

Overview

- Some Tools of the Trade

- Image/ Graphics Forensics
 - How Forensic Experts Uncover Doctored Images
 - Doctored Photography
 - Types of Graphical File Formats



Some Tools of the Trade

- This rugged briefcase device enables investigators to **extract data from 220 various cell phones and PDAs**
- Displays the downloaded records and can retrieve data such as **incoming and outgoing calls, text messages, voicemail, photos, and video**, allowing forensics investigators to gather intelligence without tampering
- Federal Agencies use this – recently featured in a CSI: NY episode – terrorists, blown up phone

CellIDEK®



Some Tools of the Trade

- When forensic tools are unable to capture data from an obscure or new mobile phone it can mean reverting to a painstaking manual process of photographing each screen.
- This **fixed digital camera** is used to capture screens from phones, a time-consuming process that can run to hundreds of images but is necessary to produce screenshots to show in court



Some Tools of the Trade

XBox Forensics

<http://www.physorg.com/news160304799.html>

Criminals often **hide illicit data on the Xbox** in the hope that a gaming console will not be seen as a likely evidence target especially when conventional personal computers are present in the same premises, for instance.

The toolkit developed by Computer Scientist, David Collins allows police and other investigators the chance to lay bare the contents of Xbox hard disks



Tools for the Would-Be-Hacker?

This degausser generates a magnetic field to wipe clean any hard disks and other storage devices.

Comes with a remote control that looks like a car central locking key ring to allow it to be used from a safe distance.

Stand back at least 2 m otherwise it can be dangerous if you have a pacemaker and it can't be used too close to other equipment because it resets a lot of the machines

Why would a forensics expert also use/want this degausser



Key Concepts

- Fraudulent photographs produced with powerful, commercial software appear constantly, spurring a new field of digital image forensics.
- Algorithms are used (check out Dartmouth)
 - Many fakes can be exposed using algorithms because of inconsistent lighting, including the specks of light reflected from people's eyeballs (specular highlights).
 - Algorithms can spot when an image has a “cloned” area or does not have the mathematical properties of a raw digital photograph.
 - (Exchangeable Image File - EXIF)

Qinghai-Tibet rail line + Endangered Tibetan Antelopes living in harmony? (2008)



The Fake Exposed



Iranian Missile (2008)

“original”

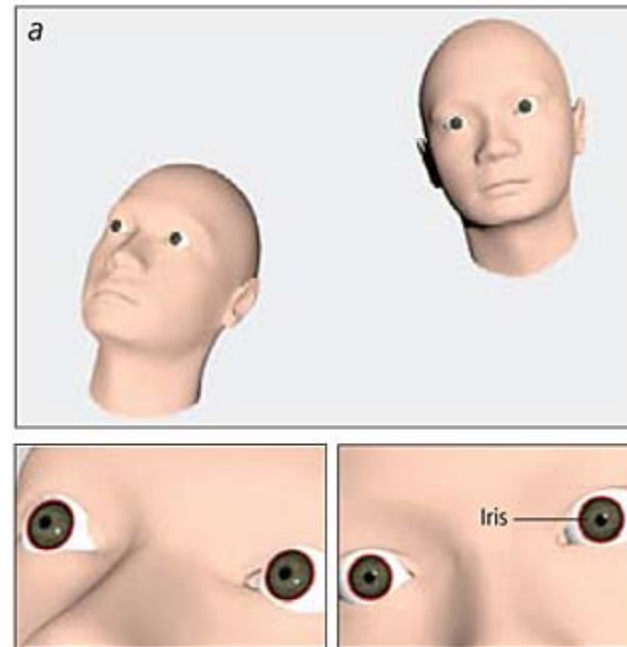


“edited”



4 Ways to Spot a Fake – 1. Eye Position

- Because eyes have very consistent shapes, they can be useful for assessing whether a photograph has been altered
- A person's **irises** are **circular in reality** but will **appear increasingly elliptical as the eyes turn to the side or up or down**
- An algorithm can approximate how eyes will look in a photograph by tracing rays of light running from them to a point called the camera center



4 Ways to Spot a Fake – 2. Direction of Light Source

- Were the ducks or the MPs added?



4 Ways to Spot a Fake – 3. Specular Highlights

Q. Were these 4 hanging out together for the photograph?

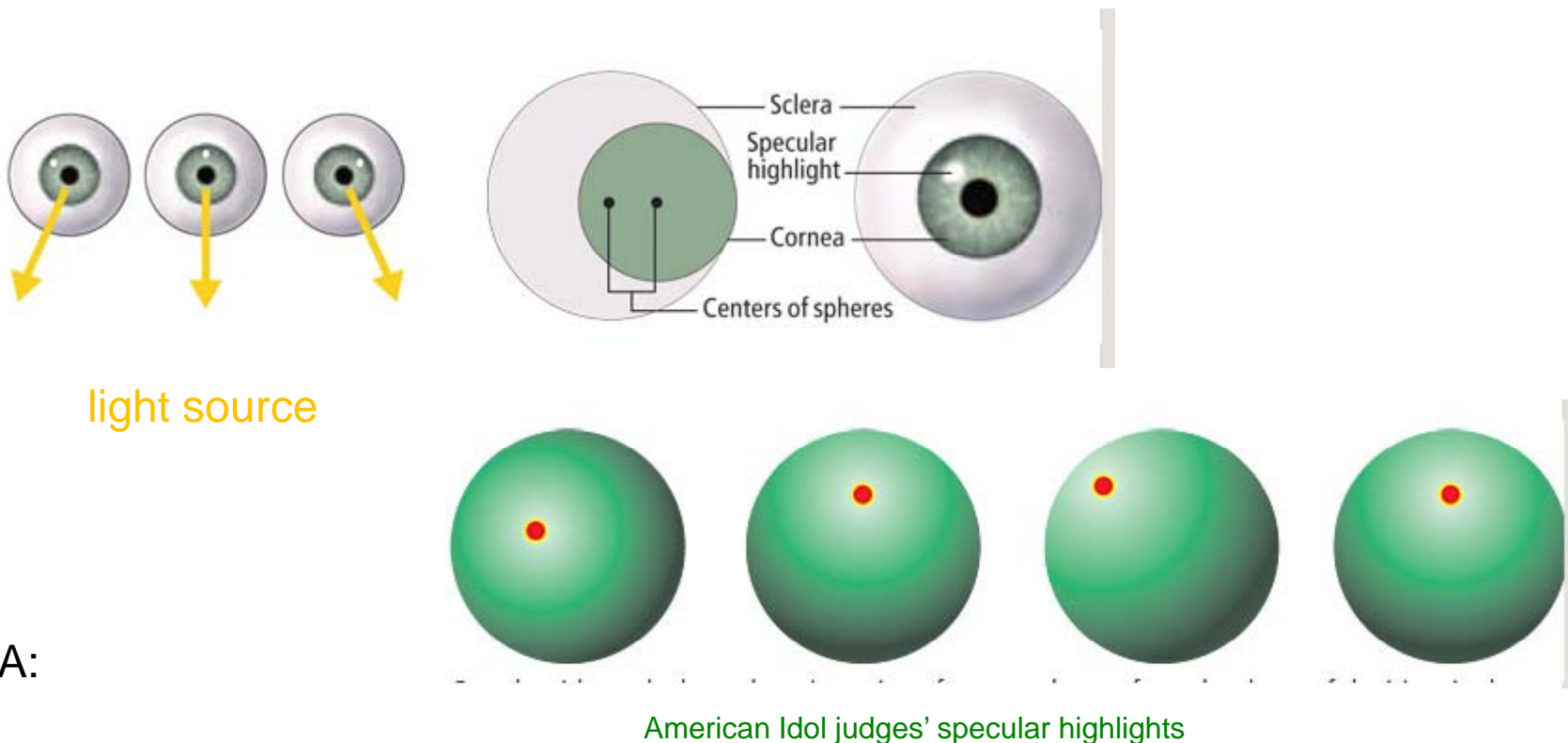
Surrounding lights reflect in eyes to form small white dots called **specular highlights**.

The **shape, color and location** of these **highlights** give us info about the lighting



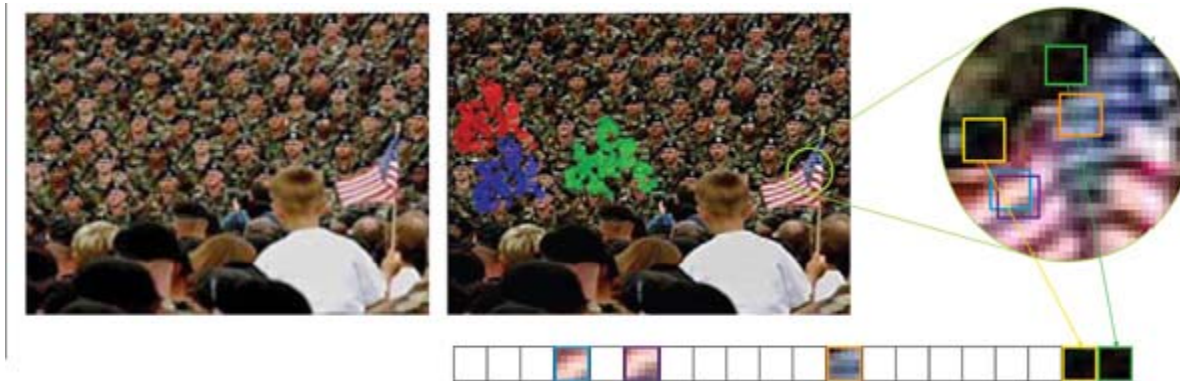
Doctored?

- The highlight position indicates where the light source is located.
- As the direction to the light source (*yellow arrow*) moves from left to right, so do the specular highlights.
- Many cases, however, require a **mathematical analysis**. To determine light position precisely requires taking into account **the shape of the eye and the relative orientation between the eye, camera and light**



4 Ways to Spot a Fake – 4. Finding Cloned Regions

- Political Ad from a 2004 US election campaign
- Algorithm scans image and for, say a 6x6 block image, characterizes the make-up of color (pixels)
- When the algorithm is applied to the image below from the political ad, it detects three identical regions (red, blue and green).



Recognizing a Graphics File

- Bitmap images
 - Collection of dots or pixels in a grid format that form a graphic

- Vector graphics
 - Based on mathematical instructions that define lines, curves, text, ovals and other geometric shapes

- Metafile graphics

- When you use a graphics editor/ image viewer you can open a file in one of many graphics file formats - .bmp, .jpg, .gif – save in a different format - but that changes the quality (jpg, gif compressed ‘map of bits’)

- Raster images
 - Pixels are stored in rows for easier printing (rasterize an image)

- Resolution

Exchangeable Image File Format (EXIF)

- Most cameras store graphics files as EXIF JPEG
- When a digital picture is taken, certain information is stored in the graphics file such as:
 - shutter speed
 - focal length
 - resolution
 - date/ time
- Since EXIF format collects metadata, investigators can learn more about the type of digital camera and the environment in which the pictures were taken

Digital Forensics Throughout History

- Why is the understanding of “adding” and “deleting” (“photoshopping”) of people and items important in digital forensics?



Circa 1860: Lincoln-Calhoun



Circa 1930: Stalin



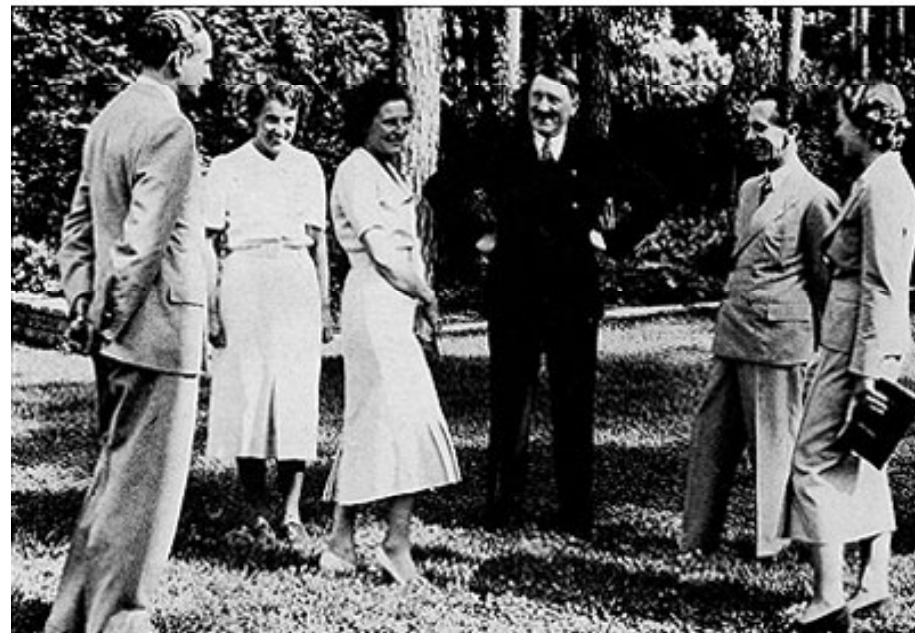
What digital forensic algorithm could be used to showcase the removal?



Circa 1936: Mao Zedong unhearts Po Ku



Circa 1937: Hitler unhearts Goebbels



Circa 1997: Luxor, Egypt

