MAGINI DIGITALI: VERITĂ E BUGIE alessandro tanasi (@jekil)

= 50 mm

Nippon





Nikon

Japa

4000 AND

Nippon

TRUE OR FALSE?





Umberto Smaila





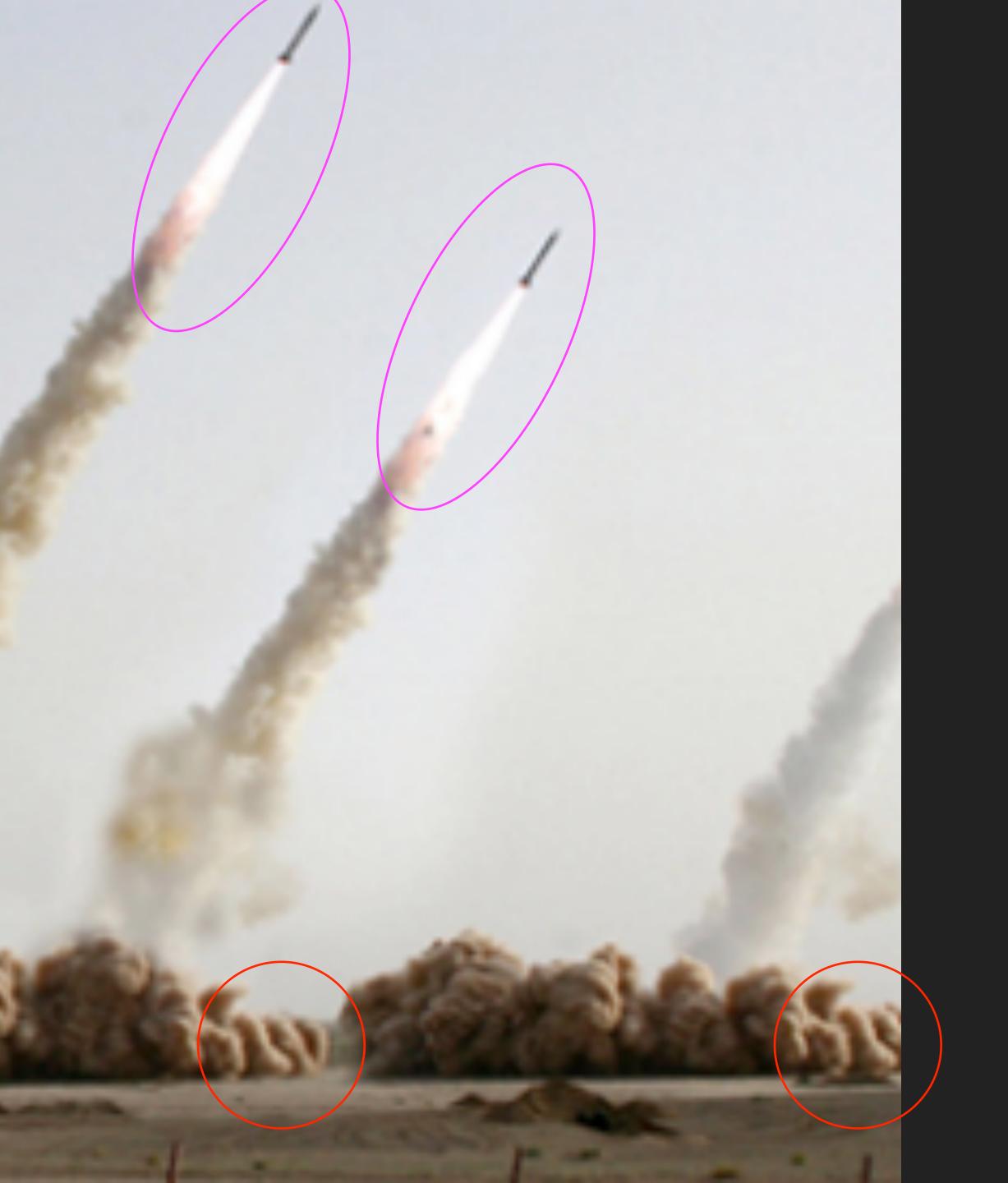
TRUE

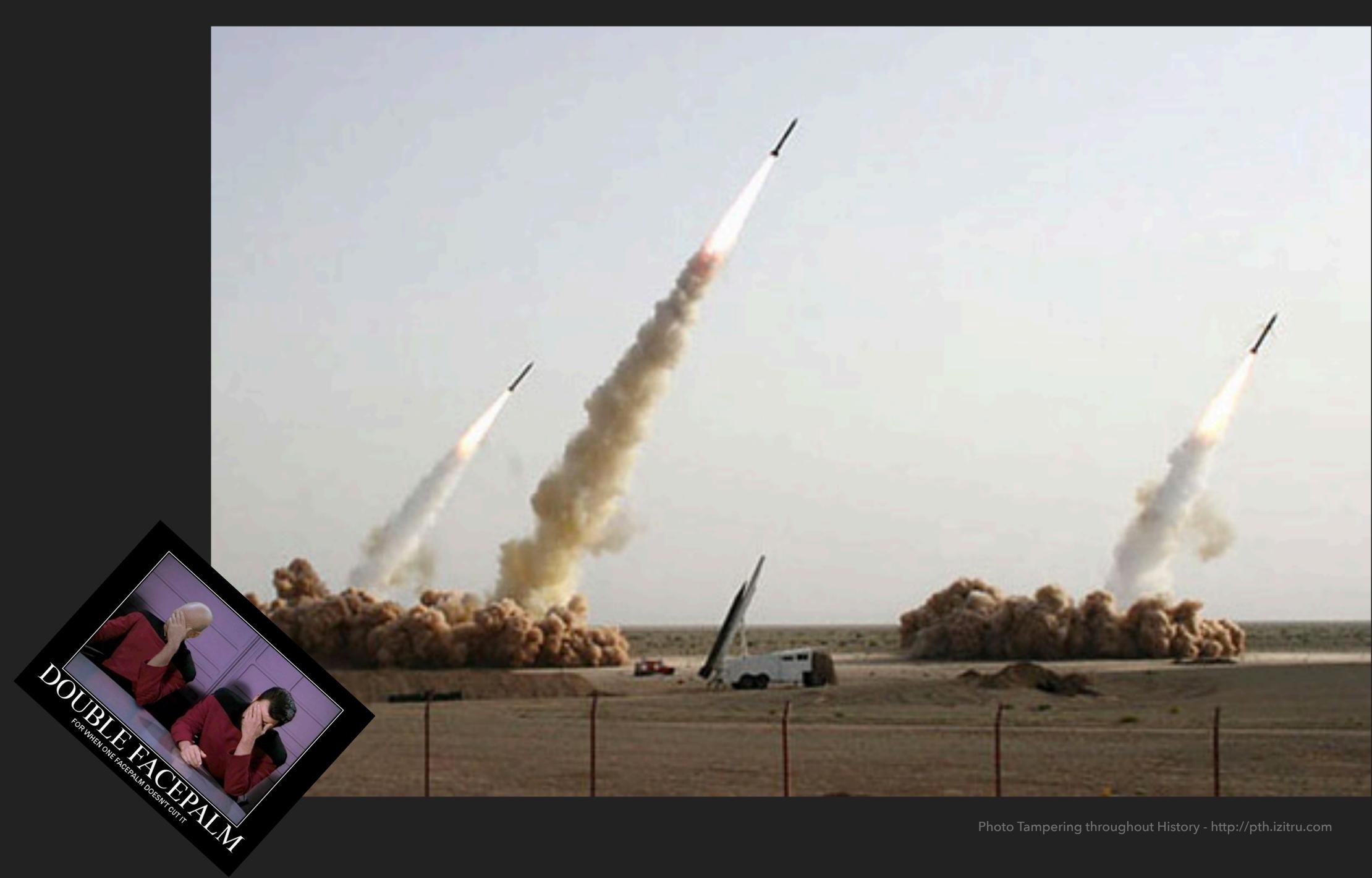






FALSE





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.

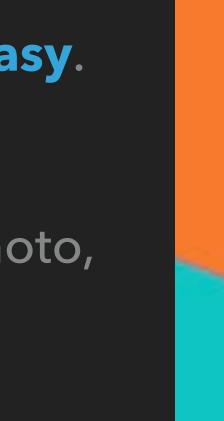
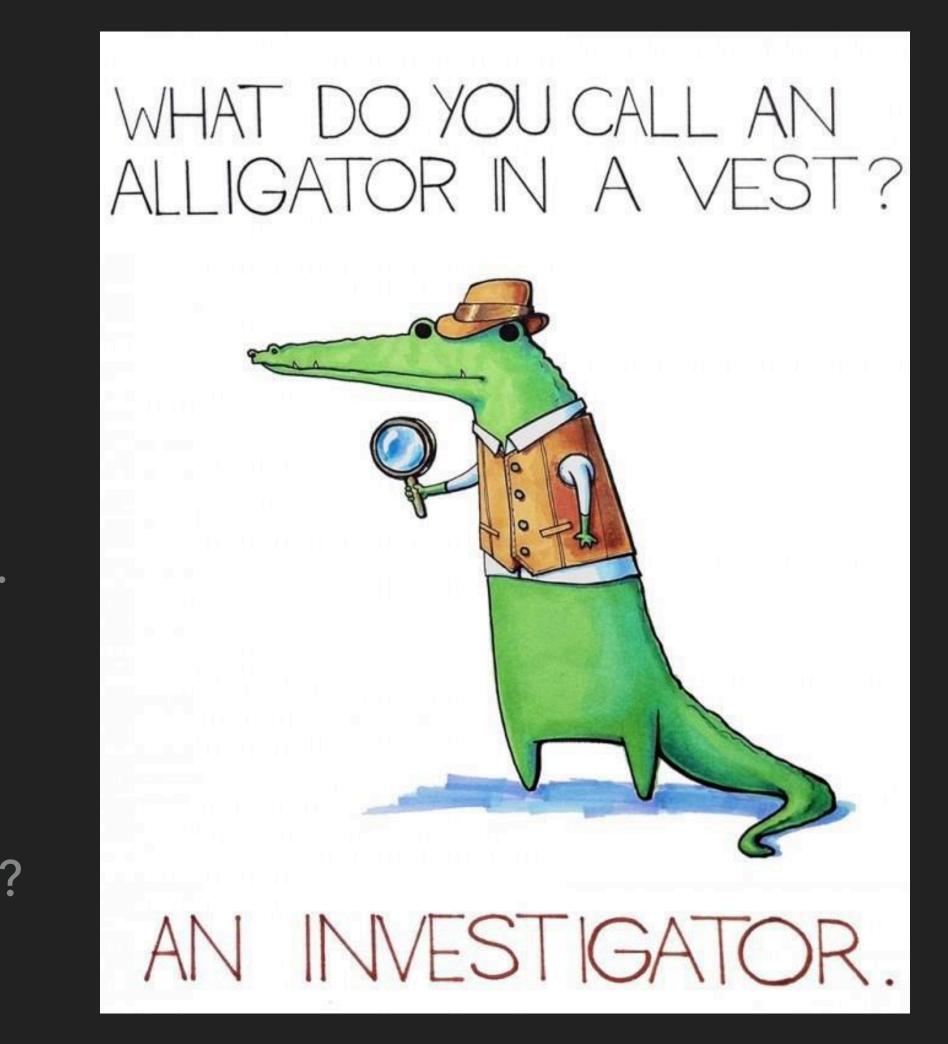




IMAGE FORENSICS

- 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 ?



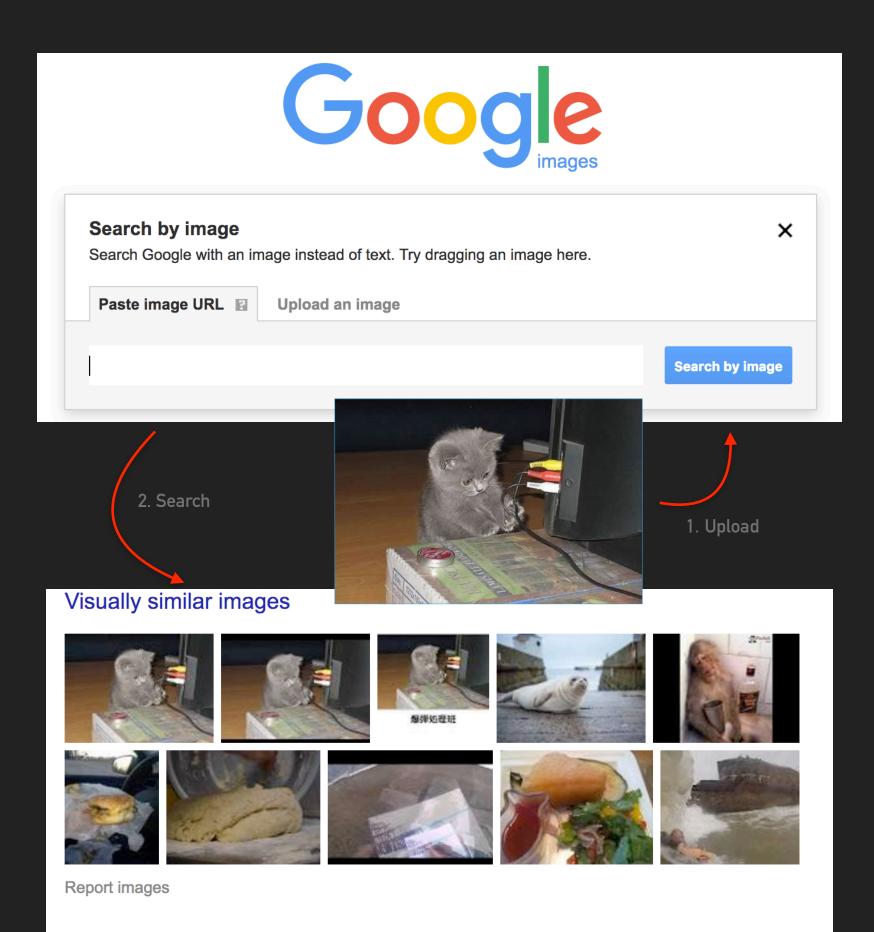


TECHNIQUES

HOW TO SPOT A FAKE IMAGE?

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.



Pages that include matching images

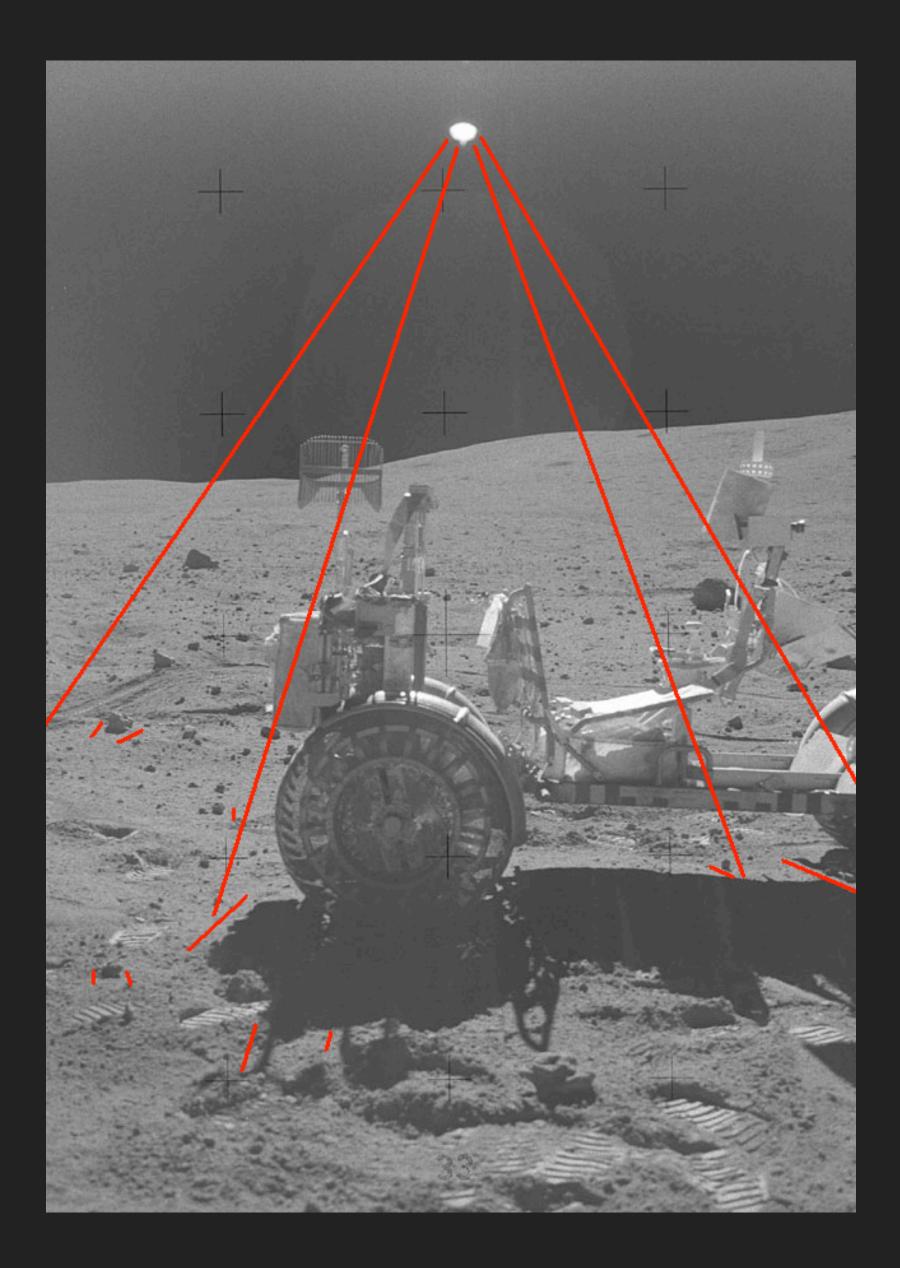
Unf**king My Relationship with Technology | Catherynne M. Valente

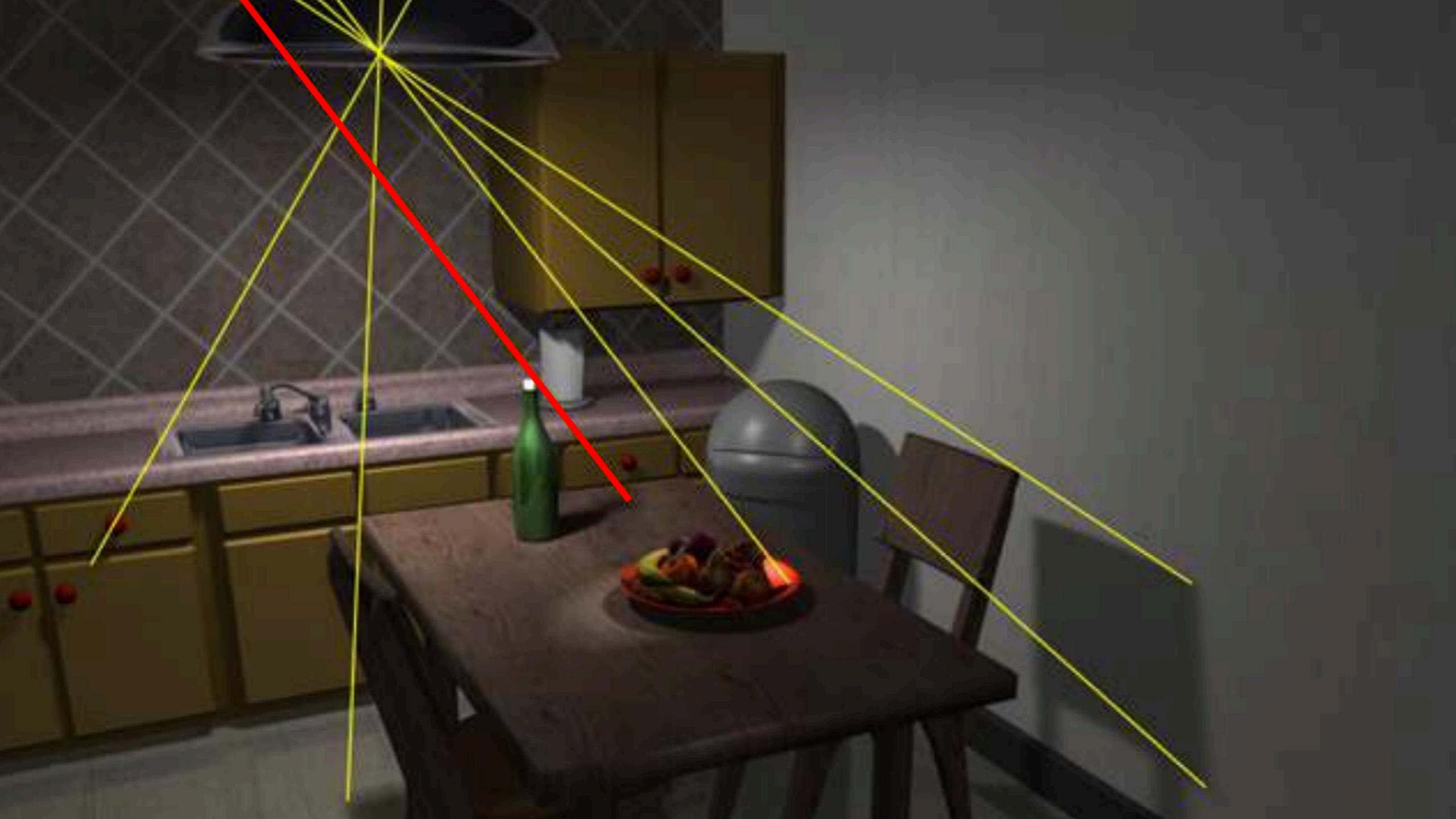


www.catherynnemvalente.com/unfucking-my-relationship-with-technology/ 400 × 341 - Feb 28, 2012 - Cross-posted from my tumblr, with gifs, because that's how I roll over there, because I think it's important enough to say twice. I gotta be honest, ...

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**.

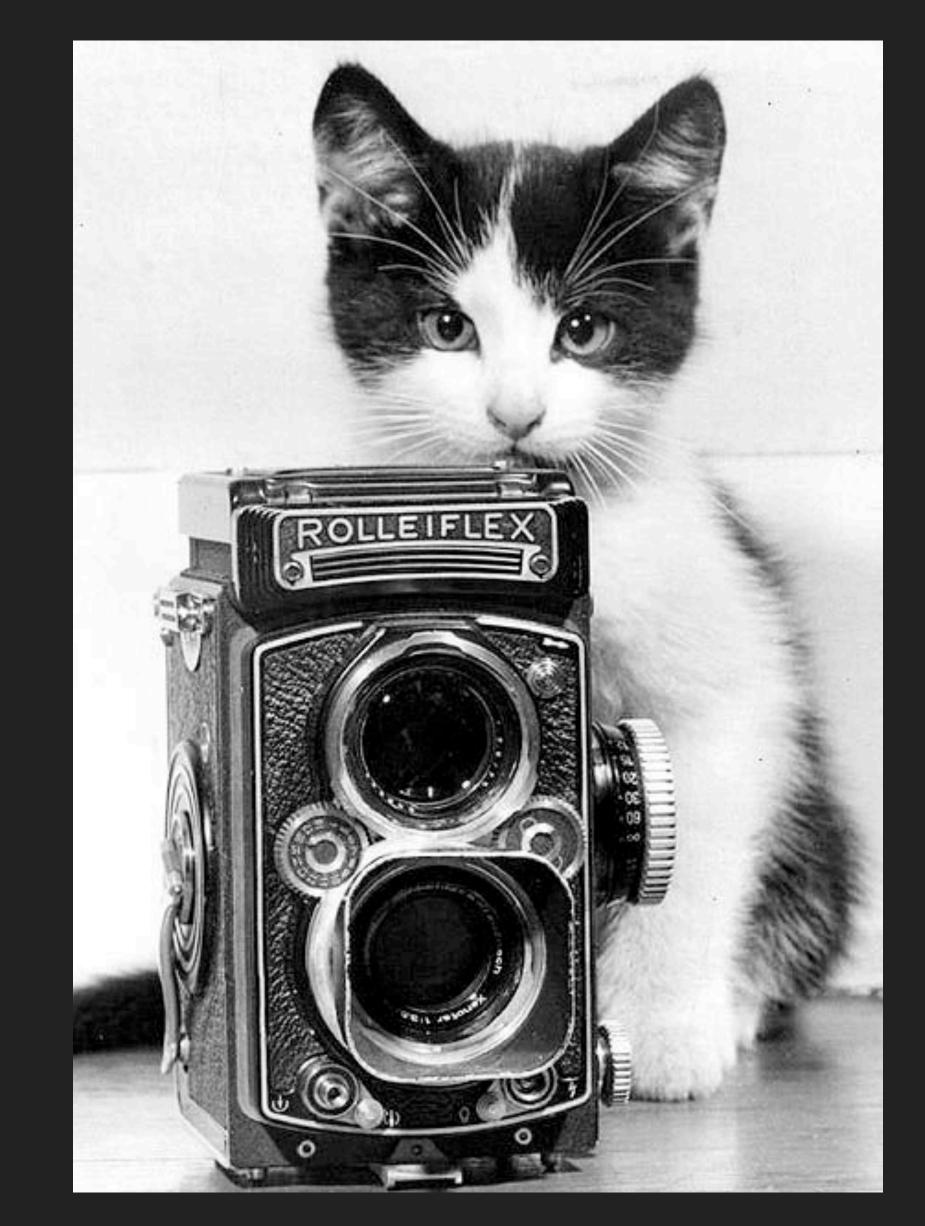






CAMERA FINGERPRINTING

- Compression schemes, Huffman tables, etc. can be used to fingerprint the camera or software program that created the image.
- Quantisation¹ 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.



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'

JPEG FILE INTERCHANGE FORMAT APPLICA START HUFFMA 0B0: 01 FF C4 00 15 00 01 01 00 00 00 00 00 00 00 00 00 9C0: 00 00 00 00 00 00 00 09 FF C4 00 19 10 01 00 02 HUFFMAN 0E0: 38 88 86 FF C4 00 15 01 01 01 00 00 00 00 00 00 HUFFMAN 0F0: 00 00 00 00 00 00 00 00 07 0A FF C4 00 1C 11 00 110: 00 07 B8 09 38 39 76 78 FF DA 00 0C 03 01 00 0 HUFFMA 120: 11 03 11 00 3F 00 86 F7 E7 1D A9 16 CA 77 30 D0 130: 14 F7 41 DC 5A 8E FB 31 19 26 5D C4 2A F4 5C 81 140: 7B DB 06 84 A0 75 17 FF D9 START C ANGE ALBERTINI IMAGE END OF

JPEG IS THE ENCODING STANDARD, JFIF IS TH

ENTS	FELDS	VALUES
TIONO HEADER)	marker/length identifier version units density thumbnail	FFE0/16 JFIF\0 1.1 1 (dpi) 72x72 0x0
ION TABLE	marker/length destination table (8x8)	FFDB/67 0 (luminance) {1} (100% quality)
TION TABLE	marker/length destination table (8x8)	FF08/67 1 (chrominance) {1} (100% quality)
F FRAME	marker/length precision line Nb samples/line components Id factor ta Id factor ta Id factor ta	8 2 6 3 able 1 1x1 0 (LunY) able 2 2x2 1 (ChronCb)
N TABLE	marker/length class destination 1 code of 1 t 1 code of 2 t	0 (DC) 0 bit 00
N TABLE	marker/length class destination 1 code of 1 t 2 code of 3 t 3 code of 4 t	\$\$C4/25 0 (DC) 0 0 0 0 0 0 0 0 0 0 0 0 0
N TABLE	marker/length class destination 1 code of 1 t 1 code of 2 t	FFC4/21 0 (DC) 1 bit 07
N TABLE	marker/length class destination 1 code of 2 to 3 code of 3 to 5 code of 4 to	1 (AC)
F SCAN	3/	3 C, AC table 3, 0 1, 1
DATA DED SEGMENT	spectral selec successive app 86F7E71DA916C/ F741DC5A8EF831 2AF45C8178D800	ct. 063 prox. 00 177300014 1192650C4
MAGE	marker	1109

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.

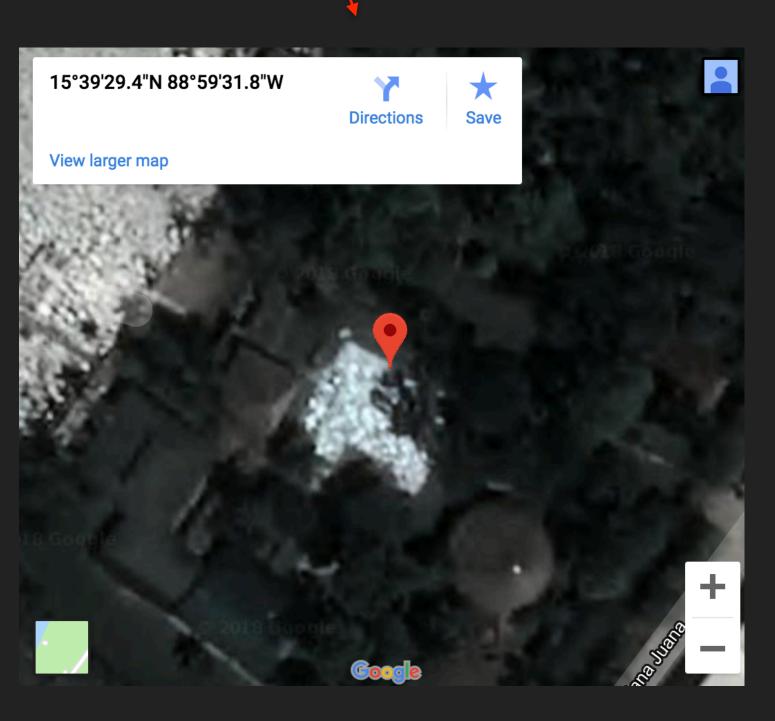
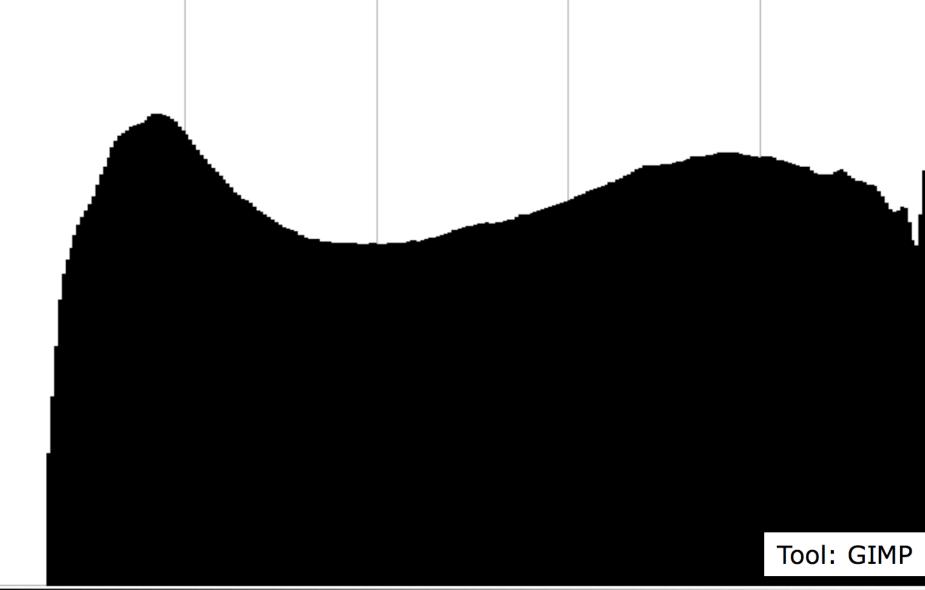


IMAGE PROPERTIES

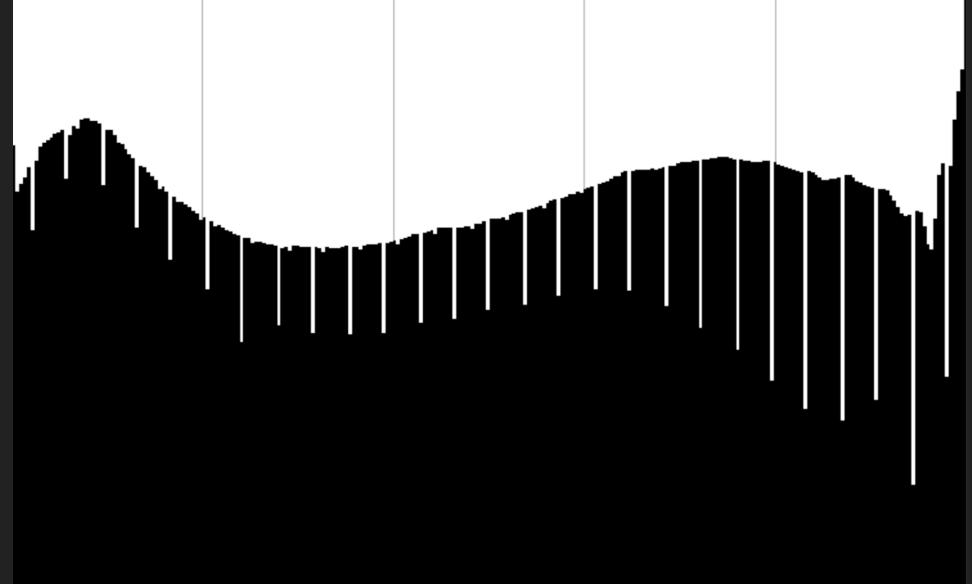
- Clone detection.
- Histogram Analysis (detecting) colour manipulation).
- Error Level Analysis (ELA).
- Luminance Gradient (backgrounds) are artificially enhanced).

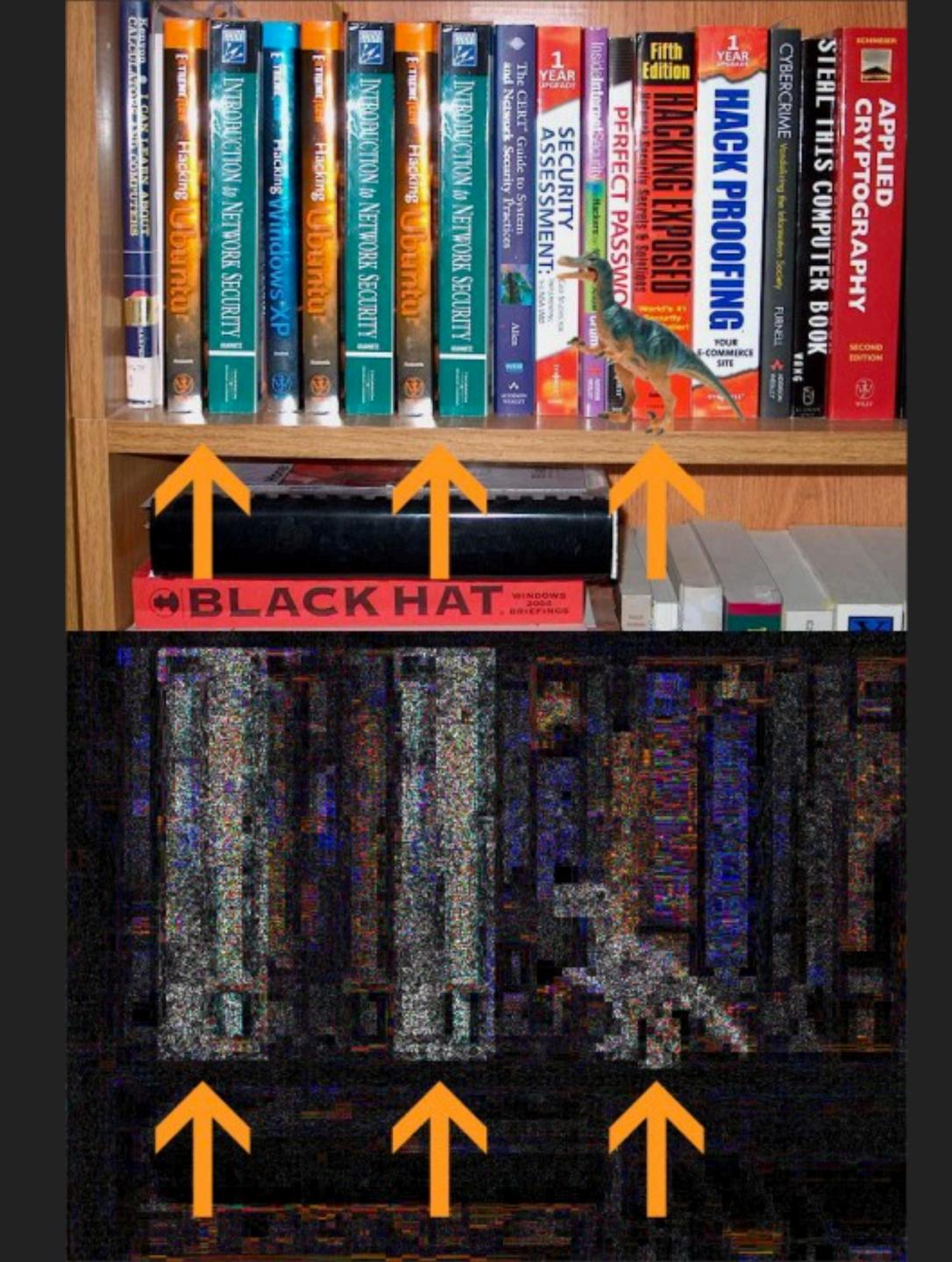
























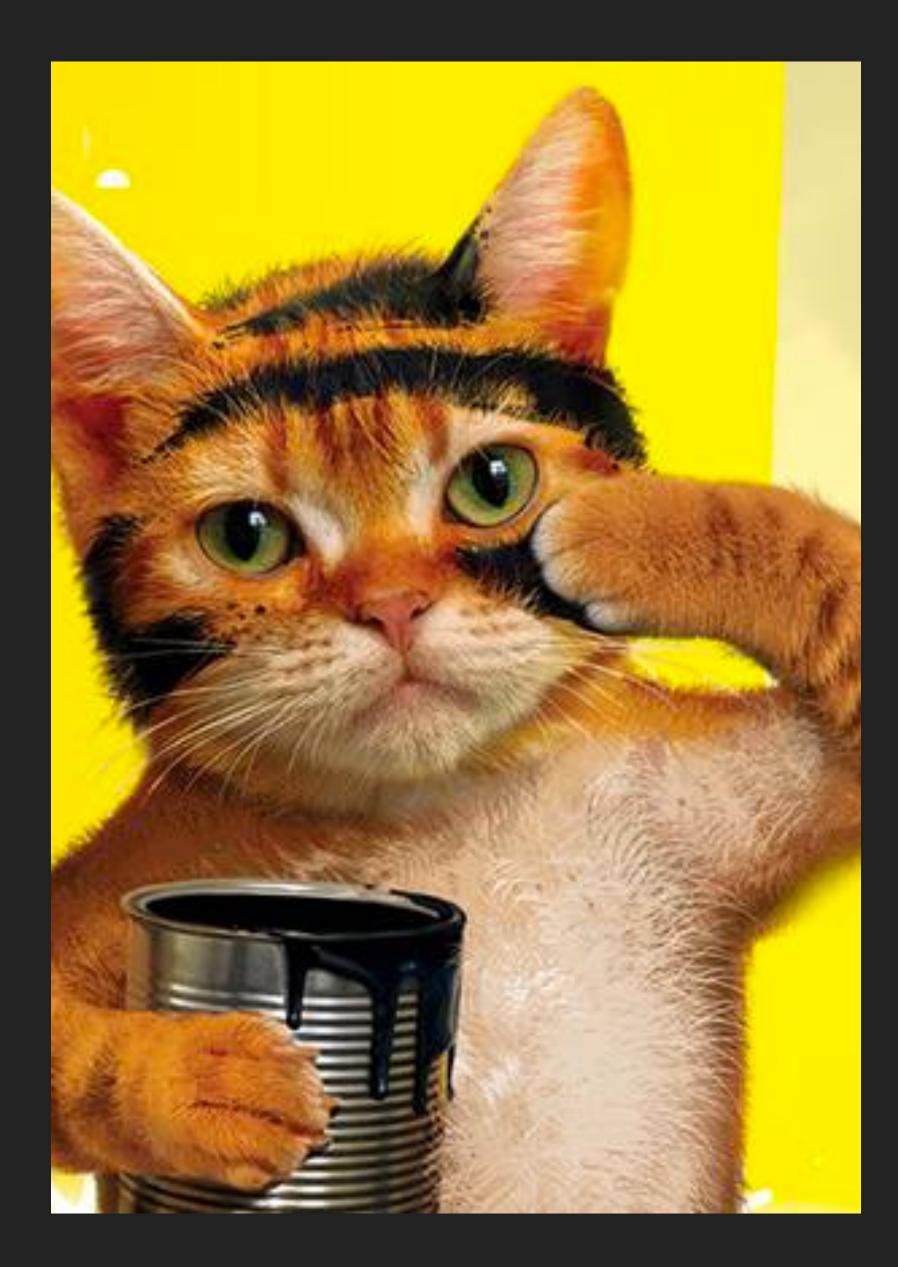


PROTECT THE AUTHENTICITY

- 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 print¹.



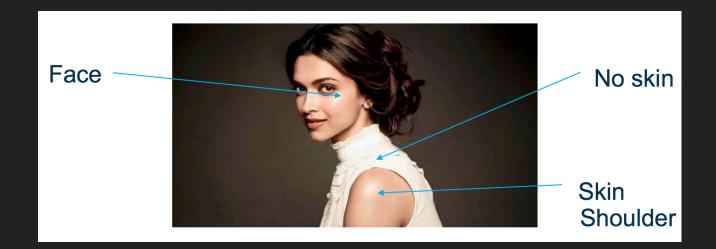


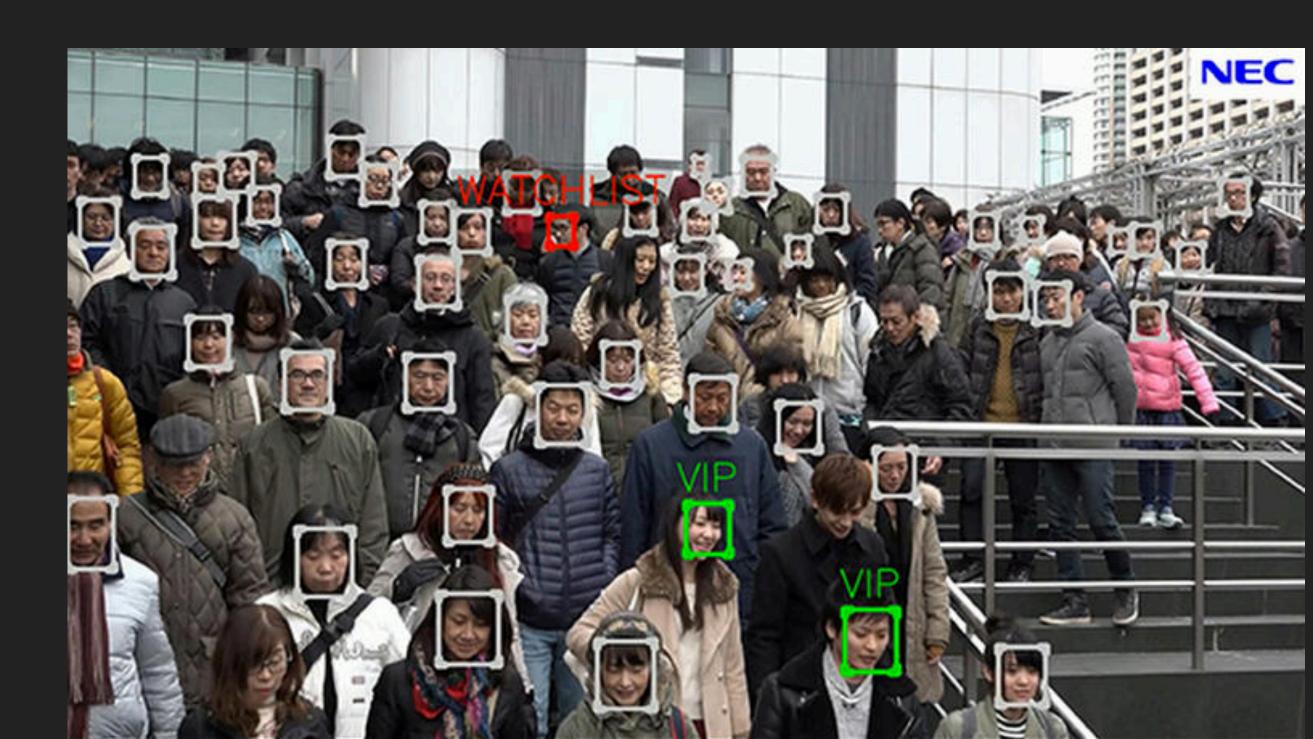


TONS OF STUFF

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









GOT WEAPONS

TOOLS

- Commercial Tools / Free and Open Source Tools:
 - Ghiro¹ full image forensics framework.
 - ▶ Jpegsnoop² uses EXIF data, quantisation matrices, Huffman tables to assess what created the image.
 - Phoenix³ small image forensics tool that can run some common analyses on images.

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



^{1.} http://www.getghiro.org

IMAGE VERIFICATION CHECKLIST

Reverse image search.

Check for image physics.

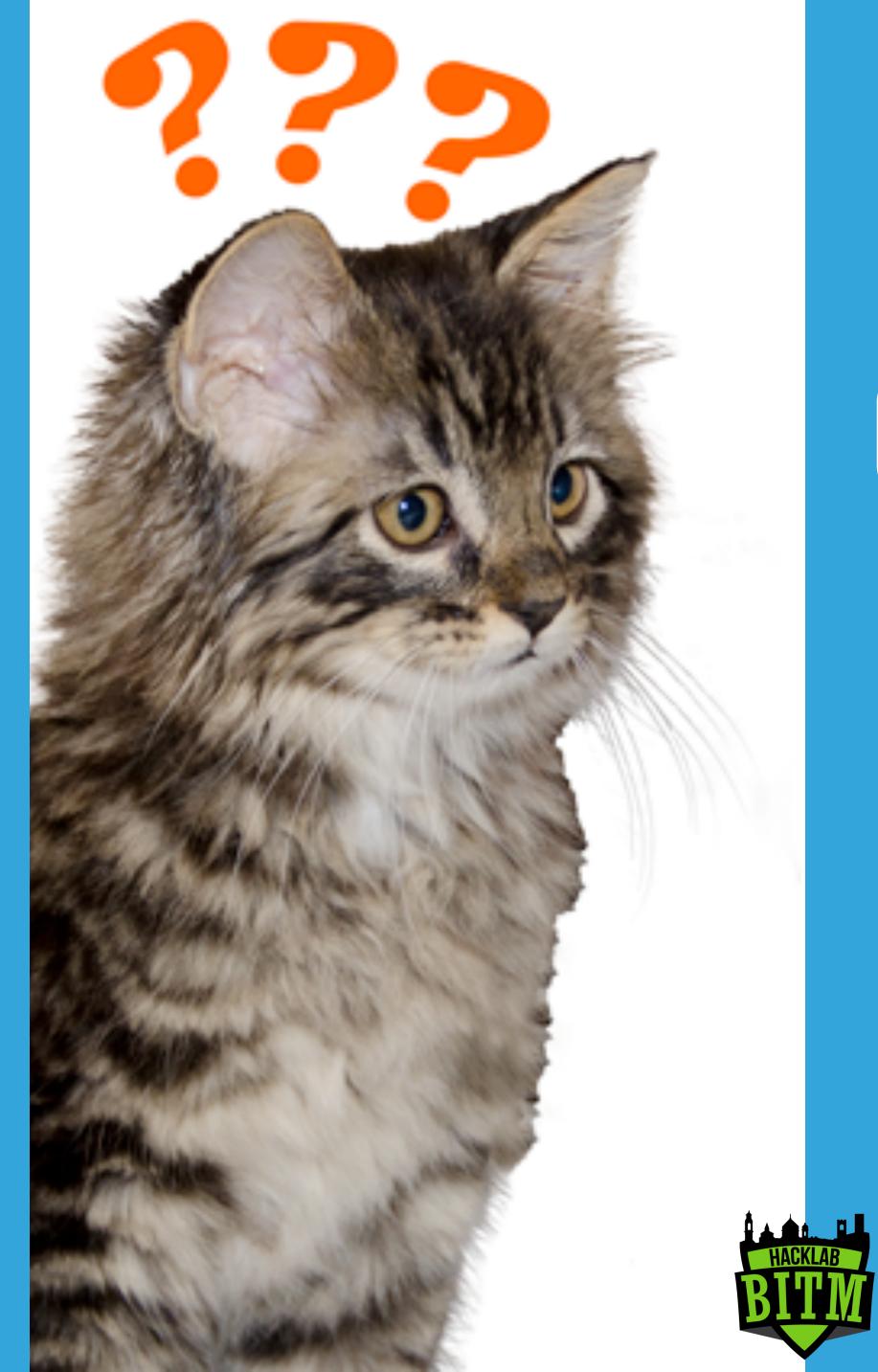
Metadata analysis.

► 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