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

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

FOR408
Windows Forensics
GCFE

FOR518
Mac Forensics

FOR526
Memory Forensics In-Depth

FOR585
Advanced Smartphone Forensics GASF

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 ☺

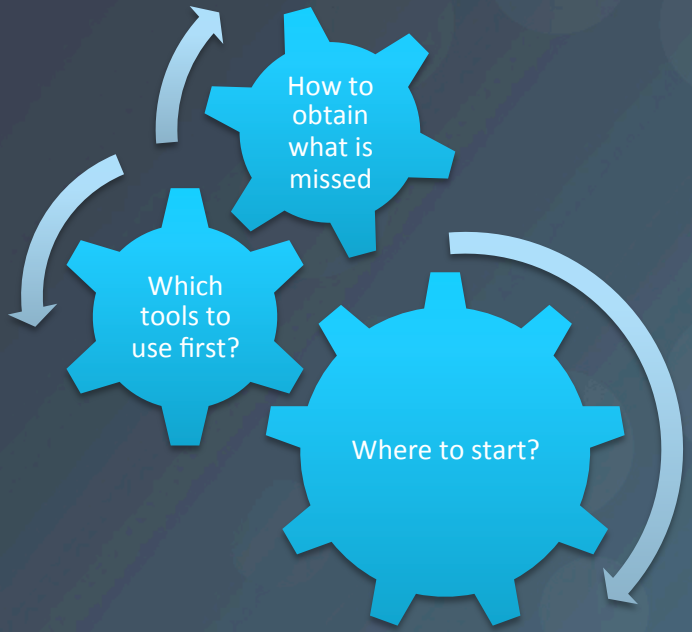
Some considerations

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

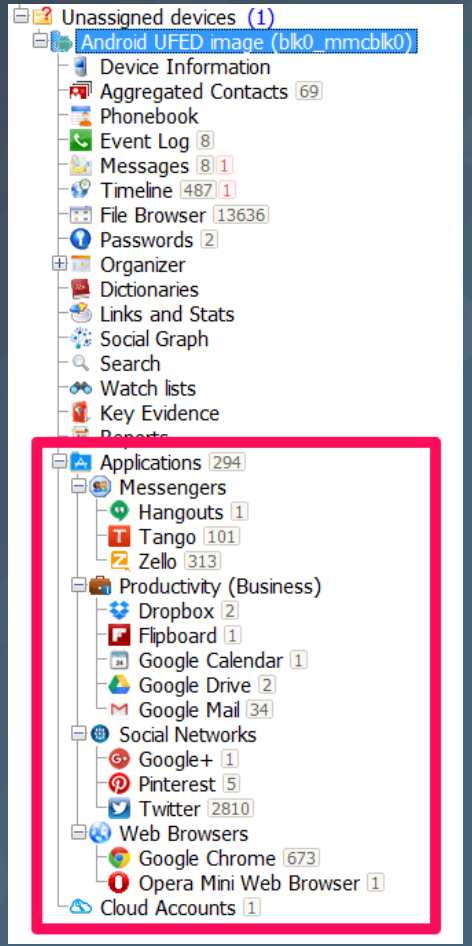
Consider your actions



I paid $$$, it better work

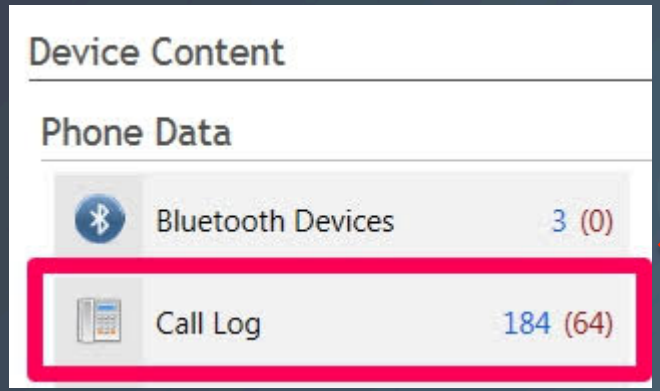
Why the tools fail…

- 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!



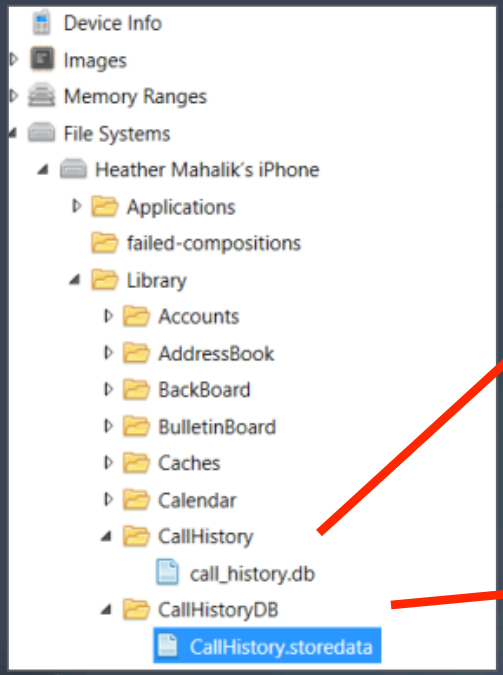
Example 1: Simple communication

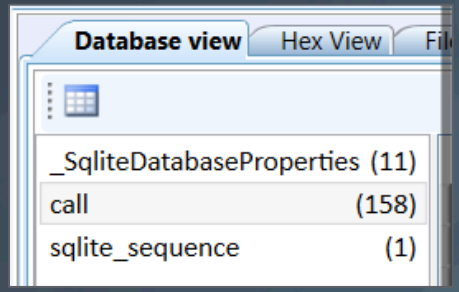
Magnet IEF



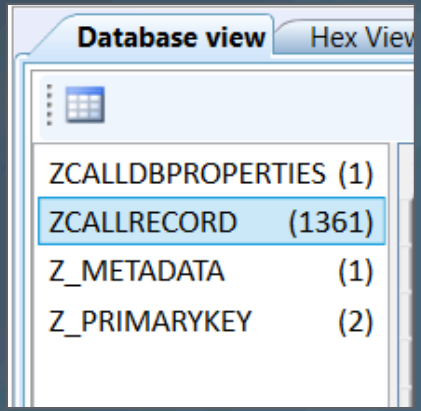
UFED Physical Analyzer

What's really behind that call?





iOS 7



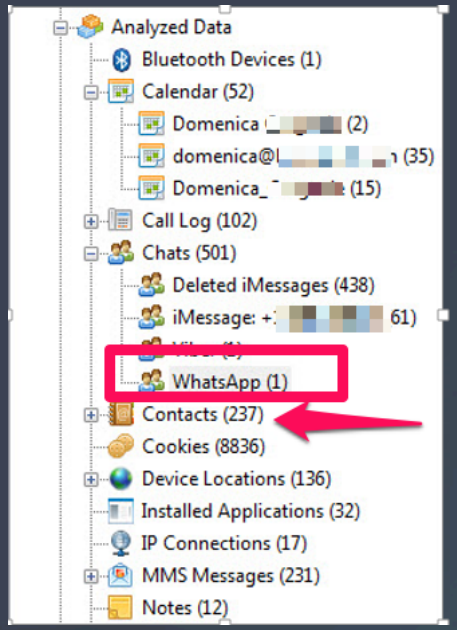
iOS 8 &
iOS 9

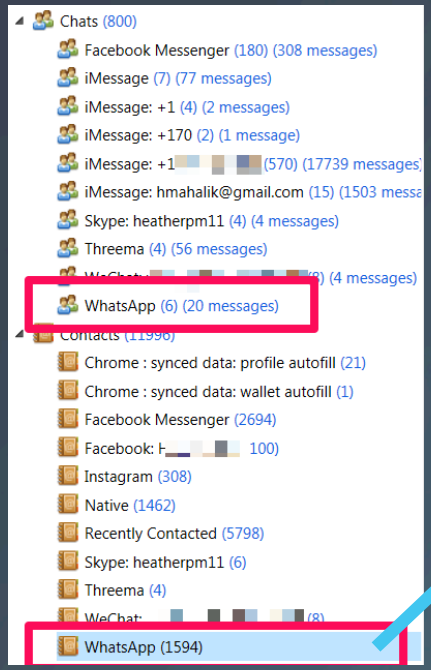
Example 2: Application Data

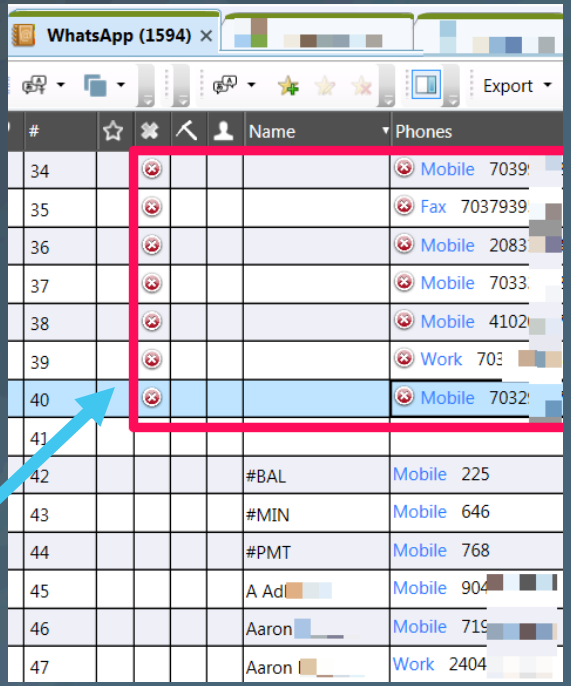
- Yes, I know that they are claiming encryption now
  - Stay tuned…
  - I never trust developer claims
- I love to prove them wrong
- FOR585 teaches you how to do this for almost every app

WhatsApp scenarios

What is Physical Analyzer doing here?

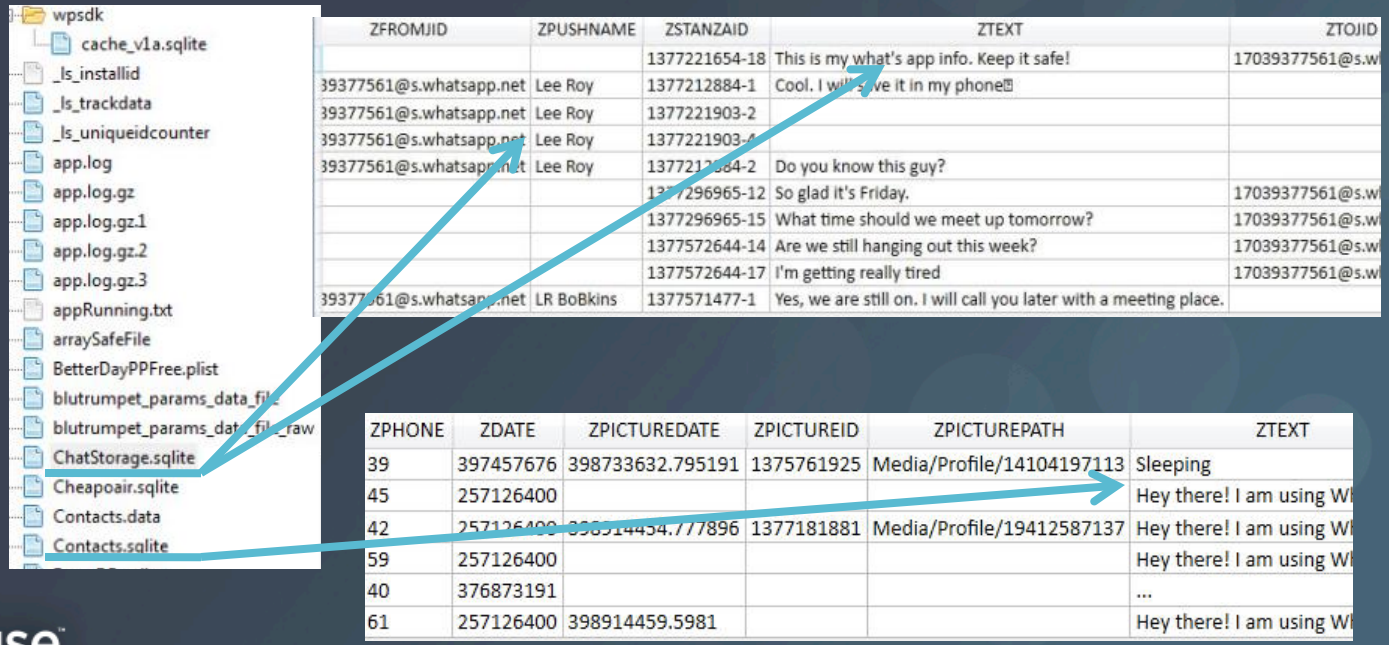






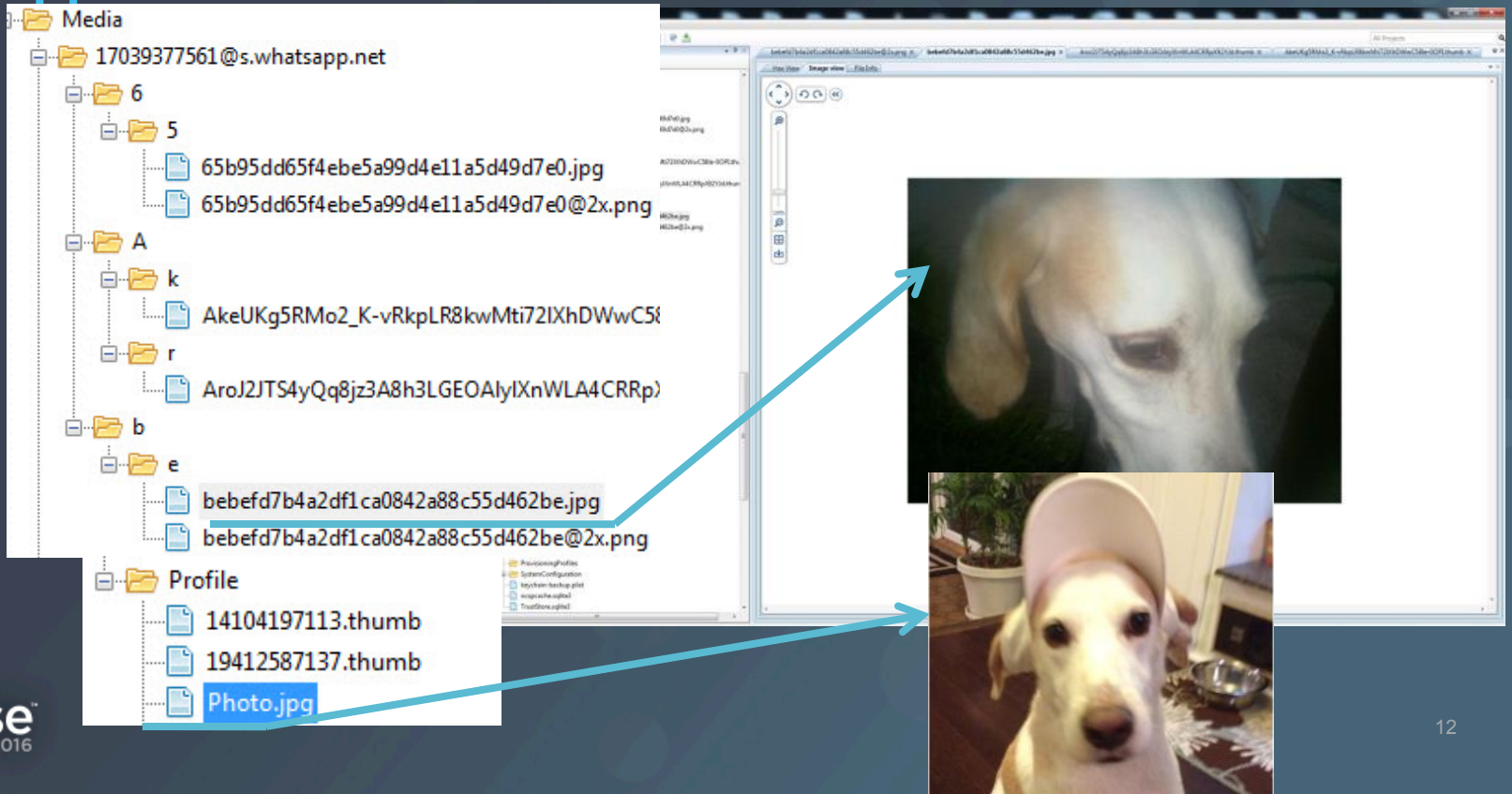
WhatsApp Chat – Manual Examination (1)

WhatsApp stores data in more than one place



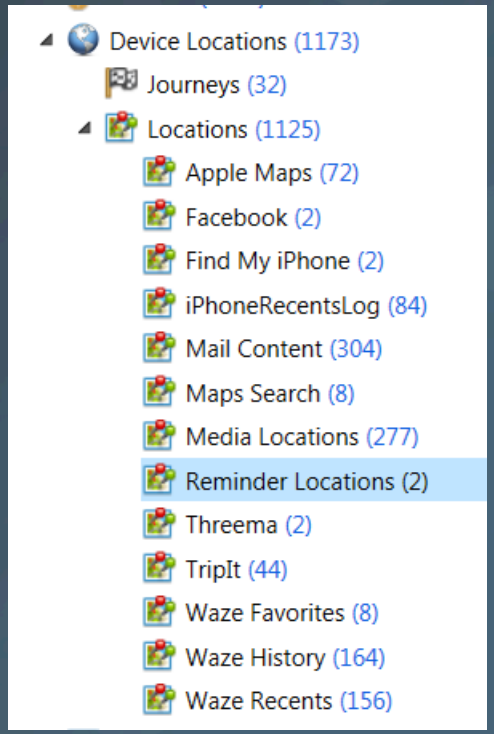
WhatsApp Chat – Manual Examination (2)

WhatsApp – Residual Artifacts



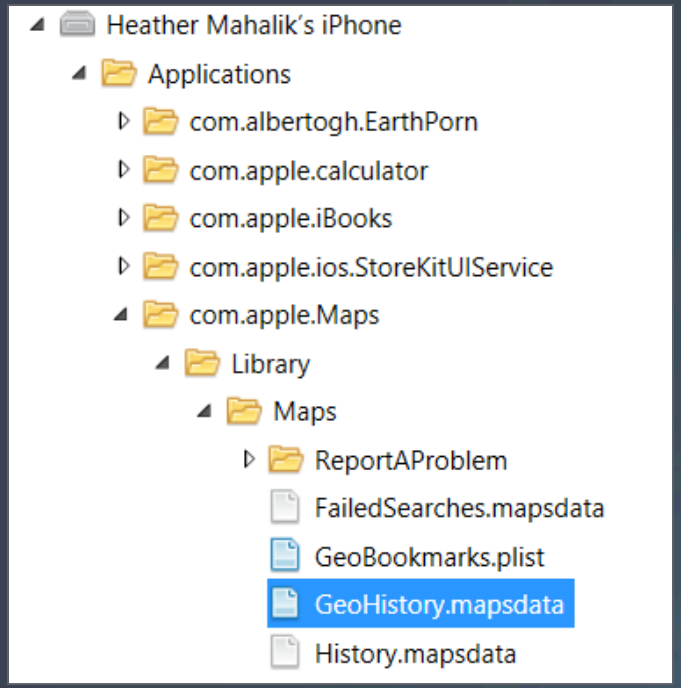
Example 3: Location Artifacts (1)

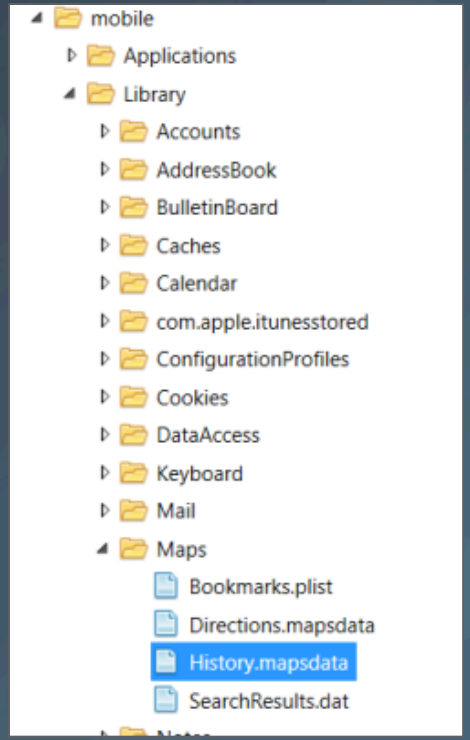
The tools are getting too much…



Example 3: Location Artifacts (2)

Why data is missed (1)





7

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…

docid	c0entry_id	c1text	c2modified_date
1	8CC1B93F56974CD594104E20E33FBB61	First tomatoes from my garden!	1373325781
2	6967D3A0F4054D399E3F937A15B97F5C	Test	1373325858

<?xml version="1.0" encoding="UTF-8"?>.<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">.<plist version="1.0">.<dict>..<key>Creation Date</key>..<date>2013-07-08T23:22:35Z</date>..<key>Entry Text</key>..<string>First tomatoes from my garden!</string>..<key>Location</key>..<dict>...<key>Administrative Area</key>...<string>Virginia</string>...<key>Country</key>...<string>United States</string>...<key>Latitude</key>...<real>38.897663774005039</real>...<key>Locality</key>...<string>Dunn Loring</string>...<key>Longitude</key>...<real>-77.240605317128114</real>...<key>Place Name</key>...<string>8521 Minerva Ct</string>..</dict>..<key>Starred</key>..<true/>..<key>Time Zone</key>..<string>America/New_York</string>..<key>UUID</key>..<string>8CC1B93F56974CD594104E20E33FBB61</string>..<key>Weather</key>..<dict>...<key>Celsius</key>...<string>29</string>...<key>Description</key>...<string>Partly Cloudy</string>...<key>Fahrenheit</key>...<string>84</string>...<key>IconName</key>...<string>pcloudy.png</string>..</dict>.</dict>.</plist>.

Recommended steps for success

WARNING - You won't always be successfull

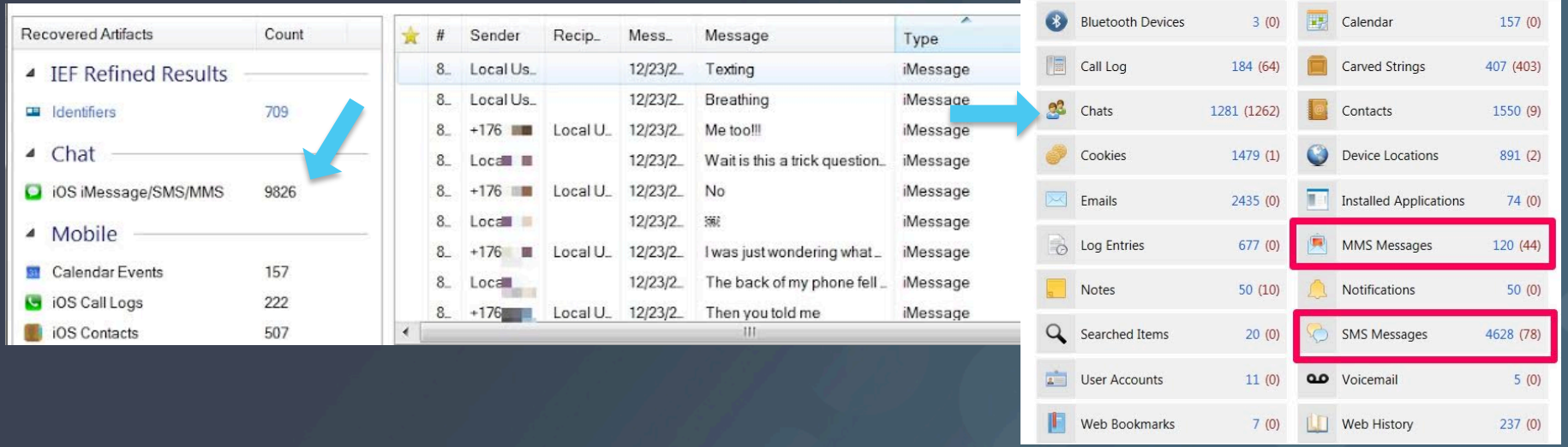
- Use tools for Triage
  - Which tool – well, it depends…
- Use more than one tool
  - Acquisition
  - Analysis
- Don't be afraid to do it yourself!
- Always verify your results

Case Scenario

Bullying investigation involving iMessage

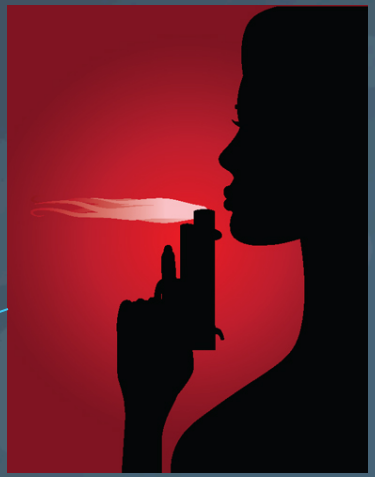
Step 1: Traige

What are you looking for?



Step 2: Examine the artifacts

Digging Deeper

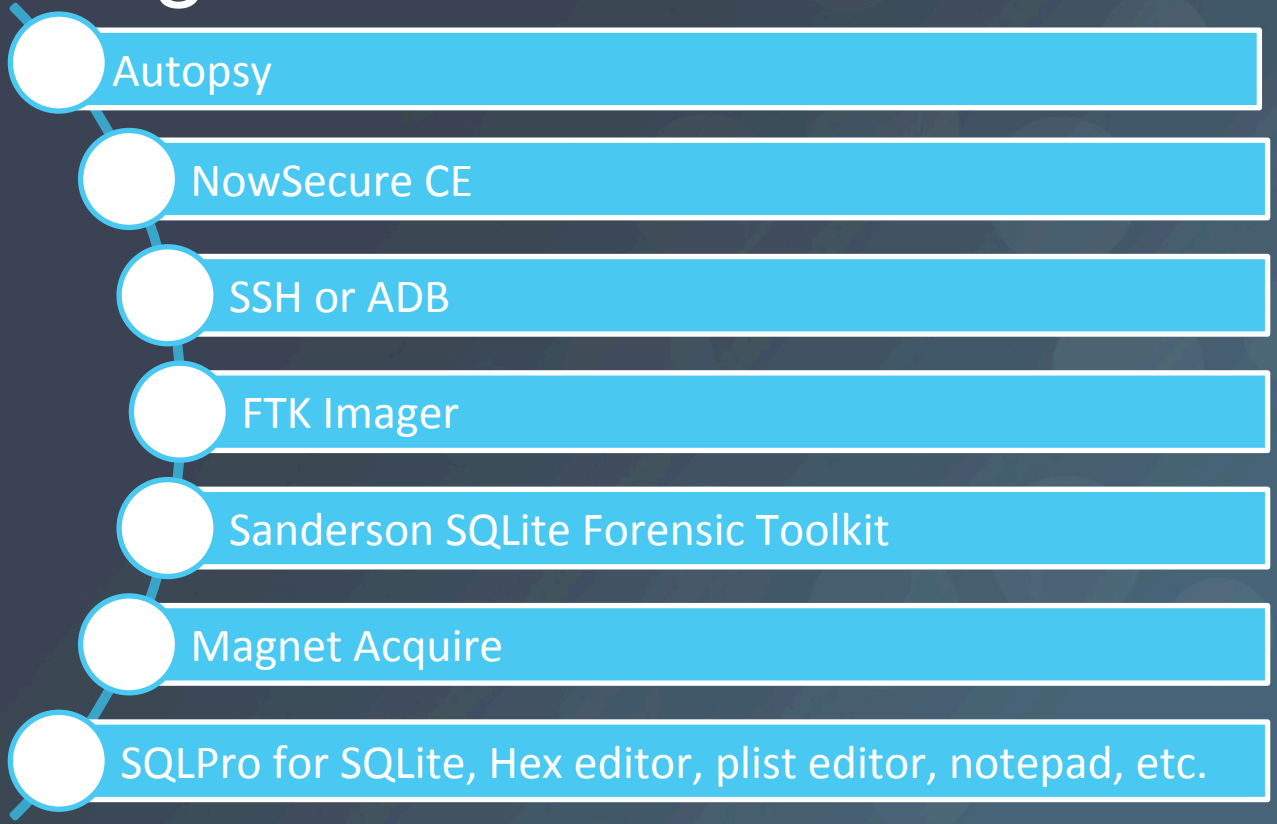


Step 3: Report what is correct

Can you defend that artifact?

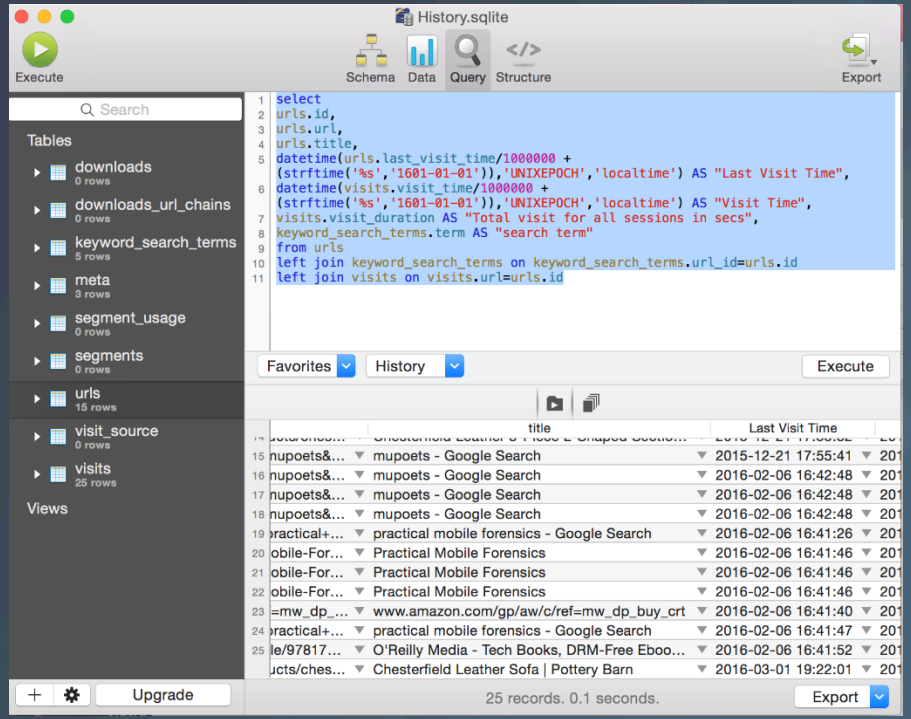
- Did you validate the finding with the manual database or file?
- Have you verified all discrepancies?
- Are the dates and times being decoded correctly?
- Have you carved for data?
- Have you recovered deleted artifacts?
- Are you prepared to point a finger at someone based upon your work?

Small budget?



SQLPro for SQLite

Creating a query for Chrome history



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 l Oceans Edge, Inc
Senior Instructor and Authorl SANS
heather@smarterforensics.com l @heathermahalik
For585.com/blog