A glimpse of the NEW FOR585: Advanced Smartphone course

Heather Mahalik (@HeatherMahalik)

FOR585: Advanced Smartphone Forensics training events:

**SANSFIRE**
Washington, DC
July 24-29
Heather Mahalik
www.sans.org/sansfire

**Chicago**
Chicago, IL
Aug 21-26
Cindy Murphy
www.sans.org/chicago

**San Francisco Fall**
San Francisco, CA
Sept 5-10
Cindy Murphy
www.sans.org/san-francisco-fall

**Network Security**
Las Vegas, NV
Sept 10-15
Heather Mahalik
www.sans.org/network-security-2017

**vLive**
July 10-16
Heather Mahalik
www.sans.org/vlive

**Simulcast**
Sep 10-15
Heather Mahalik
www.sans.org/simulcast

“Simply brilliant! The best SANS course I have ever taken, excellently developed and expertly delivered.”

-R. Pittman, NASA
Why the Change?

2 updates per year for the course
- 1 Major and 1 Minor

OS versions are progressing with no signs of slowing

Phones become obsolete and need to be replaced with newer devices

New methods for manual analysis available

We have learned a lot since the last major update
- It’s time to share it with you!

Smartphones evolve quickly!

We have new tools and scripts to introduce
What’s New in FOR585

- 7 new labs
- Tool changes (SQLite tools, new scripts, AXIOM, etc.)
- Bonus labs x 4
- Extraction methods updated
- Password cracking and lock bypass methods updated
- Methods for manual extraction and analysis updated
- Choose your own adventures!

Schedule changes

- Day 1 – Malware, Smartphone Overview and SQLite Forensics
- Day 2 – Android Forensics
- Day 3 – Android Backup and iOS Forensics
- Day 4 – iOS Backup, Windows and BlackBerry 10 Forensics
- Day 5 – Third-Party Apps and SQLite Forensics
- Day 6 – Expect a new challenge in summer 2018
What Does This Mean For Me?

**Future Students**

- Take FOR585 to get the most current material
  - 20 Hands-on Labs to test your smartphone knowledge
  - Vendor neutral – we teach the best methods and tools for extracting and analyzing smartphone data
- Take the GIAC GASF cert upon completion

**FOR585 Alumni**

- Refer to smarterforensics.com in your FOR585 portal
  - Bonus information
  - Updated Cheat Sheets
- 50% discount if you want to take the course again!
- GIAC Cert is based on course version
  - You will not see questions for the updated material
  - Your books will work for the cert if you have not attempted it yet
- Keep testing your tools and stay current!
<table>
<thead>
<tr>
<th>SANS DFIR</th>
<th>FOR585 SIFT Programs Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SQLite Spy</td>
<td>• SQLite Browser</td>
</tr>
<tr>
<td>• XRY Reader</td>
<td>• Wireshark</td>
</tr>
<tr>
<td>• Cellebrite Physical Analyzer</td>
<td>• DeCode</td>
</tr>
<tr>
<td>• UFED4PC</td>
<td>• Android Developer Toolkit</td>
</tr>
<tr>
<td>• UFED Link Analysis</td>
<td>• Dex2Jar</td>
</tr>
<tr>
<td>• PList Editor</td>
<td>• Java Decompiler/Dev Kit</td>
</tr>
<tr>
<td>• iTunes</td>
<td>• FTK Imager</td>
</tr>
<tr>
<td>• Oxygen Forensics Detective</td>
<td>• Frhed</td>
</tr>
<tr>
<td>• IEF Mobile</td>
<td>• Autopsy</td>
</tr>
<tr>
<td>• AXIOM</td>
<td>• BlackLight</td>
</tr>
<tr>
<td>• NBU Backup Explorer</td>
<td>• Andriller</td>
</tr>
<tr>
<td>• Sanderson SQLite Forensic Browser</td>
<td>• And more!</td>
</tr>
<tr>
<td>• Android SDK</td>
<td></td>
</tr>
</tbody>
</table>

FOR585 | Advanced Smartphone Forensics 5
A Glimpse of the NEW FOR585…

Advanced Smartphone Forensics
What Nougat Introduced

- VR Daydream
- Use 2 Applications simultaneously via multi-windows
- Multi Chrome tabs
- Clear all recently used Applications
- Application install tracking
Verifying a Lock Setting (2)

- Gesture or Pattern = 65536
- Simple 4-digit PIN = 131072
- Complex PIN = 196608
- Alphabetic Password = 262144
- Alphanumeric Password = 327680
- Complex Password = 393216
iBackupBot Method for Obtaining Log Files
How are Android Apps Different on BlackBerry 10?

- appdata
  - data/app
    - .APK files for each application
  - data/dalvik-cache
    - Classes.dex file for each application
  - data/data
    - Application directory folder
WiFi Access Points

/settings/var/etc/netsecure/wpa_pps.conf

- **RED** – Number of saved profiles
- **Orange** – Name of Wireless Access Point
- **Blue** – Modified Timestamp
- **Purple** – Password (if available)
Apps Today Can Do it All!

- Mapping
- Video messaging
- Share files
- Send pictures
- Self-destruct
- Record audio
- Encrypt messages
- Make phone calls

I can do EVERYTHING!
Is the App BeingParsed?

• Does the tool parse the application or not?
• What data is presented to the analyst?
• Are there other details stored in the database that could be useful?

Below are the results of the same device with Oxygen and Cellebrite.
### Information Overload

**SQL Queries can eliminate unwanted or unnecessary data**

<table>
<thead>
<tr>
<th>Z_PK</th>
<th>Z_ENT</th>
<th>Z_OPT</th>
<th>ZFLAGS</th>
<th>ZINTERNALID</th>
<th>ZSTATE</th>
<th>ZSYSTEMSTATE</th>
<th>ZTYPE</th>
<th>ZBODY</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>0</td>
<td>0</td>
<td>16</td>
<td>0</td>
<td>1</td>
<td>Welcome to Kik, the super fast questions, let me know. I'll do r</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>You started chatting with Ace</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>0</td>
<td>0</td>
<td>16</td>
<td>12</td>
<td>1</td>
<td>Hey lloyd, so glad we're finally i</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>4</td>
<td>2</td>
<td>16</td>
<td>12</td>
<td>1</td>
<td>7cbf883b-8672-44e0-97fe-c376</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>0</td>
<td>3</td>
<td>16</td>
<td>12</td>
<td>1</td>
<td>WHAT do you think of this picture?</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5</td>
<td>0</td>
<td>30</td>
<td>0</td>
<td>2</td>
<td>I just sent you one of my current phone</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>6</td>
<td>30</td>
<td>0</td>
<td>2</td>
<td>Hello microphone</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>6</td>
<td>30</td>
<td>0</td>
<td>2</td>
<td>I saved the pic of the trash and</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>6</td>
<td>30</td>
<td>0</td>
<td>2</td>
<td>I saved a kik picture too</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>6</td>
<td>10</td>
<td>30</td>
<td>2</td>
<td>3cbaf5e30-d11d-456c-960a-a1a</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>6</td>
<td>16</td>
<td>12</td>
<td>1</td>
<td>Hi kik</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>16</td>
<td>1</td>
<td>Kik Team at your service!</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>4</td>
<td>13</td>
<td>30</td>
<td>2</td>
<td>You started a group with Ace Vc</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
Choosing the Correct Timestamp Conversion

Based on the timestamps from the kik.sqlite database from the previous examples, which one of these conversions will provide the correct datetime result?

<table>
<thead>
<tr>
<th>User</th>
<th>Timestamp</th>
<th>Message</th>
<th>Message Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>497800782.474</td>
<td>Welcome to Kik, the super fast smartphone...</td>
<td>497800782.987472</td>
</tr>
<tr>
<td>2</td>
<td>497803811.6537</td>
<td>You started chatting with Ace</td>
<td>497803811.6537</td>
</tr>
<tr>
<td>3</td>
<td>497804196.154</td>
<td>Hey Lloyd, so glad we’re finally in touch</td>
<td>497804389.586069</td>
</tr>
<tr>
<td>4</td>
<td>497805067.896</td>
<td>7cbf883b-8672-44e0-97fe-c3705e75f7c7</td>
<td>497805068.863391</td>
</tr>
<tr>
<td>5</td>
<td>497805067.915</td>
<td>WHAT do you think of this picture?</td>
<td>497805068.963701</td>
</tr>
</tbody>
</table>
Adding the Timestamp String to the Query

```sql
SELECT
    ZUSER AS "User",
    datetime(ZTIMESTAMP+ 978307200,'unixepoch','localtime') AS "Timestamp",
    ZBODY AS "Message",
    datetime(ZRECEIVEDTIMESTAMP+ 978307200,'unixepoch','localtime') AS "Message Received"
FROM ZKIKMESSAGE
```

<table>
<thead>
<tr>
<th>User</th>
<th>Timestamp</th>
<th>Message</th>
<th>Message Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>2016-10-10 09:59:42</td>
<td>Welcome to Kik, the super fast smartphone messenger! ...</td>
<td>2016-10-10 09:59:42</td>
</tr>
<tr>
<td>41</td>
<td>2016-10-10 10:50:11</td>
<td>You started chatting with Ace</td>
<td>2016-10-10 10:50:11</td>
</tr>
<tr>
<td>41</td>
<td>2016-10-10 10:56:36</td>
<td>Hey Lloyd, so glad we’re finally in touch</td>
<td>2016-10-10 10:59:49</td>
</tr>
<tr>
<td>41</td>
<td>2016-10-10 11:11:07</td>
<td>7cbf883b-8672-44e0-97fe-c3705e75f7c7</td>
<td>2016-10-10 11:11:08</td>
</tr>
<tr>
<td>41</td>
<td>2016-10-10 11:11:07</td>
<td>WHAT do you think of this picture?</td>
<td>2016-10-10 11:11:08</td>
</tr>
</tbody>
</table>
Locating Attachments by Joining two Tables

<table>
<thead>
<tr>
<th>android_metadata (1)</th>
<th>_id</th>
<th>_video_id</th>
<th>_key</th>
<th>_localPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.mltygjUscSyueuc1W8YPiw</td>
<td></td>
<td></td>
<td></td>
<td>/data/user/0/co.happybits.marcopolio/files/d2696aca-a254-c524-92c3-eb9cd56f183e.mp4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>android_metadata (1)</th>
<th>_id</th>
<th>_video_id</th>
<th>_key</th>
<th>_localPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.mltygjUscSyueuc1W8YPiw</td>
<td></td>
<td></td>
<td></td>
<td>/data/user/0/co.happybits.marcopolio/files/d1c1cc5a-6a27-c506-ba1d-5b4d637a027c.mp4</td>
</tr>
</tbody>
</table>
Who Should Take FOR585?

- Examiners interested in smartphone forensics
- Experienced digital forensic examiners who want to extend their knowledge and experience to forensic analysis of mobile devices, especially smartphones
- Media exploitation analysts who need to master Tactical Exploitation or Document and Media Exploitation (DOMEX) operations on smartphones and mobile devices
- Information security professionals who respond to data breach incidents and intrusions
- Incident response teams tasked with identifying the role that smartphones played in a breach
- Law enforcement officers, federal agents, or detectives who want to master smartphone forensics and expand their investigative skills beyond traditional host-based digital forensics
- IT auditors who want to learn how smartphones can expose sensitive information
- Examiners working accident reconstruction
- Graduates of SANS SEC575, FOR408/500, FOR508, FOR572, FOR526 or FOR518 who want to take their skills to the next level
Questions?

Heather Mahalik
heather@smarterforensics.com
Twitter: @HeatherMahalik
http://smarterforensics.com
A glimpse of the NEW FOR585: Advanced Smartphone course

Heather Mahalik (@HeatherMahalik)

FOR585: Advanced Smartphone Forensics training events:

**SANSFIRE**  
Washington, DC  
July 24-29  
Heather Mahalik  
www.sans.org/sansfire

**Chicago**  
Chicago, IL  
Aug 21-26  
Cindy Murphy  
www.sans.org/chicago

**San Francisco Fall**  
San Francisco, CA  
Sept 5-10  
Cindy Murphy  
www.sans.org/san-francisco-fall

**Network Security**  
Las Vegas, NV  
Sept 10-15  
Heather Mahalik  
www.sans.org/network-security-2017

**vLive**  
July 10-16  
Heather Mahalik  
Cindy Murphy  
www.sans.org/vlive

**Simulcast**  
Sep 10-15  
Heather Mahalik  
www.sans.org/simulcast

“Simply brilliant! The best SANS course I have ever taken, excellently developed and expertly delivered.”  
-R. Pittman, NASA