How To Track Down Your Ex(if)

Adding Jpeg Exif detection to your penetration regiment and learning how to practice Safe (s)Exif

Jay Ball, GSNA, CISSP, CRISC

Aspect Security | 9175 Guilford Road, Suite 300 | Columbia, MD 21046 | www.aspectsecurity.com

ASPECT SECURITY
Application Security Experts

AGENDA

Hello OWASP

Breaker

- Real-World Scenario
- Discuss Photos & EXIF
- New Hacking Toys

Builder & Defender

Future

Conclusions

ASPECT SECURITY
Application Security Experts

BREAKER

ASPECT SECURITY
Application Security Experts

VIRTUAL EDUCATION SITE

Scenario: distance learning website

Two-way, multi-user video chat infrastructure

Teachers and students post profile pictures

Authenticated user can browse peers

Anybody can browse instructors

Lessons occur in-home or in-office

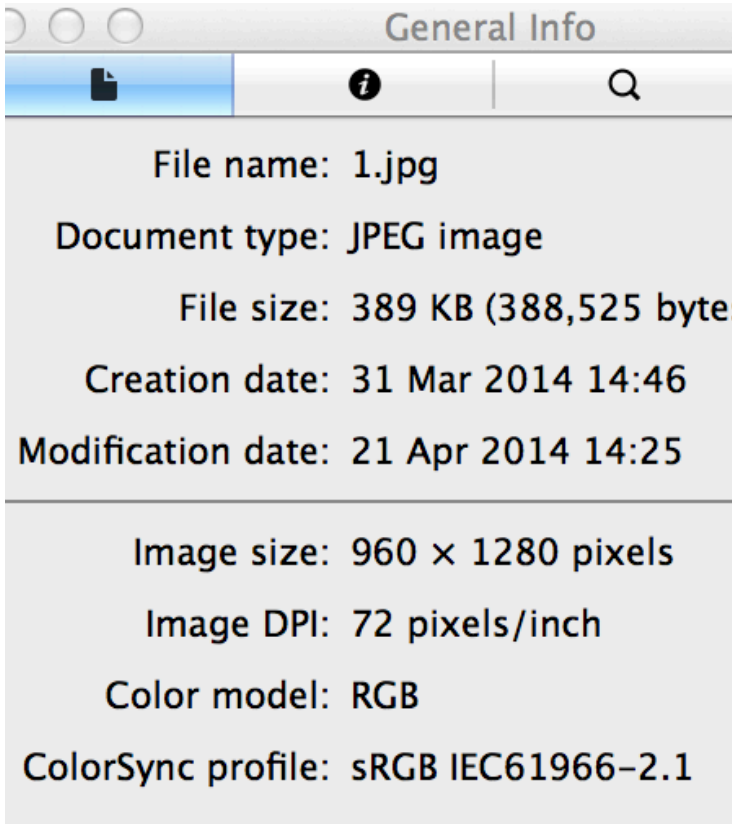
Privacy of the users is important

ASPECT SECURITY
Application Security Experts

EXAMPLE PROFILE PICTURE

- Attractive lady
- Lower part of a house
- Stairwell that goes half a floor up
- White steel door with a metal mail slot

DEEPER LOOK

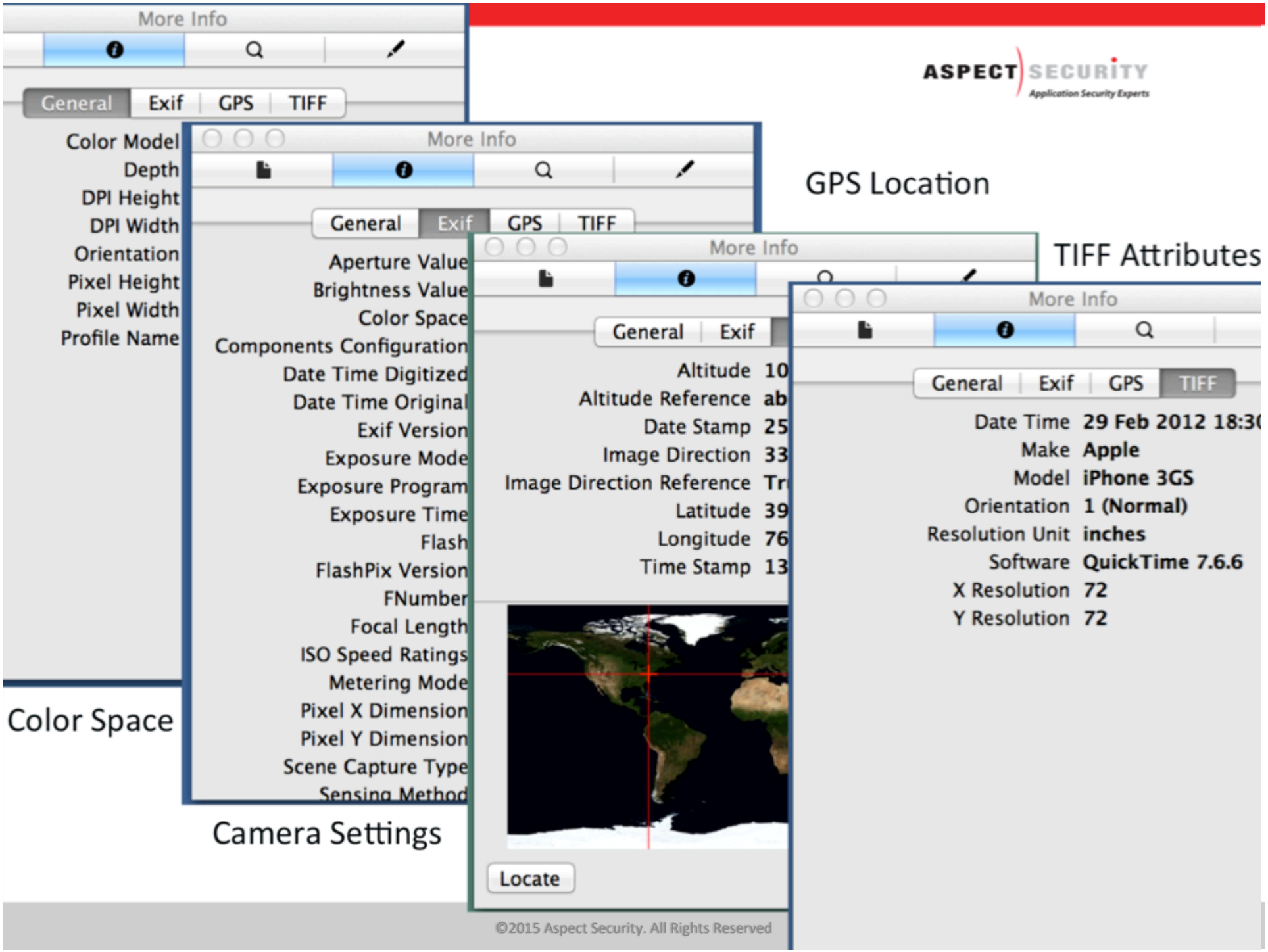


Save image file to disk and examine it

On OS X, use Preview

- Other tools on Windows
- exifdata.com
- readexifdata.com

This gives us all kinds of basic information, like file size, resolution, creation date, …

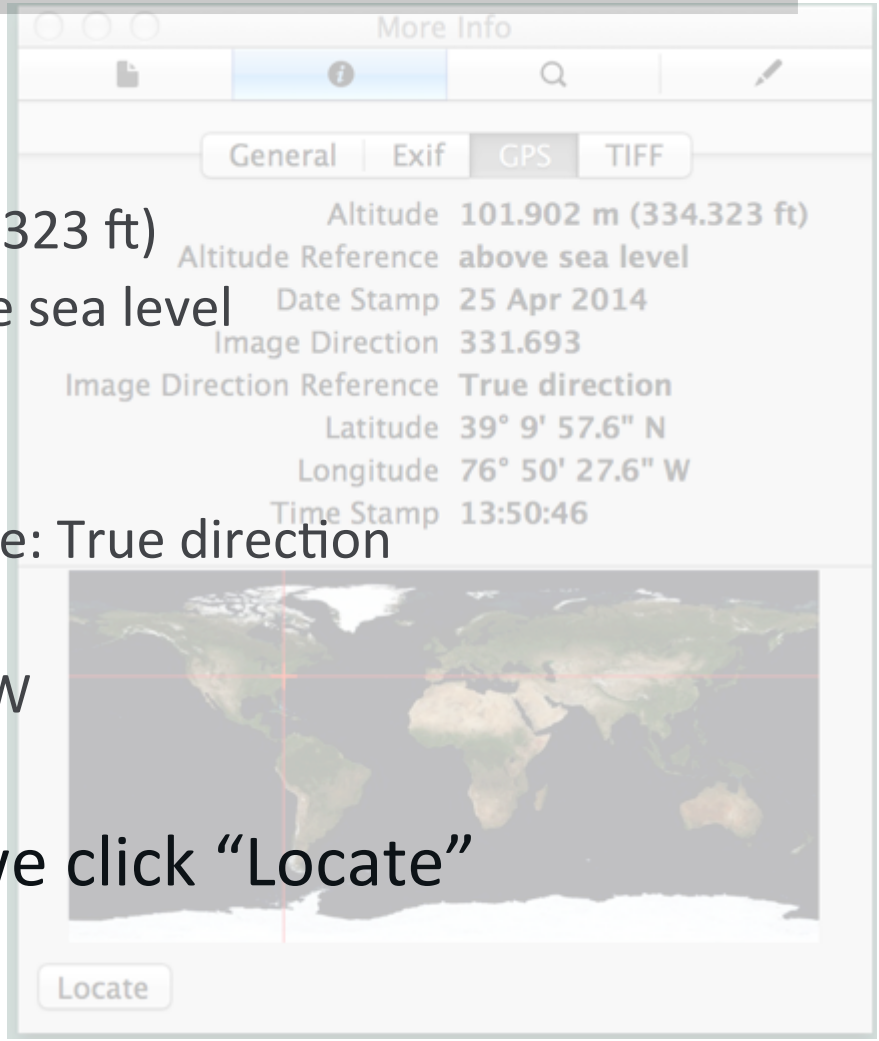

More Info
General
Exif
GPS
TIFF
Color Model
Depth
DPI Height
DPI Width
Orientation
Pixel Height
Pixel Width
Profile Name
Color Space
ASPECT SECURITY
Application Security Experts
GPS Location
TIFF Attributes
Aperture Value
Brightness Value
Color Space
Components Configuration
Date Time Digitized
Date Time Original
Exif Version
Exposure Mode
Exposure Program
Exposure Time
Flash
FlashPix Version
FNumber
Focal Length
ISO Speed Ratings
Metering Mode
Pixel X Dimension
Pixel Y Dimension
Scene Capture Type
Sensing Method
Camera Settings
Altitude 10
Altitude Reference ab
Date Stamp 25
Image Direction 33
Image Direction Reference Tr
Latitude 39
Longitude 76
Time Stamp 13
Locate
Date Time 29 Feb 2012 18:3
Make Apple
Model iPhone 3GS
Orientation 1 (Normal)
Resolution Unit inches
Software QuickTime 7.6.6
X Resolution 72
Y Resolution 72
©2015 Aspect Security. All Rights Reserved

WAIT A SEC… GPS?

Full GPS included:

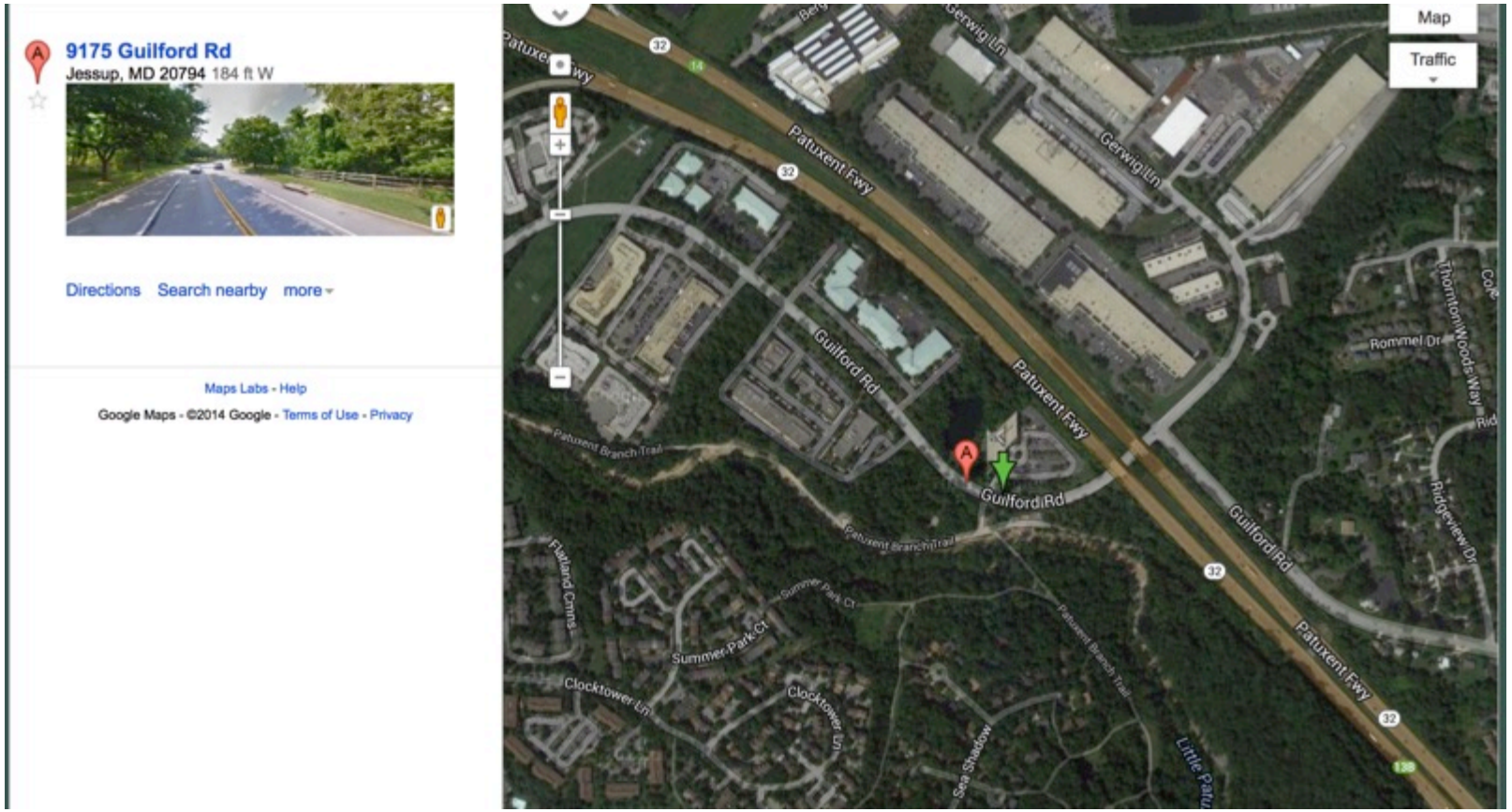
- Altitude: 101.902 m (334.323 ft)
- Altitude Reference: above sea level
- Date Stamp: 25 Apr 2014
- Image Direction: 331.693
- Image Direction Reference: True direction
- Latitude: 39° 9' 57.6" N
- Longitude: 76° 50' 27.6" W
- Time Stamp: 13:50:46

So, what happens when we click “Locate”



ASPECT SECURITY
Application Security Experts

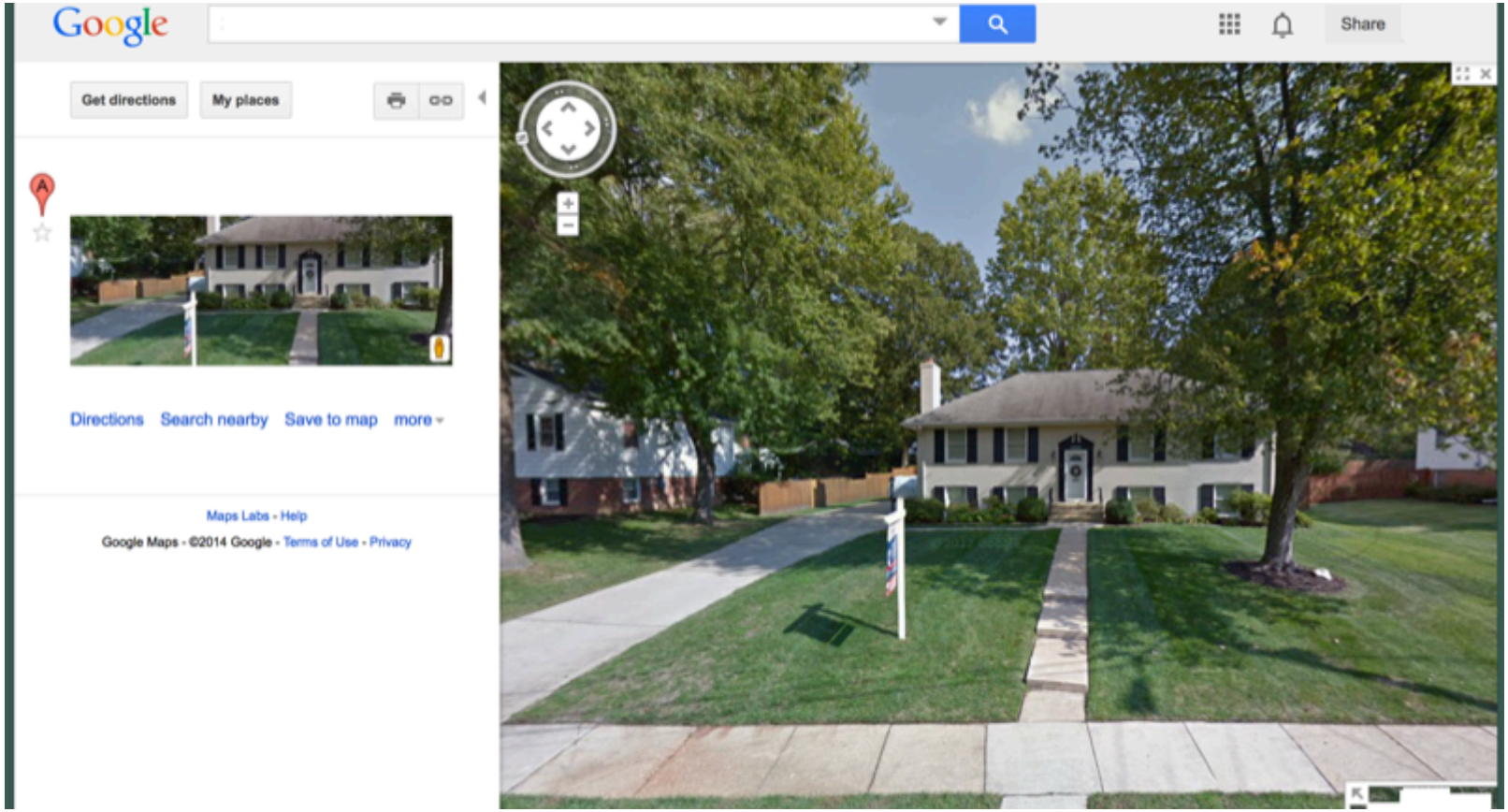
HIDE AND SEEK



Hey, can I use street view on this?

ASPECT SECURITY
Application Security Experts

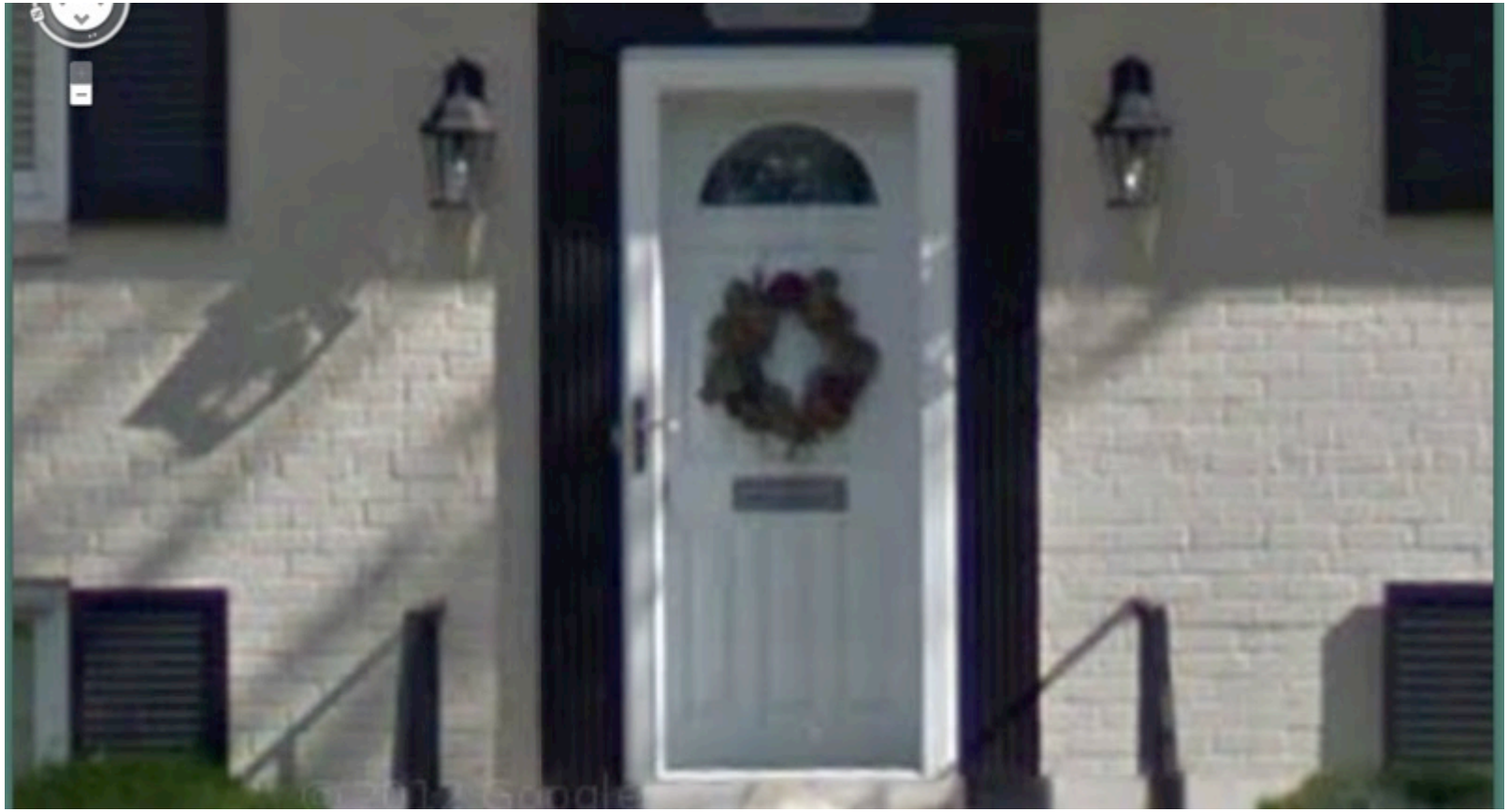
ROUND THE CORNER



Oh look, a split level ranch-style house

ASPECT SECURITY
Application Security Experts

TELEPHOTO LENS



With a white steel door containing a metal mail slot

ASPECT SECURITY
Application Security Experts

ONE PICTURE, LOTS OF INFORMATION

From this online profile, we determined:

- First and last name
- Where she lives
- What the house looks like, in and out
- Date picture taken
- Trying to sell her house (or just bought)

Basically, huge exposure of private information

ASPECT SECURITY
Application Security Experts

WHAT'S GOING ON HERE?

Modern cameras embed all kinds of stuff:

- Flash fired, ISO factor, camera model, etc.
- Stored in JPEG's generic "Application Segment"
- Encoded via "Exchangeable Image File Format"

EXIF is "directory" of defined tags and subtags

- GPS data is tag ID 0x8825 with multiple subtags
  - 0x8825 ⇛ 0x0002 (GPSLatitude) ⇛ data type "rational64" (32bit numerator / 32bit denominator)
- EXIF is really a TIFF subset, but don't tell anyone

ASPECT SECURITY
Application Security Experts

DETECTION DIFFICULTIES

Not all images contains GPS information

- For my test site, only 2½% of images had GPS info
- Some people didn't upload the data
- Most images were manipulated, destroying EXIF
  - Trigger criteria for automatic server editing was not known
  - Thus, my image uploads didn't have GPS when viewed later
- Must browse many profiles to find GPS leakage

In a black box test, image GPS detection is not quick or easy, nor is it guaranteed

ASPECT SECURITY
Application Security Experts

DETECTION STEPS

Must browse all user profiles

Copy images from Safari cache, ZAP history, etc

Filter profile images from chaff

Run “jpeg_exif_grep” for GPS

ASPECT SECURITY
Application Security Experts

AUTOMATIC DETECTION

Wouldn't it be nice if we auto-detected this?

- Browse website, see privacy exposure…

What if ZAP scanned for GPS information and did it without us doing extra work?

ASPECT SECURITY
Application Security Experts

ZAP RECORDED DEMO

\begin{QuicktimeVideo}

- www.veggiespam.com/talks/ils-2015-02-90sec.mp4

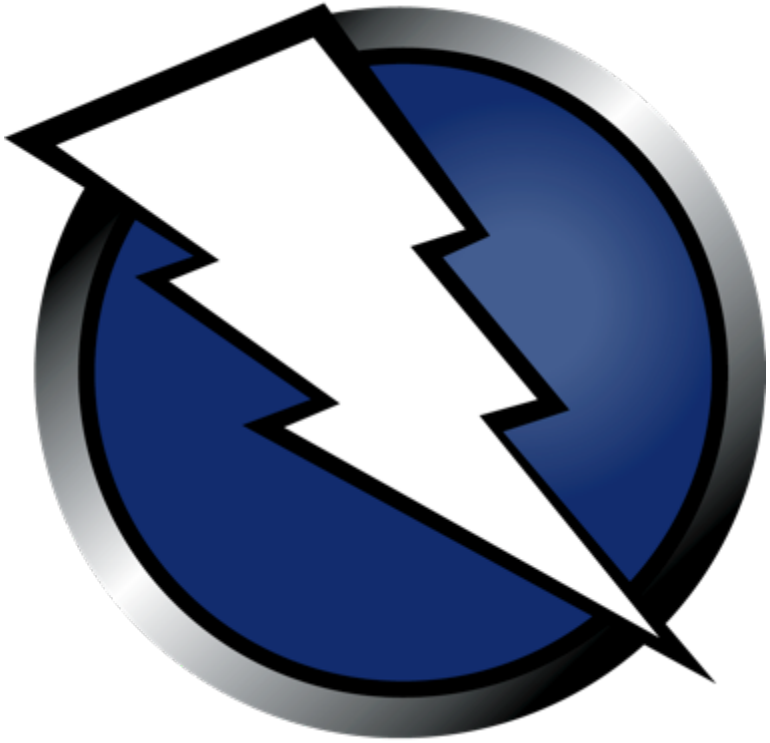
\end{QuicktimeVideo}

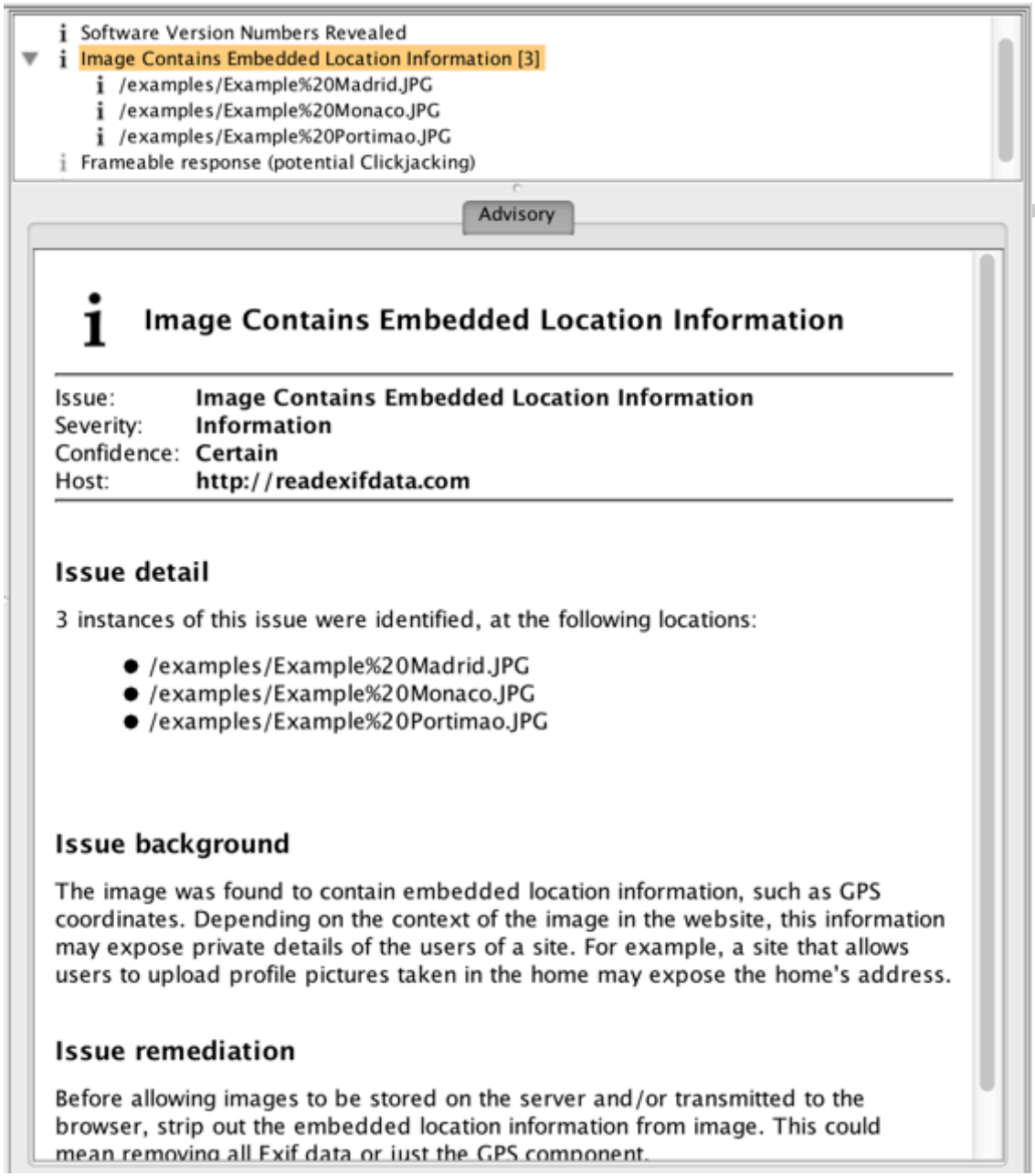
"The only way this [live demo] wouldn't work is if Google went down."

- Kai Huang (aka Chai Squared)
  - Audience Response: laughter & yeah right
  - Situation: Google died in first major outage

ASPECT SECURITY
Application Security Experts

BUT I WANT TO BURP…





ASPECT SECURITY
Application Security Experts

BURP: SUMMARY RESULTS

BURP: DETAILS FOR SINGLE IMAGE

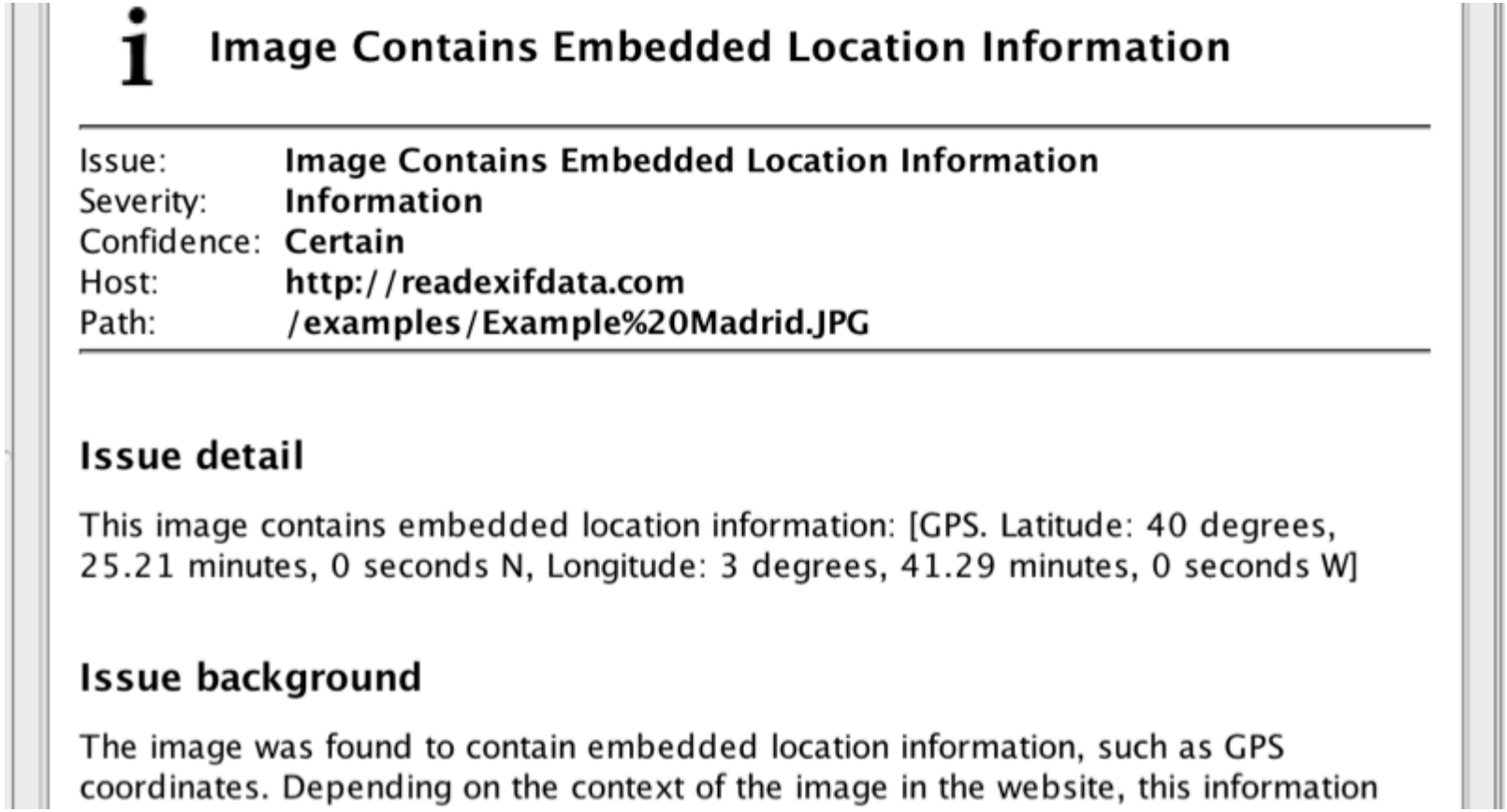


Image Contains Embedded Location Information

Issue:	**Image Contains Embedded Location Information**
Severity:	**Information**
Confidence:	**Certain**
Host:	**http://readexifdata.com**
Path:	**/examples/Example%20Madrid.JPG**

Issue detail

This image contains embedded location information: [GPS. Latitude: 40 degrees, 25.21 minutes, 0 seconds N, Longitude: 3 degrees, 41.29 minutes, 0 seconds W]

Issue background

The image was found to contain embedded location information, such as GPS coordinates. Depending on the context of the image in the website, this information

ASPECT SECURITY
Application Security Experts

REMEMBER THE CONTEXT

Just because image contains GPS information does not automatically mean security issue

- GPS location is obvious in Eiffel Tower selfies
- Being photographed during magazine interview from a secret location might be "bad" †
- You prefer the NSA to know your location ‡

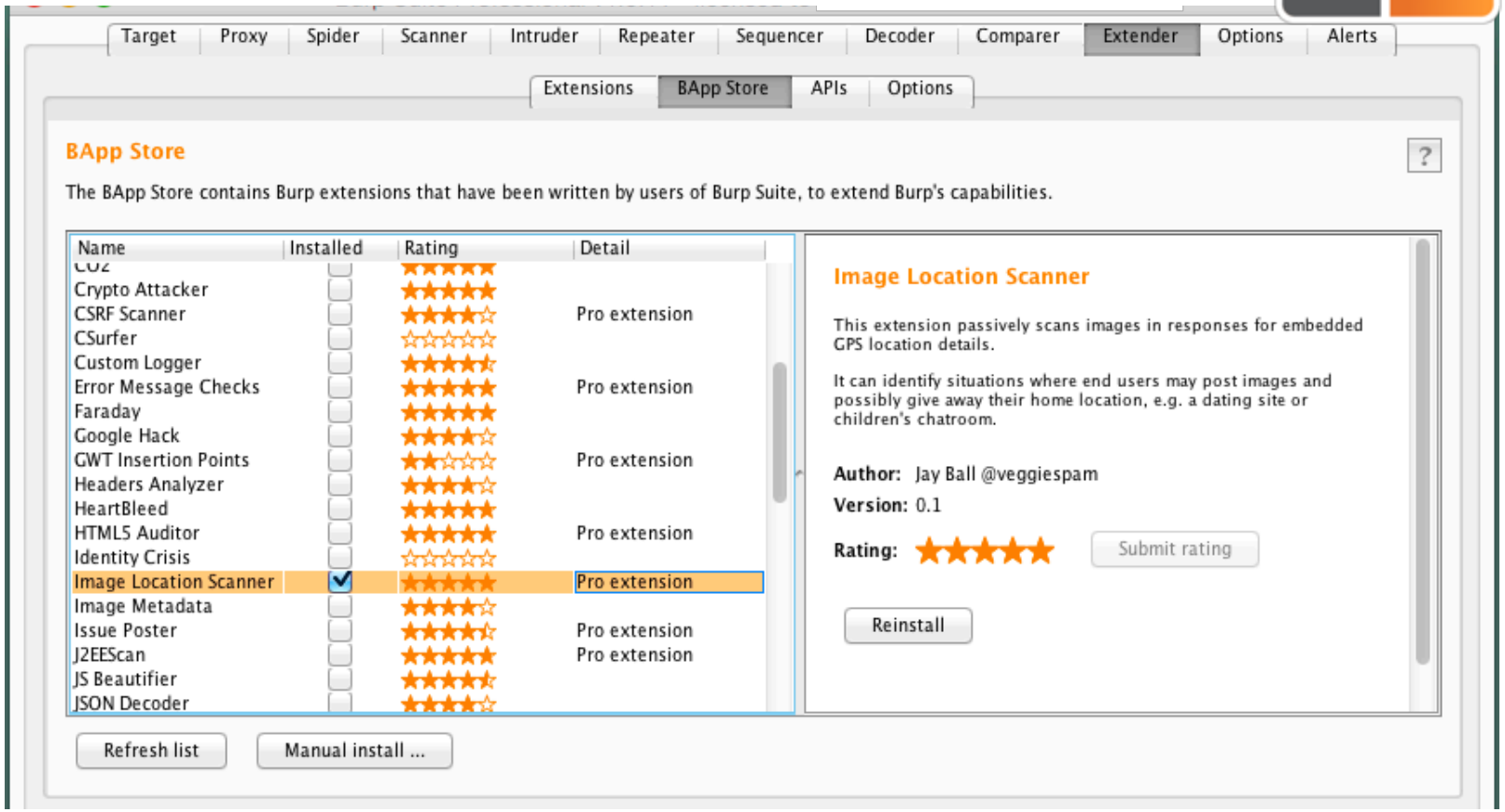
ZAP & Burp plug-ins flag as "Informational"

- The tester must determine security posture

† http://.../metadata-in-photo-of-john-mcafee-pinpointing-him-to-a-location-in-guatemala
‡ http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

ASPECT SECURITY
Application Security Experts

WHERE DO I BUY THIS TOOL



ASPECT SECURITY
Application Security Experts

WHAT ABOUT ZAP

Will be available in ZAP 2.4.0 Marketplace

- ZAP 2.4.0 release coming in early March 2015

Beta / Alpha channel

- Code is production quality
- Beta channel due to:
  - Language translations are done
  - Java package namespace not finalized

ASPECT SECURITY
Application Security Experts

BUILDER & DEFENDER

ASPECT SECURITY
Application Security Experts

PROTECTION

Nearly all camera phones insert GPS data

- Many medium- to high-end cameras do too

Don't let users upload GPS information

- Opens our clients' websites to liability
- Suggest your clients strip GPS information or set latitude & longitude to 0° 0' 0.0"

Be careful about fully removing all EXIF data, you may not have legal permission to edit files

ASPECT SECURITY
Application Security Experts

PROGRAMMATIC GPS REMOVAL

Apache Imaging Library for Java (née Sanselan)

- http://commons.apache.org/proper/commons-imaging
- See example WriteExifMetadataExample.html

ExifLibrary for .NET

- http://www.codeproject.com/Articles/43665/ExifLibrary-for-NET

Python

- https://github.com/bennoleslie/pexif
- https://wiki.gnome.org/Projects/gexiv2/PythonSupport

Perl

- CPAN Image::ExifTool
- ExifTool has API wrappers for Python, Ruby, Java, AppleScript

PHP

- *sigh* Here's a nickel kid. Get yourself a better language † ‡

† http://dilbert.com/strip/1995-06-24
‡ http://tnx.nl/php.html

ASPECT SECURITY
Application Security Experts

JAVA: REMOVE ALL EXIF DATA

```
import org.apache.commons.imaging.formats.jpeg.exif.ExifRewriter;

ExifRewriter().removeExifMetadata(
       File jpegImageFile,  OutputStream  out);
```

ASPECT SECURITY
Application Security Experts

JAVA: SET GPS LOCATION IN EXIF

```
import org.apache.commons.imaging.Imaging;
import org.apache.commons.imaging.common.ImageMetadata;
import org.apache.commons.imaging.formats.jpeg.JpegImageMetadata;
import org.apache.commons.imaging.formats.jpeg.exif.ExifRewriter;
import org.apache.commons.imaging.formats.tiff.write.TiffOutputSet;
import org.apache.commons.imaging.formats.tiff.TiffImageMetadata;

ImageMetadata metadata = Imaging.getMetadata(File jpegImageFile);
JpegImageMetadata jpegMetadata = (JpegImageMetadata) metadata;
TiffImageMetadata exif = jpegMetadata.getExif();
TiffOutputSet outputSet = exif.getOutputSet();
outputSet.setGPSInDegrees(0.0, 0.0);
ExifRewriter().updateExifMetadataLossless(jpegImageFile,
    OutputStream out, outputSet);
```

ASPECT SECURITY
Application Security Experts

COMMAND LINE TOOLS

ExifTool – most powerful EXIF doodad

- http://owl.phy.queensu.ca/~phil/exiftool/
- API wrapper for most languages

JHead – plain C, compiles on Unix & Windows

- http://www.sentex.net/~mwandel/jhead/
- Public domain license

Each program can scan and edit EXIF data

Both bottles available for Homebrew 🍺

ASPECT SECURITY
Application Security Experts

DISPLAY EXIF INFORMATION

Dump header information:

- `jhead file.jpg`
- `exiftool file.jpg`

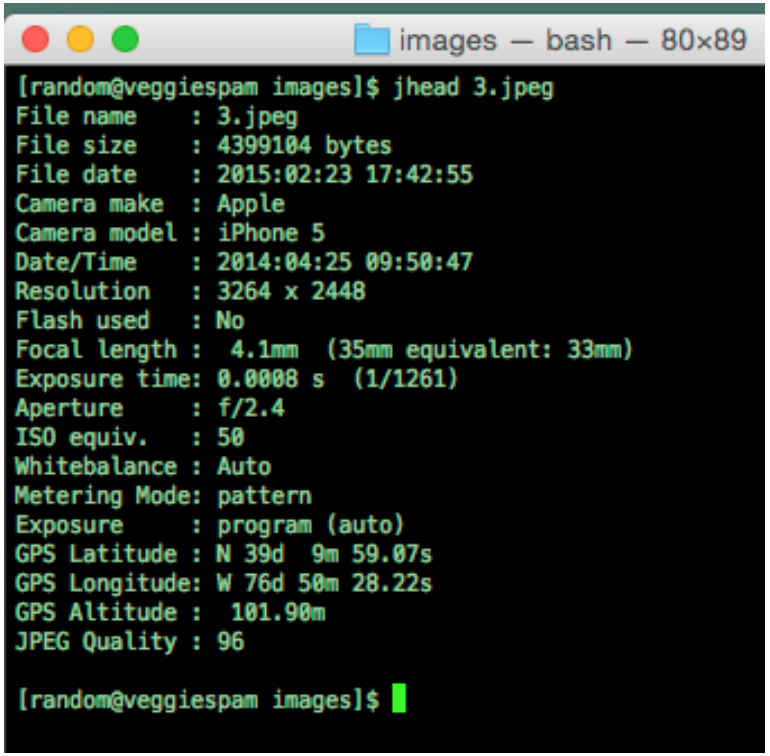
Both accept verbose flags & wildcards:

- `jhead -v *.jpg`
- `exiftool -v *.jpg`

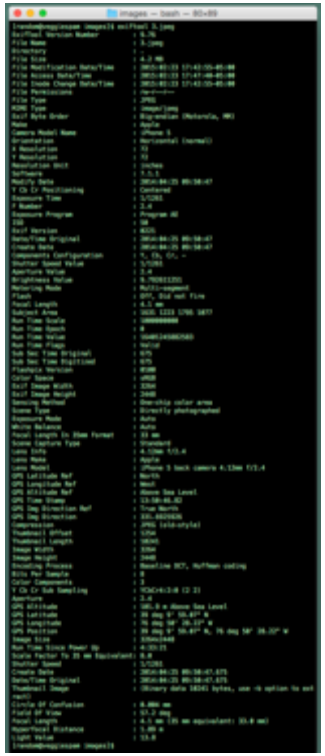
ASPECT SECURITY
Application Security Experts

INFORMATION DISPLAYED

jhead file.jpg



exiftool file.jpg



ASPECT SECURITY
Application Security Experts

BULK REMOVAL EXAMPLES

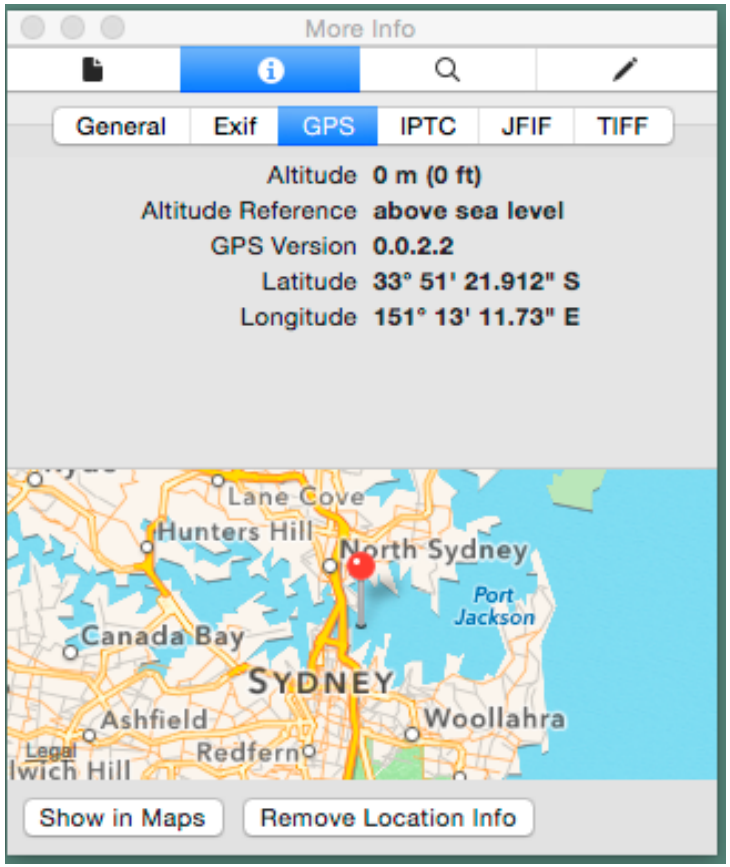
Remove all EXIF header information:

- `jhead -de *.jpg`

Set Latitude / Longitude to 0° 0’ 0.0”:

- ```
  exiftool \
    -exif:gpslatitude="0 0 0.00" \
    -exif:gpslatituderef=N \
    -exif:gpslongitude="0 0 0.00" \
    -exif:gpslongituderef=E  *.jpg
  ```
  ```

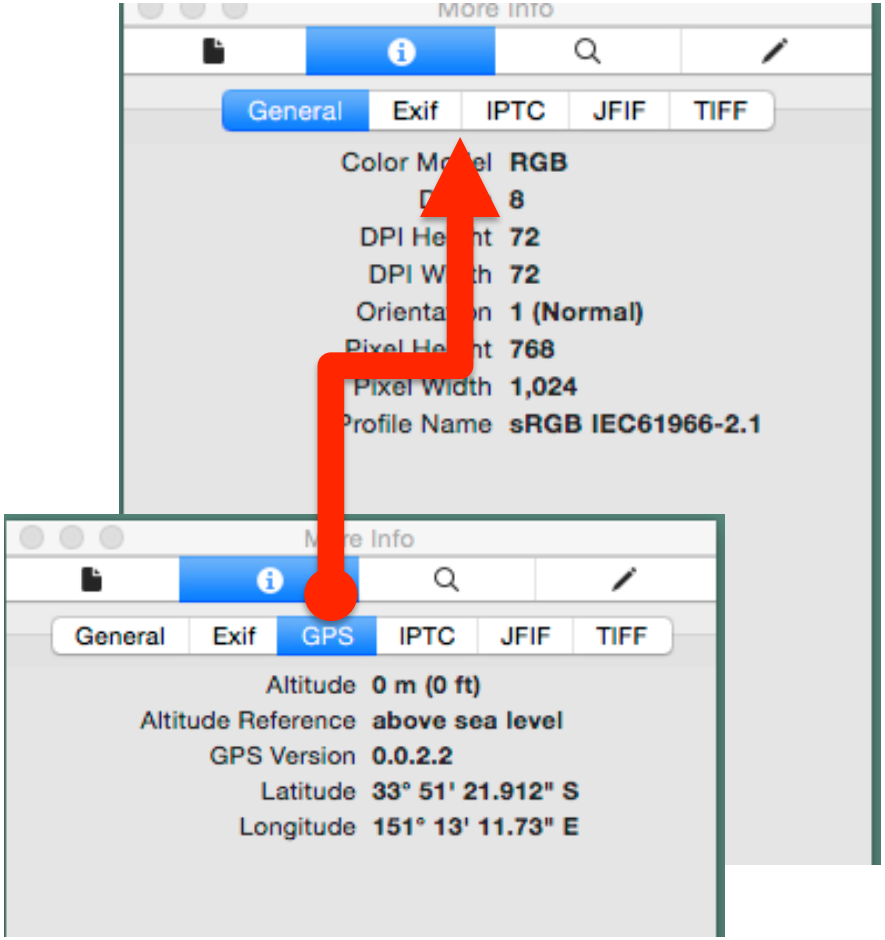
MORE DEFENSES

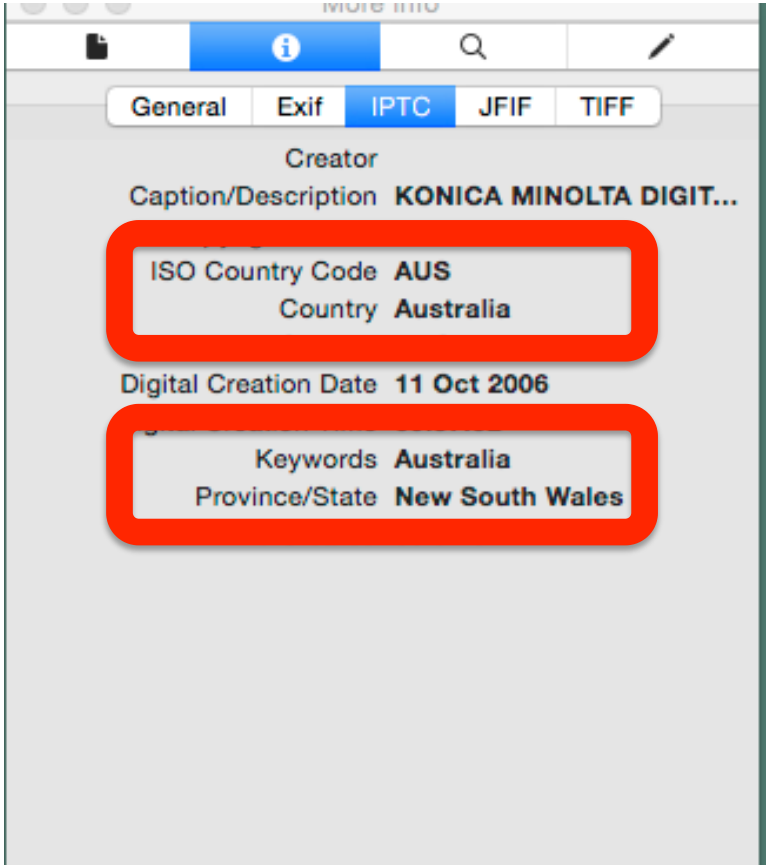


OS X 10.10's Preview added a "Remove Location Info" button!

But…

SO CLOSE…





ASPECT SECURITY
Application Security Experts

LOCATION, LOCATION, LOCATION

Location is more than EXIF

Other mechanisms exist: IPTC & XMP

- Cameras employ these alongside EXIF GPS
  - Or use non-standard EXIF GPS tag IDs too; but I digress
- May embed named locations (Statue of Liberty)
- Media companies (AP, Reuters) use IPTC & XMP

The Image Location Scanner plug-ins for ZAP and Burp do not process IPTC or XMP

ASPECT SECURITY
Application Security Experts

ITPC & XMP PROTECTION

Remove all header information:

- `jhead -dc -de -di -dx -du *.jpg`

Zero EXIF & XMP Latitude / Longitude:

-
```
exiftool \
  -exif:gpslatitude="0 0 0.00" \
  -exif:gpslatituderef=N \
  -exif:gpslongitude="0 0 0.00" \
  -exif:gpslongituderef=E  \
  -xmp:gpslatitude="0 0 0.0 S" \
  -xmp:gpslongitude="0 0 0.0 E" *.jpg
```

† Not sure about levels of support for ITPC in ExifTool

ASPECT SECURITY
Application Security Experts

THE FUTURE

ASPECT SECURITY
Application Security Experts

CODING CAVEATS

Fork the plug-in on GitHub

- github.com/veggiespam/ImageLocationScanner
- Apache License 2.0 (same as ZAP)
- Note: ZAP code will be published in early March

Utilizes the Apache Commons Image Library

GPS scanning triggered when

- ZAP sees mime-type image/jp{e}g; filename.jp{e}g
- Burp self-identifies “JPEG” data

ASPECT SECURITY
Application Security Experts

FUTURE PLUG-IN WORK

Add support for IPTC & XMP

- Plus non-standard GPS embedding techniques
- Dependency on the image library
- Need more examples of these files for testing

Examine PNG & TIFF files for EXIF data

- Uncommon, but growing in use
- Dependency on the image library

ASPECT SECURITY
Application Security Experts

MORE PLUG-IN IDEAS

Scan more data origins

- Triggers on more than just mime/types & extensions
- <img src="base64…", JSON, web sockets, raw

Is Apache Imaging Library right for us

- Avoid using ExifTool; keep plug-in pure Java
- Consider MetaData Extractor library instead
  - Reads more files types (PNG, PSD) and tags (ITPC, XMP, camera proprietary, non-standard)
  - Very generic in usage; we need to invent much
  - Read-only processing, but shouldn't matter for scanners

ASPECT SECURITY
Application Security Experts

RESEARCH TODO

More sample code for more languages

Better advice for bulk removal

Ruminate on copyright during file modification

Gather data from children-only social sites

- Do these remove GPS from profile photos or album
- My household only has vomiting fur balls; so I need your help in collecting this information
  - Jabbersmack, Kuddle, GeckoLife, Sweety High, iTwixie
  - commonsensemedia.org/lists/social-networking-for-kids

Get the word out

ASPECT SECURITY
Application Security Experts

SECRET PROJECT

More Image Location Scanning Privacy Fun

- Will change the world
- Whiter teeth, fresher breath

Need to find time to work on it

- And maybe some brains. Brains... Tasty, tasty brains
- Need to contemplate demand & effort

ASPECT SECURITY
Application Security Experts

CLOSING

ASPECT SECURITY
Application Security Experts

CONCLUSIONS

As testers, we need to scan for this to reduce our clients' risk profile

As users, we cannot trust the remote website to protect our location privacy

As consumers, "Remove GPS before emailing photo" might be a good feature request

ASPECT SECURITY
Application Security Experts

ABOUT ME: JAY BALL

Badges: MS, BS, CISSP, GSNA, CRISC

Twitters: @veggiespam

Blogs & stuffs: www.veggiespam.com
www.aspectsecurity.com/blog/

Feedbacks: owasp@veggiespam.com

This presentation and supporting materials can be found at http://veggiespam.com/ils/

Buy me coffee ☕ www.starbucks.com/shop/card/egift

Aspect Security is hiring (ask me)

Thank you!

ASPECT SECURITY
Application Security Experts

ASPECT SECURITY
Application Security Experts

REFERENCES

Official EXIF Spec:

- http://www.cipa.jp/std/documents/e/DC-008-2012_E.pdf

Detailed list of EXIF tags:

- http://www.sno.phy.queensu.ca/~phil/exiftool/TagNames/EXIF.html

ASPECT SECURITY
Application Security Experts

SAMPLE IMAGE SITES

http://readexifdata.com/

http://opanda.com/en/iexif/sample.htm

http://raia.com/

ITPC data (Sydney) came from images here: http://ptforum.photoolsweb.com/ubbthreads.php?ubb=showflat&Number=29893

https://github.com/drewnoakes/metadata-extractor-images

ASPECT SECURITY
Application Security Experts

ABSTRACT LONG

We unintentionally distribute GPS data with every photograph posted on the web or emailed. Indoor pictures may contain embedded home address, doctor's office locations, day care centers, etc. This talk will describe a real-world scenario involving remote education site where teachers and students exposed their confidential home address via their profile pictures. I will demonstrate the detailed steps to detect the location exposure. Then, I will introduce two new ZAP & Burp plug-ins to automate the GPS data discovery during normal security assessments. In addition, suggestions for websites to protect their users and to remove the GPS data will also be provided.