IMMAGINI DIGITALI: VERITÀ E BUGIE

alessandro tanasi (@jekil)

HACKLAB BITM

TRUE OR FALSE?

Umberto Smaila


TRUE

FALSE

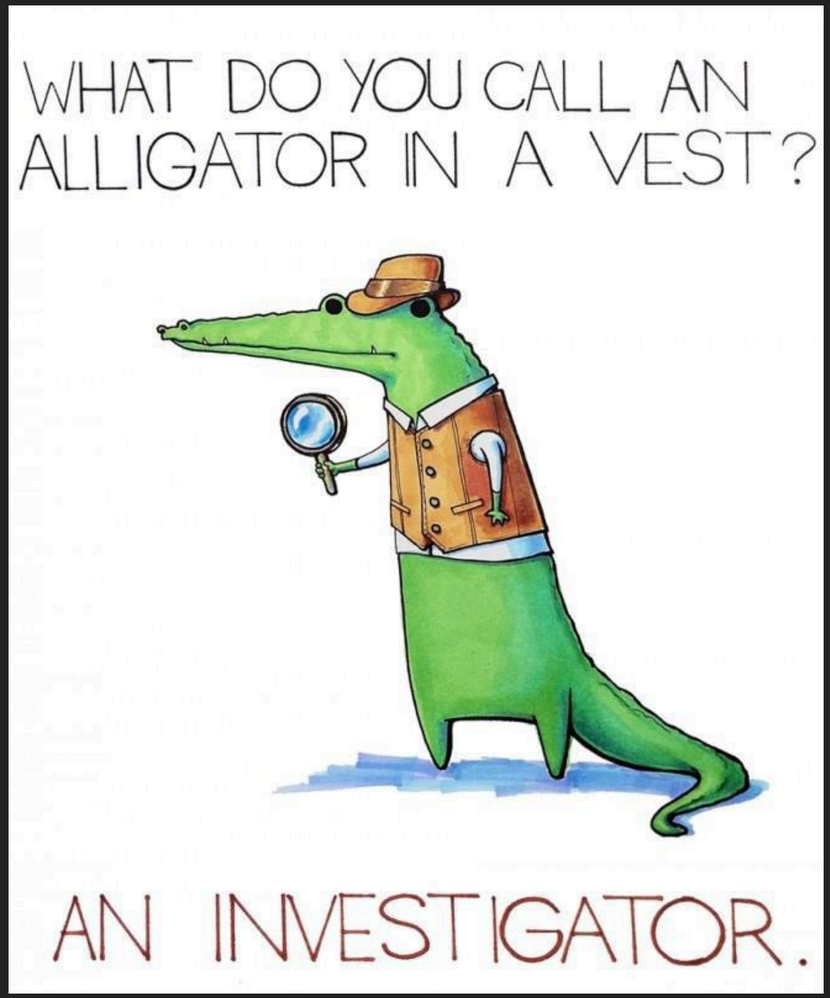

DOUBLE FACEPALM
FOR WHEN ONE FACEPALM DOESN'T CUT IT

IMAGES ARE EVERYWHERE

- Manipulating digital photos is **easy**. Detecting it can be **hard**.
- Many formats, many sources (photo, website, social, whatever).
- **Seeing** is not **believing**.
- Sometimes you need to **trust** images:
  - Journalism, investigation, law enforcement, etc.

IMAGE FORENSICS

- Forensic Image Analysis is the application of **image science** and domain expertise to interpret the content of an image and/or the image itself.
- Image Authentication to the rescue.
- People should understand how much a media content is trusted.
- Is it ever possible to be **100%** sure ?

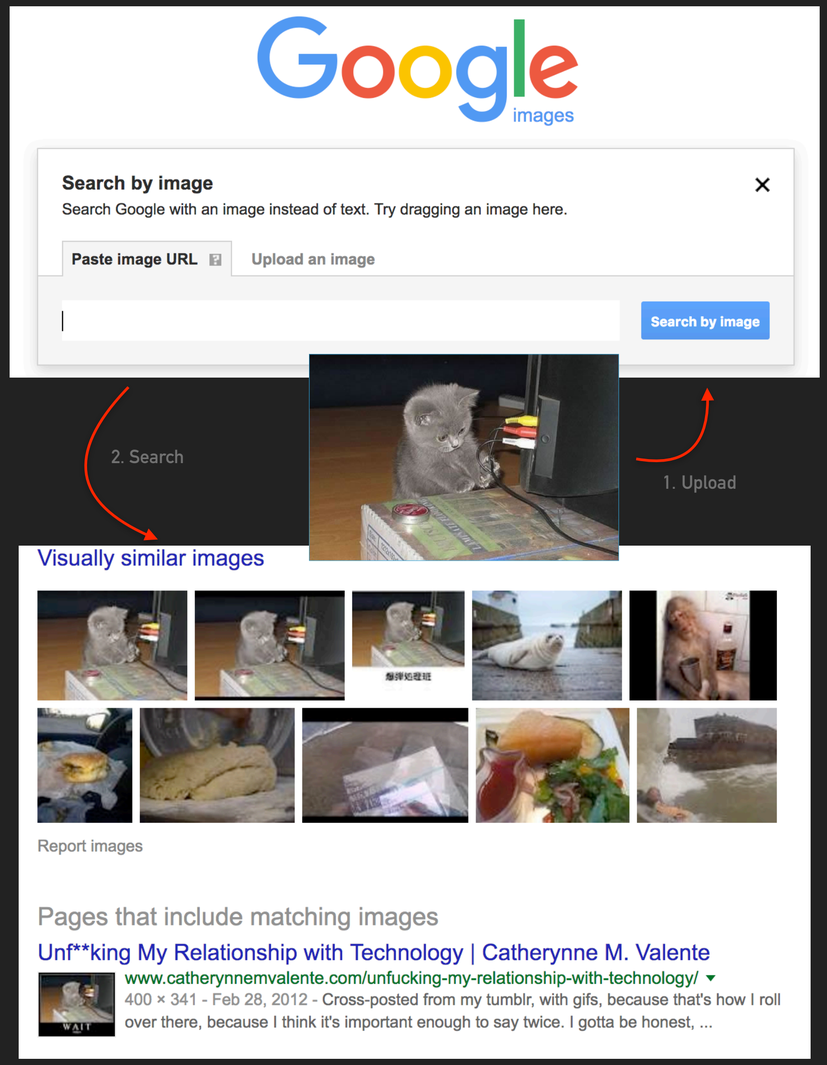


HOW TO SPOT A FAKE IMAGE?

TECHNIQUES

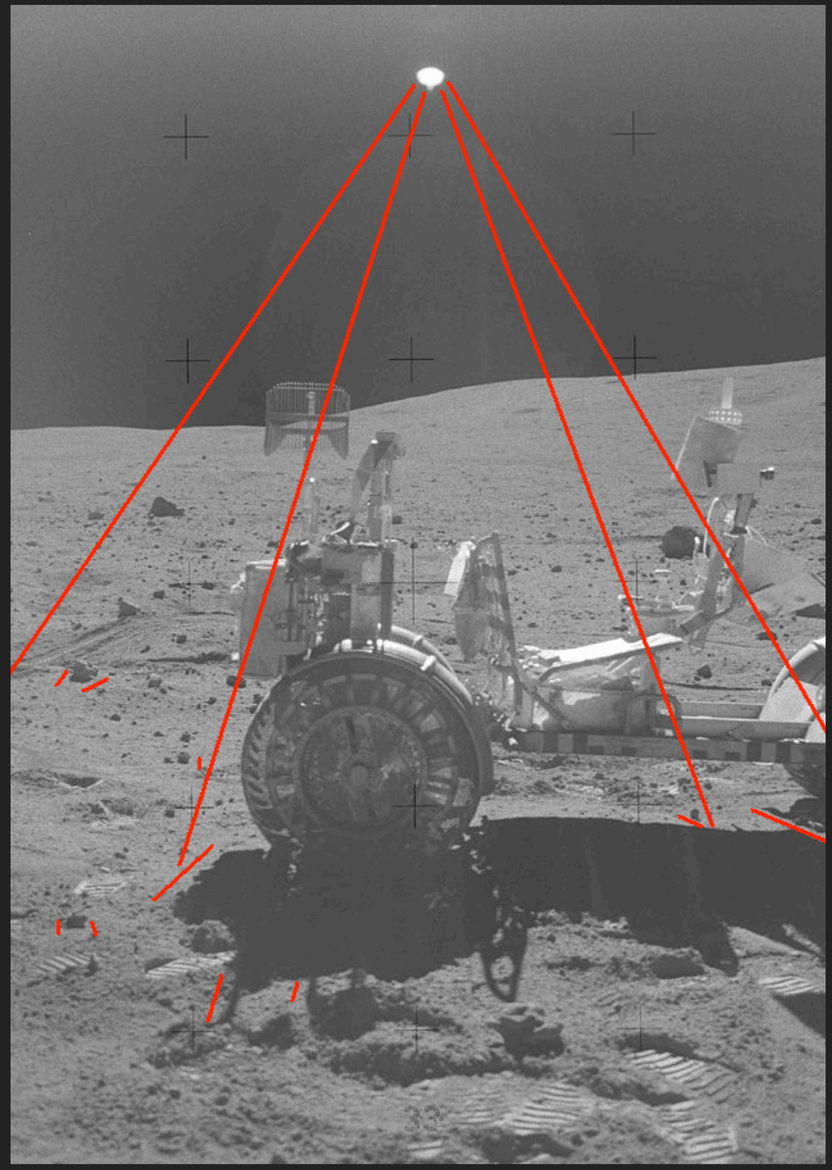
REVERSE IMAGE SEARCH

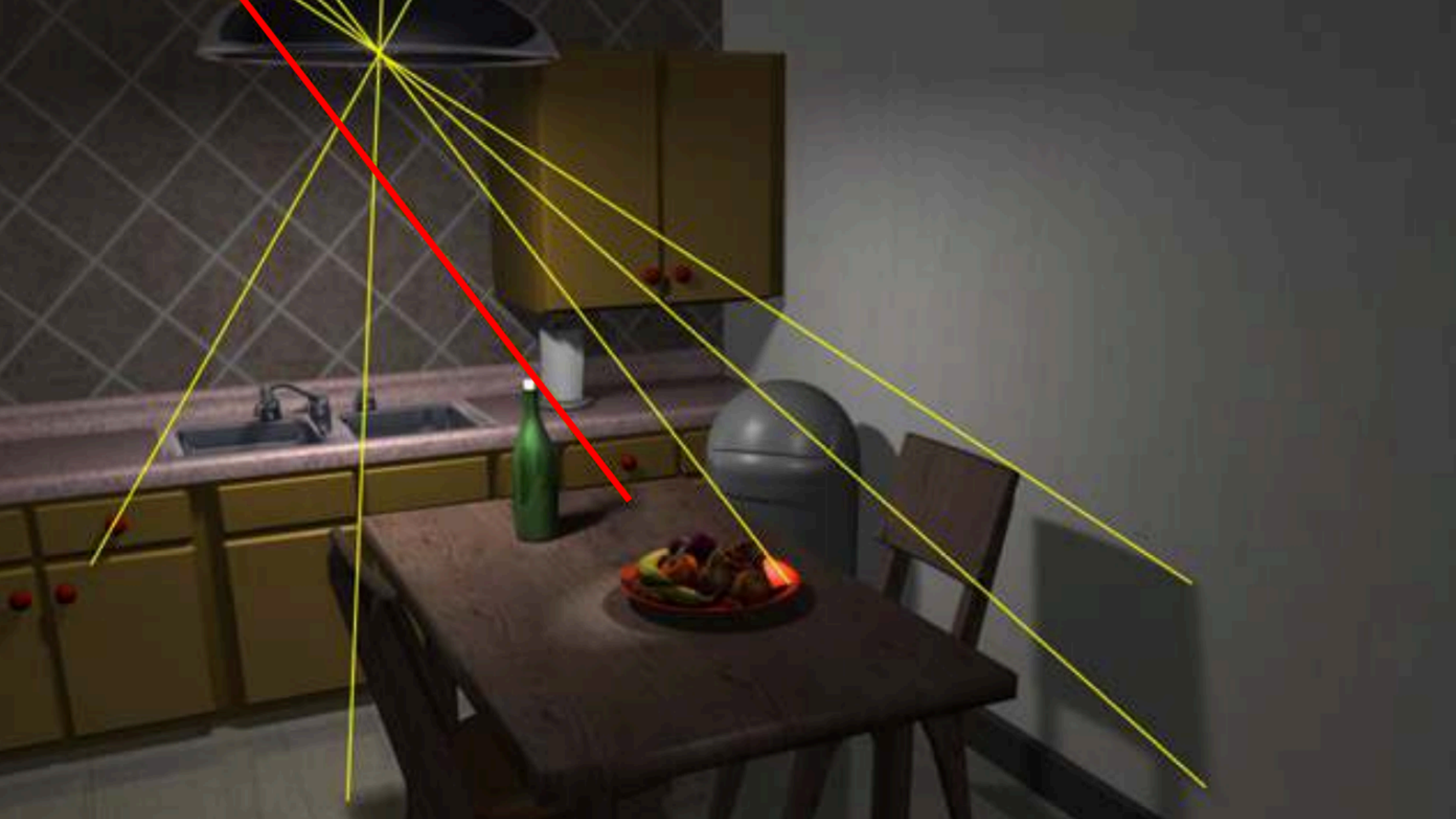
- Are you looking at the **original** version?
- Most of the image or a small part (cropped image) may be on the Internet .
- Reverse **search**:
  - Google Images
  - TinEye
  - Bing, Baidu, Yandex, etc.

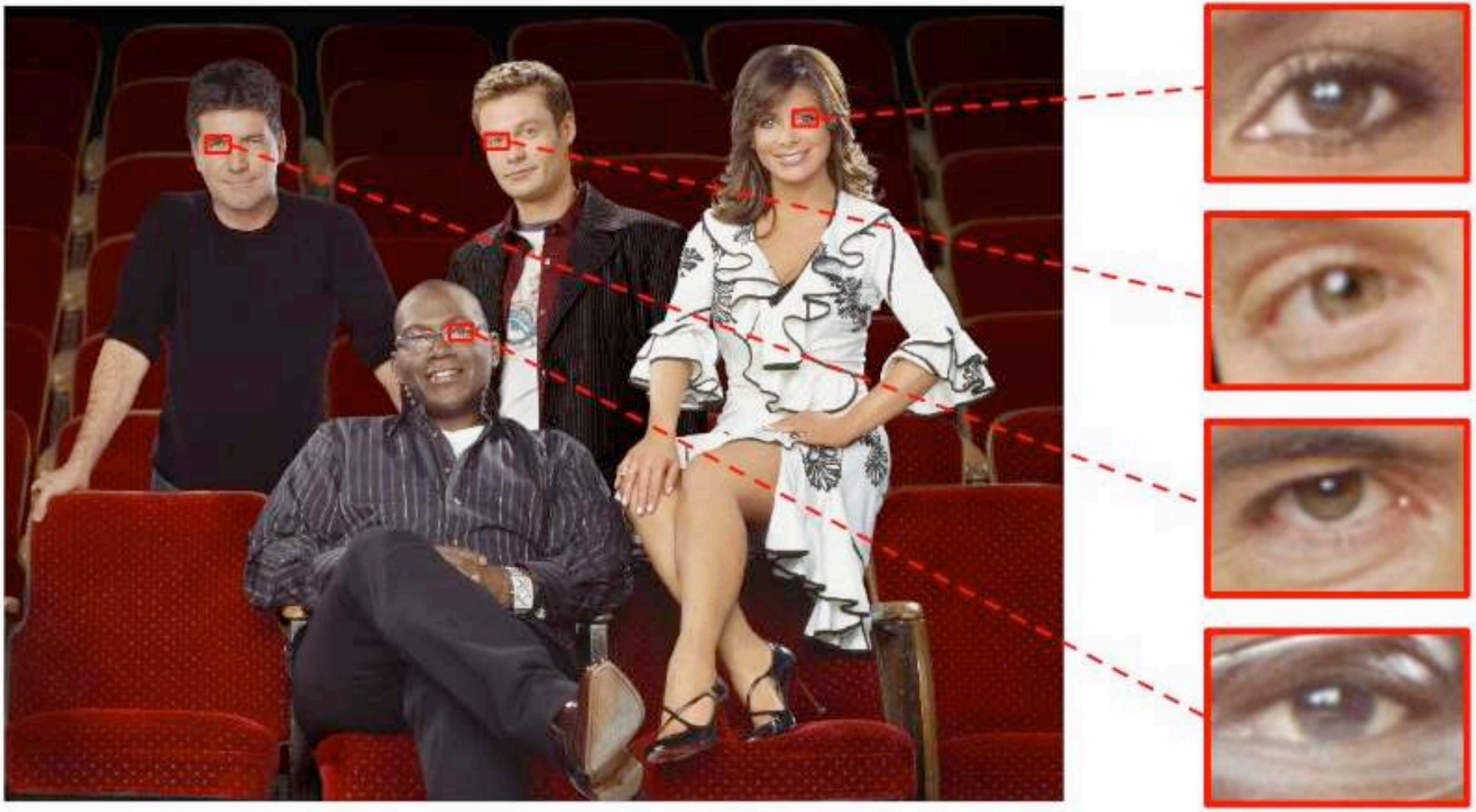


SHADOWS & REFLECTIONS

- Carefully analyse the position of **light** sources for inconsistencies.
- **Ray tracing** objects and their shadows / reflections.
- Trace **shadow** lines, look for absence of shadows
- Check **eye** reflections, eye orientation, **face** details.
- Vanishing points, distances within the image and 3D models.





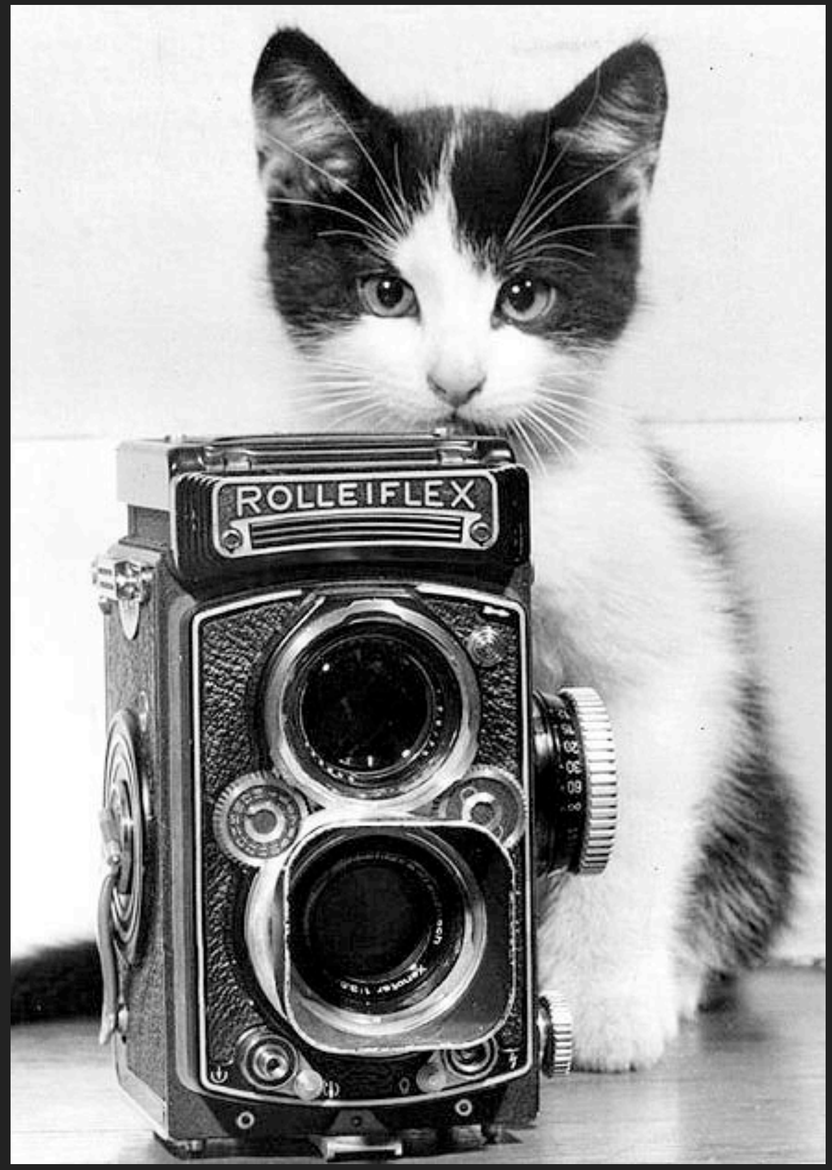


LOCATION

- Corroborate the **location**, date and approximate time the image was taken.
- **Cross** reference: weather, landmarks, plates, etc.
- Google Street is your friend.
- Get location from metadata.
- Details screw your **OPSEC**.

CAMERA FINGERPRINTING

- Compression schemes, Huffman tables, etc. can be used to **fingerprint** the camera or software program that created the image.
- Quantisation[1] matrices and Huffman tables can be used to fingerprint the image creator.
- **Lens** distortion or aberrations.
- Image **sensor**: fixed pattern noise and colour filter defects.



1. http://impulseadventure.com

METADATA

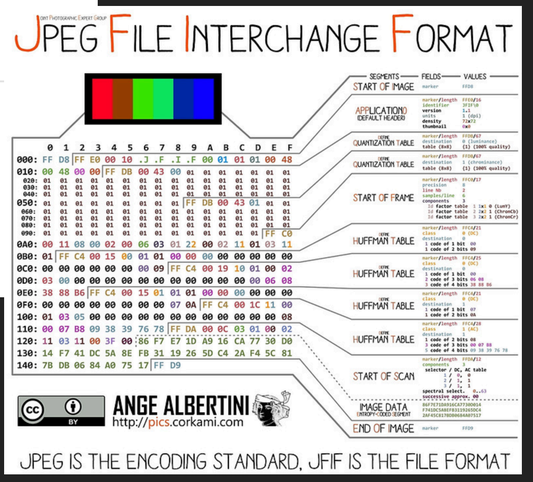
- Metadata (EXIF, XMP, IPTC) can **contain** useful information:
  - Geolocation, thumbnails, editing trails, timestamp, etc.
- **Custom** tags (by vendor).
- Fingerprinting camera by vendor metadata.
- Fusking: filenames.

YResolution: 300
ResolutionUnit: inch
ExifTag: 296
Copyright: Jeffrey Friedl
Artist: Jeffrey Friedl
Make: NIKON CORPORATION
GPSTag: 898
DateTime: 2012:11:12 21:47:45
YCbCrPositioning: Centered
XResolution: 300
Model: NIKON D4
Software: Adobe Photoshop Lightroom 4.3 (Macintosh)

InteroperabilityIndex: R98
InteroperabilityVersion: 1.00

YResolution: 72
ResolutionUnit: inch
Compression: JPEG (old-style)
XResolution: 72
JPEGInterchangeFormatLength: 25539
JPEGInterchangeFormat: 1106

GPSLatitudeRef: North
GPSLatitude: 35deg 9' 44.292"
GPSVersionID: 2.3.0.0
GPSLongitudeRef: East
GPSLongitude: 136deg 16' 48.324"



MAT HONAN GEAR 12.03.12 05:02 PM

OOPS! DID VICE JUST GIVE AWAY JOHN MCAFEE'S LOCATION WITH PHOTO METADATA?

John McAfee and Vice editor in chief Rocco Castoro. *Photo: Robert King/VICE*

Geotagging nei metadata EXIF.

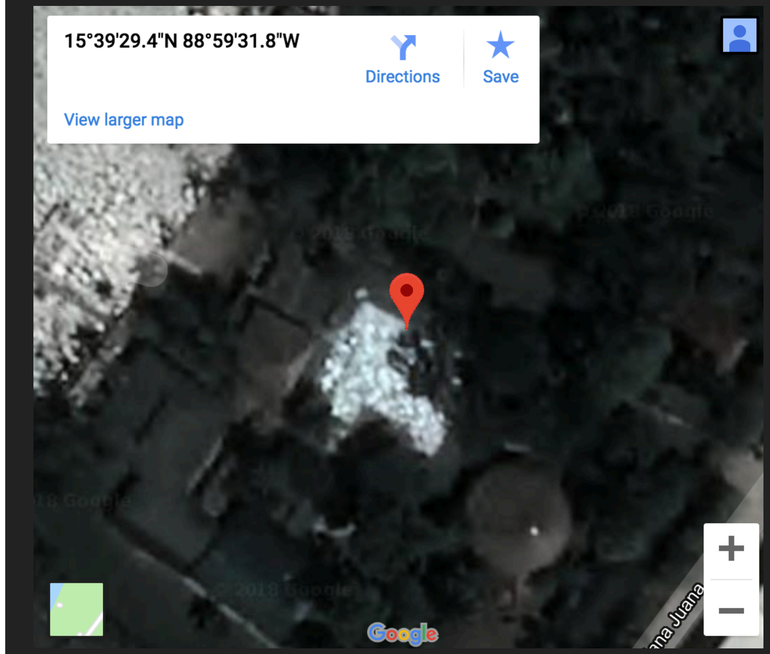
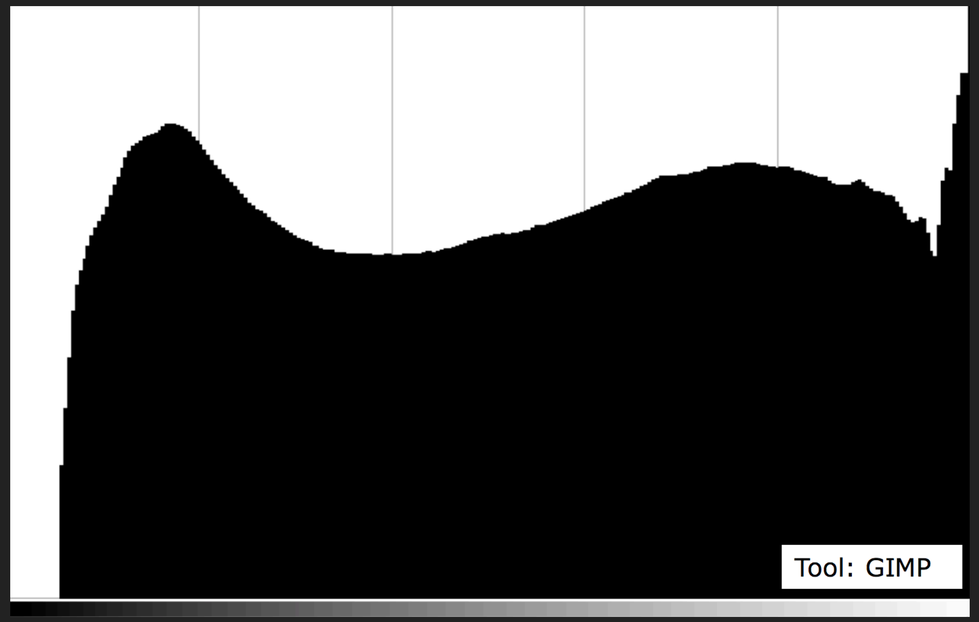


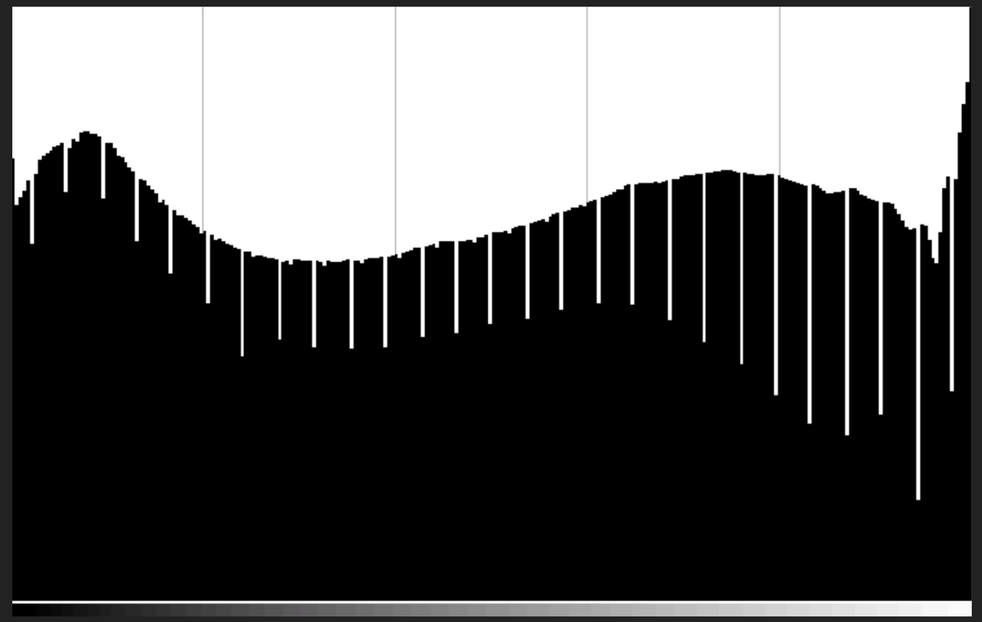
IMAGE PROPERTIES

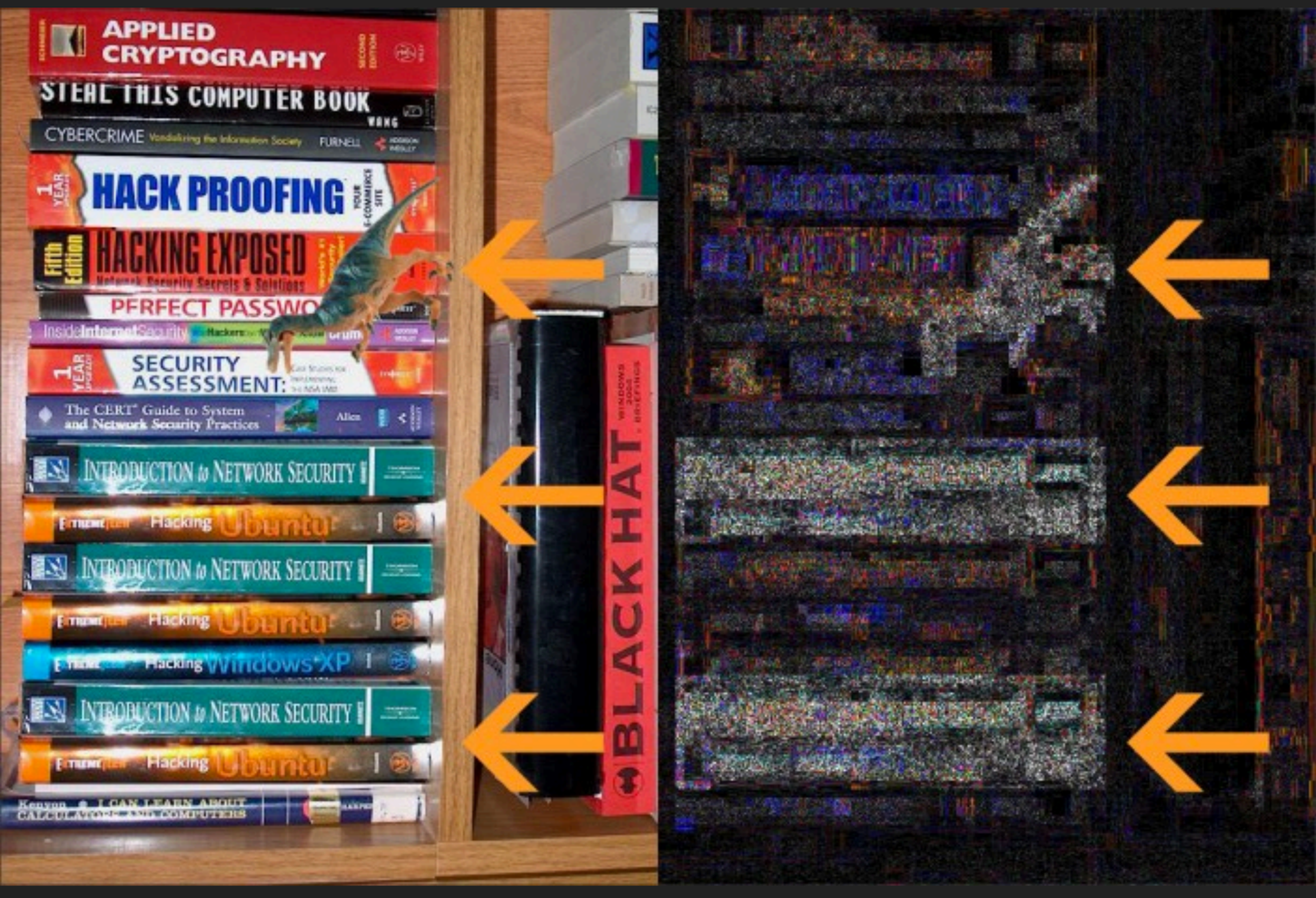
- Clone detection.
- **Histogram** Analysis (detecting colour manipulation).
- Error Level Analysis (**ELA**).
- Luminance Gradient (backgrounds are artificially enhanced).


1

2


Tool: GIMP




APPLIED CRYPTOGRAPHY
STEAL THIS COMPUTER BOOK
CYBERCRIME
HACK PROOFING
HACKING EXPOSED
SECURITY ASSESSMENT:
The CERT Guide to System and Network Security Practices
INTRODUCTION to NETWORK SECURITY
Hacking Ubuntu
INTRODUCTION to NETWORK SECURITY
Hacking Ubuntu
Hacking Windows XP
INTRODUCTION to NETWORK SECURITY
Hacking Ubuntu
BLACK HAT

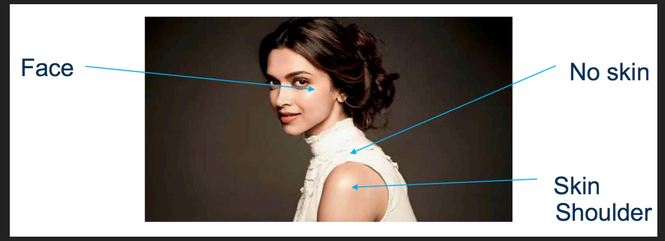
PROTECT THE AUTHENTICITY

- Methods for **authentication**, tamper detection, and robustness against different image processing operations.
- Digital **signature** / crypto.
- **Watermarking**.
  - Many color laser printers embed secret information in every page they print[1].

1. http://www.eff.org/Privacy/printers/docucolor/

TONS OF STUFF

- Image **censorship** and reversing.
- Image **classification** and ML.
- Facial recognition and biometrics.



GOT WEAPONS

TOOLS

TOOLS

- Commercial Tools / Free and Open Source Tools:
  - Ghiro[1] - full image forensics framework.
  - Jpegsnoop[2] - uses EXIF data, quantisation matrices, Huffman tables to assess what created the image.
  - Phoenix[3] - small image forensics tool that can run some common analyses on images.

1. http://www.getghiro.org
2. http://www.impulseadventure.com/photo/jpeg-snoop.html
3. https://github.com/ebemunk/phoenix

IMAGE VERIFICATION CHECKLIST

- Reverse image search.
- Check for image physics.
- Metadata analysis.
- Geolocation.
- Fingerprint camera / software / creator.
- Check for watermark / hidden data
- Do you know who, where, when, why the photo was captured?
- Search for a “second shooter”.

QUESTIONS ?

No kittens were harmed in the production of this slideshow.

@jekil

alessandro@tanasi.it