A Picture's Worth…
Digital Image Analysis

Dr. Neal Krawetz
Hacker Factor Solutions
www.hackerfactor.com

Contents

- Digital Image Analysis
  - Problem Space
  - Analysis Methods
- Accuracy and Limitations
- Case Study
- Conclusion

All images and screen shots are copyright by their respective owners and are included for academic discussion and research. This complies with the copyright law of the United States as defined and stipulated under Title 17 U. S. Code.

The methods presented here are experimental.

Digital Image Analysis Problem Space

Copyright 2007-2008 Hacker Factor

Pictures Have Power

Space Shuttle Challenger

Iwo Jima, World War II

http://grin.hq.nasa.gov/IMAGES/SMALL/GPN-2004-00012.jpg
http://www.archives.gov/publications/prologue/2004/winter/top-images.html
http://funny-insurance.blogspot.com/2007/05/top-10-best-funny-photo-of-funny.html

Copyright 2007-2008 Hacker Factor

Not All Pictures Are Real

- Why not real?
  - Modified to influence opinions
  - Enhanced to convey a point
  - Designed to show techniques
- Implications
  - Legal: Child Pornography vs. Virtual Child Porn
  - Security: Image as Authentication
  - Media: Misleading Headlines

Copyright 2007-2008 Hacker Factor

Images and the Law

Not legal advice!
I am not a lawyer!

- Pornography
  - Protected by the First Amendment
- Child Pornography
  - Child Pornography Prevention Act (1996)
  - Prevents use of children in sexually explicit materials
  - Does not distinguish real from fake
- Virtual Child Pornography
  - Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002)
  - CPPA violated free speech rights
  - Distinction between “CP” and “VCP”
  - VCP does not use real children (it is regular “pornography”)

Copyright 2007-2008 Hacker Factor

Images as Authentication

- How do you authenticate someone online?
  - Name, Address, Phone, Age
  - Collecting information from minors…
- Forging authentication
  - Yahoo!
  - Myspace

Copyright 2007-2008 Hacker Factor

Yahoo! Impersonation

Date: Fri, 20 Apr 2007 12:38:13 -0700
Subject: Re: Abuse - Impersonation
Reply-To: Yahoo! Mail <mail-abuse@cc.yahoo-inc.com>

Hello,

Thank you for contacting Yahoo! Customer Care.

If you are an individual being impersonated by a Yahoo! Mail user, we will need a signed statement from you denying any involvement with the account, as well as a copy of the email (including full Internet headers) that is going out in your name. If you do not have an actual email message, please give us a detailed explanation of why you believe you are being impersonated. We will also need a copy of your photo ID.

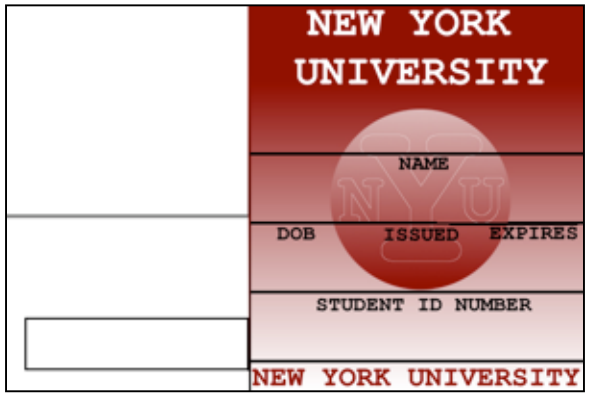
If your company is being impersonated by a Yahoo! Mail account, we will need a signed statement on company letterhead denying any involvement with the account, as well as a copy of the email (including full Internet headers) that is going out with the company name.

You may fax your statement to us at:

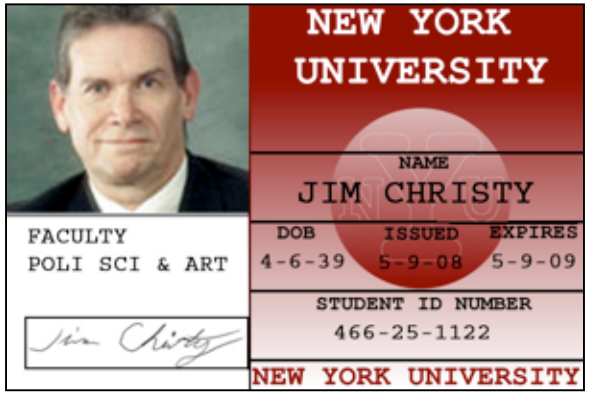
(503) 615-3883

Defeating Yahoo Identification

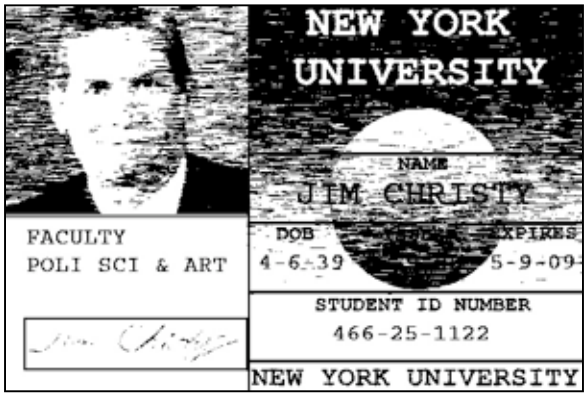
- Fake Photo ID
  - Download template
    http://www.linkbase.org/make-fake-id/



- Photoshop



- Fax!



Copyright 2007-2008 Hacker Factor

Images as Authentication

419eater.com

Copyright 2007-2008 Hacker Factor

My Problem with MySpace

http://www.peacexpeace.org/elements/images/familysignguy.jfif

Copyright 2007-2008 Hacker Factor

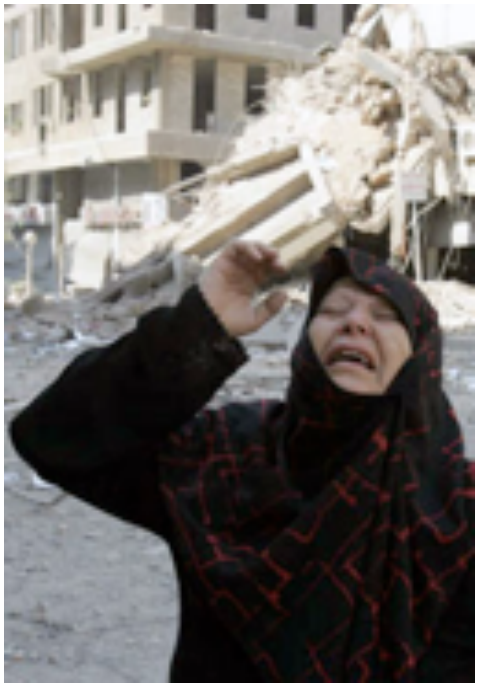
Fake Photos in the Media

- Old School
  - Staged
  - Mislabeled
  - *Not detectable*
- Old-tech
  - Negative splicing
  - Airbrushing
  - *May be detectable*
- Hi-tech
  - Digitally spliced
  - Digitally enhanced
  - “Shopped”
  - *Is detectable!*

Copyright 2007-2008 Hacker Factor

Old-School Fakes

10-Oct-1914: “I opened up the paper and what was my surprise to see a big spread picture of myself, lined up against that row of Melle cottages and being shot for the delectation of the British public.”



Adnan Hajj:
Beirut (Reuters)
22 July 2006
5 August 2006

http://www.greatwardifferent.com/Great_War/Belgium/Belgium_War_Reporters_01.htm
http://neveryetmelted.com/?cat=743

Copyright 2007-2008 Hacker Factor

Old and New

- Problem
  - Photos are REAL
  - Only identified by close inspection or tracking source
- Combined with new methods

2002 Dust Storm

2004 Tsunami

http://www.snopes.com/photos/tsunami/sumatra.asp

Copyright 2007-2008 Hacker Factor

The Big Questions

- Distinguish “real” from computer graphics
- How to detect image manipulations
- How to pull out information from images
  - Real images: who, where, when, how
  - Digitally enhanced: what, how
  - Computer graphics: what, how

Copyright 2007-2008 Hacker Factor

The Big Answers

- Observation
- Basic Image Enhancements
  - Color Tweaking
- Image Format Analysis
  - Meta Data Analysis
  - Quantization Table Fingerprinting
  - Estimated Compression Level
- Advanced Image Analysis
  - Error Level Analysis (ELA)
  - Principle Component Analysis (PCA)
  - Wavelet Transformations
  - Luminance Gradient (LG)

Copyright 2007-2008 Hacker Factor

Observation

Copyright 2007-2008 Hacker Factor

Warez Factory

Copyright 2007-2008 Hacker Factor

Warez F

Scaled, sharpened, enhanced

Things to Look For

- Time
  - Clocks, calendars
  - Dated materials
- Location
  - Language
  - Region-specific technology
  - Currency and Electrical Outlets!
- Other
  - What's on the computer screen?
  - Any other identifiable elements

Copyright 2007-2008 Hacker Factor

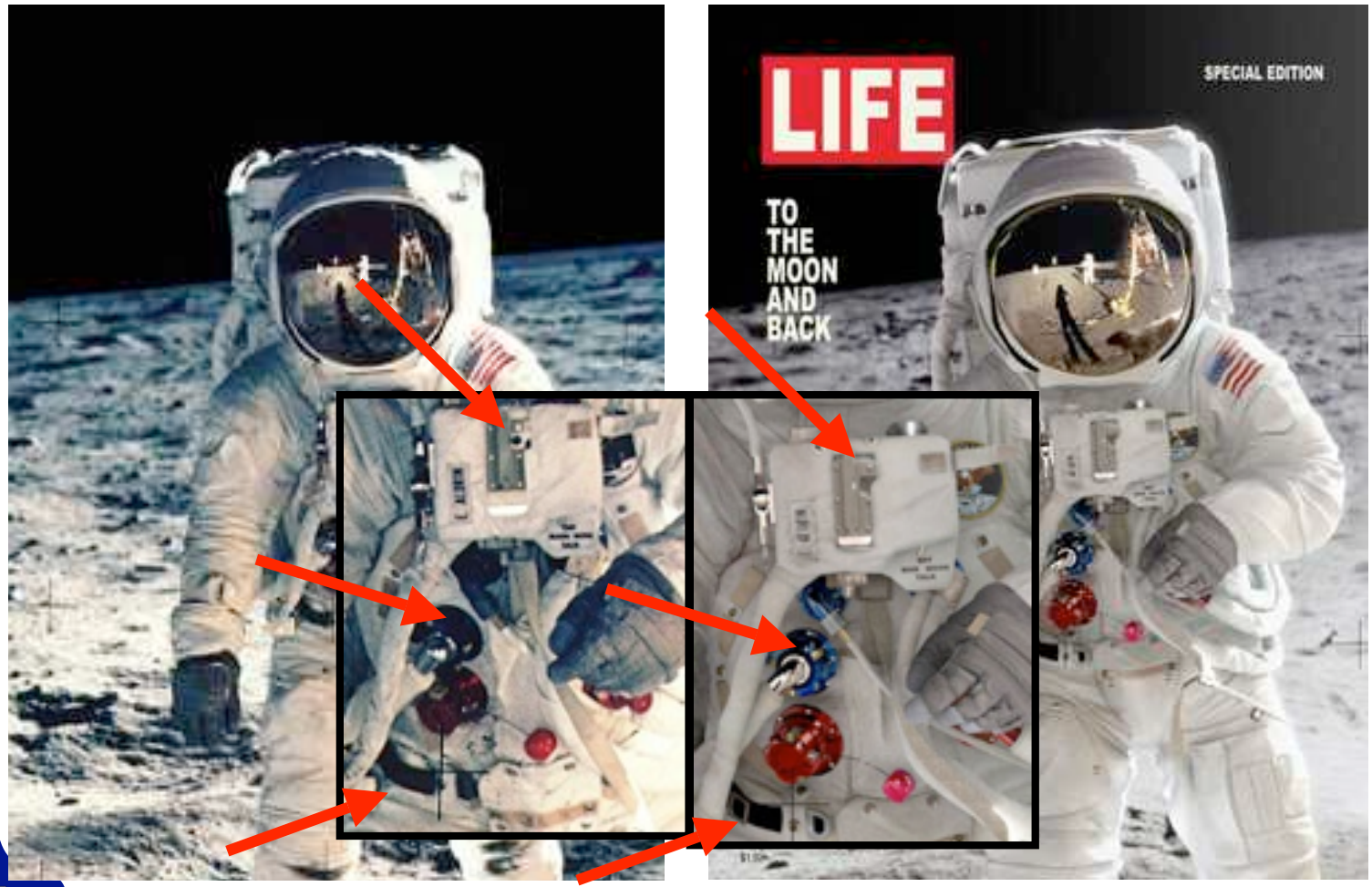
Example: Buzz

- Andrea Bertaccini
  - www.tredistudio.com
  - "CG Choice Award" from CG Society, 2006
- Says based on NASA photo

http://www.hq.nasa.gov/office/pao/History/ap11ann/kippsphotos/5903.jpg

Copyright 2007-2008 Hacker Factor

Example: Buzz Compare



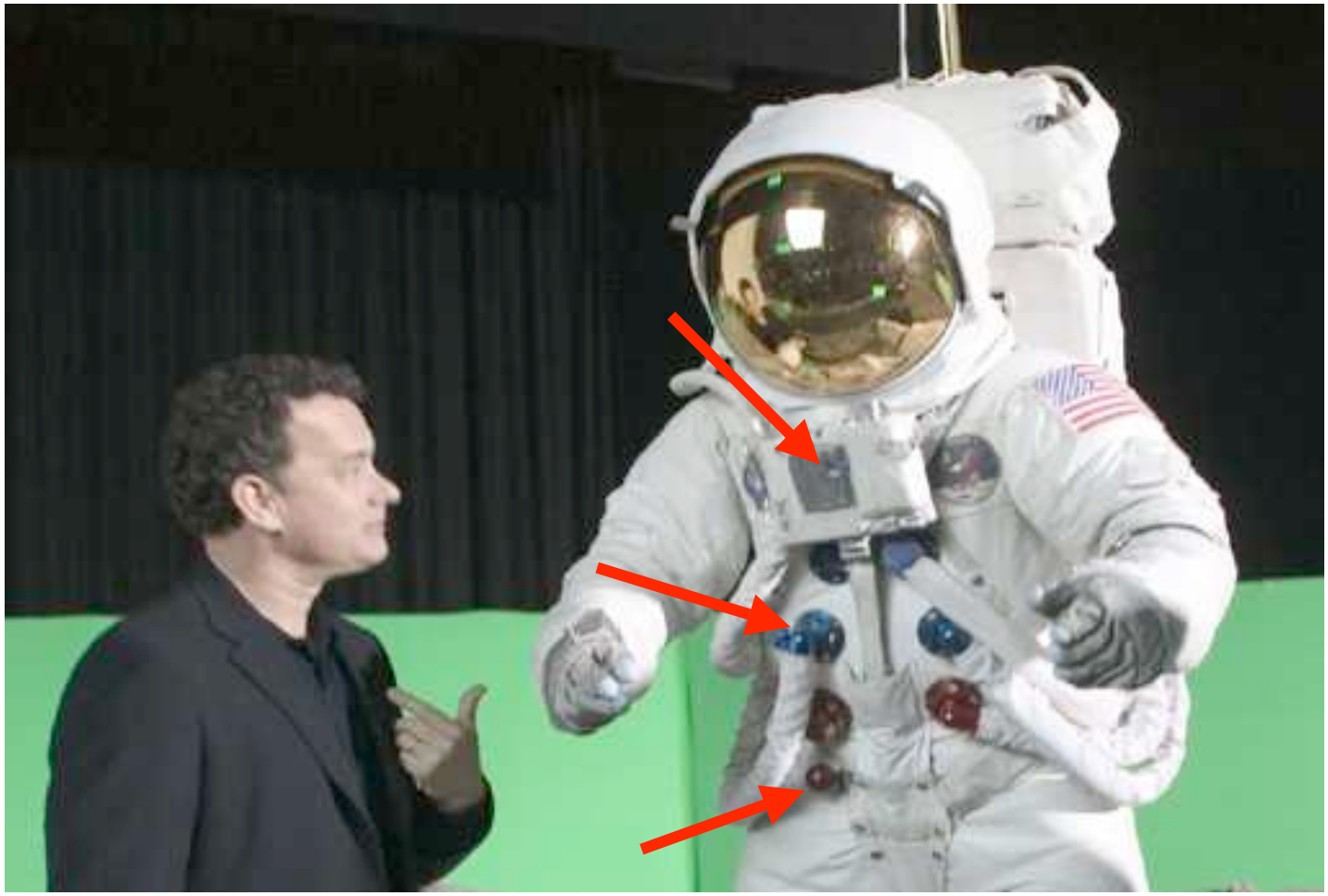
Copyright 2007-2008 Hacker Factor

IMAX: *Magnificent Desolation*

- IMAX recreated moonwalk
  - http://www.imax.com/magnificentdesolation
  - Director: Tom Hanks
- Timeframe
  - Movie in 2005
  - Artist image in 2006

Copyright 2007-2008 Hacker Factor

IMAX: *Magnificent Desolation*



Copyright 2007-2008 Hacker Factor

What Happened?

- Artist likely:
  - Modeled position after NASA
  - Modeled spacesuit after IMAX

Copyright 2007-2008 Hacker Factor

Format Analysis

Copyright 2007-2008 Hacker Factor

Image Format Analysis

- Formats *are* information
  - Formats are data that contain data
  - Changes to image yield changes to format
- JPEG as an example
  - Most methods work with any image format

Copyright 2007-2008 Hacker Factor

JPEG Feature Set

- Key Features of JPEG
  - Meta data
  - Quantization matrix for lossy compression
  - Lossy data format
  - Divide image into 8x8 cells
    - JPEG artifacts are usually visible 8x8 cells
- Feature Detection
  - Feature leads to manipulation detection

Copyright 2007-2008 Hacker Factor

JPEG Meta Data

- Information about image
  - Camera type and settings
  - Date and time
- Multiple images
  - Varying quality
  - Useful for distinguishing cameras
- Meta data problem:
  - Modified or inaccurate
  - Applications do not update meta data!
    - Photoshop keeps camera info (even if picture changes)
    - Photoshop does not log Photoshop changes

```
$ exiftool IM001022.JPG
MIME Type                       : image/jpeg
JFIF Version                    : 1.1
Make                            : Hewlett-Packard
Camera Model Name               : HP PhotoSmart 618
Orientation                     : Horizontal (normal)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/125
F Number                        : 3.7
ISO                             : 100
Exif Version                    : 0210
Date/Time Original              : 2007:05:28 09:19:49
Components Configuration        : YCbCr
Compressed Bits Per Pixel       : 1.6
Shutter Speed Value             : 1/128
Aperture Value                  : 4.0
Exposure Compensation           : 0
Max Aperture Value              : 4.0
Subject Distance                : 0.13 m
...
```

Copyright 2007-2008 Hacker Factor

Quantization Fingerprinting

- Should compute optimal quantization tables
  - CPU intensive!
  - Slow user experience!
- Hard-coded quantization tables
  - Few systems actually generate Q tables
  - Digital cameras use different Q tables
    - Vary by make and model
    - Optimized for CCD, data size, manufacturer
    - Canon pictures look best on Canon printers (colors optimized)
  - Cannot just “copy over” Q tables
- Forensics
  - Match Q tables to application or camera
    - Media outlets: Pay attention!

Copyright 2007-2008 Hacker Factor

Quantization Quality

- What if Q tables not known?
- JPEG uses a quality value
  - Save at 95%, 80%, 65%…
  - Quality corresponds with size
- Quality not saved in JPEG!
  - Fingerprint Q table? Know tool and quality
  - Unknown Q table? Need to determine quality
- Derive quality value!

Copyright 2007-2008 Hacker Factor

Quantization Tables

- Q tables: compression and quality
- Two tables for YCrCb
  - 1 for luminance (Y)
  - 1 for both Cr and Cb
  - Optional:
    - 3 tables: Y, Cr, and Cb
- 64 elements
  - 1st element = DC
  - 63 elements = AC
    - Compression by frequency

```
# Quantization table
#   Table index=0 (luminance)
    3   2   2   3   2   2   3   3
    3   3   4   3   3   4   5   8
    5   5   4   4   5  10   7   7
    6   8  12  10  12  12  11  10
   11  11  13  14  18  16  13  14
   17  14  11  11  16  22  16  17
   19  20  21  21  21  12  15  23
   24  22  20  24  18  20  21  20

# Quantization table
#   Table index=1 (chrominance)
    3   4   4   5   4   5   9   5
    5   9  20  13  11  13  20  20
   20  20  20  20  20  20  20  20
   20  20  20  20  20  20  20  20
   20  20  20  20  20  20  20  20
   20  20  20  20  20  20  20  20
   20  20  20  20  20  20  20  20
   20  20  20  20  20  20  20  20
```

Copyright 2007-2008 Hacker Factor

Example Derivation

- Average AC values
  - Table 0: 11.63
  - Table 1: 17.57
- Average Y, Cr, Cb

  (11.63 + 17.57 + 17.57) / 3 = 15.59
- Get RGB/YCrCb conversion

  ||17.57 - 11.63|| = 5.94 convert
- Combine to find quality

  100.0 - 15.59 + 5.94 = 90.35%

  Call it 90%

  See jpegquality.c

```
# Quantization table
#   Table index=0 (luminance)
     3   2   2   3   2   2   3   3
     3   3   4   3   3   4   5   8
     5   5   4   4   5  10   7   7
     6   8  12  10  12  12  11  10
    11  11  13  14  18  16  13  14
    17  14  11  11  16  22  16  17
    19  20  21  21  21  12  15  23
    24  22  20  24  18  20  21  20

# Quantization table
#   Table index=1 (chrominance)
     3   4   4   5   4   5   9   5
     5   9  20  13  11  13  20  20
    20  20  20  20  20  20  20  20
    20  20  20  20  20  20  20  20
    20  20  20  20  20  20  20  20
    20  20  20  20  20  20  20  20
    20  20  20  20  20  20  20  20
    20  20  20  20  20  20  20  20
```

Copyright 2007-2008 Hacker Factor

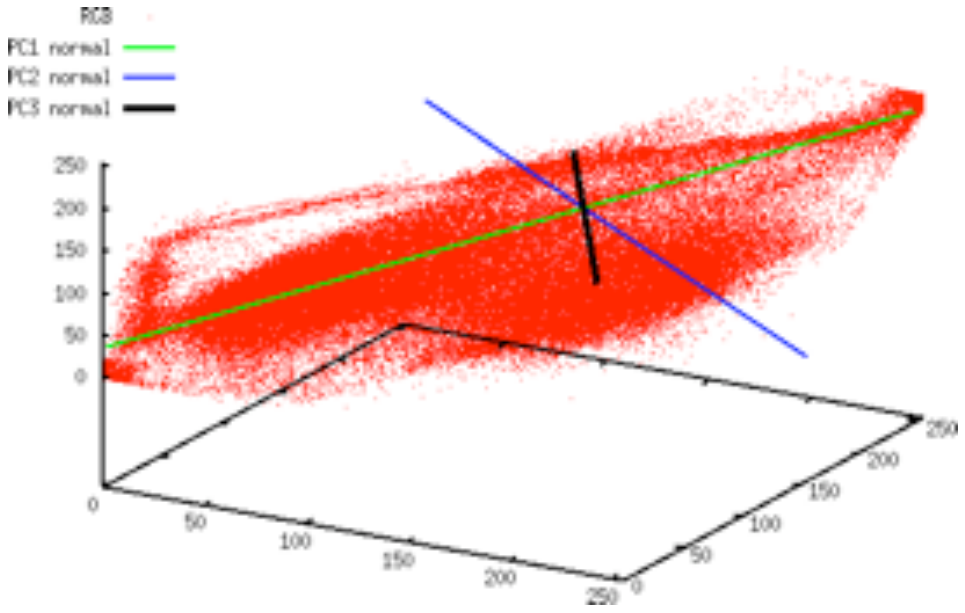
Quantifiable Problem

- Data loss is cumulative
- Resave problem:
  - Save an image at quality of 75%
  - Resave image at 90%
  - Image does *not* get better!
    - 90% of 75% = 67.5%
  - Quantization tables reflect 90%, not 75% or 67.5%
- How to detect image resaves?
  - Principal Component Analysis!

Copyright 2007-2008 Hacker Factor

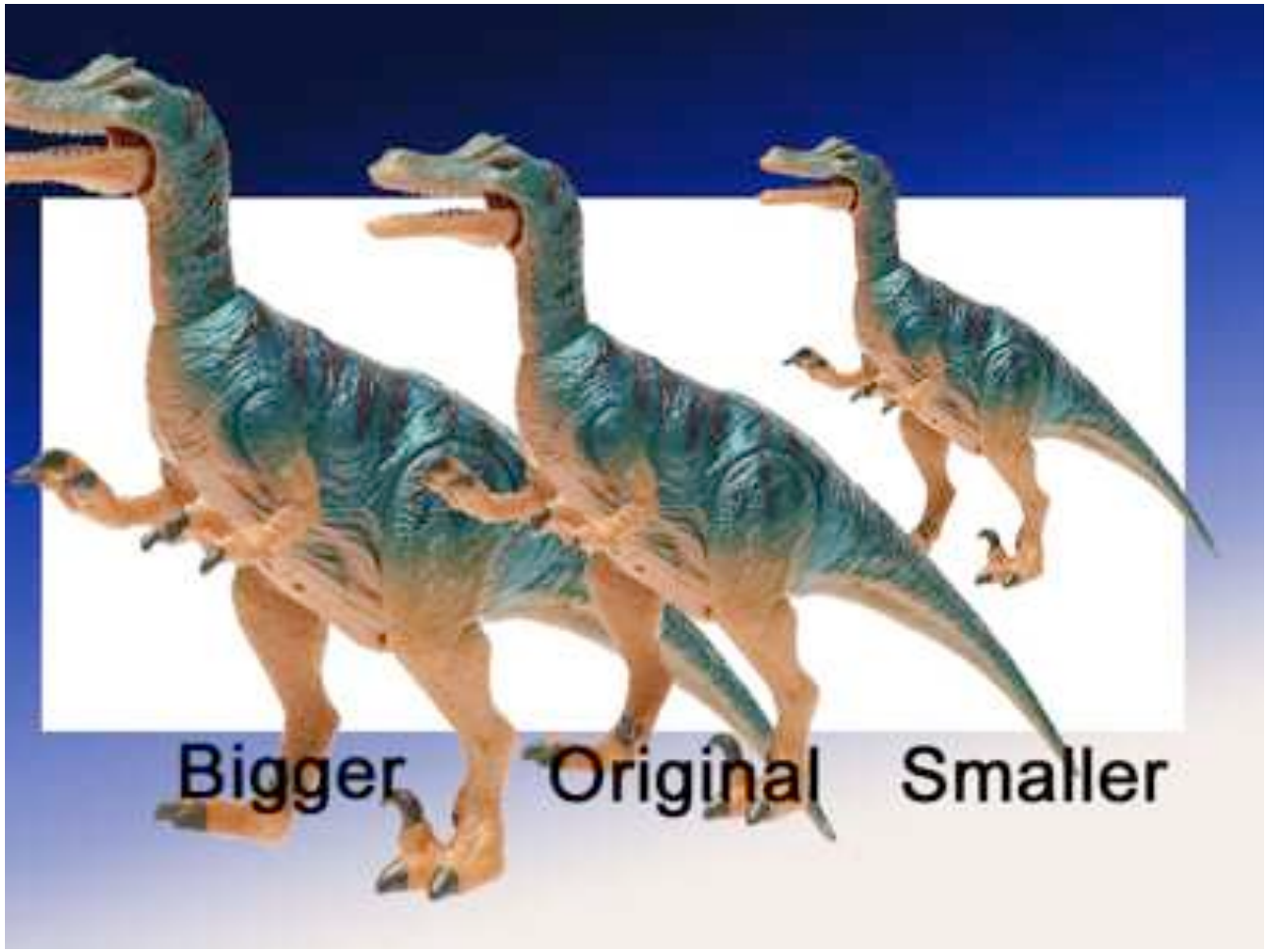
Principal Component Analysis

- PCA separates info
  - Computer vision
  - Data compression
- Identifies widest variance among points
  - 3D = 3 components
    - PC1 = widest
    - PC2 = next widest
    - PC3 = narrowest



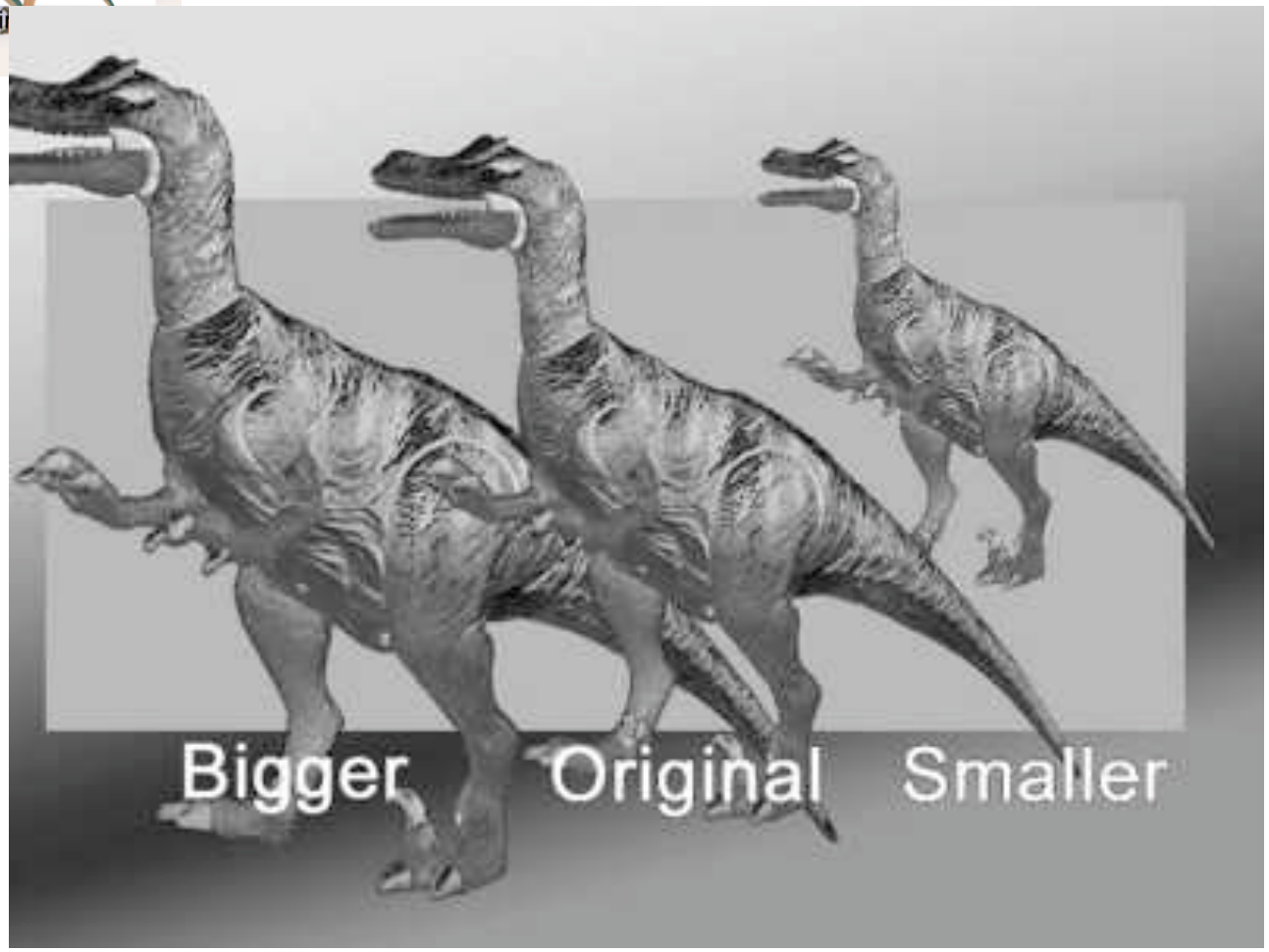
Copyright 2007-2008 Hacker Factor

PCA Example



Copyright 2007-2008 Hacker Factor

PCA Example



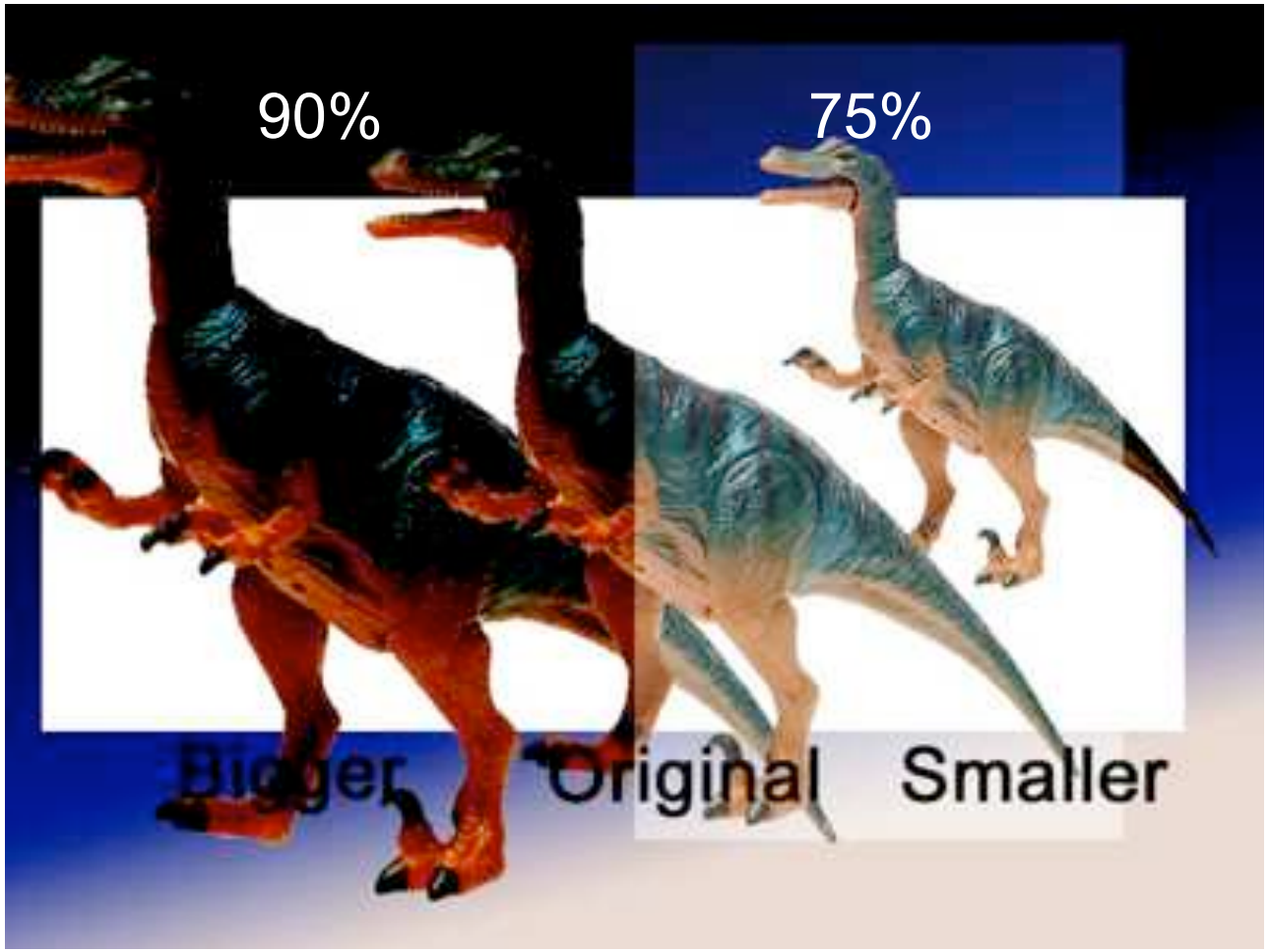
Copyright 2007-2008 Hacker Factor

PC1 with Artifacts

95%
90%
80%
70%
60%
50%

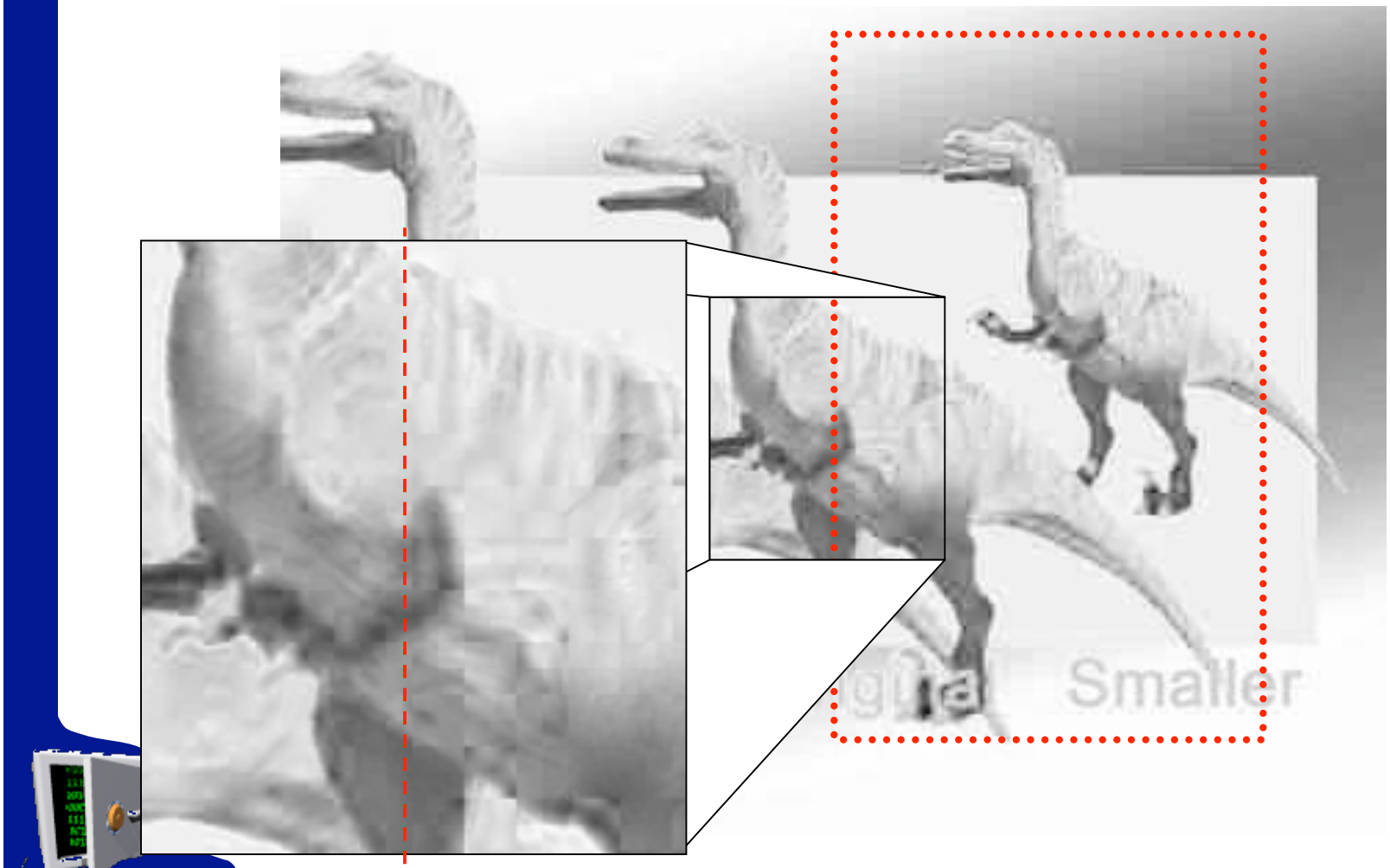
Copyright 2007-2008 Hacker Factor

PCA Mixing: 90% with 75%



Copyright 2007-2008 Hacker Factor

PCA Mixing: 90% with 75%



Copyright 2007-2008 Hacker Factor

Example: Back to the Moon

Copyright 2007-2008 Hacker Factor

Buzz Aldrin Moon Walk

- "All the image are made in 3DS MAX and postprocessed in Combustion and Photoshop."

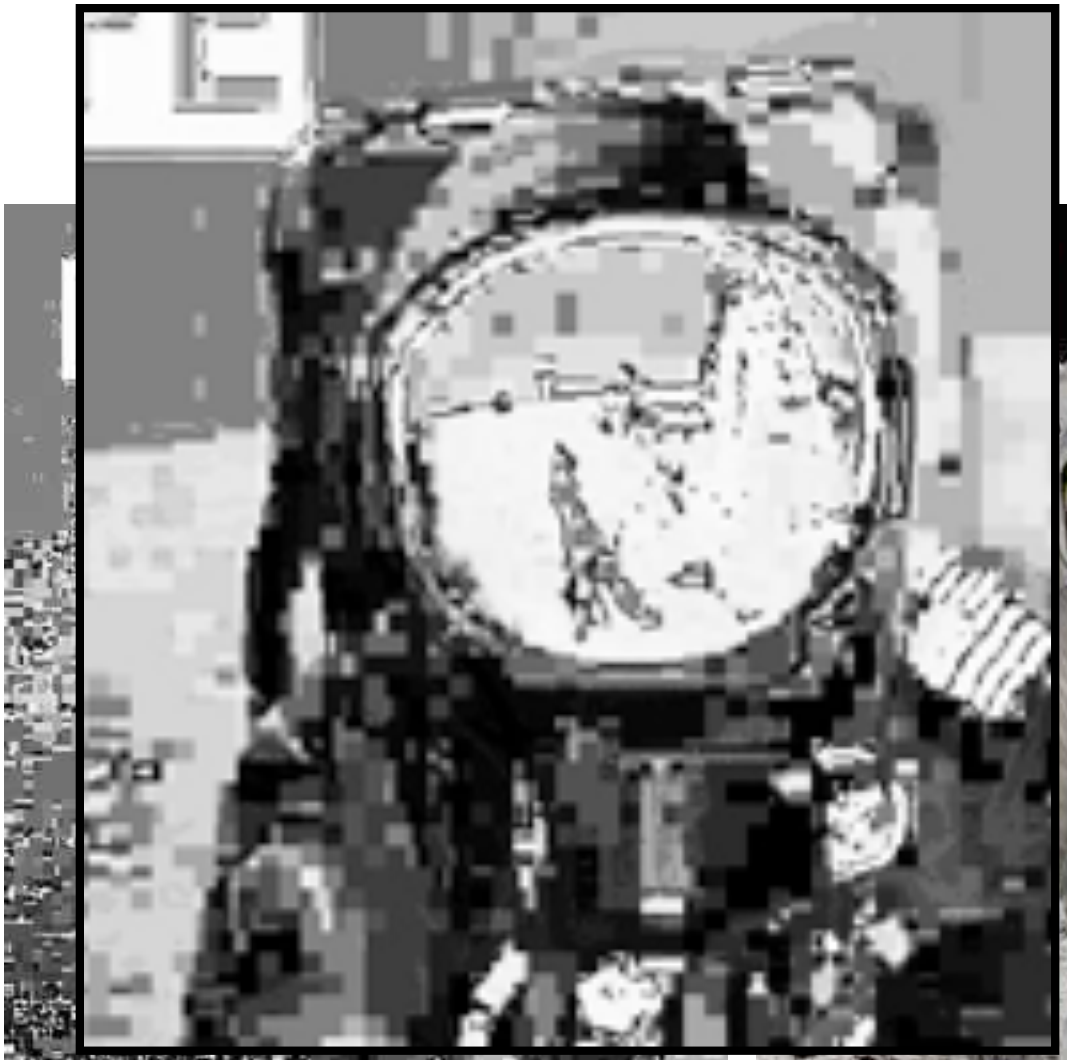
  http://forums.cgsociety.org/showthread.php?t=323480
- JPEG Q tables say:
  - Photoshop
  - 89% quality

Copyright 2007-2008 Hacker Factor

Buzz Aldrin Moon Walk

Copyright 2007-2008 Hacker Factor

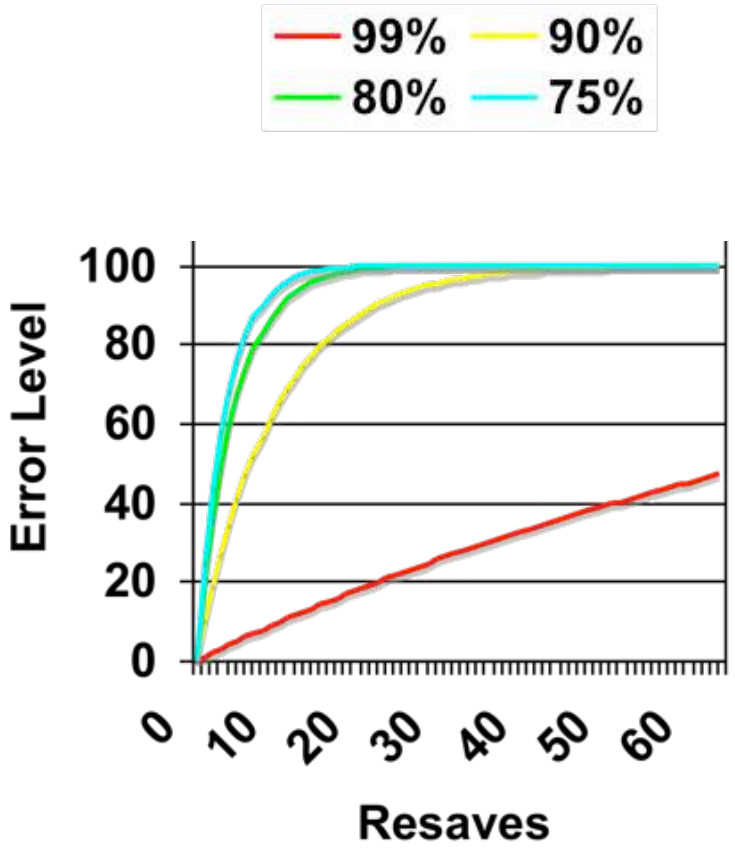
Walk



Copyright 2007-2008 Hacker Factor

Error Level Methodology

- JPEG is lossy format
- Each resave introduces more error
  - But “copy” does not
- Error rate not linear!



Copyright 2007-2008 Hacker Factor

Error Level Analysis

- Each 8x8 cell should be at same quality level
- Changes to image change quality level for the 8x8 cell

Methodology

- Save image at 95%
  - Intentionally introduce known error rate
- Compare original and new 95% image
- Difference = error state
  - No difference = image local minima
  - Large difference = unstable 8x8 cell = original pixels!

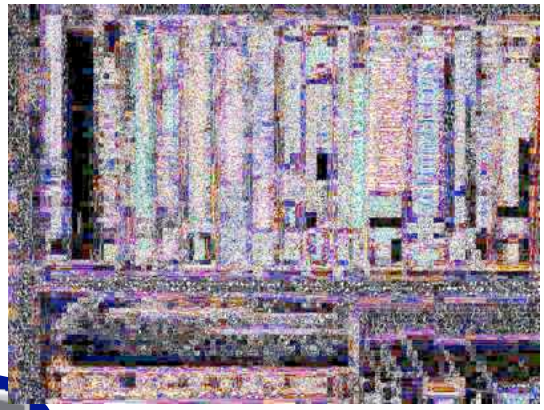
Copyright 2007-2008 Hacker Factor

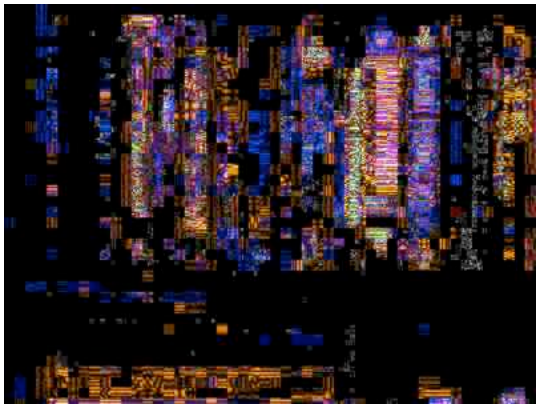
Error Rate Example

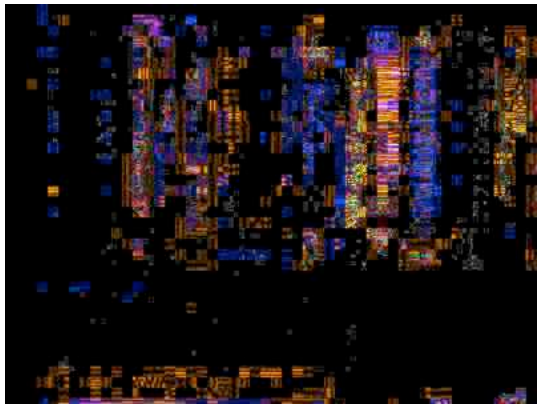
Original

Resave #1, 75%

Resave #2, 75%





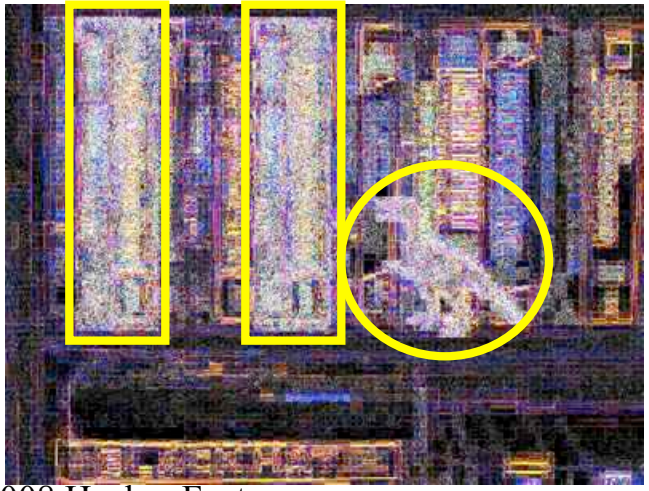


Copyright 2007-2008 Hacker Factor

Modification Detection

Resave #1, 75%

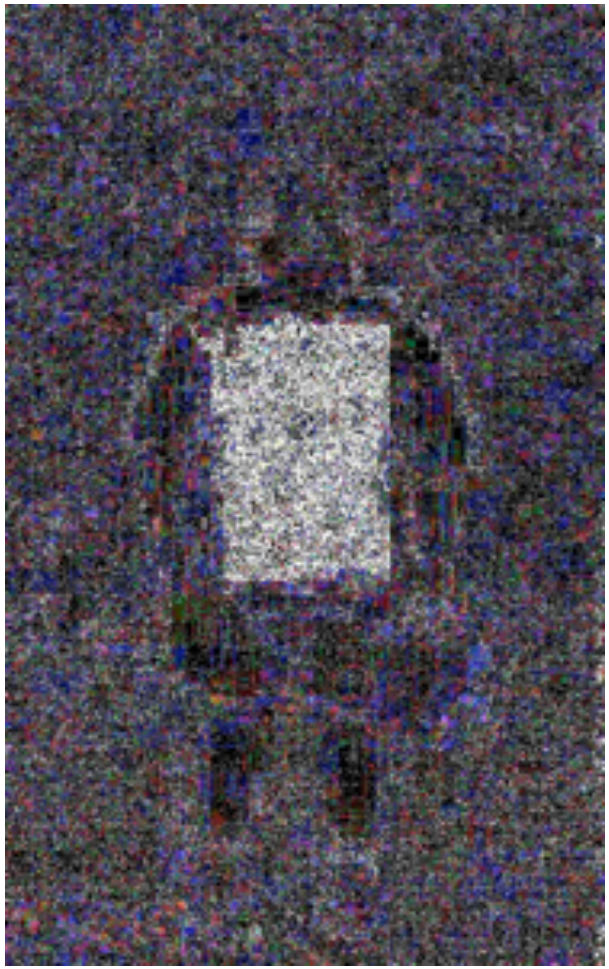
Edited: Books, Dinosaur



Copyright 2007-2008 Hacker Factor

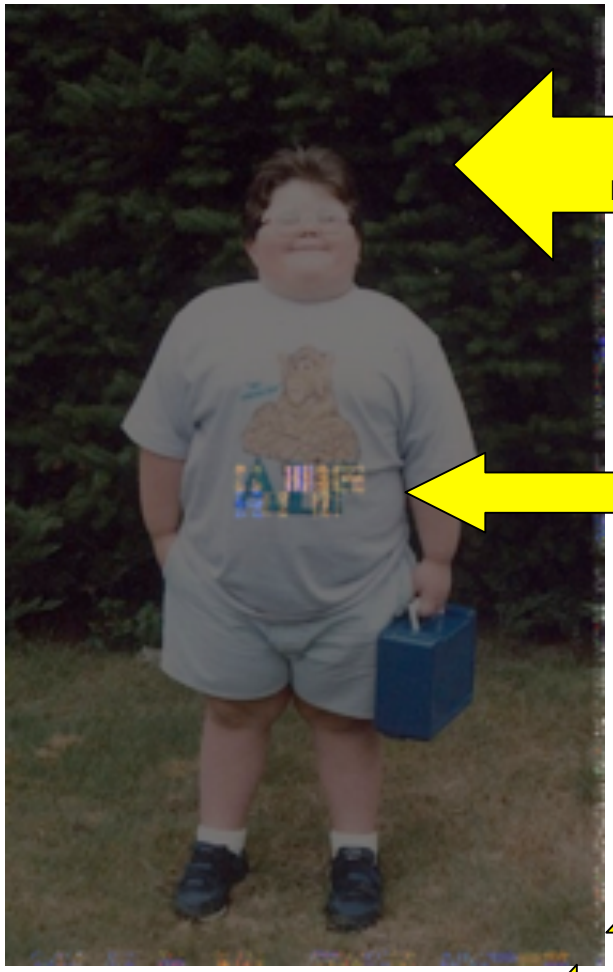
The “Alf Kid”!

“Alf Kid” Error Level Analysis



Copyright 2007-2008 Hacker Factor

Original “Alf Kid”?



Multiple resaves

?

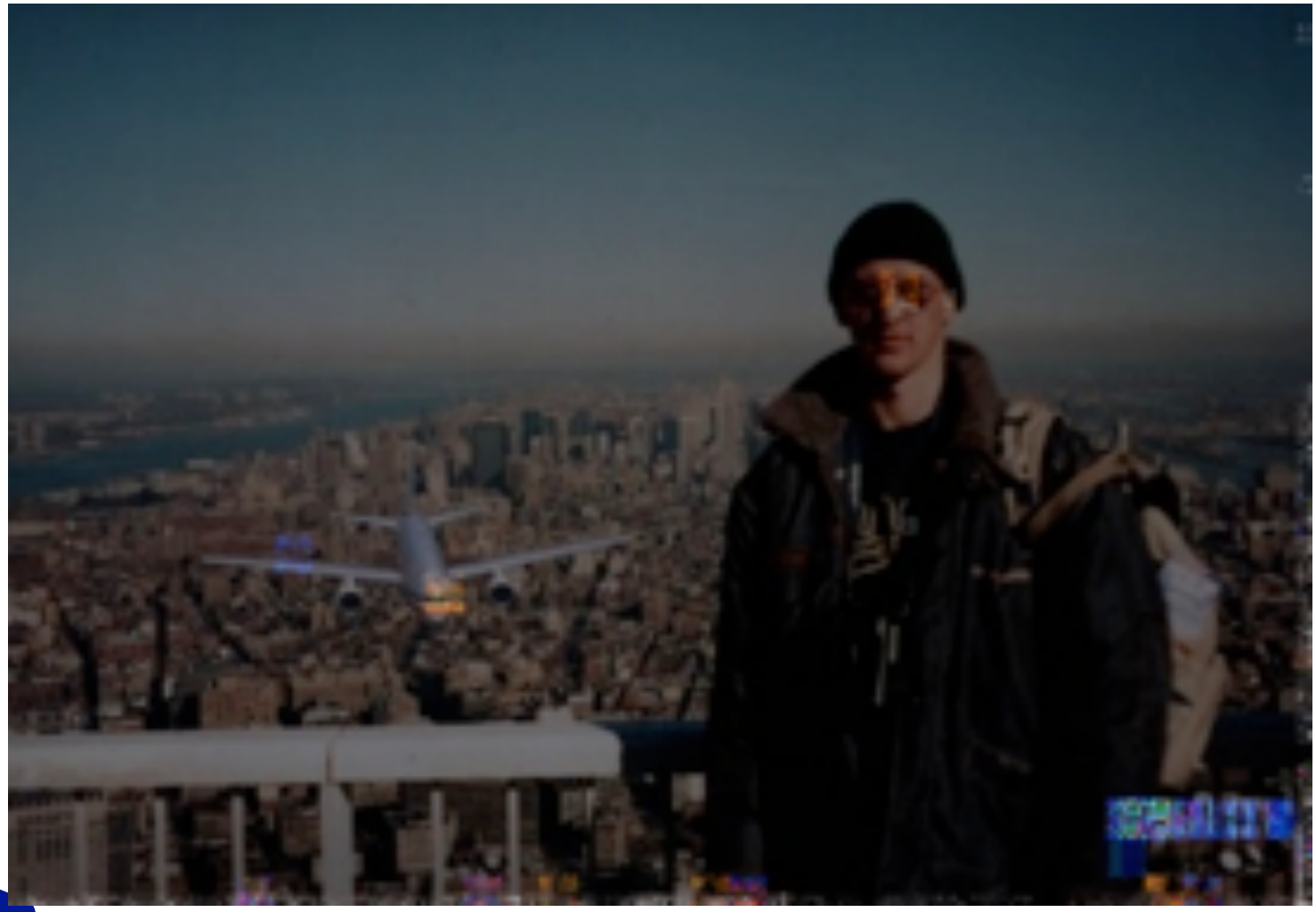
Cropped

Copyright 2007-2008 Hacker Factor

Crash Modifications

Copyright 2007-2008 Hacker Factor

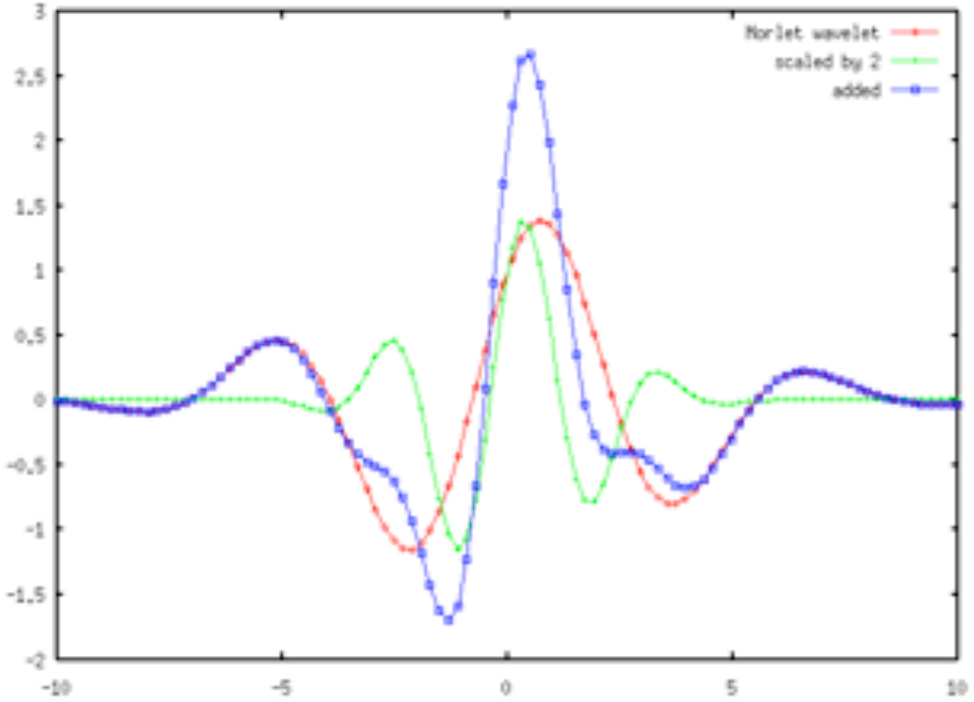
Crash Modifications



Copyright 2007-2008 Hacker Factor

Wavelet Transformations

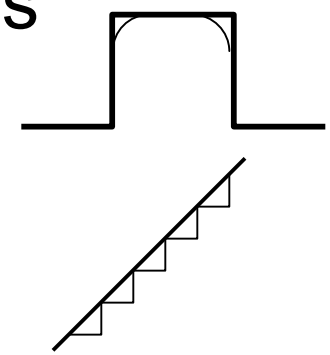
- Problem:
  - If quality is same, how can you find differences?
  - How to identify layers?
- Solution?
  - WAVELETS!



Copyright 2007-2008 Hacker Factor

Wavelet Limitations

- Any signal can be approximated
- Some signals more difficult than others
  - Square waves or sharp color changes
  - Smooth, linear transitions
  - Extreme values (black or white)
- Some signals easier to approximate
  - “Natural” colors
  - Noisy images (e.g., CCDs)



Copyright 2007-2008 Hacker Factor

Wavelet Image Analysis

- An 800x600 picture has 480,000 wavelets
  - Render only a few % to get general picture
    - Picture will appear blurry
  - Entire image should sharpen at same rate
- Image modification detection
  - Scaled images sharpen at different rates
  - Images from different focal lengths sharpen at different rates
  - Why? Images have different signal patterns

Copyright 2007-2008 Hacker Factor

Wavelet Example

Original
1%
2%
3%
5%
8%
10%
20%
30%
40%

Copyright 2007-2008 Hacker Factor

Harper's
BAZAAR
QUICK & EASY IDEAS
THAT FLATTER YOU
Fabulous
At Every
Age
HILLARY'S
NEW LOOK
FOR THE
PRIMARIES
Harper's
BAZAAR
HILLARY CLINTON
QUICK & EASY IDEAS
THAT FLATTER YOU
BEST HAIR & MAKEUP
BUYS & TIPS
Fabulous
HILLARY'S
NEW LOOK
WHY BILL IS BACK

Analysis Limitations

- Small Images
  - Wavelets fail
- Scaled Images
- Low Quality
  - Image Corruption
  - GIF and limited-color images
- Wavelets and harmonics
- Mixing Media
  - From Photo to Magazine to JPEG…
- Extremely Talented Artists (rare)

Copyright 2007-2008 Hacker Factor

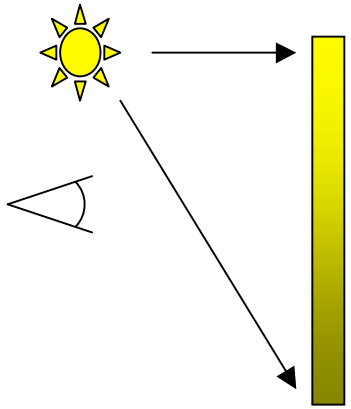
Luminance Gradient

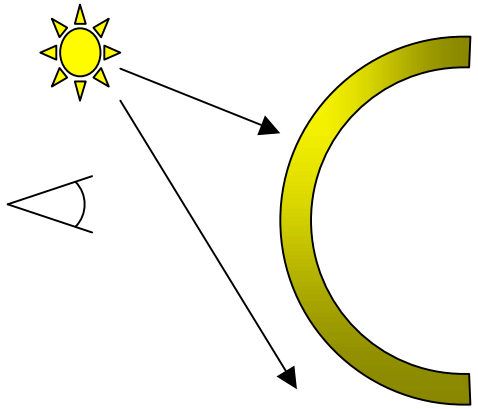
- Original plan: detect lights and direction
  - Turns out: the algorithm sucks.
  - Identifies general direction, but not specific
- The Power of LG
  - Distinguish CG from Real, manipulations
    - Vastly different light sources implies splicing
    - Edge and surface detection
      - Crisp edges, sharp curves, smooth gradients
      - Clean = computer graphics

Copyright 2007-2008 Hacker Factor

LG Concept

- Lighting is never “even” (but coloring is)
  - Given an item with a uniform color…
  - Area closest to the light will be brightest

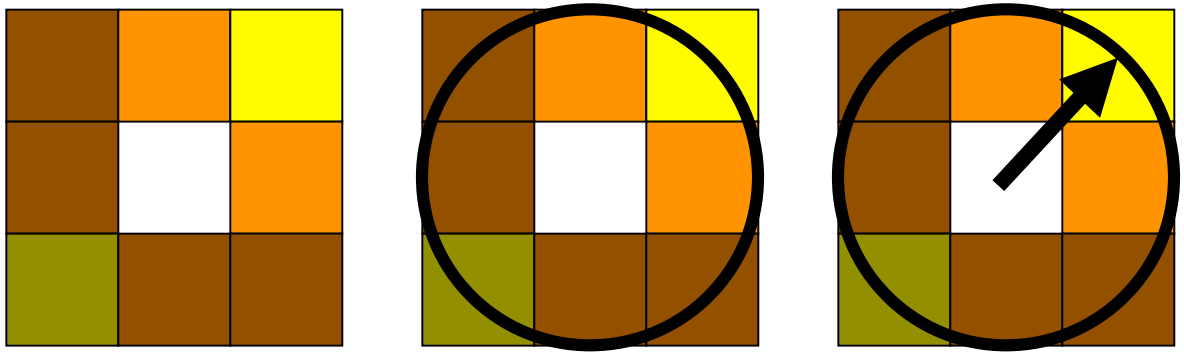




Copyright 2007-2008 Hacker Factor

LG Algorithm

- Many many many variations

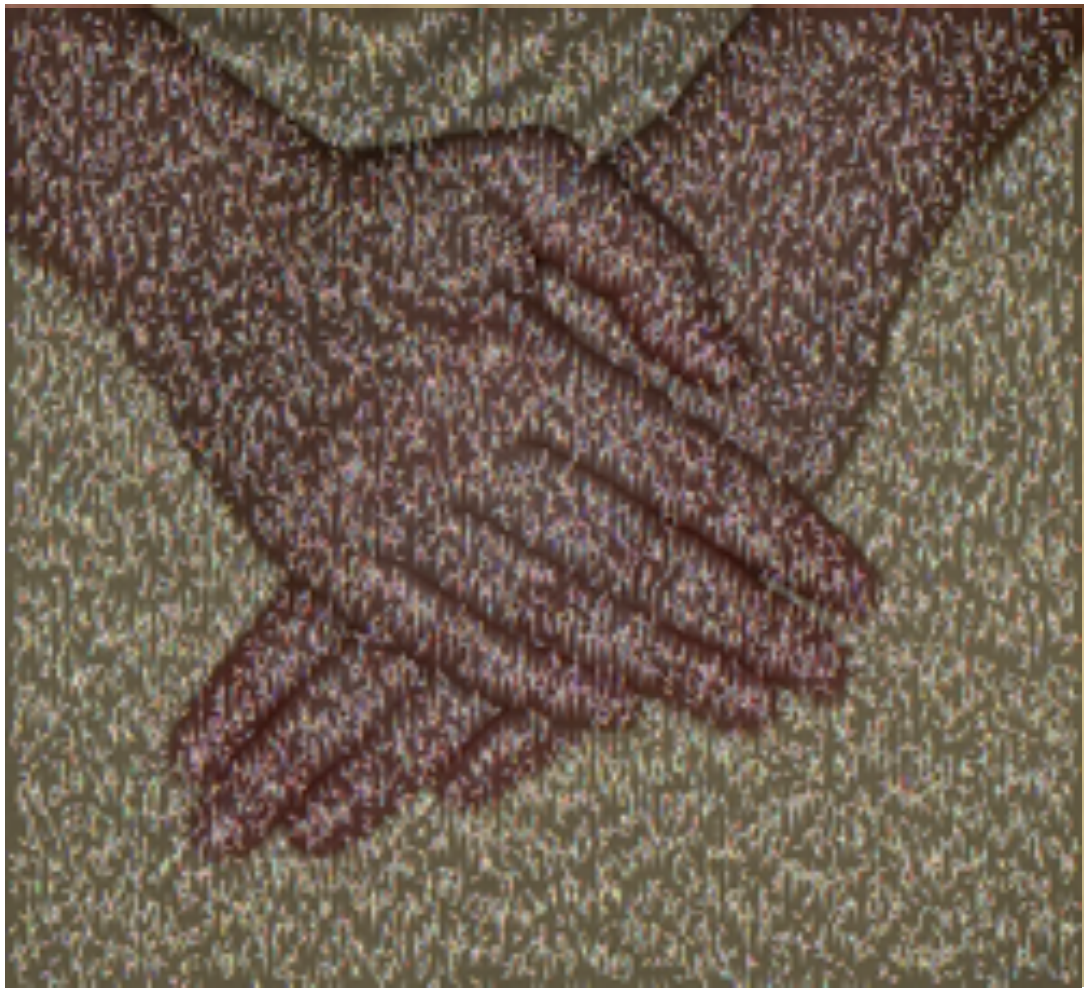


Copyright 2007-2008 Hacker Factor

LG Arrows: Hands

Copyright 2007-2008 Hacker Factor

LG Arrows: Hands



Copyright 2007-2008 Hacker Factor

LG Arrows: Hands

Image source: DC3 Forensic Challenge, 2007

Copyright 2007-2008 Hacker Factor

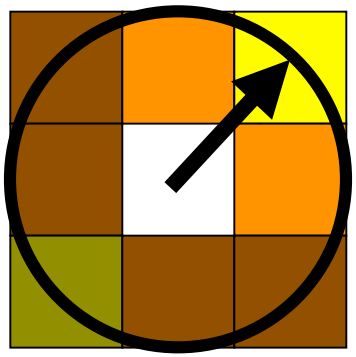
LG Arrows: Hands

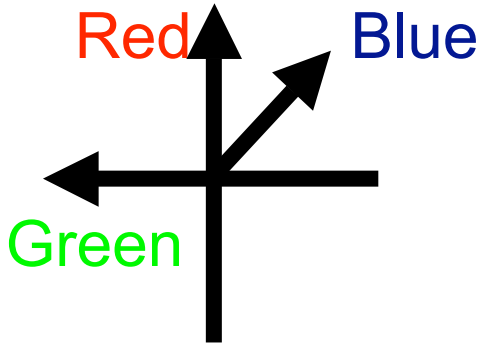
Image source: DC3 Forensic Challenge, 2007

Copyright 2007-2008 Hacker Factor

LG Colorized Algorithm

- Recolor based on arrow direction

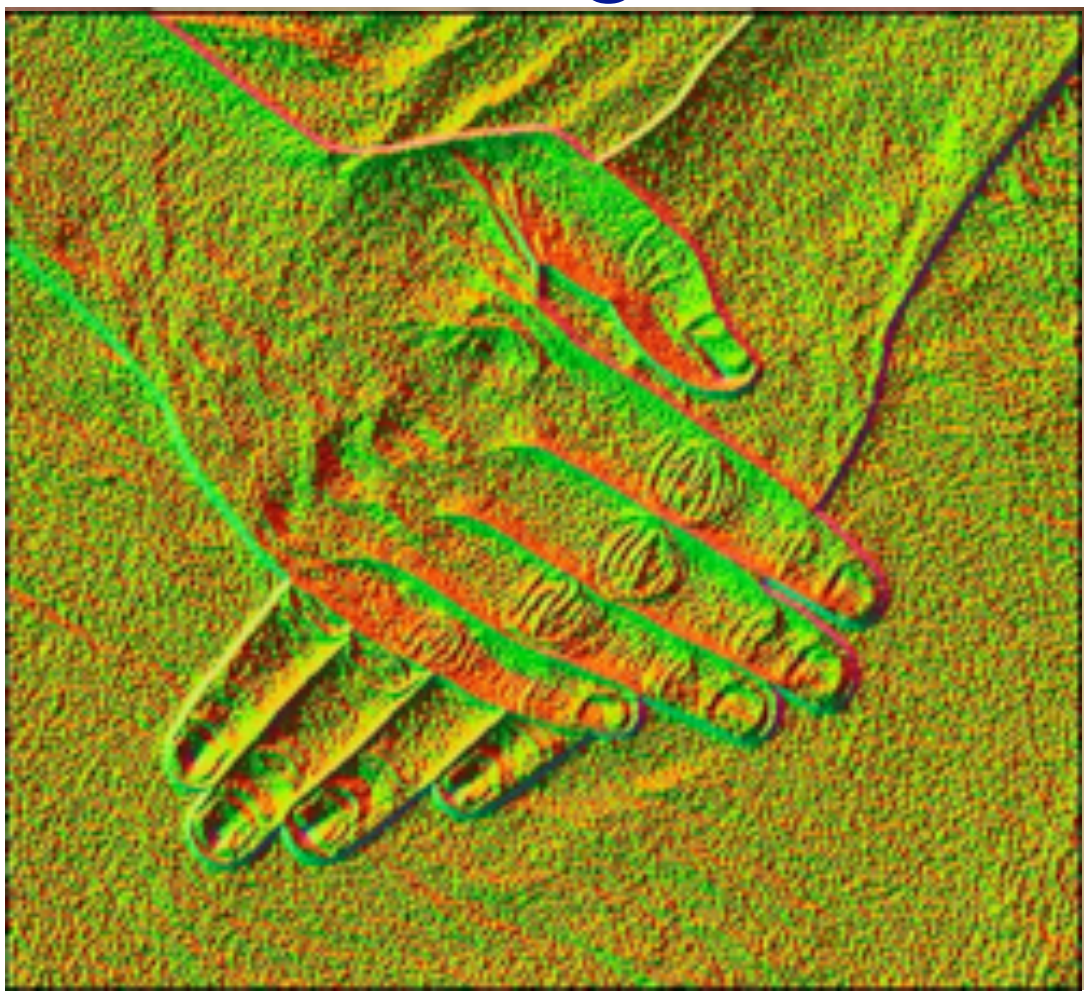




- Look for color transitions
  - Colors make people look like death…

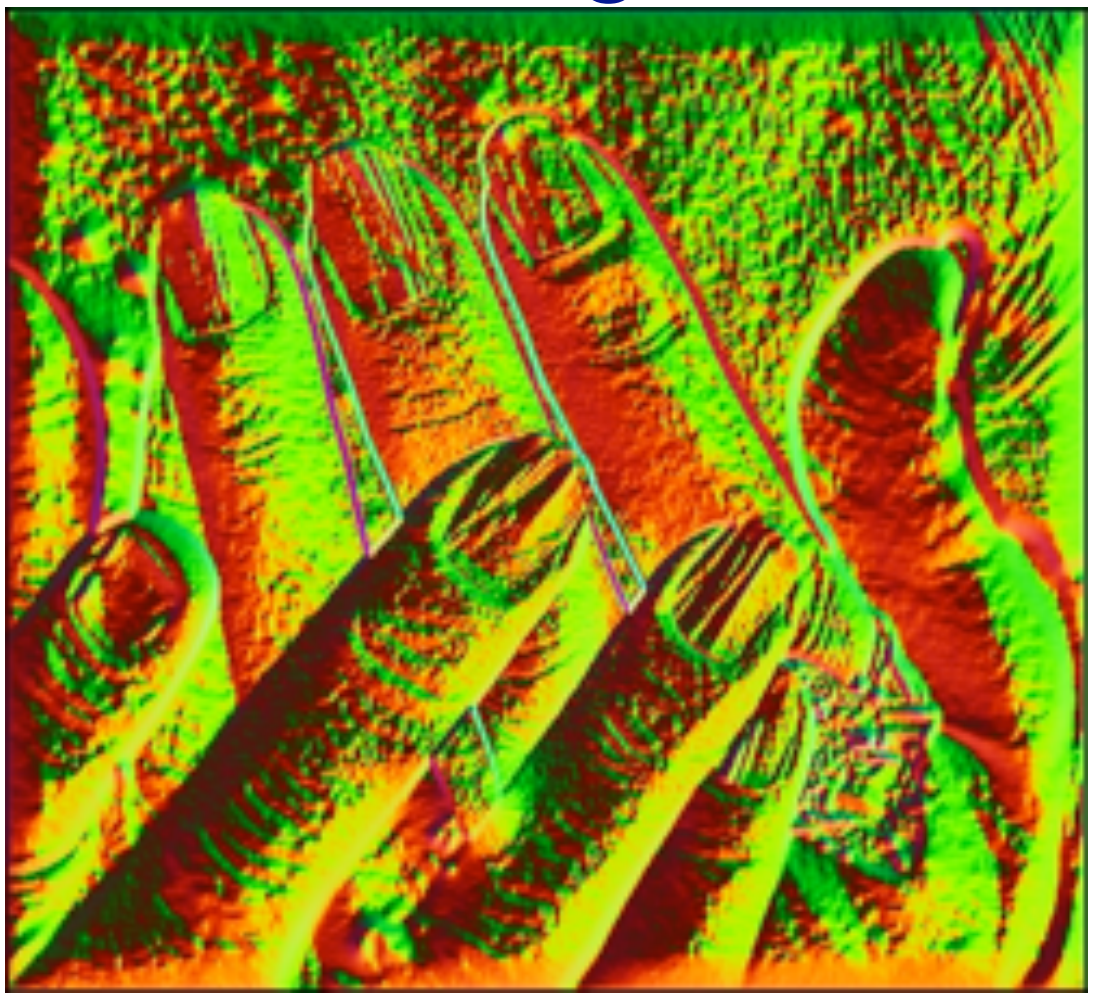
Copyright 2007-2008 Hacker Factor

LG Coloring: Hands



Copyright 2007-2008 Hacker Factor

LG Coloring: Hands



Copyright 2007-2008 Hacker Factor

LG: More Hands…

Image source: http://i146.photobucket.com/albums/r253/pjbaker_2006/hands.jpg

Copyright 2007-2008 Hacker Factor

LG: More Hands…

Image source: http://i146.photobucket.com/albums/r253/pjbaker_2006/hands.jpg

Copyright 2007-2008 Hacker Factor

LG: More Hands…

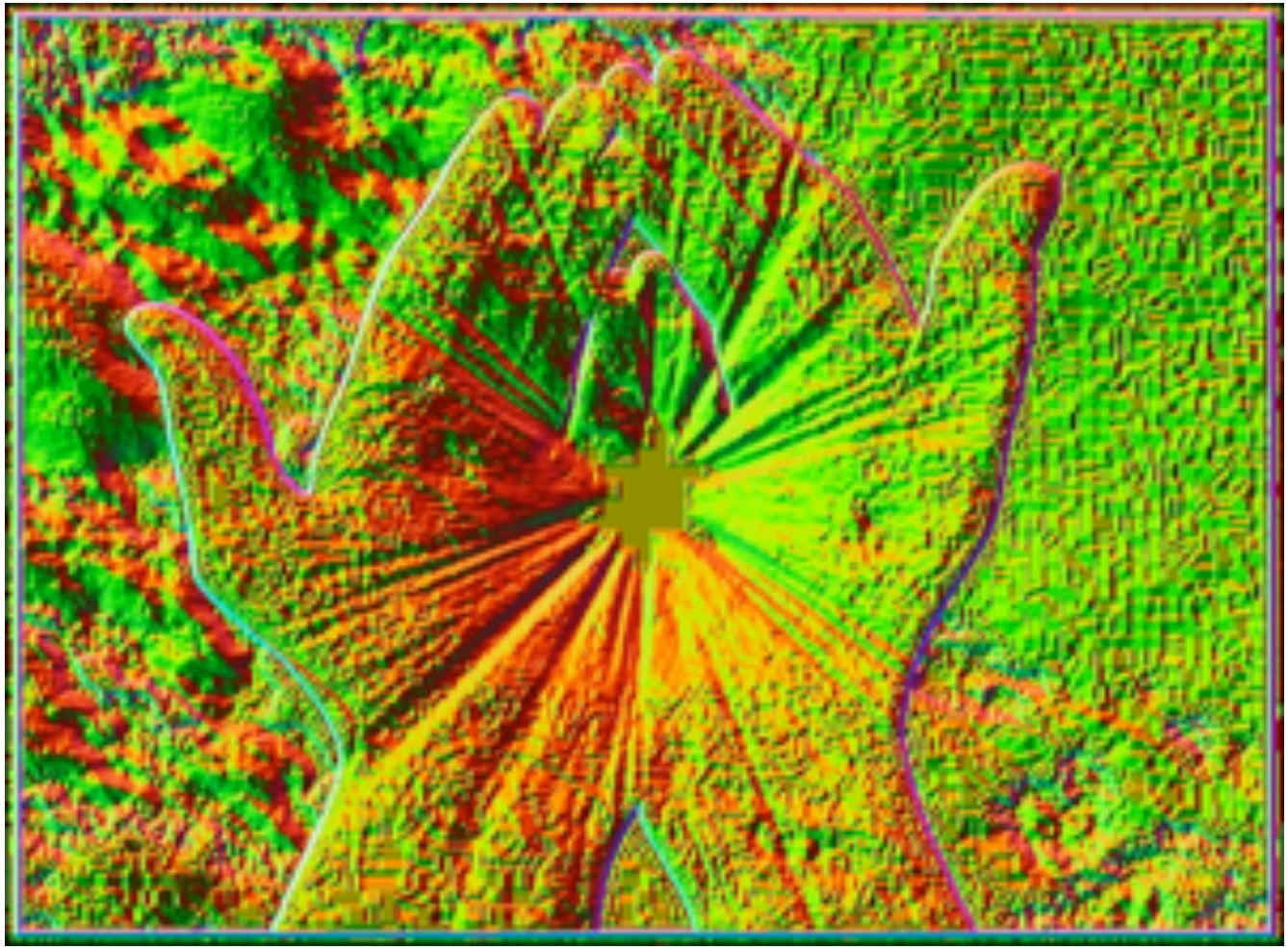


Image source: http://i146.photobucket.com/albums/r253/pjbaker_2006/hands.jpg

Copyright 2007-2008 Hacker Factor

Fun with Dubya

- President George W. Bush
  - January 2006
  - Visited the NSA (Fort Meade)
  - Photo from Newsweek & Washington Post
- Dshield and Nmap mailing lists

Copyright 2007-2008 Hacker Factor

It's a Trap!

http://images.insecure.org/nmap/images/wash-post-nsa.jpg
http://img378.imageshack.us/img378/5967/itsatrap7dz.jpg

Copyright 2007-2008 Hacker Factor

It's a Trap!

http://images.insecure.org/nmap/images/wash-post-nsa.jpg
http://img378.imageshack.us/img378/5967/itsatrap7dz.jpg

Copyright 2007-2008 Hacker Factor

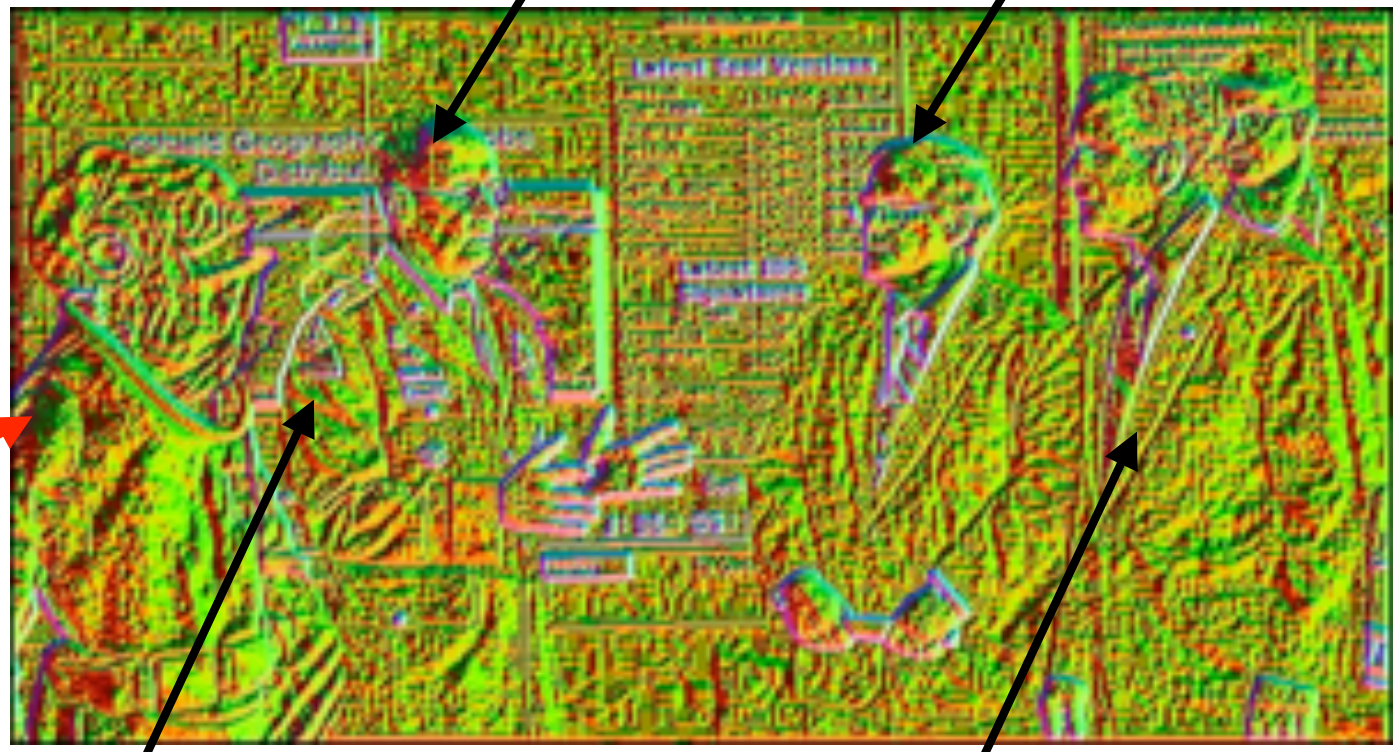
It's a Trap! (ELA)

Copyright 2007-2008 Hacker Factor

It's a Trap! (PCA)

Copyright 2007-2008 Hacker Factor

It's a Trap! (LG)



Copyright 2007-2008 Hacker Factor

Every Day with Rachael Ray

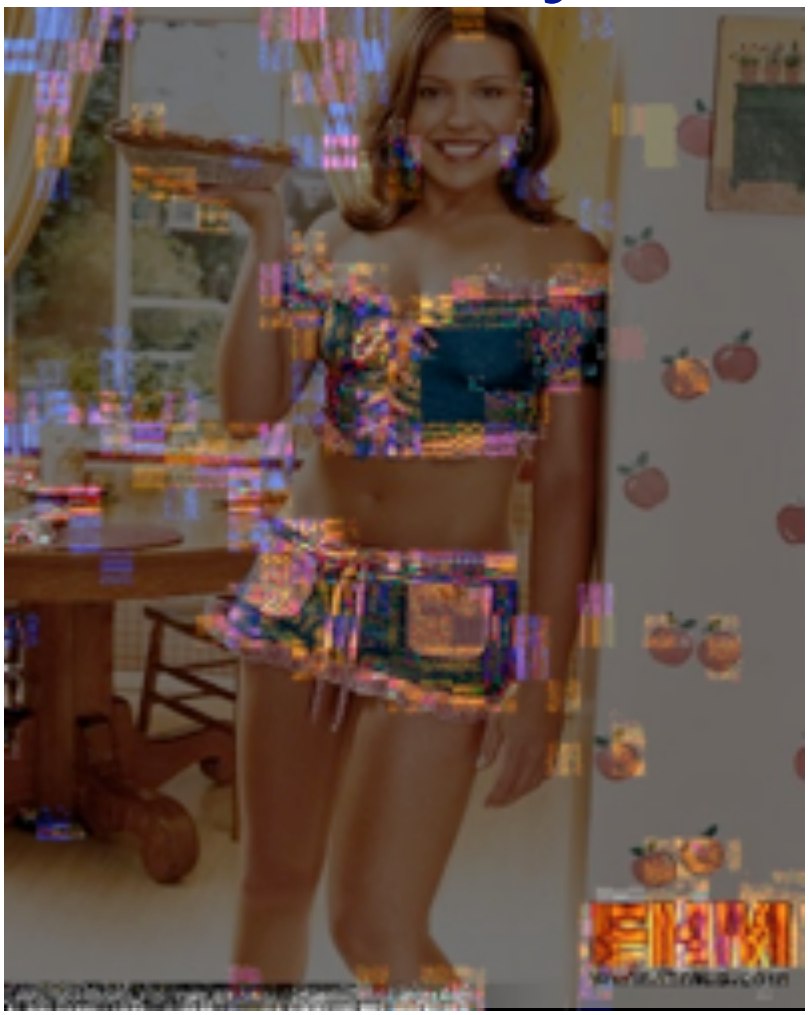
- FHM Magazine
  - October 2003
  - Later: Internet
- Adam Bates *claims* to have been looking at a cooking blog when he came across this picture. “Is this really her?”

Copyright 2007-2008 Hacker Factor

Rachael Ray: Observation

Copyright 2007-2008 Hacker Factor

Rachael Ray: ELA



Copyright 2007-2008 Hacker Factor

Rachael Ray: LG

Copyright 2007-2008 Hacker Factor

From the Photographer…

- Photographer:

  "This is Eric Cahan. I took the photos of rachael ray that appeared in FHM a few back [sic]. It's just bad over retouching that FHM did but it's her."
- Photoshop: Magic wand and "Liquify"
- Other pictures not tampered as badly

Copyright 2007-2008 Hacker Factor

Perfectly Imperfect

- Analysis Limitations
  - Image Quality
  - Algorithm Limitations
  - Humans…
- Overall Accuracy

Copyright 2007-2008 Hacker Factor

Limitations: Quality

- Size Matters
  - Small images: Wavelets fail (use > 300x300)
  - Very small images: ELA, PCA, LG fail
- Scaled Images
- Low Quality
  - Image corruption (resaves)
  - Limited-color (e.g., GIF or monochrome)
- Image coloring
  - High contrast
  - Specular reflections and “washed out” areas

Copyright 2007-2008 Hacker Factor

Limitations: Algorithm

- Wavelets and harmonics
- ELA and color selection
- Complex lighting and LG
- Mixing Media
  - From Photo to Magazine to JPEG…
  - Scanner, camera, video capture card

Copyright 2007-2008 Hacker Factor

Limitations: Humans…

- Human Interpretation
  - Algorithms only highlight
  - Humans interpret
- Extremely Talented Artists (rare)
  - Most people already have the tools
  - Better tools can be purchased
  - Few people have the skill

Copyright 2007-2008 Hacker Factor

Method Accuracy

- DoD Cyber Crime Center (DC3)
  - Blind test: “Real or CG?”
    - 51 images
    - 6 were “unknown” to the DC3
- Results
  - 86% accurate for known images
  - 0 false-positives (no “real” called “CG”)
  - 4 of 6 false-negatives were CG Society award winners

Copyright 2007-2008 Hacker Factor

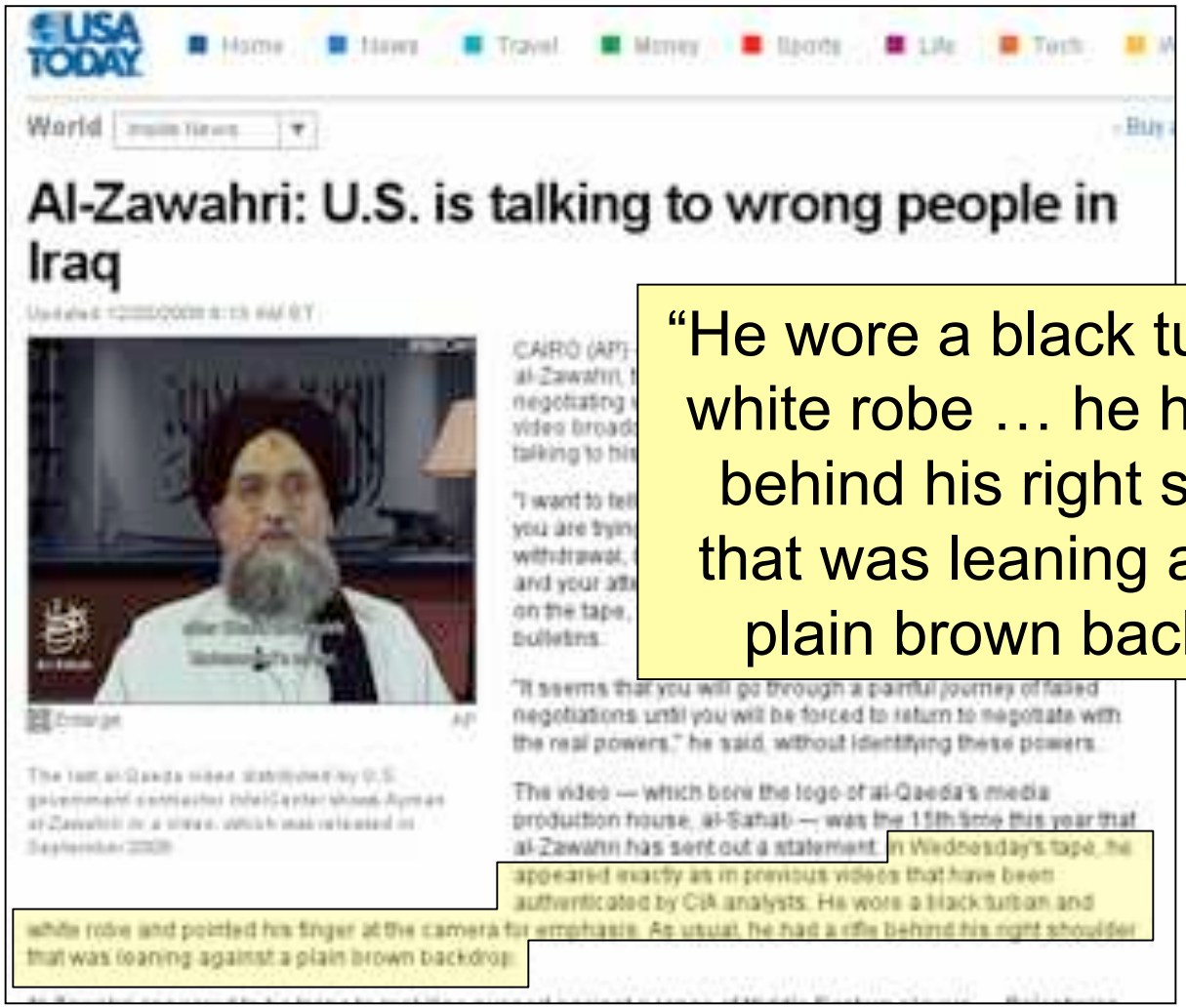
Case Study: Dr. Z

Dr. Ayman al-Zawahiri

#2 guy in Al Qaeda

Copyright 2007-2008 Hacker Factor

USA Today



USA TODAY

Home News Travel Money Sports Life Tech

World

Al-Zawahri: U.S. is talking to wrong people in Iraq

"He wore a black turban and white robe … he had a rifle behind his right shoulder that was leaning against a plain brown backdrop."

Copyright 2007-2008 Hacker Factor

USA Today Picture

"He wore a black turban and white robe … he had a rifle behind his right shoulder that was leaning against a plain brown backdrop."

Copyright 2007-2008 Hacker Factor

USA Today Picture

28-Sept-2006

20-Dec-2006

Copyright 2007-2008 Hacker Factor

USA Today Picture

IntelCenter

Copyright 2007-2008 Hacker Factor

What Else Added?

IntelCenter

- Last Things Added:
  - Image Cropped
    - Observed, to 8x8 grid
  - "IntelCenter"
  - Subtitles & Logo
  - Al-Zawahiri!
    - Outline = chroma key
  - Banner text!

Copyright 2007-2008 Hacker Factor

And in the Original?

Original

Error

PCA

LG

Copyright 2007-2008 Hacker Factor

And in the Original?

Original
Error
PCA
LG

Copyright 2007-2008 Hacker Factor

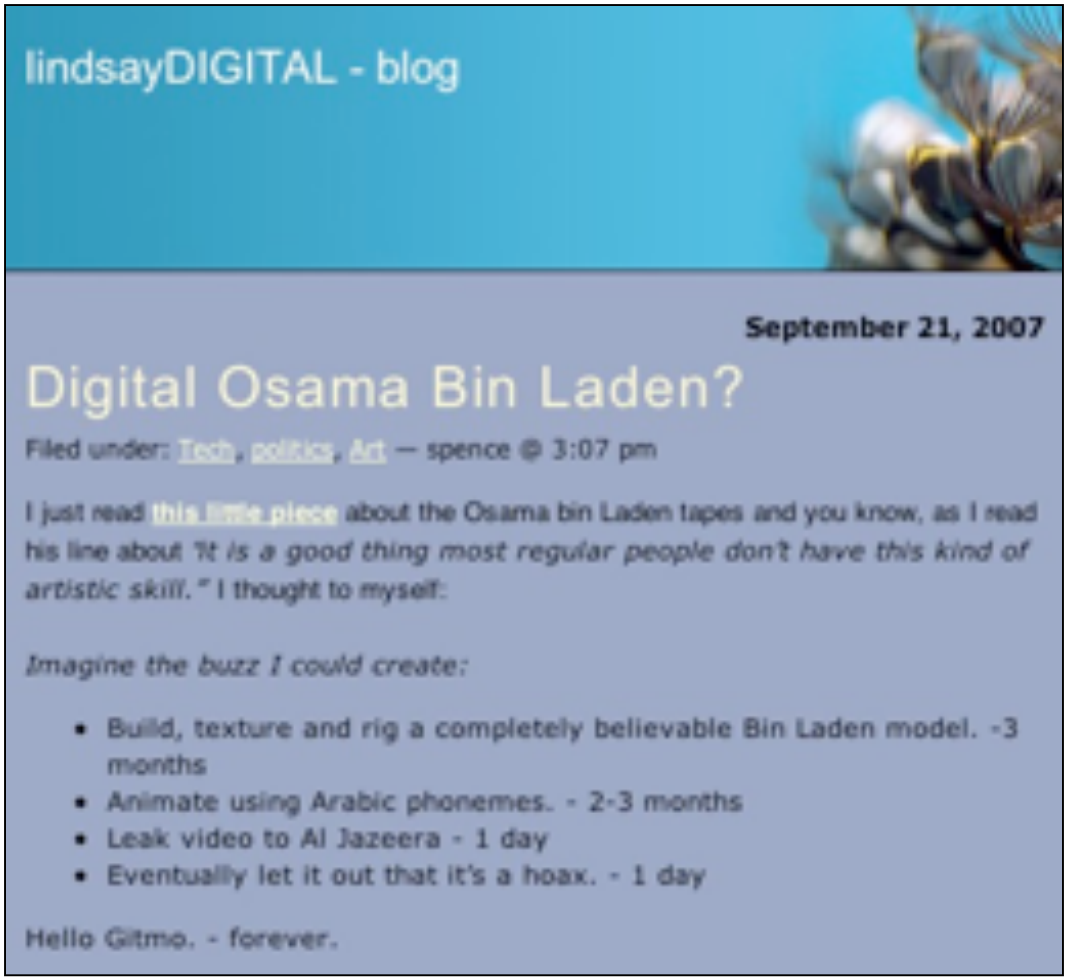
About the Room…

- Background is independent of Dr. Z
- Claims it was computer generated
  - Possibly 3D Studio Max
- Can the room be recreated?

Copyright 2007-2008 Hacker Factor

Recreating the Room?

lindsay|digital is a 3D design and visual effects studio in Pacific Grove, California run Spencer Lindsay, a 20-year veteran of digital design, game development and 3D design. He provides contract 3D modeling and Motion Graphics services.



lindsayDIGITAL - blog

September 21, 2007

Digital Osama Bin Laden?

Filed under: Tech, politics, Art — spence @ 3:07 pm

I just read this little piece about the Osama bin Laden tapes and you know, as I read his line about *"It is a good thing most regular people don't have this kind of artistic skill."* I thought to myself:

Imagine the buzz I could create:

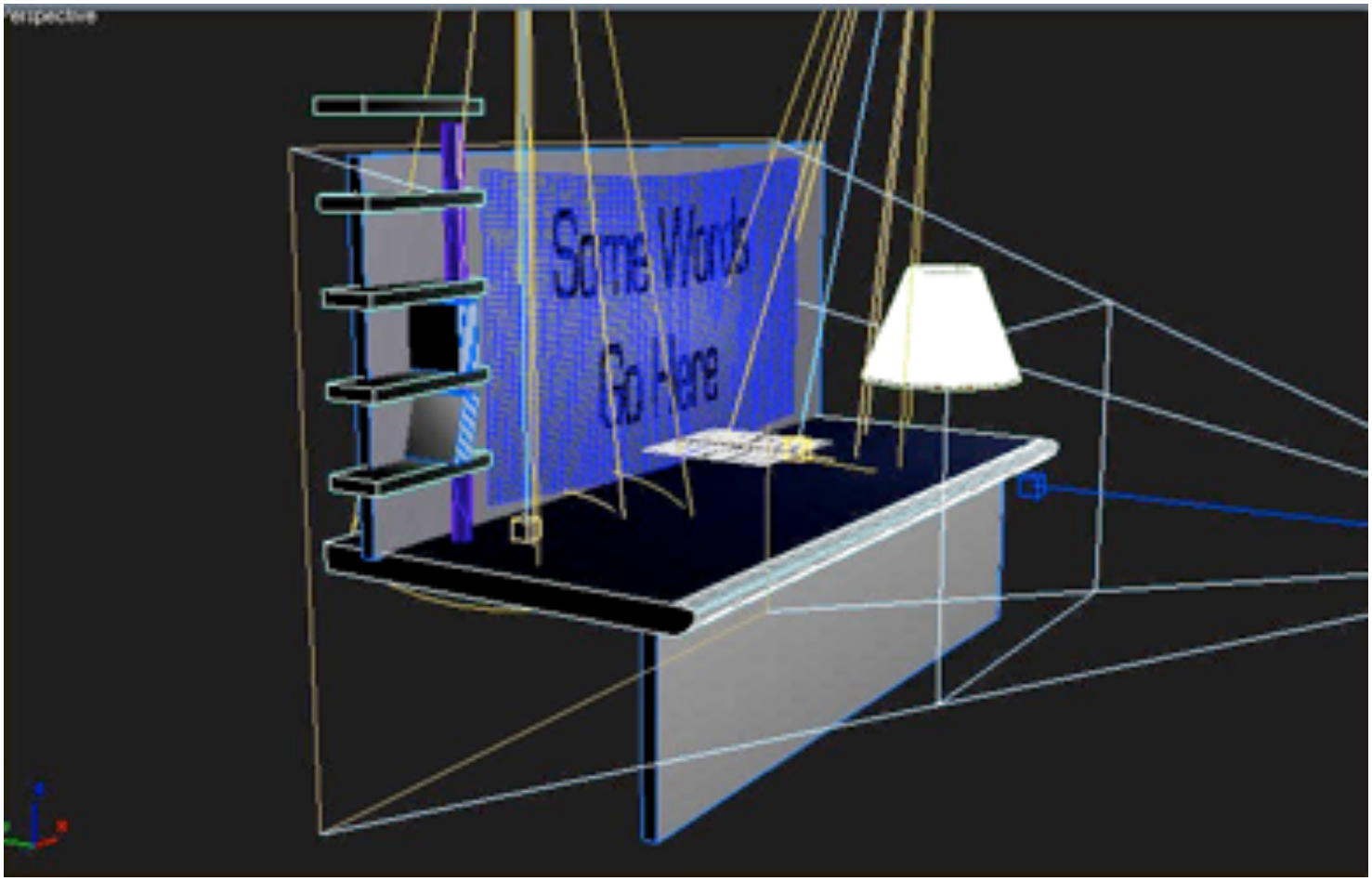
- Build, texture and rig a completely believable Bin Laden model. -3 months
- Animate using Arabic phonemes. - 2-3 months
- Leak video to Al Jazeera - 1 day
- Eventually let it out that it's a hoax. - 1 day

Hello Gitmo. - forever.

http://www.lindsaydigital.com/blog/wordpress/?p=90

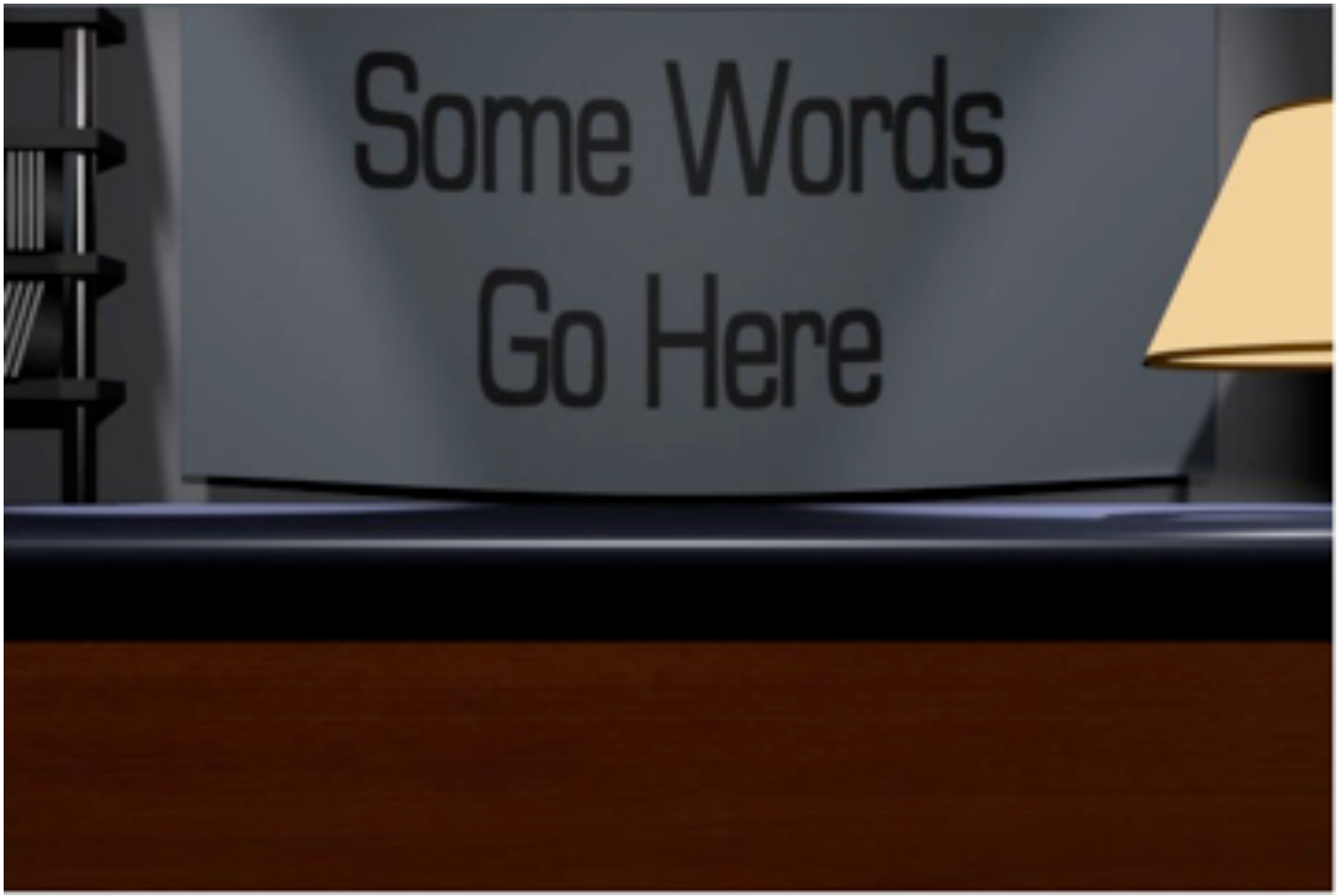
Copyright 2007-2008 Hacker Factor

The Room!

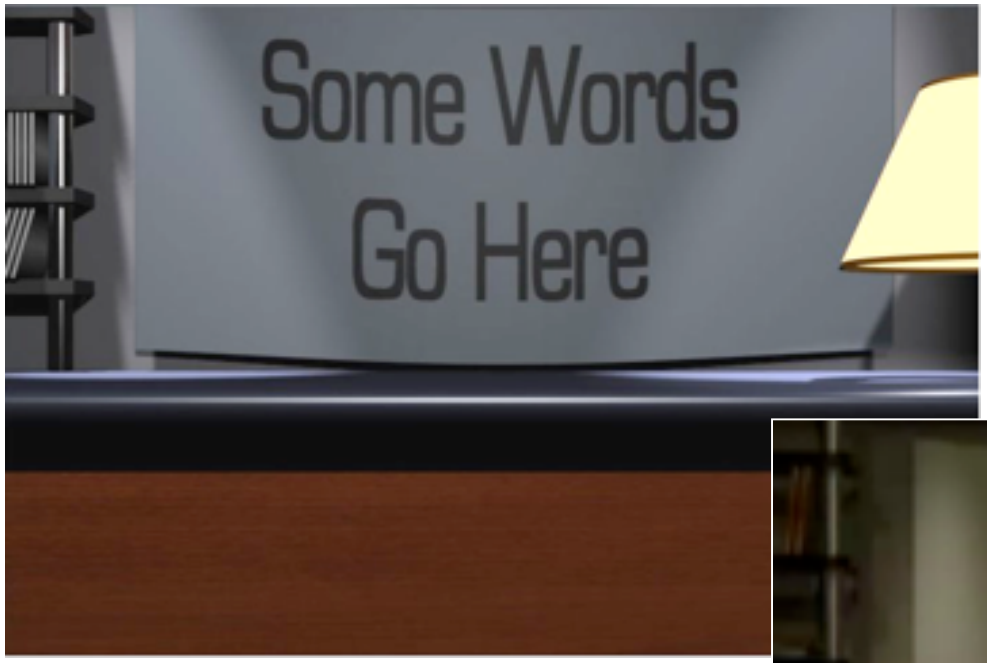


Copyright 2007-2008 Hacker Factor

The Room!



Copyright 2007-2008 Hacker Factor



Side by Side

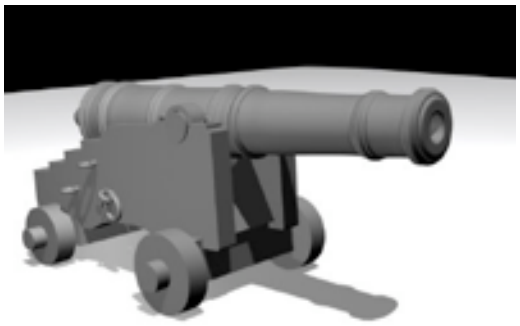
Copyright 2007-2008 Hacker Factor

What About the Cannon?

- Cannon
  - Blurry, low-res
  - Style:
    - 18th Century British Naval Cannon
  - Carriage
    - Stepped wood
    - No visible slats
    - Big wheel in front
  - Trunnion inset in top

Copyright 2007-2008 Hacker Factor

CG Cannon?



- http://www.turbosquid.com/FullPreview/Index.cfm/ID/253444
- Missing big tire
- 3D model: $39

- http://www.turbosquid.com/FullPreview/Index.cfm/ID/255325
- Looks much closer
- 3D model: $34.75

Copyright 2007-2008 Hacker Factor

What About Other Videos?

27-July-2006

Zawahiri Video Speech Regarding Lebanon and Gaza

Copyright 2007-2008 Hacker Factor

Analysis: Error Level and PC1

Error

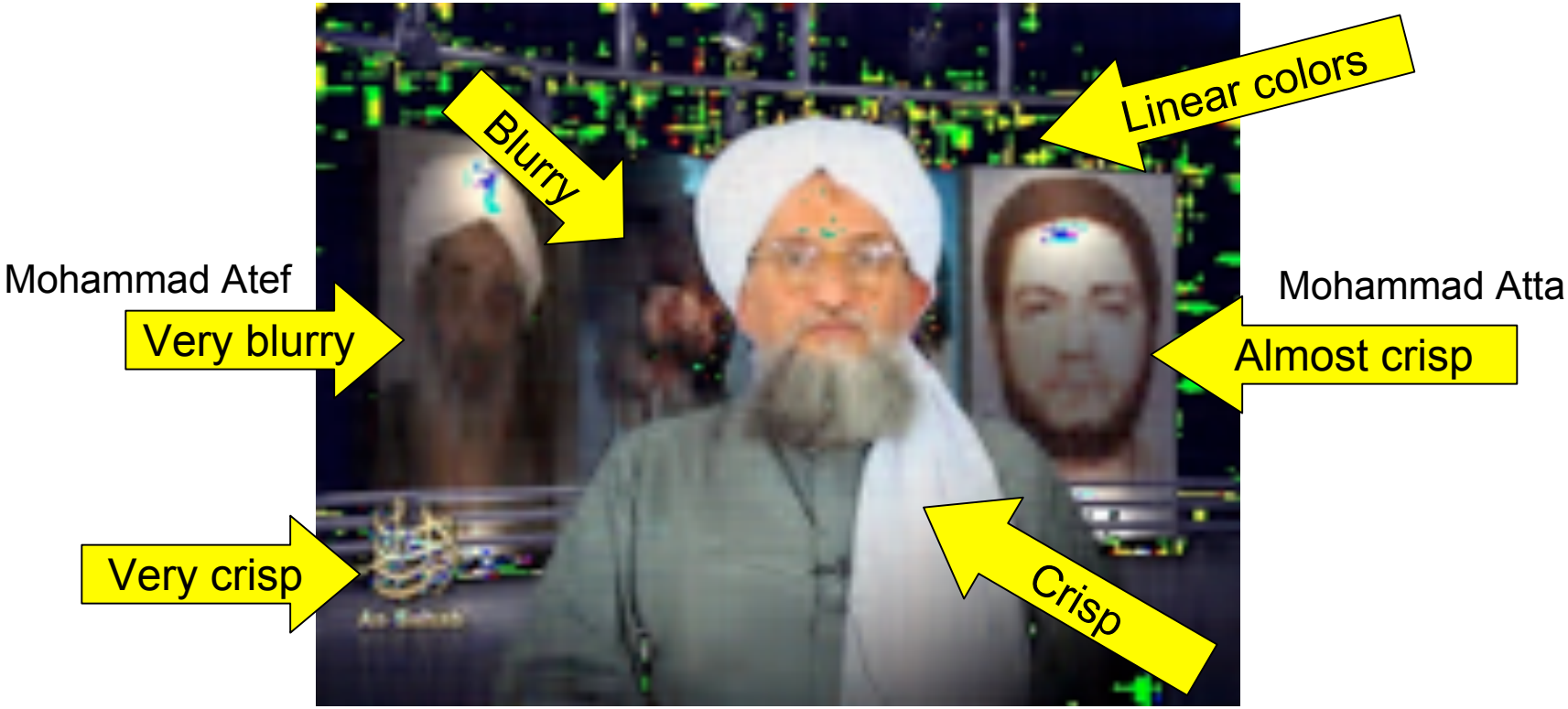
PCA

Copyright 2007-2008 Hacker Factor

Analysis: PC3!

Copyright 2007-2008 Hacker Factor

Wavelets 5%: 6 Layers!



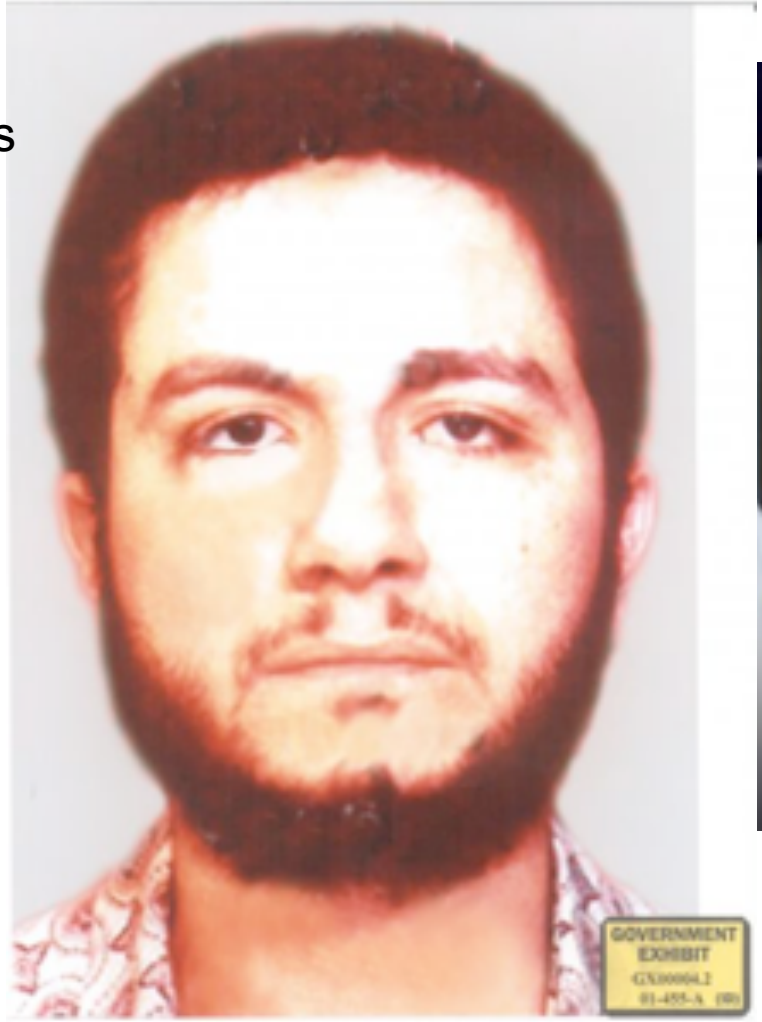
Ayman al-Zawahiri

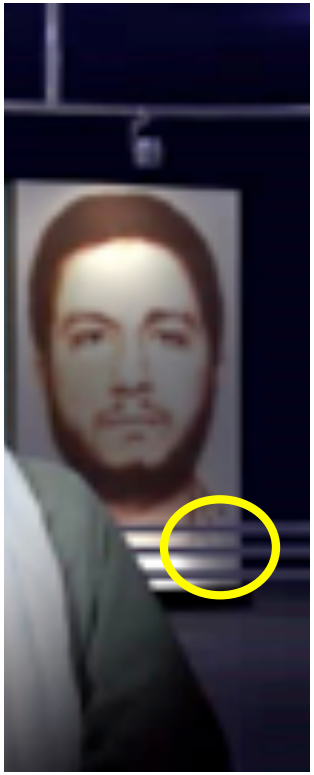
Copyright 2007-2008 Hacker Factor

Mohammad Atta

Made in Layers

Identify any sources?





Copyright 2007-2008 Hacker Factor

SITE Seeing

- *Saying* that there is a green screen is **not** the same as *seeing* the green screen

- SITE Institute (www.siteinstitute.org)
  - 22-Jan-2007: Intercepted Al Qaeda video!
  - 25-Jan-2007: Video released by Al Qaeda

Copyright 2007-2008 Hacker Factor

Back in Black

Copyright 2007-2008 Hacker Factor

Lighting

Copyright 2007-2008 Hacker Factor

Green Screen Fun

Copyright 2007-2008 Hacker Factor

Green Screen Fun

Copyright 2007-2008 Hacker Factor

Green Screen Fun

PC1

Copyright 2007-2008 Hacker Factor

Azzam al-Amriki

2-Sept-2006

Copyright 2007-2008 Hacker Factor

Azzam al-Amriki

2-Sept-2006

Copyright 2007-2008 Hacker Factor

Azzam al-Amriki

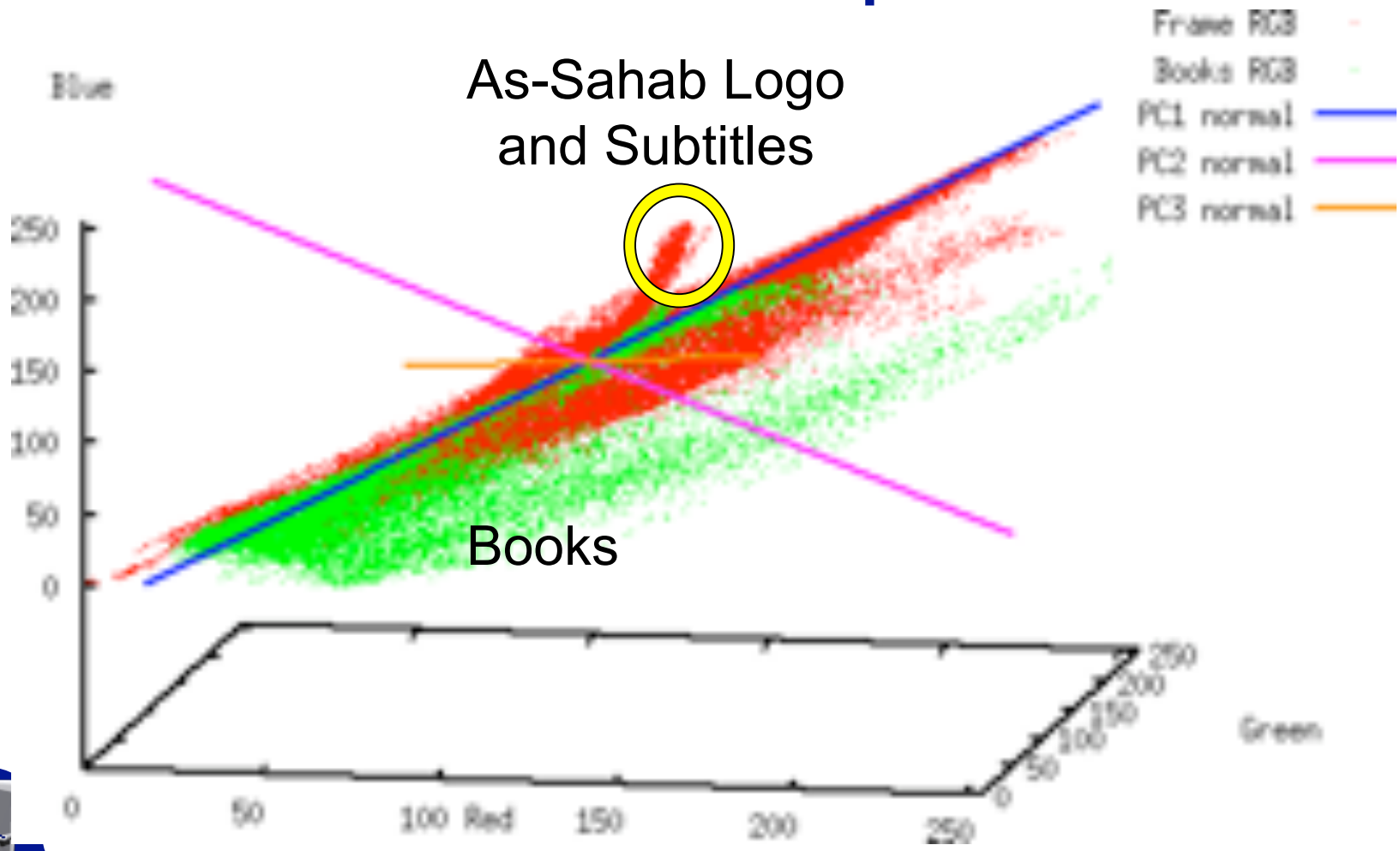
Logo

Books?

2-Sept-2006

Copyright 2007-2008 Hacker Factor

Color Graph



Copyright 2007-2008 Hacker Factor

Case Study
Bin Laden's Beard

Copyright 2007-2008 Hacker Factor

The Big Gap

- 29-Oct-2004: “Graybeard”
  - 14 minute video
  - Only aired on Al Jazeera
  - Screen shots and low quality video available online
- 7-Sept-2007: “Blackbeard”
  - First video in nearly three years
  - Released online!
  - Lots and lots of oddities…

Copyright 2007-2008 Hacker Factor

Graybeard Video

- 29-Oct-2004
  - Very low quality videos available online
  - Better quality only via screen shots

Copyright 2007-2008 Hacker Factor

Blackbeard Video

- 7-Sept-2007
  - 26 minute video titled “The Solution”
  - Released online (677 Meg MPG)

Copyright 2007-2008 Hacker Factor

7-Sept-2007 Video Timeline

- 26 minute video
  - Total: 3.5 minutes of animation
  - Current events only mentioned after audio splice and during frozen frames

Copyright 2007-2008 Hacker Factor

Animation Oddity

- Animated segments are different!

Frame 1:56

Frame 12:47

Copyright 2007-2008 Hacker Factor

Animation Oddity

- Animated segments are different!

Frame 1:56

Frame 12:47

Copyright 2007-2008 Hacker Factor

Animation Oddity: Wider

Frame 1:56 Frame 12:47

Copyright 2007-2008 Hacker Factor

The Big Question: "Is the Black Beard Real?"

Could it be digitally modified?

Copyright 2007-2008 Hacker Factor

Image Analysis

2004

2007 - 2nd segment

Copyright 2007-2008 Hacker Factor

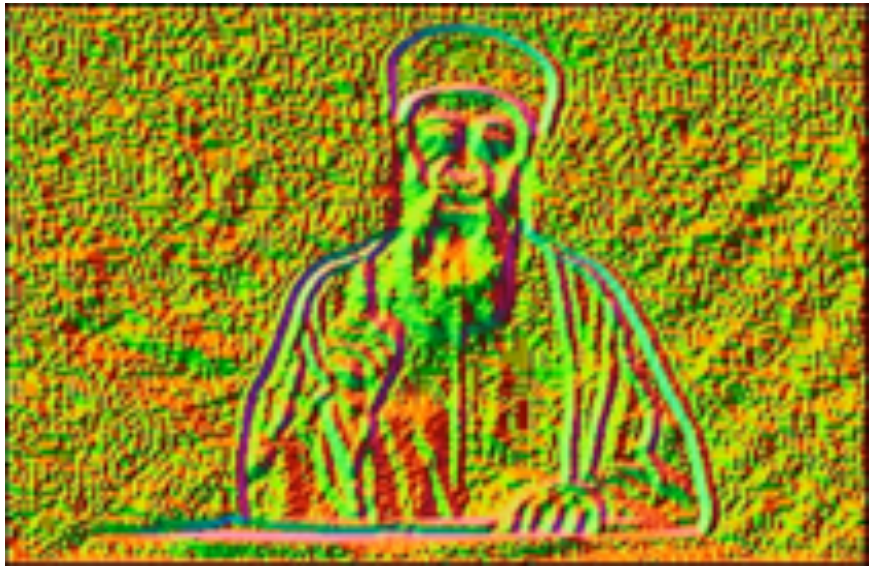
Image Analysis

2004

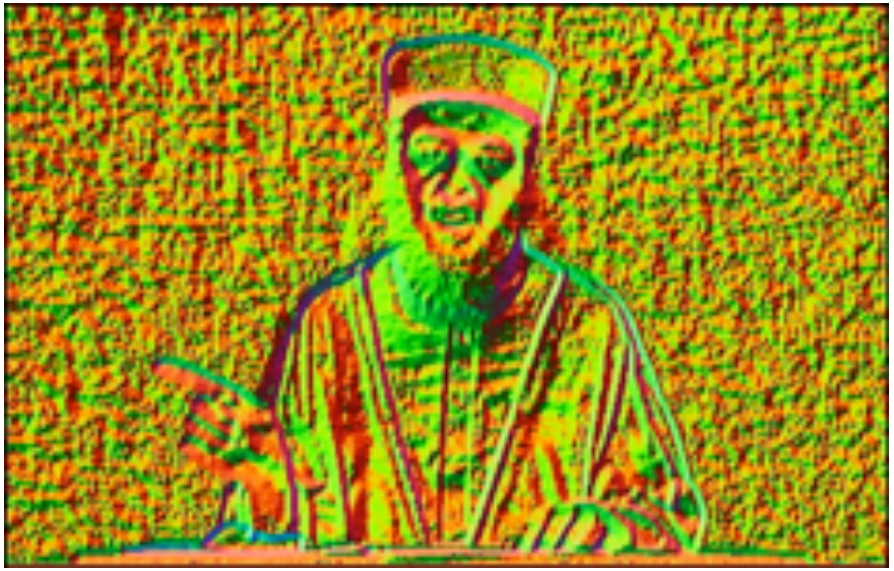
2007 - 2nd segment

Copyright 2007-2008 Hacker Factor

Image Analysis



2004



2007 - 2nd segment

Copyright 2007-2008 Hacker Factor

What Can We Tell?

- No indication of digital manipulation
- Similar lighting
- Similar clothing
- Similar background
- Anything else?
  - Camera angle, aspect ratio, and coloring

Copyright 2007-2008 Hacker Factor

Camera Setting

2004

2007 - 2nd segment

Copyright 2007-2008 Hacker Factor

Camera Setting

ent

Copyright 2007-2008 Hacker Factor

Recolor Image

2004

2007 - 2nd segment

Copyright 2007-2008 Hacker Factor

Analysis Summary

- No indication of digital modification
- Align on eyes
  - Same eyes, eyebrows, nose, mouth, hairline
  - Shoulder position matches
  - Hat is worn higher
  - Desk and papers align
  - SAME ASPECT RATIO
  - Overall color of 2004 likely altered during post-processing
- Implies
  - Extremely similar setting, lighting, camera setup
  - Same person but with a different beard

Copyright 2007-2008 Hacker Factor

What About the Beard

- Option #1: All recorded in 2004
- Option #2: Recreation

Copyright 2007-2008 Hacker Factor

Beard Option #1

- Option 1: All video recorded in 2004
  - Similar set, lighting
  - Similar camera position and aspect ratio
  - Similar clothing & hairline
- Implies:
  - Dyed or costume beard
    - Gray beard is larger with dark edges
    - Gray is likely fake
  - Multiple recordings hours or days apart
  - 2007 audio is dubbed
  - No Bin Laden since 2004

Copyright 2007-2008 Hacker Factor

Beard Option #2

- Option 2: Recreation
  - Recreated lighting and set (including papers)
  - Recreated camera position and aspect ratio
  - Match clothing, hairline
  - And all 3 years later!
- Implies:
  - Significance to the set
    - But the set is plain…
    - Forgot beard, robe…
  - Bin Laden dyed beard
  - Beard shrank in length

Copyright 2007-2008 Hacker Factor

Which Option is Right?

- Cannot tell from image analysis
- Practical view: Occam's Razor
  - Simplest solution is likely correct.
  - Which is simpler?
    - Recording all video at once, and releasing over the years with audio-dubbed current events
    - Recreating the set, lighting and minutia but forgetting the big things

Copyright 2007-2008 Hacker Factor

Conclusion

Copyright 2007-2008 Hacker Factor

Need for Image Analysis

- Real versus Computer Generated
- If Modified, How?
- Uses
  - Media: Reality vs Fiction
  - Legal: Child Pornography vs VCP
  - Authentication: Real vs Doctored

Copyright 2007-2008 Hacker Factor

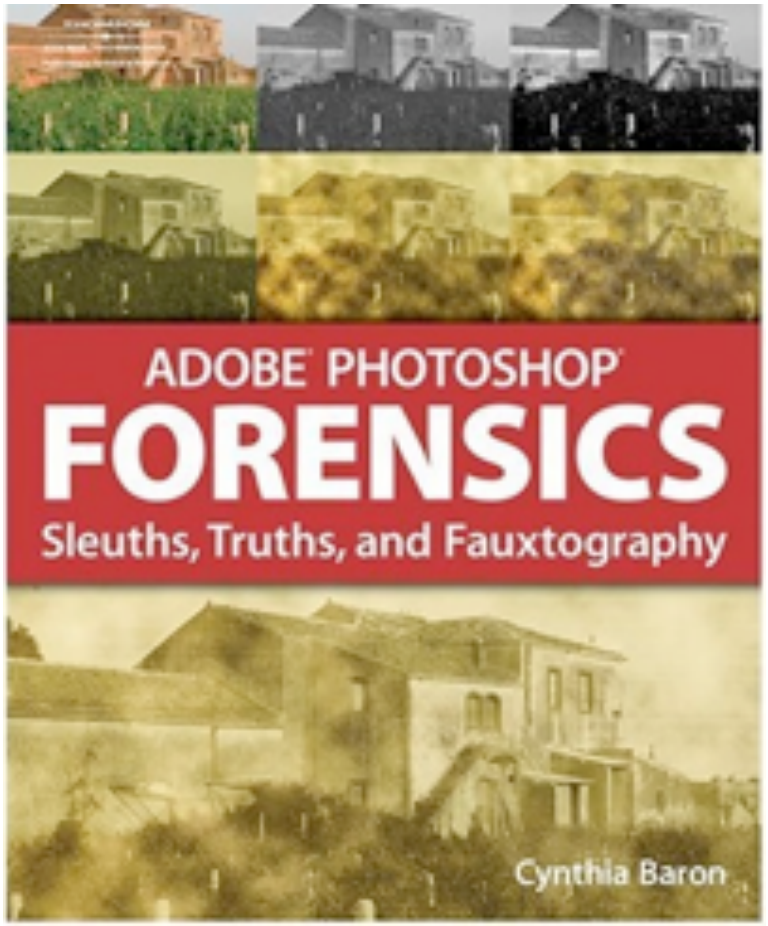
Methods Covered

- Observation
- Basic Image Enhancements
  - Color Tweaking
- Image Format Analysis
  - Meta Data Analysis
  - Quantization Table Finge
  - Estimated Compression I
- Advanced Image Analys
  - Error Level Analysis
  - Principle Component Ana
  - Wavelet Transformations
  - Luminance Gradient

Other types of analysis:
Shadow Detection
Mixture of Gaussians
Minimum Variance Color Selection
Minimum Variance Quantization
K-Means
Scale-Invariant Feature Transform
Signal-to-Noise Ratio
Color Filter Array Detection
... and the list goes on ...

Copyright 2007-2008 Hacker Factor

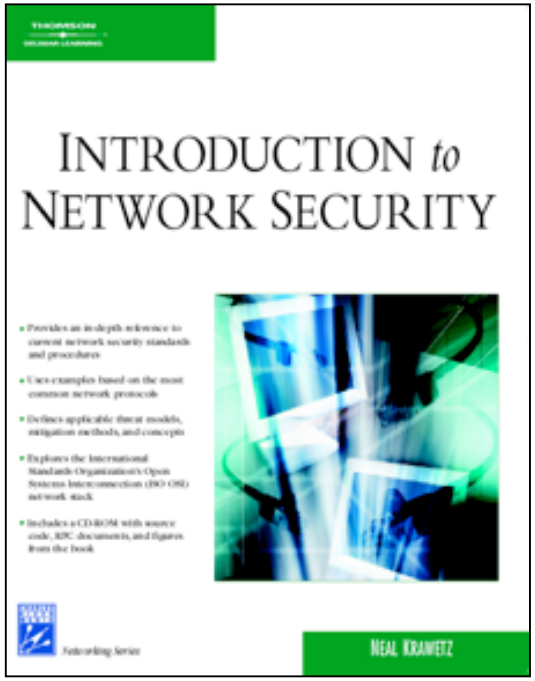
Where to Start?



Copyright 2007-2008 Hacker Factor

Questions?

Shameless self-promotion.



Dr. Neal Krawetz
Hacker Factor Solutions
www.hackerfactor.com

Copyright 2007-2008 Hacker Factor

Acknowledgements

Thanks to the following people:

Cynthia Baron, Northeastern University

Adam Bates, University of Colorado at Boulder

Paul Whyman and Bob Gobeille

Spencer Lindsay, lindsayDIGITAL

Pedro Bueno, Internet Storm Center

Hany Farid, Dartmouth College

Mark Rasch, J.D.

Department of Defense Cyber Crime Center

Copyright 2007-2008 Hacker Factor