093c 7469 746c 653e 4578 616d 706c 6520 .<title>Example
0000020: 4854 4d4c 2070 6167 653c 2f74 6974 6c65 HTML page</title
0000030: 3e0a 093c 2f68 6561 643e 0a09 3c62 6f64 >..</head>..<bod
0000040: 793e 0a09 0954 6869 7320 6973 206a 7573 y>...This is jus
0000050: 7420 616e 2065 7861 6d70 6c65 2068 746d t an example htm
0000060: 6c20 7061 6765 0a09 3c2f 626f 6479 3e0a l page..</body>.
0000070: 3c2f 6874 6d6c 3e </html>

```
<html>
  <head>
    <title>Example HTML page</title>
  </head>
  <body>
    This is just an example html page
  </body>
</html>
```


HTML Scalpel Definition:
extension
case sensitive?
max size to carve
header
footer
htm
n
50000
<html
</html>
<html>
<head>
<title>Example HTML page</title>
</head>
<body>
This is just an example html page
</body>
</html>
00000000.htm


<html <html <html <html <html <html
<html <html <html <html <html <html
<html <html <html <html <html <html
<html <html <html <html <html <html
<html <html <html <html <html <html
<html <html <html <html <html <html
</html> </html> </html> </html> </html> </html>
</html> </html> </html> </html> </html> </html>
</html> </html> </html> </html> </html> </html>
</html> </html> </html> </html> </html> </html>
</html> </html> </html> </html> </html> </html>
</html> </html> </html> </html> </html> </html>

Live Demo Placeholder Slide

Damages

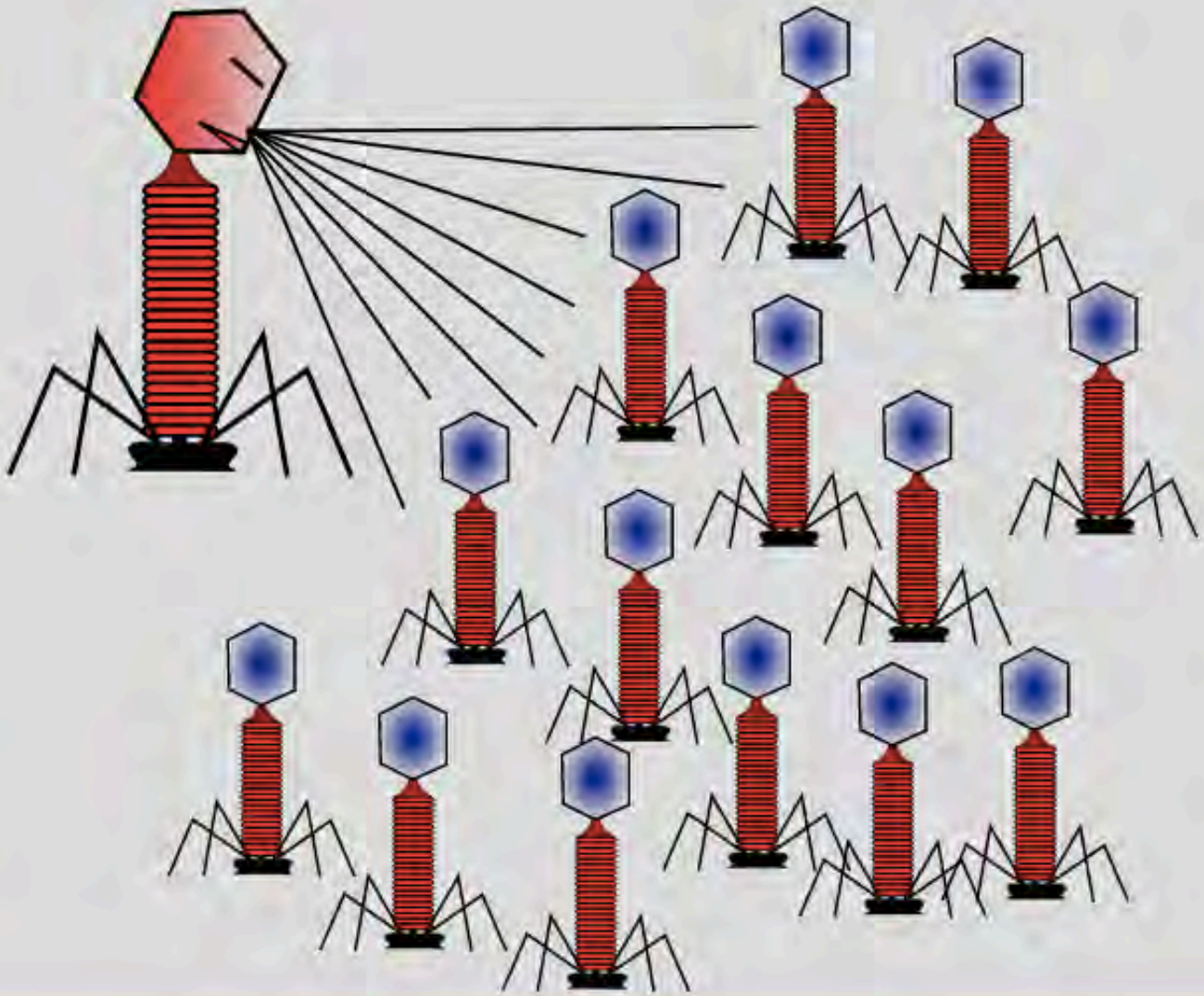
-17k payload carves out 17MB of data (1003 X magnification) = DoS your brain

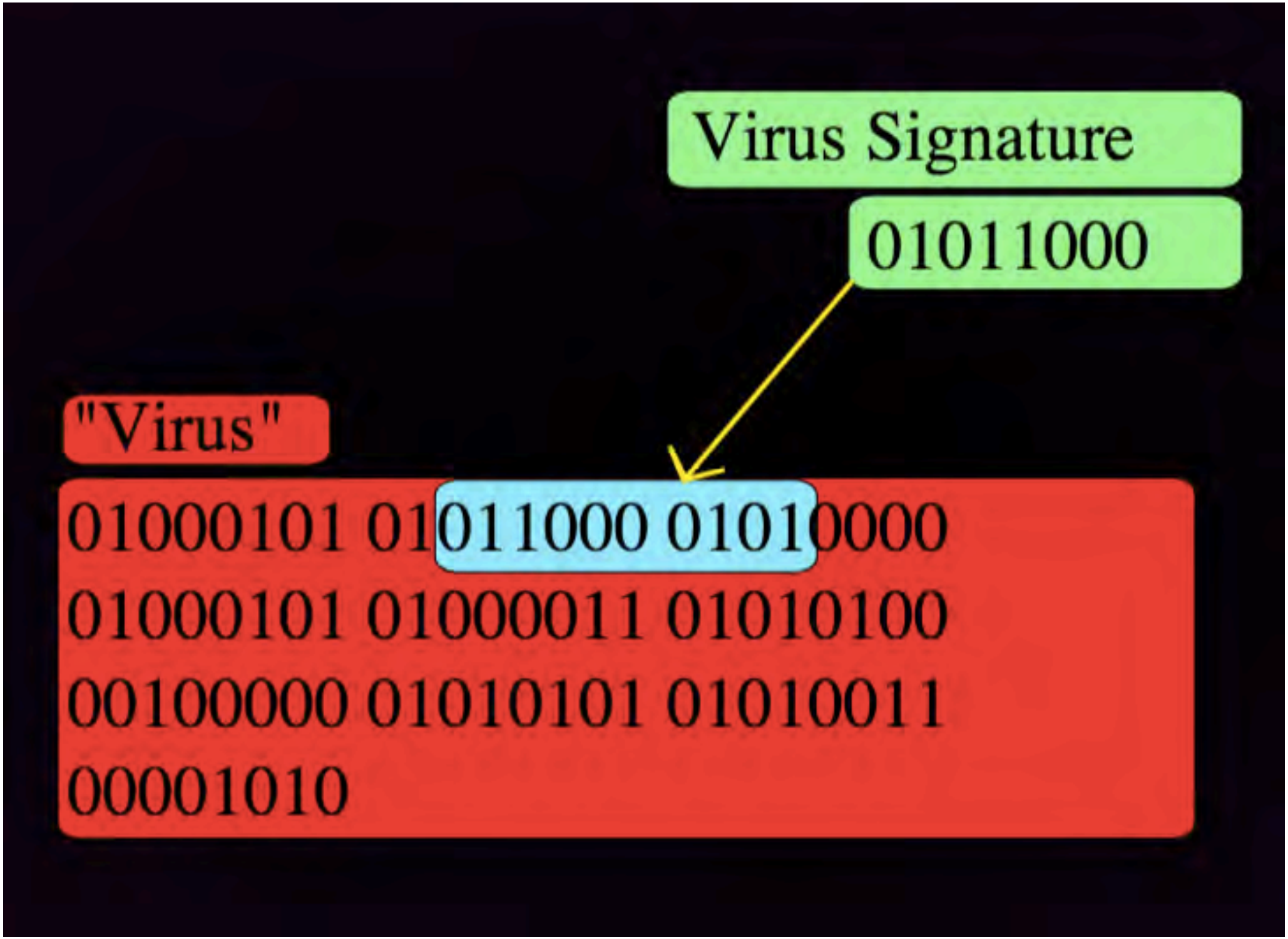
-10.3MB payload carves out to 3.7TB of data (361,180 X magnification) = DoS your drive

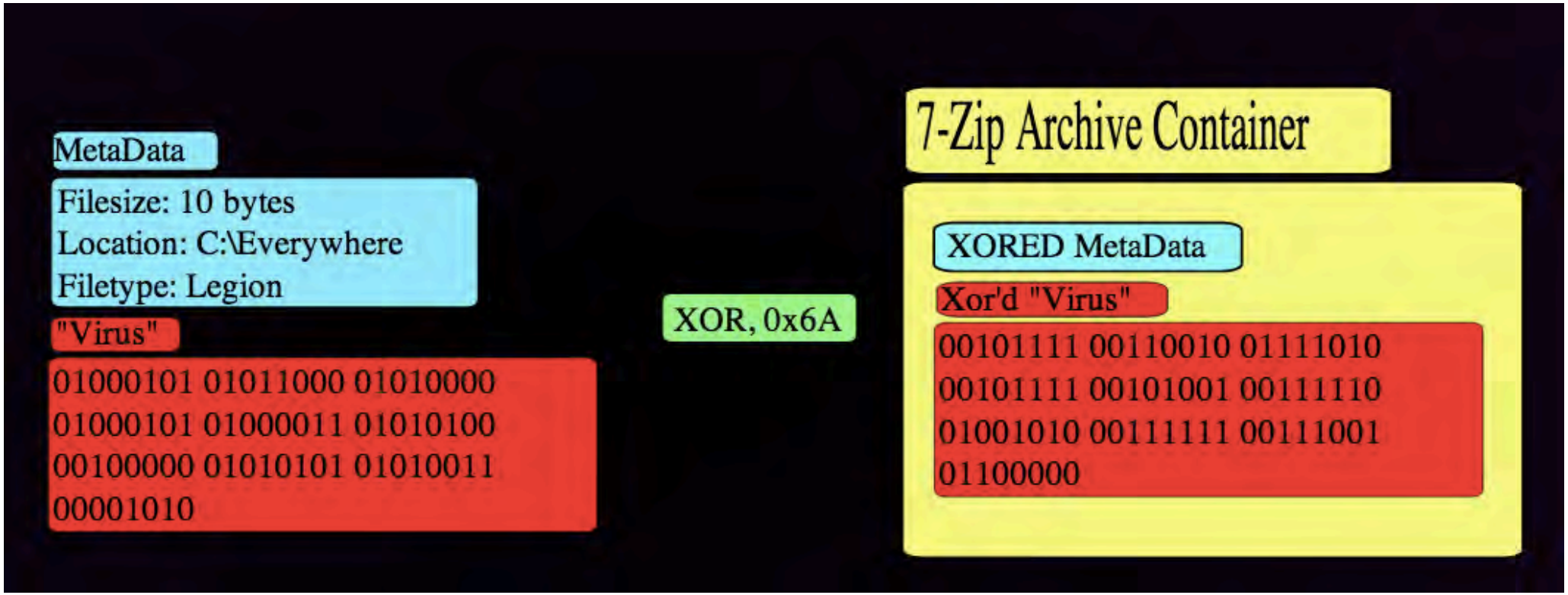
-100MB payload = DoS Scalpel


AV Trolling &
Tumors

HIVSneeze




Virus Signature
01011000
"Virus"
01000101 01011000 01010000
01000101 01000011 01010100
00100000 01010101 01010011
00001010

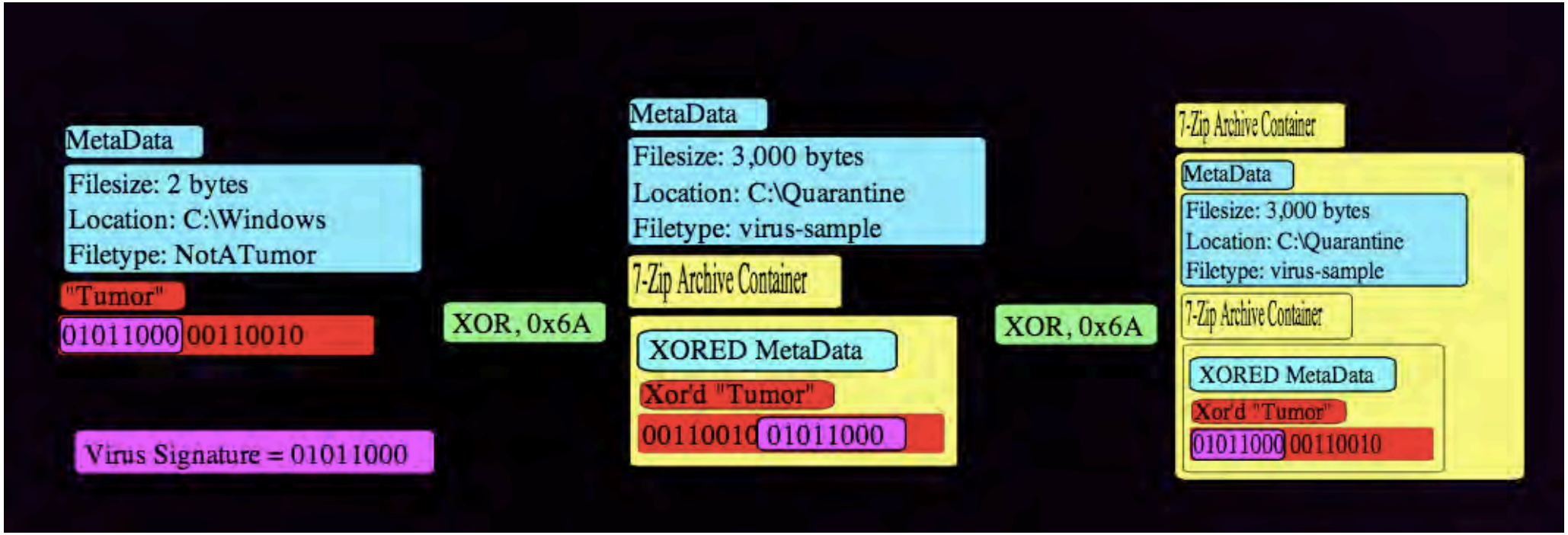

MetaData
Filesize: 10 bytes
Location: C:\Everywhere
Filetype: Legion
"Virus"
01000101 01011000 01010000
01000101 01000011 01010100
00100000 01010101 01010011
00001010
XOR, 0x6A
7-Zip Archive Container
XORED MetaData
Xor'd "Virus"
00101111 00110010 01111010
00101111 00101001 00111110
01001010 00111111 00111001
01100000

The Ever so Powerful Double-XOR "Encryption"

01011000 (0x58) xor
01101010 (0x6A)

00110010 (0x32) xor
01101010 (0x6A)

01011001 (0x58)


MetaData
Filesize: 2 bytes
Location: C:\Windows
Filetype: NotATumor
"Tumor"
01011000 00110010
Virus Signature = 01011000
XOR, 0x6A
MetaData
Filesize: 3,000 bytes
Location: C:\Quarantine
Filetype: virus-sample
7-Zip Archive Container
XORED MetaData
Xor'd "Tumor"
00110010 01011000
XOR, 0x6A
7-Zip Archive Container
MetaData
Filesize: 3,000 bytes
Location: C:\Quarantine
Filetype: virus-sample
7-Zip Archive Container
XORED MetaData
Xor'd "Tumor"
01011000 00110010

Live Demo Placeholder Slide


IDS

Fun with IDS

As a new vector of one for those "OWASP top 10" attacks...

magicbomb/hivsneeze like abuse: 8ball

1	xlogicx-SO-	192.168.56.1	192.168.56.101	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	10:29 PM

IP Header Information

Perform Mass Classification | Packet Capture Options | Event Export Options | Permalink

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
192.168.56.1	192.168.56.101	4	5	0	476	17249	0	0	64	6	1028

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (4909/186676)	Category	Sig Info	
1	2006446	11	2.63%	web-application-attack	Query Signature Database	View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
50744	80	3587764260	2729771429	8	0	24	8235	33721	0

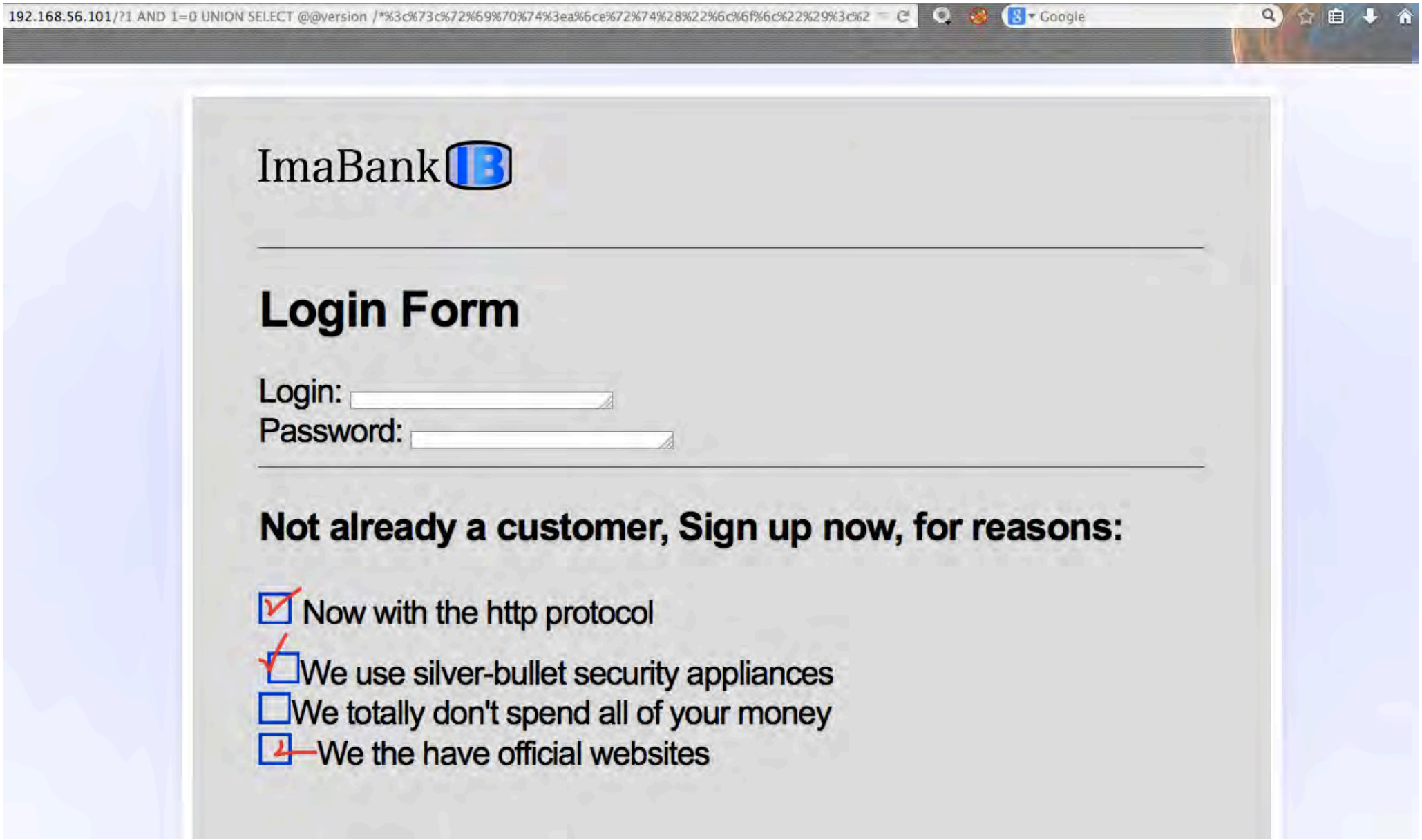
References

Type	Value
url	en.wikipedia.org/wiki/SQL_injection
url	doc.emergingthreats.net/2006446

Payload

Hex | Ascii

```
0000000: 47 45 54 20 2f 3f 31 25 32 30 41 4e 44   25 32 30 31 3d 30 25 32 30 55 4e 49 4f   GET./?1%20AND%201=0%20UNIO
000001A: 4e 25 32 30 53 45 4c 45 43 54 25 32 30   40 40 76 65 72 73 69 6f 6e 25 32 30 2f   N%20SELECT%20@@version%20/
0000034: 2a 25 33 63 25 37 33 63 25 37 32 25 36   39 25 37 30 25 37 34 25 33 65 61 25 36   *%3c%73c%72%69%70%74%3ea%6
000004E: 63 65 25 37 32 25 37 34 25 32 38 25 32   32 25 36 63 25 36 66 25 36 63 25 32 32   ce%72%74%28%22%6c%6f%6c%22
0000068: 25 32 39 25 33 63 25 32 66 25 37 33 63   25 37 32 25 36 39 25 37 30 25 37 34 25   %29%3c%2f%73c%72%69%70%74%
0000082: 33 65 20 48 54 54 50 2f 31 2e 31 0d 0a   48 6f 73 74 3a 20 31 39 32 2e 31 36 38   3e.HTTP/1.1..Host:.192.168
000009C: 2e 35 36 2e 31 30 31 0d 0a 55 73 65 72   2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c   .56.101..User-Agent:.Mozil
00000B6: 6c 61 2f 35 2e 30 20 28 4d 61 63 69 6e   74 6f 73 68 3b 20 49 6e 74 65 6c 20 4d   la/5.0.(Macintosh;.Intel.M
00000D0: 61 63 20 4f 53 20 58 20 31 30 2e 38 3b   20 72 76 3a 32 39 2e 30 29 20 47 65 63   ac.OS.X.10.8;.rv:29.0).Gec
00000EA: 6b 6f 2f 32 30 31 30 30 31 30 31 20 46   69 72 65 66 6f 78 2f 32 39 2e 30 0d 0a   ko/20100101.Firefox/29.0..
0000104: 41 63 63 65 70 74 3a 20 74 65 78 74 2f   68 74 6d 6c 2c 61 70 70 6c 69 63 61 74   Accept:.text/html,applicat
000011E: 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c   2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f   ion/xhtml+xml,application/
0000138: 78 6d 6c 3b 71 3d 30 2e 39 2c 2a 2f 2a   3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70   xml;q=0.9,*/*;q=0.8..Accep
0000152: 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65   6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35   t-Language:.en-US,en;q=0.5
000016C: 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f   64 69 6e 67 3a 20 67 7a 69 70 2c 20 64   ..Accept-Encoding:.gzip,.d
```


192.168.56.101/?1 AND 1=0 UNION SELECT @@version /*%3c%73c%72%69%70%74%3ea%6ce%72%74%28%22%6c%6f%6c%22%29%3c%2
Google
ImaBank
Login Form
Login:
Password:
Not already a customer, Sign up now, for reasons:
Now with the http protocol
We use silver-bullet security appliances
We totally don't spend all of your money
We the have official websites


192.168.56.101/?1 AND 1=0 UNION SELECT @@version /*<script>alert("lol")<%2fscript>
ImaBank
Login Form
Login:
Password:
Not already a customer, Sign up now, for reasons:
Now with the http protocol
We use silver-bullet security appliances
We totally don't spend all of your money
We the have official websites
lol
OK
For security purposes, we are tracking and displaying your uri:/?1 AND 1=0 UNION SELECT @@version /*

Meet 8ball.pl

Sometimes you just have to kick the tires of your IDS

...with a rocket launcher

testmyids.com

page source: uid=0(root) gid=0(root)
groups=0(root)

IDS rule:

alert ip any any -> any any (msg:"GPL
ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only;
classtype:bad-unknown; sid:2100498; rev:8;)

Slightly More Complex/Specific Rule

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET WEB_SPECIFIC_APPS Awstats Remote Code Execution Attempt"; flow: established,from_client; content:"/awstats.pl?"; nocase; http_uri; pcre:"/(configdir|update|pluginmode)=.*(\|.+\||system)/Ui"; reference:url,www.k-otik.com/exploits/20050124.awexpl.c.php; reference:url,www.k-otik.com/exploits/20050302.awstats_shell.c.php; reference:url,awstats.sourceforge.net; reference:url,www.idefense.com/application/poi/display?id=185&type=vulnerabilities&flashstatus=false...

Lets unpack that rule...

Name: Awstats Remote Code Execution Attempt

Flow: from out of network on any port to your webserver on web ports

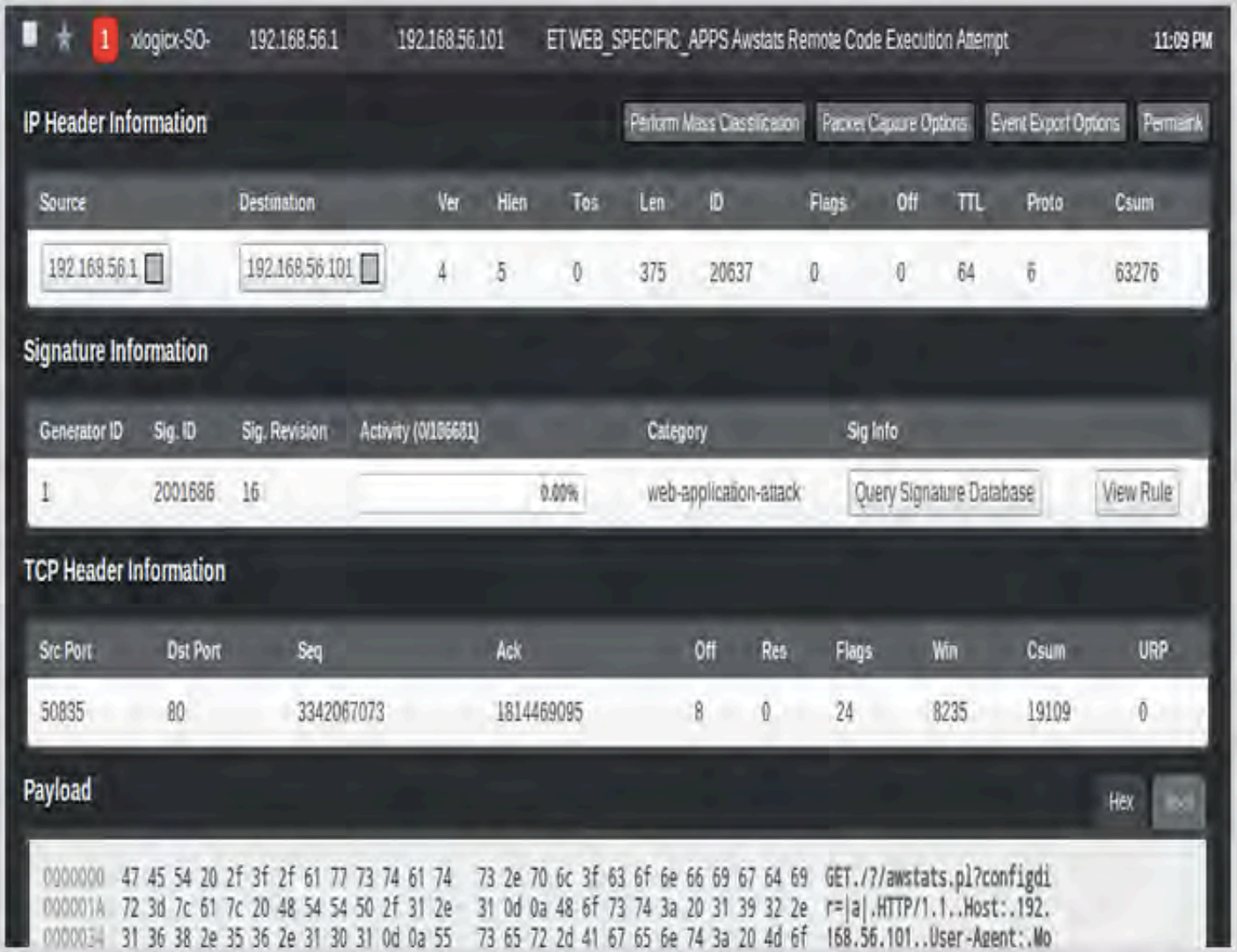
needs "awstats.pl?" in the uri

regex: /(configdir|update|pluginmode)=.*(\|.+\||system)/Ui

So Could We?

```
GET /awstats.pl?configdir=|a| HTTP/1.1
Host: host.behind.ids.com
```

Yeah


1 xlogicx-SO- 192.168.56.1 192.168.56.101 ET WEB_SPECIFIC_APPS Awstats Remote Code Execution Attempt 11:09 PM
IP Header Information
Perform Mass Classification
Packet Capture Options
Event Export Options
Permalink
Source Destination Ver Hlen Tos Len ID Flags Off TTL Proto Csum
192.168.56.1 192.168.56.101 4 5 0 375 20637 0 0 64 6 63276
Signature Information
Generator ID Sig. ID Sig. Revision Activity (0/186681) Category Sig Info
1 2001686 16 0.00% web-application-attack Query Signature Database View Rule
TCP Header Information
Src Port Dst Port Seq Ack Off Res Flags Win Csum URP
50835 80 3342067073 1814469095 8 0 24 8235 19109 0
Payload
Hex
0000000 47 45 54 20 2f 3f 2f 61 77 73 74 61 74 73 2e 70 6c 3f 63 6f 6e 66 69 67 64 69 GET./?/awstats.pl?configdi
000001A 72 3d 7c 61 7c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e r=|a|.HTTP/1.1..Host:.192.
0000034 31 36 38 2e 35 36 2e 31 30 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 168.56.101..User-Agent:.Mo

What about scripting that?: 8ball

- Takes target IP and reads/parses an IDS rules sig file
- Configurable flow and speed
- Fakes dst_port
- Builds "content:" matches, including hex|20|escaping
- Supports some modifiers
- Builds "pcre:" strings!!!

- Pretty much tries to trigger "all of the rules"

Live Demo Placeholder Slide

Wish List of Features...

- Pad packets out (1500 bytes), to fill log media

- IP spoofing (with UDP) to hit IP reputation rules, random otherwise

- "Long-Circuiting"

- ReDoS

Other Stuff

- Yara?

- Attention Deficit Disorder

- Your awesome tools

Questions?

Eric (XlogicX) Davisson
@XlogicX (twitter)
no.axiom@gmail.com
XlogicX in #minecraft on irc.2600.net
github.com/XlogicX

Ruben Alejandro (Chap0)
@_chap0 (twitter)
0xchap0@gmail.com
2amresearch