black hat USA 2014

Fingerprinting web application platforms by variations in PNG implementations

Dominique Bongard
@reversity

Who am I ?

- From Switzerland
- Founder of 0xcite LLC
- Reverse engineer
- Focusing on embedded devices
- Mobile application developer

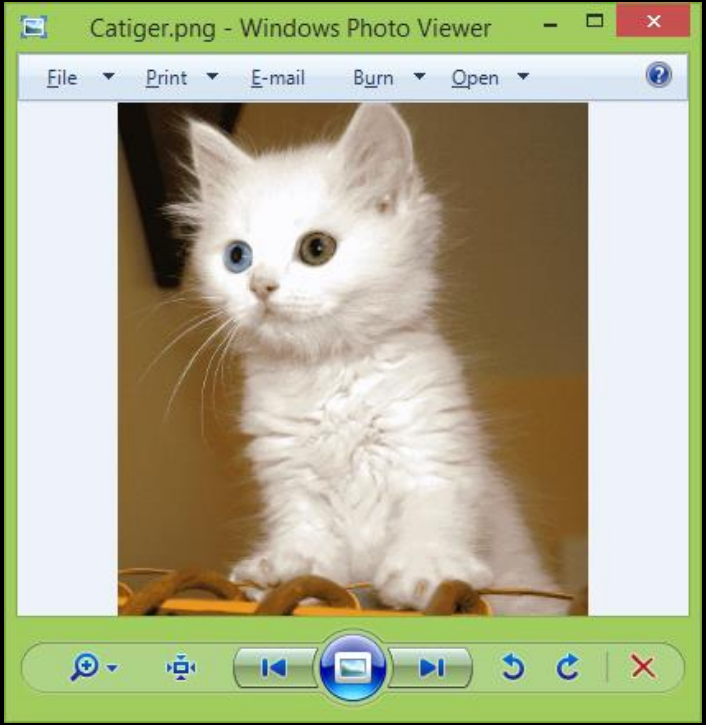
Agenda

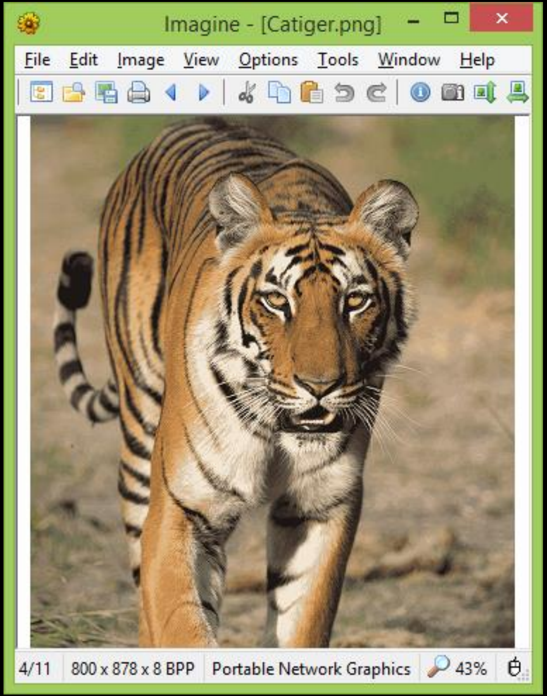
- Schizophrenic files
- Motivation for fingerprinting image libraries
- PNG file format 101
- MNG and JNG files
- Various PNG libraries put under stress
- Fingerprinting web applications with PNG
- Practical results on major websites
- Introducing the fingerping tool

Schizophrenic files

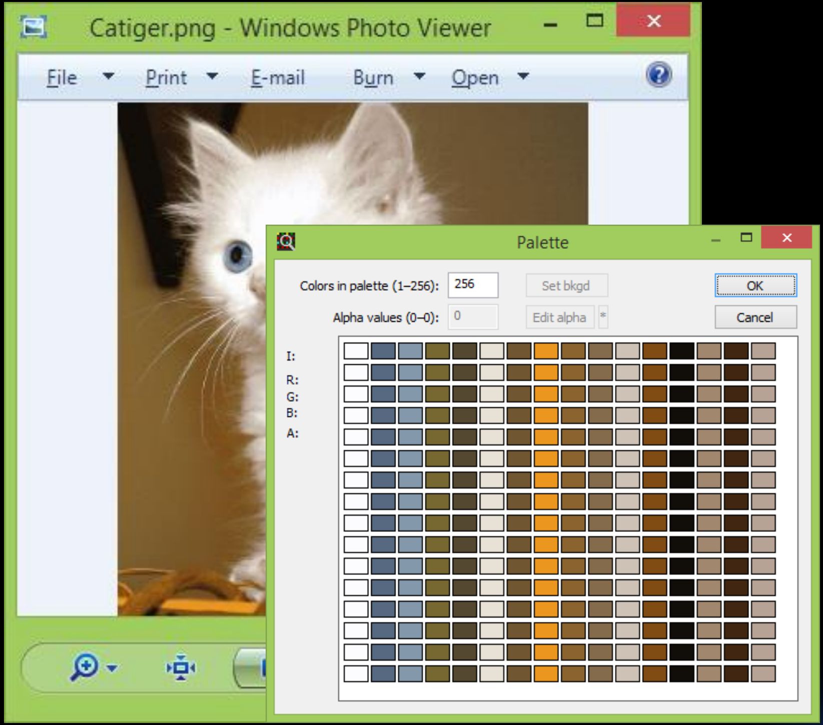
- Files that render differently depending on the viewer that is used
- Takes advantage of bugs or ambiguities in the file format spec.
- Popularized by Ange Albertini in the PoC||GTFO security e-zine

Schizophrenic PNG



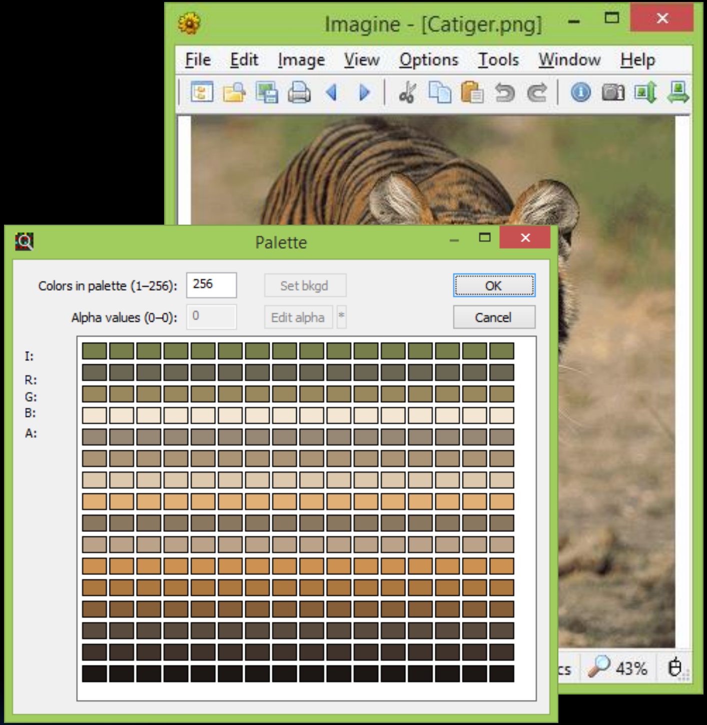


Schizophrenic PNG



Colors in palette (1–256): 256

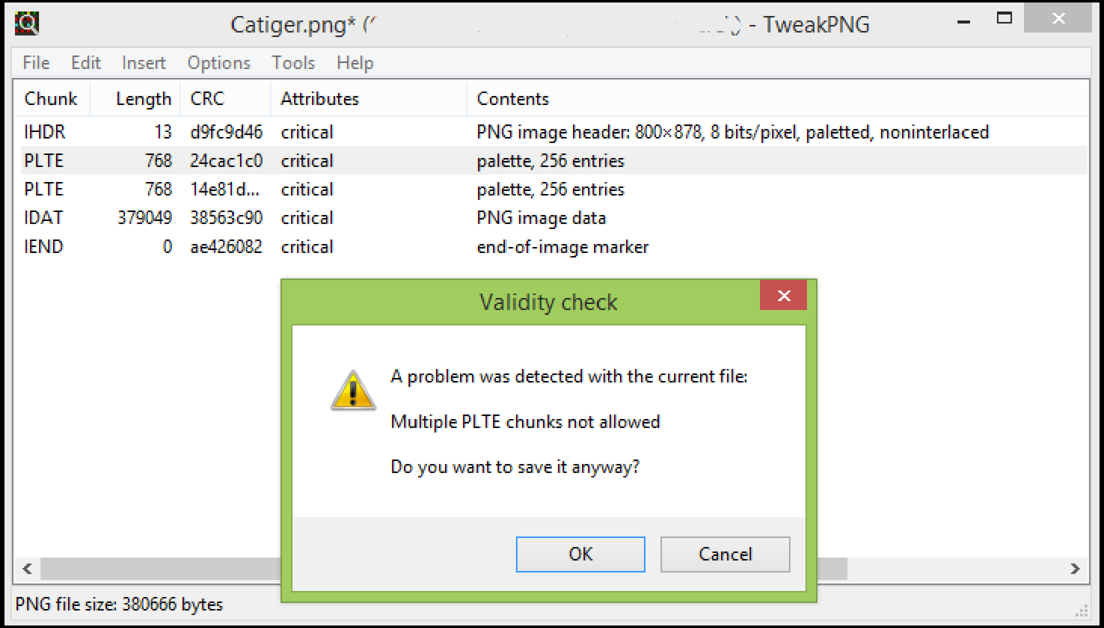
Alpha values (0–0): 0



Colors in palette (1–256): 256

Alpha values (0–0): 0

Schizophrenic PNG



Chunk	Length	CRC	Attributes	Contents
IHDR	13	d9fc9d46	critical	PNG image header: 800×878, 8 bits/pixel, paletted, noninterlaced
PLTE	768	24cac1c0	critical	palette, 256 entries
PLTE	768	14e81d...	critical	palette, 256 entries
IDAT	379049	38563c90	critical	PNG image data
IEND	0	ae426082	critical	end-of-image marker

Validity check

A problem was detected with the current file:

Multiple PLTE chunks not allowed

Do you want to save it anyway?

PNG file size: 380666 bytes

Motivation for fingerprinting image libraries

Web server fingerprinting is a critical task for the Penetration tester.

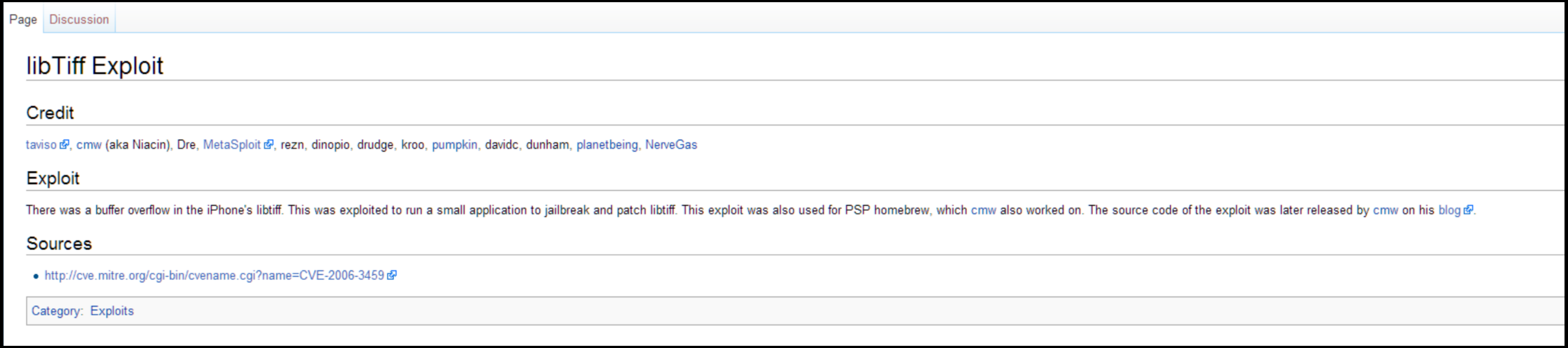
Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing.

(OWASP)

Motivation for fingerprinting image libraries

- Gives information about the application framework and language
- Can give information about system libraries
- May uncover an attack vector through native libraries
- Usually hard to hide the fingerprints

Motivation for fingerprinting image libraries



libTiff Exploit

Credit

taviso, cmw (aka Niacin), Dre, MetaSploit, rezn, dinopio, drudge, kroo, pumpkin, davidc, dunham, planetbeing, NerveGas

Exploit

There was a buffer overflow in the iPhone's libtiff. This was exploited to run a small application to jailbreak and patch libtiff. This exploit was also used for PSP homebrew, which cmw also worked on. The source code of the exploit was later released by cmw on his blog.

Sources

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3459

Category: Exploits

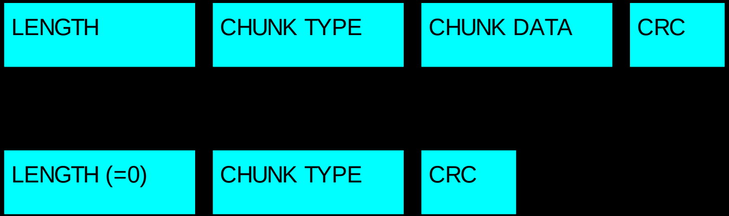
PNG file format 101

- Signature:

137 80 78 71 13 10 26 10

PNG file format 101

- Chunks:



LENGTH | CHUNK TYPE | CHUNK DATA | CRC

LENGTH (=0) | CHUNK TYPE | CRC

PNG file format 101

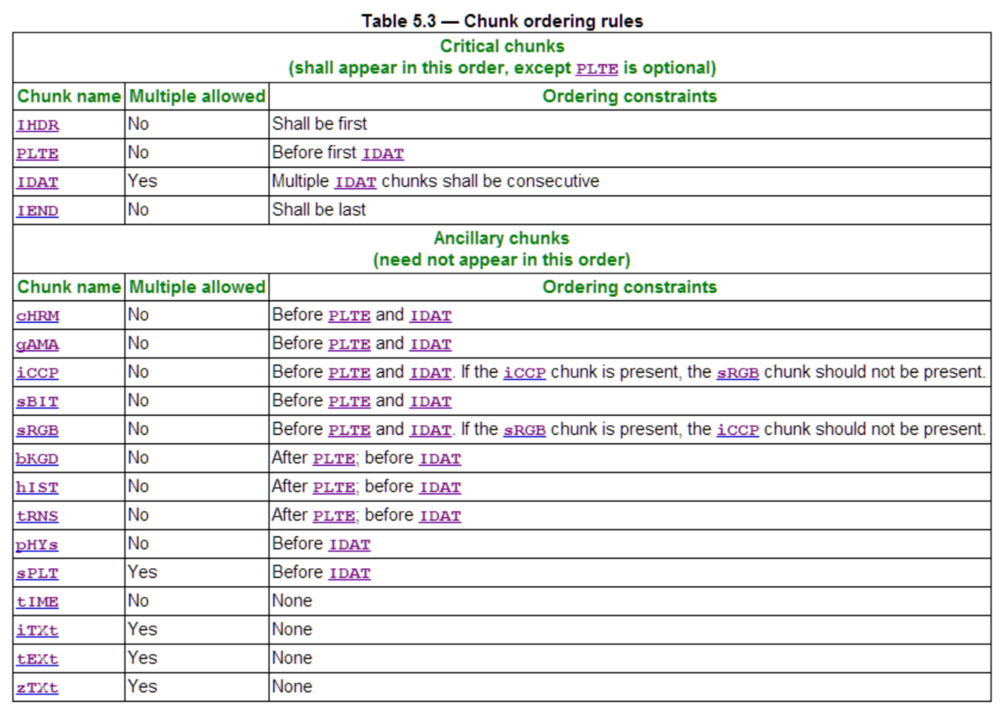


Table 5.3 — Chunk ordering rules

Critical chunks (shall appear in this order, except PLTE is optional)		
Chunk name	Multiple allowed	Ordering constraints
IHDR	No	Shall be first
PLTE	No	Before first IDAT
IDAT	Yes	Multiple IDAT chunks shall be consecutive
IEND	No	Shall be last
Ancillary chunks (need not appear in this order)		
Chunk name	Multiple allowed	Ordering constraints
cHRM	No	Before PLTE and IDAT
gAMA	No	Before PLTE and IDAT
iCCP	No	Before PLTE and IDAT. If the iCCP chunk is present, the sRGB chunk should not be present.
sBIT	No	Before PLTE and IDAT
sRGB	No	Before PLTE and IDAT. If the sRGB chunk is present, the iCCP chunk should not be present.
bKGD	No	After PLTE; before IDAT
hIST	No	After PLTE; before IDAT
tRNS	No	After PLTE; before IDAT
pHYs	No	Before IDAT
sPLT	Yes	Before IDAT
tIME	No	None
iTXt	Yes	None
tEXt	Yes	None
zTXt	Yes	None

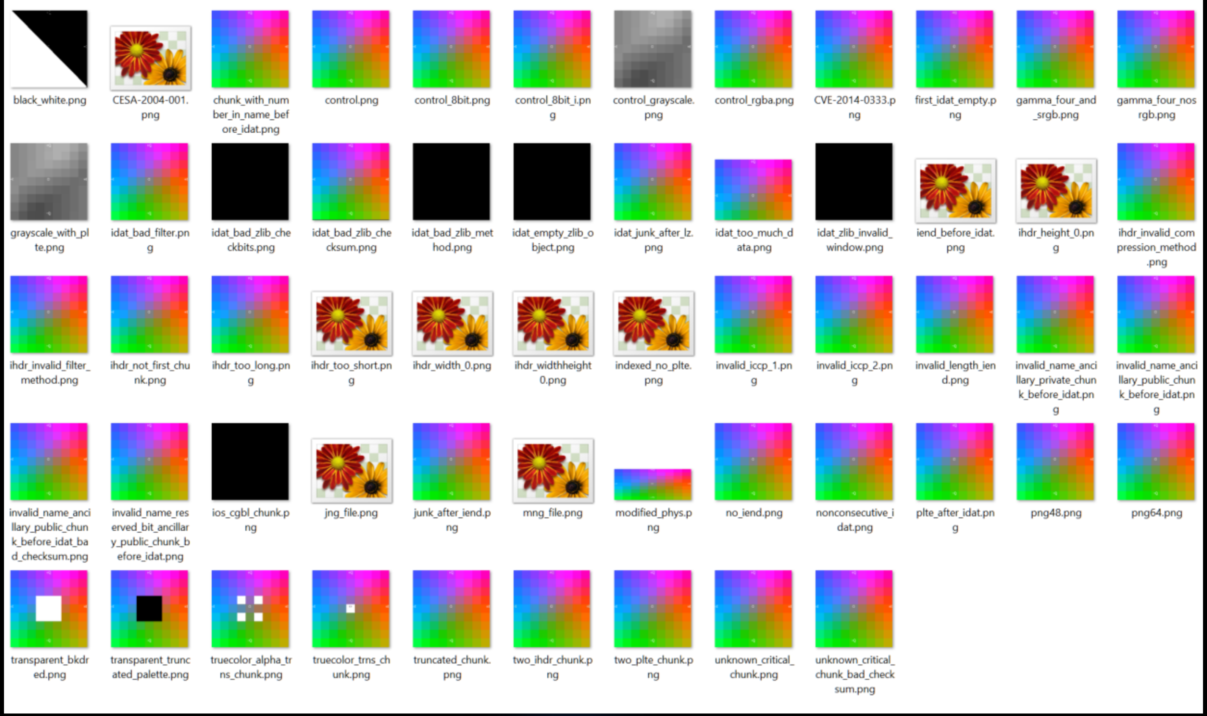
MNG and JNG files

- MNG files are the PNG equivalent of GIF anims
- JNG is the lossy version of PNG
- Both formats have their own signature different from PNG
- Supported (only ?) by ImageMagick
- ImageMagick treats MNG and JNG files as PNG

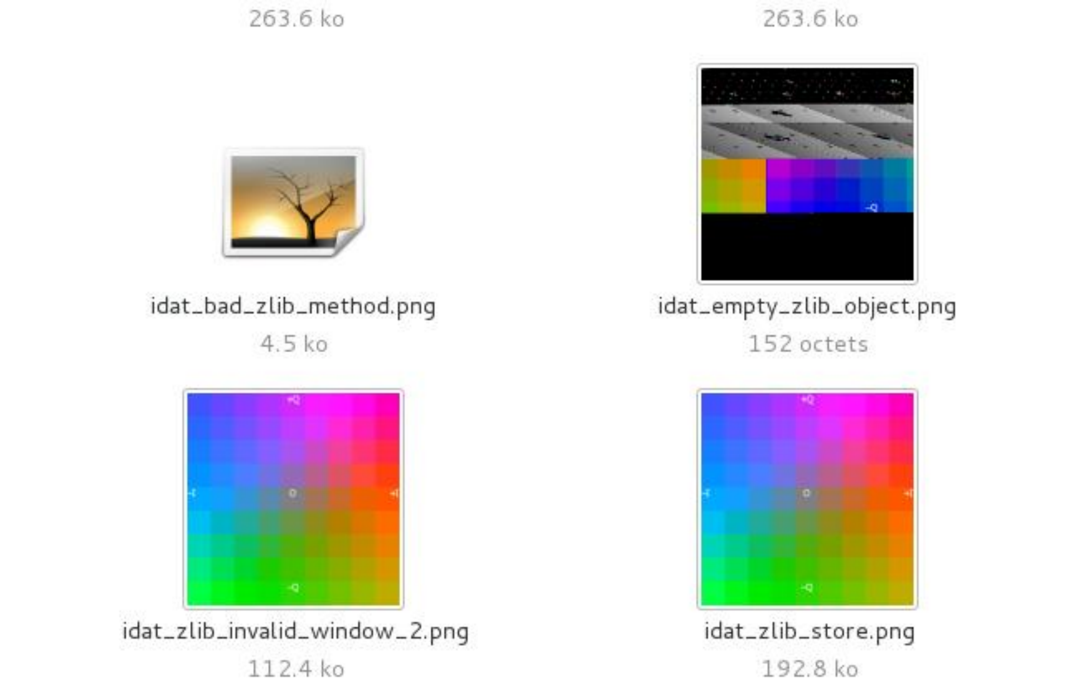
Various PNG libraries put under stress

Golang	1.0.2 linux
PHP 5 GD	5.4.9-4ubuntu2.4
OpenJDK 7	7u21-2.3.9-1ubuntu1
Python	PyPNG 0.0.16
Python	PIL 1.1.17
C# Mono	Debian 2.10.8.1-5ubuntu1
C# MS .NET	12.0.21005.1
Node.js	Pngjs 0.4.0
Ruby	ChunkyPNG 1.3.1
ImageMagick	6.7.7-10 2013-09-10 Q16
Dart	Dart Image 1.1.21
Erlang	erl_img evanmiller fork
LodePNG	20140609
Haskell	JuicyPixels 3.1.5.2

Various PNG libraries put under stress



Various PNG libraries put under stress



263.6 ko

263.6 ko

idat_bad_zlib_method.png
4.5 ko

idat_empty_zlib_object.png
152 octets

idat_zlib_invalid_window_2.png
112.4 ko

idat_zlib_store.png
192.8 ko

Various PNG libraries put under stress

```
Exception in thread "main" java.lang.NegativeArraySizeException
        at com.sun.imageio.plugins.png.PNGImageReader.readMetadata(PNGImageReader.java:745)
        at com.sun.imageio.plugins.png.PNGImageReader.readImage(PNGImageReader.java:1229)
        at com.sun.imageio.plugins.png.PNGImageReader.read(PNGImageReader.java:1577)
        at javax.imageio.ImageIO.read(ImageIO.java:1448)
        at javax.imageio.ImageIO.read(ImageIO.java:1308)
        at Test.main(Test.java:15)
```

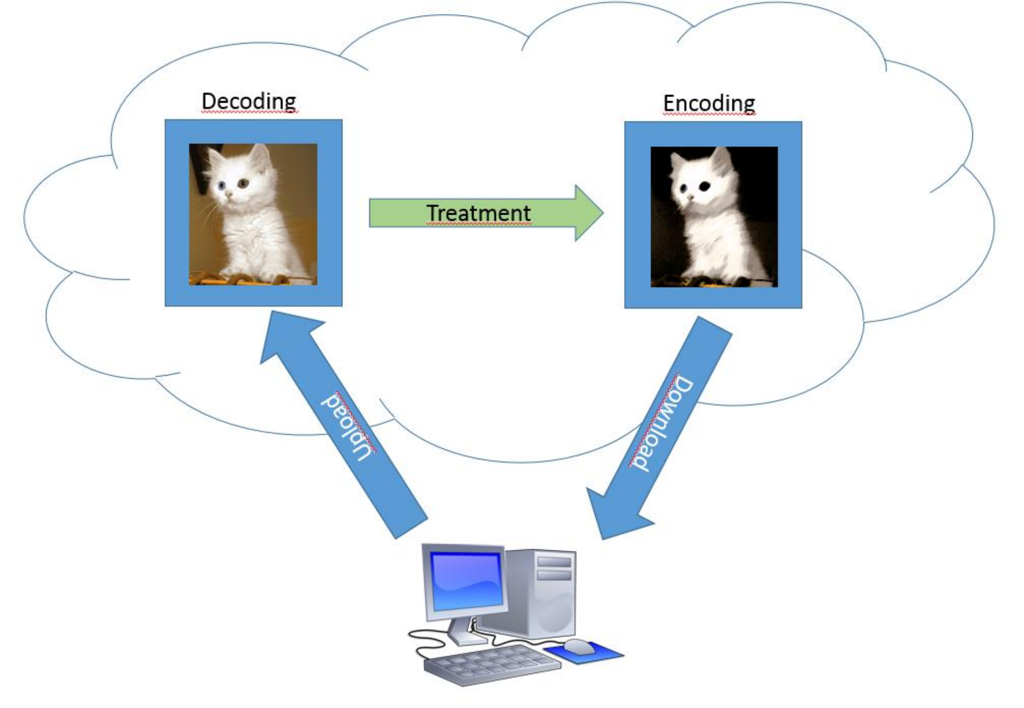
Various PNG libraries put under stress

```
22698 Segmentation fault      ./test $1
```

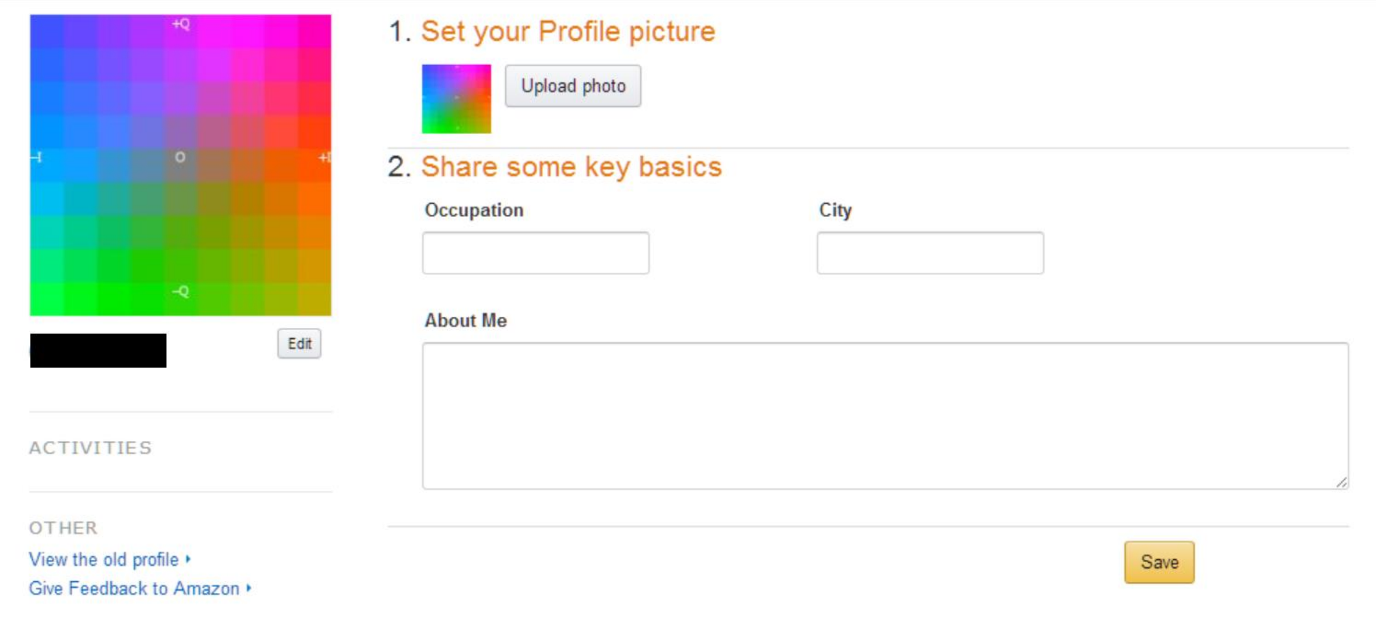
Various PNG libraries put under stress

```
panic: runtime error: invalid memory address or nil pointer dereference
[signal 0xb code=0x1 addr=0x20 pc=0x4246cd]
```

Fingerprinting web applications with PNG



Fingerprinting web applications with PNG



[redacted]

ACTIVITIES

OTHER

View the old profile ▸

Give Feedback to Amazon ▸

1. Set your Profile picture

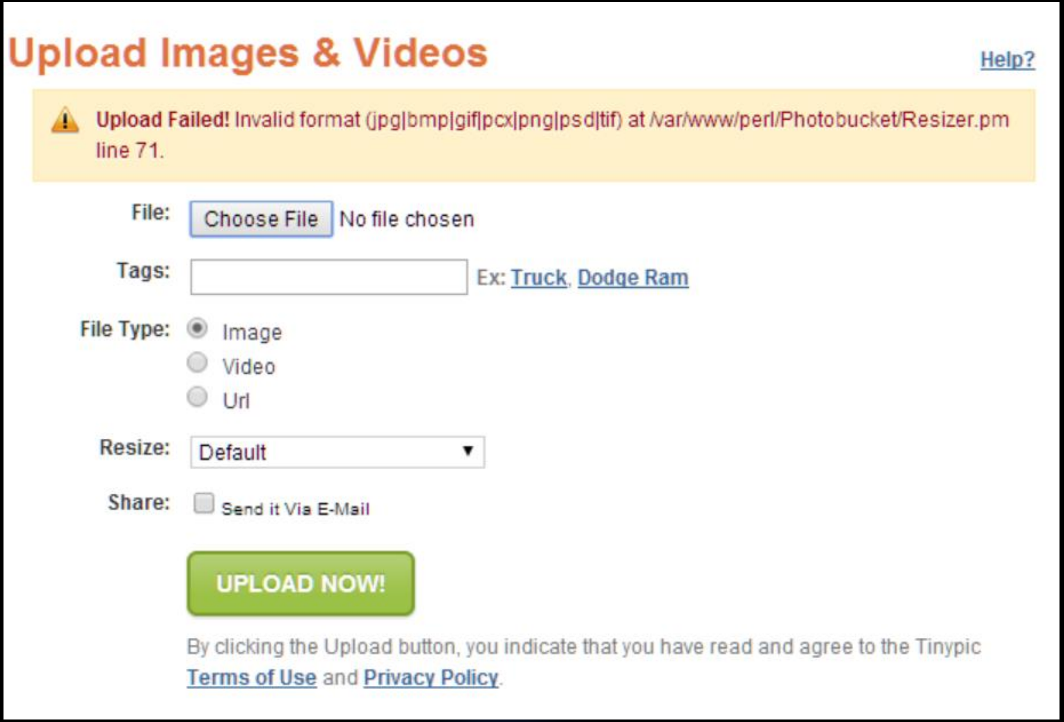
2. Share some key basics

Occupation

City

About Me

Practical results on major websites



Upload Images & Videos

⚠ **Upload Failed!** Invalid format (jpg|bmp|gif|pcx|png|psd|tif) at /var/www/perl/Photobucket/Resizer.pm line 71.

File: Choose File No file chosen

Tags: Ex: Truck, Dodge Ram

File Type: ● Image ○ Video ○ Url

Resize: Default

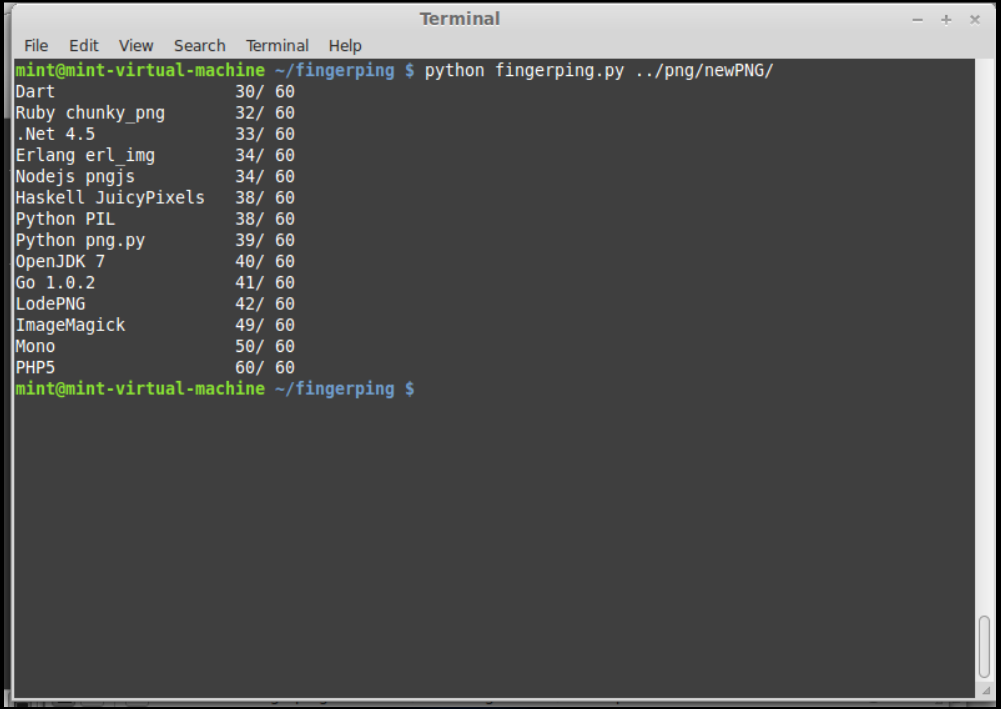
Share: □ Send it Via E-Mail

By clicking the Upload button, you indicate that you have read and agree to the Tinypic Terms of Use and Privacy Policy.

Practical results on major websites

ImageMagick (libpng)	Amazon, Shopify, Yandex, Github, Bayimg, Tinypic …
PHP / GD	Tumblr
Java	Imdb, Linkedin
Python PIL	Pinterest

Introducing the fingerping tool



```
mint@mint-virtual-machine ~/fingerping $ python fingerping.py ../png/newPNG/
Dart                   30/ 60
Ruby chunky_png        32/ 60
.Net 4.5               33/ 60
Erlang erl_img         34/ 60
Nodejs pngjs           34/ 60
Haskell JuicyPixels    38/ 60
Python PIL             38/ 60
Python png.py          39/ 60
OpenJDK 7              40/ 60
Go 1.0.2               41/ 60
LodePNG                42/ 60
ImageMagick            49/ 60
Mono                   50/ 60
PHP5                   60/ 60
mint@mint-virtual-machine ~/fingerping $
```

https://github.com/0xcite/fingerping

Conclusion

Look for 0-days in ImageMagick

THANK YOU!