Mobile Chat and Social Apps
Presented By: Geoff, Tayfun

Agenda

1. Introductions
2. Mobile Application Growth
3. Artifact Updates
4. Anatomy of a Mobile App
5. Questions
Who are we?

Geoff
Geoff joined Magnet Forensics in the Fall of 2014 and is responsible for Product Management. Prior to Magnet he has held a variety of Product Management and Leadership roles within the technology community. Most recently Geoff held some senior Product Management roles at BlackBerry.
Geoff holds an MBA and Bachelor of Engineering degrees from Queen’s University.

Tayfun
Tayfun joined Magnet Forensics in 2011 with a goal of evolving the flagship product Internet Evidence Finder. With a background in software engineering, Tayfun is currently responsible for defining products to assist in digital investigations as well as leading the development team responsible for artifacts.
Tayfun holds an Honours Bachelor of Applied Science degree from the University of Waterloo.

**Time Spent With the Internet, by Device, in the US**

*total minutes (mm) per month*

_February 2013 - January 2014*

[Graph showing time spent on the internet by device from February 2013 to January 2014.](#)
WhatsApp Messaging App User Growth

- **2012**: WhatsApp had approximately 100 million monthly active users
- **2013**: 400 million monthly active users
- **2015**: WhatsApp has more than 700 million monthly active users
every day our users now send over 30 billion messages.

---

**FACEBOOK ACTIVE MONTHLY USERS**

- **Q1'13**: 189, 562, 359
- **Q2'13**: 219, 600, 336
- **Q3'13**: 254, 620, 315
- **Q4'13**: 296, 649, 283
- **Q4'14**: 341, 667, 268
- **Q1'15**: 399, 671, 247
- **Q2'14**: 456, 668, 226
- **Q3'14**: 526, 663, 204
- **Q4'14**: 581, 667, 193

Facebook Quarterly/Annual Reports
Frequency of Application Appearance
Top 50 Since 2011 in US Social Networking

129 Applications Have Appeared in the Top 50 in 5 years on May 22nd

# of Applications

1 77
2 19
3 8
4 13
5 12

# of Appearances in the Top 50 List on May 22 between 2011 and 2015

Top iOS Social Networking Apps  Average Days between Updates

1. Facebook  21
2. 3. Whats App  49
3. KiK  31
4. Skype  39
5. Viber  40
6. Tango  24
Artifact Support

- Find the most relevant and current evidence
- Regular artifact updates so that IEF keeps pace with the rapidly changing app environment.
- Maintain existing apps and add new apps based on:
  - Popularity
  - Customer Requests

The Anatomy of a Mobile Application (Chat/Social)
Storage Location

There are various locations where an application can store it’s user data. In general there are **three major locations**:

**Application Sandbox**
- Standard location for applications
- Complexity: Medium

**External Storage (Android)**
- Usually used for backups or data they want to share with other applications on the device (i.e. Camera pictures, PDF documents etc.)
- Files that they want accessible by PC over USB
- Complexity: Easy

**Cloud/Internet**
- Storage of user information on proprietary servers
- Application downloads messages while in-use but doesn’t save them to the device
- Complexity: Difficult
Application Sandbox

With App Sandbox

Other user data

No access

Unrestricted access

Other system resources

Your app

Android Skype
/data/data/com.skype.raider

iOS Skype
/private/var/mobile/Applications/79928363-ACA7-43AD-9289-5F14051F28EE

PC Skype
C:/Users/UserName/AppData/Roaming/Skype
Encryption
Chat app developers are seeing the demand for better privacy in their communications. This is leading them to introduce different types of encryption to their apps.

File Encryption
- Entire storage file is encrypted
- SQLite encrypted databases (e.g. WhatsApp .crypt#)

Field Encryption
- Encrypting specific fields within the file
- A certain column of data in a SQLite table could be encrypted

End-to-End Encryption (E2EE)
- This covers encryption of data over the wire (network traffic encryption)
- Prevents ‘man in the middle’ type attacks
- Doesn’t directly affect Smartphone forensics
End-To-End Encryption

End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties without being intercepted or read by other parties.

“This is the largest deployment of end-to-end encryption ever.”

WhatsApp End-To-End Encryption

WhatsApp Security cheat sheet

encrypted

cleartext

iOS

Android

Android

Hi Bob!

Hi Alice!

iOS

iOS
There are various structures that a chat/social app may use to store its data. Some of these are easily understood with specs in the public domain, others are not.

**Database Storage**
- SQLite
- ESEDB

**Flat File Storage**
- CSV
- Text
- Log Files

**Structured Storage**
- JSON
- XML

**Complex Structured Storage**
- Plist (binary, xml)
- Proprietary structures

In general, databases have tables of data with columns to represent different properties of a data point.

**SQLite**
- Open source
- Most common storage for Mobile apps
- Multi-platform
- Data is 'queried' using a Structured Query Language (SQL)

**ESEDB**
- Windows proprietary
- Started with IE 10, continued in 11, 12 and EDGE
- Windows Phone
  - SMS
  - Contacts
  - Call Logs
  - Emails
File Structure

Structured

- **JSON**
  - Javascript Object Notation
  - Useful for representing ‘objects’ in string form
  - A thing that has one or more properties
- **XML**
  - eXtensible Markup Language
  - Also useful for representing objects in string form
  - A thing that has one or more properties

---

"Beautified" JSON

```
"results": [  
  {  
    "venue": {  
      "id": "4e7e7f65d5fb7a1d34f57c71",  
      "name": "Beertown Public House",  
      "location": {  
        "address": "75 King St S",  
        "crossStreet": "Willis Way",  
        "lat": 43.46396196208276,  
        "lng": -80.52240371704102,  
        "distance": 2107,  
        "postalCode": "N2J 1P2",  
        "cc": "CA",  
        "city": "Waterloo",  
        "state": "ON",  
        "country": "Canada",  
        "contextLine": "Waterloo, ON",  
        "formattedAddress": {  
          "75 King St S (Willis Way)",  
          "Waterloo ON N2J 1P2"  
        }  
      }  
    }  
  }  
]```
Mobile Chat and Social App Forensics

File Structure

Complex Structured

- Often apps on iOS will use the property-list structure (plist)
- Developers create their own complex storage mechanisms for a few reasons
  - Increase read/write performance
  - Create a format that works for the type of data they are storing
  - Because they can…engineers like to make things

Skype Android Mobile App

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>chatsync</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>cache</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>tdata</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>tdata.lock</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>media</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>media.messages</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>envmanager</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>skub</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>settings</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>simcache</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>themanager</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>thumbnails</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>voicecall</td>
<td>2/11/2015 15:16 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Structured</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td>2/3/2013 10:35 AM</td>
<td>File folder</td>
<td></td>
</tr>
</tbody>
</table>

Twitter streams utilizes the complex Apple Binary Plist structure

Skype "chatsync" proprietary complex structured file
Data Format

The format the data is stored in can affect the way you interpret it or try and parse it into a readable string

- **Plain Text**
  - Complexity: Easy

- **Dates**
  - Unix, Apple timestamps
  - String formatted local timestamps
  - Non-UTC
  - Complexity: Varies

- **Encoding**
  - Base64
    - Common way to store binary data in a structured file
    - Complexity: Medium
  - UTF8, 16 etc.
    - Multiple languages
    - Complexity: Varies

- **Structured**
  - Geo-location Co-ordinates
    - Latitude and Longitude
    - Complexity: Medium
  - JSON/XML
    - Storage of geolocation data
    - Complexity: Difficult

Artifact Engineering

At Magnet Forensics we have a team dedicated to researching and developing products to automate the recovery of mobile application artifacts, this includes peeling back the layers of the onion.

- Every time a new app emerges, the onion must be peeled.
- Every time an app updates, the onion must be re-peeled to see what’s new.
Find Mobile Artifacts with IEF

Types of Images Supported

• Physical (Raw binary dump)
• Logical (Full file system or partial file system)
• iTunes backups (coming soon)
• Android AB backup files (coming soon)
• JTAG binary data dump
• Chip-off binary data dump

Find Mobile Artifacts with IEF

Most popular Chat and Social Artifacts

Other categories include:

• Cloud, Web, Documents, Email, P2P, Media and native application information
In IEF 6.6 we enabled digital forensic examiners to dive deeper and validate the mobile evidence being found with the Hex and Text viewer.
Analyze Mobile Evidence

Investigators can review evidence using our visualizations that help show data in its most natural form.

Dynamic App Finder

Dynamic App Finder enables examiners to find chat messages from potentially thousands of chat apps.

- It has the ability to detect obscure or custom chat apps
- With the frequency of application updates it can provide a stop-gap solution if an app changes the storage mechanism
How does it work?
Dynamic App Finder

Dynamic App Finder looks for SQLite databases in the mobile image and runs heuristics to determine if the database in question is a chat database.

A correctly identified chat database will be parsed as an artifact with the following fields identified:

- Sender
- Receiver
- Chat Message
- Date/Time

Remapping Fields
Dynamic App Finder

Format and map data to better represent the application storage.

After an IEF search has completed, you will be presented with this option screen.
Viewing Results
Dynamic App Finder

Date Formatted (Unix Timestamp)

Thank you.
Please feel free to ask questions, and take some time to give us feedback by filling out the survey.