Computer forensics and e-discovery for the iPad.

By Peter Coons, D4 LLC

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. It's a revolution!

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)
- And all my Family Guy episodes

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 review. The amount of data 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 e-mails, 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 I found most interesting 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.