Image & Video Forensics

A Picture is Worth 1000 Frauds
- Robert Winkel

saltbushgroup

Who Am I?

- Bull
- @RobertWinkel
- Natural skeptic
- Online sleuth / debunker

Intro

- With software such as Photoshop and GIMP so readily available, we see more and more faked images and videos everyday.
- These could range from fun videos to faked credentials.

Agenda

- Methods to determine whether an image is fake
- Dabble in fake video detection too
- Geolocate images and videos

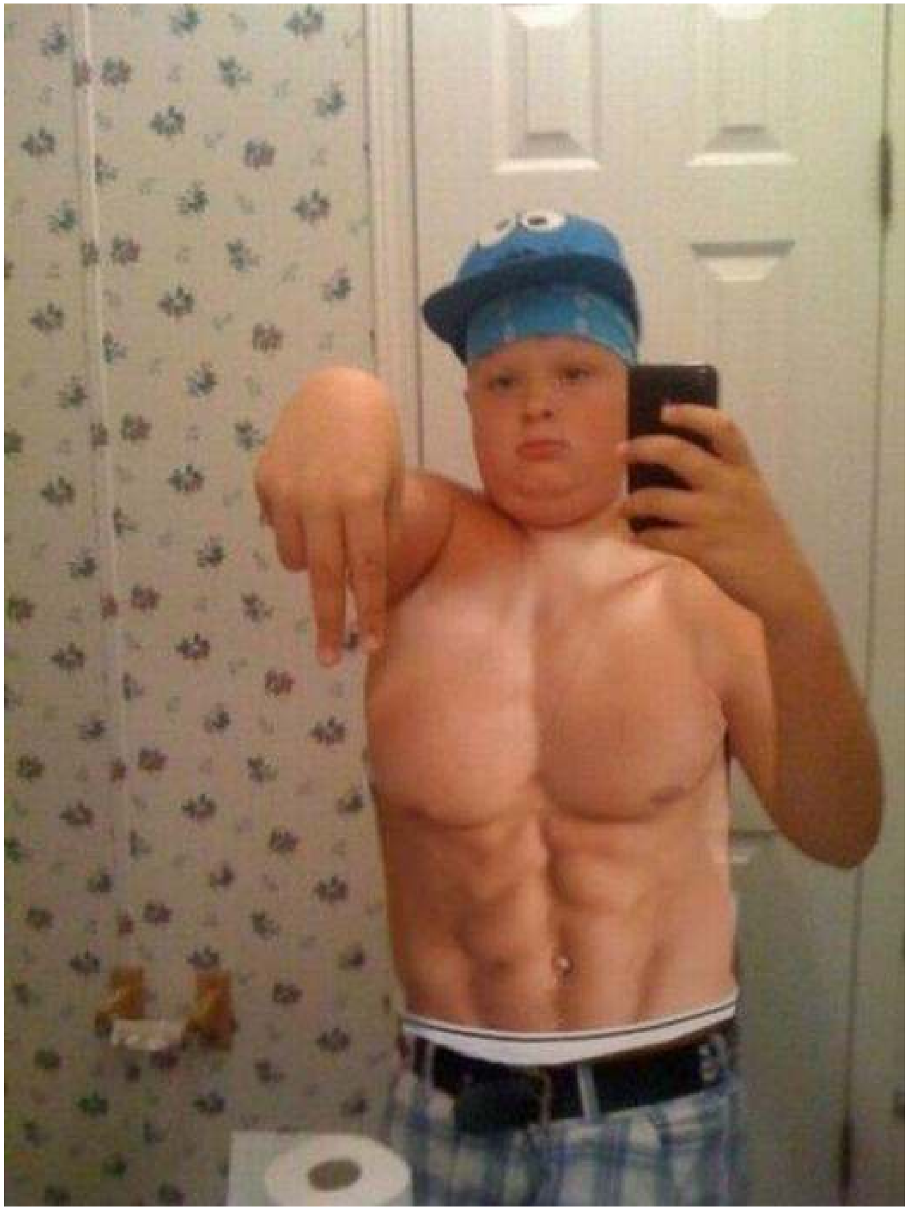
saltbushgroup

First Some Fun

ARE THESE REAL OR FAKE?

Some are obvious. Some not so…

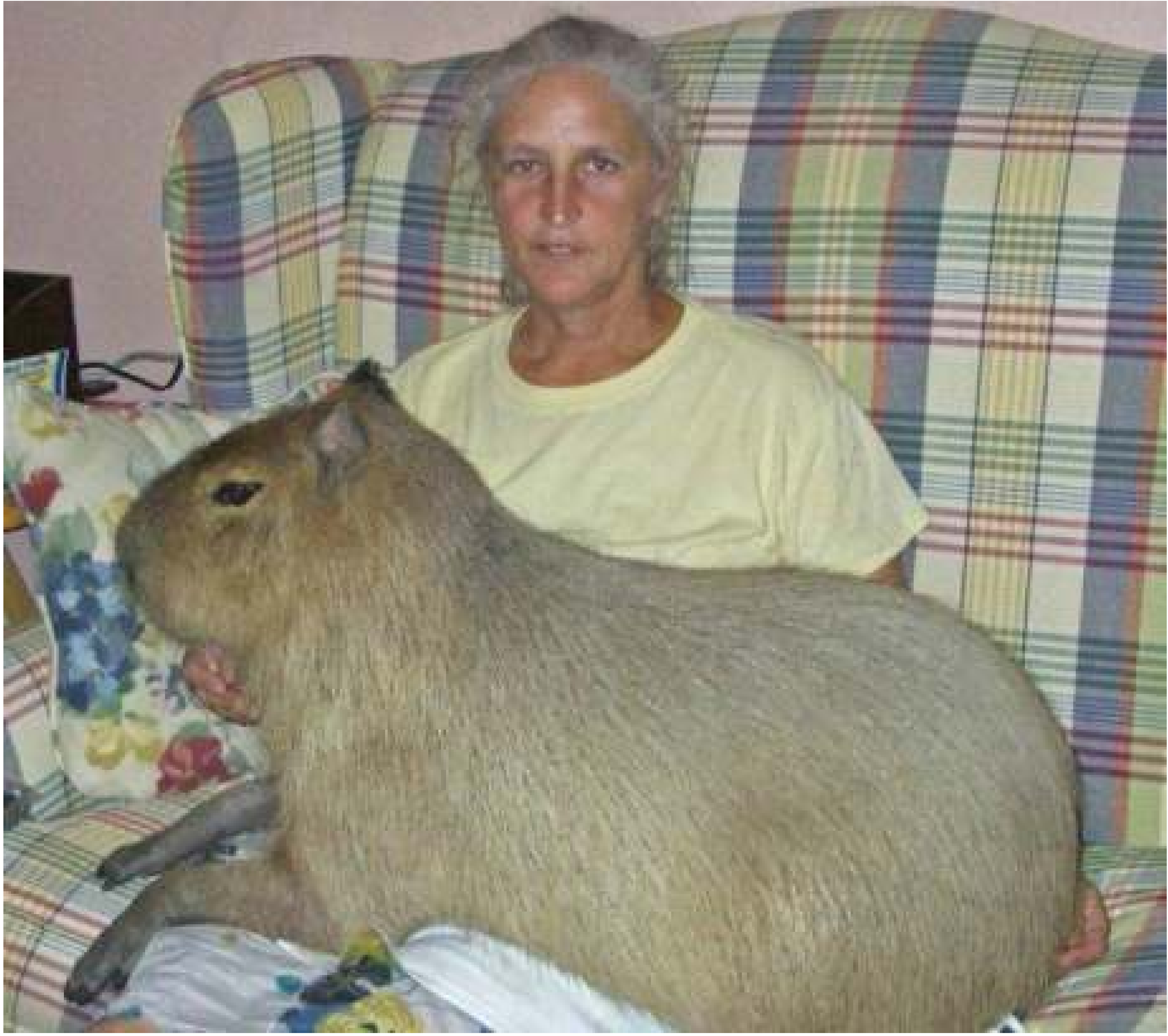
Real or Fake?



saltbushgroup

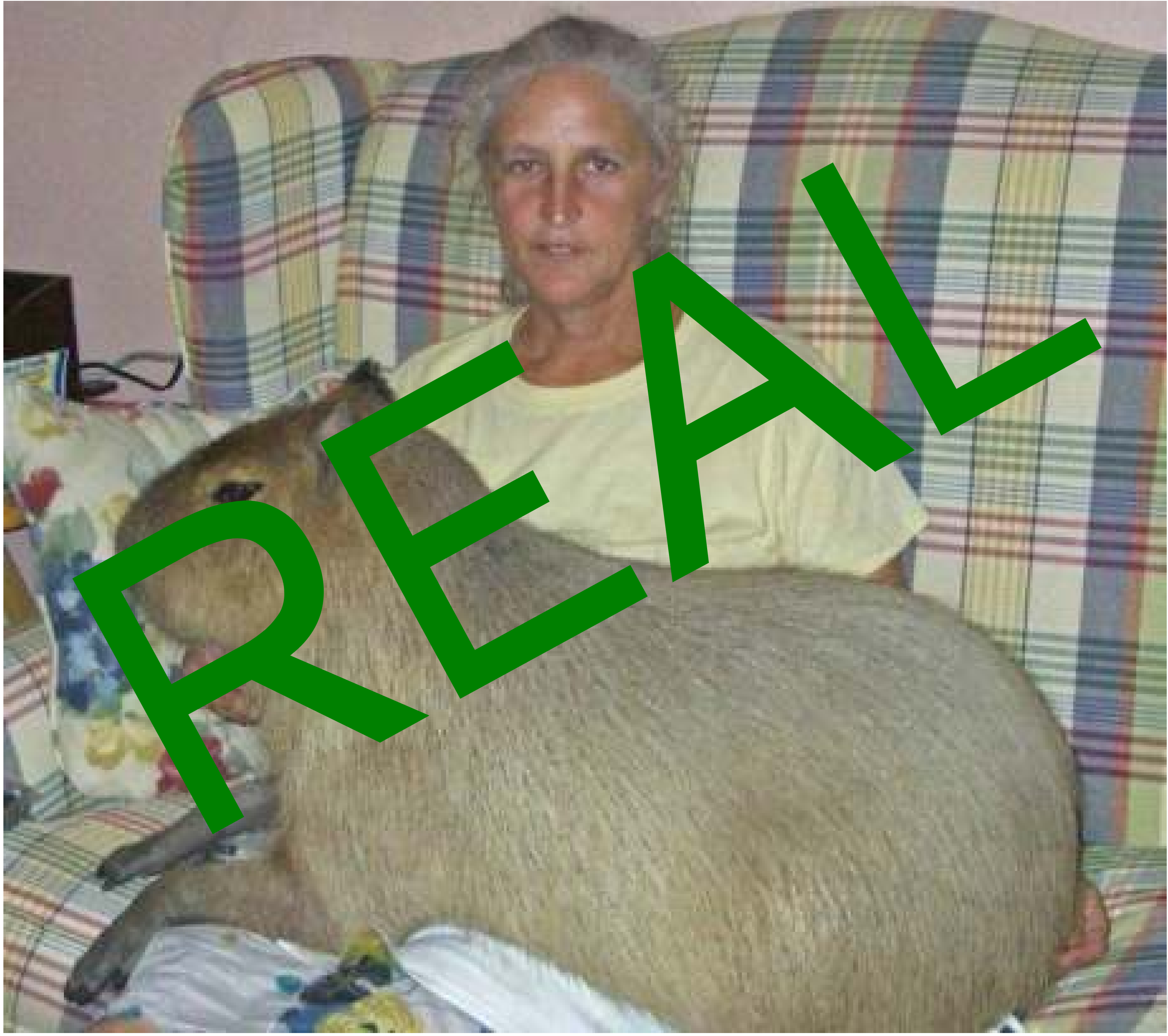
Real or Fake?

Real or Fake?

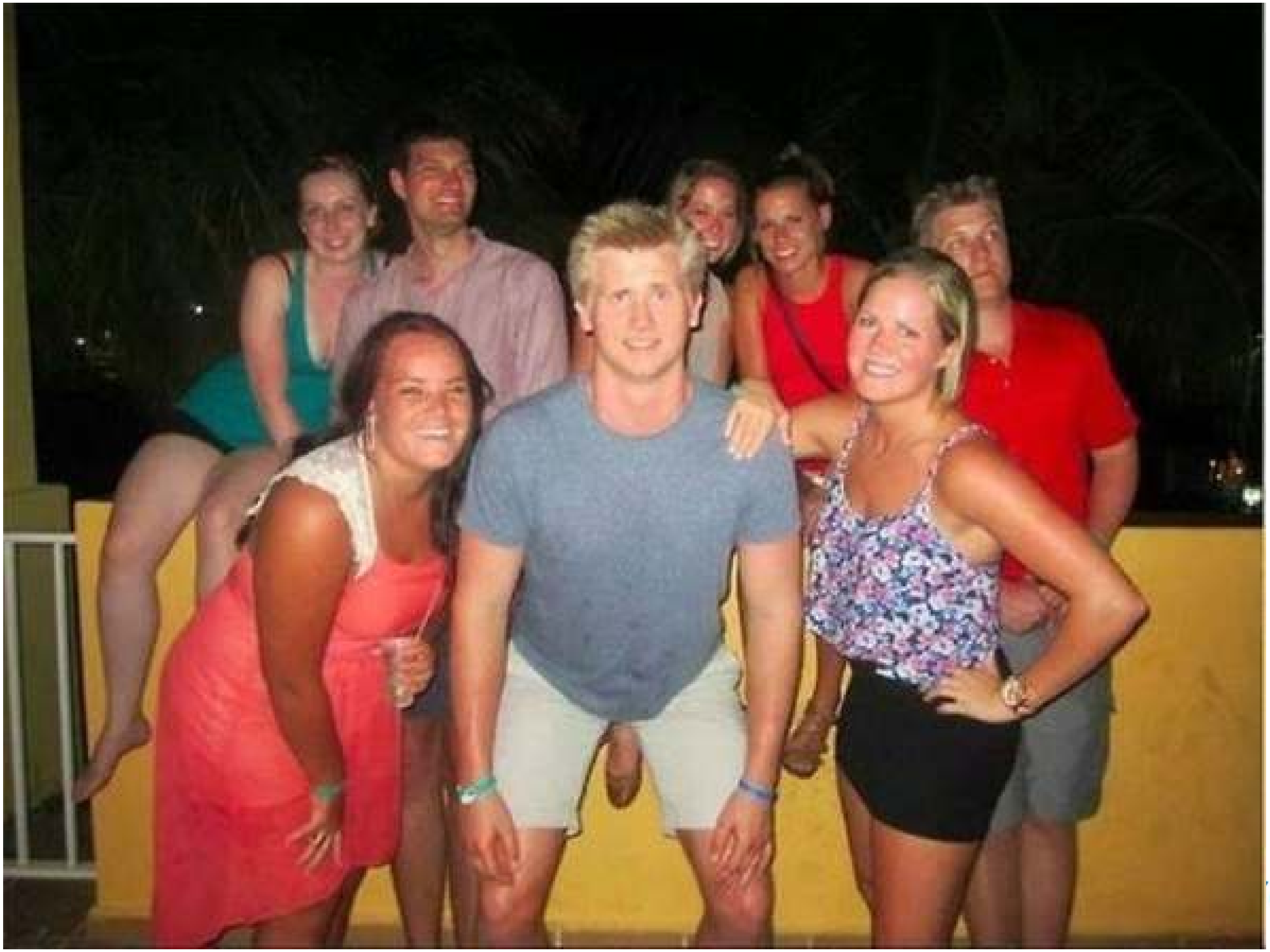


hgroup

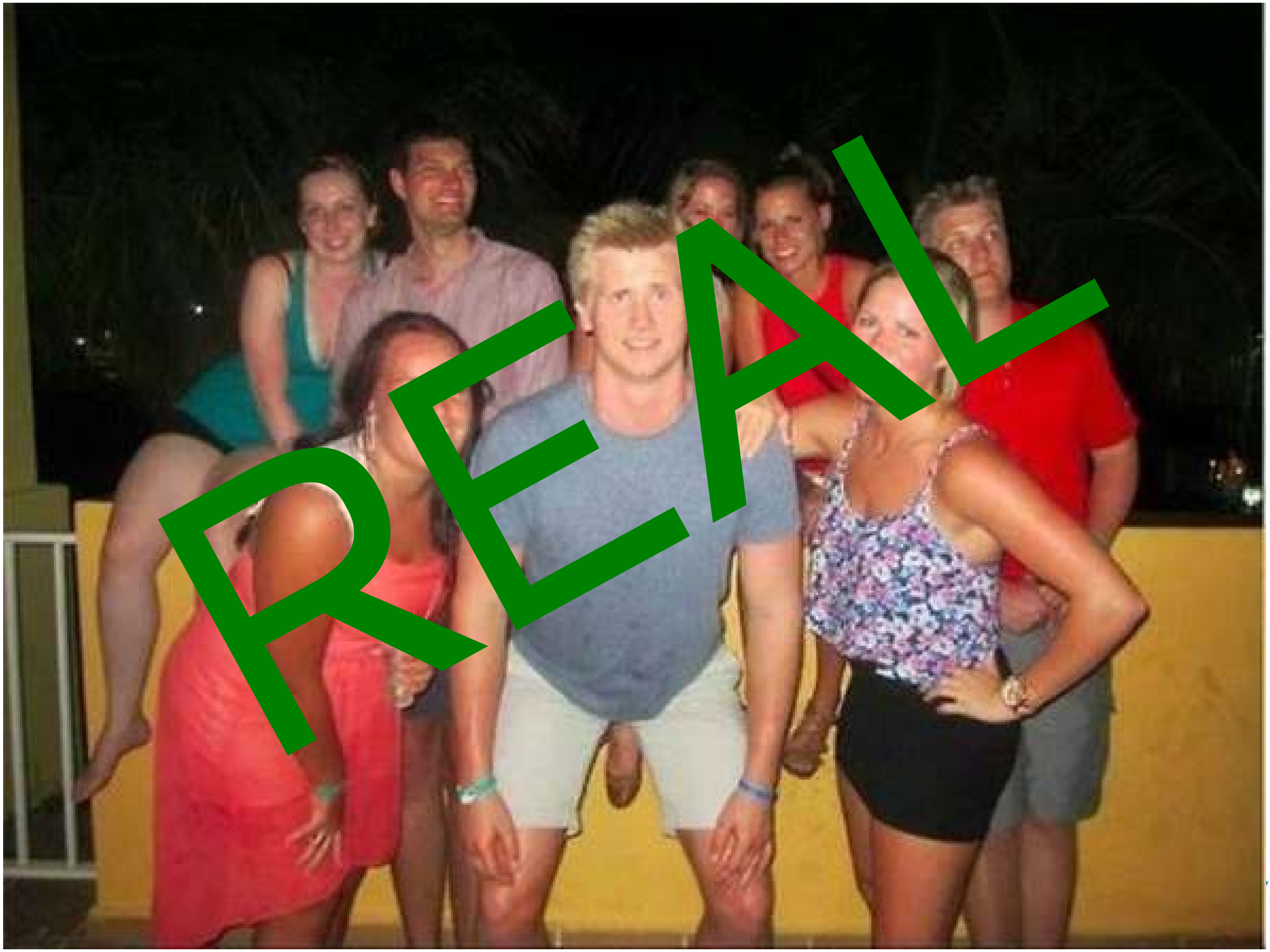
Real or Fake?



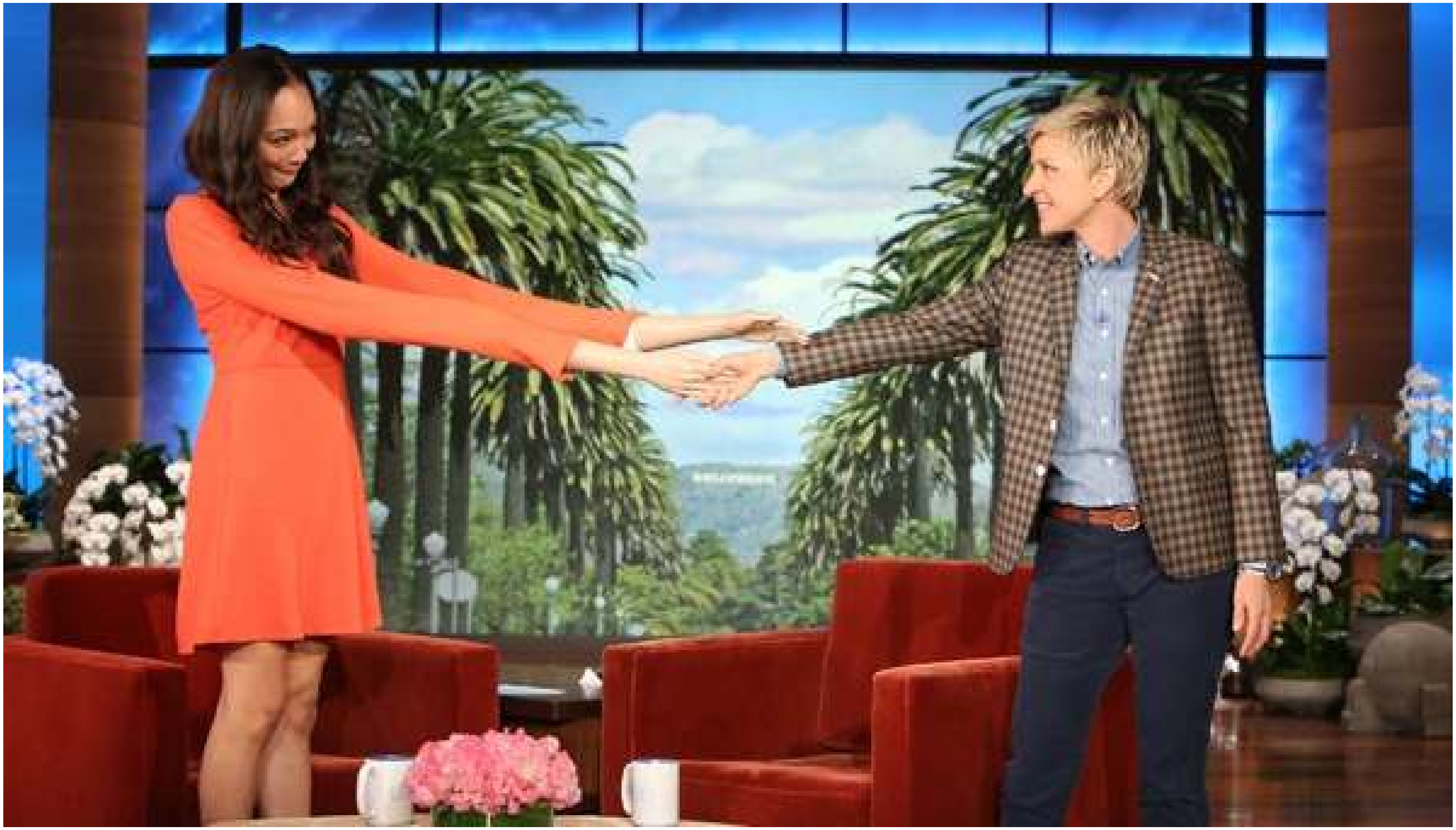
Real or Fake?



Real or Fake?



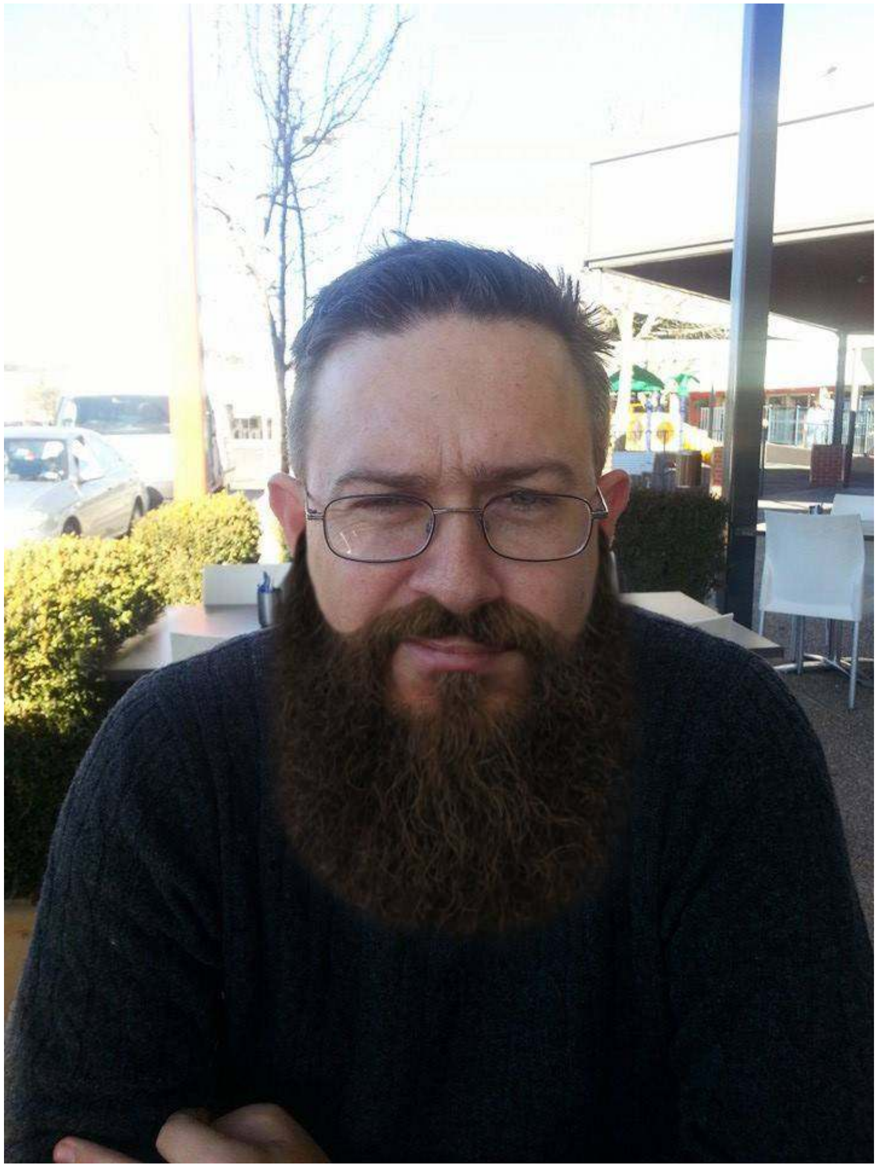
Real or Fake?



saltbushgroup

Real or Fake?

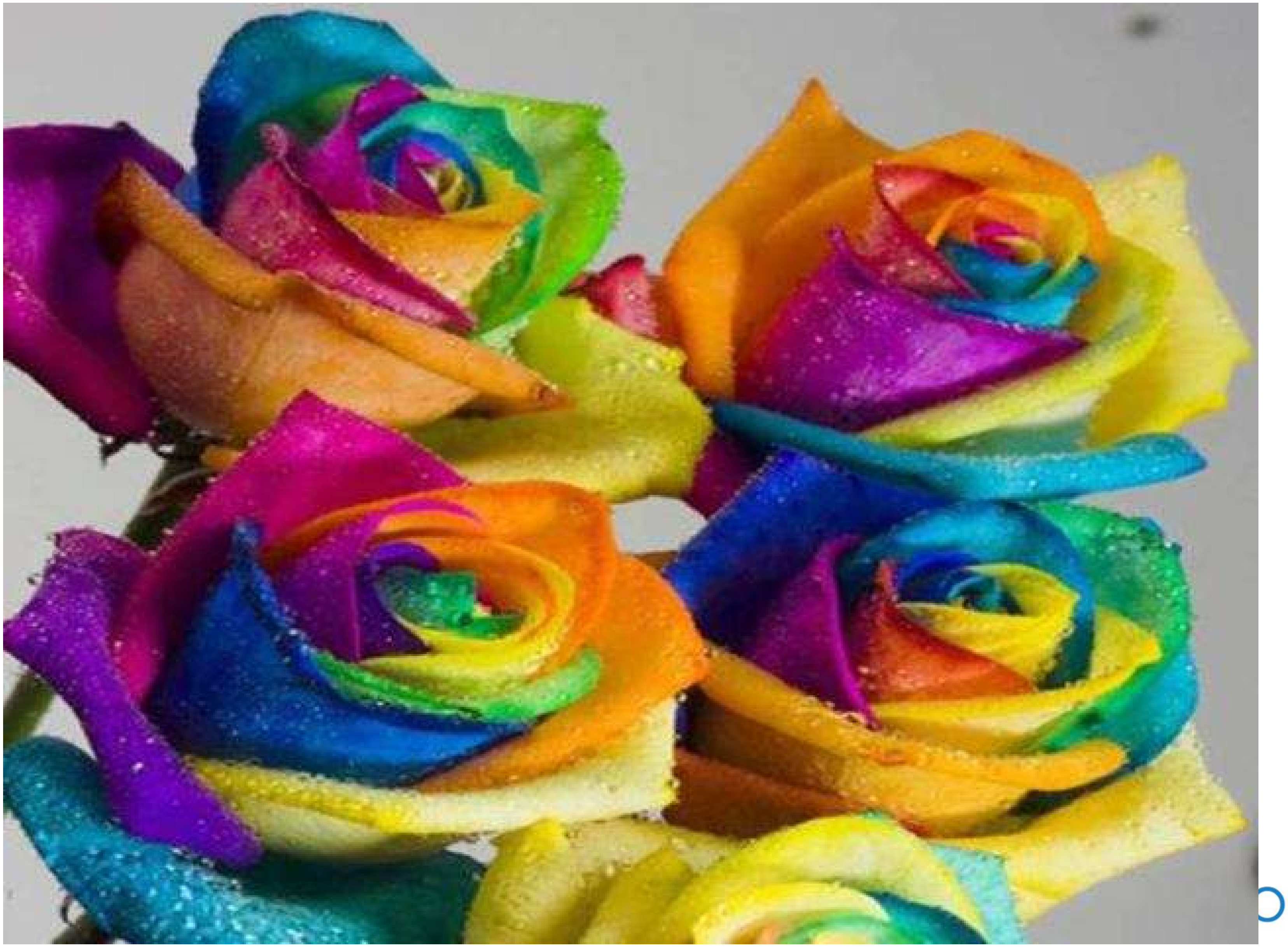
Real or Fake?



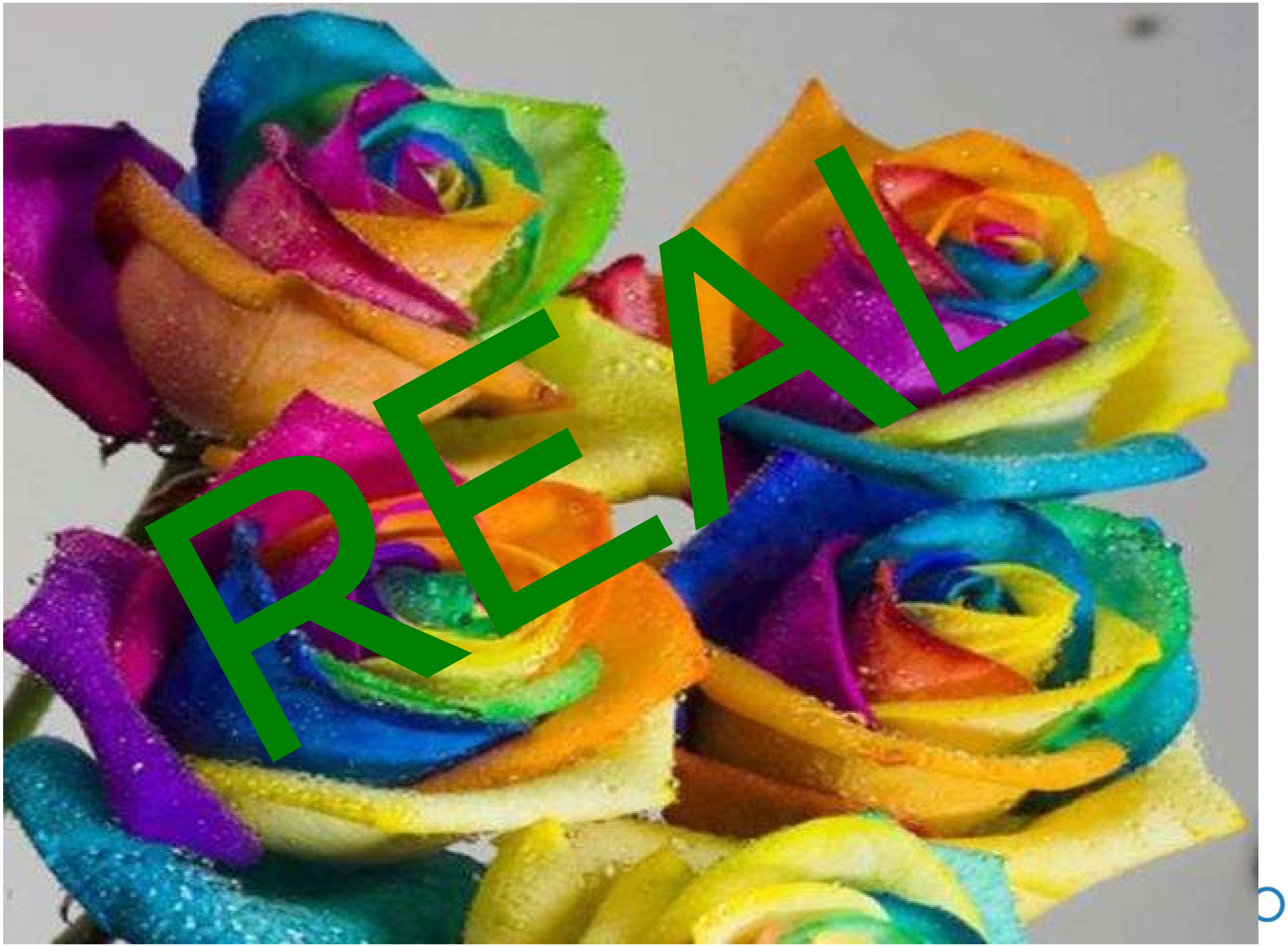
saltbushgroup

Real or Fake?

Real or Fake?

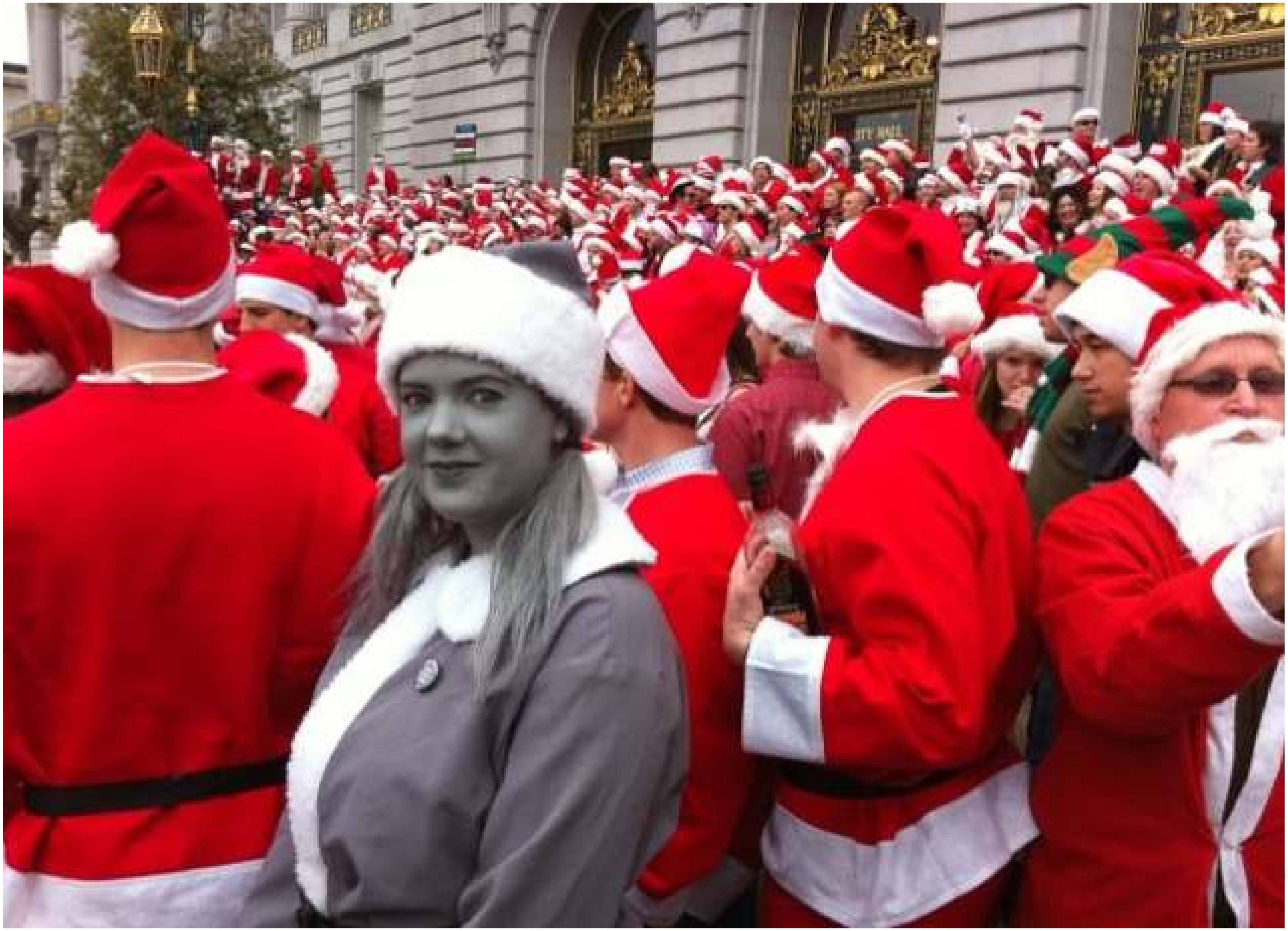


Real or Fake?

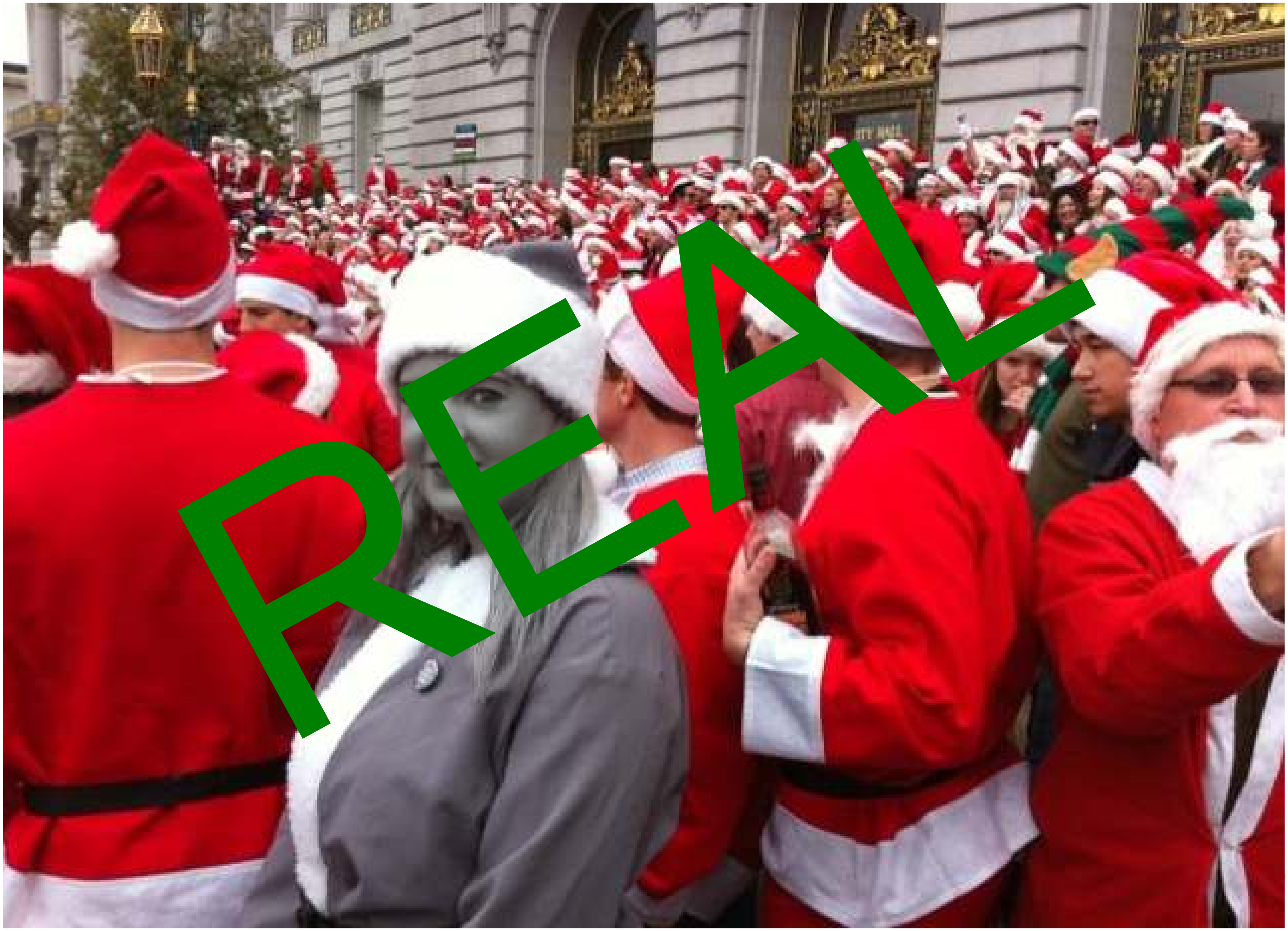


REAL

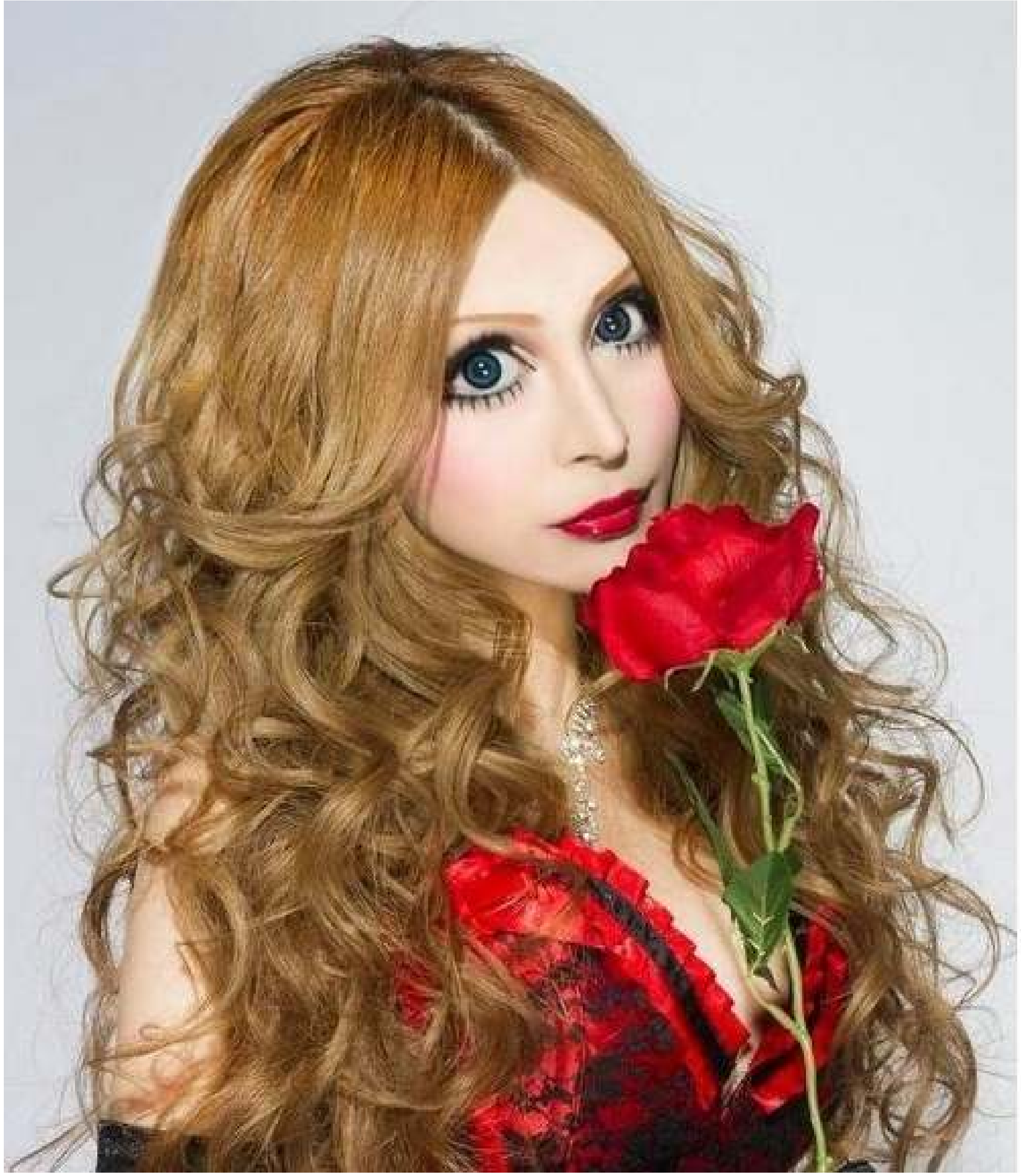
Real or Fake?



Real or Fake?

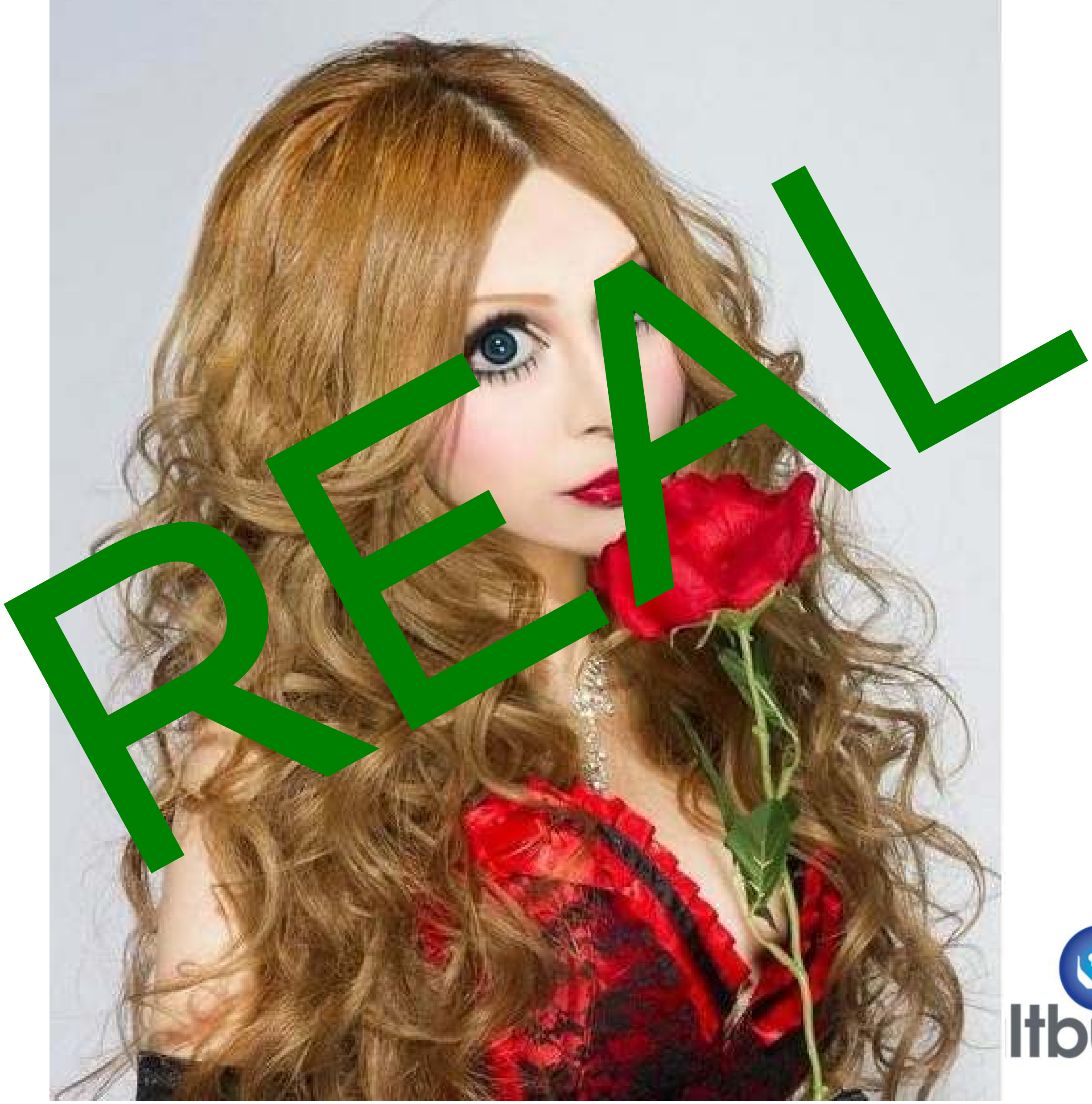


Real or Fake?



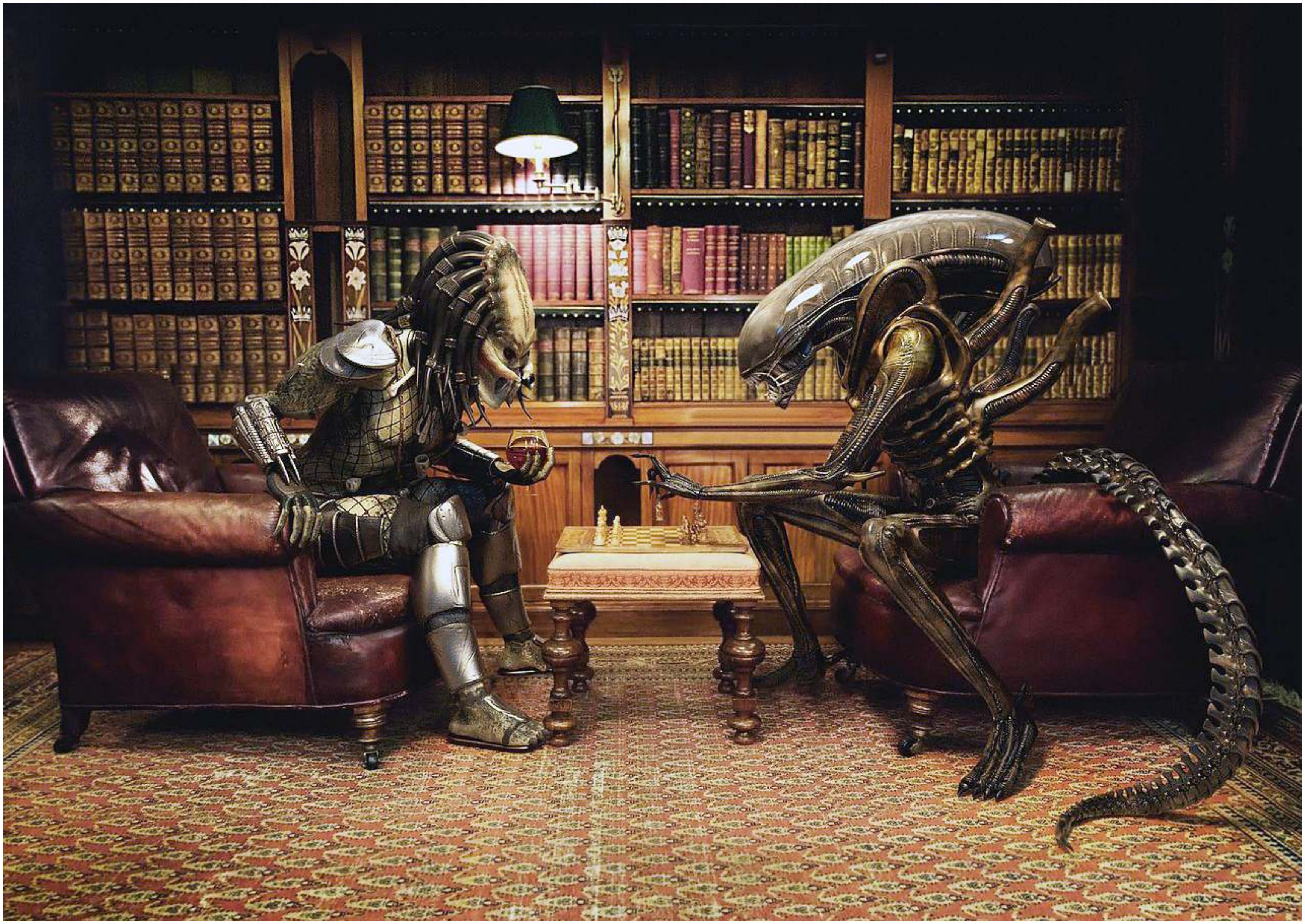
Itbushgroup

Real or Fake?



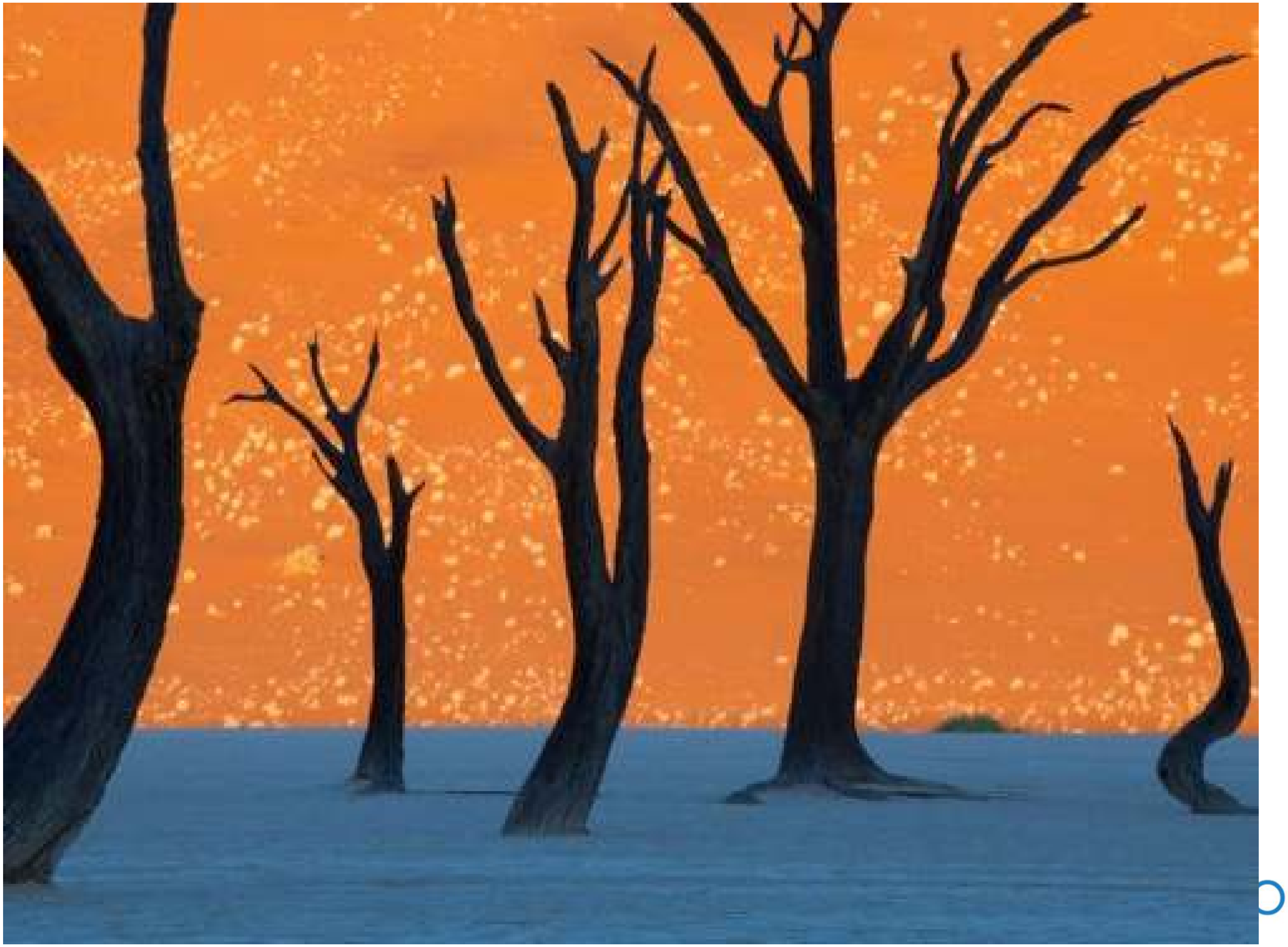
REAL

Real or Fake?

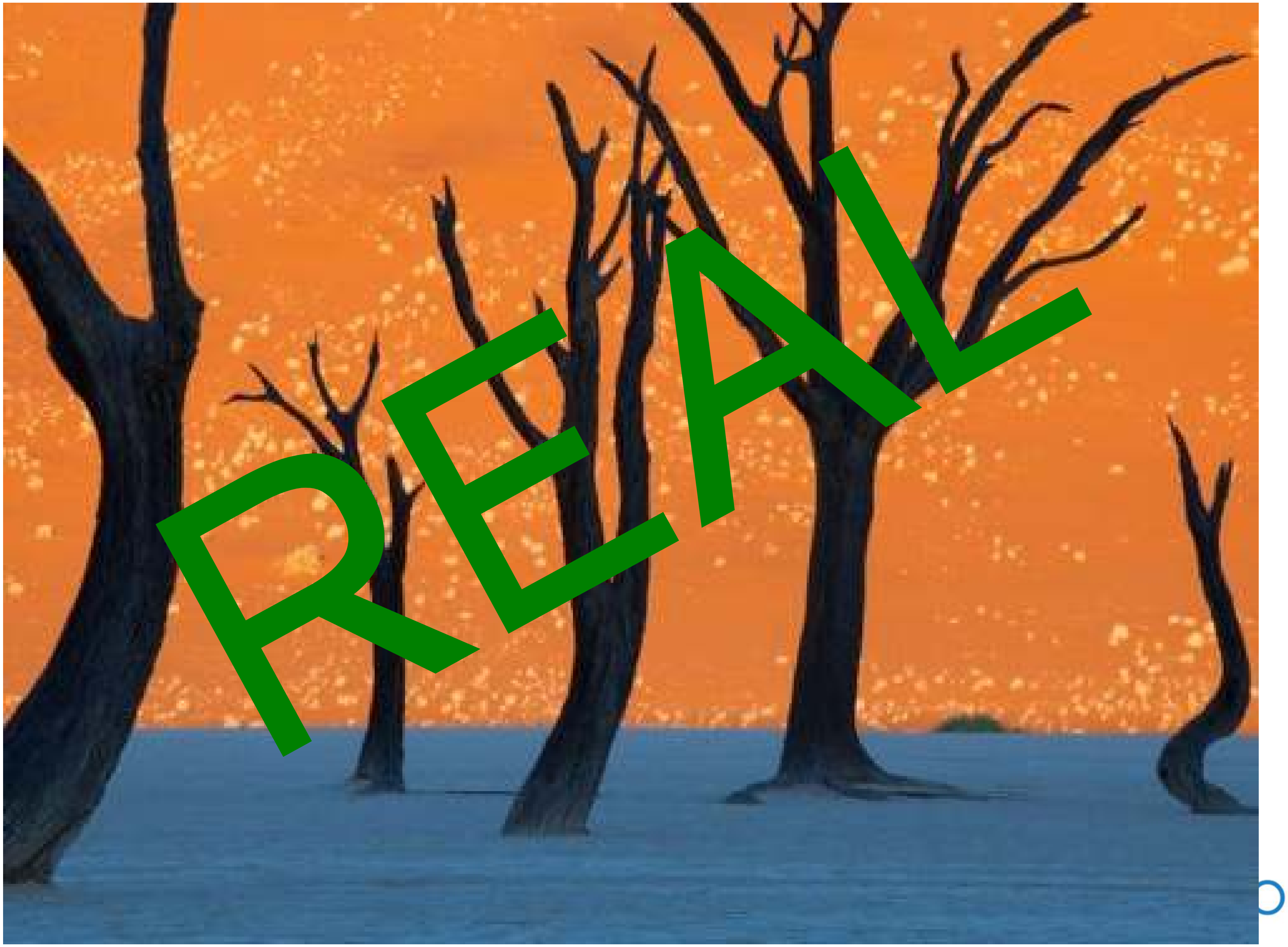


Real or Fake?

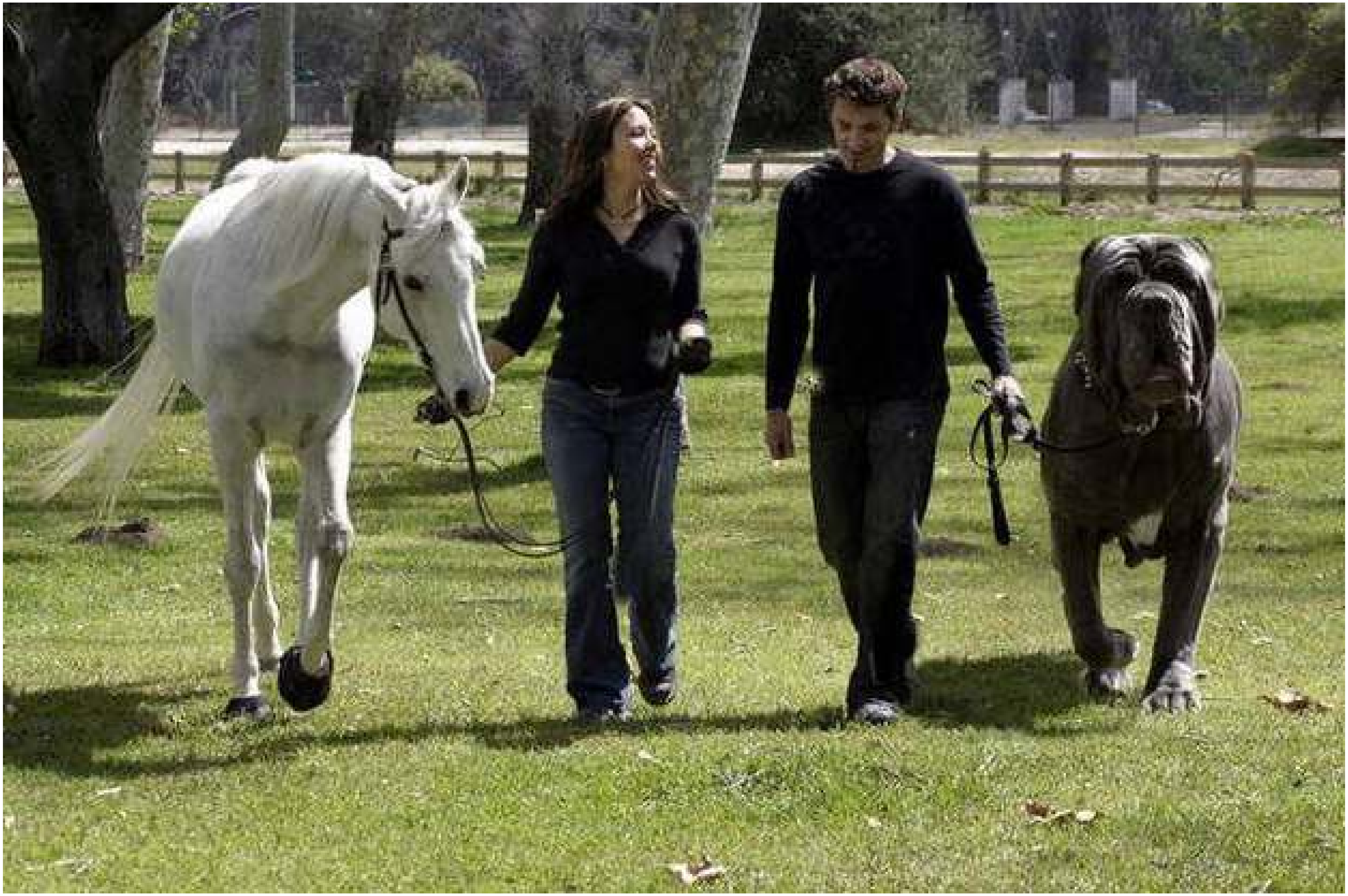
Real or Fake?



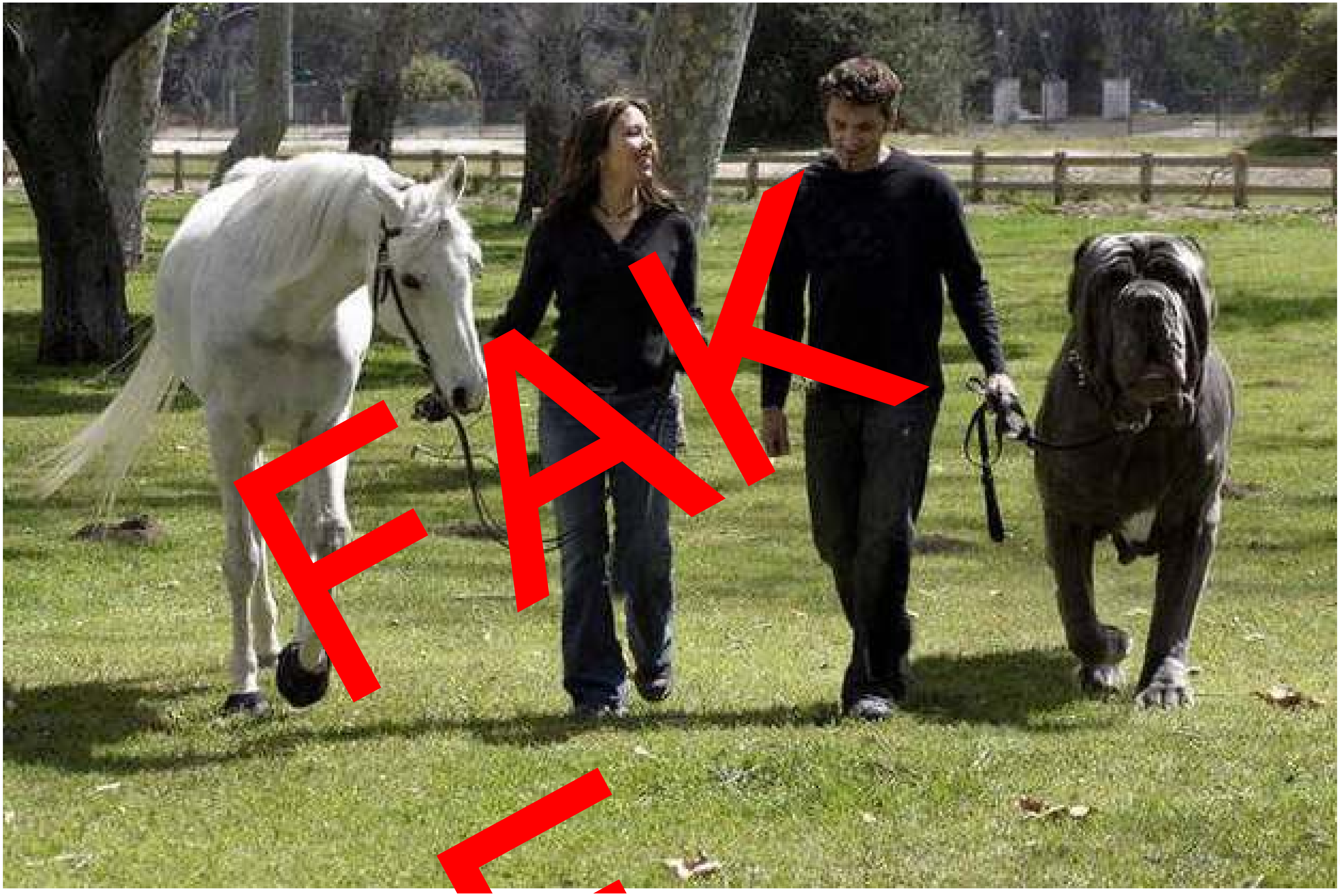
Real or Fake?



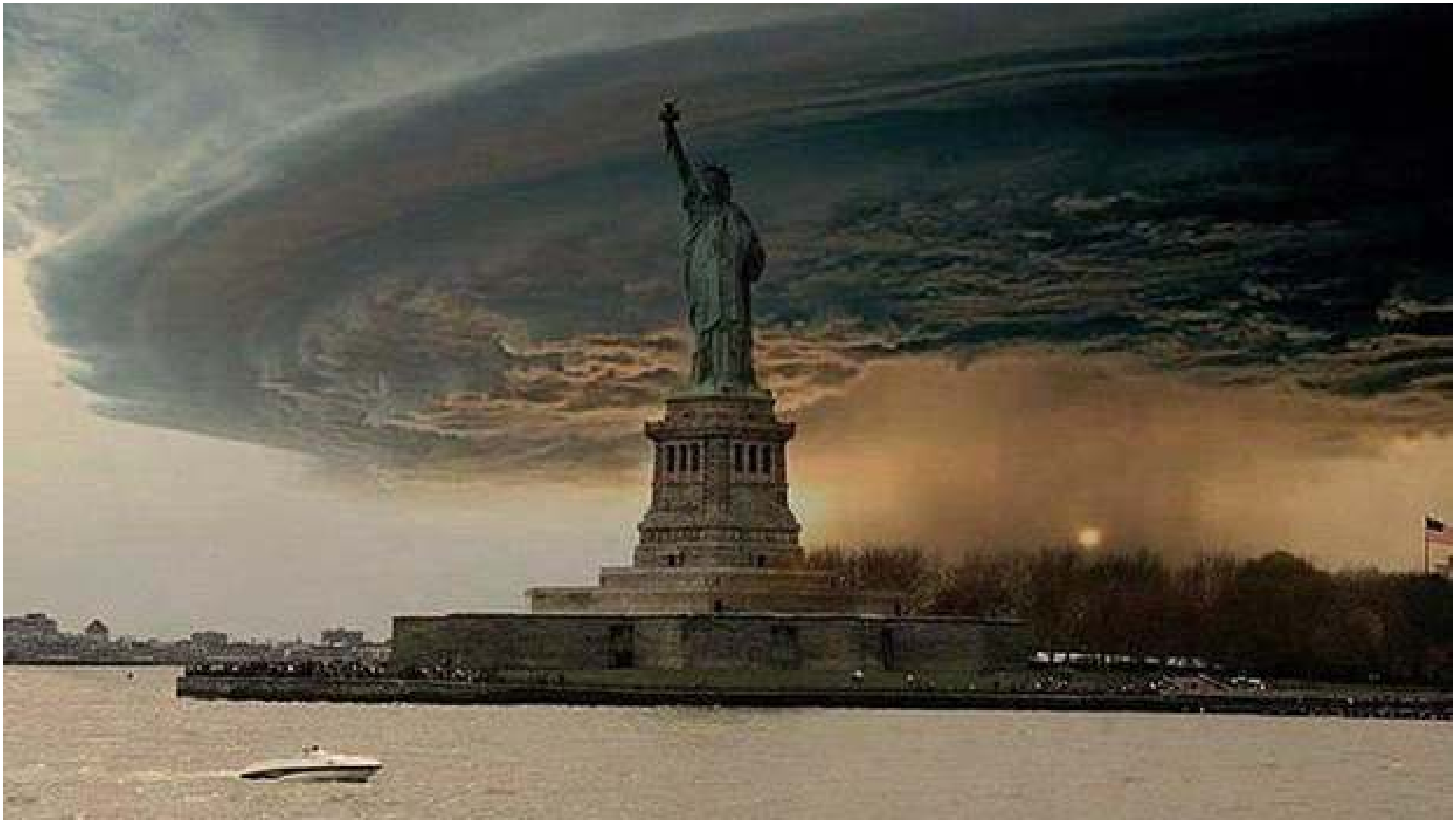
Real or Fake?



Real or Fake?



Real or Fake?



saltbushgroup

Real or Fake?

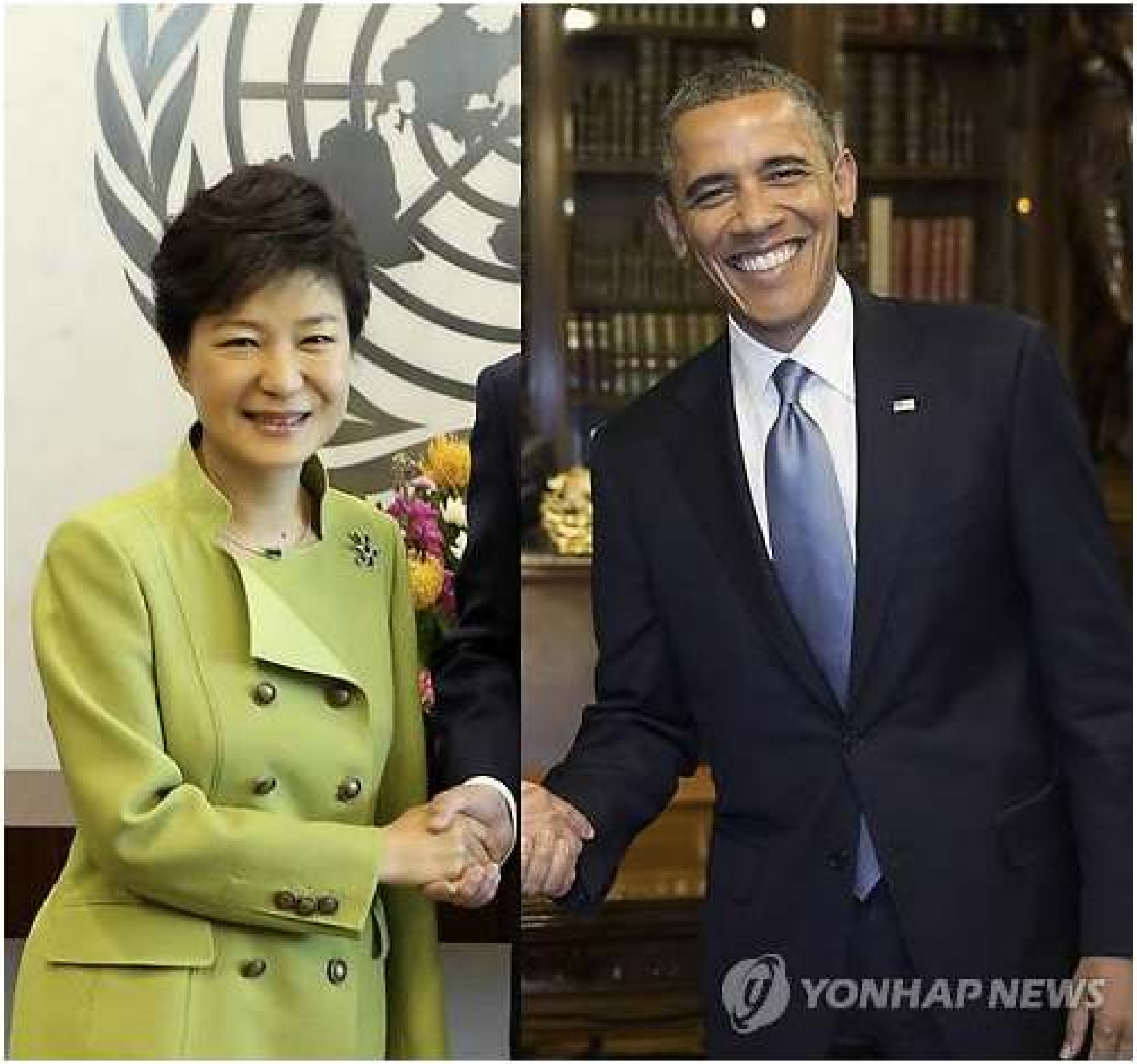
Technique – Look for the Obvious

- As we just saw. “Obvious” is subjective.
- But sometimes obvious is just obvious…

Technique – Look for the Obvious

- As we just saw. “Obvious” is subjective.
- But sometimes obvious is just obvious…

Technique – Look for the Obvious



South Korean President Park Geun-hye (L) shakes hands with US President Barack Obama at a White House meeting on May 7. (Yonhap)

TECHNIQUES

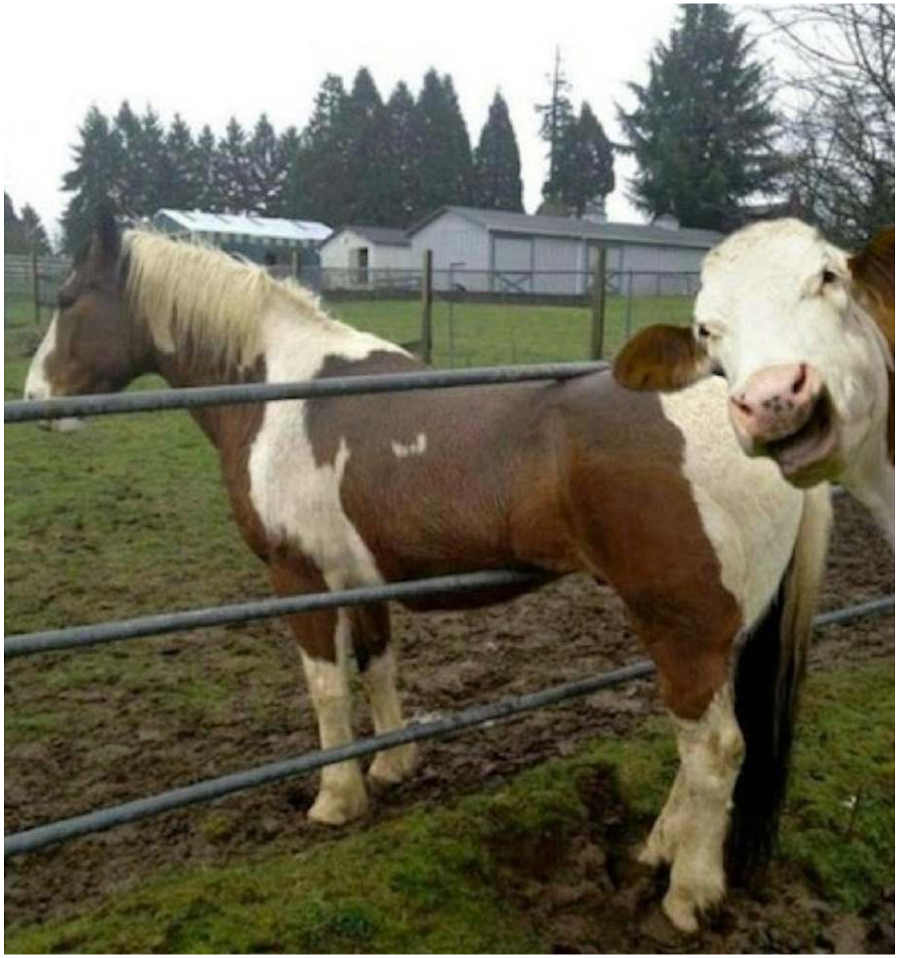
Technique – Look for the Original

Use Google Reverse Image Search to find the original image.

saltbushgroup

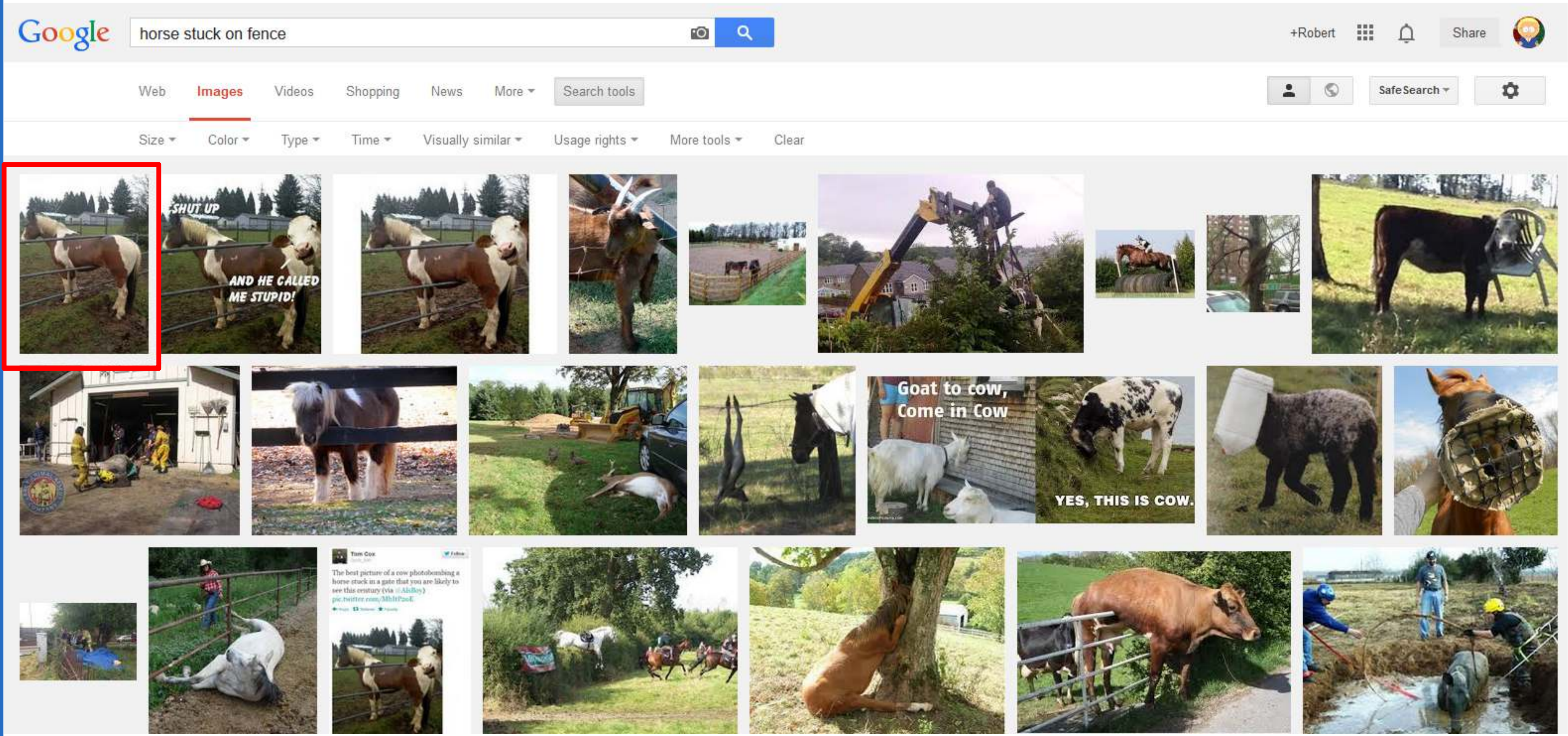
Technique – Look for the Original

Use Google Image Search to find the original image.



saltbushgroup

Technique – Look for the Original

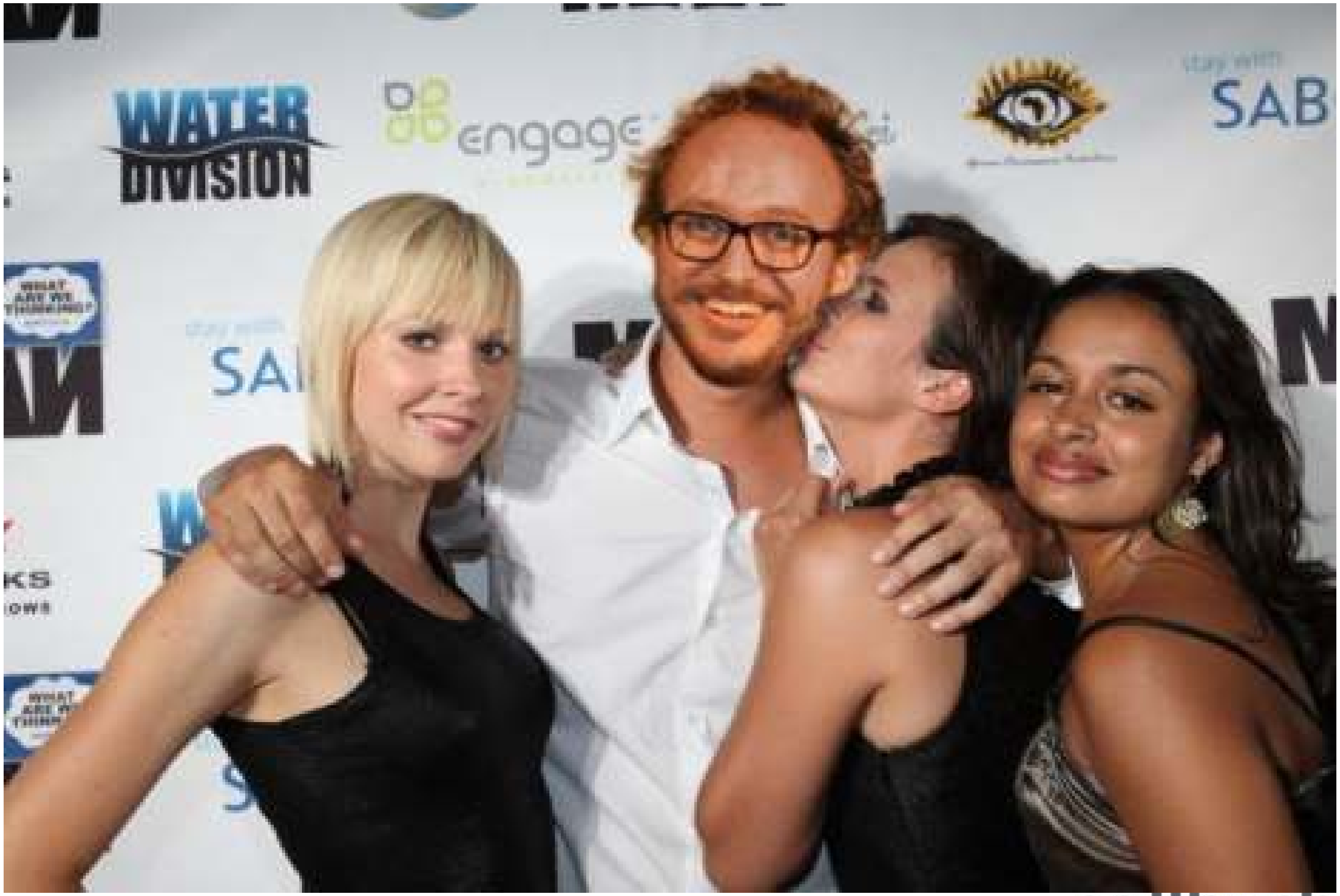


horse stuck on fence

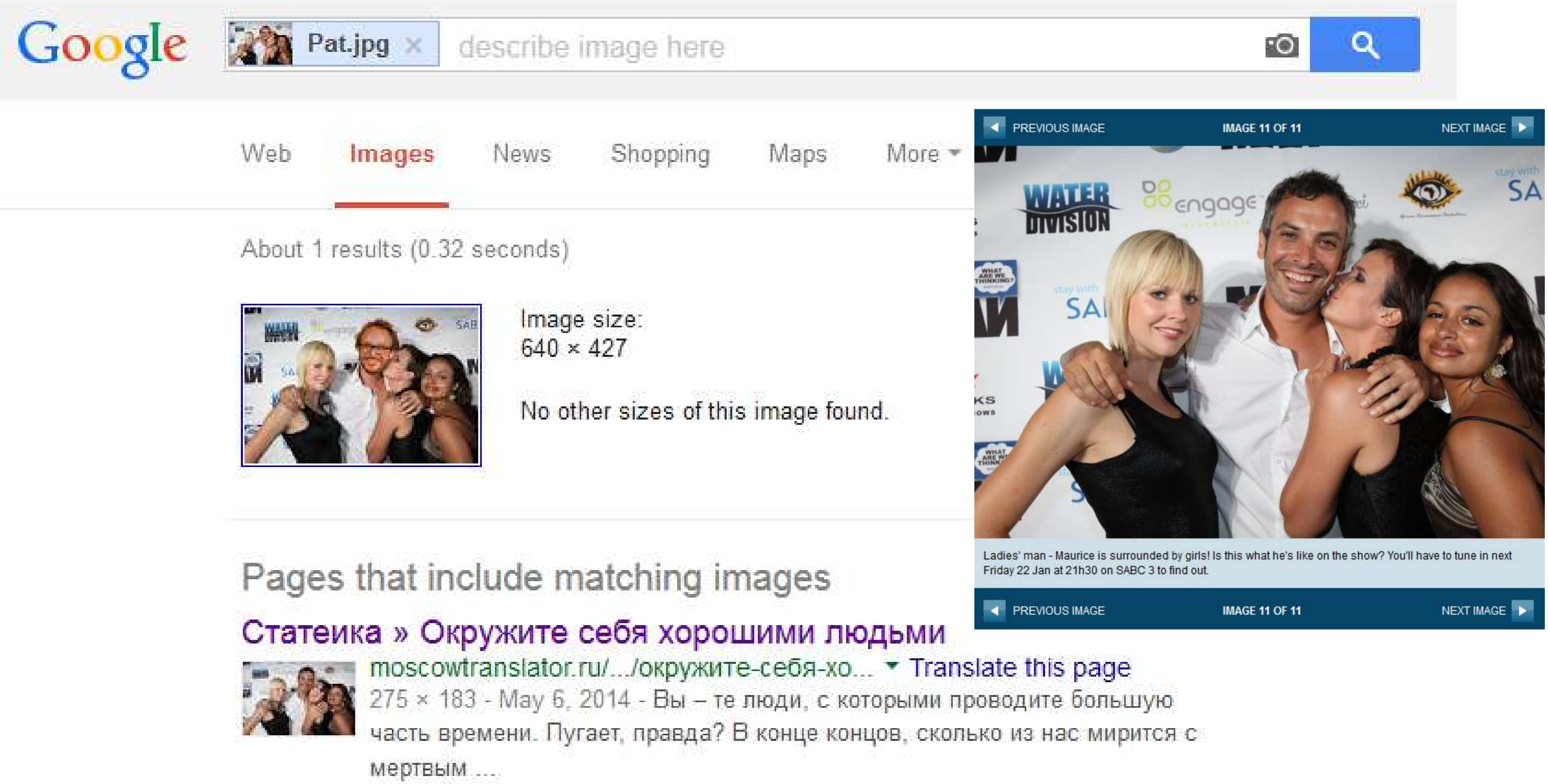
The best picture of a cow photobombing a horse stuck in a gate that you are likely to see this century (via @AlsBoy) pic.twitter.com/MbItPaoE

Technique – Look for the Original

When you suspect that most of the image may be on the Internet somewhere, just put the whole image into Google Image Search.



Technique – Look for the Original



About 1 results (0.32 seconds)

Image size:
640 × 427

No other sizes of this image found.

Pages that include matching images

Статеика » Окружите себя хорошими людьми

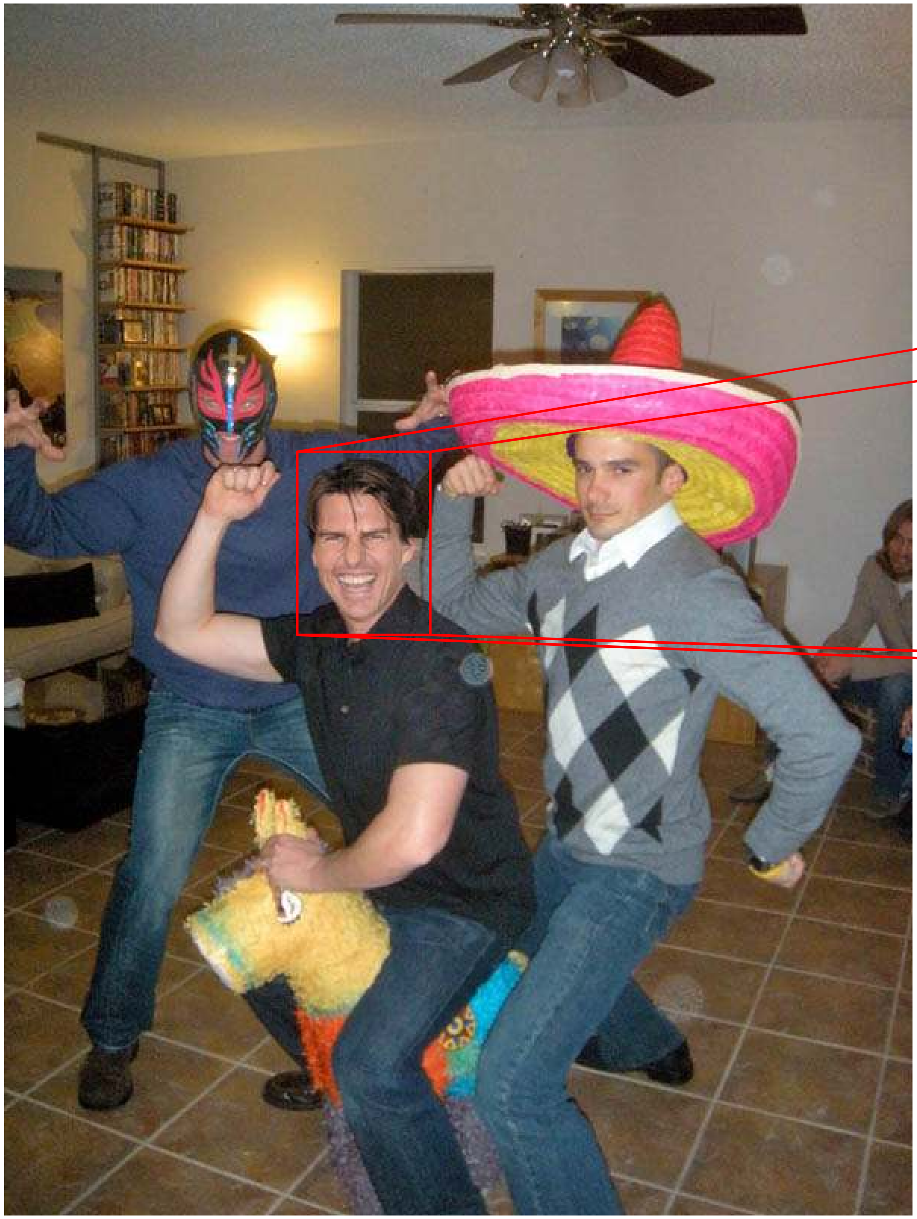
moscowtranslator.ru/.../окружите-себя-хо... ▾ Translate this page

275 × 183 - May 6, 2014 - Вы – те люди, с которыми проводите большую часть времени. Пугает, правда? В конце концов, сколько из нас мирится с мертвым ....

Ladies' man - Maurice is surrounded by girls! Is this what he's like on the show? You'll have to tune in next Friday 22 Jan at 21h30 on SABC 3 to find out.

saltbushgroup

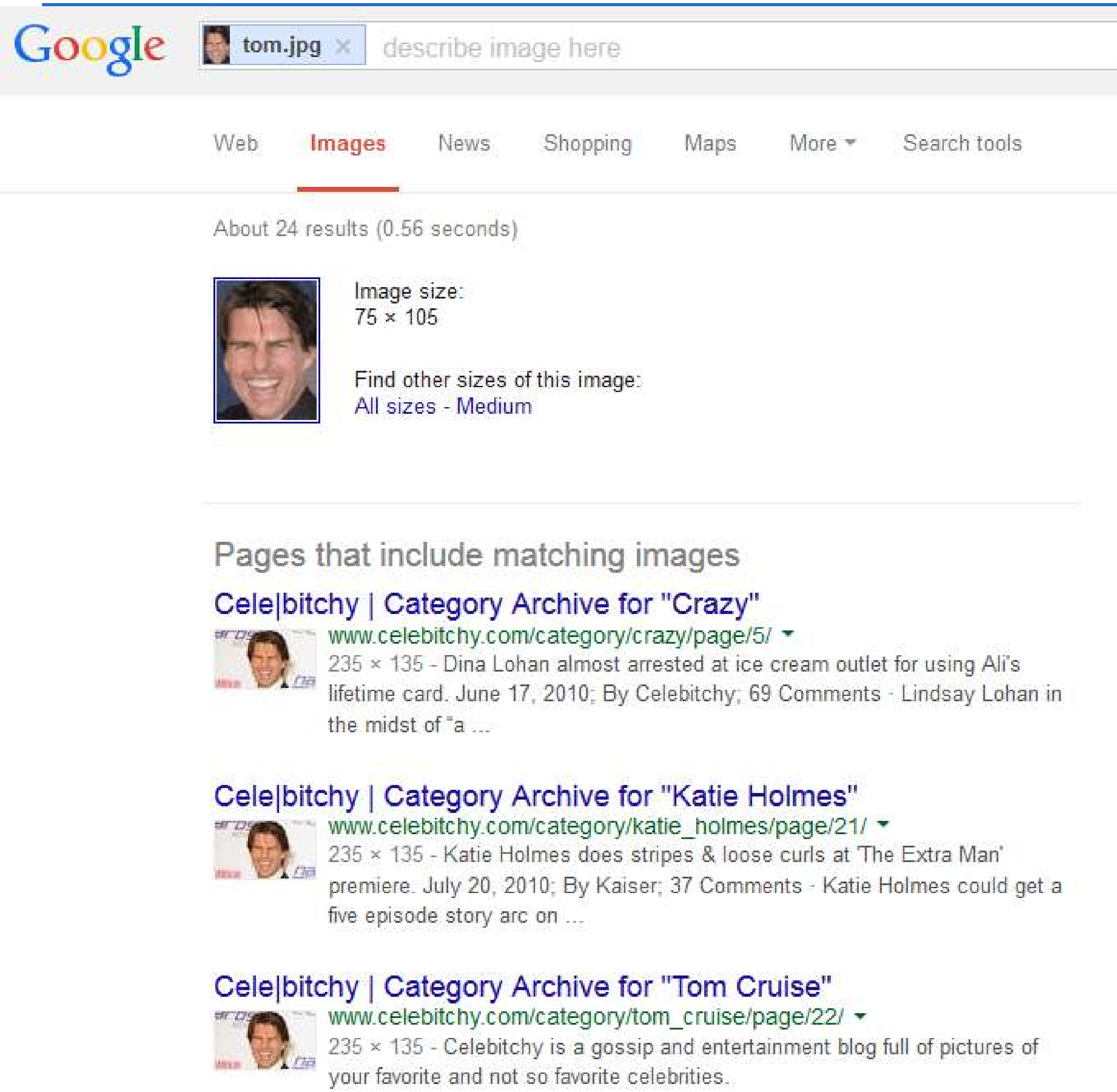
Technique – Look for the Original



When you suspect that a small part of the image may be on the Internet somewhere…

Crop

Technique – Look for the Original



About 24 results (0.56 seconds)

Image size:
75 × 105

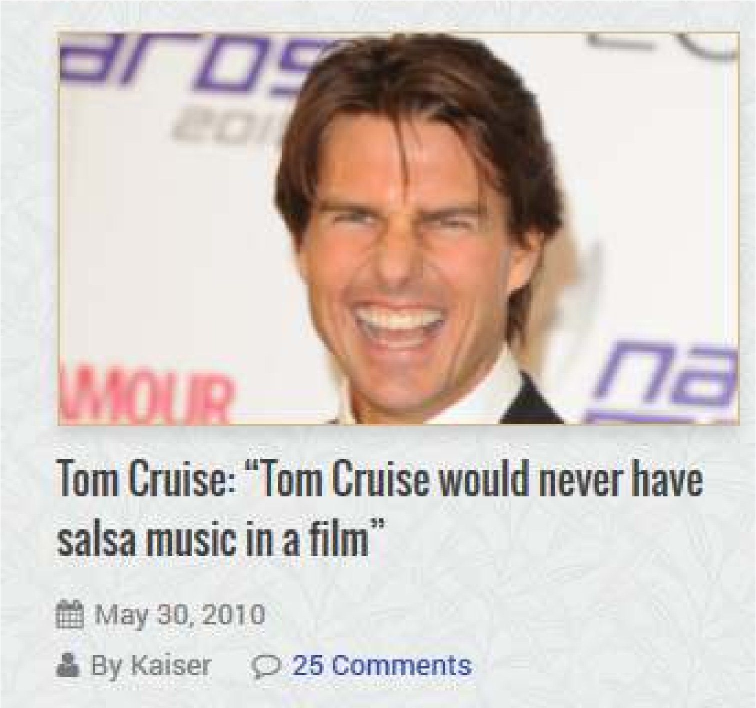
Find other sizes of this image:
All sizes - Medium

Pages that include matching images

Cele|bitchy | Category Archive for "Crazy"
www.celebitchy.com/category/crazy/page/5/
235 × 135 - Dina Lohan almost arrested at ice cream outlet for using Ali's lifetime card. June 17, 2010; By Celebitchy; 69 Comments · Lindsay Lohan in the midst of "a ...

Cele|bitchy | Category Archive for "Katie Holmes"
www.celebitchy.com/category/katie_holmes/page/21/
235 × 135 - Katie Holmes does stripes & loose curls at 'The Extra Man' premiere. July 20, 2010; By Kaiser; 37 Comments · Katie Holmes could get a five episode story arc on ...

Cele|bitchy | Category Archive for "Tom Cruise"
www.celebitchy.com/category/tom_cruise/page/22/
235 × 135 - Celebitchy is a gossip and entertainment blog full of pictures of your favorite and not so favorite celebrities.



Tom Cruise: "Tom Cruise would never have salsa music in a film"

May 30, 2010

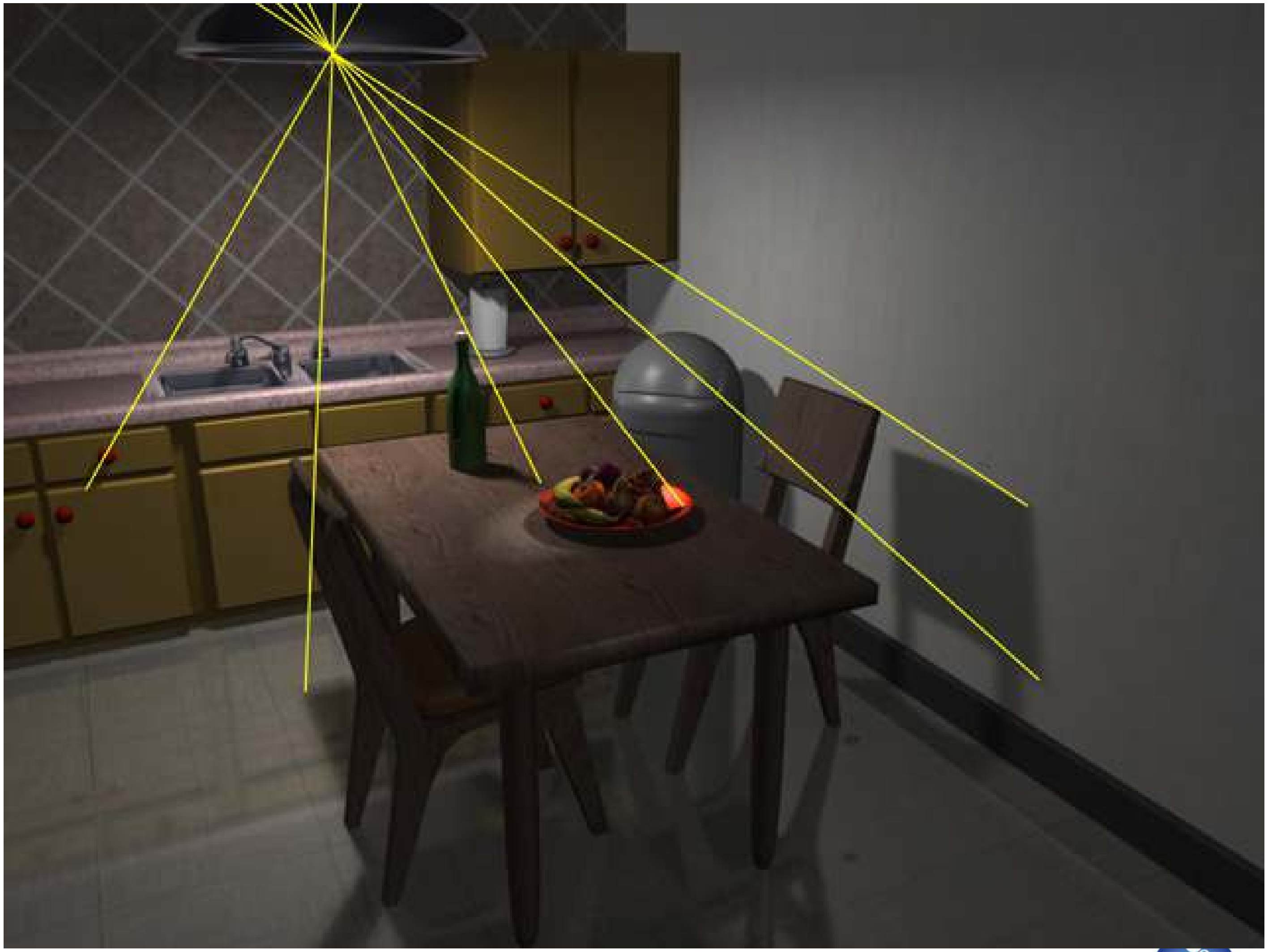
By Kaiser 25 Comments

saltbushgroup

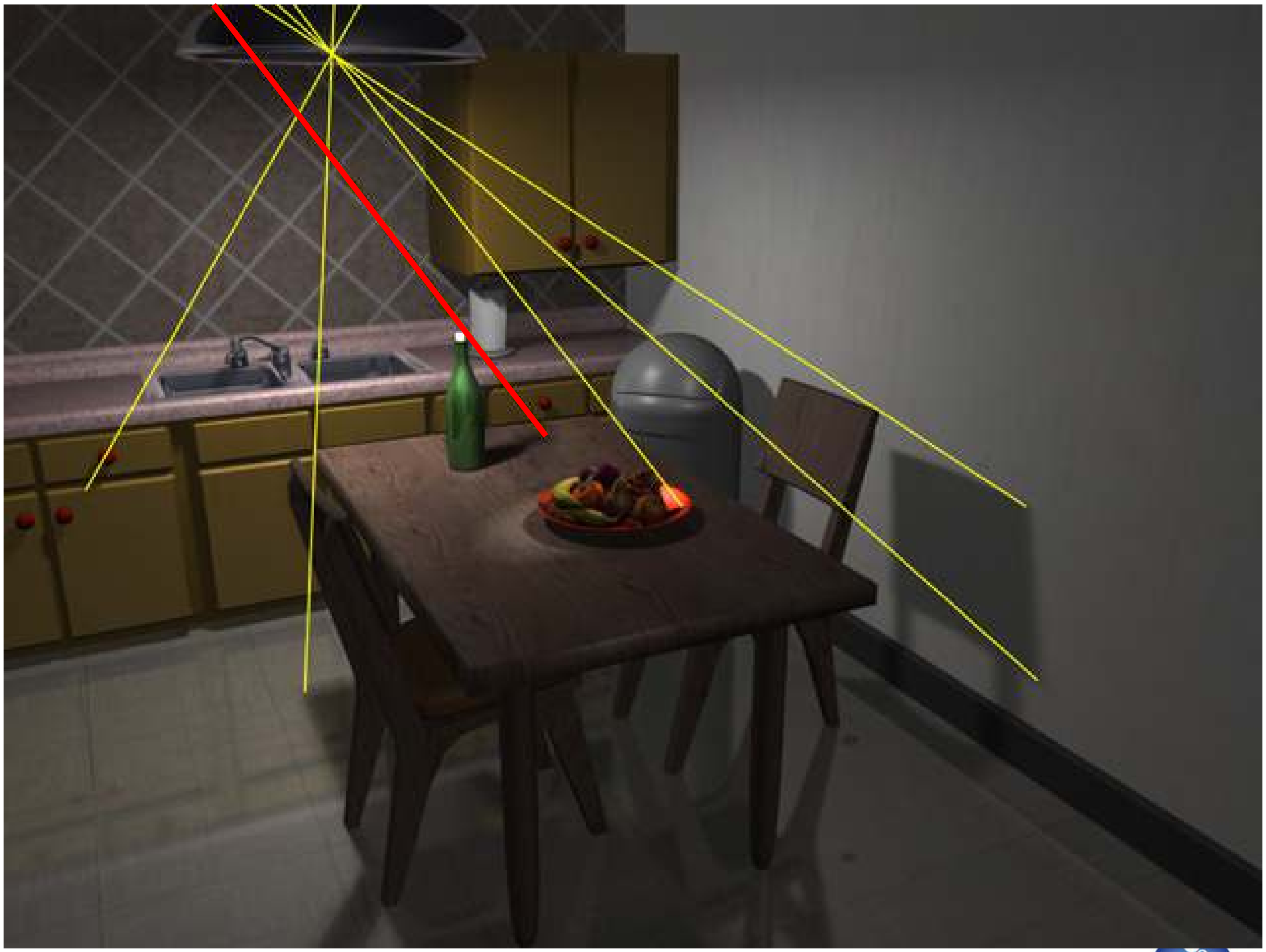
Technique – Shadows and Reflections

- Carefully analysing the position of light sources can reveal inconsistencies.
- This can be done by ray tracing objects and their shadows or reflections.

Technique – Shadows and Reflections

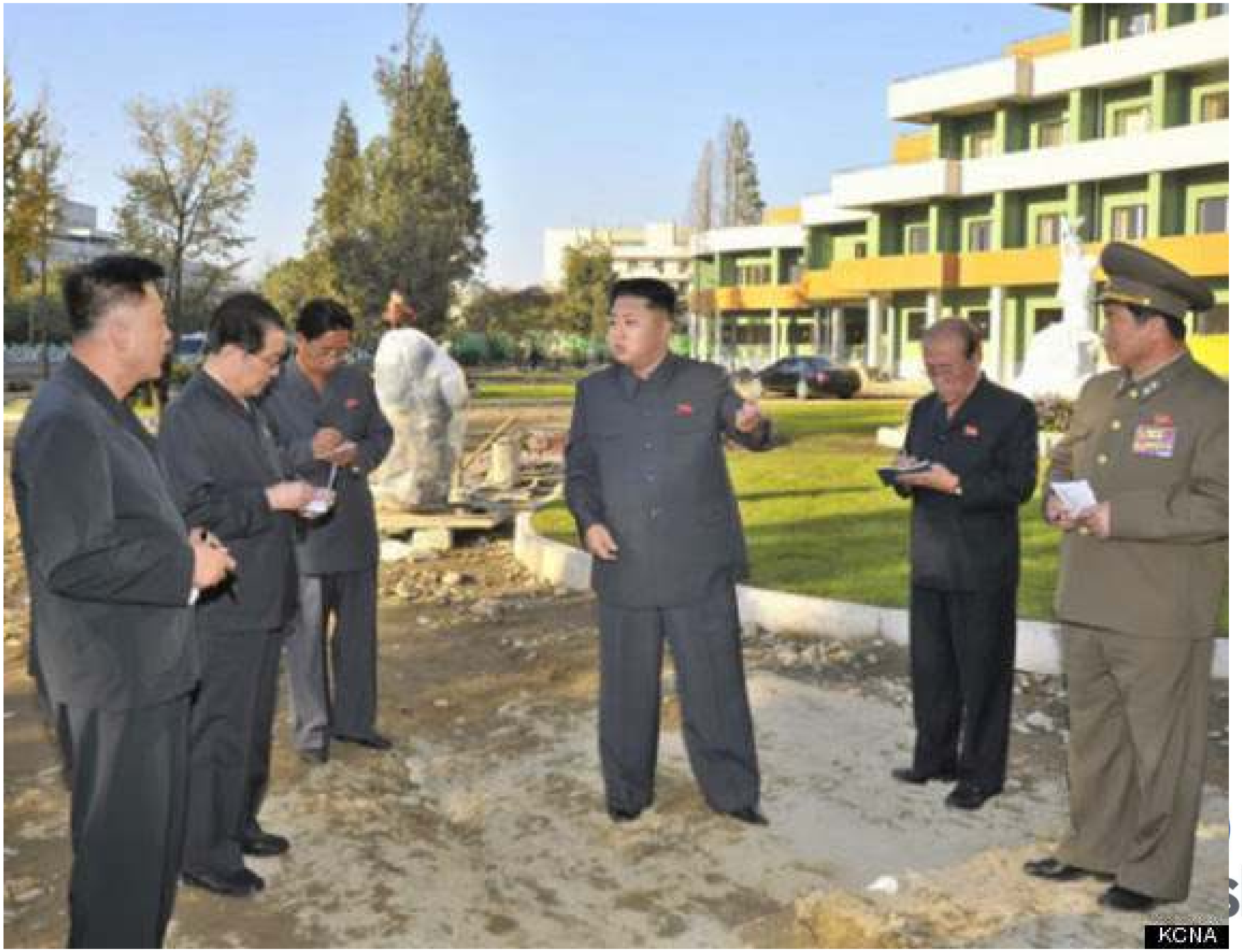


Technique – Shadows and Reflections

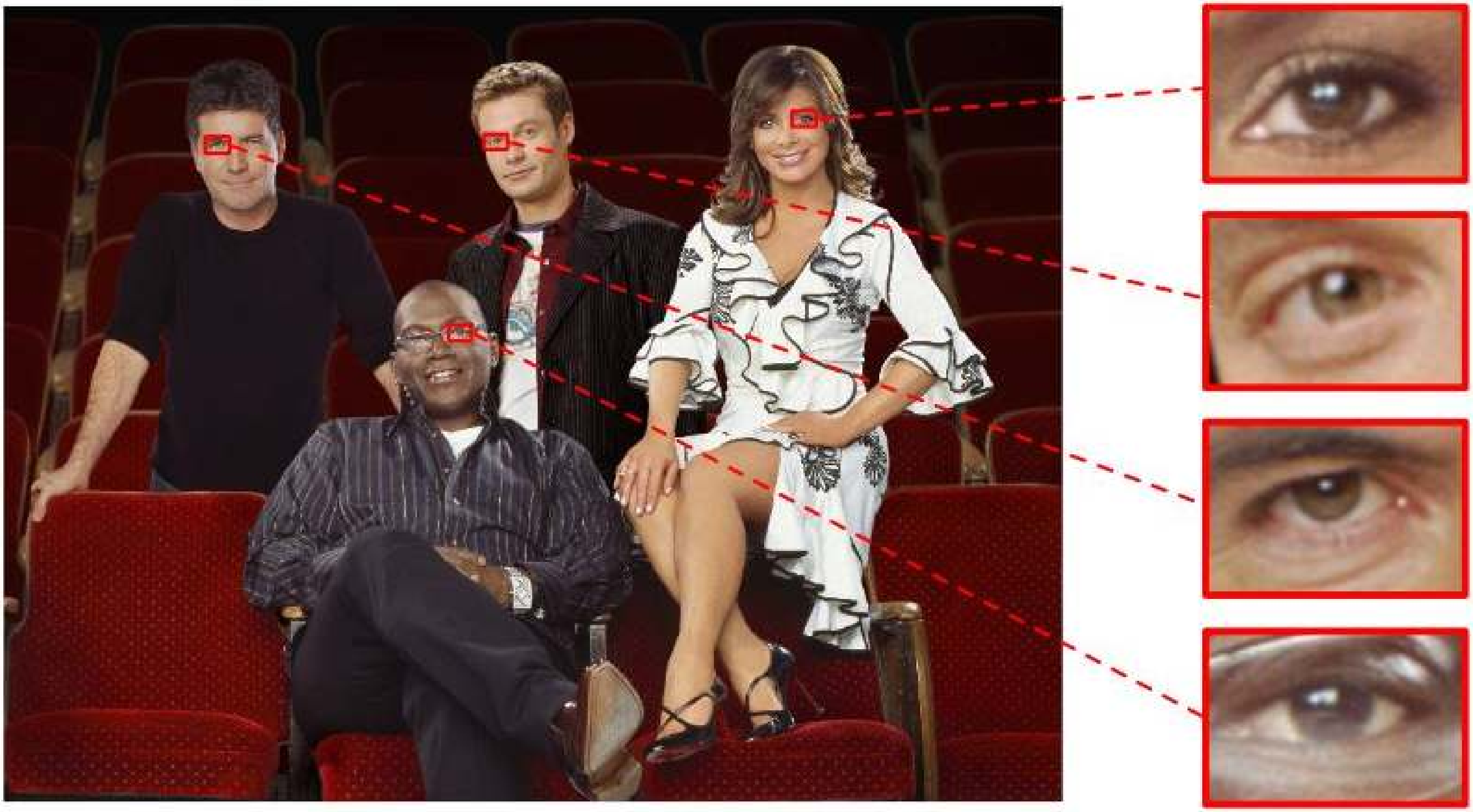


Technique – Shadows and Reflections

- The absence of shadows is a giveaway…



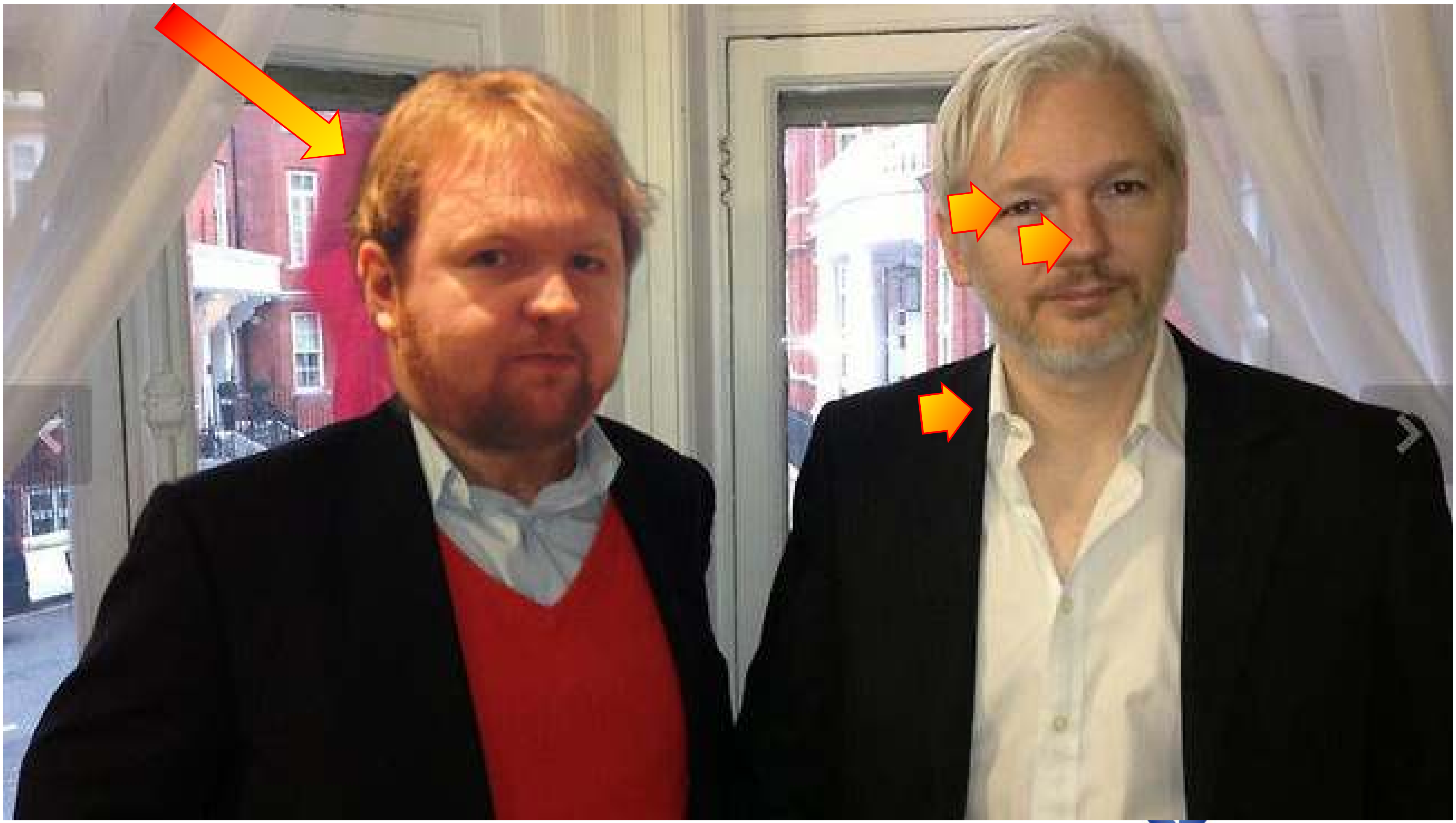
Technique – Shadows and Reflections



Technique – Shadows and Reflections

saltbushgroup

Technique – Shadows and Reflections



saltbushgroup

Technique – Look at the Metadata

- EXIF data can contain useful information such as the camera or software program that created the image.
- Compression schemes, Huffman tables, etc. can be used to fingerprint the camera or software program that created the image.

saltbushgroup

Technique – Look at the Metadata

saltbushgroup

Technique – Look at the Metadata

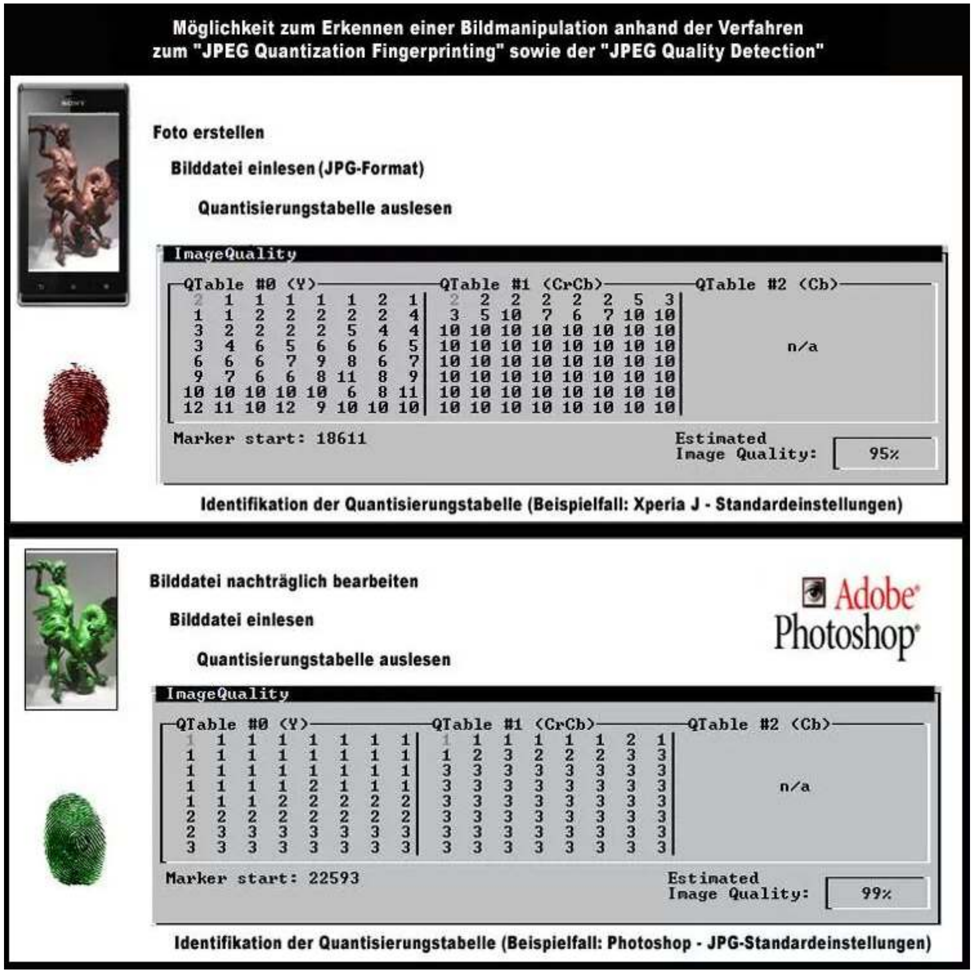
EXIF data

X Resolution	72
Y Resolution	72
Displayed Units X	inches
Photoshop Resolution 0x0003	2
Displayed Units Y	inches
Photoshop Resolution 0x0007	2
Global Angle	21
Global Altitude	39
Print Flags	(8 null bytes)%01
Copyright Flag	False
Print Flags Info	%00%01%00%00%00%00%00%00%00%02
Color Halftoning Info	(72 bytes binary data)
Color Transfer Funcs	(112 bytes binary data)
Layer State Info	%00%0c
Layers Group Info	(28 null bytes)
Grid Guides Info	%00%00%00%01%00%00%02@%00%00%02@%00%00%00%00
URL List	%00%00%00%00
Slices	(119 bytes binary data)
ICC Untagged	%01
IDs Base Value	%00%00%00%1f
Photoshop Thumbnail	(3,099 bytes binary data)
Version Info	Adobe Photoshop Adobe Photoshop 6.0
Photoshop Quality	9
Photoshop Format	Optimised
Progressive Scans	3 Scans

saltbushgroup

Technique – Look at the Metadata

- Quantisation matrices and Huffman tables can be used to fingerprint the image creator.



Möglichkeit zum Erkennen einer Bildmanipulation anhand der Verfahren
zum "JPEG Quantization Fingerprinting" sowie der "JPEG Quality Detection"

Foto erstellen

Bilddatei einlesen (JPG-Format)

Quantisierungstabelle auslesen

```
ImageQuality
┌QTable #0 (Y)─────────────────────QTable #1 (CrCb)────────────────QTable #2 (Cb)──────
  2  1  1  1  1  1  2  1 |  2  2  2  2  2  2  5  3 |
  1  1  2  2  2  2  2  4 |  3  5 10  7  6  7 10 10 |
  3  2  2  2  2  5  4  4 | 10 10 10 10 10 10 10 10 |
  3  4  6  5  6  6  6  5 | 10 10 10 10 10 10 10 10 |         n/a
  6  6  6  7  9  8  6  7 | 10 10 10 10 10 10 10 10 |
  9  7  6  6  8 11  8  9 | 10 10 10 10 10 10 10 10 |
 10 10 10 10 10  6  8 11 | 10 10 10 10 10 10 10 10 |
 12 11 10 12  9 10 10 10 | 10 10 10 10 10 10 10 10 |
Marker start: 18611                                   Estimated
                                                      Image Quality:   95%
```

Identifikation der Quantisierungstabelle (Beispielfall: Xperia J - Standardeinstellungen)

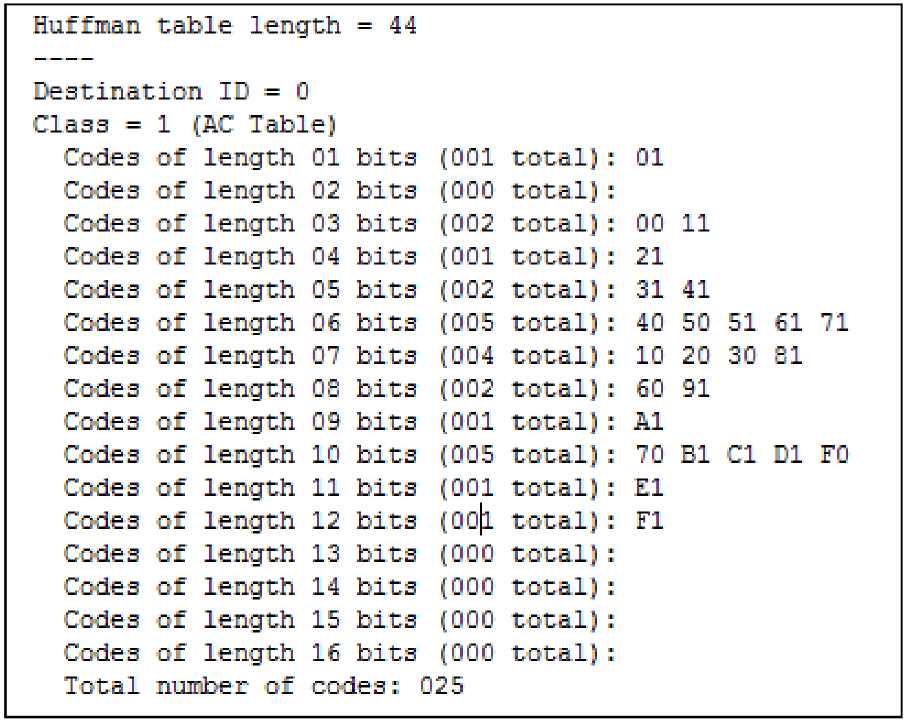
Bilddatei nachträglich bearbeiten

Bilddatei einlesen

Quantisierungstabelle auslesen

```
ImageQuality
┌QTable #0 (Y)─────────────────────QTable #1 (CrCb)────────────────QTable #2 (Cb)──────
  1  1  1  1  1  1  1  1 |  1  1  1  1  1  1  2  1 |
  1  1  1  1  1  1  1  1 |  1  2  3  2  2  2  3  3 |
  1  1  1  1  1  1  1  1 |  3  3  3  3  3  3  3  3 |
  1  1  1  1  2  1  1  1 |  3  3  3  3  3  3  3  3 |         n/a
  1  1  1  2  2  2  2  2 |  3  3  3  3  3  3  3  3 |
  2  2  2  2  2  2  2  2 |  3  3  3  3  3  3  3  3 |
  2  3  3  3  3  3  3  3 |  3  3  3  3  3  3  3  3 |
  3  3  3  3  3  3  3  3 |  3  3  3  3  3  3  3  3 |
Marker start: 22593                                   Estimated
                                                      Image Quality:   99%
```

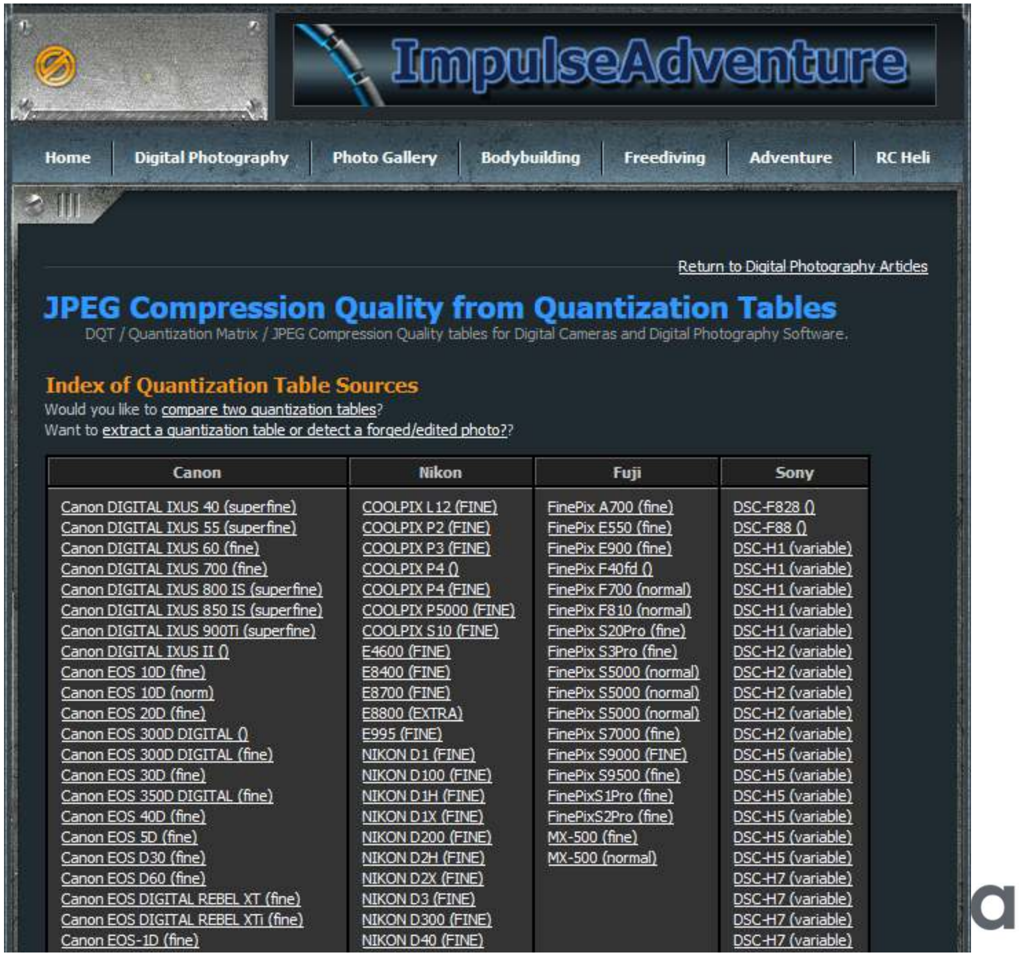
Identifikation der Quantisierungstabelle (Beispielfall: Photoshop - JPG-Standardeinstellungen)



```
Huffman table length = 44
----
Destination ID = 0
Class = 1 (AC Table)
  Codes of length 01 bits (001 total): 01
  Codes of length 02 bits (000 total):
  Codes of length 03 bits (002 total): 00 11
  Codes of length 04 bits (001 total): 21
  Codes of length 05 bits (002 total): 31 41
  Codes of length 06 bits (005 total): 40 50 51 61 71
  Codes of length 07 bits (004 total): 10 20 30 81
  Codes of length 08 bits (002 total): 60 91
  Codes of length 09 bits (001 total): A1
  Codes of length 10 bits (005 total): 70 B1 C1 D1 F0
  Codes of length 11 bits (001 total): E1
  Codes of length 12 bits (001 total): F1
  Codes of length 13 bits (000 total):
  Codes of length 14 bits (000 total):
  Codes of length 15 bits (000 total):
  Codes of length 16 bits (000 total):
  Total number of codes: 025
```

Technique – Look at the Metadata

- ImpulseAdventure.com has a large list of quantisation tables.



JPEG Compression Quality from Quantization Tables

DQT / Quantization Matrix / JPEG Compression Quality tables for Digital Cameras and Digital Photography Software.

Index of Quantization Table Sources

Would you like to compare two quantization tables?

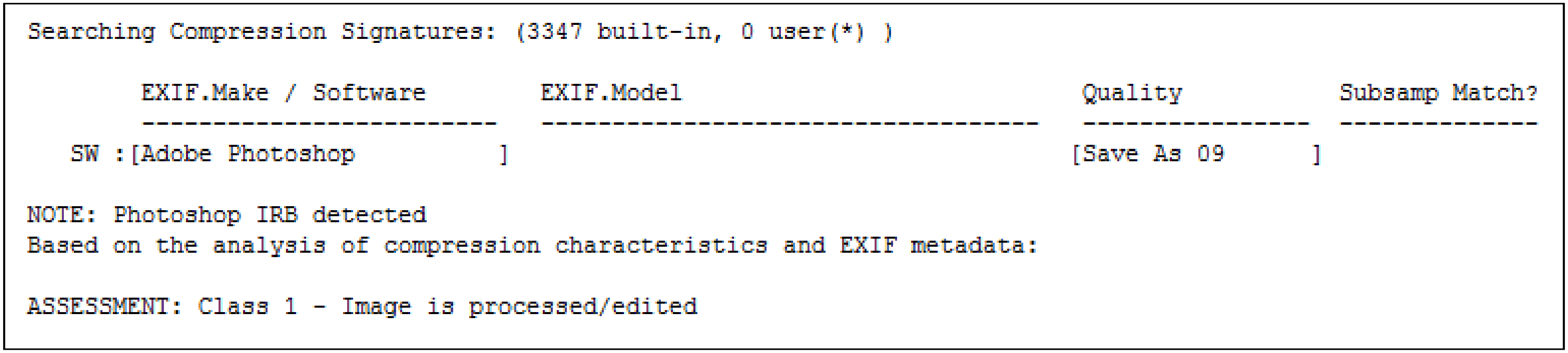
Want to extract a quantization table or detect a forged/edited photo??

Canon	Nikon	Fuji	Sony
Canon DIGITAL IXUS 40 (superfine)	COOLPIX L12 (FINE)	FinePix A700 (fine)	DSC-F828 ()
Canon DIGITAL IXUS 55 (superfine)	COOLPIX P2 (FINE)	FinePix E550 (fine)	DSC-F88 ()
Canon DIGITAL IXUS 60 (fine)	COOLPIX P3 (FINE)	FinePix E900 (fine)	DSC-H1 (variable)
Canon DIGITAL IXUS 700 (fine)	COOLPIX P4 ()	FinePix F40fd ()	DSC-H1 (variable)
Canon DIGITAL IXUS 800 IS (superfine)	COOLPIX P4 (FINE)	FinePix F700 (normal)	DSC-H1 (variable)
Canon DIGITAL IXUS 850 IS (superfine)	COOLPIX P5000 (FINE)	FinePix F810 (normal)	DSC-H1 (variable)
Canon DIGITAL IXUS 900Ti (superfine)	COOLPIX S10 (FINE)	FinePix S20Pro (fine)	DSC-H1 (variable)
Canon DIGITAL IXUS II ()	E4600 (FINE)	FinePix S3Pro (fine)	DSC-H2 (variable)
Canon EOS 10D (fine)	E8400 (FINE)	FinePix S5000 (normal)	DSC-H2 (variable)
Canon EOS 10D (norm)	E8700 (FINE)	FinePix S5000 (normal)	DSC-H2 (variable)
Canon EOS 20D (fine)	E8800 (EXTRA)	FinePix S5000 (normal)	DSC-H2 (variable)
Canon EOS 300D DIGITAL ()	E995 (FINE)	FinePix S7000 (fine)	DSC-H2 (variable)
Canon EOS 300D DIGITAL (fine)	NIKON D1 (FINE)	FinePix S9000 (FINE)	DSC-H5 (variable)
Canon EOS 30D (fine)	NIKON D100 (FINE)	FinePix S9500 (fine)	DSC-H5 (variable)
Canon EOS 350D DIGITAL (fine)	NIKON D1H (FINE)	FinePixS1Pro (fine)	DSC-H5 (variable)
Canon EOS 40D (fine)	NIKON D1X (FINE)	FinePixS2Pro (fine)	DSC-H5 (variable)
Canon EOS 5D (fine)	NIKON D200 (FINE)	MX-500 (fine)	DSC-H5 (variable)
Canon EOS D30 (fine)	NIKON D2H (FINE)	MX-500 (normal)	DSC-H5 (variable)
Canon EOS D60 (fine)	NIKON D2X (FINE)		DSC-H7 (variable)
Canon EOS DIGITAL REBEL XT (fine)	NIKON D3 (FINE)		DSC-H7 (variable)
Canon EOS DIGITAL REBEL XTi (fine)	NIKON D300 (FINE)		DSC-H7 (variable)
Canon EOS-1D (fine)	NIKON D40 (FINE)		DSC-H7 (variable)

altbushgroup

Technique – Look at the Metadata

- “jpegsnoop” uses EXIF data, quantisation matrices, Huffman tables (and more?) to assess what created the image.



```
Searching Compression Signatures: (3347 built-in, 0 user(*) )

        EXIF.Make / Software        EXIF.Model                            Quality           Subsamp Match?
        -------------------------   -----------------------------------   ----------------  --------------
   SW :[Adobe Photoshop          ]                                       [Save As 09      ]

NOTE: Photoshop IRB detected
Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited
```

Technique – Look at the Metadata

- At Blackhat 2014, Dominique Bongard showed that web application platforms can be fingerprinted through their underlying image libraries. Tool: Fingerping[1]

```
$ python fingerping.py www.site.com/
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
```

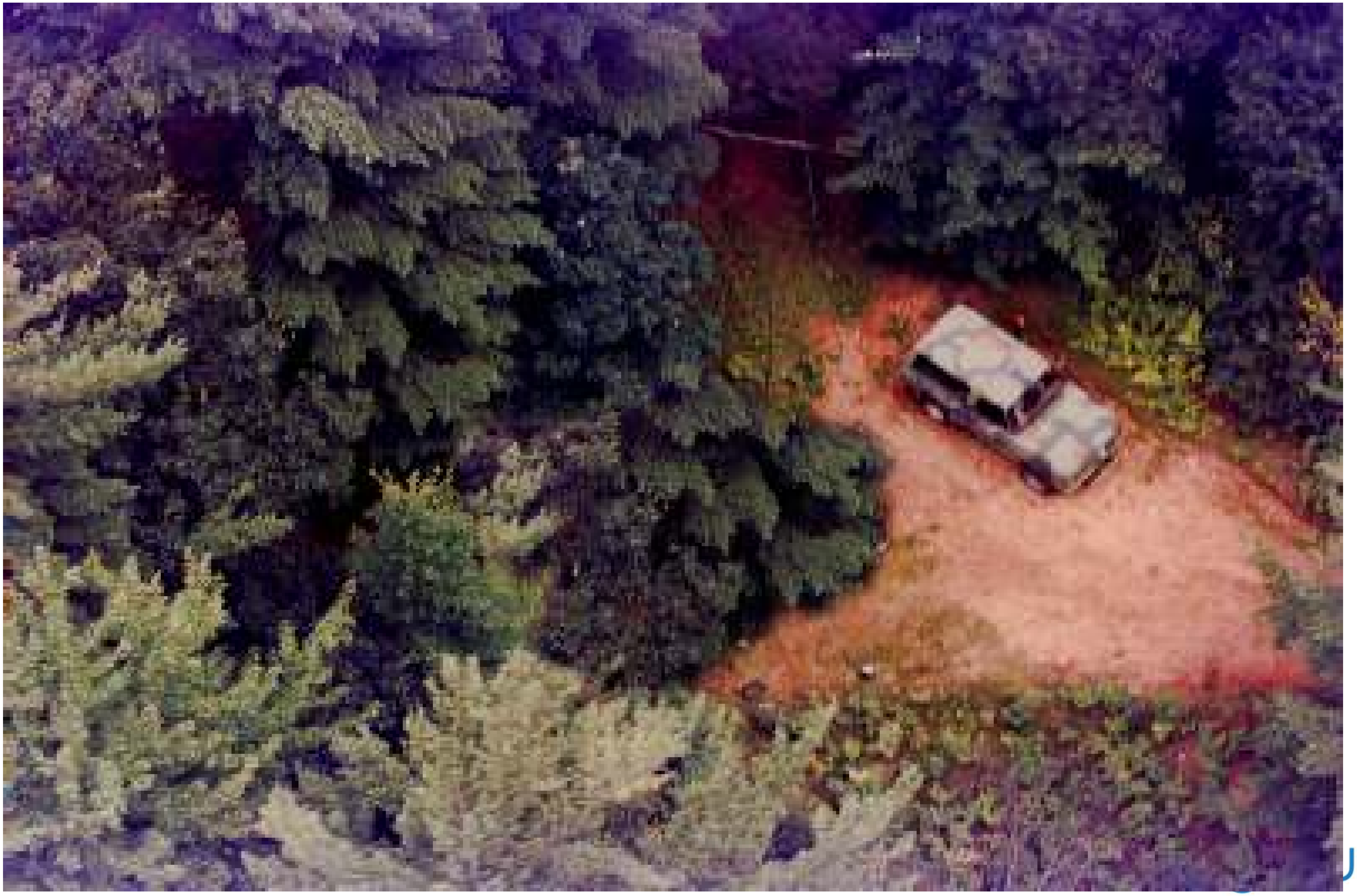
From this, we can deduce that www.site.com is most likely a PHP site.

[1] https://github.com/0xcite/fingerping

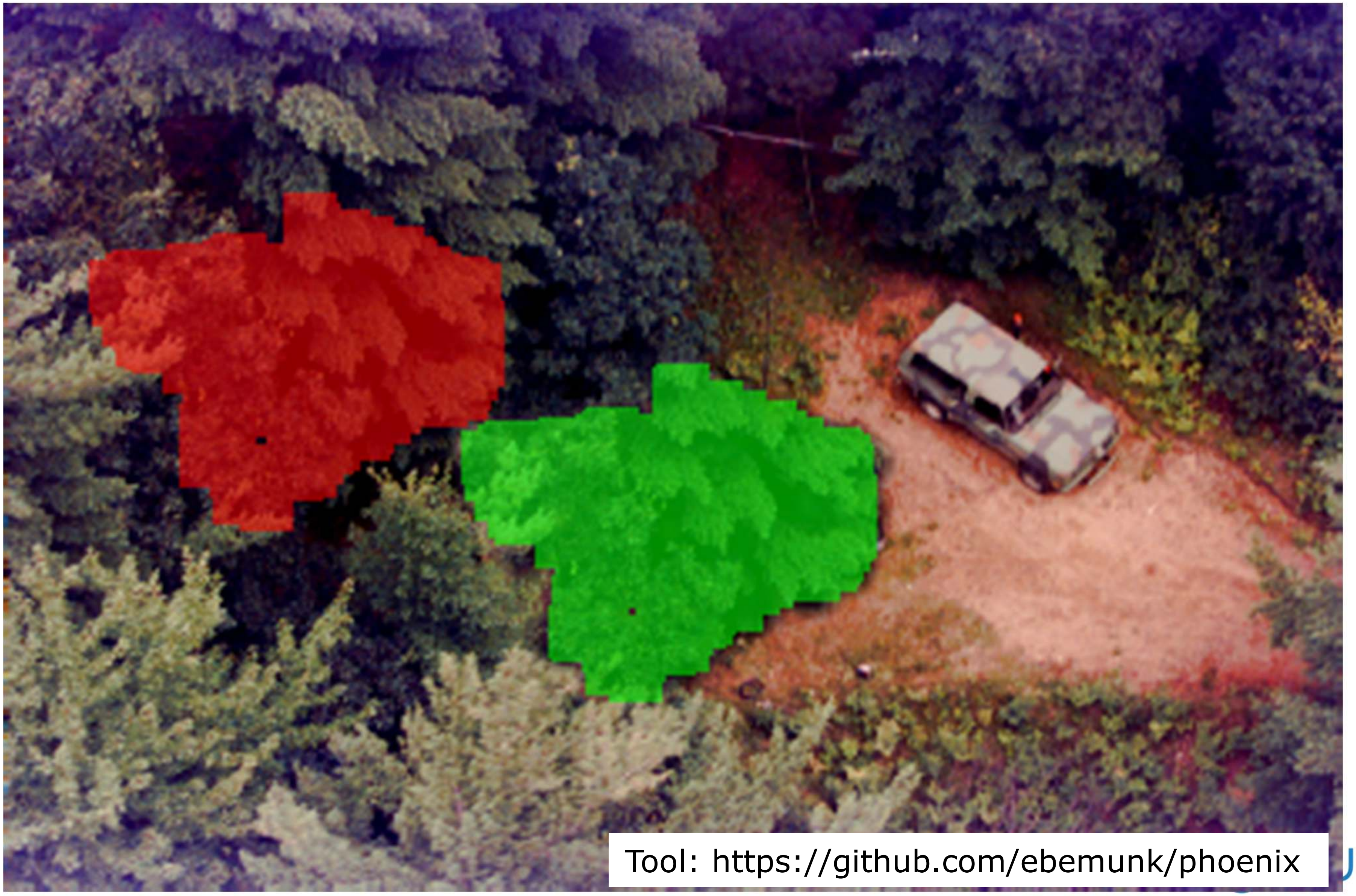
Technique – Clone Detection

- Find areas in the image that have been copied and pasted into other areas of the image.
  - This can be done automatically.
- The Photoshop “clone” tool is often used to hide parts of an image.

Technique – Clone Detection

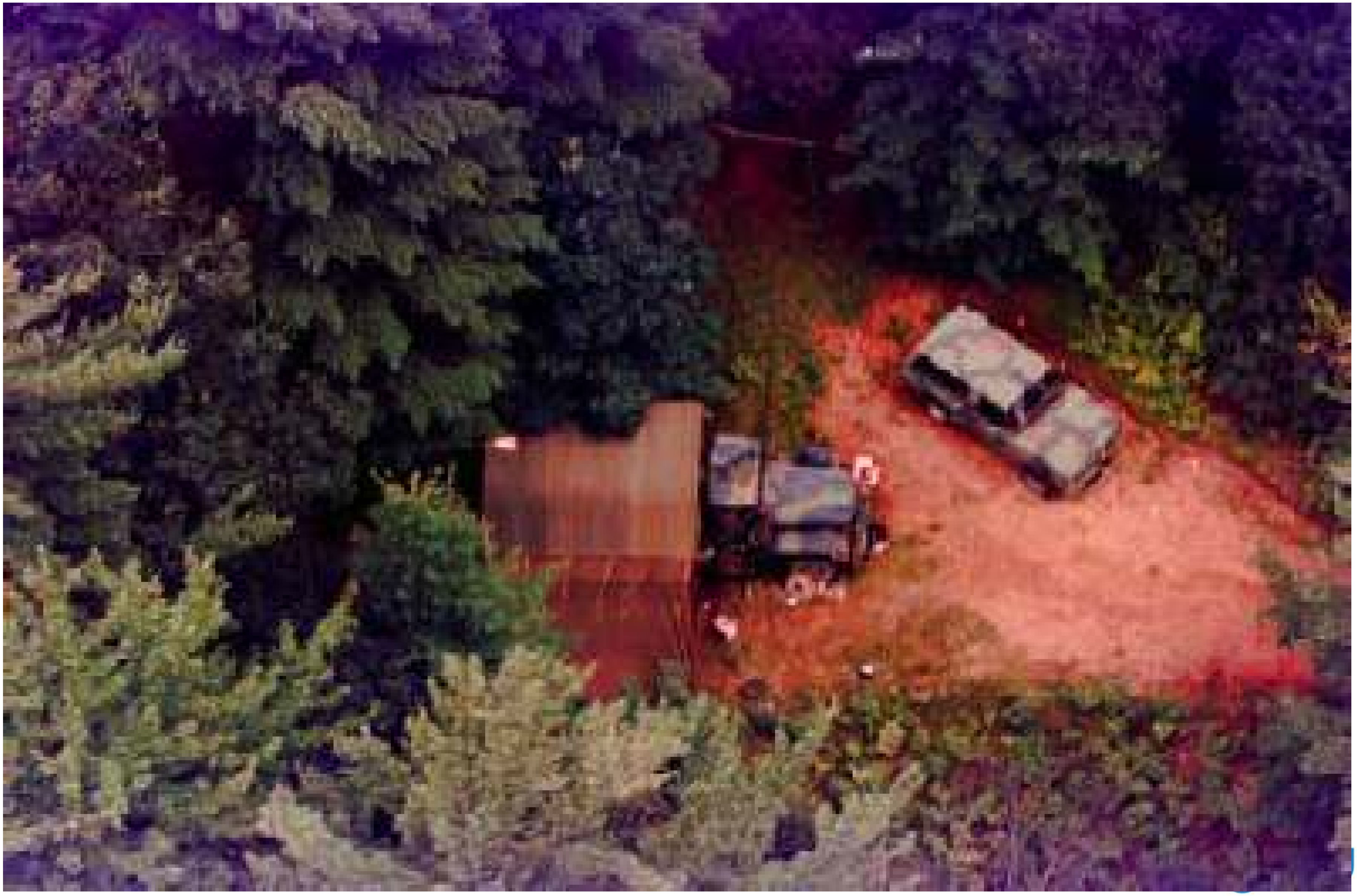


Technique – Clone Detection



Tool: https://github.com/ebemunk/phoenix

Technique – Clone Detection



Technique – Clone Detection

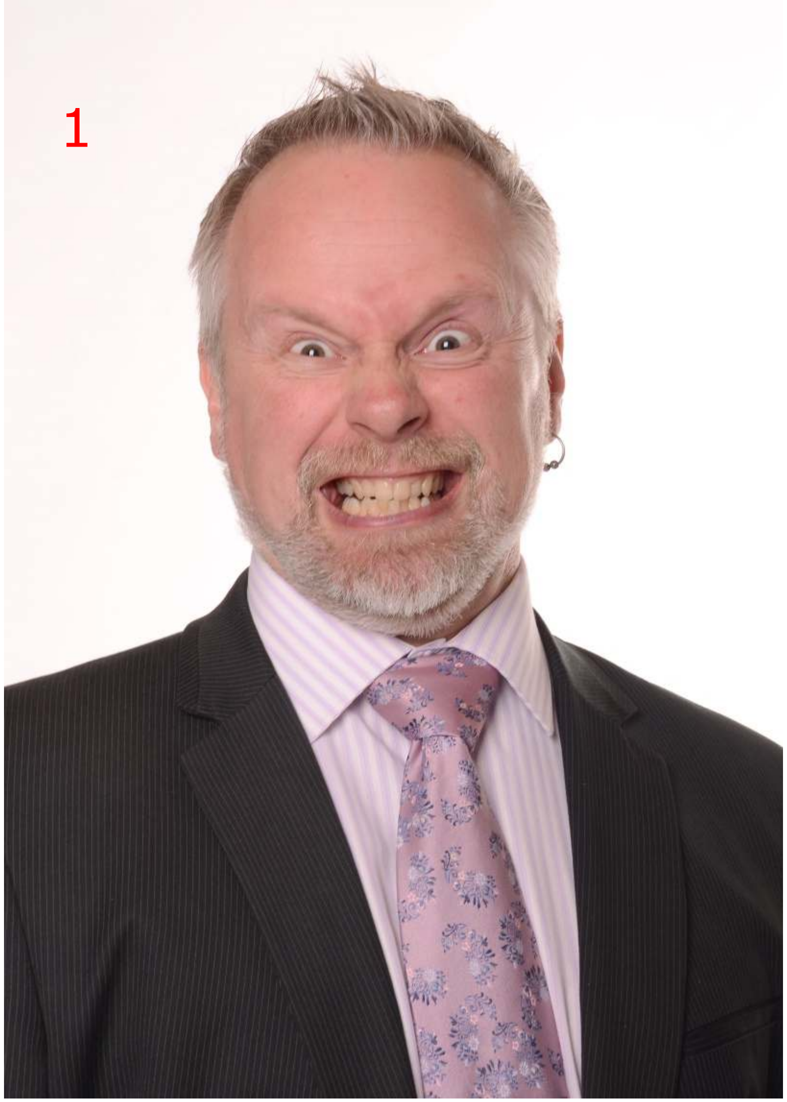
Technique – Clone Detection

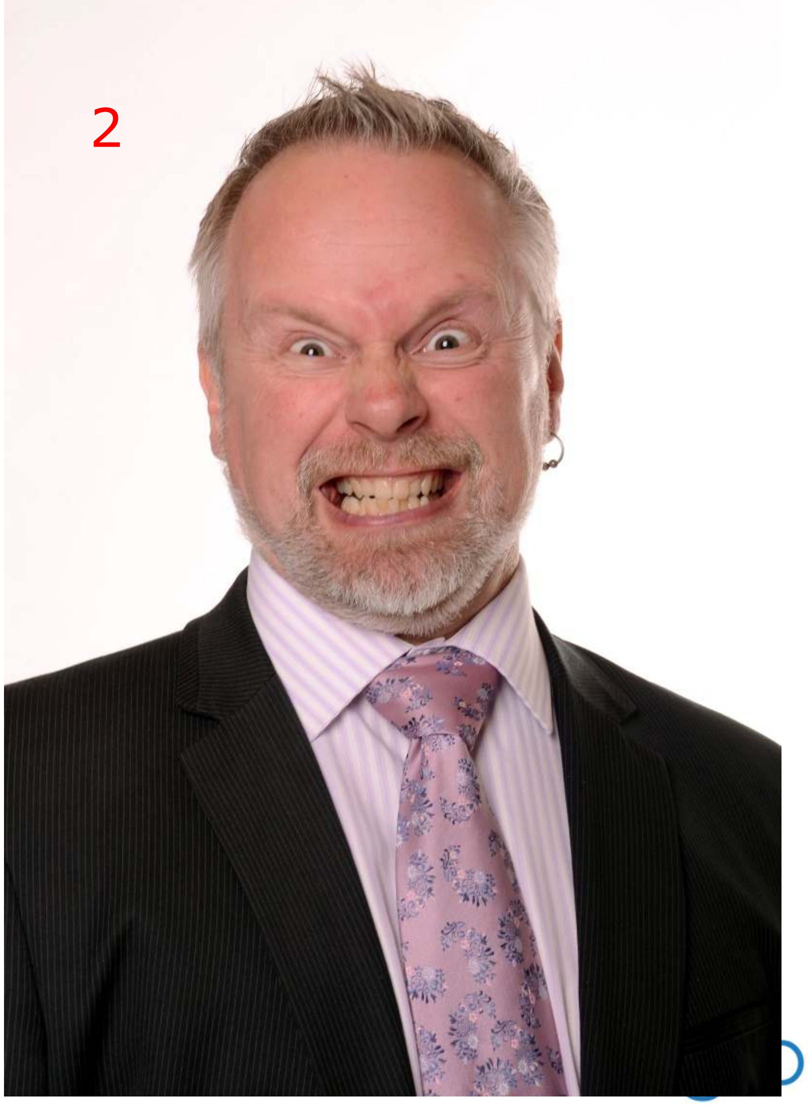
Technique – Histogram Analysis

- Useful for detecting colour manipulation (which is common).

Technique – Histogram Analysis

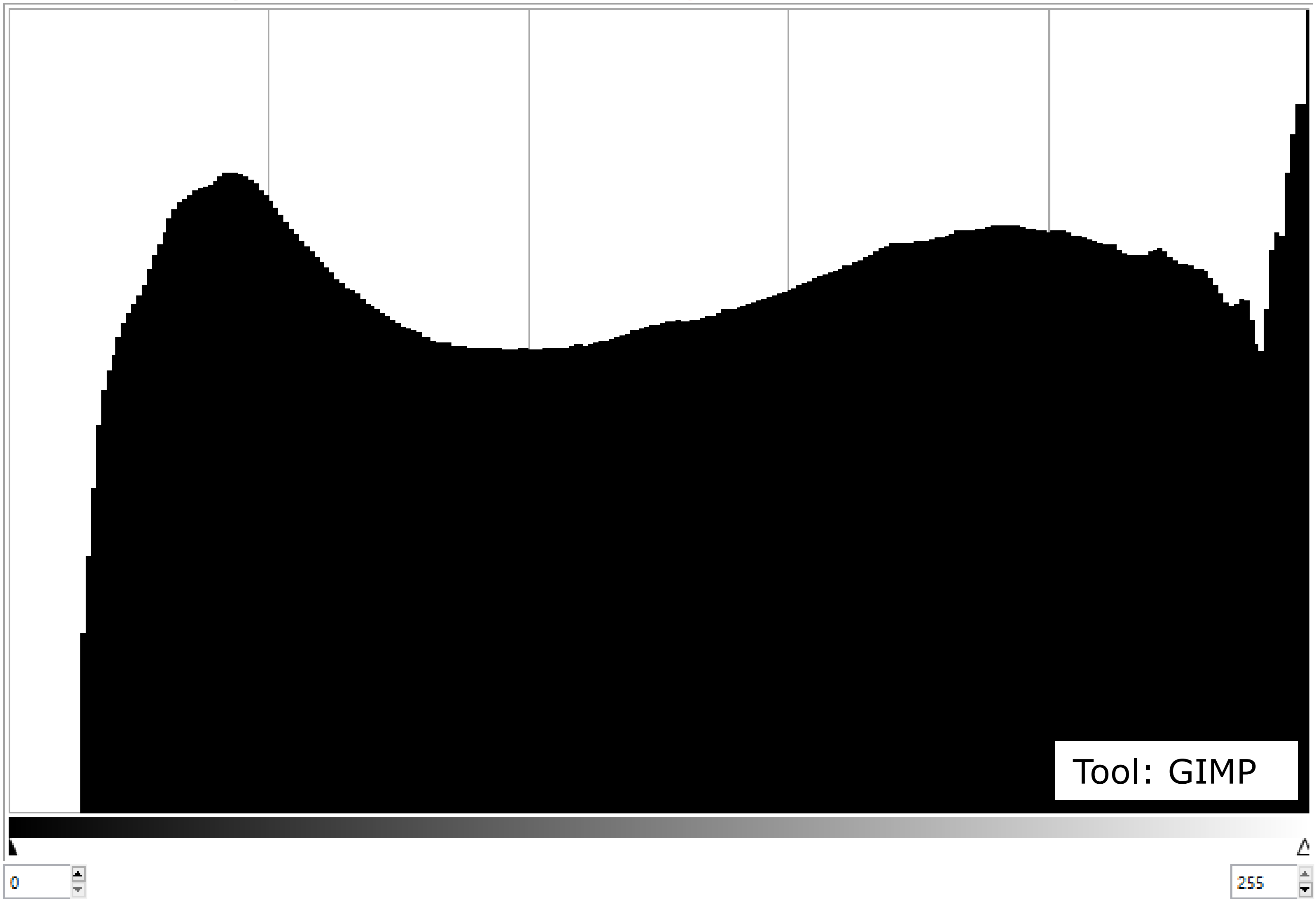
Which is the original?


1


2

Technique – Histogram Analysis

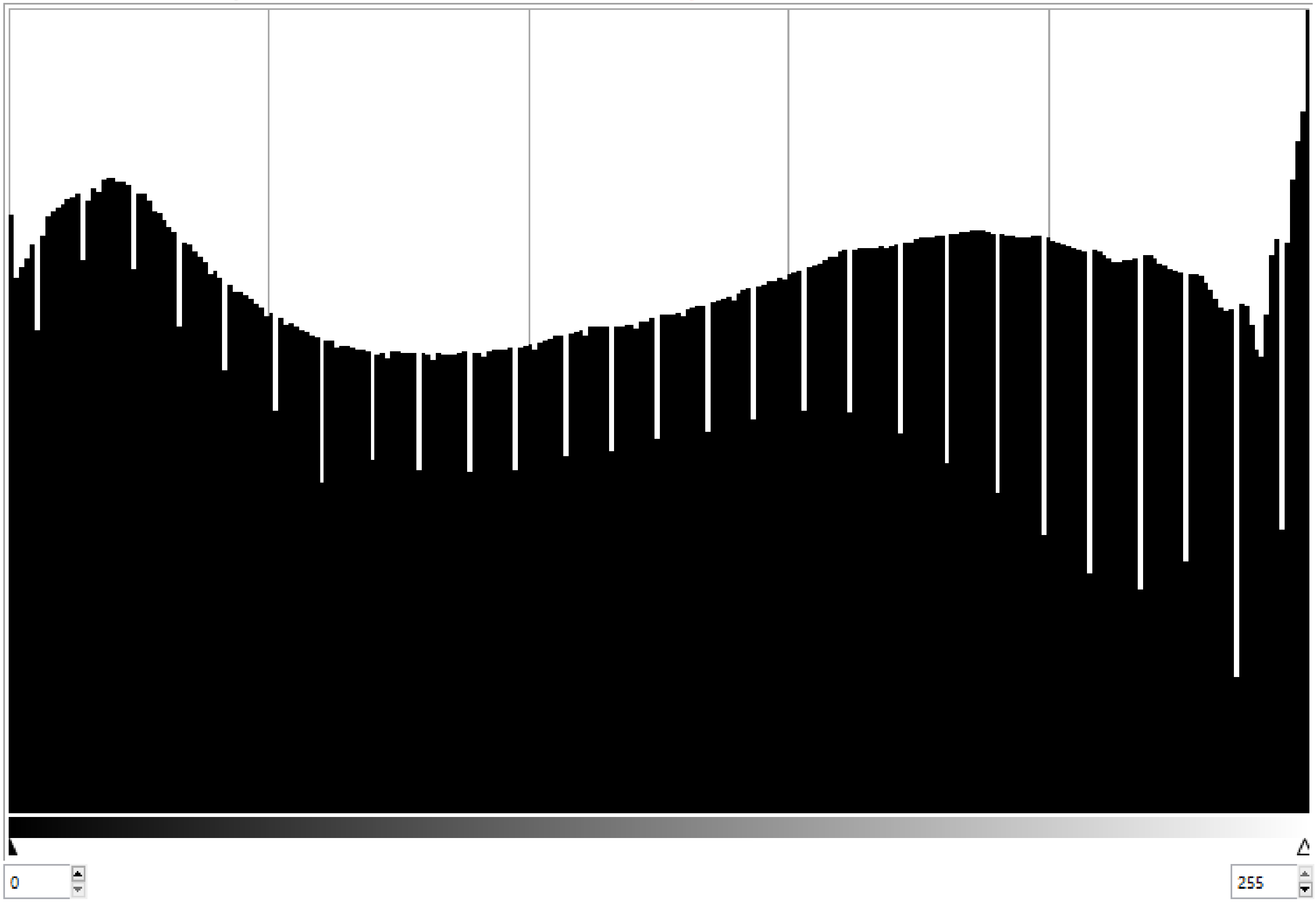
The Histogram for Image 1:



Tool: GIMP

Technique – Histogram Analysis

The Histogram for Image 2:

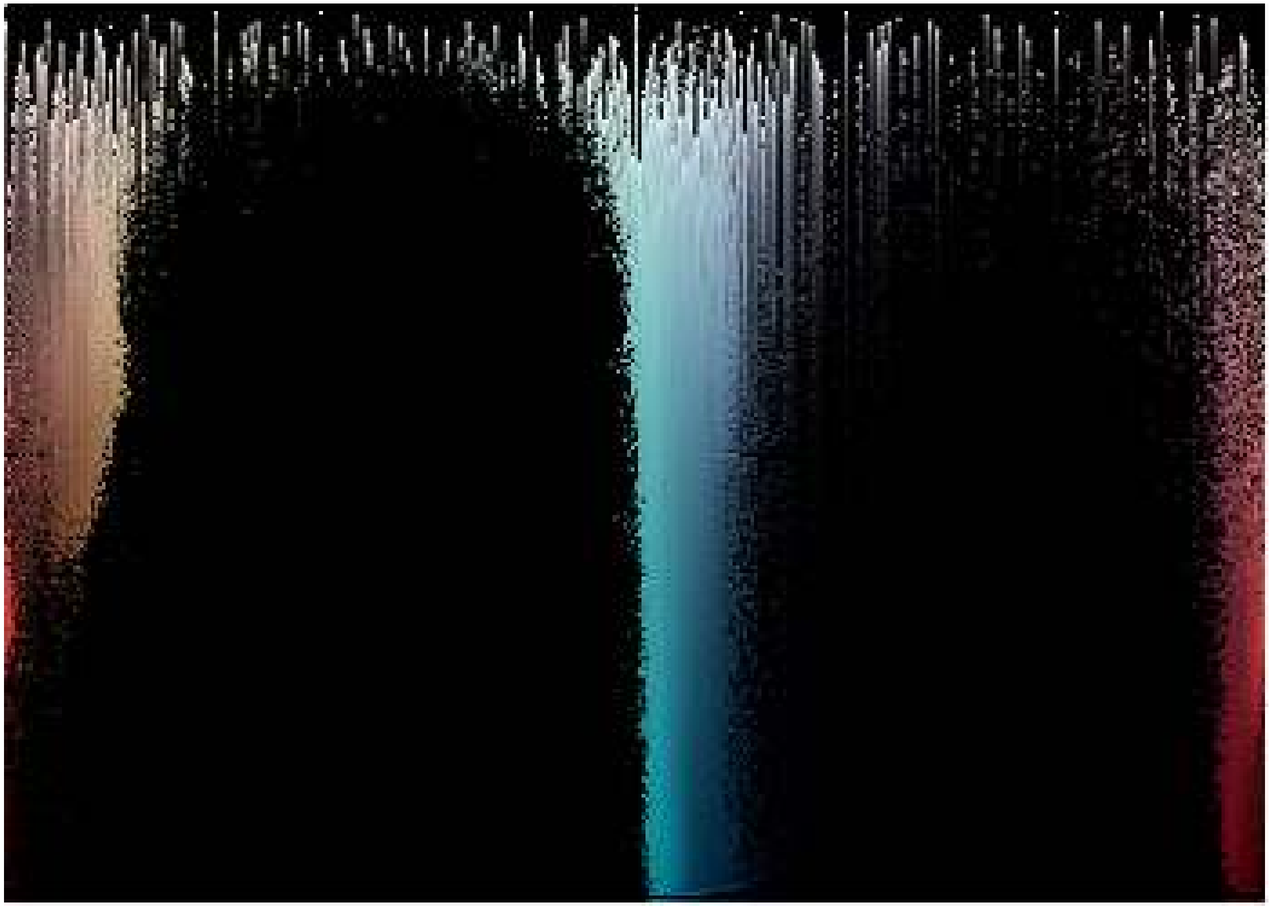


oup

Technique – Histogram Analysis

Technique – Histogram Analysis

- HSV Histogram

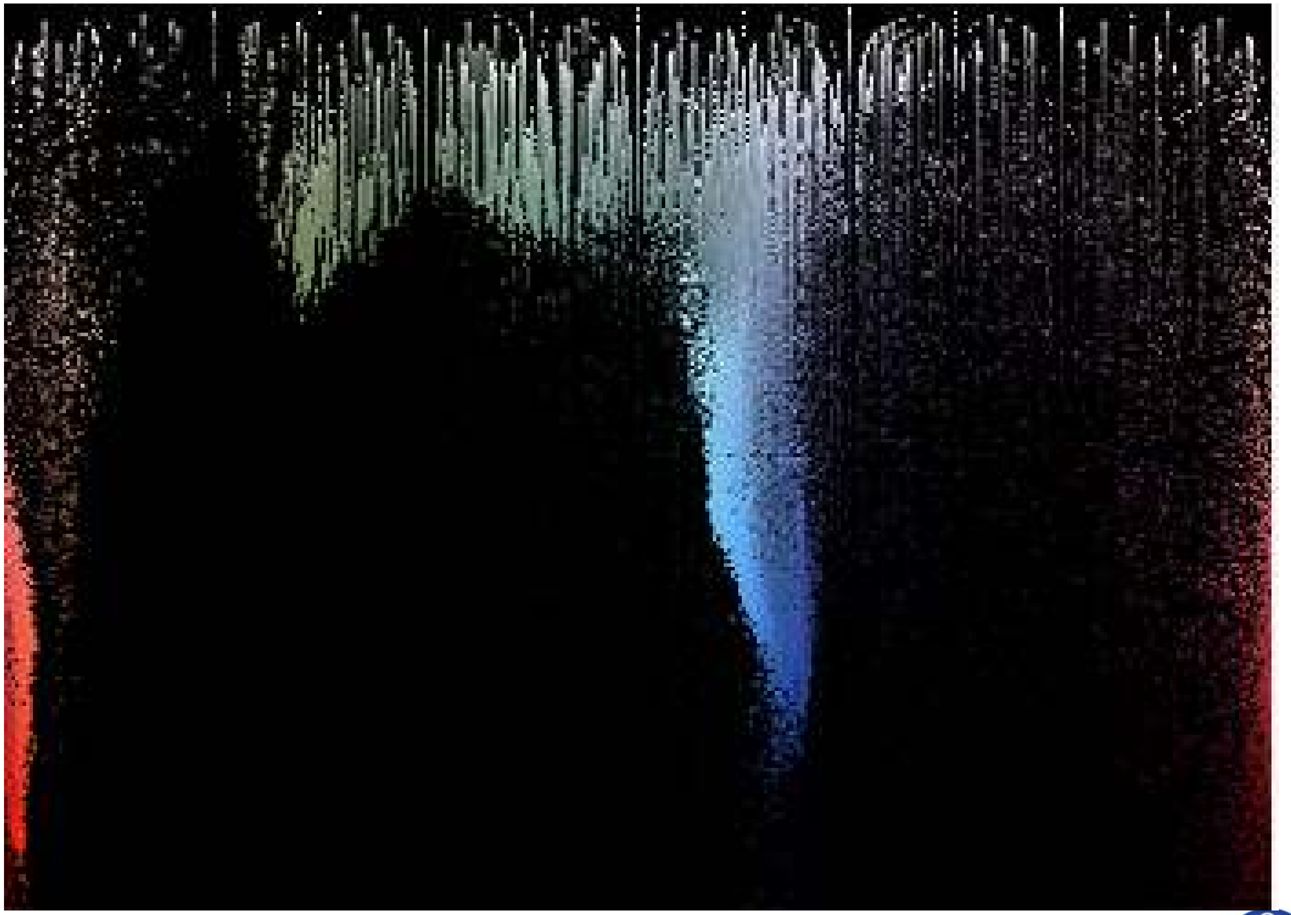


Tool: https://github.com/ebemunk/phoenix

Technique – Histogram Analysis

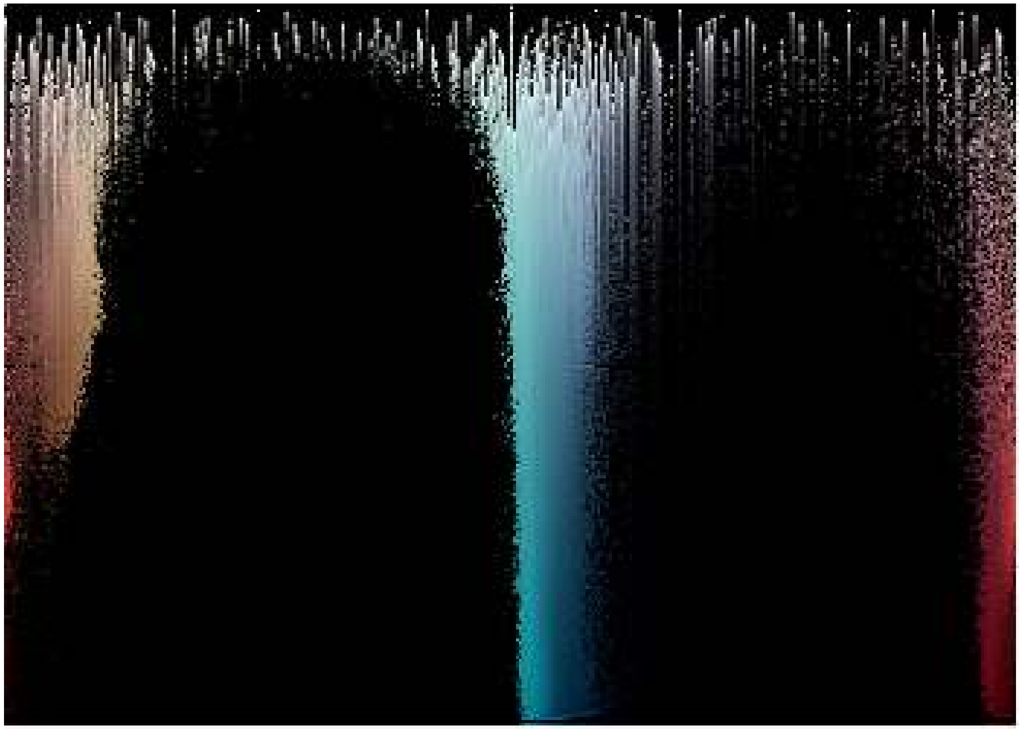
Technique – Histogram Analysis

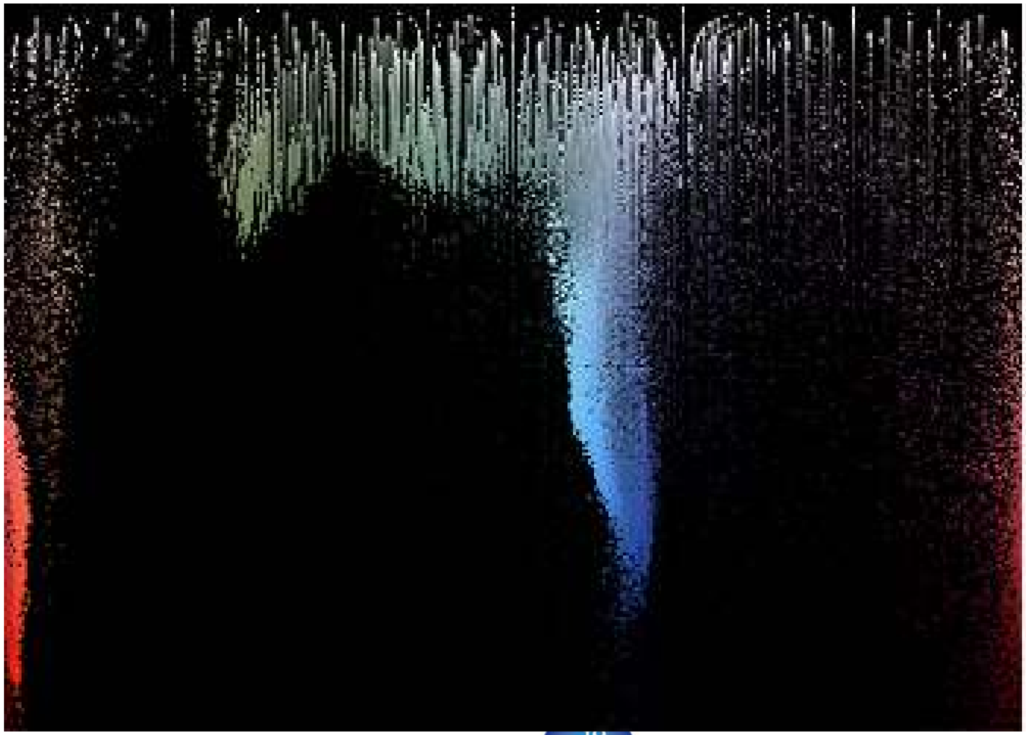
- HSV Histogram



Technique – Histogram Analysis

- Compare the HSV Histograms



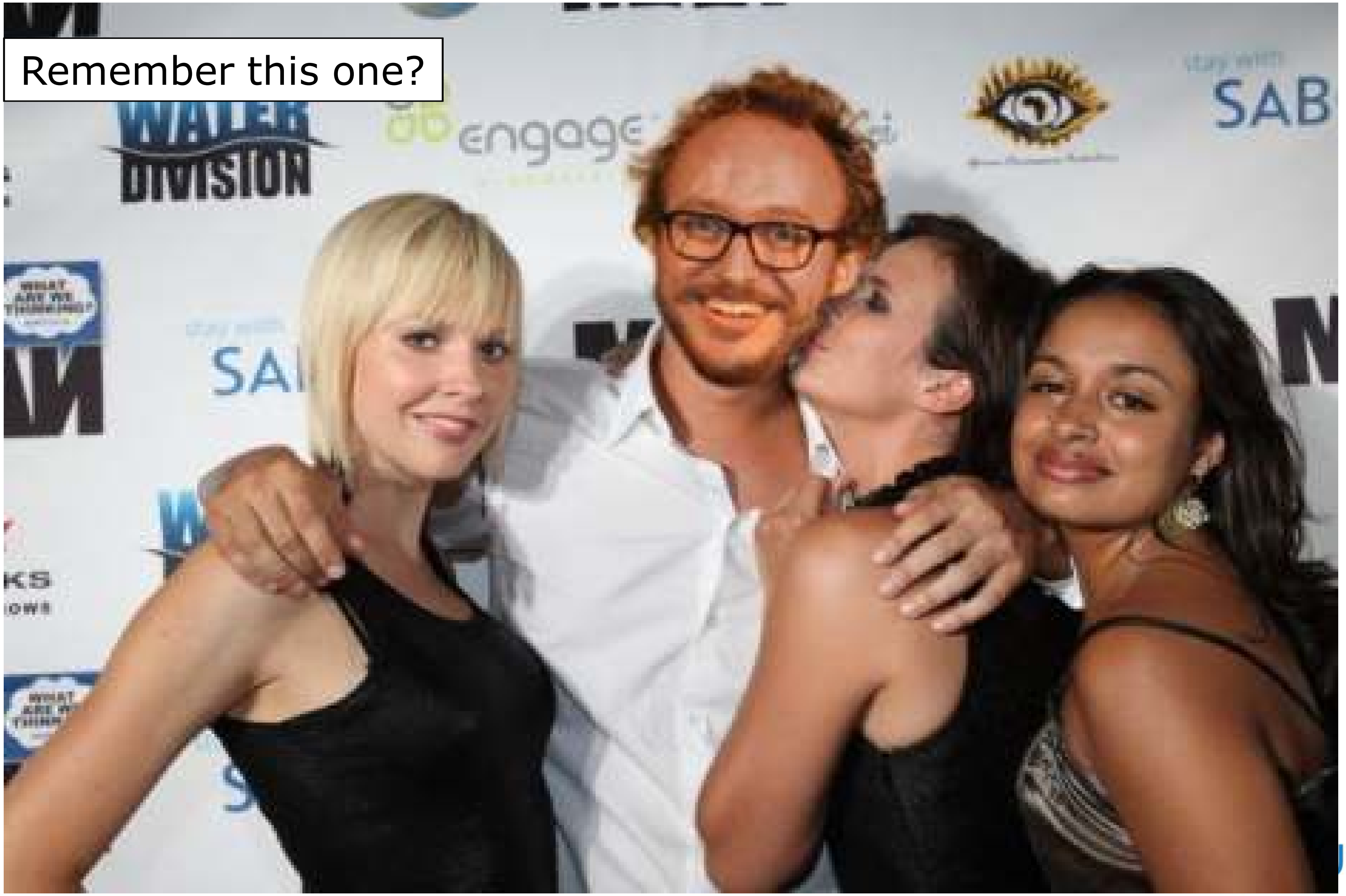


Technique – Error Level Analysis

- Useful in detecting images that have sections of differing quality.
- Generally, recently edited sections of images have a higher quality.

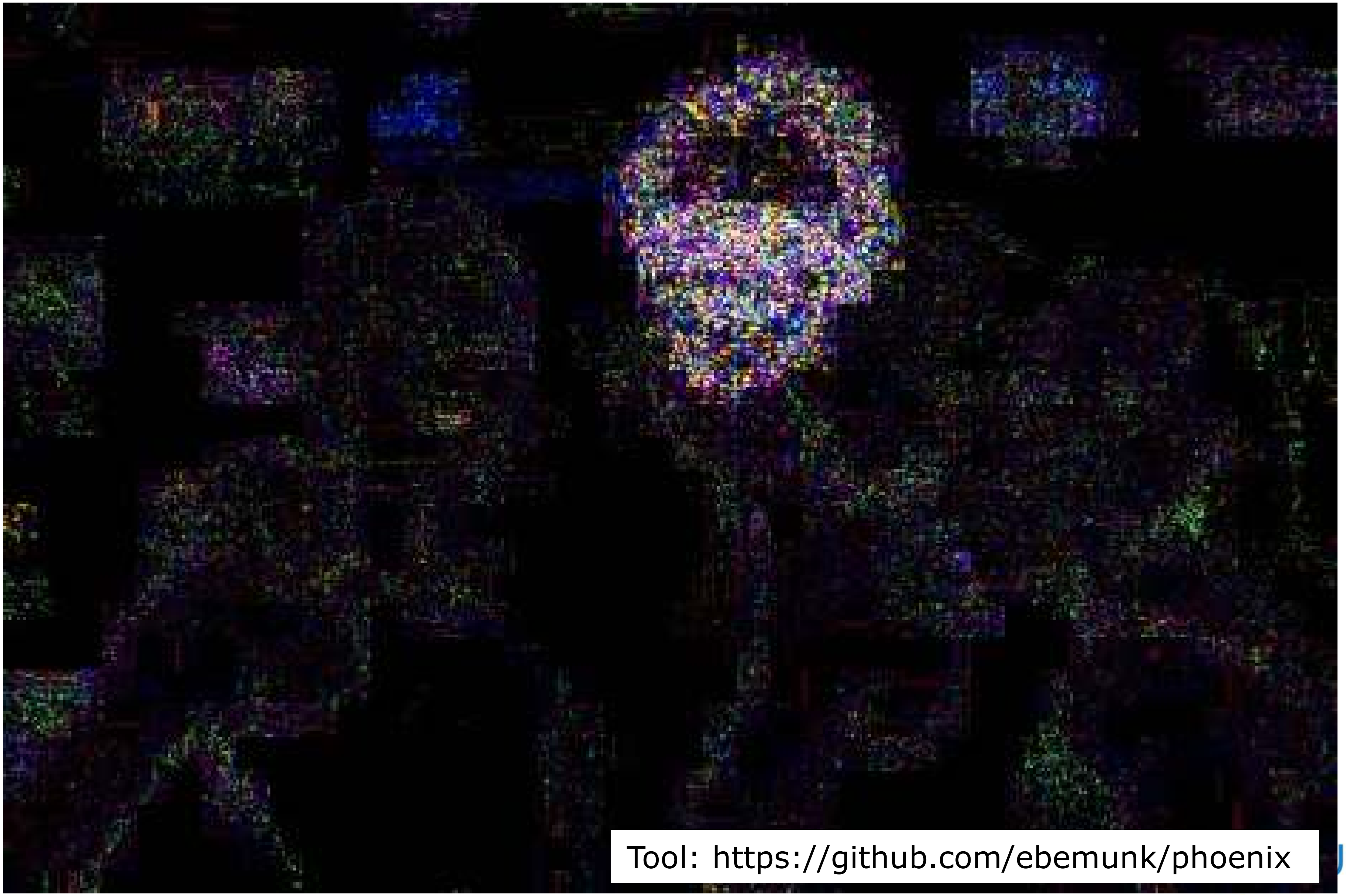
1. Resaves the image at a lower compression rate.
2. Looks at the difference between the original image and the recompressed image.

Technique – Error Level Analysis



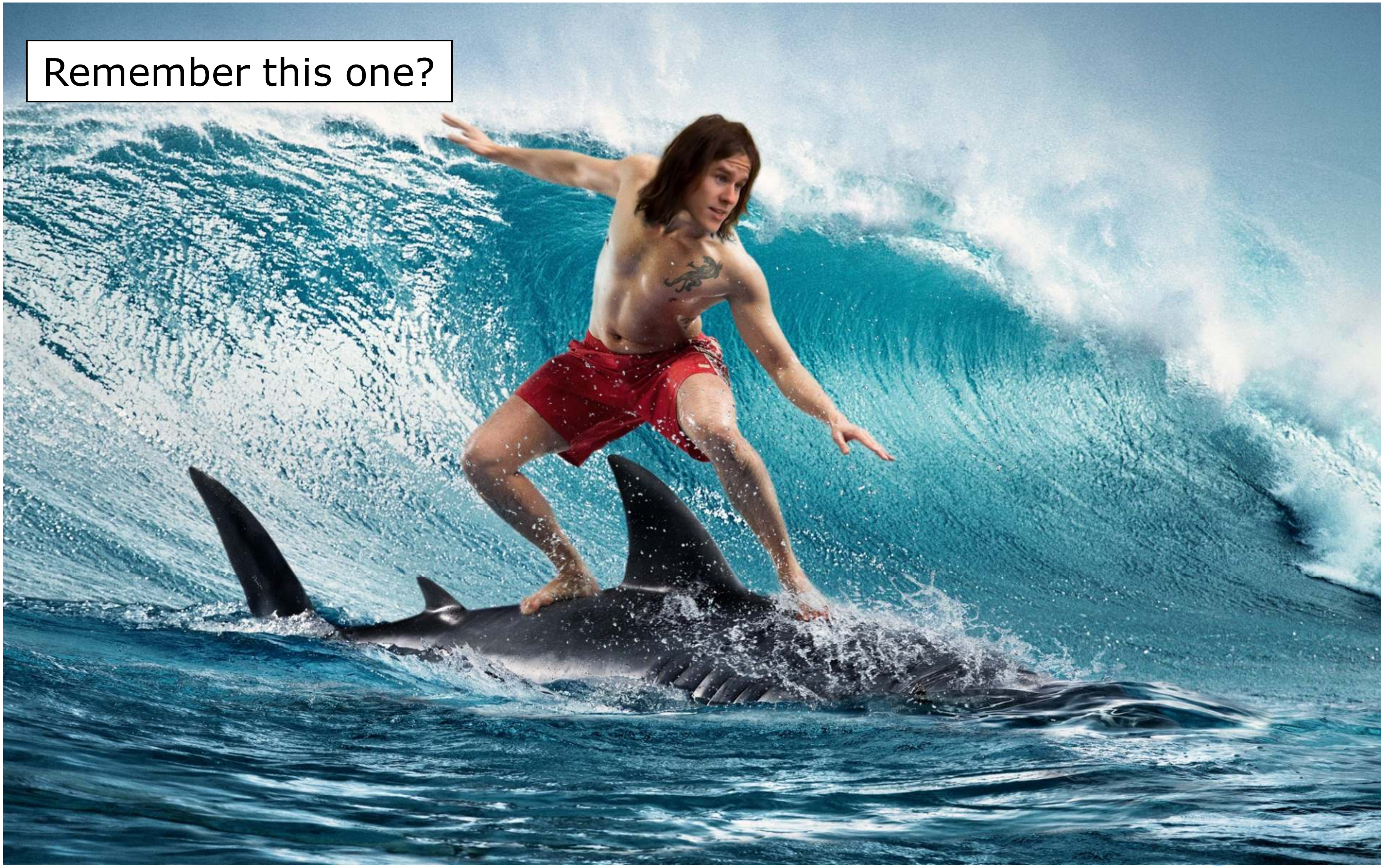
Remember this one?

Technique – Error Level Analysis



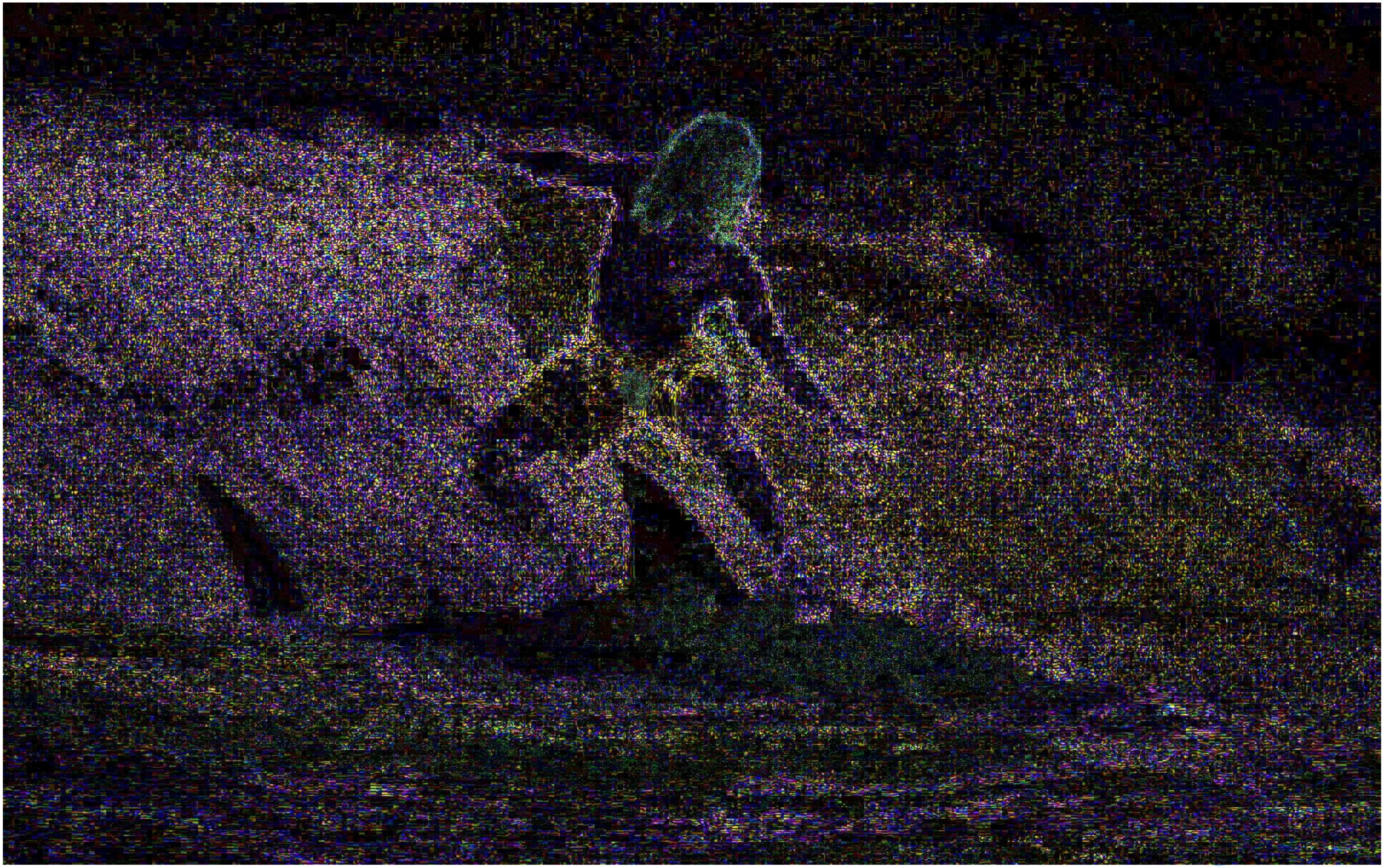
Tool: https://github.com/ebemunk/phoenix

Technique – Error Level Analysis



Remember this one?

Technique – Error Level Analysis



Technique – Luminance Gradient

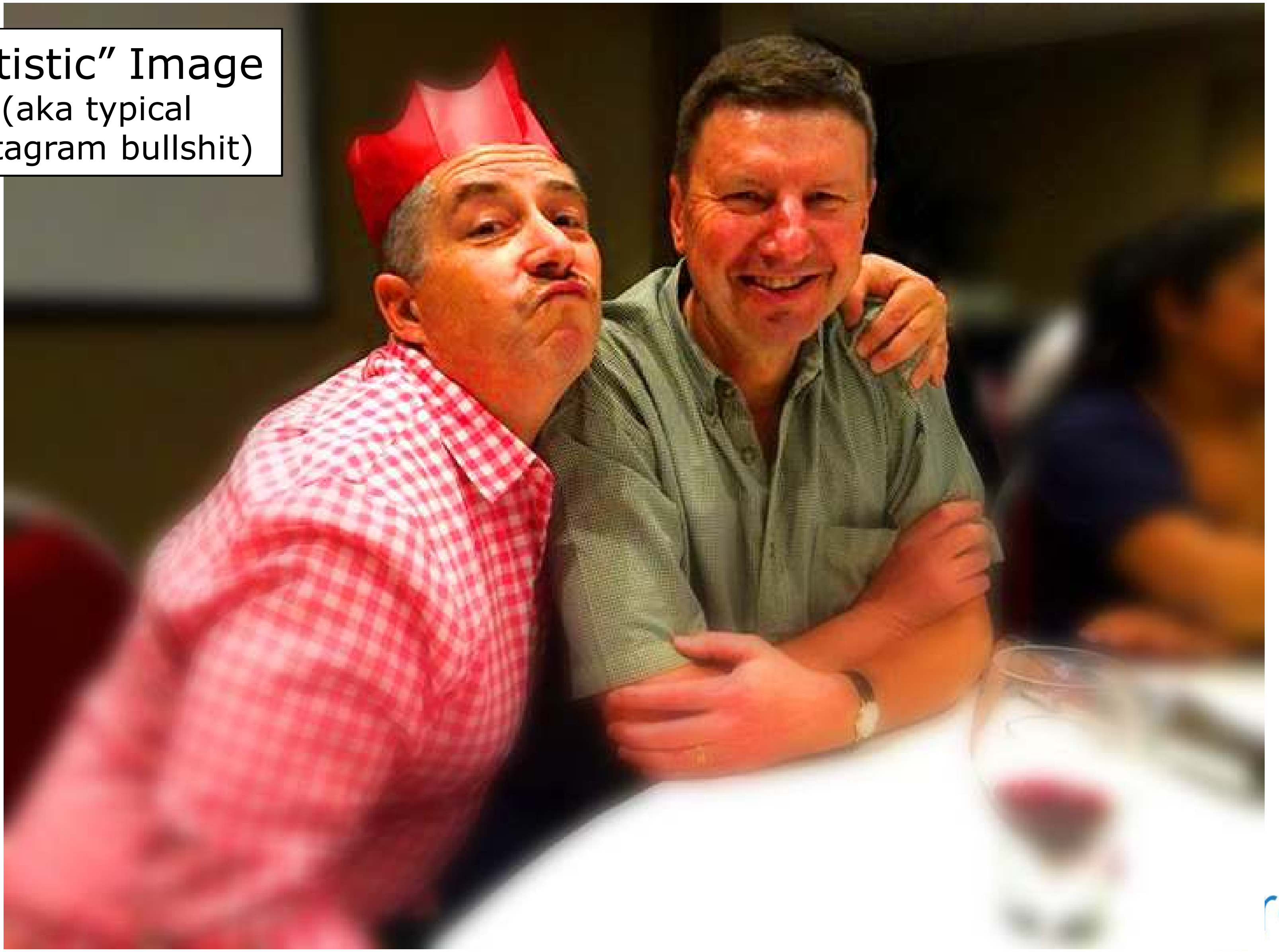
- Useful in detecting images that backgrounds that are artificially enhanced, e.g. defocused.
- The colour of every pixel indicates the direction of greatest change in brightness among its neighbours.
- Natural images show a lot of bumpy noise and jaggy lines.
- Smooth strokes or straight edges indicate digital manipulation.

Technique – Luminance Gradient

Original Image

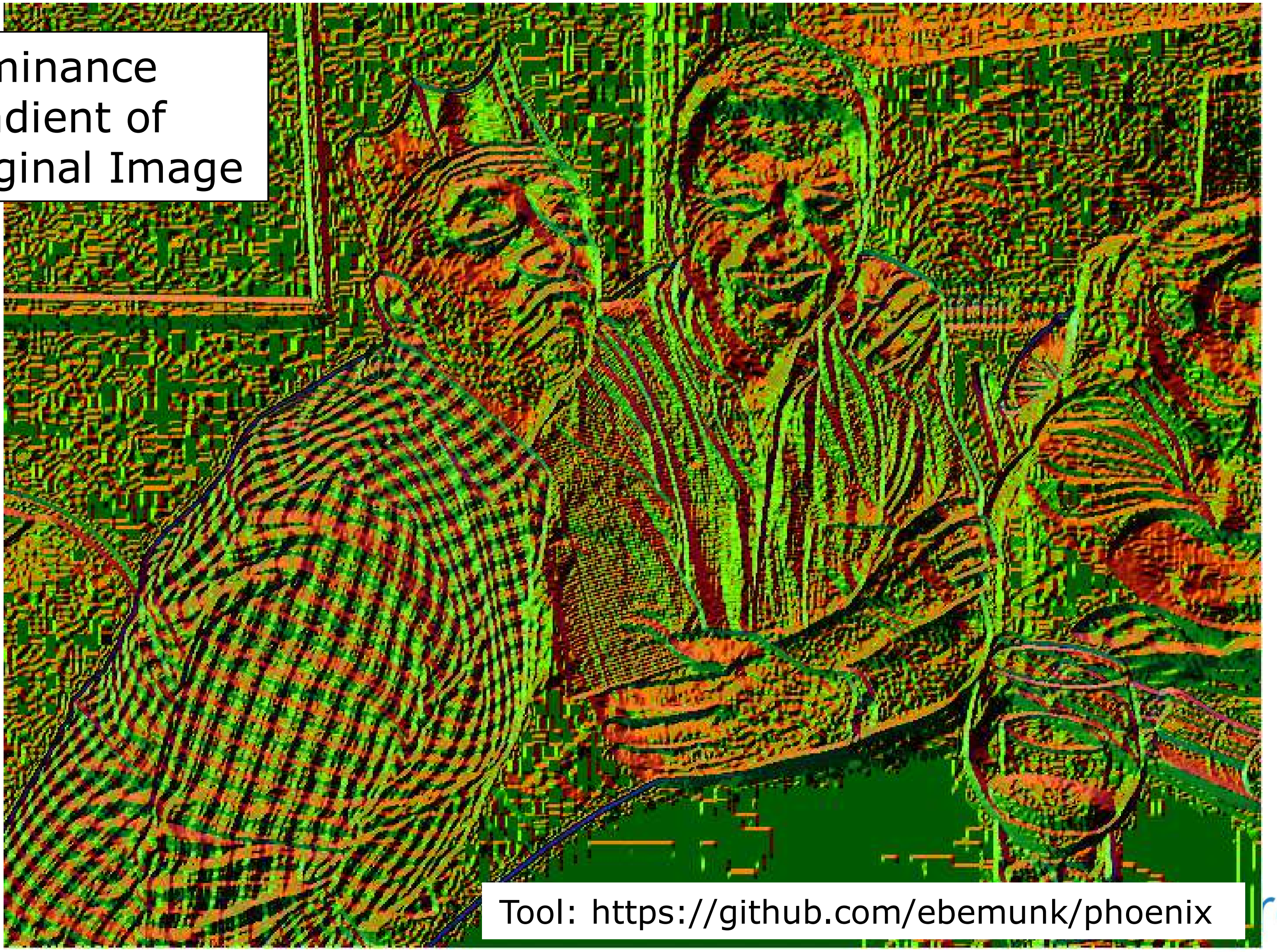
roup

Technique – Luminance Gradient



“Artistic” Image
(aka typical
Instagram bullshit)

Technique – Luminance Gradient

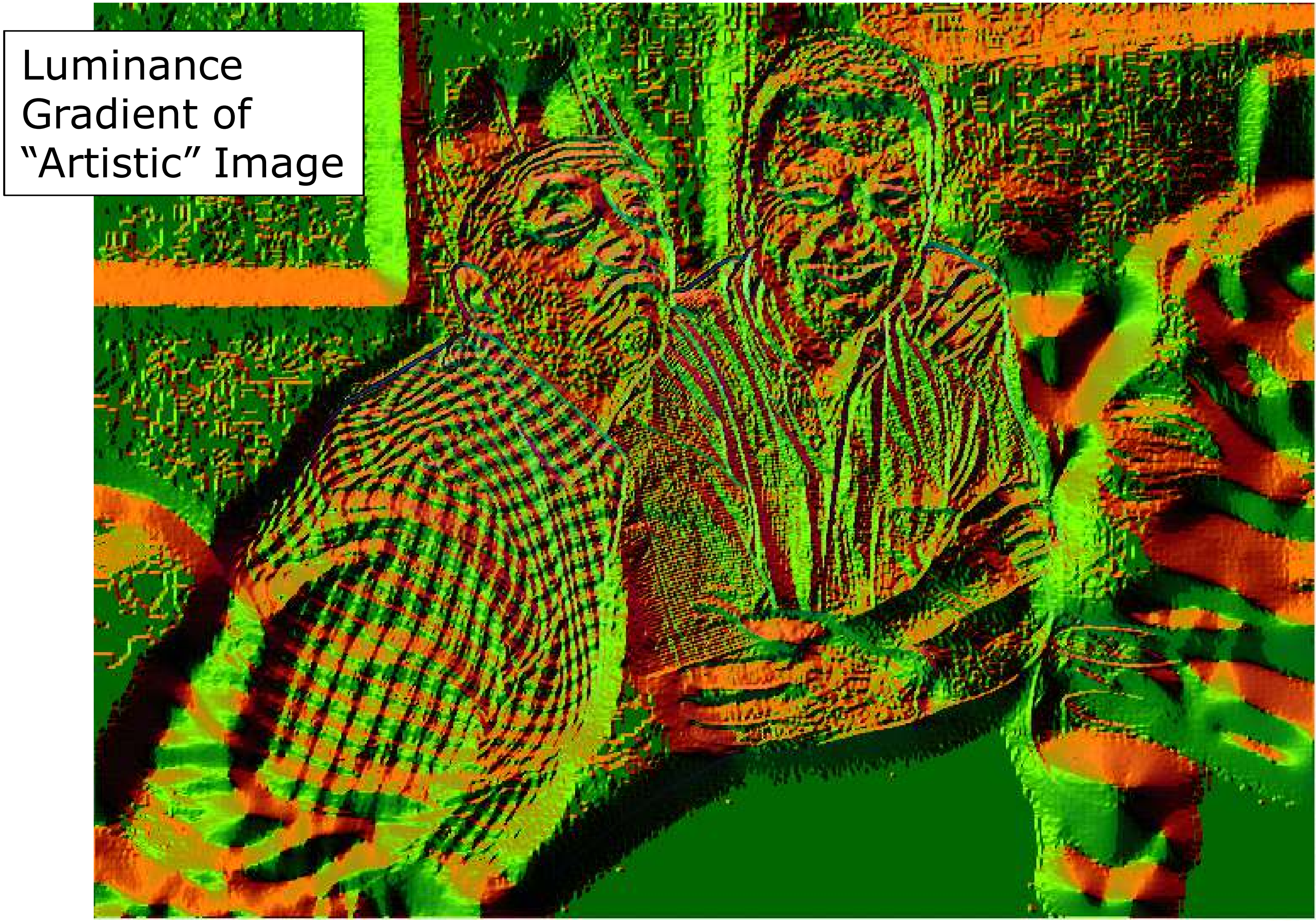


Luminance Gradient of Original Image

Tool: https://github.com/ebemunk/phoenix

roup

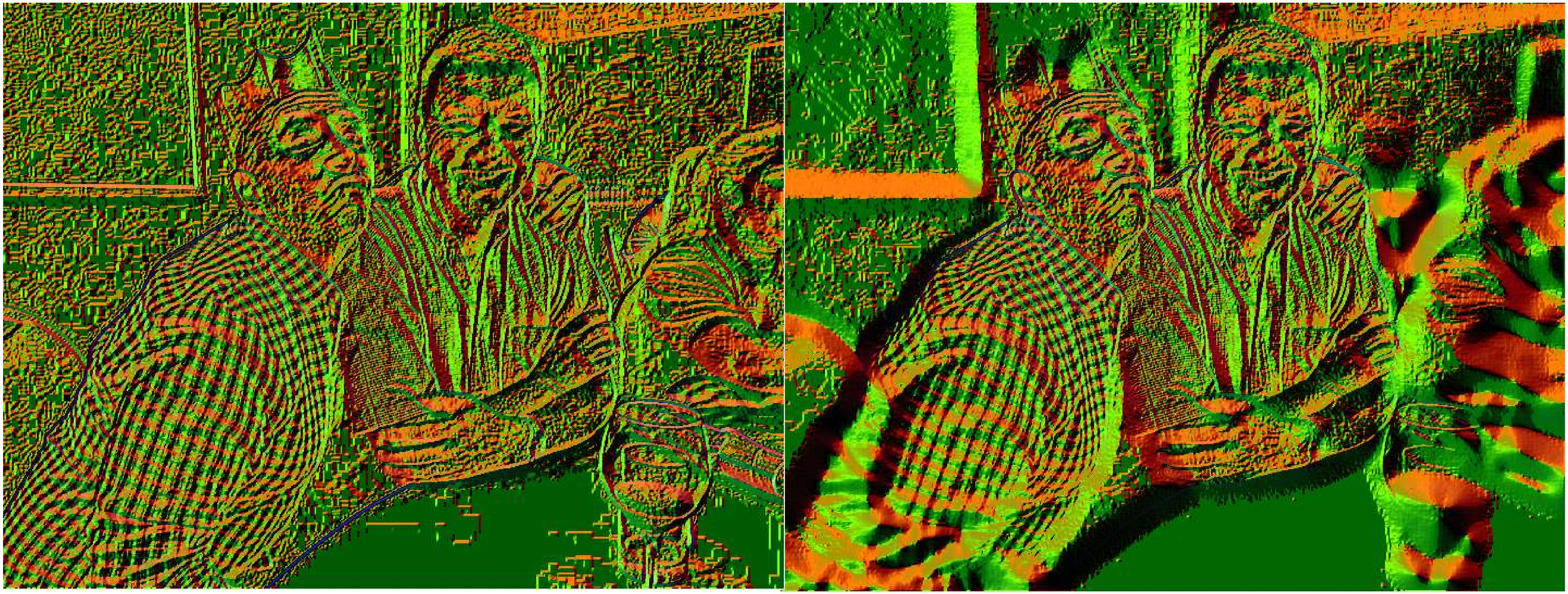
Technique – Luminance Gradient



Luminance Gradient of "Artistic" Image

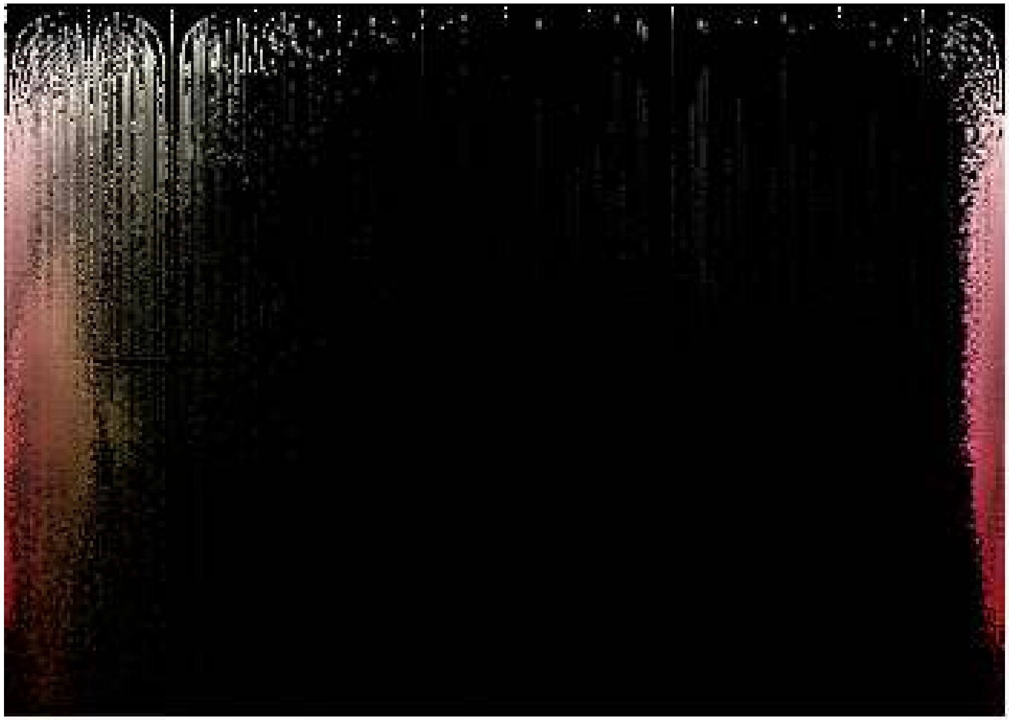
Technique – Luminance Gradient

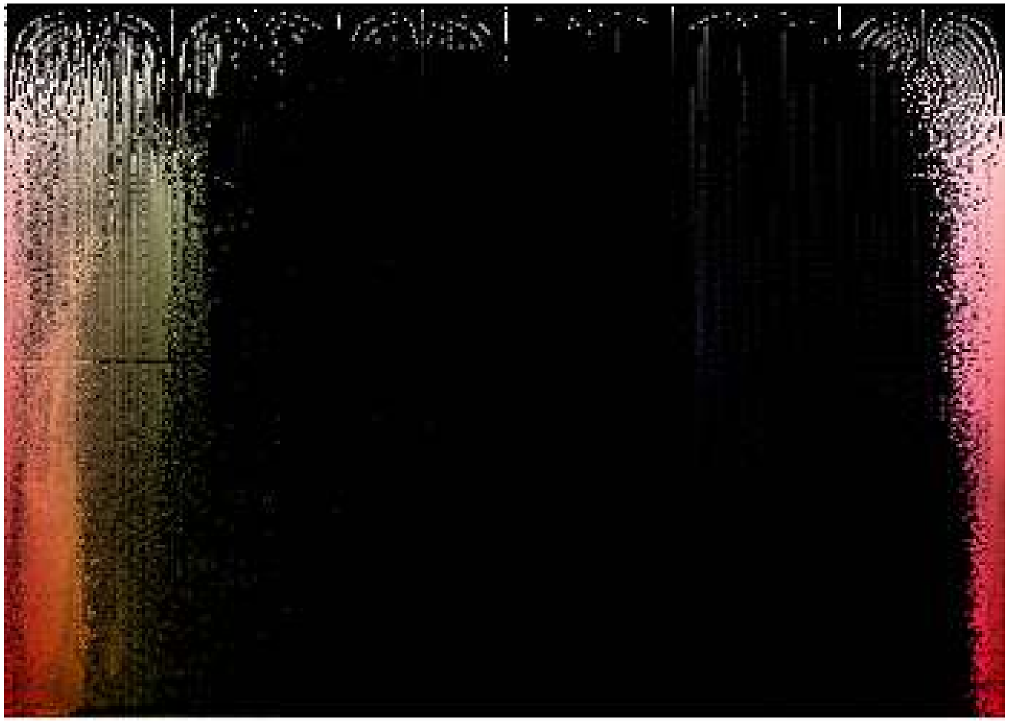
- Compare the Luminance Gradients
  - Notice the brush-stroke effect



Technique – Luminance Gradient

- Also compare the HSV Histograms





VIDEO ANALYSIS

saltbushgroup

Technique – Physics

saltbushgroup

Technique – Physics

- Break out your high-school physics books.
- Use formulas to track trajectory of objects.
- Great source: http://www.wired.com/2014/10/physics-fake-videos/

Technique – Physics

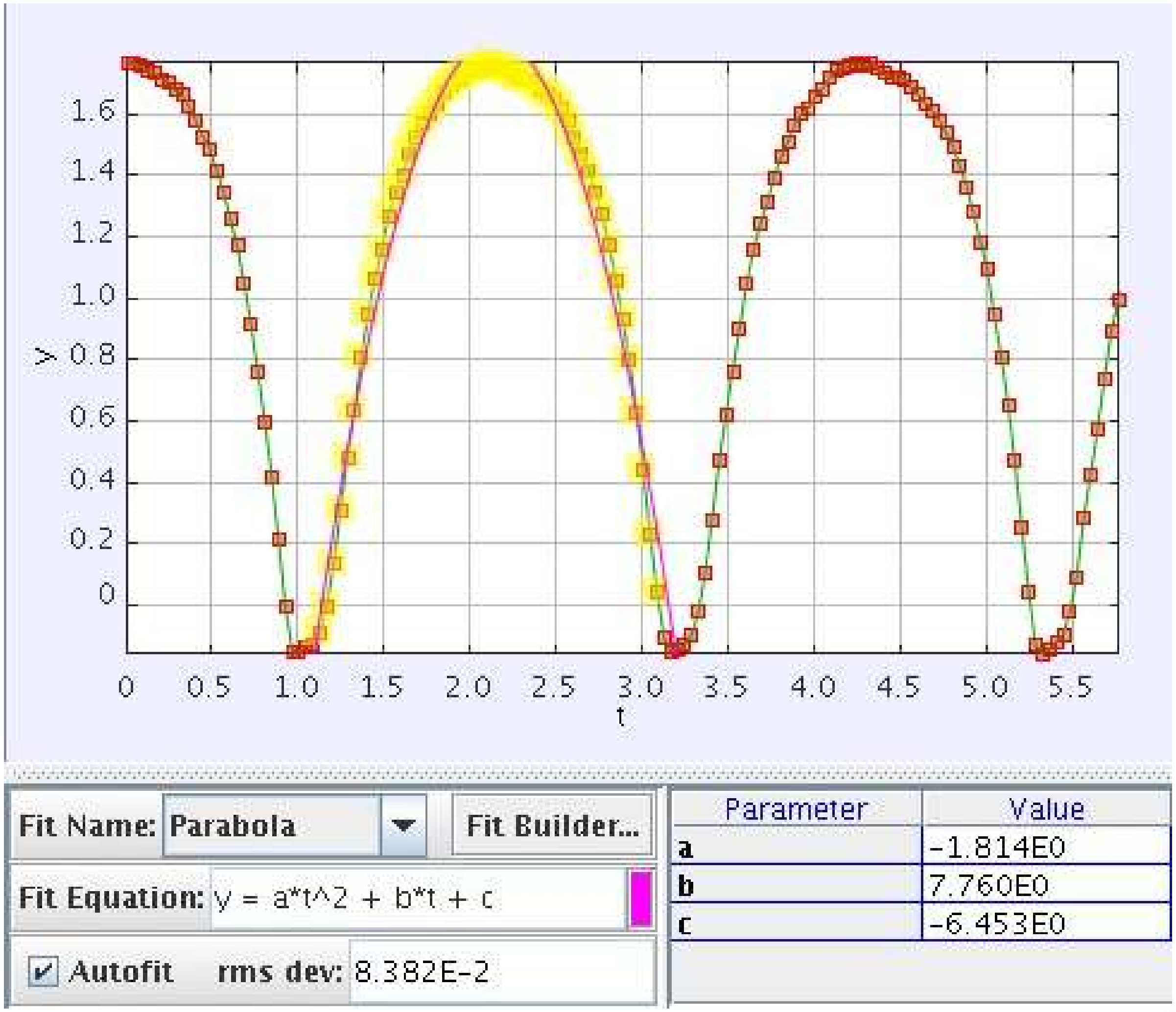
- We can use the physics analysis tool, Tracker[1], to track objects in a video.

[1] https://www.cabrillo.edu/~dbrown/tracker/

Technique – Physics

saltbushgroup

Technique – Physics



Fit Name: Parabola

Fit Equation: y = a*t^2 + b*t + c

☑ Autofit rms dev: 8.382E-2

Parameter	Value
a	-1.814E0
b	7.760E0
c	-6.453E0

Technique – Jitter Analysis

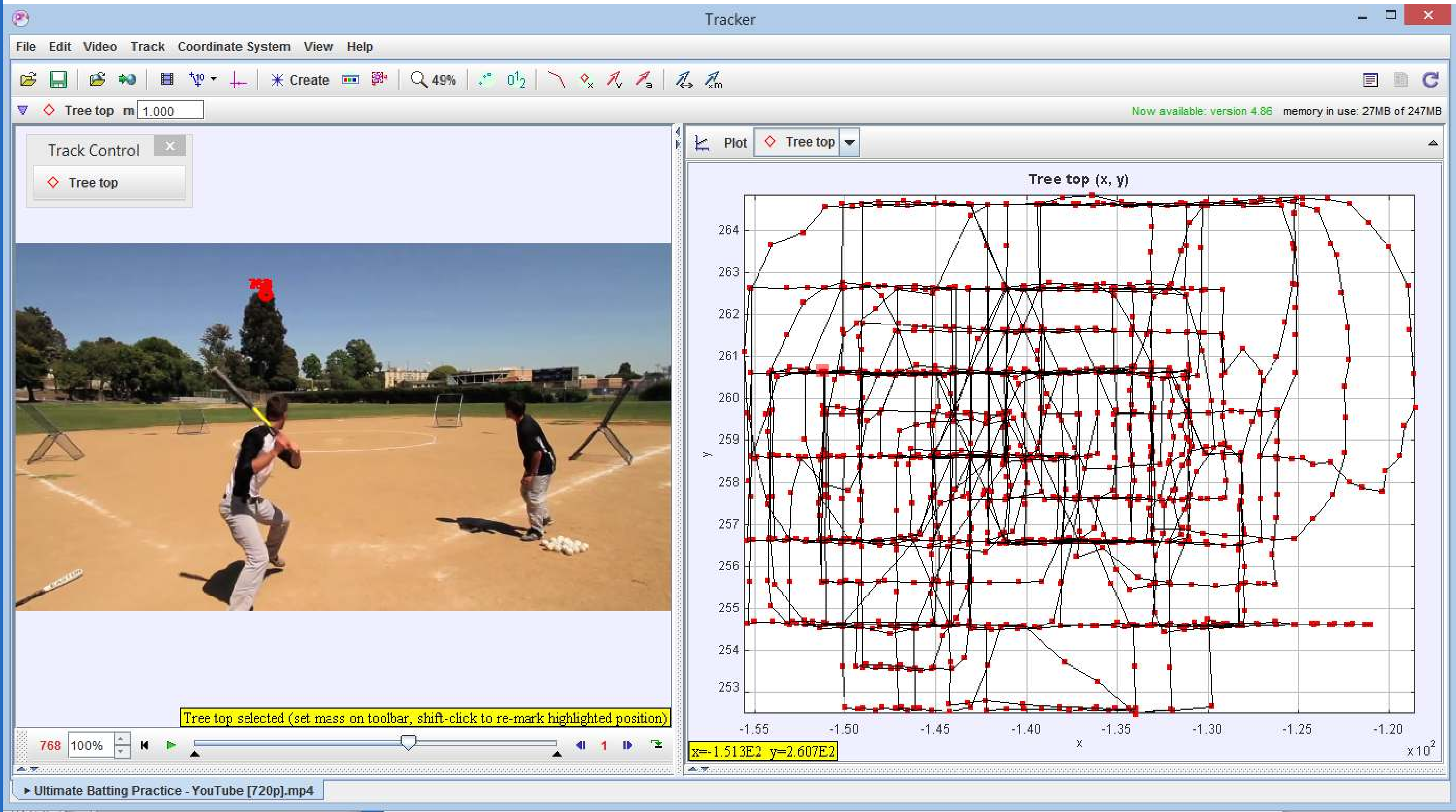
1. Hand held cameras are subject to the jitter of a human’s hand.
2. Real jitter tends to be fairly erratic, like a random-walk.
3. Fake jitter tends to be smoother.

Technique – Jitter Analysis

- Again, we can use Tracker, to track a still object in a moving video, allowing us to track the hand jitter and comparing it to a typical, real hand jitter.

Technique – Jitter Analysis

Technique – Jitter Analysis



Tree top m 1.000

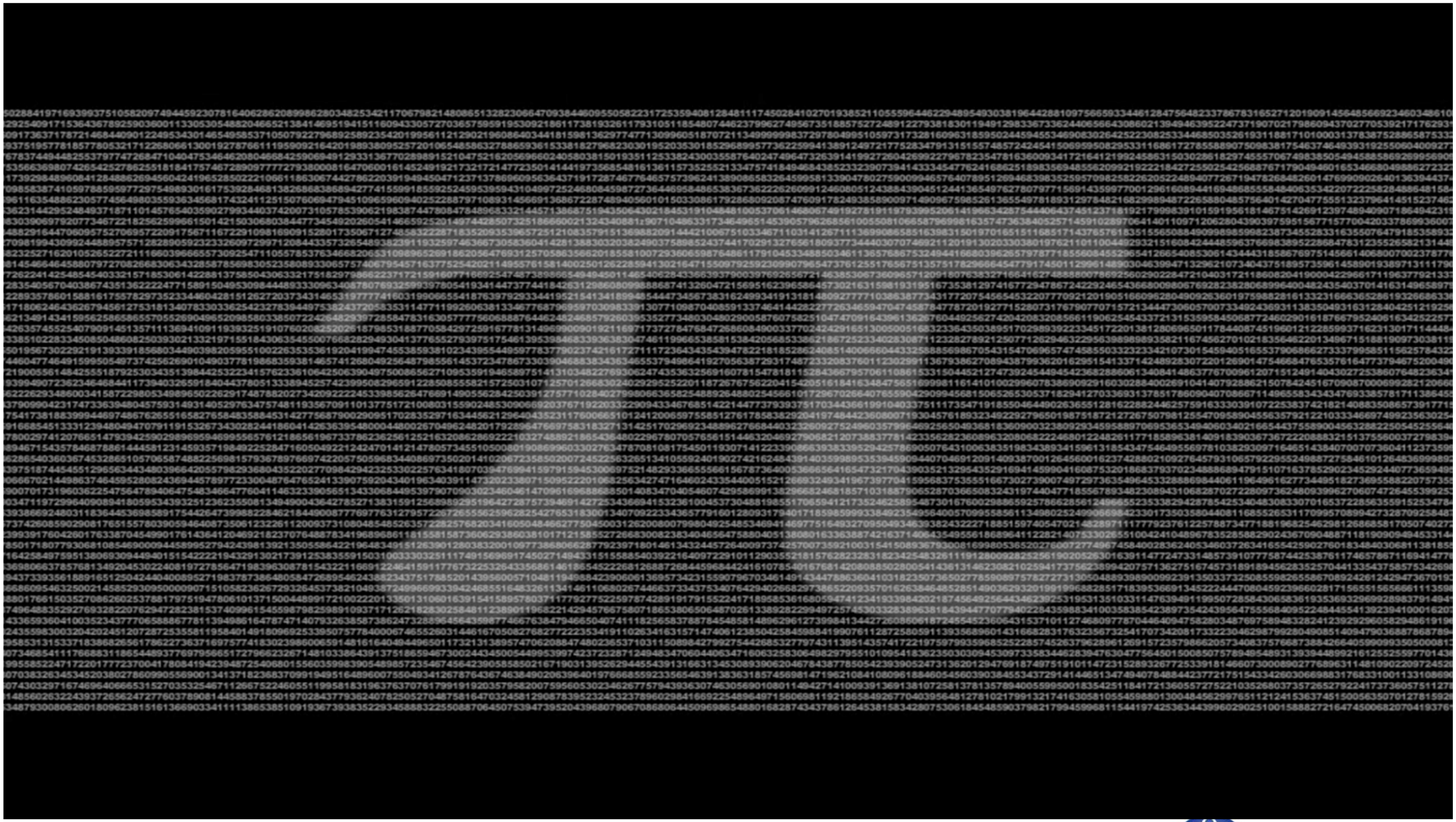
Now available: version 4.86 memory in use: 27MB of 247MB

Tree top selected (set mass on toolbar, shift-click to re-mark highlighted position)

x=-1.513E2 y=2.607E2

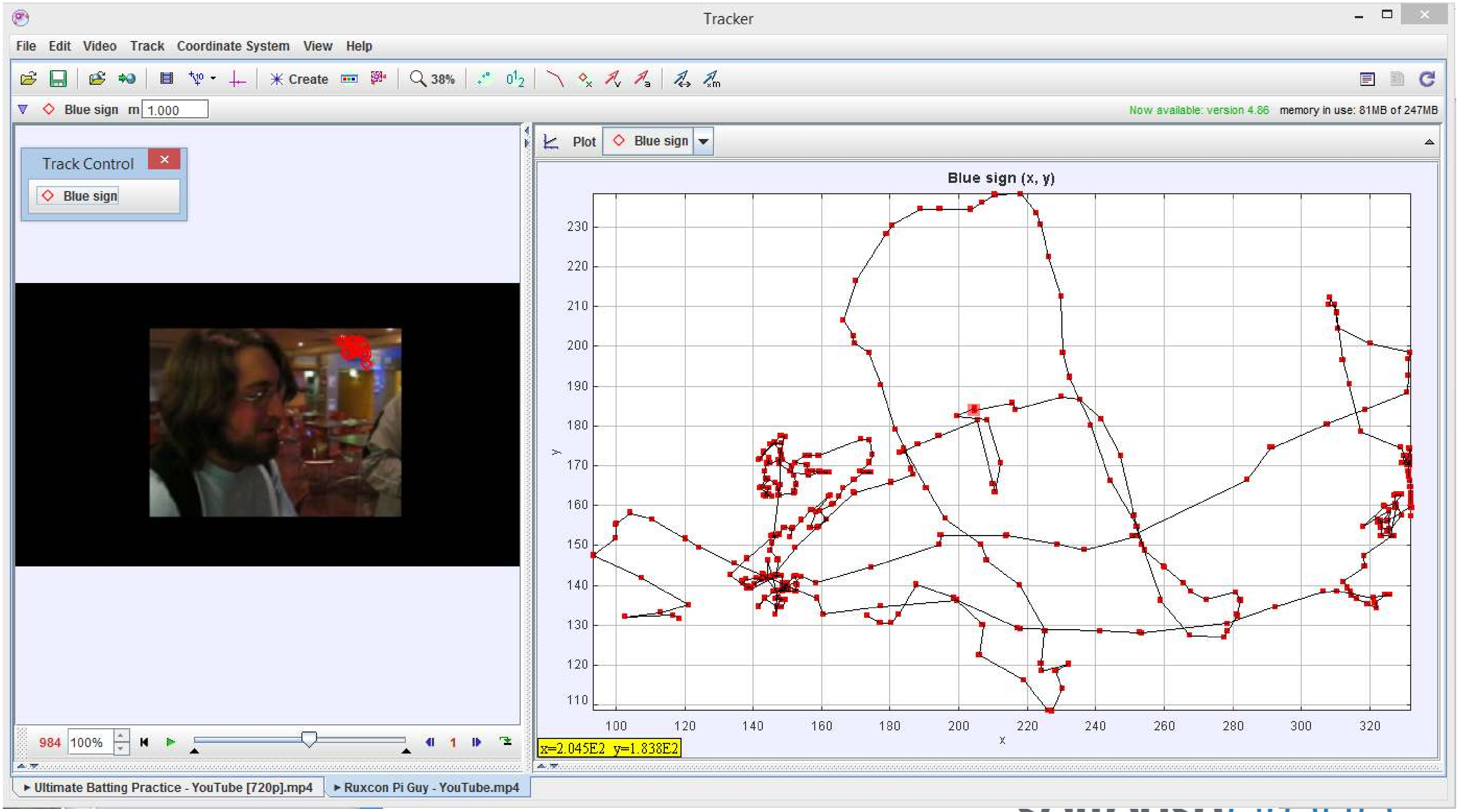
Ultimate Batting Practice - YouTube [720p].mp4

Technique – Jitter Analysis



saltbushgroup

Technique – Jitter Analysis



Tracker

Blue sign m 1.000

Now available: version 4.86 memory in use: 81MB of 247MB

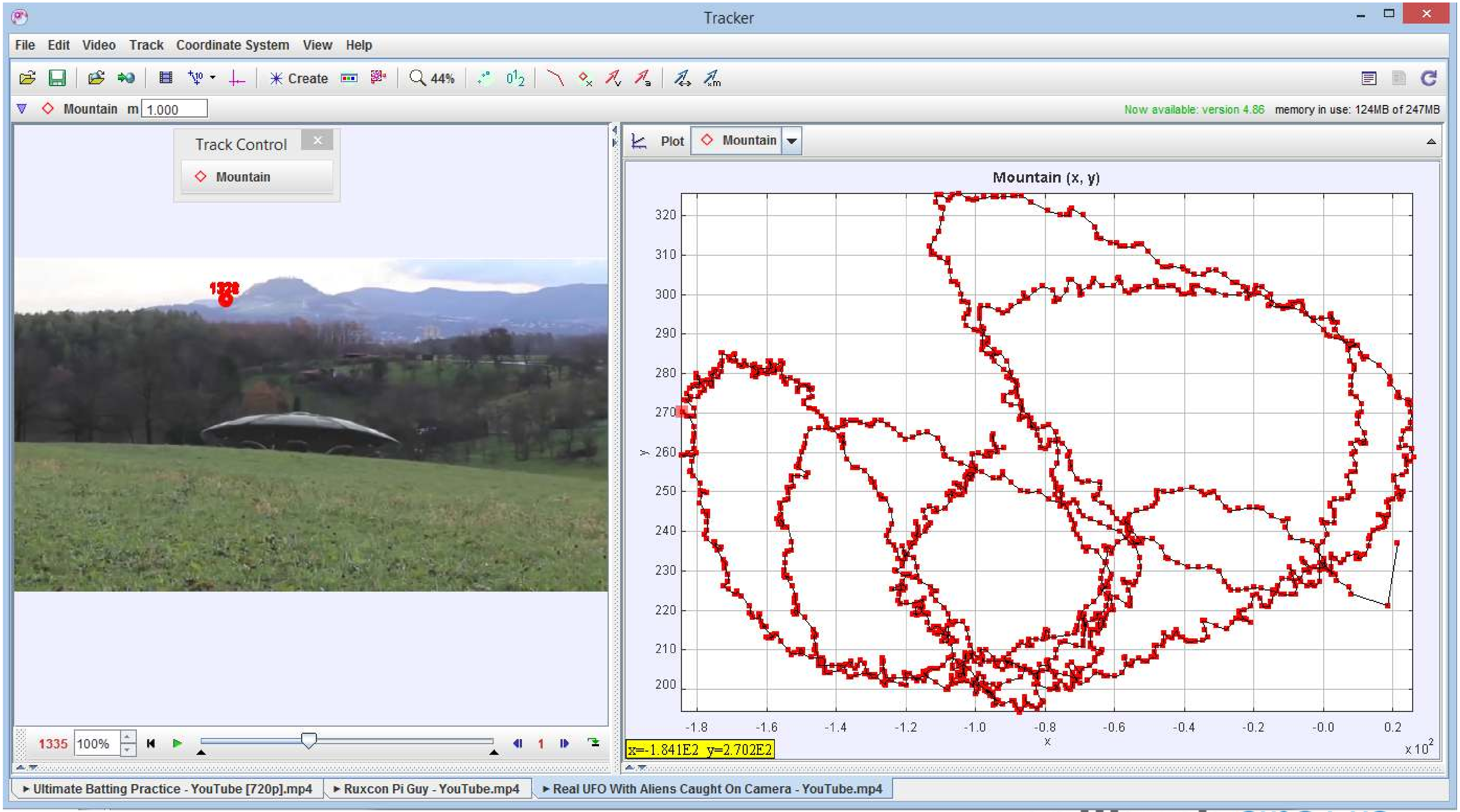
x=2.045E2 y=1.838E2

▸ Ultimate Batting Practice - YouTube [720p].mp4

▸ Ruxcon Pi Guy - YouTube.mp4

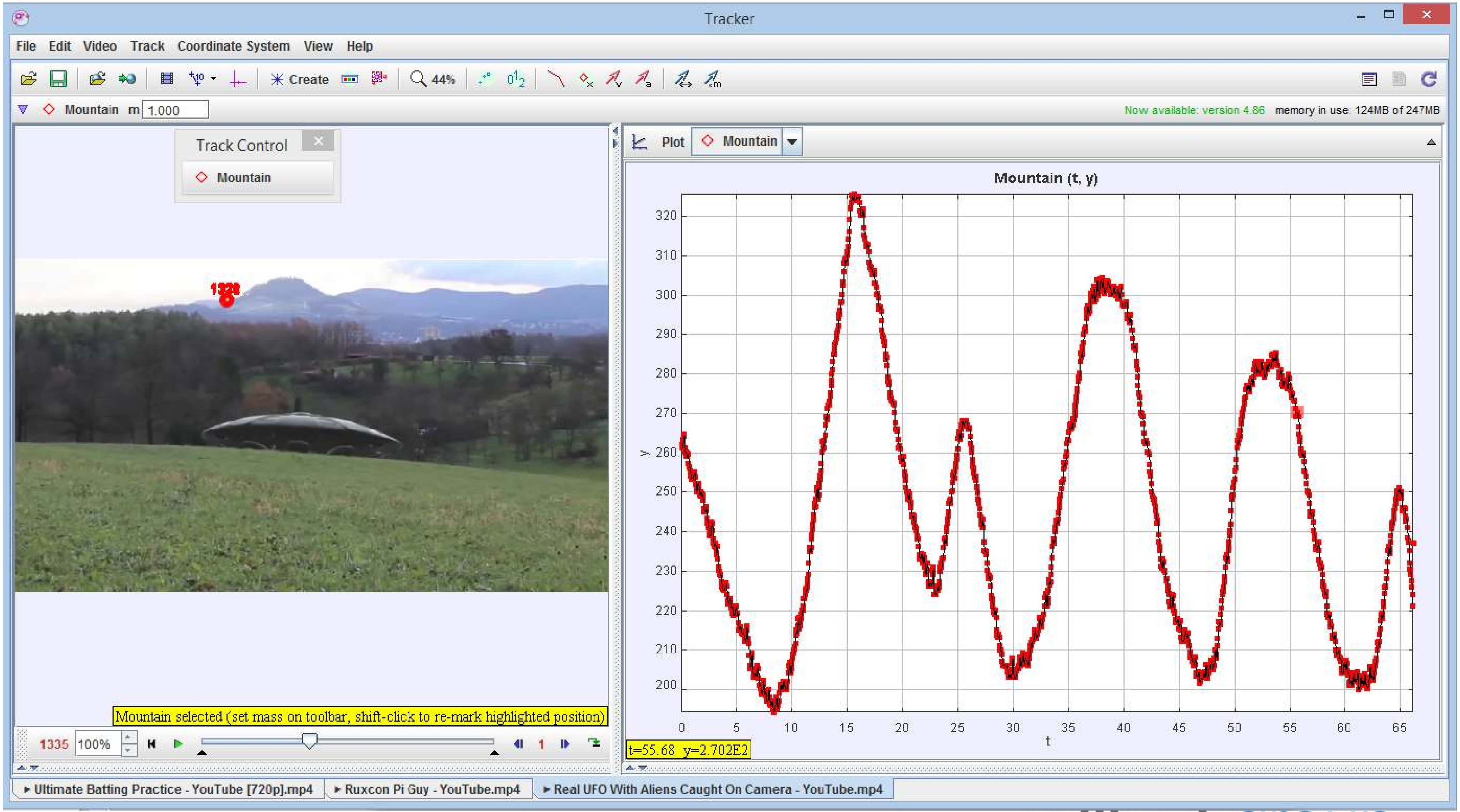
Technique – Jitter Analysis

Technique – Jitter Analysis


Tracker
File Edit Video Track Coordinate System View Help
Create 44%
Mountain m 1.000
Now available: version 4.86 memory in use: 124MB of 247MB
Track Control
Mountain
Plot Mountain
Mountain (x, y)
320
310
300
290
280
270
260
250
240
230
220
210
200
y
-1.8 -1.6 -1.4 -1.2 -1.0 -0.8 -0.6 -0.4 -0.2 -0.0 0.2
x
x 10^2
x=-1.841E2 y=2.702E2
1335 100% 1
▸ Ultimate Batting Practice - YouTube [720p].mp4
▸ Ruxcon Pi Guy - YouTube.mp4
▸ Real UFO With Aliens Caught On Camera - YouTube.mp4

saltbushgroup

Technique – Jitter Analysis



Mountain m 1.000

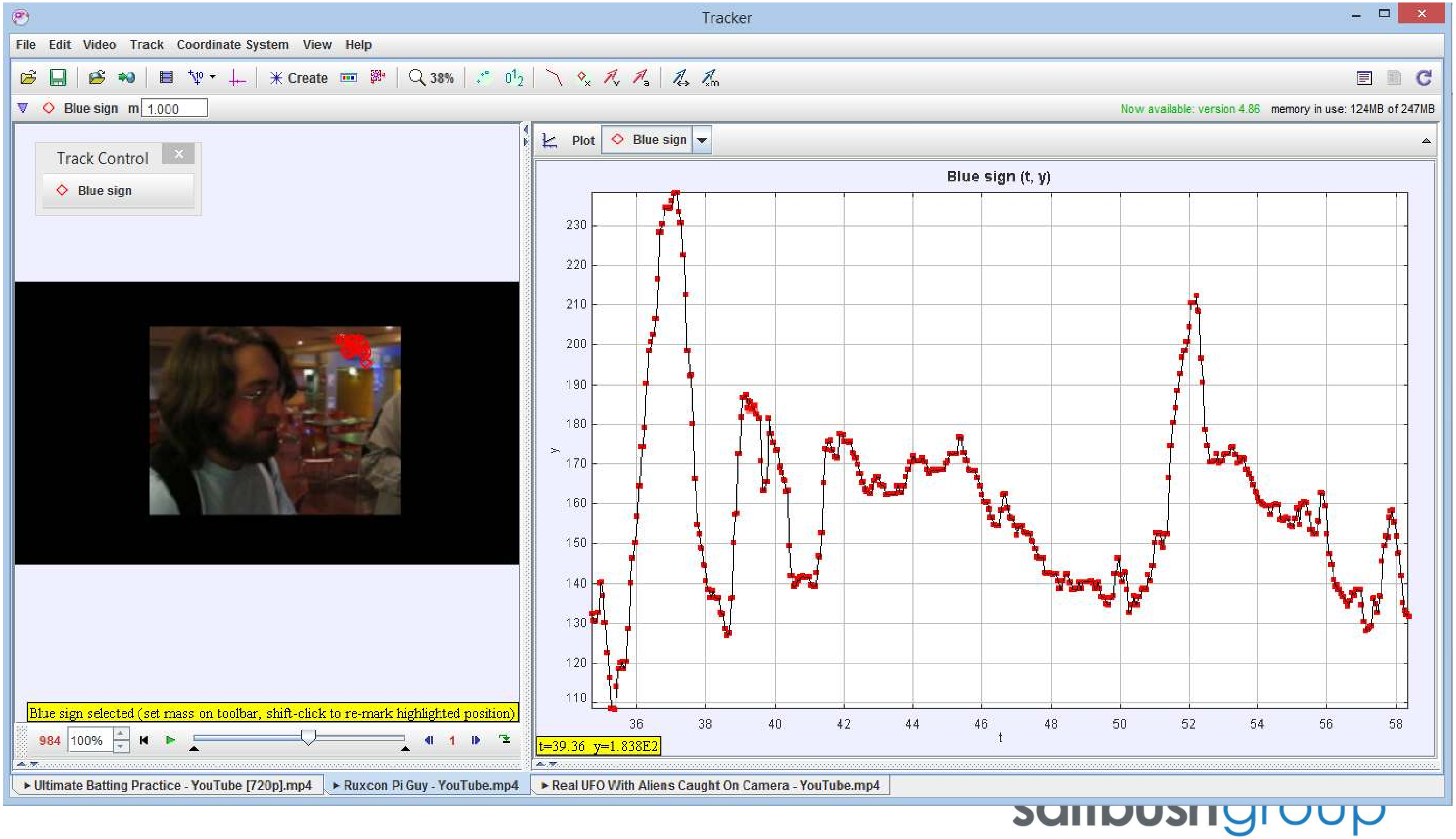
Now available: version 4.86 memory in use: 124MB of 247MB

Mountain selected (set mass on toolbar, shift-click to re-mark highlighted position)

t=55.68 y=2.702E2

saltbushgroup

Technique – Jitter Analysis



Blue sign m 1.000

Now available: version 4.86 memory in use: 124MB of 247MB

Blue sign selected (set mass on toolbar, shift-click to re-mark highlighted position)

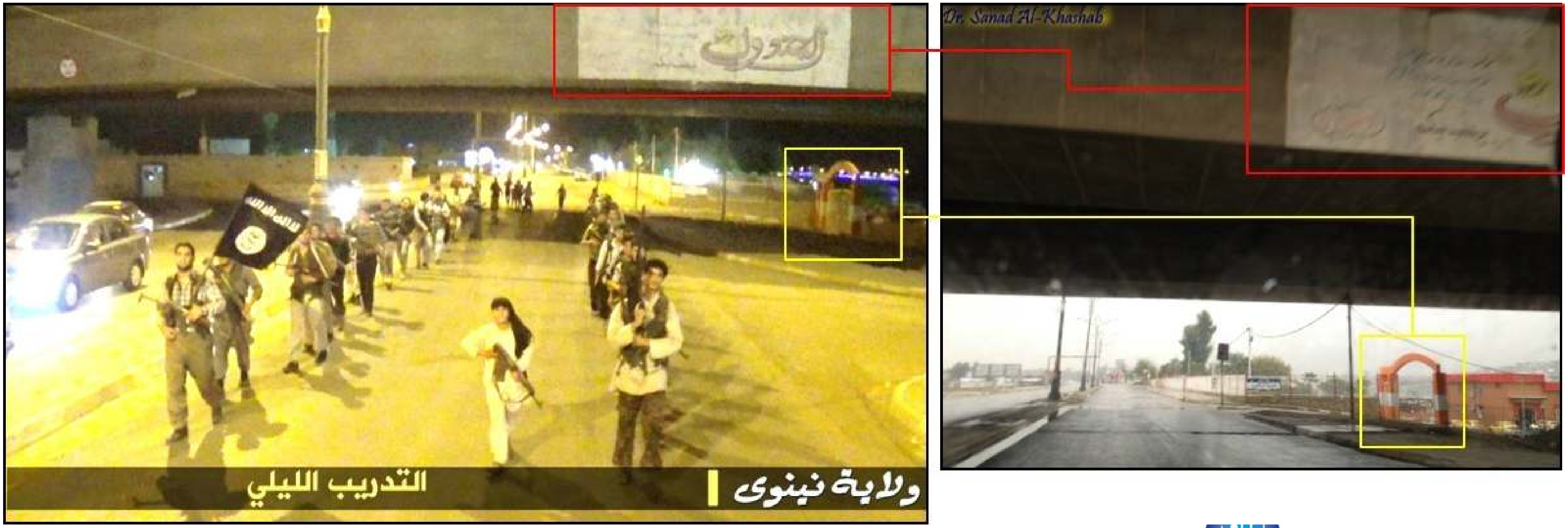
t=39.36 y=1.838E2

GEOLOCATION

saltbushgroup

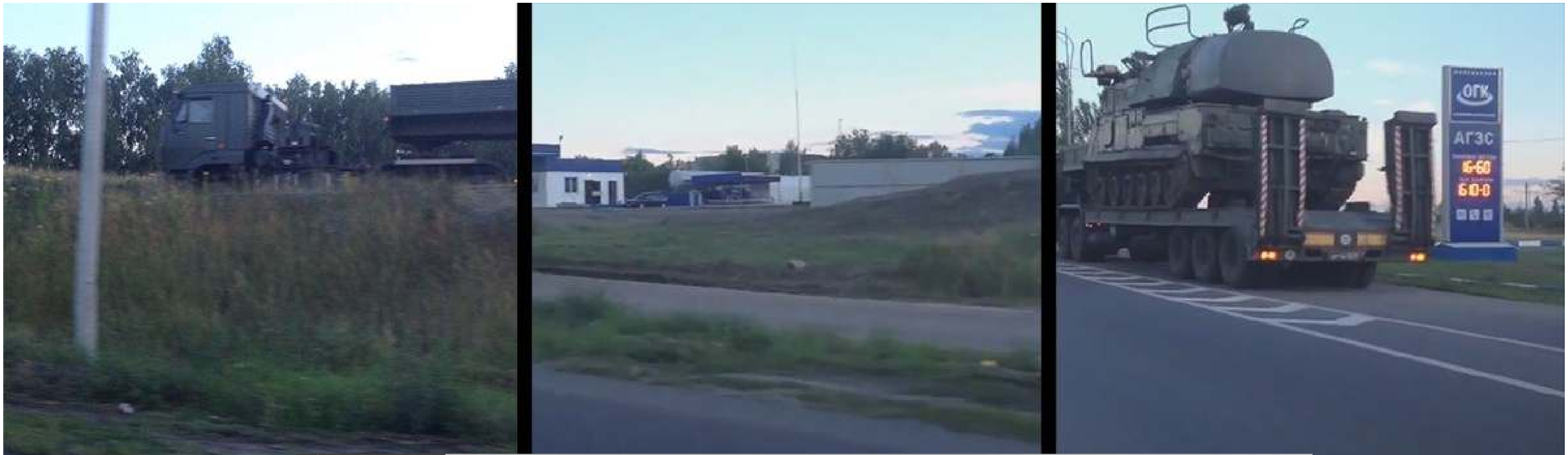
Technique – Geolocation through Eyeballing

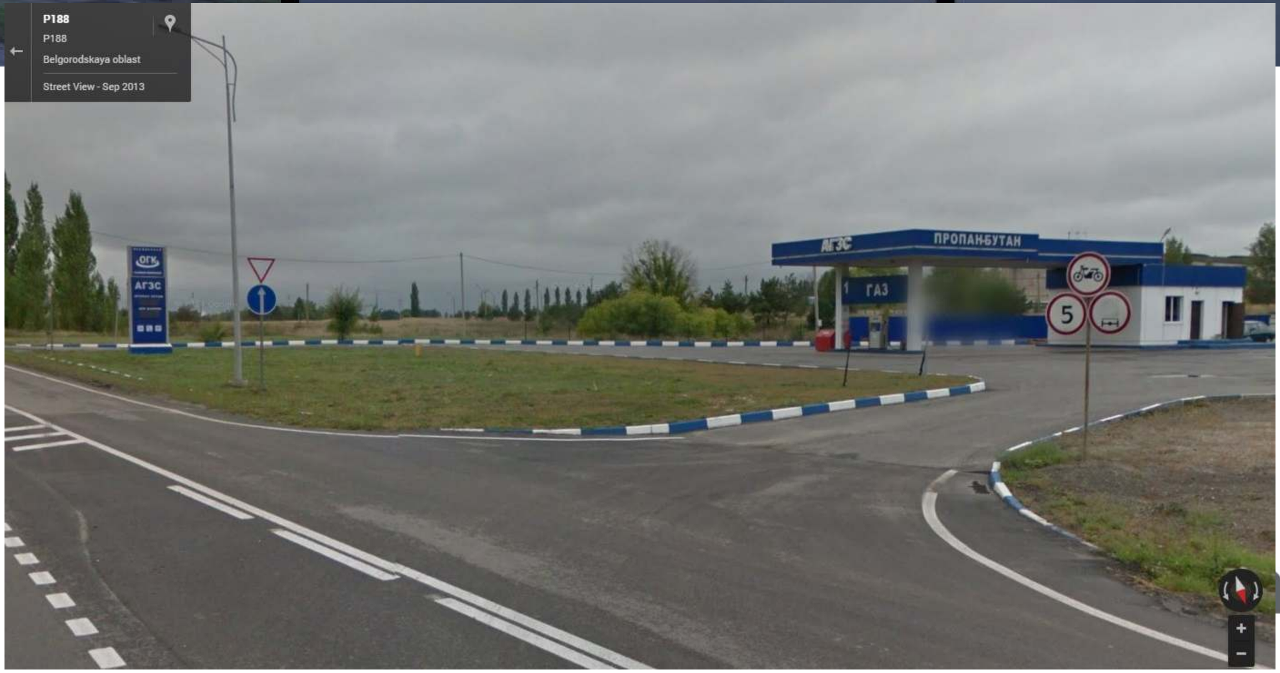
- Bell¿ngcat[1] (Kickstarter-funded journos) use online mapping tools to geolocate ISIS training camps, MH17 convoys in Russia, etc.



[1] https://www.bellingcat.com/

Technique – Geolocation through Eyeballing




P188

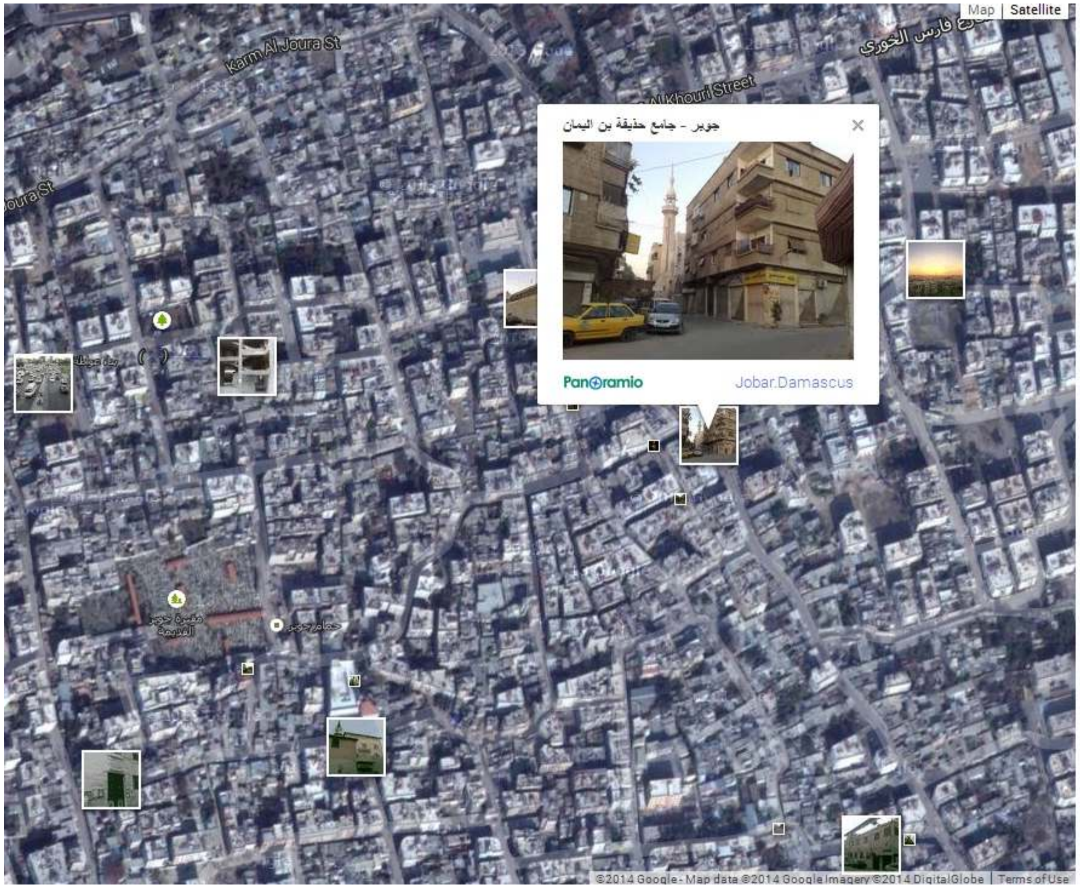
P188

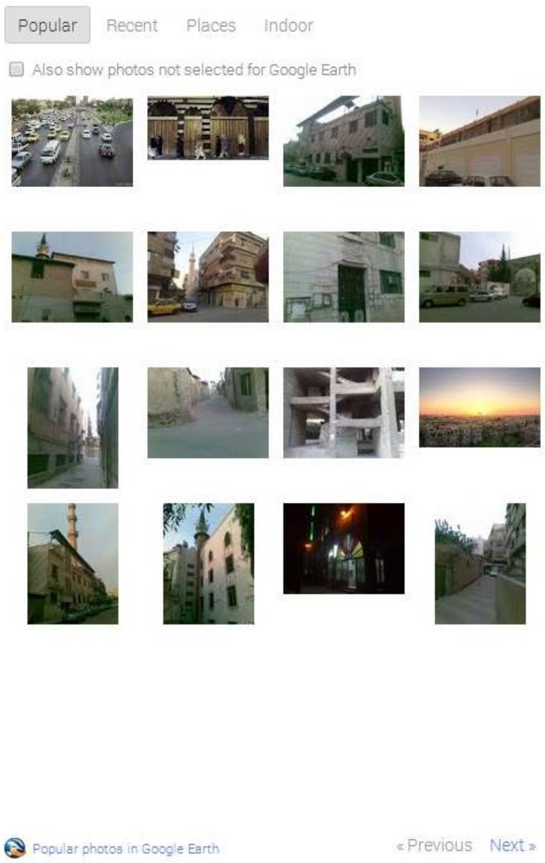
Belgorodskaya oblast

Street View - Sep 2013

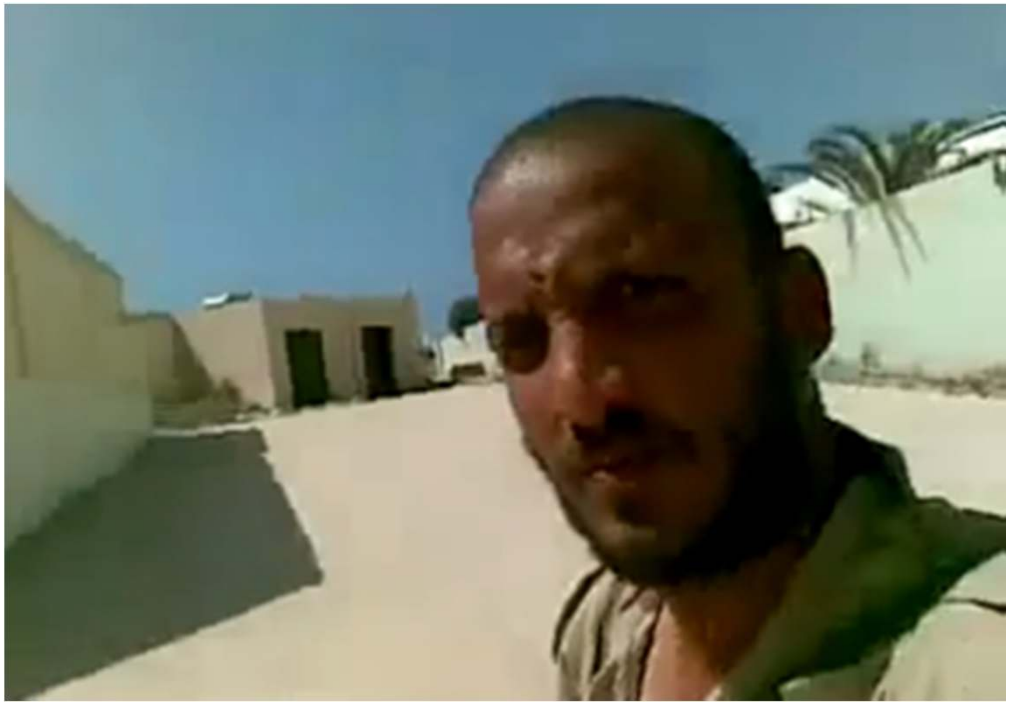
Technique – Geolocation through Eyeballing

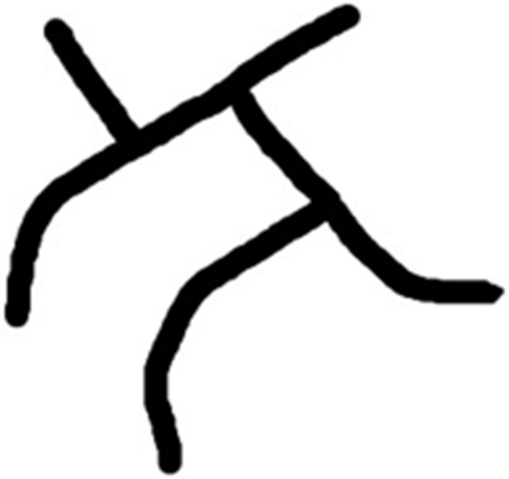
- Use Wikimapia, Panoramio, Google Earth, and Google Maps to identify landmarks in area of interest.


Map | Satellite
Karm Al Joura St
Joura St
Alkhouri Street
شارع فارس الخوري
جوبر - جامع حذيفة بن اليمان
Panoramio
Jobar.Damascus
©2014 Google - Map data ©2014 Google Imagery ©2014 DigitalGlobe | Terms of Use

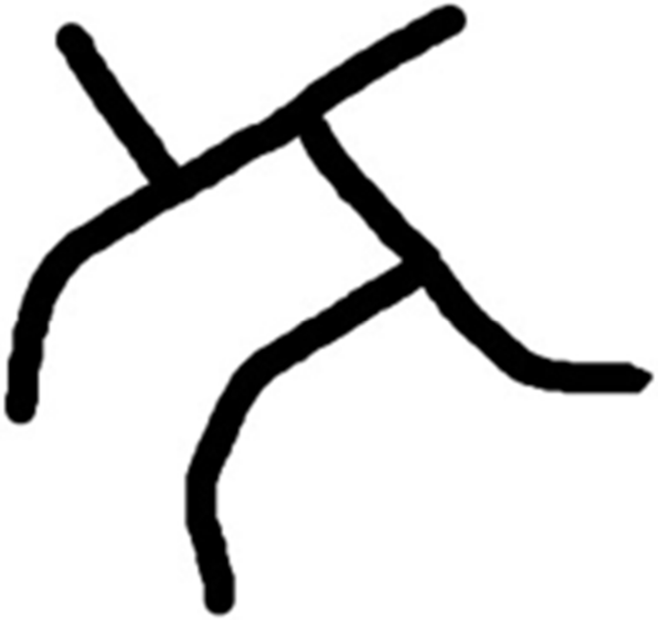

Popular
Recent
Places
Indoor
□ Also show photos not selected for Google Earth
Popular photos in Google Earth
« Previous
Next »

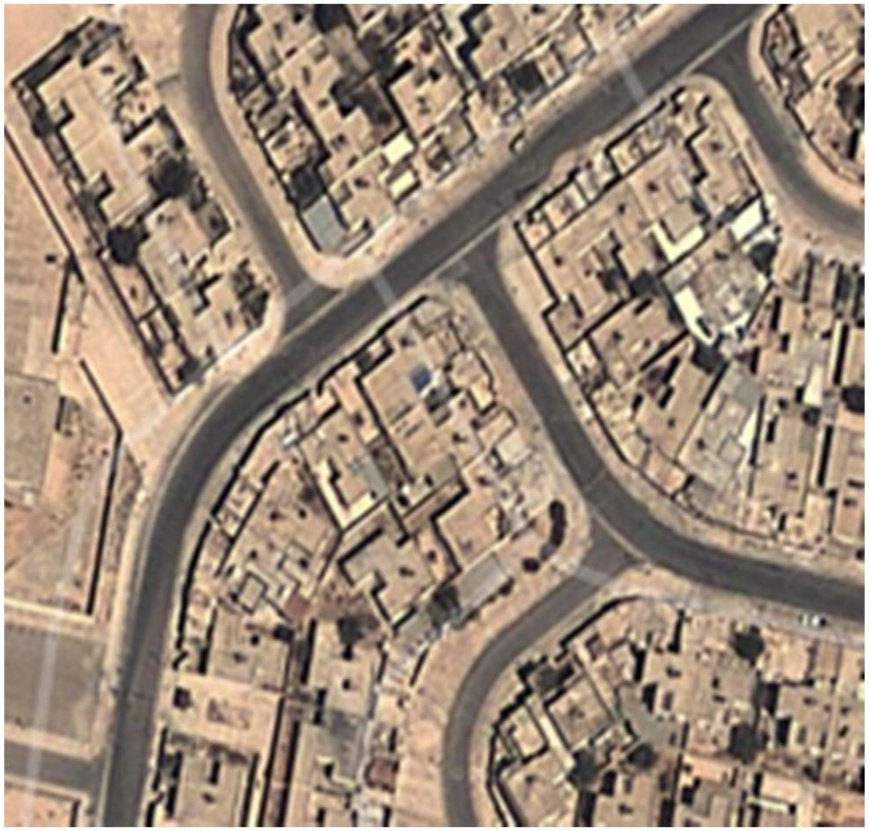
Technique – Geolocation through Eyeballing





Technique – Geolocation through Eyeballing



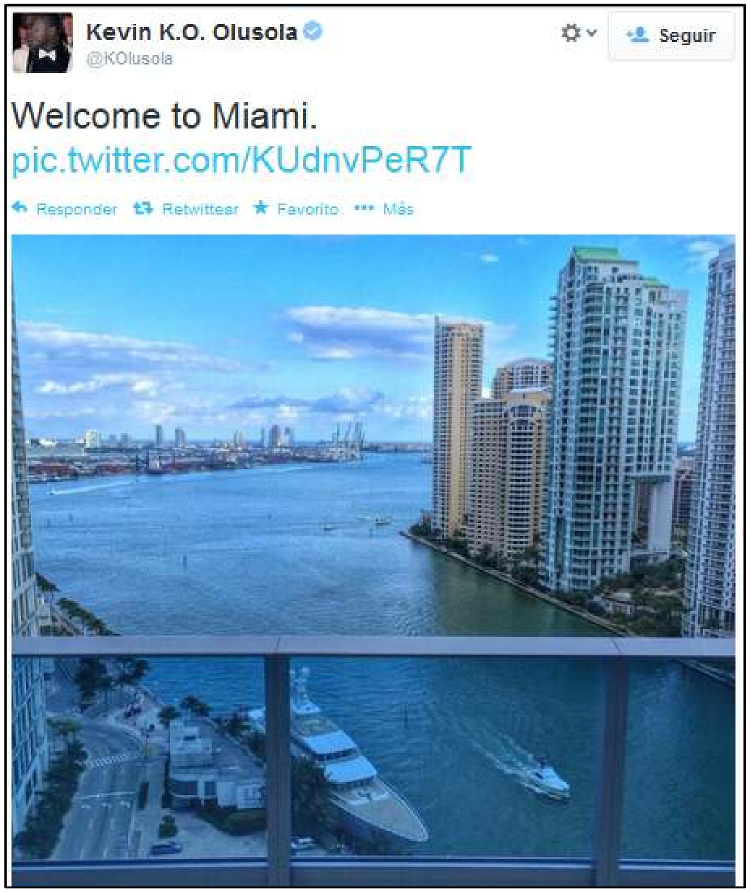


Technique – Geolocation through Eyeballing

- IOActive Labs Research show how to geolocate hotel location through window view photos[1], even down to the exact room.

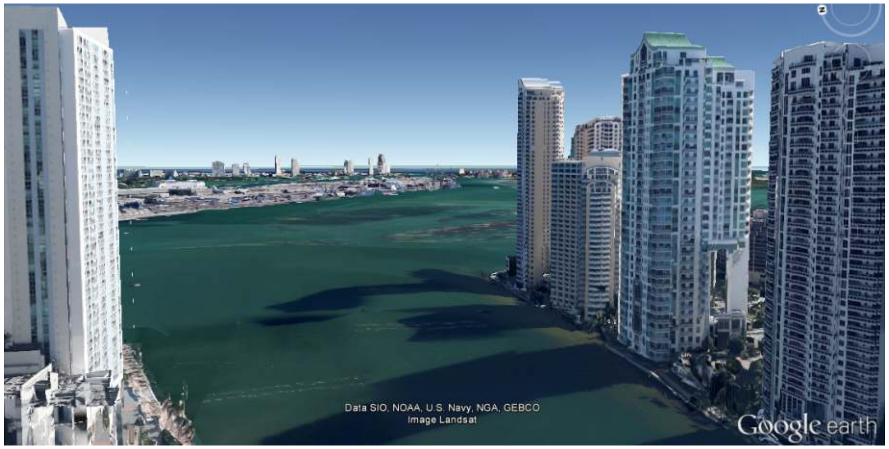
[1] http://ow.ly/CuFGA

Technique – Geolocation through Eyeballing



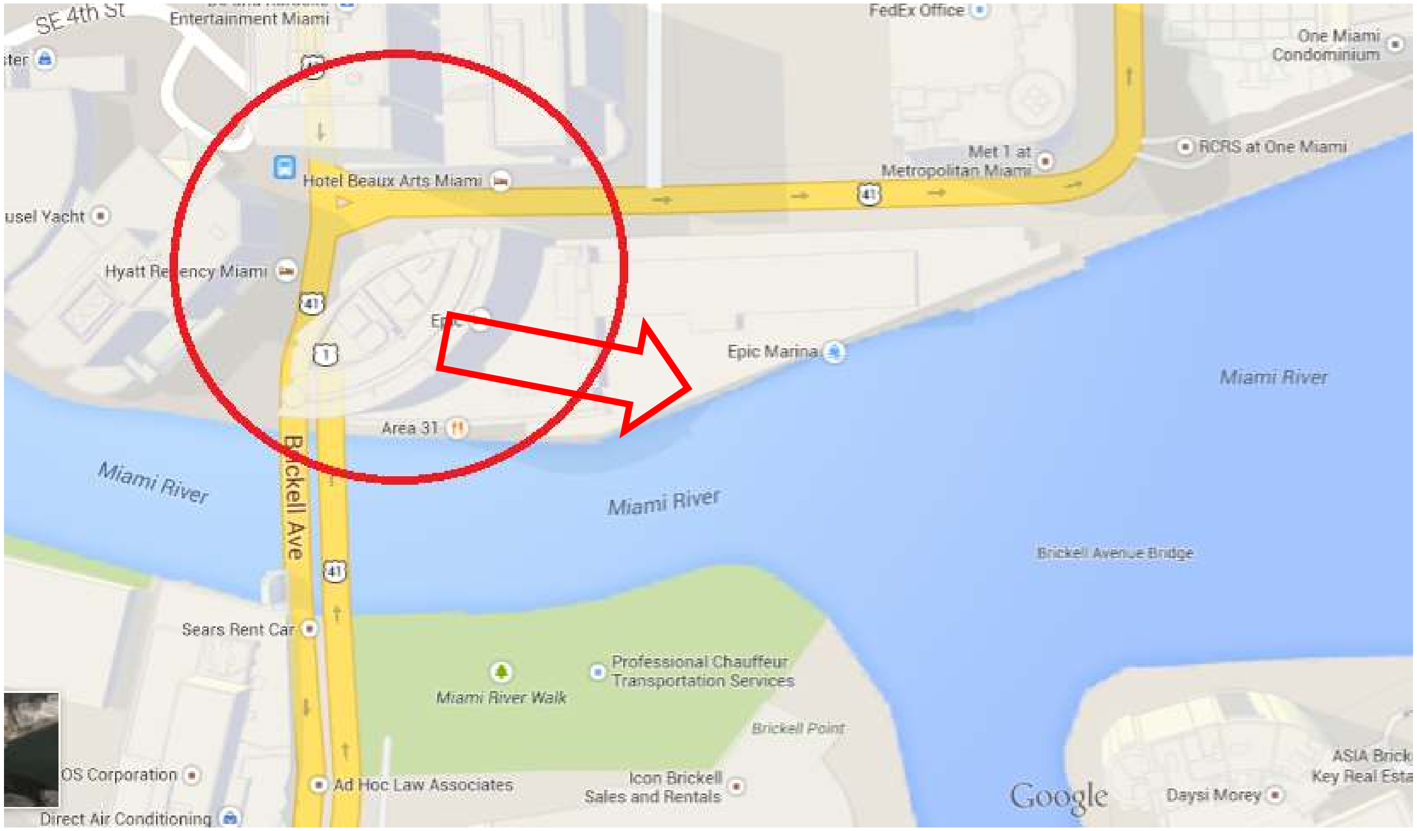
Kevin K.O. Olusola
@KOlusola

Welcome to Miami. pic.twitter.com/KUdnvPeR7T



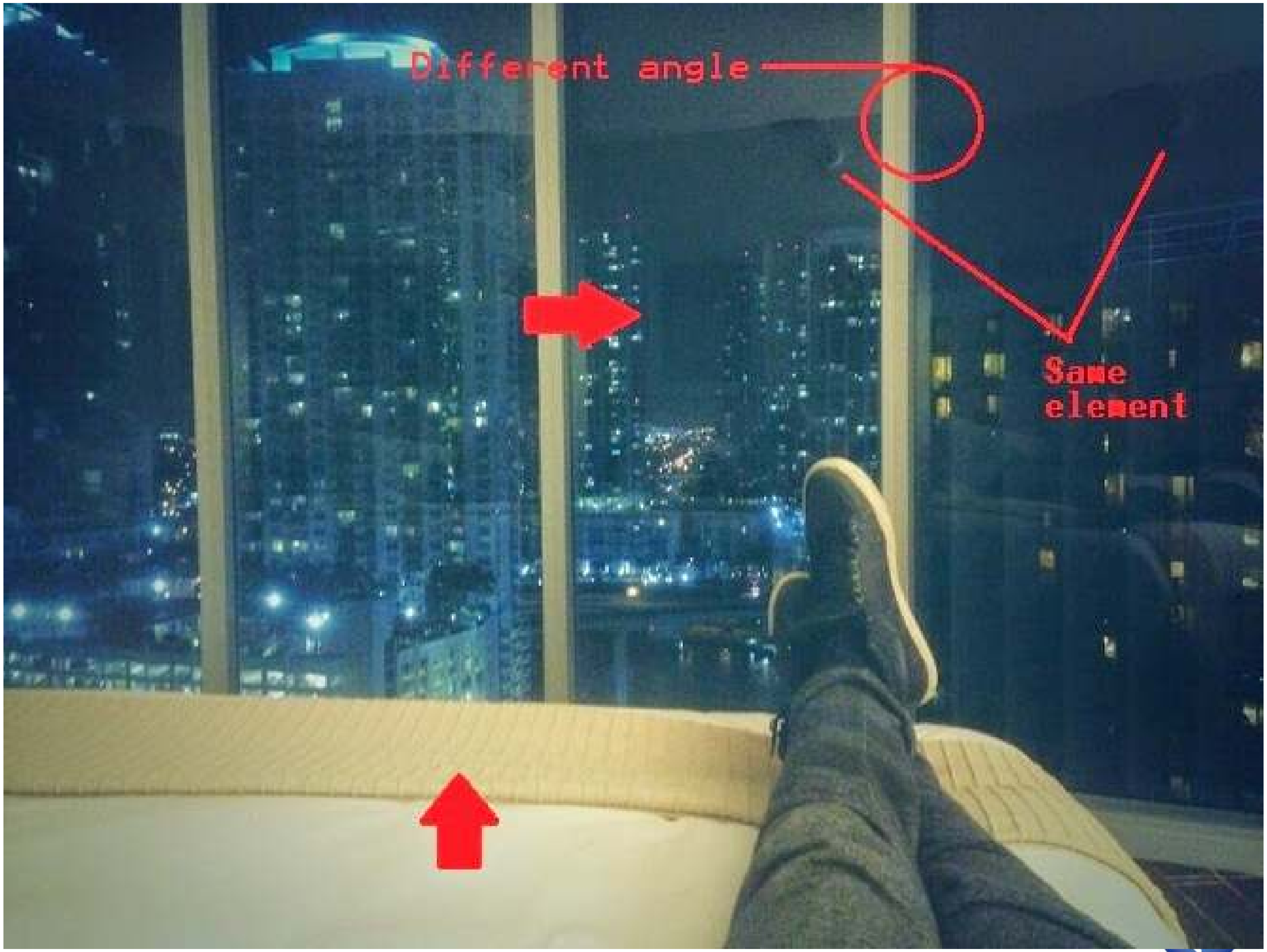
saltbushgroup

Technique – Geolocation through Eyeballing



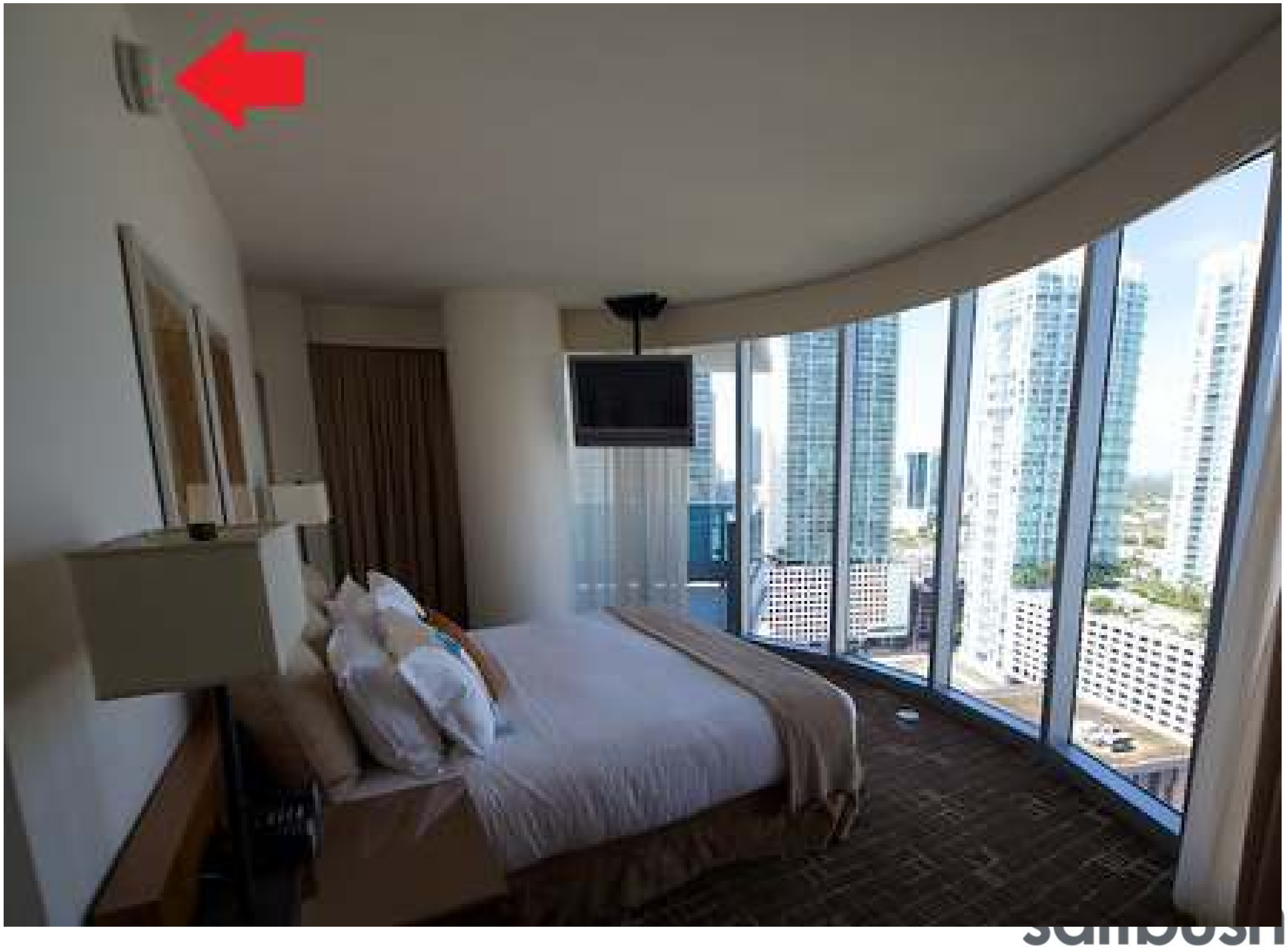
saltbushgroup

Technique – Geolocation through Eyeballing



Technique – Geolocation through Eyeballing

- Using Foursquare and TripAdvisor…



Questions?

- Robert "Bull" Winkel
- @RobertWinkel
- http://ow.ly/Ce87f

saltbushgroup