



Carney Forensics

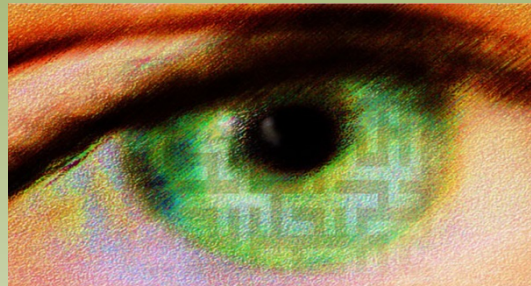
What Digital Evidence Looks Like, and How to Obtain It Professionally

Paralegal Program

Minnesota CLE

John J. Carney, Esq.

September 18, 2018



Carney Forensics

Why Mobile Evidence?

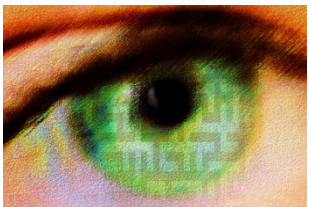
“The reason why the cell phone is important is that you are carrying around a **personal diary** of who you talk to and often what you talked about.” Robert Morgester—California Deputy Attorney General



“The PC may have been personal; a smartphone or tablet, held in your hand rather than perched on your desk, is **almost intimate**, and you can take it **almost anywhere**.”

The
Economist

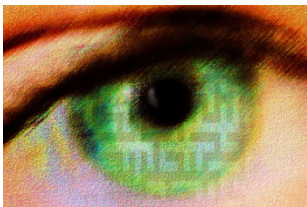
“Your phone is your **alter ego**, an extension of everything we do.”
Eric Schmidt, Chairman,



Why Mobile Evidence?

“My day starts and stops with my phone. I am not my phone, but my phone is a **reflection of me**. It does a pretty good job of taking my life and folding it up into a nice little lightweight, pocket-sized summary. It's almost like I am holding a **copy of my brain** in my hands.”

Derek Smith, Louisville Med-School Student (as reported by CNN)

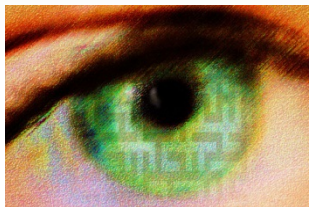


Why Mobile Evidence?

“We must stop kidding ourselves that handhelds don’t hold unique or discoverable information. Look up from your phones and tablets! *They are now the center of our digital lives.*”

Craig Ball, Esq.

Dem Phones, Dem Phones, Dem iPhones
Ball in Your Court



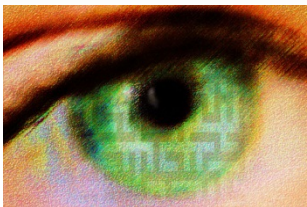
Why Mobile Evidence?

“Phones contain more probative evidence per byte of data than computer hard drives do.”

Gary C. Kessler, Ph.D.

The Year Ahead for Mobile Forensics

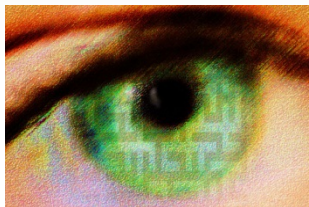
Cellebrite's Panel Predictions for 2013



Discoverable Evidence in Smart Devices



- E-mail and Attachments
- Documents
- Text Messages
- Multi-media Messages
- Instant Messaging and Chat
- Contacts
- Appointments and Calendar
- Voice Calls
- Voice Mail
- Photographs
- Video and Audio Recordings
- Web Browsing History
- Social Media
- Apps



Discoverable Evidence in Smart Devices

Metadata

Smart Phone Device

- Make, Model, Equipment IDs, Phone Number
- Software Versions, Language
- Date, Time, Time Zone, DST

Forensic Tool

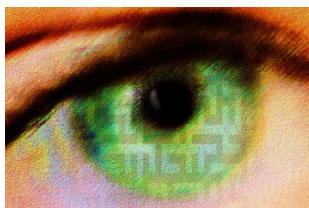
- Identification (Make, Model, Serial Number)
- Software Versions
- Exam Date, Time, Time Zone, DST

Case

- Case Id, Evidence Id, Agency, Examiner

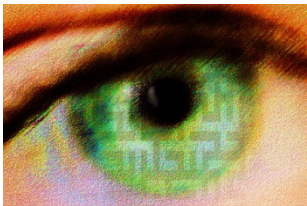
Smart Phone Content

- Hash codes (MD5, SHA1)
- Date and Time Stamps
- Geolocation Information (Geotags)
 - EXIF data from onboard camera snapshots and video
 - Access point data from Wi-Fi logins and activity
 - Reminders



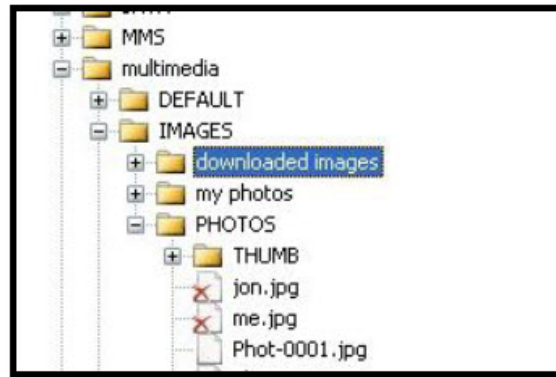
New Approach to Mobile

- New Genre of Automation for Mobile Evidence Acquisition, Analysis, and Reporting
- Fresh, Breakthrough Approach
- 10X More Evidence than Service Providers' CDRs
- Used by Law Enforcement
- Best Practice Today
- Why?
 - Deleted Texts
 - Other Smoking Guns



Recovering Deleted Evidence

- Data Often “*remembered*” though Marked “deleted”
- Increased Complexity and Cost to Recover
- But Can Yield Crucial “*smoking gun*” Evidence



Operating System

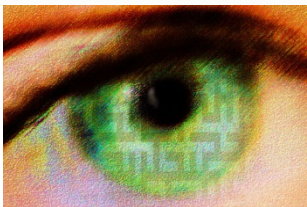
File System

Physical Memory

Live

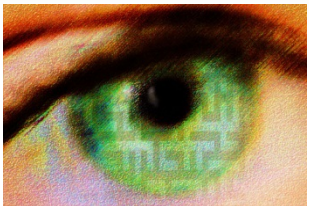
**Deleted (but
“remembered”)**

**Unallocated
 (“forgotten”)**



Challenging Device Solutions

- Phone or Tablet Damage
 - Repairs
 - Water
- Passcode or Pattern Locks
 - Recovery
 - Bypass
 - Cloud
- Pre-Paid “Burner” Phones
 - Bootloaders
 - Chip-off





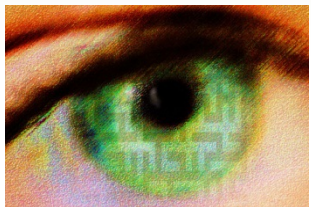
“Apps are nuggets of magic”

Bart Decrem, CEO, Tapulous

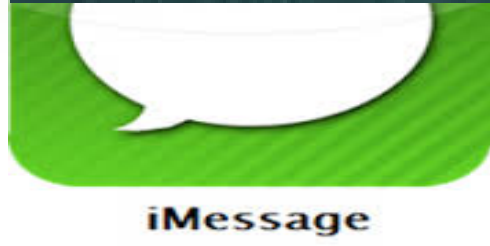
Apps – Categories to Watch



Mobile Messaging – Text Messages Declining
Personal Navigation (GPS) – Where? When?
Payment – Apple Pay, Google Wallet, PayPal
Social Media – Facebook, Instagram, Twitter
Photo Share – iCloud, Google Photos, Dropbox
Document Creation – Office 365, Google Docs
Web Mail – Gmail, Outlook.com, Yahoo
Productivity – Calendars, Notes, To-Do List
Storage/Backup – Google Drive, OneDrive, Box
Games – Candy Crush, Pokémon Go, Fortnite
Spyware – SpouseWare, FlexiSPY



Mobile Messaging Apps



Mobile Messaging Apps



- ***Popular “Text Message Killers”***
- ***Use Internet and App Servers***
- ***Text Free from Costs & Quotas***
- ***Multi-platform for Many Devices***
- ***Global to Bypass Country Limits***
- ***Special and Unique Features***

Mobile Messaging Apps



- ***Attorneys often Unaware of Exploding Use in U.S. and Abroad***
- ***Evidence Recovery Challenging***
- ***Subpoena or Court Order Issues***
- ***Advanced Decoding Required***

Mobile Messaging Apps

Expiration / Retention



Social Media Apps

facebook®

You Tube

flickr™

LinkedIn

twitter

Blogger™

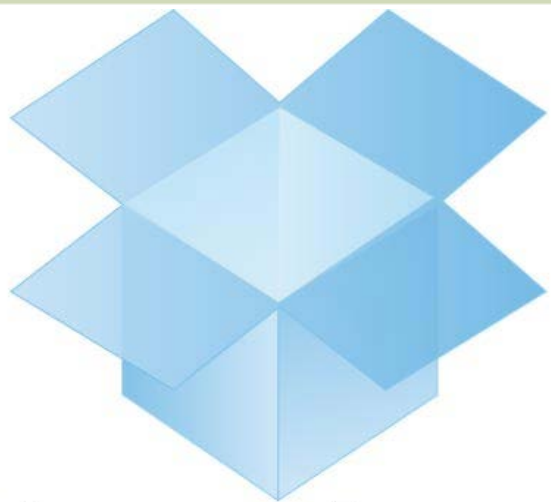


Instagram

foursquare™

Pinterest

Cloud Storage Apps



Dropbox



EVERNOTE

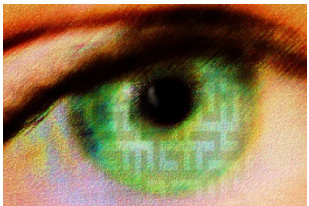


iCloud



iPhone Personal Navigation Apps

- Apple Maps
- Garmin USA
- Magellan RoadMate
- TomTom
- Navigon North America
- Google Maps
- CoPilot Live
- MotionX GPS Drive
- MapQuest
- Scout by TeleNav
- Bing Maps
- Waze – Social GPS

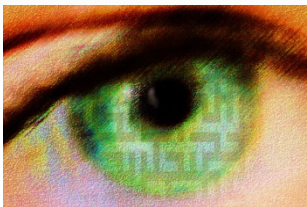


Android Personal Navigation Apps

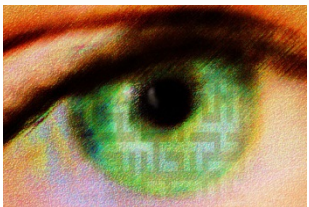
- Google Maps
- Wisepilot
- Navigon North America
- CoPilot Live
- MapQuest
- Scout by TeleNav
- Waze – Social GPS Maps
- GPS Navigation by Sygic
- iGO My Way
- BackCountry Navigator
- MapFactor
- OsmAnd+ Maps & Navigation

Waze

- 48MM Users, +2x Y/Y
- 1B+ Miles Driven per Month w/ Waze Open



Web Mail Apps



Wearables

Technology Cycles Have Tended to Last Ten Years

*Mainframe
Computing*
1960s



*Mini
Computing*
1970s



*Personal
Computing*
1980s



*Desktop Internet
Computing*
1990s



*Mobile Internet
Computing*
2000s



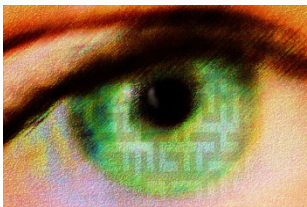
*Wearable /
Everywhere
Computing*
2014+



Others?

Mobile Evidence Collection

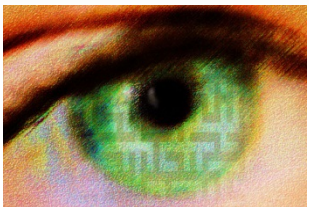
- Highly automated initial scans of device
- Quickly find and collect evidence
- Narrow mobile device selection
- Focus on custodian devices with most compelling evidence
- Cost effective first step after imaging device
- Enables and supports “proportionality”



Mobile Evidence Review

Digital Evidence Viewer Apps

- Apps Support Easy, Visual, Interactive Review
 - Search
 - Bookmarks
 - Create Your Own Reports
- Enables Timely Discovery of Material Mobile Evidence

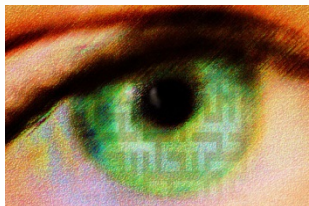


Mobile Viewer App Review

Recovered Artifacts	Items
IEF Refined Results	
Classifieds URLs	109
Dating Sites URLs	1
Facebook URLs	143
Google Analytics First Visit Cookies	29
Google Analytics Referral Cookies	29
Google Analytics Session Cookies	20
Google Analytics URLs	95
Google Searches	612
Social Media URLs	83
Chat	
Android AIM Messages Carved	1
Android LINE Messages Carved	9
Android MMS	21
Android SMS	639
Android Tinder Messages	1

Recovered Artifacts	Items
Documents	
Excel Documents	20
PDF Documents	6
PowerPoint Documents	2
RTF Documents	1
Text Documents	49
Word Documents	4
Email	
Android Gmail	4
Android Yahoo Mail Attachments	1
Media	
AMR Files	15
Carved Video	866
Pictures	104572
Videos	30
Mobile	
Android Call Logs	133
Android Contacts	786

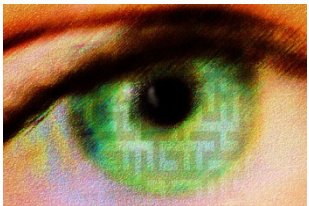
Web Related	
Android Chrome Cookies	23
Android Downloads	57
Android Firefox Bookmarks	6
Browser Activity	439
Chrome Autofill	10
Chrome Cookies	922
Chrome FavIcons	872
Chrome Keyword Search Terms	53
Chrome Logins	1
Chrome Top Sites	11
Chrome Web History	968
Chrome Web Visits	2018
Chrome/360 Safe Browser/Opera Carved We...	1941
Google Analytics First Visit Cookies Carved	335
Google Analytics Referral Cookies Carved	99
Google Analytics Session Cookies Carved	84
Google Analytics URLs Carved	100
Google Maps	58
Google Maps Tiles	1



Mobile e-Discovery is Coming

Mobile Devices are Everywhere & Touch Everything

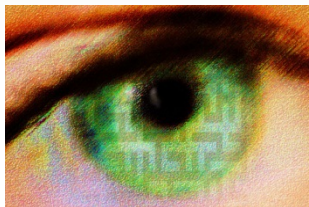
- 41% of Americans Have No Landline
- 66% of Ages 25 to 29 are Wireless
- 71% of Americans Use SmartPhones
- 57% of Americans Use Tablets
- 80% Use SmartPhone within 15 Mins of Wake Up
- Apple Sold 13M New iPhone6S Units in 1st Weekend



Mobile Evidence is Here



- Our Evidence isn't in our desks or file shares
- We must stop kidding ourselves that handhelds don't hold unique or discoverable information
- Phones and tablets are now the center of our digital lives and an ESI goldmine
- We must preserve, collect, review & produce them



Craig Ball's blog post: "Dem Phones, Dem Phones, Dem iPhones", Ball in Your Court, Sept., 2014.

Mobile Evidence Demo



Questions & Answers

Carney Forensics

Cell Phones / Smart Phones

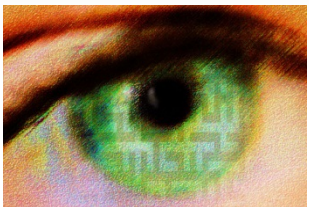
Smart Tablets

Computer Forensics

GPS Devices

Social Media / Email

Mobile App Testing / Litigation Readiness



Sign up for our Newsletter!!

www.carneyforensics.com



Carney Forensics