



Geo-location Forensics On Mobile Devices

Yi Sun

Meiya Pico Information Co.



Yi Sun

Manager of Training & Technical Support

EnCE/ACE/MCT/MCSE/MCDBA/MCITP

Member of HTCIA

Sun.yi@mail.com





- More Mobile Devices
- More Smart Devices
- More Apps
 - Things Changed





- Satellite
 - GPS/A-GPS
 - GLONASS
- Cellular Network
 - MCC, MNC, LAC, CellID
- WLAN Network
 - IP Address
 - MAC





- iPod Touch 5th generation
- iPhone 3G / 3Gs / 4 / 4s / 5
- iPad with both WIFI and Cellular





- consolidated.db
- GPS data in Exif





- Cache.cell & Cache.wifi
 - Can found in most Android devices
- Photo with location data



- Google Latitude
- Google Map
- SNS Apps
 - Twitter
 - Facebook
 - Sina Weibo

```
<dict>
  <key>commentnum</key>
  <string>0</string>
  <key>content</key>
  <string>我在这里: #厦门高崎国际机场#
  <key>latitude</key>
  <string>24.53456</string>
  <key>level</key>
  <string>1</string>
  <key>longitude</key>
  <string>118.13217</string>
  <key>morologid</key>
  <string>y1GEDatUA</string>
  <key>nick</key>
  <string>我</string>
  <key>portrait</key>
```




- JPEG without Latitude & Longitude
 - Unique Background
 - Compare Manually
 - Try different Search Engines



Q & A