(U) Converged Analysis of Smartphone Devices

Identification/Processing/Tasking – All in a day's work

[redacted]

May 2010

Smartphone

Converged mobile devices offering advanced capabilities, often with PC-like functionality. No set industry standard definition.

Boasts powerful processors, memory, larger screens and open operating systems.

Economics of Transportation

- The gradual “blurring” of telecommunications, computers, and the Internet
- Multifaceted layering technologies
- Examples of convergence in SIGINT:
  - Blackberry, iPhone data, Smartphones
  - VOIP
  - Wireless Local Loop
  - GPRS – General Packet Radio Service

SmartPhone Applications

- Visual Communicator – Free application that combines Instant Messaging, Photo-Messaging and Push2Talk capabilities on a mobile platform. VC used on GPRS or 3G networks; [redacted]
- Symbian Operating System supporting encryption programs.
- WinZip, compression and encryption program.

Usage/Features

- Social Networking via Flixster

Social Networking site allowing users to share movie ratings, discover new movies and meet others with similar movie taste.

- Google Maps features
- Photo capture and editing capabilities
- Phone settings
- Mobile Facebook Apps (iPhone/Android)

Location Based Services

Where is the target?

- GPRS Dataset – breaking down barriers
- Providers catering to users based on location
- Android Phones pass GPS data in the clear
- No longer DNI/DNR

Taking a Closer Look

Photo Capture Software -

- iPhone Geotags for Photos

Raw tags coming through from a variety of devices

- Flixster App uses GPRS
- Flickr/Photobucket
- Mobile Facebook Apps Uploads

Processing

All in the Metadata, not the pretty pictures

- Unique applications require unique analysis
- GPS Indicators (sent to the server and towers for both phone and application)
- VoIP Indicators (multiple services)
- Type of Phone and Apps

Identification via Xkeyscore

- Make use of fingerprints in Xkeyscore via the EXIF metadata plugin
- Fingerprints for images (jpeg, tiff, gifs etc.)
- Examine the raw XML
- Provides device and time/location for the image

[redacted]

Golden Nugget!

Perfect Scenario – Target uploading photo to a social media site taken with a mobile device.

What can we get?

User Activity Leads

- Examine settings of phone as well as service providers for geo-location; specific to a certain region
- Networks connected
- Websites visited
- Buddy Lists
- Documents Downloaded
- Encryption used and supported
- User Agents

Targeting

Targeting both Telephony and DNI systems

- Call Logs
- SMS
- SIM Card Leads
- Email address
- IMEI/IMSI
- Unique Identifiers
- Blackberry PINS

Why do we care?

- Additional exploitation
- Target Knowledge/Leads
- Location
- Target Technology
- Denote Media used

Conclusion

- Challenge is how to tag data for analysts
- We can geo phones from virtually anywhere
- Buried GeoStamp from Phone or Apps
- Xkeyscore/Marina
- Tasking systems