SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

THE WEBCAST WILL BEGIN SHORTLY

A glimpse of the NEW FOR585: Advanced Smartphone course

Heather Mahalik (@HeatherMahalik)

FOR585: Advanced Smartphone Forensics training events:

SANSFIRE	Chicago	San Francisco Fall	Network Security	vLive	Simulcast
Washington, DC	Chicago, IL	San Francisco, CA	Las Vegas, NV	July 10-16	Sep 10-15
July 24-29	Aug 21-26	Sept 5-10	Sept 10-15	*Heather Mahalik*	*Heather Mahalik*
Heather Mahalik	*Cindy Murphy*	*Cindy Murphy*	*Heather Mahalik*	*Cindy Murphy*	
www.sans.org/sansfire	www.sans.org/chicago	www.sans.org/san-francisco-fall	www.sans.org/network-security-2017	www.sans.org/vlive	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!

FOR585 SIFT Programs Installed

- SQLite Spy
- XRY Reader
- Cellebrite Physical Analyzer
- UFED4PC
- UFED Link Analysis
- PList Editor
- iTunes
- Oxygen Forensics Detective
- IEF Mobile
- AXIOM
- NBU Backup Explorer
- Sanderson SQLite Forensic Browser
- Android SDK
- SQLite Browser
- Wireshark
- DeCode
- Android Developer Toolkit
- Dex2Jar
- Java Decompiler/Dev Kit
- FTK Imager
- Frhed
- Autopsy
- BlackLight
- Andriller
- And more!

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


```
{" wifi_power":"1"}{" wifi_notify_mhs_to_sta":"0"}
{"num_profiles_saved":3}

{"uid":"bd353ce0-e26b-11e6-b6bf-
eb593d9ac7af","last_modified_ts":"509.254882732","name":"CRGS","type":"wifi","reason_code":0,"owner":"UI","d
hcp":"auto","manual":"no","_enable":"1","priority":"0","_user_enable":"1","enterprise":false,"_saved":"1","ss
id":"CRGS","scan_ssid":"0","key_mgmt":"WPA-PSK","psk":"\"1234password
\"","band_select":"0","ap_handover":"0","_editability":"editable","_proxy_editability":1,"_proxy_enable":fals
e,"manual6":"off","aggregator_status":0}

{"uid":"a9e5bc02-a7cf-11e3-ac44-f3122509850f","last_modified_ts":"509.531859157","name":"FiOS-
FiOS","type":"wifi","reason_code":0,"owner":"UI","dhcp":"auto","manual":"no","_enable":"1","priority":"1","_u
ser_enable":"1","enterprise":false,"_saved":"1","ssid":"FiOS-FiOS","scan_ssid":"0","key_mgmt":"WPA-
PSK","psk":"\"PASSWORD1\"","band_select":"0","ap_handover":"0","_editability":"editable","_proxy_editability"
:1,"_proxy_enable":false,"manual6":"off","aggregator_status":0}
```


- **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

Self-destruct

Encrypt messages

Send pictures

Record audio

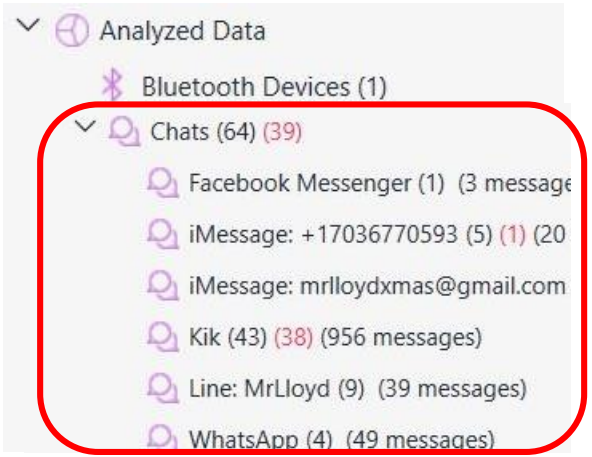
Make phone calls

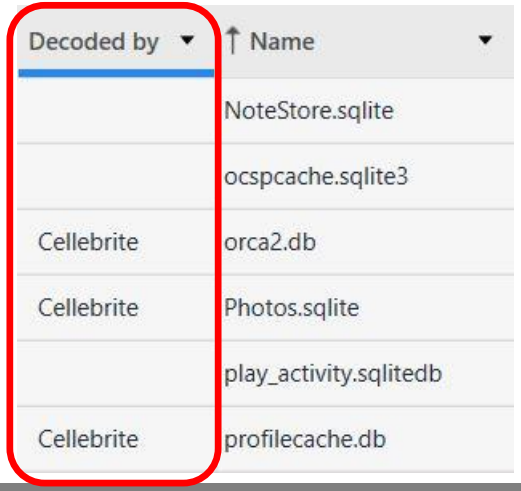
I can do EVERYTHING!

Is the App Being Parsed?

- 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

Z_PK	Z_ENT	Z_OPT	ZFLAGS	ZINTERNALID	ZSTATE	ZSYSTEMSTATE	ZTYPE	ZBODY
1	6	4	0	0	16	0	1	Welcome to Kik, the super fast questions, let me know. I'll do r
2	6	4	0	0	2	0	5	You started chatting with Ace
3	6	3	0	1	16	12	1	Hey lloyd, so glad we're finally i
4	6	2	4	2	16	12	1	7cbf883b-8672-44e0-97fe-c370
5	6	4	0	3	16	12	1	WHAT do you think of this pic
7	6	5	0	5	30	0	2	I just sent you one of my currer
8	6	6	0	6	30	0	2	Hello microphone
9	6	6	4	7	30	0	2	
10	6	3	0	8	16	12	1	Test chat from ace to lloyd
11	6	4	0	9	16	12	1	I saved a kik picture too
12	6	6	0	10	30	0	2	I saved the pic of the trash and
14	6	4	4	12	16	12	1	3cba5c30-d11d-456c-960a-a1a
15	6	5	0	1	30	0	2	Hi kik
16	6	2	0	2	16	12	1	Kik Team at your service!
17	6	6	4	13	30	0	2	
18	6	2	0	0	0	0	3	You started a group with Ace V

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?

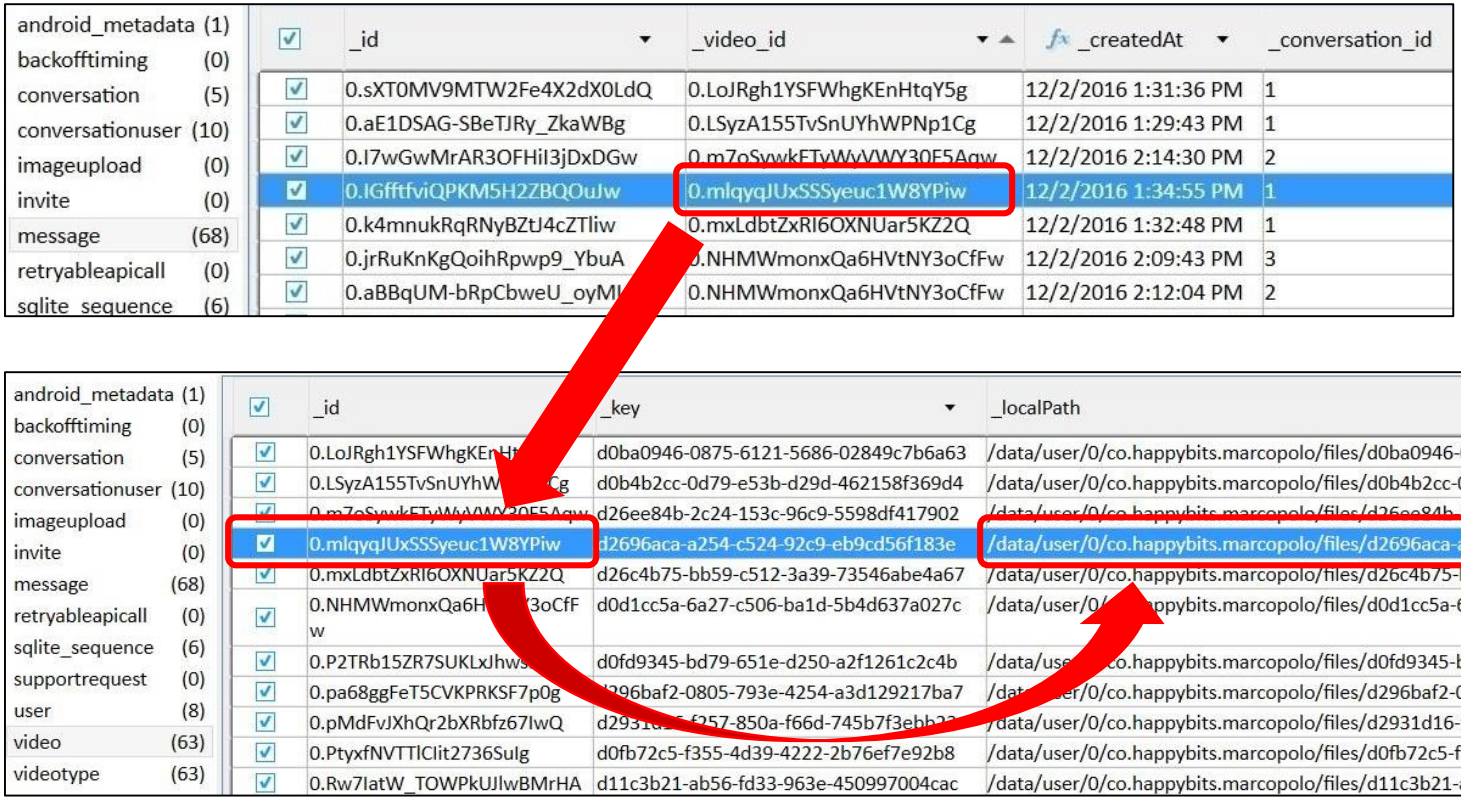
	User	Timestamp	Message	Message Received
1	37	497800782.474	Welcome to Kik, the super fast smartphon...	497800782.987472
2	41	497803811.6537	You started chatting with Ace	497803811.6537
3	41	497804196.154	Hey lloyd, so glad we're finally in touch	497804389.586069
4	41	497805067.896	7cbf883b-8672-44e0-97fe-c3705e75f7c7	497805068.863391
5	41	497805067.915	WHAT do you think of this picture?	497805068.963701

Adding the Timestamp String to the Query

```
1  SELECT
2  ZUSER AS "User",
3  datetime(ZTIMESTAMP+ 978307200,'unixepoch','localtime') AS "Timestamp",
4  ZBODY AS "Message",
5  datetime(ZRECEIVEDTIMESTAMP+ 978307200,'unixepoch','localtime') AS "Message Received"
6  FROM ZKIKMESSAGE
```

	User	Timestamp	Message	Message Received
1	37	2016-10-10 09:59:42	Welcome to Kik, the super fast smartphone messenger! ...	2016-10-10 09:59:42
2	41	2016-10-10 10:50:11	You started chatting with Ace	2016-10-10 10:50:11
3	41	2016-10-10 10:56:36	Hey lloyd, so glad we're finally in touch	2016-10-10 10:59:49
4	41	2016-10-10 11:11:07	7cbf883b-8672-44e0-97fe-c3705e75f7c7	2016-10-10 11:11:08
5	41	2016-10-10 11:11:07	WHAT do you think of this□ picture?	2016-10-10 11:11:08

Locating Attachments by Joining two Tables



android_metadata	(1)
backofftiming	(0)
conversation	(5)
conversationuser	(10)
imageupload	(0)
invite	(0)
message	(68)
retryableapicall	(0)
sqlite_sequence	(6)

_id	_video_id	_createdAt	_conversation_id
0.sXT0MV9MTW2Fe4X2dX0LdQ	0.LoJRgh1YSFWhgKEnHtqY5g	12/2/2016 1:31:36 PM	1
0.aE1DSAG-SBeTJRy_ZkaWBg	0.LSyzA155TvSnUYhWPNp1Cg	12/2/2016 1:29:43 PM	1
0.I7wGwMrAR3OFHiI3jDxDGw	0.m7oSywkFTyWyVWY30F5Aqw	12/2/2016 2:14:30 PM	2
0.IGfftfviQPKM5H2ZBQOuJw	0.mlqyqJUxSSSyeuc1W8YPiw	12/2/2016 1:34:55 PM	1
0.k4mnukRqRNyBZtJ4cZTliw	0.mxLdbtZxRI6OXNUar5KZ2Q	12/2/2016 1:32:48 PM	1
0.jrRuKnKgQoihRpwp9_YbuA	0.NHMWmonxQa6HVtNY3oCfFw	12/2/2016 2:09:43 PM	3
0.aBBqUM-bRpCbweU_oyMI	0.NHMWmonxQa6HVtNY3oCfFw	12/2/2016 2:12:04 PM	2

android_metadata	(1)
backofftiming	(0)
conversation	(5)
conversationuser	(10)
imageupload	(0)
invite	(0)
message	(68)
retryableapicall	(0)
sqlite_sequence	(6)
supportrequest	(0)
user	(8)
video	(63)
videotype	(63)

_id	_key	_localPath
0.LoJRgh1YSFWhgKEnHt	d0ba0946-0875-6121-5686-02849c7b6a63	/data/user/0/co.happybits.marcopolo/files/d0ba0946-0875-6121-5686-02849c7b6a63.mp4
0.LSyzA155TvSnUYhW Cg	d0b4b2cc-0d79-e53b-d29d-462158f369d4	/data/user/0/co.happybits.marcopolo/files/d0b4b2cc-0d79-e53b-d29d-462158f369d4.mp4
0.m7oSywkFTyWyVWY30F5Aqw	d26ee84b-2c24-153c-96c9-5598df417902	/data/user/0/co.happybits.marcopolo/files/d26ee84b-2c24-153c-96c9-5598df417902.mp4
0.mlqyqJUxSSSyeuc1W8YPiw	d2696aca-a254-c524-92c9-eb9cd56f183e	/data/user/0/co.happybits.marcopolo/files/d2696aca-a254-c524-92c9-eb9cd56f183e.mp4
0.mxLdbtZxRI6OXNUar5KZ2Q	d26c4b75-bb59-c512-3a39-73546abe4a67	/data/user/0/co.happybits.marcopolo/files/d26c4b75-bb59-c512-3a39-73546abe4a67.mp4
0.NHMWmonxQa6H 3oCfF w	d0d1cc5a-6a27-c506-ba1d-5b4d637a027c	/data/user/0/ ppybits.marcopolo/files/d0d1cc5a-6a27-c506-ba1d-5b4d637a027c.mp4
0.P2TRb15ZR7SUKLxJhw	d0fd9345-bd79-651e-d250-a2f1261c2c4b	/data/use co.happybits.marcopolo/files/d0fd9345-bd79-651e-d250-a2f1261c2c4b.mp4
0.pa68ggFeT5CVKPRKSF7p0g	296baf2-0805-793e-4254-a3d129217ba7	/dat er/0/co.happybits.marcopolo/files/d296baf2-0805-793e-4254-a3d129217ba7.mp4
0.pMdFvJXhQr2bXRbfz67IwQ	d2931d f257-850a-f66d-745b7f3ebb23	/data/user/0/co.happybits.marcopolo/files/d2931d16-f257-850a-f66d-745b7f3ebb23.mp4
0.PtyxfNVTTlClit2736Sulg	d0fb72c5-f355-4d39-4222-2b76ef7e92b8	/data/user/0/co.happybits.marcopolo/files/d0fb72c5-f355-4d39-4222-2b76ef7e92b8.mp4
0.Rw7IatW_TOWPkUJlwBMrHA	d11c3b21-ab56-fd33-963e-450997004cac	/data/user/0/co.happybits.marcopolo/files/d11c3b21-ab56-fd33-963e-450997004cac.mp4

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

SANS DFIR Webcast Series

DIGITAL FORENSICS & INCIDENT RESPONSE

THANK YOU FOR ATTENDING

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