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.
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
Comparison of iPhone storage capacity:

- **2007**: 4GB
- **2010**: 32GB
iPhones Worldwide
Total 35 Million and growing
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!
Why so serious?
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.mdbakup

iOS 3 backups,

0dc926a1810f7aee4e8f38793ed788701f93bf9d.mdata
0dc926a1810f7aee4e8f38793ed788701f93bf9d.mdinfo

iOS 4 backups,
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 3 Synced Photos
iOS 4
Synced Images
iOS 3
Geo Tracking

Geo Data was all in .plist format
<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>310,410,0x9087,0x1f504d0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Latitude</td>
<td>36.119055733333333333333333333333333333333</td>
</tr>
<tr>
<td>HorizontalAccuracy</td>
<td>300.2058267542113</td>
</tr>
<tr>
<td>VerticalAccuracy</td>
<td>454.2918533532134</td>
</tr>
<tr>
<td>Longitude</td>
<td>-115.173776133333333333333333333333333333</td>
</tr>
<tr>
<td>Altitude</td>
<td>614</td>
</tr>
<tr>
<td>Timestamp</td>
<td>256714314.483819</td>
</tr>
<tr>
<td>RSSI</td>
<td>-59</td>
</tr>
<tr>
<td>UMTSNeighbors</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RSCP</td>
<td>59</td>
</tr>
<tr>
<td>ARFCN</td>
<td>4385</td>
</tr>
<tr>
<td>PSC</td>
<td>76</td>
</tr>
<tr>
<td>ECN0</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>RSCP</td>
<td>72</td>
</tr>
<tr>
<td>ARFCN</td>
<td>9925</td>
</tr>
<tr>
<td>PSC</td>
<td>76</td>
</tr>
<tr>
<td>ECN0</td>
<td>7</td>
</tr>
</tbody>
</table>
iOS 4
Geo Location
<table>
<thead>
<tr>
<th>MCC</th>
<th>MNC</th>
<th>LAC</th>
<th>CI</th>
<th>Timestamp</th>
<th>Latitude</th>
<th>Longitude</th>
<th>HorizontalAccuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>310</td>
<td>410</td>
<td>7985</td>
<td>158494439</td>
<td>38.8857305</td>
<td>-77.08129543</td>
<td>500.0</td>
</tr>
<tr>
<td>2</td>
<td>310</td>
<td>410</td>
<td>7970</td>
<td>160761839</td>
<td>38.99729001</td>
<td>-76.58929085</td>
<td>500.0</td>
</tr>
<tr>
<td>3</td>
<td>310</td>
<td>410</td>
<td>7970</td>
<td>160761842</td>
<td>38.99759525</td>
<td>-76.5902422</td>
<td>500.0</td>
</tr>
<tr>
<td>4</td>
<td>310</td>
<td>410</td>
<td>7003</td>
<td>2036</td>
<td>38.97900587</td>
<td>-76.595685</td>
<td>2236.0</td>
</tr>
<tr>
<td>5</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>159451127</td>
<td>38.97786432</td>
<td>-76.59514242</td>
<td>2059.0</td>
</tr>
<tr>
<td>6</td>
<td>310</td>
<td>410</td>
<td>7020</td>
<td>2033</td>
<td>38.98040455</td>
<td>-76.59689146</td>
<td>2803.0</td>
</tr>
<tr>
<td>7</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>159451121</td>
<td>38.97991001</td>
<td>-76.59833091</td>
<td>2292.0</td>
</tr>
<tr>
<td>8</td>
<td>310</td>
<td>410</td>
<td>7970</td>
<td>159665688</td>
<td>38.9939197</td>
<td>-76.59843456</td>
<td>1295.0</td>
</tr>
<tr>
<td>9</td>
<td>310</td>
<td>410</td>
<td>7965</td>
<td>160774114</td>
<td>38.9644984</td>
<td>-76.58490574</td>
<td>1699.0</td>
</tr>
<tr>
<td>10</td>
<td>310</td>
<td>410</td>
<td>7003</td>
<td>1483</td>
<td>38.96925669</td>
<td>-76.60188108</td>
<td>1108.0</td>
</tr>
<tr>
<td>11</td>
<td>310</td>
<td>410</td>
<td>7020</td>
<td>14303</td>
<td>38.95828437</td>
<td>-76.57820677</td>
<td>1693.0</td>
</tr>
<tr>
<td>12</td>
<td>310</td>
<td>410</td>
<td>7965</td>
<td>160774642</td>
<td>38.97664427</td>
<td>-76.61203467</td>
<td>2418.0</td>
</tr>
<tr>
<td>13</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>158808566</td>
<td>38.97017753</td>
<td>-76.60790634</td>
<td>1168.0</td>
</tr>
<tr>
<td>14</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>159463391</td>
<td>38.95746797</td>
<td>-76.58152931</td>
<td>1655.0</td>
</tr>
<tr>
<td>15</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>159463397</td>
<td>38.98160874</td>
<td>-76.61495906</td>
<td>2644.0</td>
</tr>
<tr>
<td>16</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>159463397</td>
<td>38.95797337</td>
<td>-76.57731842</td>
<td>1738.0</td>
</tr>
<tr>
<td>17</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>159461327</td>
<td>38.9343169</td>
<td>-76.5651924</td>
<td>1686.0</td>
</tr>
<tr>
<td>18</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>15805961</td>
<td>38.9833917</td>
<td>-76.56602269</td>
<td>1929.0</td>
</tr>
<tr>
<td>19</td>
<td>310</td>
<td>410</td>
<td>7992</td>
<td>15805961</td>
<td>38.98313194</td>
<td>-76.56661653</td>
<td>895.0</td>
</tr>
</tbody>
</table>
Today we live in a world of instant gratification, where data is streamed instantiously.
News
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
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
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
The future is...

- Smartphones
- Apple iDevices
- Android Devices
- RIM?
- Windows?
Last Man Standing

- Apple - iOS
- Google - Android
Sean Morrissey

smorrissey@katanaforensics.com

(410) 714-1413

www.katanaforensics.com