Computer Forensics and Collections Industry Insight

by

Peter Coons, SVP, Computer Forensics and Collections

Tom Groom, VP, Discovery Engineering

Table of Contents

iPhone Forensic Capture and Analysis Results

by Peter Coons

Recently Apple claimed that 80% of the Fortune 100 are currently assessing iPhone's for corporate use (50% are assessing the iPad). Will the iPhone usurp BB as the Smartphone leader in the corporate world? Apple products seem to be everywhere already (I saw the iPod Touch highlighted in a "Toys R Us" Black Friday advertisement). I don't consider myself a MAC person yet I own 5 iPods, an iPhone, an iPad and a Mac Book. OK. Wow. Maybe I am a MAC person. Is there a 12 step program for that affliction?

Regardless of who the leader is today or tomorrow it's a fact that Smartphones and tablets will continue to be used and may even replace the traditional desktop or laptop for everyday business computing needs. My iPad has replaced my traditional pencil and notepad. I use it for most everything in my daily business activities. This is a potential problem or boon for attorneys and eDiscovery practitioners.

D4 recently invested in some wonderful new hardware that allows for the capture of iPhones, iPads, and 3000 other Smartphones and tablets! I thought I would take an old iPhone we had laying around office and give it a test run. Results are below.

Phone Stats: iPhone 3G 8 GB; Software version 3.1.2

Use: Used for personal and business purposes for about 12 months; heavy texting; pictures of family; heaving web browsing; multiple applications installed

Two Modes Tested (both modes are logical captures and not capturing data at physical device level):

Basic Capture ("BC") - Includes captures of Pictures, SMS (texts), call logs, videos, phone book, audio and music files

File System Capture ("FS") - Captures files stored on the iPhone file system - think MAC file system

Scenario 1: Basic Capture - No deletions performed. Phone imaged as is.

Scenario 2: BC after manual deletion - I deleted all the pictures, call logs, SMS, videos, and contacts. I did not delete music files.

Scenario 3: BC after system reset - I used the iTunes application in Windows to reset the device to factory settings. When undertaking this action I was forced to upgrade the iPhone to version 4.1.2 OS.

Scenario 4: File System capture after manual deletion - I captured the file system after

manually deleting pictures, call logs, SMS, videos, and contacts. I did not delete music files.

Scenario 5: FS capture after system reset - I used the iTunes application in Windows to reset the device to factory settings. When undertaking this action I was forced to upgrade the iPhone to version 4.1.2 OS.

Scenario 1 Findings:

Basic Capture - No deletions performed. Phone imaged as is.

Item	Basic Capture (BC)
Call Log	**22 incoming; 55 outgoing; 23 missed**
SMS	**4491**
Email	NA
Contacts	NA
Calendar	NA
Notes	NA
Pictures	**652**
Songs	**5**
Web History	NA
Bookmarks	NA
Cookies	NA
Kayak Travel	NA
Google Maps	NA
Passwords	NA
Plists	NA
Video	**1**
Phone Information	**YES**
Podcasts	NA
Network Info	**YES**
Bluetooth Info	**YES**
YouTube	NA
HTML	NA
GPS	NA
Google Mobile App	NA
Safari History	NA

Capture reported on all items I expected. Nothing shocking.

Scenario 2 Findings:

BC after manual deletion - I deleted all the pictures, call logs, SMS, videos, and contacts. I did not delete music files.

Item	BC after manual Delete
Call Log	0
SMS	**52**
Email	NA
Contacts	NA
Calendar	NA
Notes	NA
Pictures	**10**
Songs	**5**
Web History	NA
Bookmarks	NA
Cookies	NA
Kayak Travel	NA
Google Maps	NA
Passwords	NA
Plists	NA
Video	**1**
Phone Information	**YES**
Podcasts	NA
Network Info	**YES**
Bluetooth Info	**YES**
YouTube	NA
HTML	NA
GPS	NA
Google Mobile App	NA
Safari History	NA

The pictures that remained after the manual deletion were actually album art from iPod. I did not delete the music when I perfomed manual deletions. I was surprised to find 52 text messages remaining. When the texting app was viewed on the iPhone none were viewable. From a forensics and electronic discovery this is interesting as items can be recovered even after manual deletions. Other than the texts that were recovered I was not shocked by the results.

Scenario 3 Findings:

BC after system reset - I used the iTunes application in Windows to reset the device to factory settings. When undertaking this action I was forced to upgrade the iPhone to version 4.1.2 OS.

Item	BC after system reset
Call Log	0
SMS	0
Email	NA
Contacts	NA
Calendar	NA
Notes	NA
Pictures	0
Songs	0
Web History	NA
Bookmarks	NA
Cookies	NA
Kayak Travel	NA
Google Maps	NA
Passwords	NA
Plists	NA
Video	0
Phone Information	YES
Podcasts	NA
Network Info	YES
Bluetooth Info	YES
YouTube	NA
HTML	NA
GPS	NA
Google Mobile App	NA
Safari History	NA

The only information available was the phone information, which is most likely from the SIM card. I am not surprised by the results as a full system restore would purge the items purported to be captured by the Basic Capture.

Scenario 4 Findings:

File System capture after manual deletion - I captured the file system after manually deleting pictures, call logs, SMS, videos, and contacts. I did not delete music files.

Item	File System dump after manual delete
Call Log	0
SMS	52
Email	0
Contacts	210; 26 deleted; 236 total
Calendar	YES
Notes	YES in full
Pictures	264
Songs	20
Web History	YES
Bookmarks	YES
Cookies	YES
Kayak Travel	Evidence it was installed
Google Maps	YES; history
Passwords	None I could Find
Plists	Many
Video	1
Phone Information	YES
Podcasts	None I could find
Network Info	YES
Bluetooth Info	YES
YouTube	YES
HTML	YES
GPS	YES, info from Maps App, previous searches and destinations
Google Mobile App	Search History
Safari History	Search History

Jackpot! Even after the manual deletion of what a typical user would be able to delete through the iPhone interface I was able to recover a lot of great information. A cornucopia of forensics goodies including browsing history, deleted contacts, the same 52 text messages as in scenario 2, Google Maps information, calendar entries, notes and much more.

Scenario 5 Findings:

FS capture after system reset - I used the iTunes application in Windows to reset the device to factory settings. When undertaking this action I was forced to upgrade the iPhone to version 4.1.2 OS.

Item	5. FS dump after system reset
Call Log	0
SMS	0
Email	0
Contacts	0
Calendar	0
Notes	0
Pictures	0
Songs	0
Web History	0
Bookmarks	0
Cookies	0
Kayak Travel	0
Google Maps	0
Passwords	0
Plists	0
Video	0
Phone Information	YES
Podcasts	0
Network Info	0
Bluetooth Info	0
YouTube	0
HTML	0
GPS	0
Google Mobile App	0
Safari History	0

Blanked! I was somewhat surprised of what a good job the system restore did. The only information was the basic phone information (probably from SIM).

Conclusion: Without a full system restore there is plenty of useful information to be had on the iPhone for forensic analysis and traditional eDiscovery. If you plan on selling your old iPhone make sure you do a full system wipe through iTunes. That's still no guarantee traces of data won't be left behind but it's better than a manual deletion of texts, call logs, etc. In addition to the phone itself, a wealth of information would likely be available on the PC or MAC used to manage the iPhone. That's a different article and test!

Final Thoughts: I wish I was able to perform a full forensic physical capture to grab deleted space. With that type of capture I would expect to find deleted photos and other information even after a fully system reset through iTunes. There are a few methods to accomplish this task and that will be the next test.

Attorneys dealing with eDiscovery preservation issues must realize the importance of identifying evidence that may exist outside traditional email boxes and server shares. The world is changing!

In January of 2011, there were roughly 60,000 apps available for the iPad on iTunes.

Even though it's not technically a computer, Apple's latest sales figures show that it has captured about 7% of what used to be the global "PC" market.

Over 10 Billion apps have been downloaded on iTunes! In case you are wondering, the 10 billionth download was the "Paper Glider" app.

I purchased my iPad in May of 2010, and haven't put it down since. It has replaced my laptop when I travel, my paper notebook in meetings, and changed the way I buy and read books. I use apps such as LogMeIn, Whistle, Dropbox, and the built in e-mail capabilities to keep me connected to the office. You may have read some legal blogs and articles about lawyers and law firms adopting the iPad. Well, it's happening all over and there is no disputing that the iPad, and devices like it, are changing computing habits.

I purchased the data plan for $30 a month and as long as there is a cell signal I can access the Internet. I haven't synced my iPad to my computer in over a month. I have used it extensively in that time and I suspect that a lot of data (evidence) resides on my iPad that doesn't exist anywhere else. So naturally, as a computer forensics and eDiscovery practitioner, I wanted to know what I could extract from my iPad with some forensic tools. I uncovered some interesting information.

After imaging the iPad I used Access Data's FTK 3.2 to view the data. FTK does an excellent job of parsing property lists, commonly referred to as plist files. In the MAC Operating System property list files are often used to store a user's settings.

As expected, I was able to recover standard items like contact and calendar items. What really caught my eye was the extensive information captured about the apps on my iPad.

Some Interesting Finds:

- Safari Browser history
- Safari Bookmarks
- Safari search history (what I typed into Google)
- Google Map searches (Hotels I searched for in NYC and other directions)
- Information about my personal GMAIL account
- Listing of folders from my corporate Exchange account
- Cookies indicating websites I visited
- Names of documents stored in my Dropbox account

- Photos from websites visited
- Books that I downloaded from Kindle
- My iTunes Apple ID
- LinkedIn connections with contact information
- Entire spreadsheets, PDF's, and documents stored in my GoodReader app
- Craigslist app information about items I had searched for and specific locations/cities
- Random text that I typed in e-mails and other apps (revealed a lot of personal and business information)
- Login name and password for an app that I use daily for business!
- Phone numbers that I called with the Whistle app (VOIP phone app for iPad)

Do you think that any of this information would be useful in the eDiscovery or computer forensics world? I do.

There was more information available than I had time to go through. The amount of information blew me away and the fact that an app stored my login name and password in plain text was very disconcerting. Although the iPad is not a phone like it's cousin the iPhone, the Whistle app had all the numbers I called. The random text that I found in the keyboard directory was revealing as well. There were snippets of emails, notes, and other entries going back to May 2010. My browser history also went back to May 2010. The iPad is a virtual treasure trove when it comes to computer forensic investigations and electronic discovery. And as I stated in the beginning, I haven't synced my iPad in well over a month so there is definitely information on it that exists nowhere else.

The one thing that shocked me the most was that I found data in what appeared to be the slack space of a file. A picture I examined contained an e-mail address for a friend in an area after the file footer. This picture was taken by me while I was on vacation and it was not of my friend nor did I e-mail it to my friend. What a great forensic find.

Are you considering iPads and other devices like it when making ESI requests? Are you requesting your client or employees preserve data stored on iPads when a legal hold is issued? Are you discussing iPads at 26(f) meet and confers? NO? Why not?

Now please excuse me while I go delete the App that is storing my password in plain text.

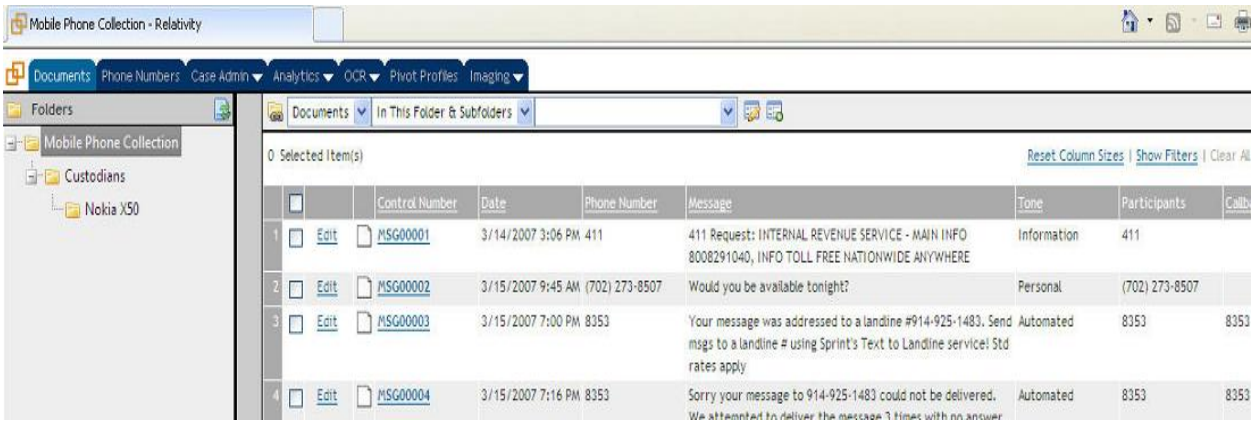
Technical Tip –Text Message Review

by Tom Groom

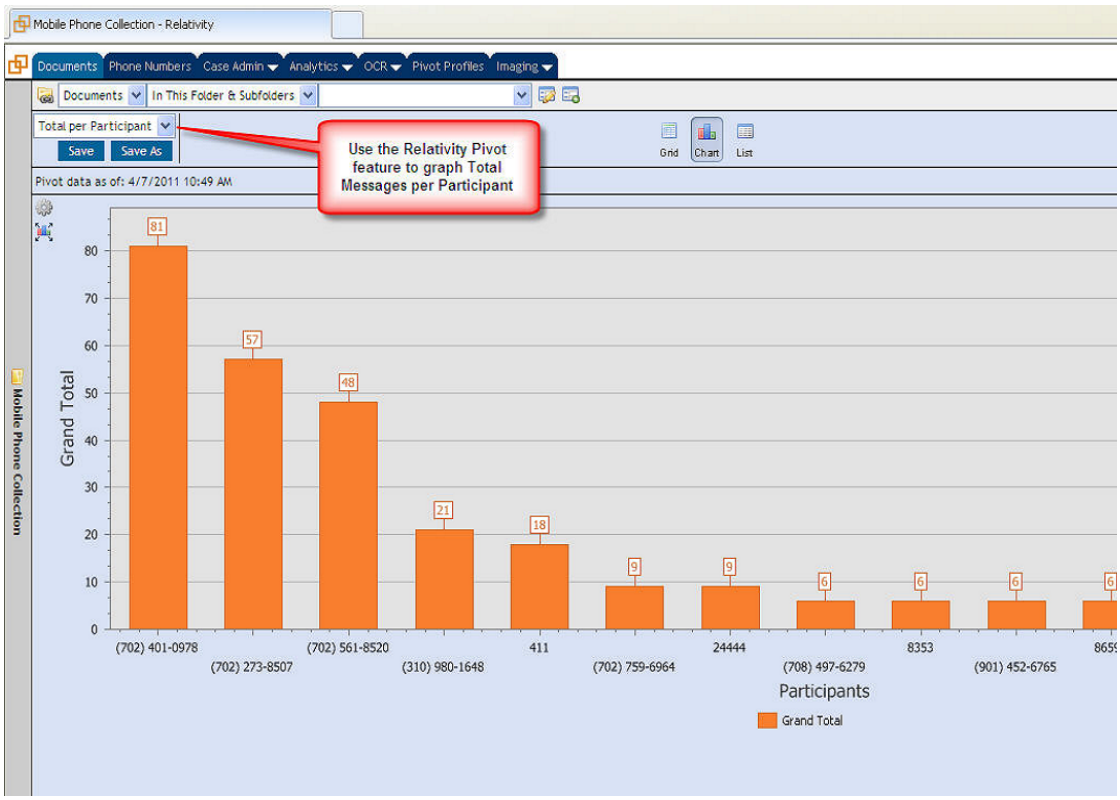
There are very few people today who don't thumb text messages on their phones. We tend to treat text messages as if they can't be retrieved once we hit send. "Nobody will find this" one may tell themselves. Oh really? What happens when opposing counsel requests text messages to be included from one of your key custodians? At first you object in that your client's text messages are not "reasonably accessible" but that argument isn't as easy to win as it used to be. Once you've accepted the fact that review of the text messages is going to happen, the question hits you -- "How can text messages most efficiently be reviewed?"

The answer may surprise you. Think of each individual text message as a record (like an email or Word document). If properly collected, each text message record has metadata associated with it that can be used to stitch together the bigger story. Text message timeframes are normally measured in seconds (vs. days as with email) so they are often reviewed in a separate database than email or scanned documents. The key for efficient text message review is to have a common "date and time" field to sort the messages in order to create a conversation. This is especially true if messages for more than one custodian are being reviewed. Another key is to leverage relational fields that can be used to associate phone numbers to participants as well as, to enable "group and pivot" reports between phones, participants, timeframes and even conversational tone.

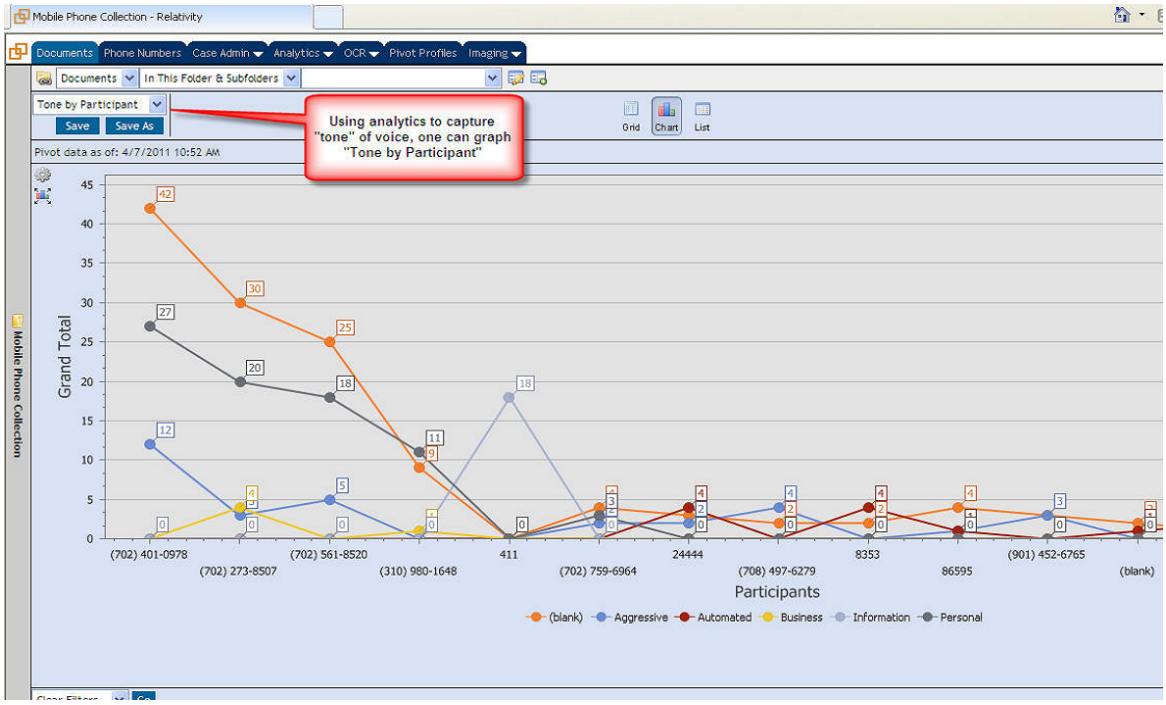
Relativity hosted by D4 provides such a platform as shown in the screen shots below. Text messages from three different phones were placed into this database. From here the reviewer can choose which phones to include as well as which participants to include in the query. Sorting by date and time will piece together the text messages between parties which can help establish intent and/or reveal interesting behavior.



Using the new "Pivot" feature in the Relativity 6.x system, one can analyze which participant created the most messages.



By grouping on participant and pivoting on "tone", one can determine which messages are sent and received for business, personal and with some enhancement, the type of conversational tone used in the message such as "aggressive" or "flirtatious".



You will likely be involved with a case involving cell phone collection and review in the future. When that happens, be assured there are processes and tools that can be leveraged to make text messages collected from phones more useful for your matter.