

# iOS Forensics

Sean Morrissey

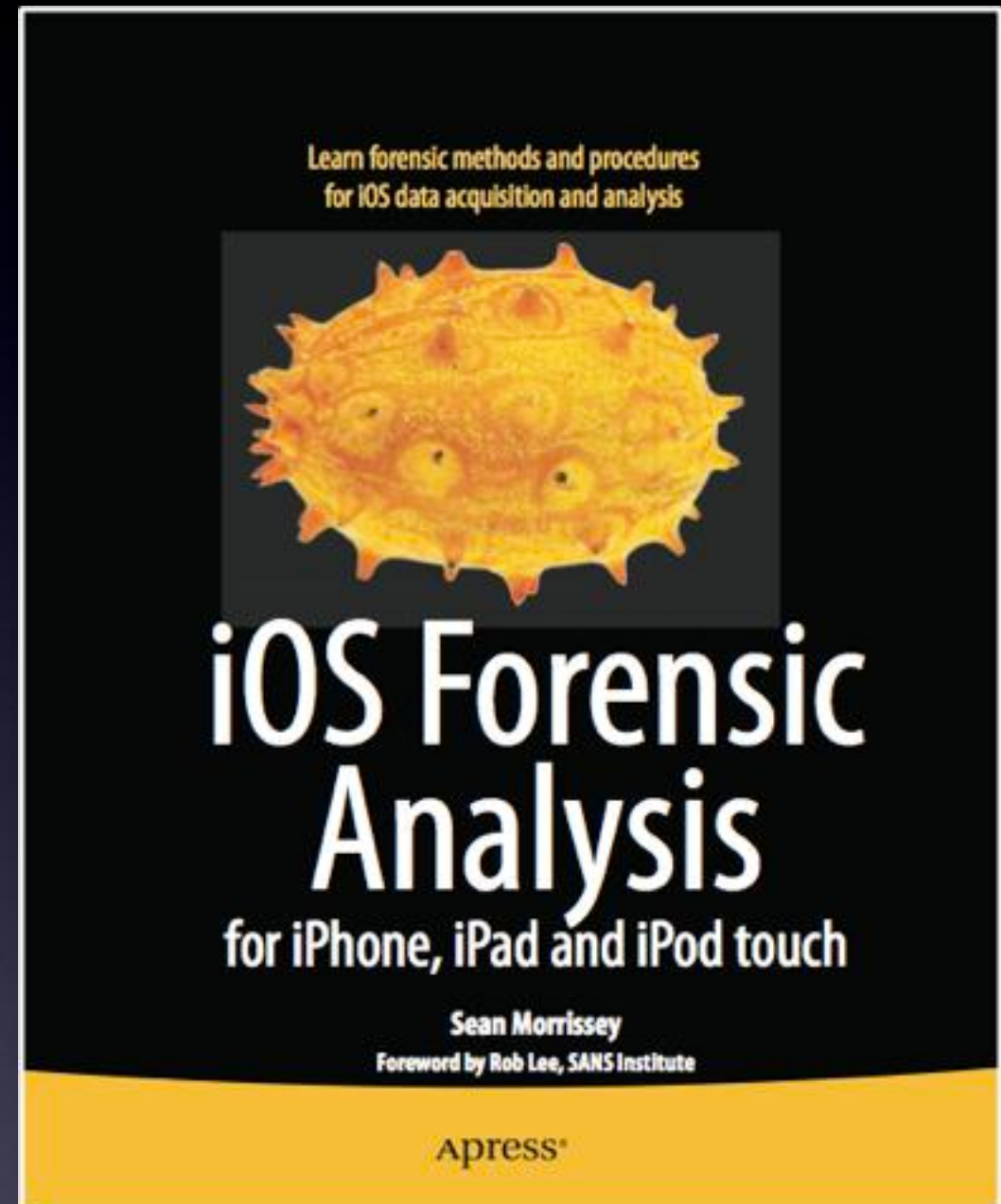
CEO

Katana Forensics, LLC

# Sean Morrissey

Computer Forensic Analyst  
Federal Agency  
CEO Katana Forensics

Former LE in Maryland  
US Army Officer

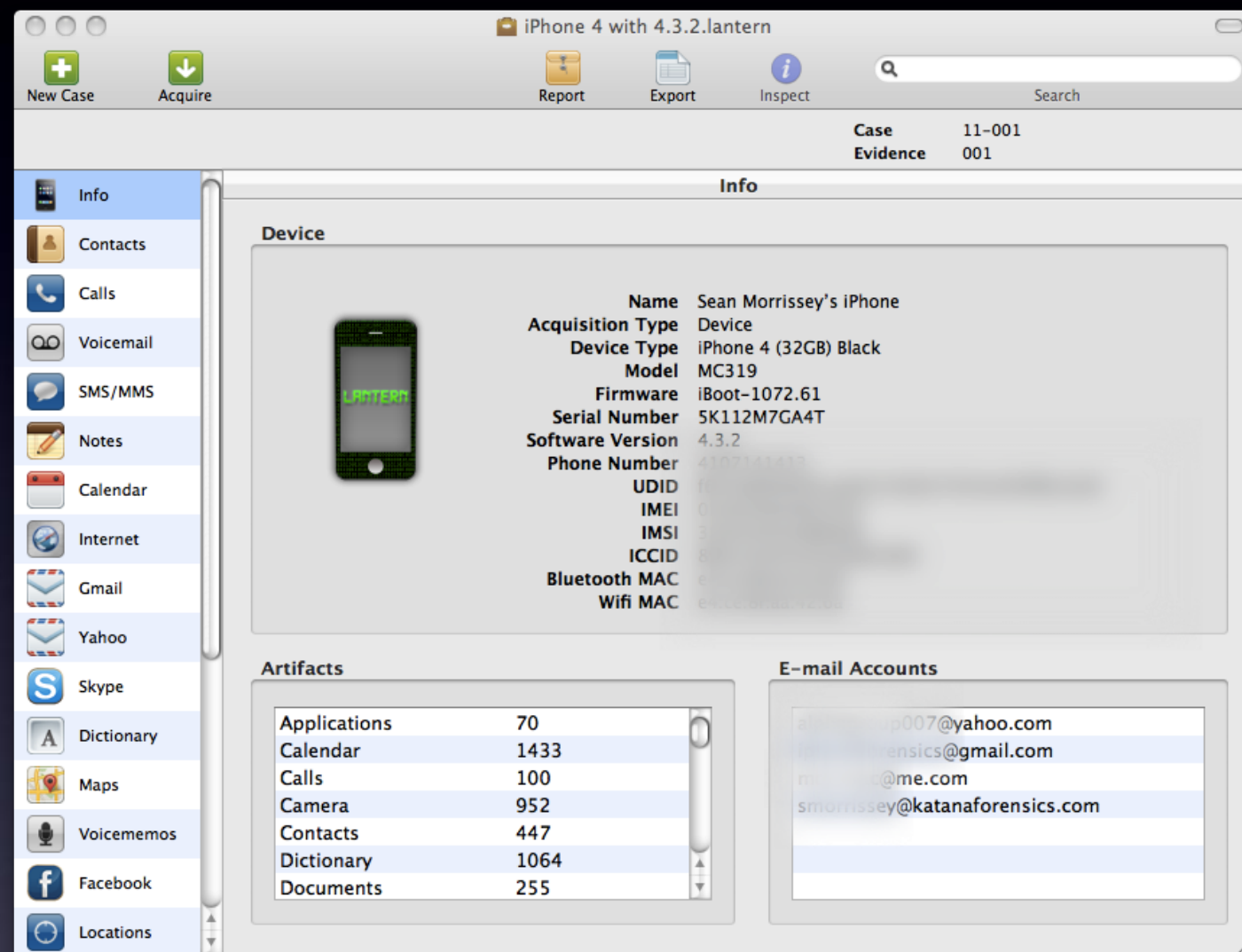


I  
Make  
These

Just Kidding.....



# Really I Make This.....



## Lantern iOS Forensics Software

But I named it  
after



# The First Logo looked Like This



LANTERN



# iOS Forensics

- What is iOS Forensics?
- How do we handle iOS Devices?
- How do we examine them?
- How are things changing?

# iOS Forensics

- The Analysis of Apple Mobile Devices



2007

4GB



2010

32GB



2011



64GB

# iPhones Worldwide

Total 35 Million and growing







500,000

Apps

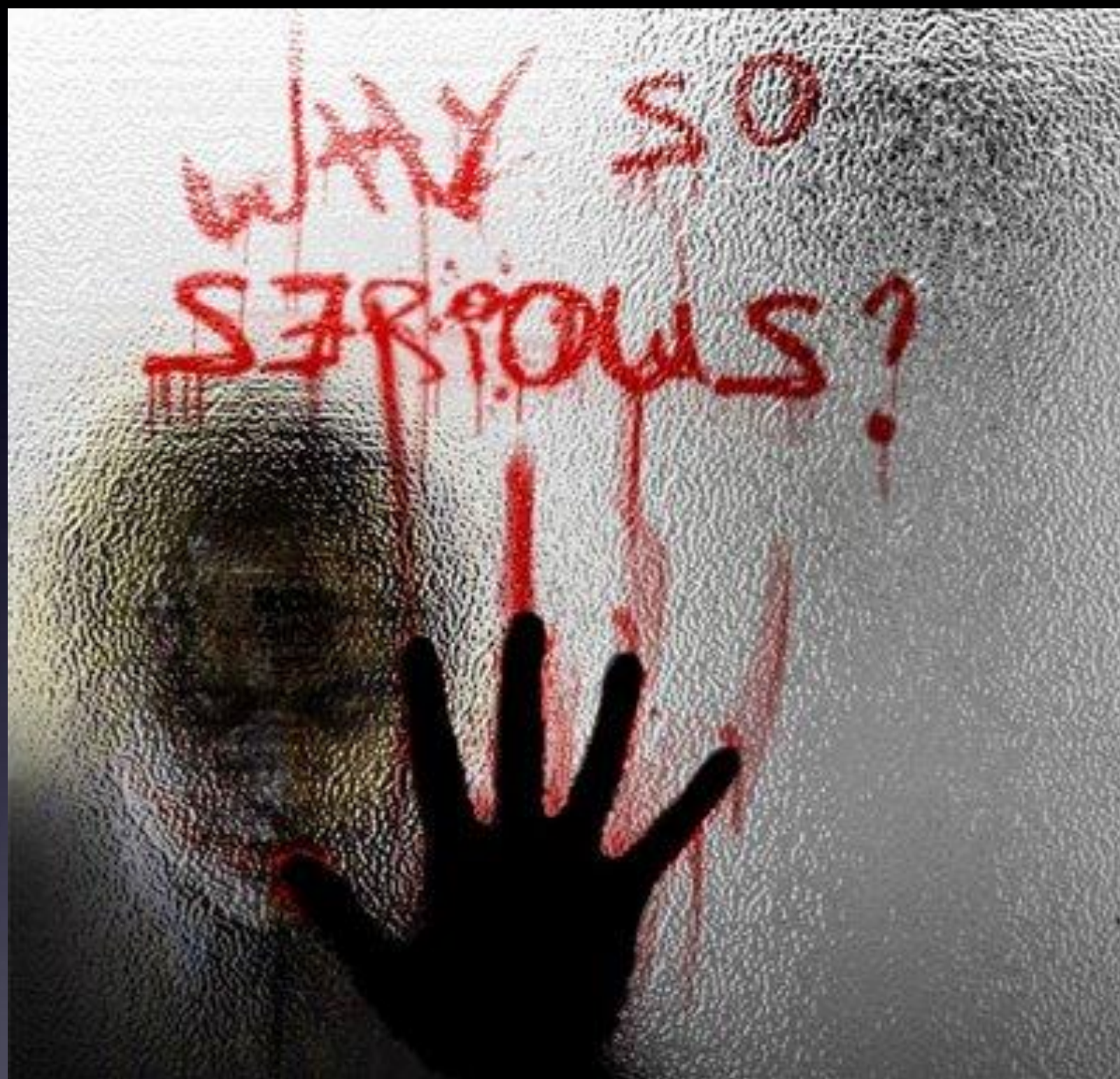
# Handling iOS Devices

- Remove Sim card - Disconnect from cellular network
- Turn off Wifi and Bluetooth
- Airplane Mode
- No access to GUI - do the above and if needed use a Faraday Bag also

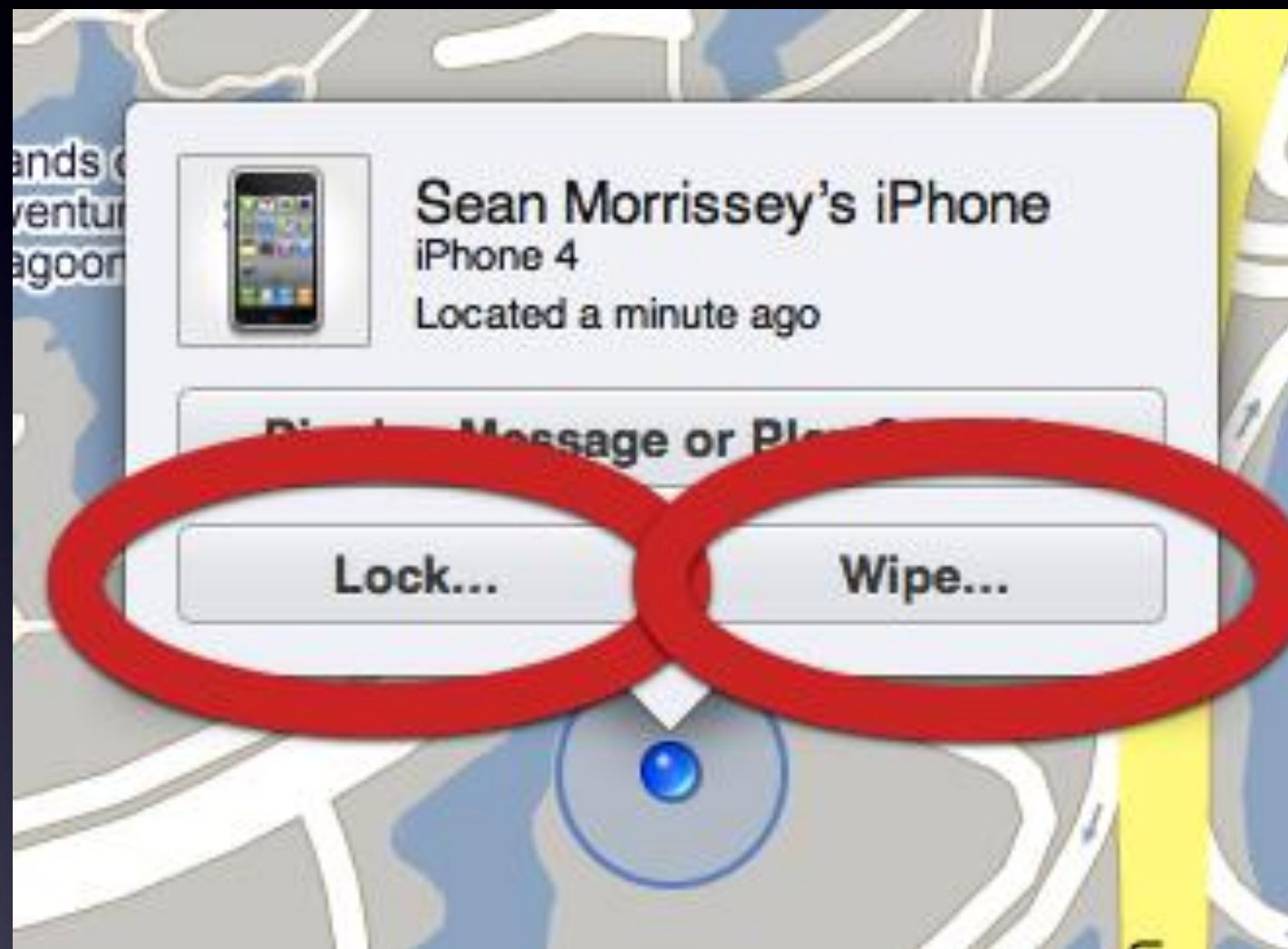


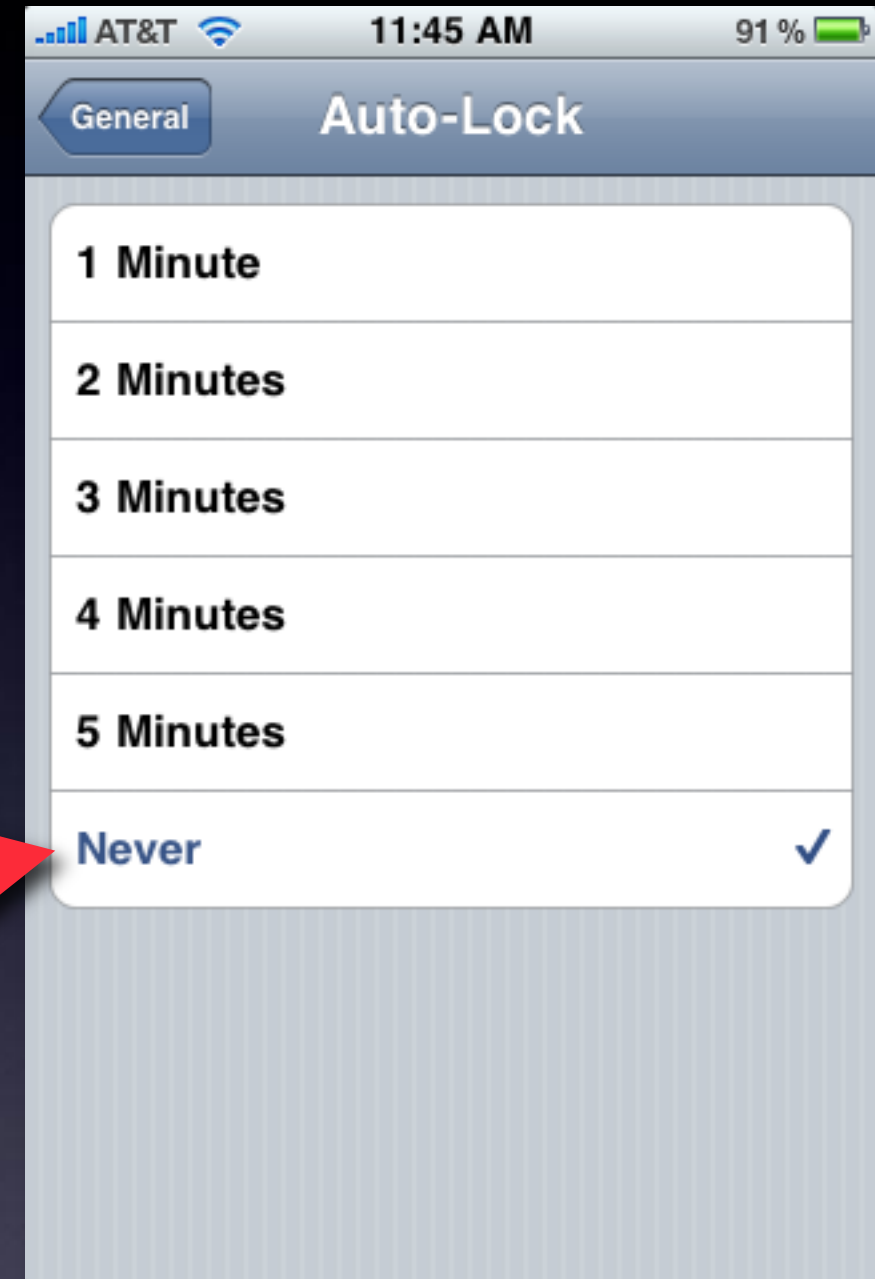
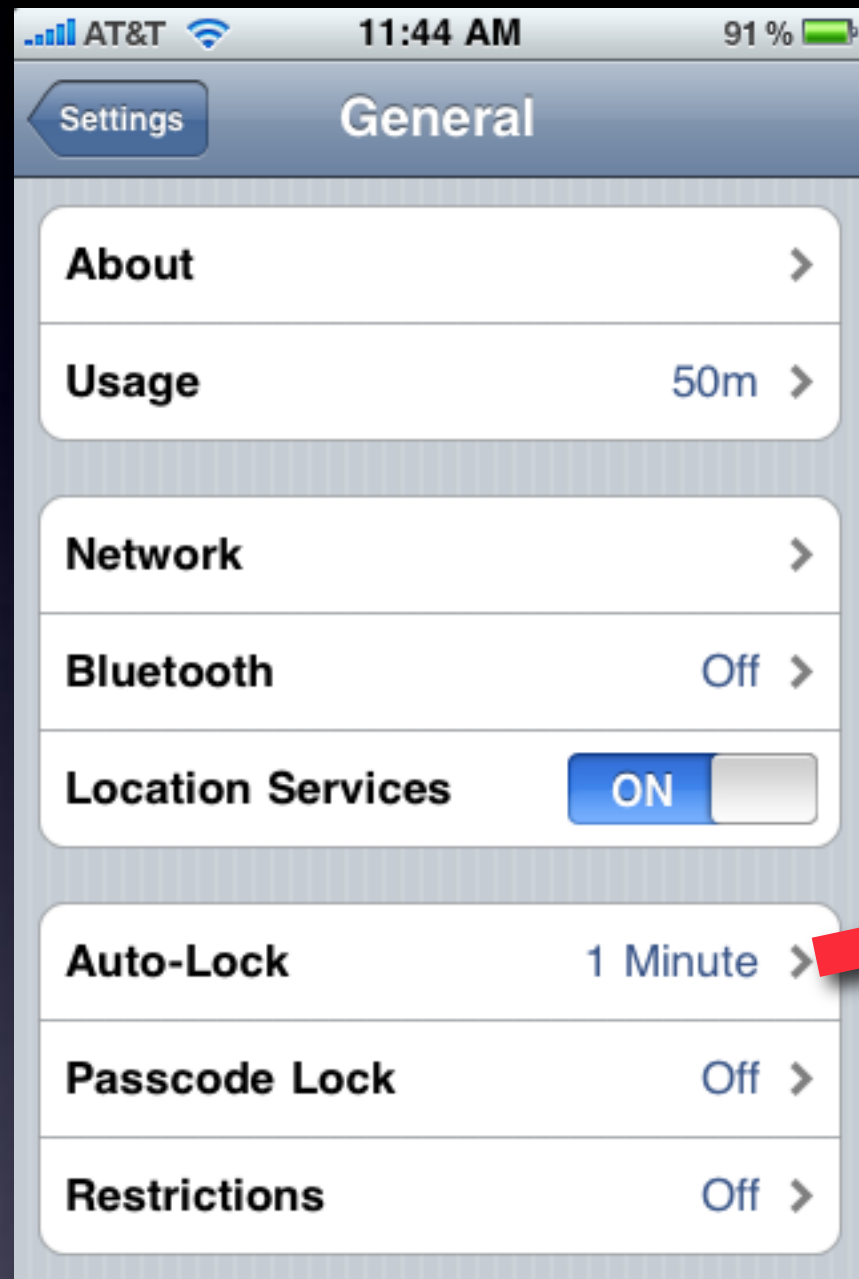


oops!









# Backup data

- Historical data from one or more devices
- Syncing certificates [.plist] that can aid in bypassing passcodes
- Windows 7:  
user/[username]/appdata/roaming/AppleComputer/MobileSync/Backup
- OSX: private/var/db/lockdown

iOS 2 backups,

0dc926a1810f7aee4e8f38793ed788701f93bf9d.mdba  
ckup

iOS 3 backups,

0dc926a1810f7aee4e8f38793ed788701f93bf9d.mdata  
0dc926a1810f7aee4e8f38793ed788701f93bf9d.mdinf  
o

iOS 4 backups,

**KATANA**  
0dc926a1810f7aee4e8f38793ed788701f93bf9d

# In Search Warrants

Don't forget, write so you can grab all the





# iCloud



Data Synced over numerous devices

# Logical Analysis



# Logical Data & Extraction

- After the release of the iPhone in 2007, forensic developers were racing to build applications to analyze the iDevices

# Logical Tools

- Lantern 2.0
- XRY
- Paraben
- Secure View 3

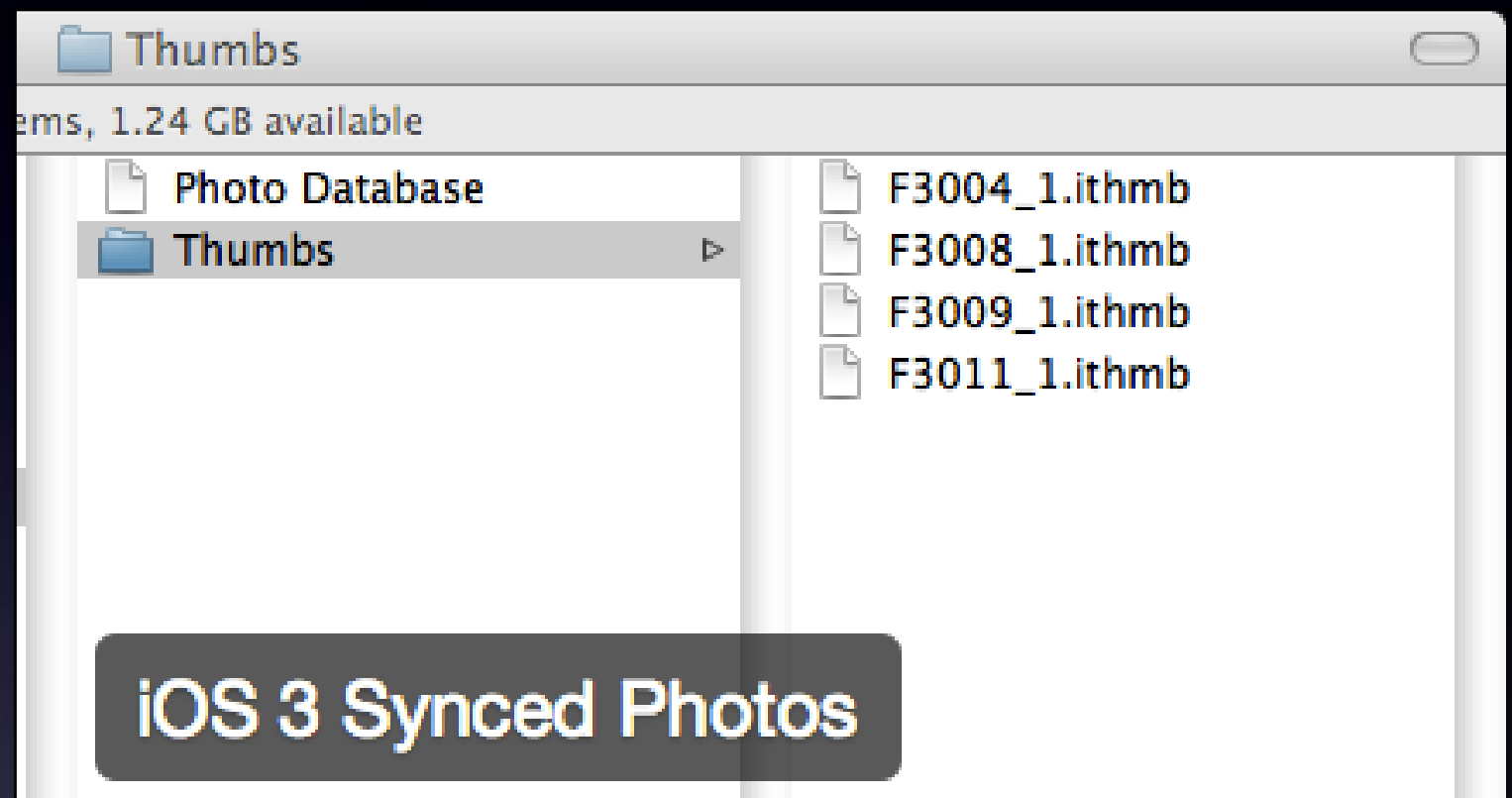
# Physical Analysis

# Physical Tools

- iXAM
- MPE+

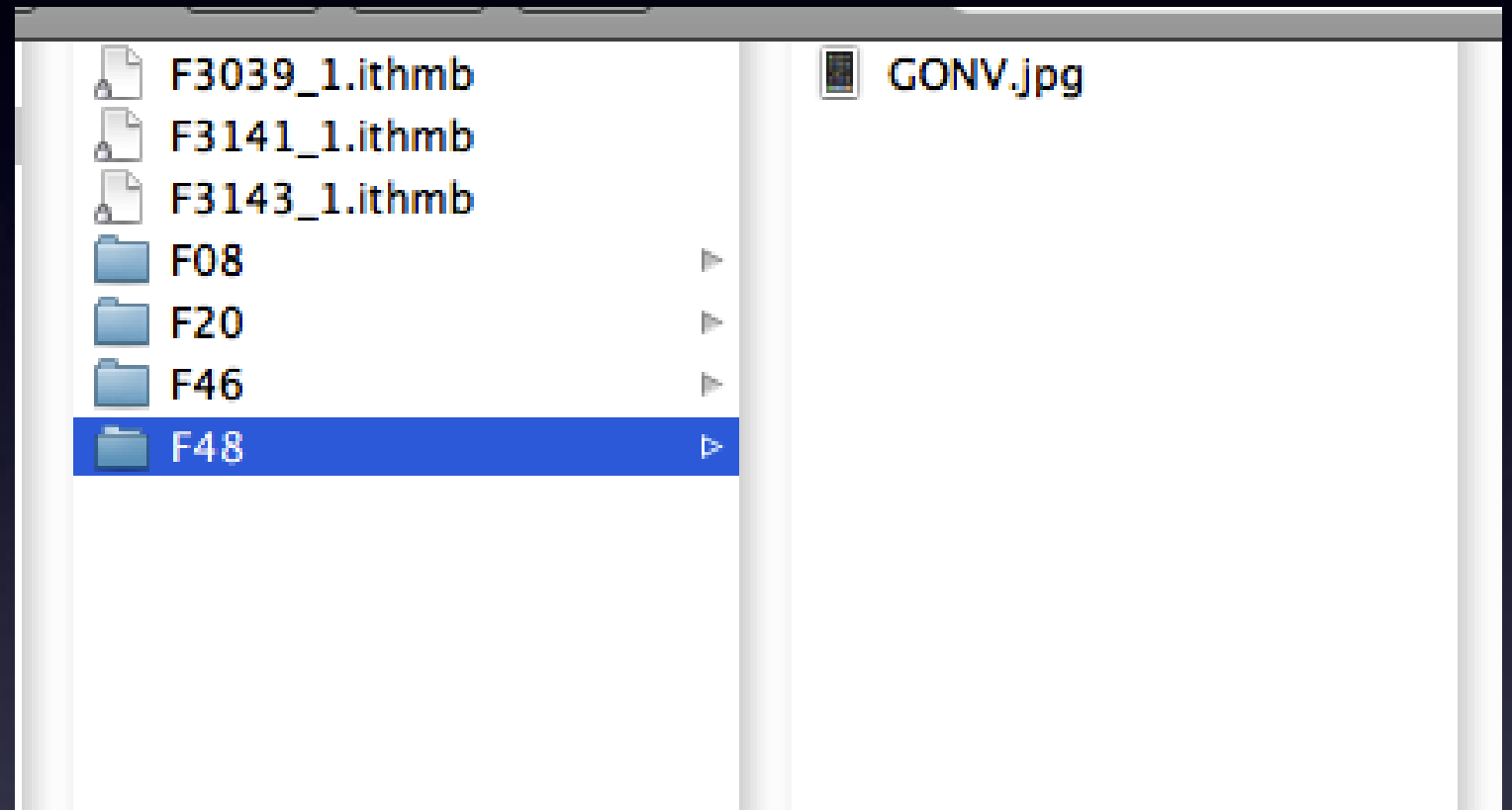
# Images

iOS 3



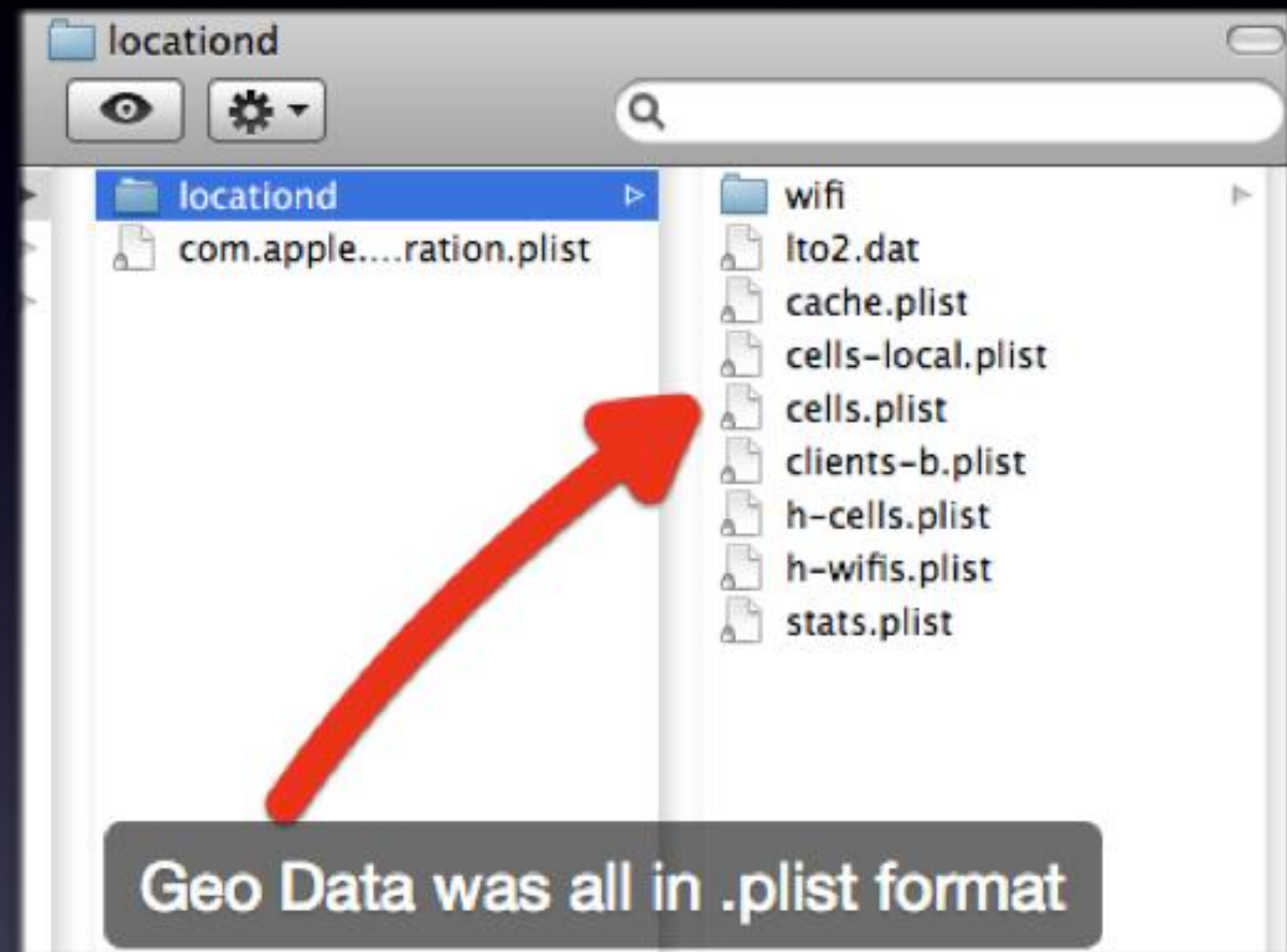
# iOS 4

## Synced Images



# iOS 3

## Geo Tracking





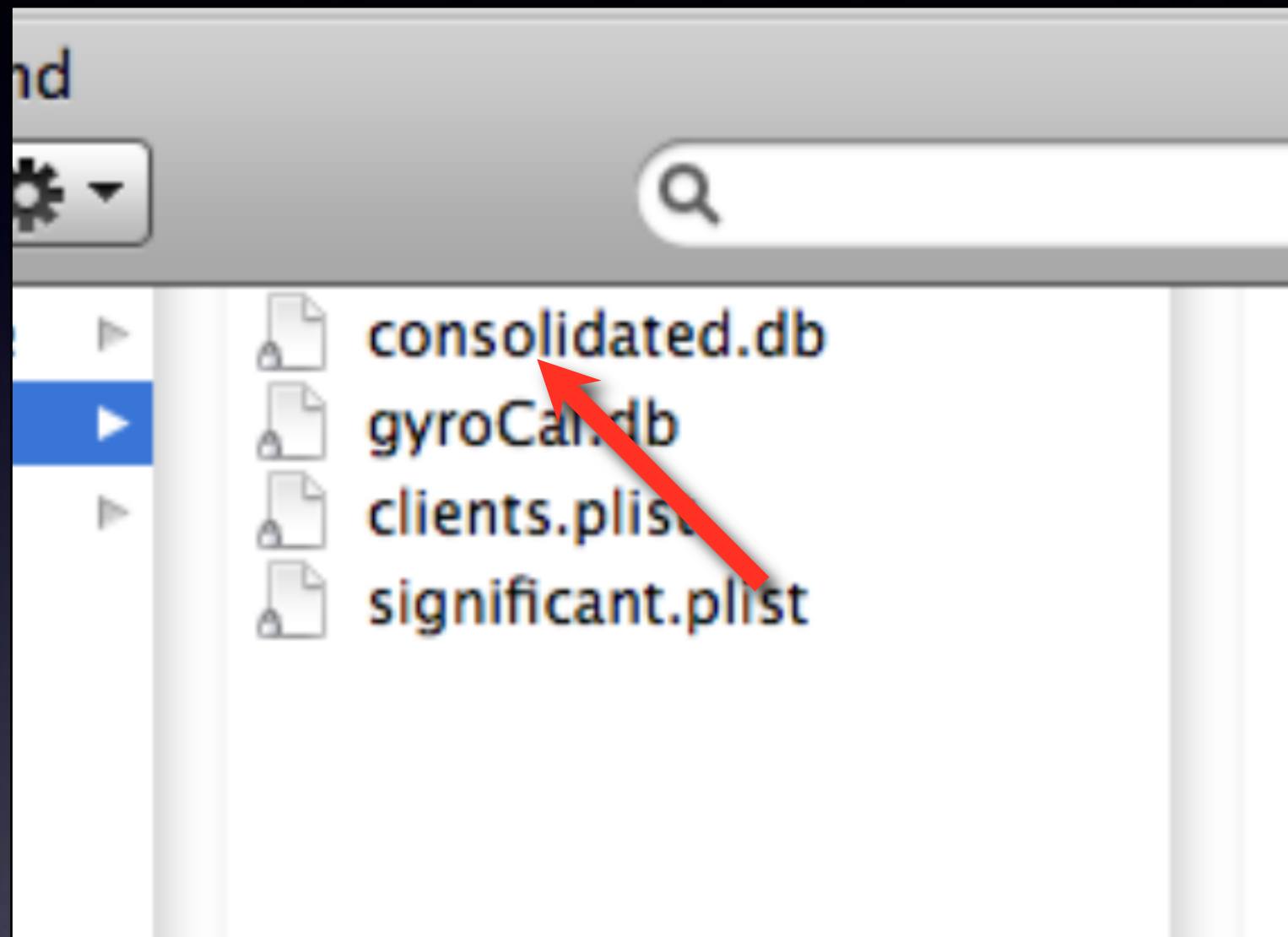
◇ Untitled

Utility Action Add Column Attach Inspect

| Key                        | Value               |
|----------------------------|---------------------|
| ▼ 310,410,0x9087,0x1f504d0 |                     |
| ▼ 0                        |                     |
| • Latitude                 | 36.11905573333333   |
| • HorizontalAccuracy       | 300.2058267542113   |
| • VerticalAccuracy         | 454.2918533352134   |
| • Longitude                | -115.17377613333333 |
| • Altitude                 | 614                 |
| • Timestamp                | 256714314.483819    |
| • RSSI                     | -59                 |
| ▼ 1                        |                     |
| ▼ UMTSNeighbors            |                     |
| ▼ 0                        |                     |
| • RSCP                     | 59                  |
| • ARFCN                    | 4385                |
| • PSC                      | 76                  |
| • ECN0                     | 6                   |
| ▼ 1                        |                     |
| • RSCP                     | 72                  |
| • ARFCN                    | 9925                |
| • PSC                      | 76                  |
| • ECN0                     | 7                   |
| ▼ 2                        |                     |

**GEO DATA**

# iOS 4 Geo Location



SQLite Database Browser - /Volumes/Mac Files/Untitled.lantern/Acquisitions/1/Extraction/private/var/mobile/Library/...

Database Structure Browse Data Execute SQL

Table: CellLocation

New Record Delete Record

|    | MCC | MNC | LAC  | CI        | Timestamp     | Latitude    | Longitude    | HorizontalAccura |
|----|-----|-----|------|-----------|---------------|-------------|--------------|------------------|
| 1  | 310 | 410 | 7985 | 158494439 | 153859.735445 | 38.88857305 | -77.08129543 | 500.0            |
| 2  | 310 | 410 | 7970 | 160761839 | 503887.045529 | 38.99729001 | -76.58929085 | 500.0            |
| 3  | 310 | 410 | 7970 | 160761842 | 503887.045529 | 38.99759525 | -76.5902422  | 500.0            |
| 4  | 310 | 410 | 7003 | 2036      | 503887.045529 | 38.97900587 | -76.595685   | 2236.0           |
| 5  | 310 | 410 | 7992 | 159451127 | 503887.045529 | 38.97786432 | -76.59514242 | 2059.0           |
| 6  | 310 | 410 | 7020 | 2033      | 503887.045529 | 38.98040455 | -76.59689146 | 2803.0           |
| 7  | 310 | 410 | 7992 | 159451121 | 503887.045529 | 38.97991001 | -76.59833091 | 2292.0           |
| 8  | 310 | 410 | 7970 | 159665688 | 503887.045529 | 38.99939197 | -76.59843456 | 1295.0           |
| 9  | 310 | 410 | 7965 | 160774114 | 503887.045529 | 38.9644984  | -76.58490574 | 1699.0           |
| 10 | 310 | 410 | 7003 | 14835     | 503887.045529 | 38.96925669 | -76.60188108 | 1108.0           |
| 11 | 310 | 410 | 7020 | 14303     | 503887.045529 | 38.95828437 | -76.57820677 | 1693.0           |
| 12 | 310 | 410 | 7965 | 160774642 | 503887.045529 | 38.97664427 | -76.61203467 | 2418.0           |
| 13 | 310 | 410 | 7992 | 158808566 | 503887.045529 | 38.97017753 | -76.60790634 | 1168.0           |
| 14 | 310 | 410 | 7992 | 159463391 | 503887.045529 | 38.95746797 | -76.58152931 | 1655.0           |
| 15 | 310 | 410 | 7992 | 159463919 | 503887.045529 | 38.98160874 | -76.61495906 | 2644.0           |
| 16 | 310 | 410 | 7992 | 159463397 | 503887.045529 | 38.95697337 | -76.57731842 | 1738.0           |
| 17 | 310 | 410 | 7992 | 159461327 | 3628519.20973 | 38.98343169 | -76.5651924  | 1686.0           |
| 18 | 310 | 410 | 7965 | 160772047 | 3628519.20973 | 38.9833917  | -76.56602269 | 1929.0           |
| 19 | 310 | 410 | 7992 | 158805961 | 3628519.20973 | 38.98313194 | -76.56661653 | 895.0            |

1 - 1000 of 2895

Go to: 0

SQLite Database Browser - /Volumes/Mac Files/Untitled.lantern/Acquisitions/1/Extraction/private/var/mobile/Library/...

Database Structure Browse Data Execute SQL

Table: CellLocation

New Record Delete Record

|    | MCC | MNC | LAC  | CI        | Timestamp      | Latitude    | Longitude    | HorizontalAccura |
|----|-----|-----|------|-----------|----------------|-------------|--------------|------------------|
| 1  | 310 | 410 | 7985 | 158494439 | 153859.735445  | 38.88857305 | -77.08129543 | 500.0            |
| 2  | 310 | 410 | 7970 | 160761839 | 1503887.045529 | 38.99729001 | -76.58929085 | 500.0            |
| 3  | 310 | 410 | 7970 | 160761842 | 1503887.045529 | 38.99759525 | -76.5902422  | 500.0            |
| 4  | 310 | 410 | 7003 | 2036      | 1503887.045529 | 38.97900587 | -76.595685   | 2236.0           |
| 5  | 310 | 410 | 7992 | 159451127 | 1503887.045529 | 38.97786432 | -76.59514242 | 2059.0           |
| 6  | 310 | 410 | 7020 | 2033      | 1503887.045529 | 38.98040455 | -76.59689146 | 2803.0           |
| 7  | 310 | 410 | 7992 | 159451121 | 1503887.045529 | 38.97991001 | -76.59833091 | 2292.0           |
| 8  | 310 | 410 | 7970 | 159665688 | 1503887.045529 | 38.99939197 | -76.59843456 | 1295.0           |
| 9  | 310 | 410 | 7965 | 160774114 | 1503887.045529 | 38.9644984  | -76.58490574 | 1699.0           |
| 10 | 310 | 410 | 7003 | 14835     | 1503887.045529 | 38.96925669 | -76.60188108 | 1108.0           |
| 11 | 310 | 410 | 7020 | 14303     | 1503887.045529 | 38.95828437 | -76.57820677 | 1693.0           |
| 12 | 310 | 410 | 7965 | 160774642 | 1503887.045529 | 38.97664427 | -76.61203467 | 2418.0           |
| 13 | 310 | 410 | 7992 | 158808566 | 1503887.045529 | 38.97017753 | -76.60790634 | 1168.0           |
| 14 | 310 | 410 | 7992 | 159463391 | 1503887.045529 | 38.95746797 | -76.58152931 | 1655.0           |
| 15 | 310 | 410 | 7992 | 159463919 | 1503887.045529 | 38.98160874 | -76.61495906 | 2644.0           |
| 16 | 310 | 410 | 7992 | 159463397 | 1503887.045529 | 38.95697337 | -76.57731842 | 1738.0           |
| 17 | 310 | 410 | 7992 | 159461327 | 13628519.20973 | 38.98343169 | -76.5651924  | 1686.0           |
| 18 | 310 | 410 | 7965 | 160772047 | 13628519.20973 | 38.9833917  | -76.56602269 | 1929.0           |
| 19 | 310 | 410 | 7992 | 158805961 | 13628519.20973 | 38.98313194 | -76.56661653 | 895.0            |

< 1 - 1000 of 2895 >

Go to: 0



Today we live in a world of instant gratification,  
where data is streamed instantiously.

EDITION: U.S. | INTERNATIONAL | MÉXICO

Set edition preference

CNN


Sign up | Log in

SEARCH

POWERED BY Google

Home | Video | NewsPulse | U.S. | World | Politics | Justice | Entertainment | Tech | Health | Living | Travel | Opinion | IReport | Money | Sports

updated 8:03 a.m. EDT, Tue June 7, 2011




Yemen's Saleh burned on 40% of body, official says

President Ali Abdullah Saleh was injured in an attack and is being treated in Saudi Arabia. It's unclear whether he will return to Yemen, where fighting continued today. [FULL STORY](#)

- What's next: Implosion or tribal bargain?
- Limited options | Doubtful future

Latest news


- Obama losing chief economic adviser
- Economy makes people sick [CNNMoney](#)
- Libyan TV: State broadcaster bombed
- Obama to honor Merkel at state dinner
- Witness: Trunk odor result of dead body
- Anthony defense: Food caused odor
- Officer jailed for using Mugabe's toilet
- Witness hid cop-shooting tape in mouth
- Ford plans 50% production boost
- Arizona wildfire threatens New Mexico
- Mistaken ID behind infant's death?
- European officials hold E. coli crisis talks
- Reporter rescues pig near highway
- Japan confirms 3 reactors melted down
- Ticker: Palin 'best thing,' says Romney
- Lenny Dykstra faces more charges
- Bruins pound Canucks in Game 3
- Kim Kardashian's pre-nup details
- USC stripped of 2004 BCS title




Ethics inquiry for Weiner?

Rep. Anthony Weiner's political future appears unclear as his fellow Democrats pursue an ethics probe into whether he used congressional resources to send explicit photos to women online. CNN's Anderson Cooper reports. [FULL STORY](#)


Featured




Martin: Weiner's lies, not tweets, did him in




Weiner's alleged contact speaks up :50




Navarrette: Weiner's only choice to resign




Tsunami orphans feel forgotten 2:49





Palin doubles down on history flap 5:05




The hidden cost of cybercrime







Make CNN Your Homepage



Goldman Sachs

PROGRESS IS

When the construction of a housing development can rebuild an entire community.

CLICK TO EXPAND

ADVERTISEMENT

Hi! Log in or sign up to personalize!

POPULAR ON FACEBOOK

NEWSPULSE

Most popular stories right now

Shooting witness alleges police misconduct

Scientist testifies about car trunk odor

Zimbabwe cop jailed for using Mugabe's toilet

Democrats turn up pressure on Weiner

Explore the news with NewsPulse »

LOCAL WEATHER & NEWS

SPORTS

MARKETS

Application

News

KATANA



[Sign In](#)☐ Remember me[Forgot it?](#)

# Follow your interests

Instant updates from your friends, industry experts, favorite celebrities, and what's happening around the world.



**New to Twitter?** Join today!

[Sign up](#)

**Languages** · [English](#) · [Français](#) · [Deutsch](#) · [Italiano](#) · [日本語](#) · [한국어](#) · [Русский](#) · [Español](#) · [Türkçe](#)

[About](#) · [Help](#) · [Blog](#) · [Mobile](#) · [Status](#) · [Jobs](#) · [Terms](#) · [Privacy](#) · [Advertisers](#) · [Businesses](#) · [Media](#) · [Developers](#) · [Resources](#) · © 2011 Twitter

# Twitter



# facebook

Email

☐ Keep me logged in

Password

Log In

[Forgot your password?](#)

Facebook helps you connect and share  
with the people in your life.



## Sign Up

It's free and always will be.

First Name:

Last Name:

Your Email:

Re-enter Email:

New Password:

I am:

Select Sex:

Birthday:

Month:

Day:

Year:

[Why do I need to provide my birthday?](#)

Sign Up

[Create a Page for a celebrity, band or business.](#)

[English \(US\)](#) [Español](#) [Português \(Brasil\)](#) [Français \(France\)](#) [Deutsch](#) [Italiano](#) [العربية](#) [हिन्दी](#) [中文\(简体\)](#) [日本語](#) »

Facebook © 2011 · [English \(US\)](#)

[Mobile](#) · [Find Friends](#) · [Badges](#) · [People](#) · [Pages](#) · [About](#) · [Advertising](#) · [Create a Page](#) · [Developers](#) · [Careers](#) · [Privacy](#) · [Terms](#) · [Help](#)

# Facebook



# Case Loads



Time is the enemy

# Case in Point

- OJ Simpson Murder Trial
- DNA Evidence Attacked
  - Made Huges Waves
    - Digital OJ.....

# Validate Your Tools

- One of the most important canon of forensics

iSheep



# Setup for Disaster



# Niche Tools

- Have their place in forensics
- Are more accurate than other tools
- Can adjust to changes quicker
- Easier to validate
- Cost effective





LANTERN



ViaExtract

# The future is...

- Smartphones
  - Apple iDevices
  - Android Devices
  - RIM?
  - Windows?

# Last Man Standing

- Apple - iOS
- Google - Android

Sean Morrissey

[smorrissey@katanaforensics.com](mailto:smorrissey@katanaforensics.com)

(410) 714-1413

[www.katanaforensics.com](http://www.katanaforensics.com)