



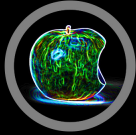
**One Tool Can't Solve all Your
Problems...But You Can!**



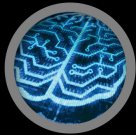
FOR408
Windows Forensics
GCFE



FOR518
Mac Forensics



FOR526
Memory Forensics
In-Depth



FOR585
Advanced Smartphone
Forensics GASF



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

OPERATING
SYSTEM &
DEVICE
IN-DEPTH



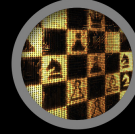
INCIDENT
RESPONSE
& THREAT
HUNTING



FOR508
Advanced Incident Response
GCFA



FOR572
Advanced Network Forensics
and Analysis GNFA



FOR578
Cyber Threat Intelligence



FOR610
REM: Malware Analysis
GREM



SEC504
Hacker Tools, Techniques,
Exploits, and Incident Handling
GCIH



MGT535
Incident Response
Team Management



@sansforensics



sansforensics



dfir.to/DFIRLinkedInCommunity



dfir.to/gplus-sansforensics



dfir.to/MAIL-LIST

About Me

Principal Forensic Scientist at Oceans Edge, Inc.

SANS Senior Instructor

Involved with Infosec/Forensics for 13+ years

Course Lead and co-author of FOR585

Instructor of FOR585 and FOR408

Co-Author of Practical Mobile Forensics (1st and 2nd Editions)

Mom and a wife

Dog, horse and wine lover 😊

Some considerations

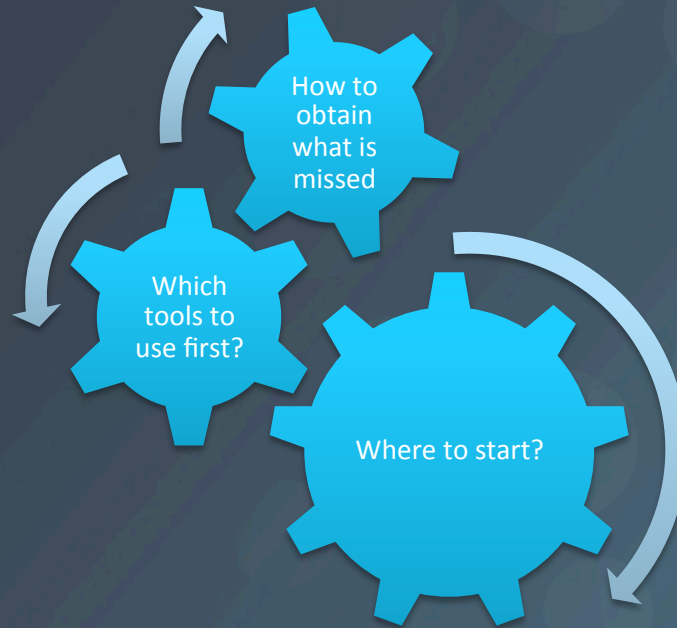
Will your tool catch you when you fall?

- Will you be able to defend the evidence?
- Can you find the data?
- What if the tools contradict one another?
- Do you understand the artifacts?
- Don't know just enough to be dangerous
 - Test your tools
 - Validate your results
 - Accept change



The steps you take can make or break the case

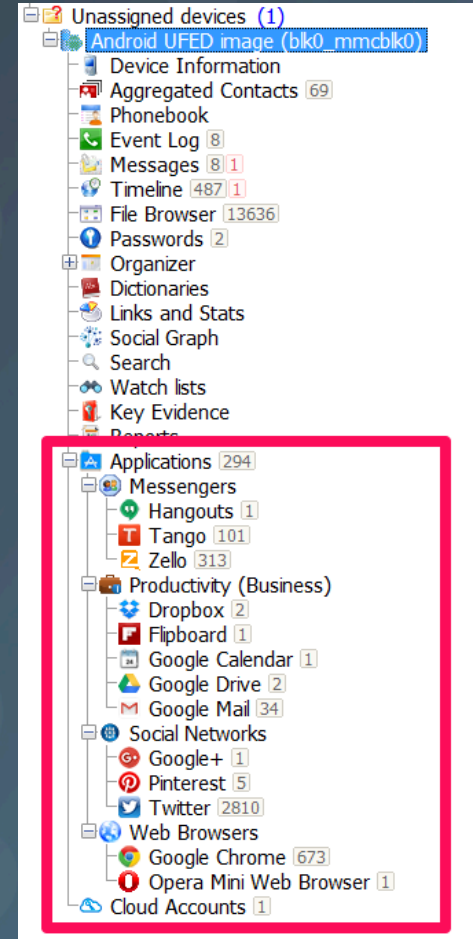
Consider your actions



I paid \$\$\$, it better work

Why the tools fail...

- There is so much data on smart devices
- Too many applications
 - Frequent updates
 - Database formats vary (timestamps)
- OS updates
- Knowing where to find this information is the hardest part
 - Do not expect your tool to know everything
- Knowing how the artifact was created is key
 - Hint – this is your responsibility!



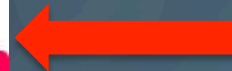
Example 1: Simple communication

Magnet IEF



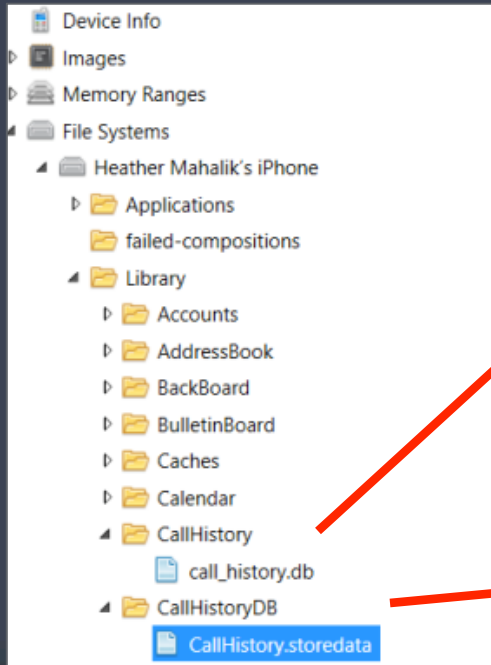
Mobile	
Calendar Events	157
iOS Call Logs	222
iOS Contacts	507

Device Content	
Phone Data	
Bluetooth Devices	3 (0)
Call Log	184 (64)



UFED Physical Analyzer

What's really behind that call?



A screenshot of an iOS 7 database view. The 'Database view' tab is selected. The table list shows:

_SqliteDatabaseProperties	(11)
call	(158)
sqlite_sequence	(1)

iOS 7

A screenshot of an iOS 8 & 9 database view. The 'Database view' tab is selected. The table list shows:

ZCALLDBPROPERTIES	(1)
ZCALLRECORD	(1361)
Z_METADATA	(1)
Z_PRIMARYKEY	(2)

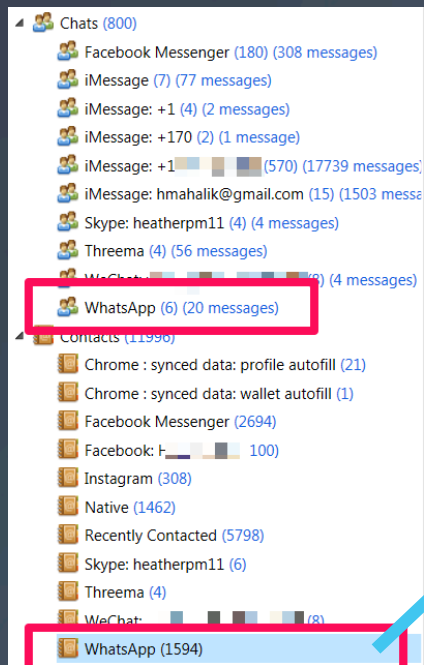
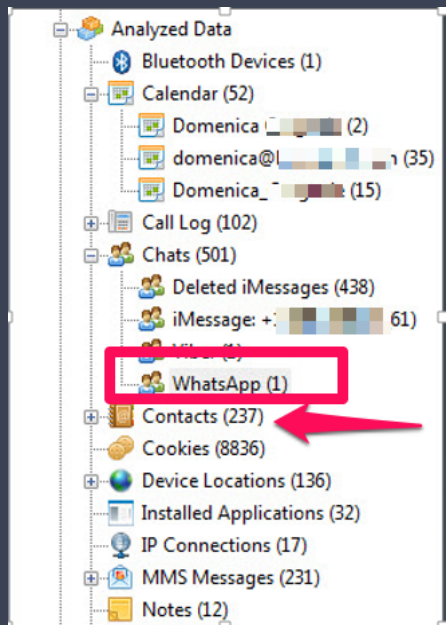
iOS 8 &
iOS 9

Example 2: Application Data

- Yes, I know that they are claiming encryption now
 - Stay tuned...
 - I never trust developer claims
- I love to prove them wrong
- FOR585 teaches you how to do this for almost every app

WhatsApp scenarios

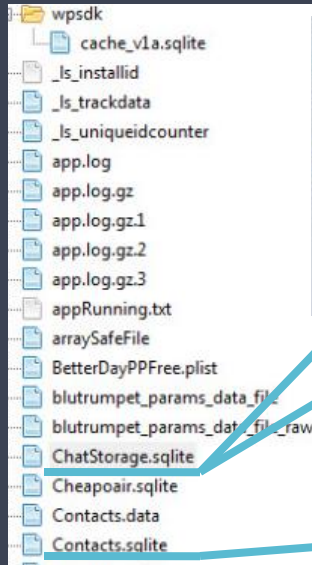
What is Physical Analyzer doing here?



#	Name	Phones
34		Mobile 7039
35		Fax 7037939
36		Mobile 2083
37		Mobile 7033
38		Mobile 4102
39		Work 703
40		Mobile 7032
41		
42	#BAL	Mobile 225
43	#MIN	Mobile 646
44	#PMT	Mobile 768
45	A Ad	Mobile 904
46	Aaron	Mobile 715
47	Aaron	Work 2404

WhatsApp Chat – Manual Examination (1)

WhatsApp stores data in more than one place



ZFROMJID	ZPUSHNAME	ZSTANZAID	ZTEXT	ZTOJID
39377561@s.whatsapp.net	Lee Roy	1377221654-18	This is my what's app info. Keep it safe!	17039377561@s.w
39377561@s.whatsapp.net	Lee Roy	1377212884-1	Cool. I will save it in my phone	
39377561@s.whatsapp.net	Lee Roy	1377221903-2		
39377561@s.whatsapp.net	Lee Roy	1377221903-4		
39377561@s.whatsapp.net	Lee Roy	1377212884-2	Do you know this guy?	
		1377296965-12	So glad it's Friday.	17039377561@s.w
		1377296965-15	What time should we meet up tomorrow?	17039377561@s.w
		1377572644-14	Are we still hanging out this week?	17039377561@s.w
		1377572644-17	I'm getting really tired	17039377561@s.w
39377561@s.whatsapp.net	LR BoBkins	1377571477-1	Yes, we are still on. I will call you later with a meeting place.	

ZPHONE	ZDATE	ZPICTUREDATE	ZPICTUREID	ZPICTUREPATH	ZTEXT
39	397457676	398733632.795191	1375761925	Media/Profile/14104197113	Sleeping
45	257126400				Hey there! I am using W
42	257126400	398914454.777896	1377181881	Media/Profile/19412587137	Hey there! I am using W
59	257126400				Hey there! I am using W
40	376873191				...
61	257126400	398914459.5981			Hey there! I am using W

WhatsApp Chat – Manual Examination (2)

WhatsApp – Residual Artifacts

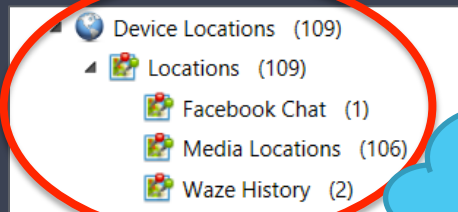
The image displays a file explorer window on the left and a browser window on the right. The file explorer shows a directory structure for a WhatsApp chat with the contact '17039377561@s.whatsapp.net'. The folders are organized as follows:

- Media
 - 17039377561@s.whatsapp.net
 - 6
 - 5
 - 65b95dd65f4ebe5a99d4e11a5d49d7e0.jpg
 - 65b95dd65f4ebe5a99d4e11a5d49d7e0@2x.png
 - A
 - k
 - AkeUKg5RMo2_K-vRkpLR8kwMti72IXhDWwC5f
 - r
 - AroJ2JTS4yQq8jz3A8h3LGEOAlyIXnWLA4CRRp)
 - b
 - e
 - bebefd7b4a2df1ca0842a88c55d462be.jpg
 - bebefd7b4a2df1ca0842a88c55d462be@2x.png
 - Profile
 - 14104197113.thumb
 - 19412587137.thumb
 - Photo.jpg

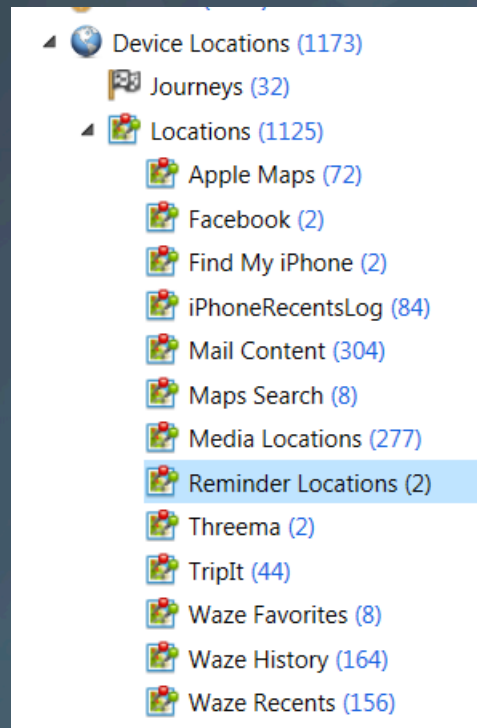
The browser window shows an image of a dog's face. A blue arrow points from the 'bebefd7b4a2df1ca0842a88c55d462be.jpg' file in the file explorer to the image in the browser. Another blue arrow points from the 'Photo.jpg' file in the Profile folder to a separate image of a dog wearing a pink cap. The dog in the separate image is a white dog with floppy ears, wearing a pink baseball cap.

Example 3: Location Artifacts (1)

The tools are getting too much...

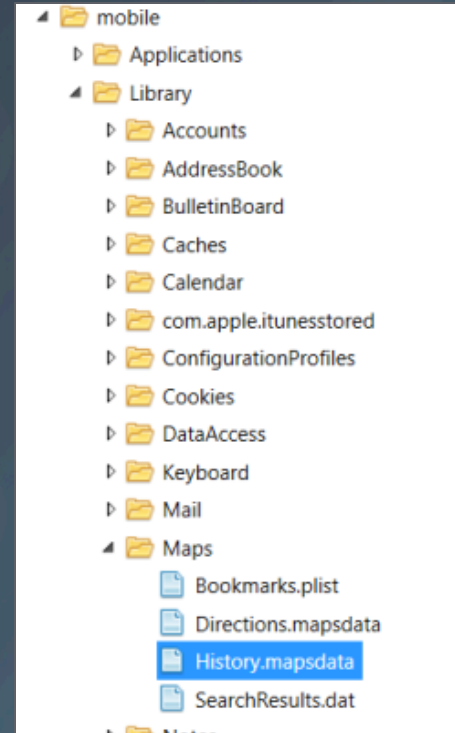
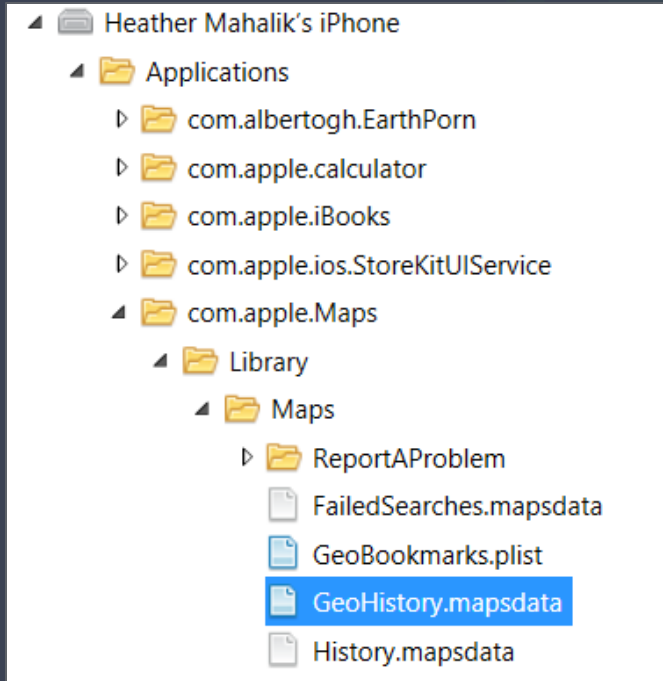


Is that really
the same
device?



Example 3: Location Artifacts (2)

Why data is missed (1)



What location information is missed?

Commonly overlooked artifacts

- Social media geo-tagging
 - Facebook
 - Google+
 - Twitter
 - Etc.
- EXIF data
- Unparsed applications
- When the device thinks or offers something...

<input checked="" type="checkbox"/>	docid	cEntry_id	c1text	c2modified_date
<input checked="" type="checkbox"/>	1	8CC1B93F56974CD594104E20E33FBB61	First tomatoes from my garden!	1373325781
<input checked="" type="checkbox"/>	2	6967D3A0F4054D399E3F937A15B97F5C	Test	1373325858



```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE  
E plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "h  
ttp://www.apple.com/DTDs/PropertyList-1.0.dtd">  
.<plist version="1.0"><dict>.<key>Creation Da  
te</key>.<date>2013-05-08T23:22:35Z</date>.<k  
ey>Entry Text</key>.<string>First tomatoes fro  
m my garden!</string>.<key>Location</key>.<di  
ct>.<key>Administrative Area</key>.<string>  
Virginia</string>.<key>Country</key>.<string>  
United States</string>.<key>Latitude</key>.  
.<real>38.897663774005039</real>.<key>Locali  
ty</key>.<string>Dunn Loring</string>.<key>  
Longitude</key>.<real>-77.240605317128114</re  
al>.<key>Place Name</key>.<string>8521 Mine  
xva Ct</string>.</dict>.<key>Starred</key>.<  
true/>.<key>Time Zone</key>.<string>America/N  
ew York</string>.<key>UUID</key>.<string>8CC1  
B93F56974CD594104E20E33FBB61</string>.<key>Wea  
ther</key>.<dict>.<key>Celsius</key>.<string>  
29</string>.<key>Description</key>.<string>  
Partly Cloudy</string>.<key>Fahrenheit</ke  
y>.<string>84</string>.<key>IconName</key>.  
.<string>partlycloudy.png</string>.</dict>.</dict>  
.</plist>.
```

Recommended steps for success

WARNING - You won't always be successful

- Use tools for Triage
 - Which tool – well, it depends...
- Use more than one tool
 - Acquisition
 - Analysis
- Don't be afraid to do it yourself!
- Always verify your results



Case Scenario

Bullying investigation involving iMessage

Step 1: Triage

What are you looking for?

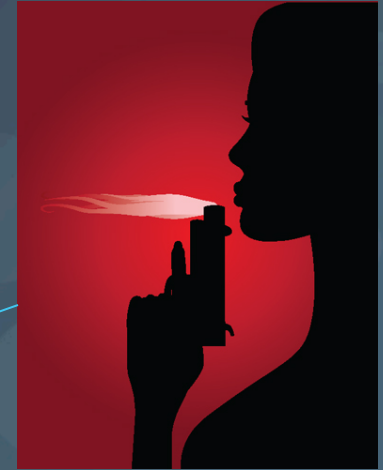
Recovered Artifacts	Count
IEF Refined Results	
Identifiers	709
Chat	
iOS iMessage/SMS/MMS	9826
Mobile	
Calendar Events	157
iOS Call Logs	222
iOS Contacts	507

#	Sender	Recip..	Mess..	Message	Type
8..	Local Us..		12/23/2..	Texting	iMessage
8..	Local Us..		12/23/2..	Breathing	iMessage
8..	+176	Local U..	12/23/2..	Me too!!!	iMessage
8..	Loca		12/23/2..	Wait is this a trick question..	iMessage
8..	+176	Local U..	12/23/2..	No	iMessage
8..	Loca		12/23/2..	👀	iMessage
8..	+176	Local U..	12/23/2..	I was just wondering what..	iMessage
8..	Loca		12/23/2..	The back of my phone fell ..	iMessage
8..	+176	Local U..	12/23/2..	Then you told me	iMessage

Device Content	
Phone Data	
Bluetooth Devices	3 (0)
Calendar	157 (0)
Call Log	184 (64)
Carved Strings	407 (403)
Chats	1281 (1262)
Contacts	1550 (9)
Cookies	1479 (1)
Device Locations	891 (2)
Emails	2435 (0)
Installed Applications	74 (0)
Log Entries	677 (0)
MMS Messages	120 (44)
Notes	50 (10)
Notifications	50 (0)
SMS Messages	4628 (78)
Searched Items	20 (0)
User Accounts	11 (0)
Voicemail	5 (0)
Web Bookmarks	7 (0)
Web History	237 (0)

Step 2: Examine the artifacts

Digging Deeper



Step 3: Report what is correct

Can you defend that artifact?

- Did you validate the finding with the manual database or file?
- Have you verified all discrepancies?
- Are the dates and times being decoded correctly?
- Have you carved for data?
- Have you recovered deleted artifacts?
- Are you prepared to point a finger at someone based upon your work?

Small budget?

- Autopsy
- NowSecure CE
- SSH or ADB
- FTK Imager
- Sanderson SQLite Forensic Toolkit
- Magnet Acquire
- SQLPro for SQLite, Hex editor, plist editor, notepad, etc.

SQLPro for SQLite

Creating a query for Chrome history

The screenshot shows the SQLPro for SQLite interface. The main window displays a SQL query that joins the 'urls', 'keyword_search_terms', and 'visits' tables. The query selects various fields including url_id, url, title, last visit time, visit time, visit duration, and search terms. The results table below shows 25 records with columns for url_id, title, and Last Visit Time.

```
1 select
2 urls.id,
3 urls.url,
4 urls.title,
5 datetime(urls.last_visit_time/1000000 +
6 (strftime('%s','1601-01-01')),'UNIXEPOCH','localtime') AS "Last Visit Time",
7 datetime(visits.visit_time/1000000 +
8 (strftime('%s','1601-01-01')),'UNIXEPOCH','localtime') AS "Visit Time",
9 visits.visit_duration AS "Total visit for all sessions in secs",
10 keyword_search_terms.term AS "search term"
11 from urls
12 left join keyword_search_terms on keyword_search_terms.url_id=urls.id
13 left join visits on visits.url=urls.id
```

url_id	title	Last Visit Time
15	mupoets - Google Search	2015-12-21 17:55:41
16	mupoets - Google Search	2016-02-06 16:42:48
17	mupoets - Google Search	2016-02-06 16:42:48
18	mupoets - Google Search	2016-02-06 16:42:48
19	practical mobile forensics - Google Search	2016-02-06 16:41:26
20	Practical Mobile Forensics	2016-02-06 16:41:46
21	Practical Mobile Forensics	2016-02-06 16:41:46
22	Practical Mobile Forensics	2016-02-06 16:41:46
23	www.amazon.com/gp/aw/c/ref=mw_dp_buy_crt	2016-02-06 16:41:40
24	practical mobile forensics - Google Search	2016-02-06 16:41:47
25	O'Reilly Media - Tech Books, DRM-Free Eboo...	2016-02-06 16:41:52
	Chesterfield Leather Sofa Pottery Barn	2016-03-01 19:22:01

Bottom line...

Jokingly: There are more people in the world with a smartphone than those who have access to a toilet!

Seriously: Most investigations involve a smartphone

- Will you know where to find the data?
- Will you need to rely on your tools?
- Do you have a cert to back you?



NEW Smartphone Analysis Certification

GIAC GASF Certification

- Beta test in progress
- All students who attend FOR585 qualify for discounted, free or bundle-pricing
- Vendor-neutral certification (just like the class)
- Proves you know how to stand behind the artifacts!
- Take FOR585 now and be one of the first with this sought after certification
- FOR585.com/course

References

Some great things are out there waiting for you...

<http://smarterforensics.com/blog/>

<http://www.mac4n6.com/>

FOR585.com/course

<https://www.magnetforensics.com>

<http://www.sandersonforensics.com/forum/content.php>

<https://andriller.com>

<http://www.sleuthkit.org>

<http://www.cellebrite.com>

Thank You

**Heather Mahalikl Principal Forensic Scientist | Oceans Edge, Inc
Senior Instructor and Author | SANS**

heather@smarterforensics.com | @heathermahalik
For585.com/blog