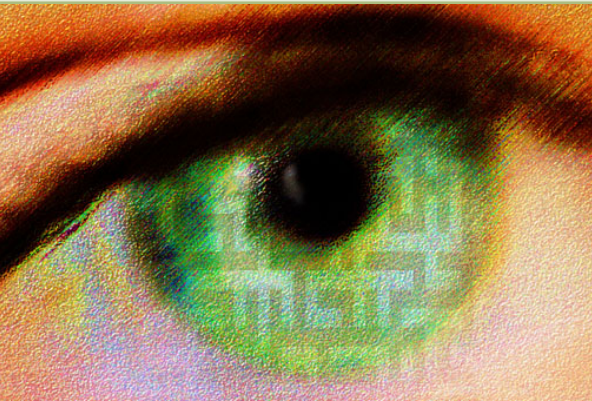# *Who is Carney Forensics?*

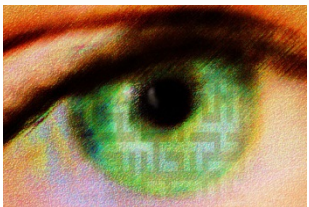## Digital Forensic Experts in Computing Platforms, Mobile Devices, and the Cloud

*John J. Carney, Esq.*

Patti Ray

Topics

- Who Is Carney Forensics?
- Our Value Proposition
- Digital Forensic Services
- Discoverable Evidence
- Mobile Evidence
- Social Media Evidence
- Expert Witness Services

Who is Carney Forensics?

- Founded in 2008 and Located in Minnesota
- Reputation
  - Integrity, Competence, Accuracy, Flexibility, Proportionality, Legally Astute and Licensed
- Work Smart
  - Evidence Strategy – Value Added, Collaboration
  - Automation – Invested Heavily in World Class, Cutting Edge Tools
- Team Approach
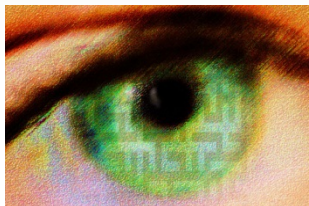 - Examiners and Forensic Automation Vendors
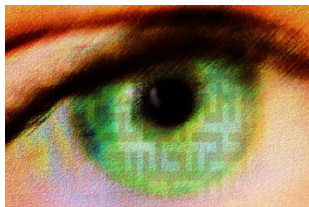
Who is Carney Forensics?

Certified Digital Forensic Experts
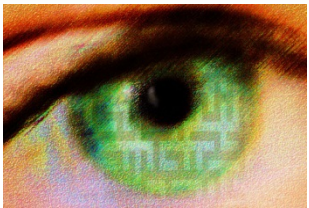
- Computer Forensics
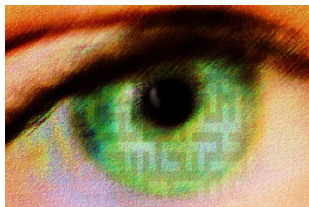

- Mobile Device Forensics

Value Proposition - Offering

- For attorneys and investigators in private practice and government service
- Who need persuasive digital evidence with written or courtroom testimony
- Our expert digital forensic services recover relevant, material evidence from computing platforms, mobile devices, and the Cloud
- To win or advantageously settle cases and close challenging investigations

Value Proposition - Positioning

- Unlike traditional, local computer forensic examiners or expensive, national consulting companies

- Our cutting-edge digital forensic services target today's computing platforms, mobile devices and cloud-based data

- Delivered cost effectively using world class tools and methods by a state and federally licensed attorney and certified forensic examiners

- With decades of professional technology experience with proven results in federal and state courts

Digital Forensic Services

- Evidence Strategy Consulting
  - Meet and Confer
  - Request for Production
- Computer Forensics
- Mobile Device Forensics
- Cloud Forensics
- Document Forensics
- E-mail Forensics
- e-Discovery Collections
- Expert Witness Testimony
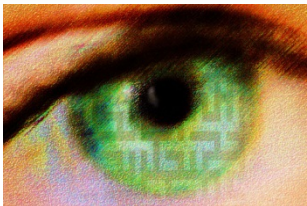
Evidence Collections

- Desktops, Laptops, Servers
  - Documents, File Shares, E-mail
  - SATA, IDE, USB, RAID, SSD
- Initial Scans Yield Rapid Evidence Discovery
  - Browser-based evidence like web mail, social media, messaging and chat, case-related web sites
  - Traditional, resident e-mail like Outlook & Thunderbird
  - iPhone and iPad backups and archives
  - Previously connected USB devices
 - Media evidence like photo, video, audio
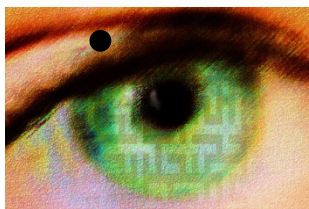
Initial Scan Evidence

Recovered Artifacts	Items
Email	
Gmail Fragments	238
Gmail Webmail	247
Media	
Facebook Pictures	15
Pictures	1160596
Videos	1652
Web Video Fragments	7
Mobile Backups	
iOS Address Book Backup	51
iOS Call Logs Backup	10
iOS Notes Backup	1
Peer to Peer	
Ares Search Keywords	9
Social Networking	
Facebook Chat	2
Facebook Pages	1540
Facebook Status Updates...	164

Recovered Artifacts	Items
Classifieds URLs	687
Cloud Services URLs	4
Dating Sites URLs	342
Facebook URLs	3869
Google Maps Queries	77
Parsed Search Queries	2197
Rebuilt Webpages	67
Social Media URLs	1193
Torrent URLs	42
Web Chat URLs	48
Chat	
QQ	2043
Skype Accounts - johnjcar...	1
Skype Calls - johnjcarney9	11
Skype Carved Messages	2
Skype Chat Messages - jo...	87
Skype Chatsync Message...	6
Skype Contacts - johnjcar...	7
Skype Voicemails - johnjc...	1
Cloud	
Google Drive	1

| Recovered Artifacts	Items
Web Related	
Browser Activity	8529
Chrome Autofill	27
Chrome Bookmarks	80
Chrome Cache Records	1211
Chrome Cookies	628
Chrome Favicons	185
Chrome History Index	139
Chrome Keyword Search ...	5
Chrome Logins	2
Chrome Top Sites	18
Chrome Web History	544
Chrome/360 Safe Browser ...	1065
Craigslist Ads	202
Firefox Bookmarks	451
Firefox Carved FormHistory	6
Firefox Carved Web History	183
Firefox Cookies	1024
Firefox Downloads	100
Firefox Favicons	60
Firefox FormHistory	108
Firefox SessionStore Artif...	211
Google Maps	1774
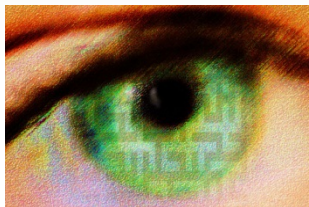
Proportionality

- Highly automated initial scans quickly find and understand "low hanging fruit" in challenging cases with several computers

- Narrow computer selection down and focus on the devices with the most compelling evidence

- Cost effective first step after imaging for discovery prior to moving on to costly manual analysis

- Enables and supports "proportionality"

Evidence Review

- Evidence Viewer Apps Available at No Charge
- Easy to Use and Discover Material Evidence
- Downloaded Online and User Installed
- Evidence Data Set Downloaded Online
- Apps Support High Touch, Interactive Evidence Search and Review
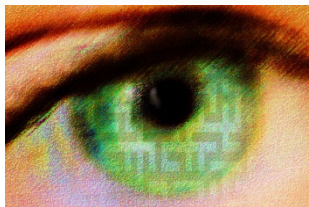- We Offer Training On Site or Remotely
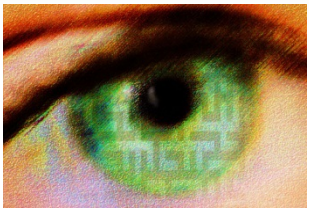
Why Mobile Evidence?

"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

Content

Phone Address Book (Contacts)
Appointments and Calendar
Dialed, Received, and Missed Call Logs
Electronic Mail and Attachments
Electronic Documents
Text Messages (SMS)
Multi-media Messages (MMS)
Instant Messaging and Chat
Dictionary (Keylogger)
Photographs
Audio and Video Recordings
Voice Mail and Messages
Web Browsing History, Bookmarks, Cookies
Social Media (Facebook, Twitter, LinkedIn)
Apps and App Data
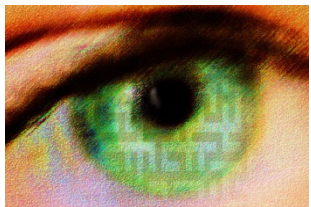
Discoverable Evidence in Smart Devices

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
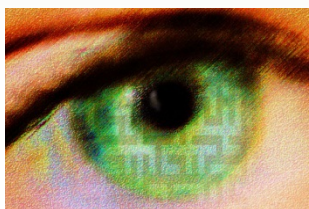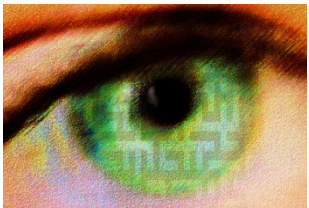
Mobile Messaging Apps

Mobile Messaging Apps
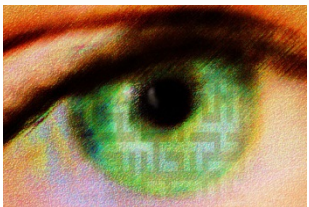
Expiration / Retention

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 Practices Today
- Basis for Mobile Collections
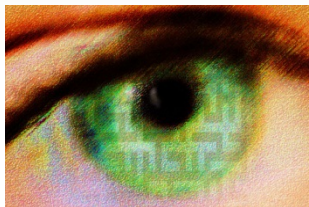- And "Mobile e-Discovery"

Solutions for Special Situations

- Phone or Tablet Damage
  - Best of Breed Repair Service
  - Chip-off
- Passcode or Pattern Locks
  - Recovery
  - Bypass
  - JTAG
- Pre-Paid "Burner" Phones
  - Bootloaders
  - Chip-off
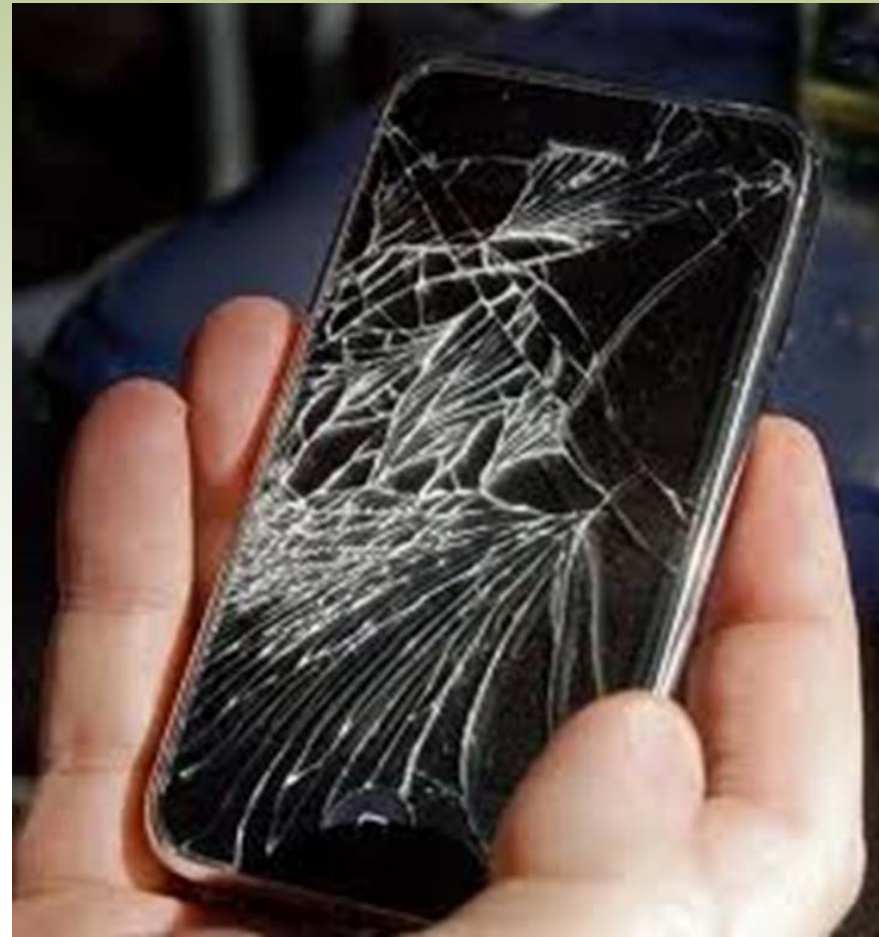
Web Mail Apps

Popular Social Media

Social Media:
# What ESI Can We Get For Review?

Content
- Friends, Friends of Friends, Connections, Followers, etc.
- Status Updates, Relationship Status
- E-mail, Chat, Text Messages, Friend Requests, Pokes
- Timeline (Profile) – Name, Picture, Gender, Contact, Birthday
- Wall, Posts, Comments, Tags
- Likes, Reads, Views, Listens, etc.
- Networks, Groups, Events
- Photos, Videos, Audio, Music, Tags
- Apps, App Data, Games

Pushed Content
- E-mail Notifications with Metadata
- RSS Feeds with Metadata

Metadata

Site Names, Uniform Resource Locators (URLs)
Date/Time Stamps, Geolocation Information (Check-ins)
IP Logs, Login/Logout Logs
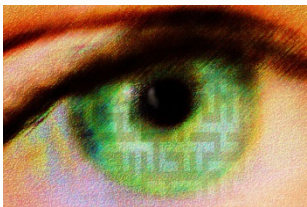
Integration Challenges

Integrate Computer, Mobile, and Cloud Evidence with Litigation Support and Document Review Tools

Nontraditional Data Types
- Multimedia – Voice, Audio, Video, Photo
- GPS – Latitude, Longitude, Elevation, Velocity
- Apps – Infinite Variety, Multi-platform, Custom Data

Computer / Mobile / Cloud Tools
- Full Text Search – All Devices in Case
- Connected Documents Moved or Copied Across Devices / Cloud
- Record bookmarks, Tags, Comments
- Reports / Export / Viewers
- Load Files to Litigation Support and Document Review Tools
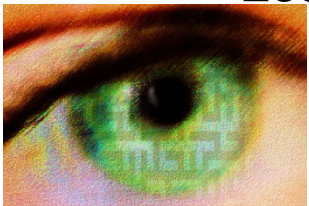
Expert Witness Services

- Affidavit and Narrative Report Drafting
- Deposition Testimony
- Trial Prep to include:
  - Consult on theory of case & evidence strategy
  - Develop voir dire for qualifying digital forensic tools
  - Draft direct and cross examinations of digital expert
  - Develop demonstrative exhibit(s) for show & tell
  - Rehearse direct and cross exams with attorney
- Courtroom Testimony
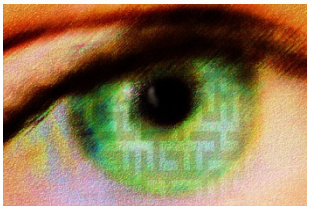
Questions & Answers

Carney Forensics

Cell Phones / Smart Phones / Smart Tablets

Computer Forensics

Mobile e-Discovery

Social Media / Email

Mobile App Litigation Readiness

Expert Witness Testimony

Sign up for our Newsletter!!

www.carneyforensics.com