Exemplary Evidence

Working Title: The Return of iPhone Forensics

Caption/Teaser: America's most popular smartphone has become a materially important source of best evidence for civil and criminal litigation. But the effectiveness of iPhone forensics to recover probative evidence has been declining for a decade. A major, transformational advance introduced earlier this year marks the return of iPhone forensics. What does it mean and how can you use it for novel, cutting edge client advocacy?

Author: John J. Carney, Esq., Chief Technology Officer
Carney Forensics, www.carneyforensics.com

Steve Jobs introduced Apple's new iPhone in June 2007 and it immediately became a successful product. Its popularity in America has grown, insanely some would say, to become the smartphone market share leader at 47% as of Q2 2020. Apple's advances in privacy and personal safety using encryption, multiple passwords, two-factor authentication, and many other security best practices have attracted millions of users.

From personal polling at digital evidence CLEs I have presented over the years here in Minnesota I have learned that the vast majority of lawyers in this state are iPhone users. So are many of their clients and the public. Thus, the iPhone has become an unparalleled source of mobile evidence from not only iPhone handsets, but also the connected, online iCloud account to which most users opt in. America's most popular smartphone has become a materially important source of best evidence for civil and criminal litigation.

iPhone Forensic History

The history of the iPhone now spans fourteen years. But, the golden era of iPhone *forensic* history began in 2007 and lasted for three years until Apple introduced the iPhone 4 in June of 2010. It came to a screeching halt in the fourth year with the release of the iPhone 4S in October of 2011. In those early days everything, all mobile evidence, live and active, deleted, and discarded evidence in unallocated storage, was ready and waiting for the examiner's recovery using straightforward tools.

The iPhone 4 introduction eliminated email evidence recovery from iPhones. And then the iPhone 4S release with its hardware encryption eliminated physical extractions in their entirety. Gone were many previously available types of evidence. And gone were the voluminous quantities of deleted evidence. Last, gone was discarded evidence in unallocated storage to include deleted, forgotten photos and videos and so much more. The year 2011 brought mobile device forensic examiners the iPhone logical extraction to rely upon exclusively for evidence recovery. And the effectiveness of iPhone forensics to produce probative evidence has been declining ever since for almost a decade.

What is a logical extraction? The term is used to refer to a technique for extracting the files and folders with none of the deleted data from a mobile device. However, some describe logical extraction narrowly as the ability to gather a particular data type, such as contacts, call logs, text messages, calendar, photographs, videos, and some mobile app evidence. A software tool is used to make a copy of the files. For example, Apple's Tunes backup is used to make a logical extraction of an iPhone or iPad.

Substantial limitations to evidence extraction and probativeness are introduced by reliance on only the logical extraction method. Apple's iTunes has controlled access to iPhone handsets for almost a decade to the chagrin of mobile device forensic examiners around the world. Besides skimming only the surface of mobile evidence on iPhone handsets, iTunes made extraction even more difficult by honoring three passcodes that hide evidence on iPhones.

But that medieval period has come to its end. A major, transformational advance introduced earlier this year of 2020 marks the return of iPhone forensics for the foreseeable future. It doesn't feature a physical extraction like the golden era of 2007 to 2010, but is the next best thing. It's called a full file system extraction by examiners and it recovers the entire iOS file system for extraordinary iPhone evidence collection and production for admissibility in legal matters. It recovers vastly greater quantities of live and deleted evidence including qualitatively new forms of highly probative evidence compared to what's been available the past decade.

How does it work? Full file system extractions exploit a weakness in Apple's iPhone operating system in a forensically sound, generally accepted way without risking changes to the file system. Recovery of the full file system without changing it exposes all the iPhone evidence to analysis, both live and deleted, including messages, chats, contacts, voice messages, device locations, health and activity tracking, and many other mobile apps. It is supported by the best, most respected tools in the mobile device forensic industry to recover, analyze, and produce admissible evidence.

Return to Probativeness

While logical iPhone extractions over the past decade have recovered a reasonable amount of live (non-deleted) evidence items, full file system extractions perform substantially better. They produce superior quantities of live and deleted evidence and are meaningfully more probative. In general lawyers can expect about three to five times more gigabytes of data capacity from an iPhone full file system extraction compared to a logical extraction. Experiments performed in my lab on two test iPhones and a test iPad show full recoveries of all gigabytes of storage in use on the device. Storage "in use" is the total storage capacity on the device minus the storage available for new evidence.

But lawyers care more about actual evidence and not the data capacity to store it. Contacts, email, documents, and text messages mean more than gigabytes of storage. Please see the table below showing a comparison of iPhone evidence items recovered during the past decade from logical extractions as contrasted with the breakthrough quantities of live and deleted evidence items recovered today from full file system extractions in my lab.

Table – iPhone Evidence Recovery Comparison

What's more, full file system extractions are unearthing qualitatively new types of iPhone evidence examiners have never seen before. These discoveries include lots of new mobile app usage data and logs to include date and time stamp metadata. Discoveries also include device events, user dictionaries, and mobile card evidence never seen before. And they include information about the iPhone's power logs that help examiners understand the status of the battery, camera, device lock, and screen autolock. A new iPhone database has been discovered that provides insight into the iPhone's activity level, device orientation, device plugged-in status, and backlight status. This information when taken together with traditional iPhone evidence assists examiners in knowing what the user was doing and when.

The iPhone full file system has also revealed more secrets from the iOS keychain. It securely saves sensitive data on the user's iPhone like user names and passwords that protect online accounts, and it saves cryptographic keys and tokens. But now using full file system extractions mobile device forensic examiners with legal authority can recover the full keychain and decrypt it from unlocked iPhones for examination and analysis.

While the breakthrough in iPhone forensics has been transformational, it does come with some limitations. Extracting full file systems from the latest iPhone 11, Xr, and Xs models is supported for only a reduced range of iOS versions. Limitations also include iPhone lock codes. For the past decade examiners were incapable of piercing or recovering iPhone lock codes. But now the new iPhone extraction technology offers the recovery of a full file system from locked, older legacy models like the iPhone 5 and 5c. And it can recover more limited evidence from newer models of locked iPhones to include a partial file system and partial keychain. The partial file system has resulted in valuable evidence recoveries from locked iPhones to include installed applications,

contacts, call logs, notes, wallet data, Wi-Fi connections, media files, notifications, device locations, network activity, web mail, mobile messaging apps, voicemail messages, and social media apps.

Evidence for Client Advocacy

What does this major, transformational advance in iPhone evidence introduced earlier this year mean for lawyers practicing civil and criminal litigation? And how can they use the recent return of iPhone forensics for novel, cutting edge client advocacy?

Full file system extractions are revealing new mobile evidence from Apple's Screen Time feature. It provides users with insights into how they are spending time with apps and websites on their iPhone. Detailed daily and weekly activity reports are generated showing the time spent in each app, usage across categories of apps, number of notifications, and how often one uses their iPhone. Screen Time, mobile app usages, and other iPhone databases and logs yield probative insights that go to user digital behaviors, life rhythms, and activities in daily life. This pattern of life evidence can lead to important evidentiary findings shown illustratively by the creation of "day in the life" timelines for litigation.

I have tested iPhones wiped by their users by performing full factory resets. The unlock code has been removed in the wipe and the iPhone forgets its user, language, and iCloud account. But the full file systems I extract from wiped iPhones have led to recovery of an impressive array of evidence. Especially valuable is the evidence timeline replete with events recorded from iPhones before the wipe. The recent past is memorialized there and is best evidence to show spoliation events and to determine if, when, where, how, and by whom the rest of the iPhone evidence was destroyed.

Next month Exemplary Evidence will explore wearable devices, including iPhone, Apple Watch, Fitbit, and Garmin watch, and the discoverable evidence these devices collect.