Hands-On Exercises in iPhone Preservation
Custodian-Directed Preservation of iPhone Content: Simple. Scalable. Proportional.
Craig Ball

This article and exercises make the case for routine, scalable preservation of potentially-relevant iPhone and iPad data by requiring custodians back up their devices using iTunes (a free Apple program that runs on PCs and Macs), then compress and encrypt the backup for *in situ* preservation or collection.

The Need

Chances are, you're reading this on your iPhone or iPad. If not, it's a virtual certainty that your phone or tablet are nearby. Few of us separate from our mobile devices for more than minutes a day. On average, cell users spend four hours a day looking at that little screen. On a*verage.* If your usage is much less, someone else's is much more.

It took 30 years for e-mail to displace paper as our primary target in discovery. It's taken barely 10 for mobile data, especially texts, to unseat e-mail as the Holy Grail of probative electronic evidence. *Mobile is where evidence lives now*; yet in most cases, mobile data remains "off the table" in discovery. It's infrequently preserved, searched or produced.

> ***No one can say that mobile data isn't likely to be relevant, unique and material.*** Today, the most candid communications aren't e-mail, they're text messages. Mobile devices are our principal conduit to online information, eclipsing use of laptops and desktops. Texts and app data reside primarily and *exclusively* on mobile devices.
>
> ***No one can say that mobile data isn't reasonably accessible.*** We use phones continuously, for everything from games to gossip to geolocation. Texts are durable (the default setting on an iPhone is to keep texts "Forever"). Mobile content easily replicates as data backed up and synched to laptops, desktops and online repositories like iCloud. The mobile preservation burden pales compared to that we take for granted in the preservation of potentially-relevant ESI on servers and personal computers.
>
> ***Modest Burden.*** That's what this article is about. My goal is that you see for yourself that the preservation burden is minimal when it comes to preserving the most common and relevant mobile data. I'll go so far as to say that *the burden of preserving mobile device content, even at an enterprise scale, is less than that of preserving a comparable volume of data on laptop or desktop computers.* Too, the workflows are as *defensible and auditable as any we accept as reasonable in meeting other ESI preservation duties.*

Three Principles

The following three principles underscore the need for efficient, defensible preservation of relevant mobile content:

- When mobile data may be unique and relevant, it should be preserved in anticipation of litigation. This principle is especially compelling when the preservation burden is trivial (as by use of the backup technique described below). You can demonstrate the absence of relevant data by, *e.g.*, sampling the contents of devices; but standing alone, a policy barring the use of a device to store relevant data is *not* sufficient proof that such device has not, in fact, been used to store data. Too often, practice belies policy, particularly for messaging
- Mobile preservation should be a customary feature of a defensible litigation hold; but absent issues of spoliation, few matters warrant the added cost of mobile preservation by forensics experts or the burden and disruption of separating users from mobile devices.
- Legitimate concerns respecting personal privacy and privilege do *not* justify a failure to preserve relevant mobile data, although they *will* dictate *how* data is protected, processed, searched, reviewed and produced.

Three Provisos:

As you undertake the exemplar workflow in the exercises and ponder how you might adapt it to your needs, consider the following three provisos:

- *The method demonstrated here is but one simple, scalable and defensible method* to preserve iPhone content. It's not necessarily the only way or the optimum way.
- *Preservation isn't production.* Lawyers' abilities to search, review and produce mobile content in utile and complete forms hasn't kept pace with the obligation to do so, or on a par with other responsive sources of ESI. This article and these exercises are about routine *preservation*; they don't address downstream processes and production except insofar as ensuring that the information preserved remains readily amenable to all methods of search, review and production in e-discovery.
- *Please challenge, but don't dismiss.* The duty to preserve is real and immediate; but there's room for honest debate about what depth and exactitude of mobile preservation is warranted case to case. In weighing any method, compare it to the alternative. *If you reject a preservation method because you deem it flawed, is the alternative a superior method or nothing at all?* "None" is rarely the proper choice when it comes to mobile evidence. Preserving "most" is better than "none," but, considerations of risk may dictate that one preserve "all" over "most." In turn, considerations of proportionality may elevate "most" over "all." It's sensible to ask, "*Is the incremental cost of forensic-level*

preservation by experts justified by relevant and unique content? If not, might 'good' be good enough?"

Defensibility

Ignoring mobile evidence isn't the path taken by competent, ethical attorneys. We must employ methods of preservation that aren't unduly costly or burdensome yet pose little risk that a judge will find the methods unreasonable. The essence of defensibility is the ability to show that an action was prudent per a good faith assessment of what was known, or in the exercise of diligence should have been known, when the action occurred. If mobile content required to be preserved is lost, the Court will ask: "*Was the preservation method employed reasonably calculated to guard against loss or corruption of potentially-relevant mobile data?*" This will entail consideration of the method, its deployment and its oversight. These considerations are addressed below in Audit and Verification.

Custodian-Directed Preservation

The predominant approach to preservation in e-discovery entails use of a legal hold directive instructing custodians to act to preserve potentially-relevant ESI. This is custodian-directed preservation, and it's been justifiably criticized for its many flaws, among them that:

- It requires custodians to make judgments concerning relevance, materiality and privilege;
- It obliges custodians to complete tasks, like lexical search, without proper tools or training;
- It demands effort without affording custodians the time, resources and guidance to succeed; and
- It doesn't deter custodians who seek to destroy or change inculpatory or embarassing data.

Custodian-directed preservation is key to a defensible legal hold process; however, it's just part of a proper process and is best paired with other efforts, like IT-initiated holds, that defray its shortcomings.

So, if custodian-directed preservation is problematic, why put custodians in charge of preserving their own devices instead of handing the devices over to digital forensics experts for imaging? Isn't that inviting the fox to guard the henhouse?

The signal challenge to preserving mobile devices is persuading custodians to part with them. By empowering custodians to preserve the data themselves, custodians need never surrender custody of their devices. Accordingly, users are less threatended by the process and less inclined to fight or subvert it. Backing up an iPhone is simple and quick; and crucially, the process affords the custodian neither the need nor the practical ability to select or omit content. Compare that

to tasking a custodian to collect e-mail or documents, where it's easy to overlook or deliberately omit material with little chance of detection.

The advantages of custodian-directed preservation of mobile devices by backup are:

- Custodians need not make judgments concerning relevance, materiality and privilege;
- Custodians need not run searches or require no special tools or training;
- The backup process is speedy, easy to autheticate and lets custodians retain their phone;
- It's difficult to omit content from a backup and, once created, backups are hard to alter.

Scalability and Proportionality

Scalability describes the ability of a system or process to handle a growing number of tasks or a larger volume of data. It's a crucial consideration in all phases of e-discovery, but particularly challenging when dealing with mobile data. Historically, preserving mobile data was a one-off task: seldom undertaken and typically for only a handful of devices. Preserving the contents of a single phone by engaging a digital forensics specialist to image the device was the norm, and though costly, the obligation rarely had to scale to dozens or hundreds of far-flung devices. For one or two phones, you could do it in a day or two for, say, a thousand dollars.

Now, imagine you must preserve the texts and call data from the mobile devices of sales reps, one each in all fifty United States, the District of Columbia, Puerto Rico and Guam. Fifty-three iPhones. What are your options? Let's compare:

1. **Instruct all custodians to overnight courier their phones to your trusty forensic examiner.** In turn, the examiner will image each device and overnight each back when the work is complete.
    - Cost: Under $30,000.00 without rush or overtime fees.
    - Timing: Assuming no glitches, most users will have their phones back within about four to five business days, as few labs possess the equipment permitting them to image more than a couple of phones simultaneously. As well, 53 packages must be correctly processed, logged as evidence, re-packaged and returned to the correct custodian.
        - How many businesses can idle their national sales staff for four to five days?
        - How many reps will be willing to hand over their phones for four to five days?

2. **Send your trusty forensic examiner to 53 locations to image each phone.**
    - Cost: $50-$60,000.00 in professional time; add a comparable sum for travel costs.

- Timing: A month or more. It's a 19-hour flight to Guam, 11 hours to Hawaii and nine to Alaska. Equipment must travel, and each custodian must part with their phone for the better part of a day.
    - Caveat: Some states license forensic examiners. It may not be legal for an unlicensed examiner to come into the jurisdiction to acquire the image.

3. **Engage 53 local, licensed (as required) examiners to image each device.**
    - Cost: $35-$50,000.00 in examiner fees, plus the professional time required to locate, vet and contract with each examiner. There will also be travel time assessed, albeit with little airfare and hotel expense.
    - Timing: Weeks, at best. Fifty-three data sets from as many senders must be correctly packaged and returned to you, and each custodian must still part with their phone.

All three options implicate proportionality concerns. All are expensive, disruptive and time-consuming. Accordingly, many litigants opt not to preserve the content of mobile devices, claiming phones don't hold relevant data in the face of compelling contrary evidence and a dearth of supportive metrics.

Let's compare the custodian-directed option:

4. **Direct and instruct 53 custodians to back up their devices, collecting the data as desired.**
    - Cost: None, insofar as discrete expenditures. Of course, discovery is never "free" because time costs money. The expense to notify the custodians and follow up on compliance is attendant to all methods, and administrative costs don't count against any. Expenses, if any, for the custodian-directed method hinge on whether you preserve backup data *in situ,* collect it via network transfer or ship it on physical media. Each method demands *some* effort of each custodian, whether that entails coordinating with an examiner to tender and retrieve a device or connecting the device to a computer for an iTunes backup. The latter is far easier and least disruptive.
    - Timing: A day or two. Sure, some custodians may be on vacation, and some may miss or ignore the request; however, such risks afflict every method. Only the custodian-directed method makes it possible to preserve the many, widespread devices in hours, not days or weeks. The custodian need only get to a computer with the device, whereas a forensic examiner must get to the device or the device must get to the examiner.

The custodian-directed method scales easily for phones and tablets. Custodians need never part with their devices, so there is no business interruption. It's speedy. It requires no special tools, cabling or software and no technical expertise. Moreover, the process poses almost no risk of loss or alteration of the relevant data and is unlikely to prompt custodians to game the process. There are no operating system compatibility issues. Remote screen-sharing handily facilitates any desired oversight and audit. In short, cost and burden are so trivial that relevance alone should be the pole star in deciding whether to preserve mobile content.

For an example of mobile backup instructions that might be directed to a custodian, look at Appendix 4. What we might ask our to do clients serves as the step-by-step of the exercises.

Audit and Verification

Recently, my friend and fellow forensic examiner, Scott Moulton, visited New Orleans. Over beignets and café au lait in the French Quarter, I made the case for the preservation methodology described here. Scott's a brilliant examiner and hard-eyed skeptic. I wanted him to kick the tires and find flaws.

At first, Scott wouldn't take off his forensic examiner hat and don an e-discovery thinking cap. He extolled the benefits of hiring a qualified forensic examiner and the specialized forensics tools we use to dig for esoteric artifacts. "Hire me. Hire *you*!" I liked the sound of that, and Scott liked the idea of motorcycling through the lower 48 and D.C. gathering digital evidence like some two-wheeled remake of Cannonball Run meets Revenge of the Nerds.

Still, Scott conceded that in the context of e-discovery, there really isn't much iPhone data preserved using a costly forensics tool versus preservation using iTunes. Our training and tool sets don't add much when preserving mobile data for discovery.

Once Scott warmed to the methodology for its speed and low cost, he questioned how the process could be quality checked for integrity. "What if the backup was interrupted or failed," he asked, "How would we know?"

It's a good point. Most experienced forensic examiners have found an image acquired in the field to be incomplete or unusable back in the lab. Thankfully, it's rare; but, sooner or later, it happens. *There are always gremlins*. Custodial-initiated preservation benefits from oversight and audit, if only because the risk of gremlins *feels* greater when custodians are in charge.

If iTunes successfully completes a backup, the backup event can be verified several ways:

1. In iTunes (with the device connected), by looking at the device summary for the attached device and noting the latest backups. ***Fig. 1, right top.***
2. In iTunes (with or without the device connected), under ***Edit>Preferences>Devices***. **Fig.2, right.** This lists the backed-up devices by name with time of backup. Hovering the mouse pointer over a listing will bring up further details about the device backed up (model, software version and build, serial number, phone number, IMEI and MEID). ***Fig. 3 right bottom.***
3. By confirming the date and time values for the folder containing the latest backup (stored by default in: C:\Users*user's account name*\AppData\Roaming\Apple Computer\MobileSync\Backup\). ***Fig. 4 below.***

Figure 12

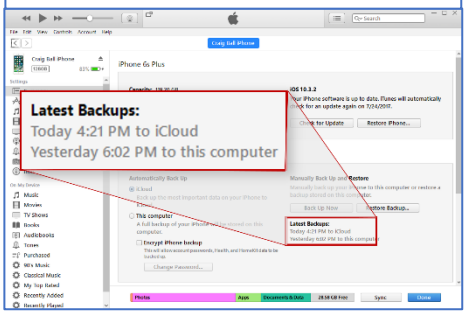


Figure 1

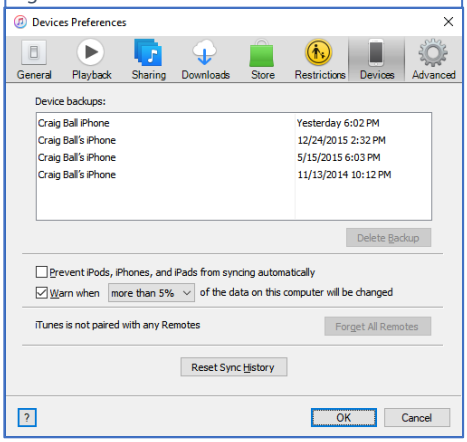


Figure 3

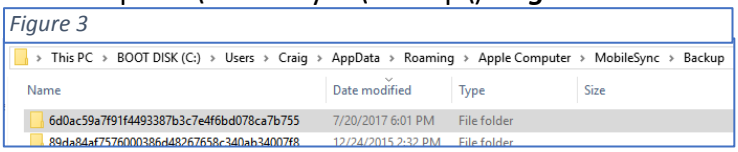
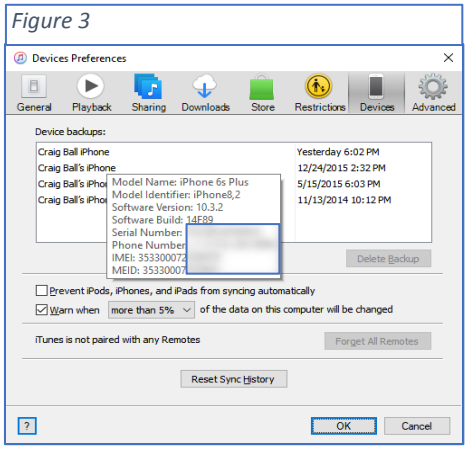


Figure 3



There are several sensible ways to verify and audit a custodian-directed preservation effort. Tailor the method to the potential for failure and the willingness of a sponsoring witness to vouch for the integrity of the process if challenged. A proper audit trail could be as simple as the custodian supplying a screenshot (ALT-Print Screen) of the details panel for the latest backup (as seen when one hovers over backups in Devices Preferences, as described above and seen in **Fig. 3**). A second approach is the use of cryptographic hashing, and a third, the use of remote screen-sharing and -recording software to permit step-by-step oversight of the work by the sponsoring witness or designee. Also, device backup sets may be sampled and tested for accuracy and completeness. It's important to do *something* to audit and verify the effort; but proportionality suggests you needn't do *everything*.

What You Won't Get with a Backup

An iPhone backup won't preserve e-mail stored on the iPhone. This is by design. Per Apple, an unencrypted iTunes backup also won't include:

- Content from the iTunes and App Stores, or PDFs downloaded directly to iBooks
- Content synced from iTunes, like imported MP3s or CDs, videos, books, and photos
- Photos already stored in the cloud, like My Photo Stream, and iCloud Photo Library
- Touch ID settings
- Apple Pay information and settings
- Activity, Health and Keychain data

Why not use iCloud?

At some point, you *will* use iCloud for preservation; but currently, an iCloud backup is not equal to an iTunes backup. It preserves less data, and byte-for-byte, it takes more time to create than an iTunes backup. Additionally, iCloud encrypts all backups, making them a future challenge for processing and search should a user's credentials be unavailable.

Why an Unencrypted Backup?

This is a compromise. On the one hand, an encrypted iTunes backup preserves more information than an unencrypted backup. Apple won't store passwords, website history, Health data and Wi-Fi settings in an unencrypted backup. On the other hand, many tools can't process the contents of an encrypted backup, even with user credentials, and no tool can process an encrypted backup without credentials. Accordingly, we collect the data as an unencrypted backup, obviating the need for user credentials. To protect the data and add efficiency, we compress and optionally encrypt the backup set using credentials chosen for the legal hold project, not each user's credentials.

Encryption

Encryption is a crucial security tool to protect client data collected in e-discovery, but it's better to manage credentials systematically for the e-discovery project instead of according to each custodian's preference. However, because mobile devices employ layers of encryption, obtaining an unencrypted backup won't serve to unlock encrypted application data. You must obtain and preserve the user's access credentials for that data.

Many users employ the same password for multiple sources, so requiring a user to disclose credentials serves to compromise the security of sources not collected. Assuage concerns by detailing steps taken to protect users' credentials. An unlocked spreadsheet with each custodian's password(s) may be a convenience for the legal team, but it's a cybersecurity

nightmare. Keep that in mind when furnishing credentials to service providers, and be sure your vendors are handling passwords securely.

Why Compress the Backup Data?

One reason we compress the data to a Zip file is to make it easier to copy to new media. Smaller data volumes move faster. However, depending upon the composition of the data backed up, the compressed Zip file may be much smaller or hardly smaller at all. My backup set compressed by just 2%. Much of the data on my iPhone consists of JPEG photos already in a compressed format, and it's hard to compress data that's already compressed as there's little 'space' to squeeze out by further compression.

So why bother compressing the backup files?

Two reasons. First, placing the preserved data in a Zip file guards against overwriting the data by a subsequent backup of the device. Second, depending upon the Zip tool employed to compress the file, the Zip process affords a means to securely encrypt the data without having to install an encryption tool. Every Windows machine can create compressed and encrypted Zip files, so will every Mac running OS X.

A New Paradigm in Mobile Device Preservation: Recently, I wrote a post (Appendix 1, next page) where I stated, "Today, if you fail to advise clients to preserve relevant and unique mobile data when under a preservation duty, you're committing malpractice." I'll go further and add that competent counsel not only tells clients what they must do but must also help clients identify practical, proportional ways to meet mobile preservation obligations. This article lays out one scalable, defensible and cost-effective way to preserve iPhone and iPad content. The purpose is to debunk claims that mobile preservation is unduly burdensome, expensive and disruptive. Practical approaches are out there for other phones and devices, too. It's our duty to insure our clients know about them and use them.

Appendix 1: Ball in Your Court, April 18, 2017

A New Paradigm in Mobile Device Preservation

Tuesday, April 18, 2017

Can anyone doubt the changes wrought by the modern "smart" cellphone? My new home sits at the corner of one-way streets in New Orleans, my porch a few feet from motorists. At my former NOLA home, my porch faced cars stopped for a street light. From my vantage points, I saw drivers looking at their phones, some so engrossed they failed to move when they could. Phones impact how traffic progresses through controlled intersections in every community. We are slow-moving zombies in cars.

Distracted driving has eclipsed speeding and drunken driving as the leading cause of motor vehicle collisions. Walking into fixed objects while texting is reportedly the most common reason young people visit emergency rooms today. Instances of "distracted walking" injury have doubled every year since 2006. Doing the math, 250 ER visits in 2006 are over half a million ER visits today, *because we walk into poles, doors and parked cars while texting*.

Look around you. CAUTION: *This will entail looking up from your phone.* How many are using their phones? At a concert, how many are experiencing it through the lens of their cell phone cameras? How many selfies? How many texts? How many apps?

Lately I've begun asking CLE attendees how many are never more than an arm's length from their phones 24/7. A majority raise their hands. These are tech-wary lawyers, and most are Boomers, not Millennials.

Smart phones have changed us. Litigants are at a turning point in meeting e-discovery duties, and lawyers ignore this sea change at peril. The "legal industry" has chosen self-deception when it comes to mobile devices. It's a lie in line with corporate bottom lines, and it once found support in the e-discovery case law and rules of procedure. But, no more.

Today, if you fail to advise clients to preserve relevant and unique mobile data when under a preservation duty, you're committing malpractice.

Yes, I used the "M" word, and not lightly.

I wouldn't have called it malpractice a few years ago. But two things have changed, and we can't hide our heads in the sand. These are paradigm shifts.

The two things are, first, the data on phones and tablets is *not* just a copy of information held elsewhere. It's unique, and often relevant, probative evidence. Second, the locking down of phone content has driven the preservation of mobile content from the esoteric realm of computer forensics to the readily accessible world of apps and backups. These developments mean that, notwithstanding the outdated rationales lawyers trot out for ignoring mobile, the time has come to accept that mobile is routinely within the scope of preservation obligations.

Too, lawyers need to stop treating mobile devices like biohazards and realize that there are easy, low-cost ways to preserve relevant mobile content *without taking phones away from users.* Because it's easy and cheap to preserve it, mobile content is accessible, and its preservation, when potentially relevant, is proportionate under the Rules.

That's a strong stand, and one some will angrily reject. I get where they're coming from. It was wonderful to be able to ignore mobile in e-discovery. Mobile was a black hole. It wasn't just that you had to hire technical experts to use expensive tools to preserve the contents of phones, it was like pulling teeth to get users to let loose of their devices for the hours or days it took to collect them. Even when they did hand them over, more than a few users claimed to have entered the wrong password too many times and "accidentally" wiped the contents of the phone. "Oops. My bad."

If that never happened to one of your clients, it may be because your client wasn't preserving phone data, indulging in the assumption that whatever they'd glean from the phone would be collected elsewhere. They deemed mobile redundant.

Lecturing about mobile and IoT in D.C. last year, an associate from a megafirm confided to me that his firm routinely advised all its litigation clients that they need not preserve the content of mobile devices because "all the relevant content would be duplicated on the servers." I asked if the firm had ever tested its advice against the relevant data to determine if there was truth in what they were telling clients. He admitted they never had, and offered that they'd never do so. The firm didn't want to know the facts because the fairy tale of "replicated elsewhere" was what the client wanted to hear.

Is it a fairy tale? I have my own views based on my own comparisons of mobile content versus other collected sources. What I see demonstrates that the claim that what's relevant on a phone is preserved elsewhere is a whopper. I am routinely finding examples of relevant data stored on

mobile devices that is not found among the other sources of data routinely preserved in e-discovery. The replication fairy tale is a relic of a bygone era of Blackberry Enterprise Servers and phones with lower IQs than the brilliant devices now our constant companions and confidantes.

But, I'm not asking you (or courts) to take my word for it. *Test it yourself.*

If you're going to tell the tale, then get some metrics to make it plausible. Use sampling. Process the phones of a few key custodians and compare all the potentially relevant items collected from their mobile devices against the other sources collected for the sampled custodians. What's the differential? Is the unique evidence from the mobile device probative and material?

I've done that, and so I know replication is a fairy tale. If you want to claim it's true *for your client in your case*, how about putting some facts to work? Bear the burden of proof, or start bearing the onus of truth. When you have the facts, you'll have to let loose of the legend and preserve relevant mobile content.

That's the bad news for those who would prefer to ignore mobile. But take heart, as that will seem like great news compared to the next development. Yet, there's a silver lining. Mobile preservation is now quick, cheap and easy.

A few years ago, mobile phones shared some of the characteristics of personal computers in that they held latent data that could be recovered using specialized tools sold for princely sums by a couple of shadowy tech companies. So, the preservation of mobile devices slipped into the shadows, too. Phones and tablets were *forensic* evidence, and only forensic examiners could collect their contents.

Although users used mobile devices all day, the contents of mobile devices were dubbed "not reasonably accessible." It was too costly and burdensome to preserve a phone. Good thing, because users were holding onto their phones tighter than Willie Nelson clutches a bong. Users protested, *"the mobile phone is the only way the kids' school can reach me in an emergency, and I can't use another phone because everyone texts now, and WHO REMEMBERS PHONE NUMBERS ANYMORE?"*

So, the next altered paradigm: In e-discovery today, the forensic-level preservation of phones—the sort geared to deleted content and forensic artifacts—is a fool's errand. As the public learned from the FBI's tussle with Apple over unlocking the iPhones of the San Bernardino terrorists, modern smart phones are locked down hard. Content is encrypted and even the keys to access

the encrypted content are themselves encrypted. Phone forensics isn't what it used to be. More and more, we can't get to that cornucopia of recoverable forensically-significant data.

At the same time, it's quick, easy and free for a user to generate a full, unencrypted backup of a phone without surrendering possession. The user can even place the backup in a designated location for safekeeping by counsel or IT. Will this be a "forensic image" of the contents? Strictly speaking, no. But as the phone manufacturers tighten their security, "forensic imaging" becomes less and less likely to yield up content of the sort encompassed by a routine e-discovery preservation obligation. Not every case is a job for C.S.I.—and I say that as someone who makes a living through computer forensics.

I grant that a full unencrypted backup of an iPhone isn't going to encompass all the data that might be gleaned by a pull-out-all-stops forensic preservation of the phone. But so what? As my corporate colleagues love to say, "*the standard for ESI preservation isn't perfect.*" I always agree adding, "*but it isn't lousy either.*" Preserving by backup isn't perfect; but, it isn't lousy. I've come to regard it as sufficient and proportionate. It's good *enough*, and in most cases, darn good.

I think this is important. It's a game changer for what most litigants are doing today. In a view I hope will come to be shared by all who think it through—preservation of mobile device content must become a standard component of a competent preservation effort except where the mobile content can be shown to be beyond scope. Mobile content has become so relevant and unique, and the ability to preserve it so undemanding, that the standard must be preservation.

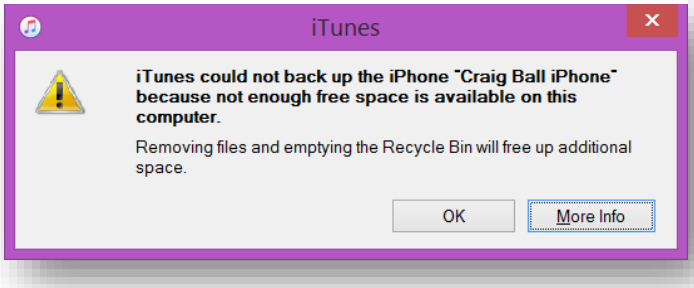
In a future post, I'll lay out the steps to make mobile preservation part of routine preservation workflows and facilitate custodial-initiated preservation of mobile device content. I'll also talk about why it's defensible, proportionate and amenable to targeted processing when it's time to move from preservation to production.

Appendix 2: Redirecting the iPhone Backup Files to External Media

Q. What if I don't have enough space on my Windows C: drive to hold the backup?

A. Smart phones have evolved to capture a *lot* of data. Ten years ago, you couldn't store more than 8GB of data on an iPhone. Today, they store up to 256GB, 32 times as much . So, an iTunes backup may fail to complete because not enough free space is available on the computer performing the backup. You may be able to resolve this by, *e.g.,* emptying the Recycle Bin; but, if you simply can't garner enough space on the boot drive where Apple stores the backup by default, you may need to "trick" your Windows machine into storing the backup on a sufficiently-sized alternate or external storage medium.

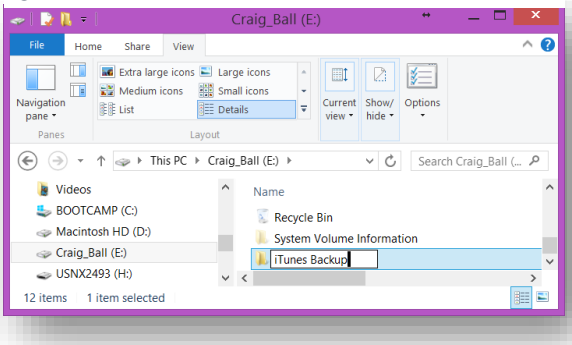
Figure 4



How to Redirect an iTunes Backup Location in Windows

Step 1. Create a new backup folder on a disk with sufficient space to create your backup (roughly. twice the capacity of your iPhone is ample). In Figure 6, I've created the new iTunes backup location on my E: drive (a 250GB thumb drive) and named it "iTunes_Backup:" You can name yours anything you'd like.

Figure 5



Step 2. Rename the current iTunes backup folder
Using Windows File Explorer, navigate to your current iTunes "Backup" folder. By default, it's:
C:\Users*your account name*\AppData\Roaming\Apple Computer\MobileSync
where "*your account name*" is the name of your Window's User ID on the machine.

Right click on the "Backup" folder and rename it. I called mine "Old_Backup;" but here again, call it whatever you like.

3. Redirect the Old Backup Folder Address to the New One
Here, it gets a tad tricky because you must use a Windows Command line interface. Make it easier on yourself by writing down the full paths to the old and new backup folders. *You must get both right for the redirection to work.*

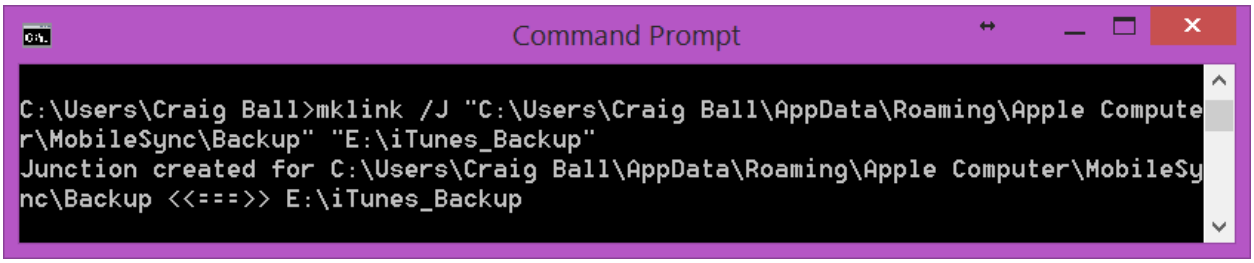
The old one *should* be:
C:\Users*your account name*\AppData\Roaming\Apple Computer\MobileSync\Backup

The new path is on whatever storage medium you chose, using whatever path and folder name you gave it in step 1, above (mine was "**E:\iTunes_Backup**").

Open a command prompt window by pressing the Windows key on your keyboard, then typing CMD or by pressing the Shift key on your keyboard while right clicking in an open area of any folder, then selecting "Y and selecting "*Open command window here*" from the menu.

At the command line, carefully type the following command:
mklink /J "*path to old backup location*" "*path to new backup location*"
where you substitute the old and new paths you've written down. *Be sure to enclose each path in quotation makes, as shown.*

On my machine, the command and response looked like Figure 7:
Figure 6



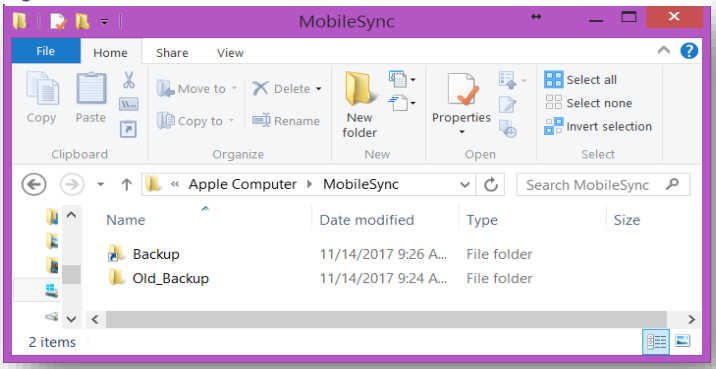
The "junction created" refers to a Windows symbolic link, a **Directory Junction,** that will serve to redirect any actions that would have been performed on the old backup folder to be redirected to the new one.

What Note: The **mklink /J** command creates a symbolic link to the new folder from the old one. It's like creating a shortcut of D:\Backup from the original MobileSync\Backup folder. You can test the effect by double-clicking on the Backup folder in MobileSync. It will take you to the new Backup folder.

Now, if you look in your MobileSync folder:
(**C:\Users*your account name*\AppData\Roaming\Apple Computer\MobileSync**

you will see a folder shortcut named "Backup" alongside your renamed former backup folder as mine appears in Figure 8.

Figure 7



4. Move your Old Backups

If desired, you can move your old iTunes backup files from your old renamed Backup folder to your new backup folder and delete them from the old location.

5. Run your iTunes Backup

Be sure the media you selected to hold the relocated backup is attached. Now, run your iTunes backup as usual and, if all is working, the backup will be created where you created the new backup folder.

Appendix 3: iPhone Backup Data Extractors

There are quite a few applications marketed as tools to extract data from iPhone backups. Though a handful are free, the ones that look promising tend to run about $40-50 single user/single computer license, a trivial sum if it obviates the need to hire a forensic examiner or technician to extract texts, call logs, photos, browsing history, contacts and the like.

My brief exploration of these applications underscored that it's hard to discern which tools work and which don't in advance of buying a license. Happily, some promise "free evaluation copies" and "money back guarantees."

iMazing: $39.99-$279.96

The only tool that worked remarkably well (which is to say, "worked *at all*") in my testing was iMazing. It allowed me to explore its capabilities and confirm that it had no trouble opening and interpreting my iPhone backup before requiring I buy a license. Licenses started at $39.99, but I paid ten dollars more for a license that runs on two machines.

iMazing seemed to have no difficulty getting the content I'd most likely need in e-discovery and, crucially, was adept at exporting the content in utile formats, including delimited CSV files for messaging and call histories.

iPhone Backup Extractor: Free

Though its interface wasn't as intuitive as iMazing's, the Lite version of iPhone Backup Extractor seemed like it might be able to extract texts to a delimited CSV format that was Excel-ready for search and review. The problem was, it hadn't done so after more than an hour and offered no way to determine if it was going to perform in due time or if it had lapsed into a coma. Neither was it a simple matter to kill the process once initiated. So, it *may* offer some functionality without buying a license, and there are basic, premium and business licenses offered for $34.95, $69.95 and $299.95 respectively.

I also tried **FonePaw, iBackup Viewer Pro, PhoneBrowse, Phone Rescue** and **Phone Trans**. All failed to perform. Though FonePaw seemed promising and worked on older iOS backups, it didn't recognize a recent iTunes backup. Likewise, purchased licenses for iBackup Viewer Pro and Phone Rescue were wasted monies in that neither could make head-nor-tails of a backup of my iPhone 6S Plus—the same backup that iMazing had no trouble parsing.

I expect that several of the tools that failed in my testing would turn out to be capable of interpreting iPhone backup files with some tweaking or when applied to other backups. I just can't prove it as I write this.

APPENDIX 4: Exemplar iPhone Backup Instruction for Custodian-Directed Backup

[[NOTE: This draft directive is offered to assist counsel in formulating language suited to the needs of the case and controlling law. It is not a form to be deployed without counsel. This example omits optional steps to encrypt the data set and transfer same to a distal repository for preservation, as such steps are frequently unnecessary to meet preservation duties].

Dear [Custodian]:

You recently acknowledged your obligation to preserve information relevant to a dispute between our company and _____. Please see the _____ hold notice for further details.

Within *48 hours of your receipt of this notice, y*ou must preserve the contents of your company-issued iPhone. If you cannot comply, please advise me at once by e-mail or phone. *Time is of the essence.*

You must make an unencrypted backup using iTunes and compress the backup folder per the instructions below. *Do not assume that you have been automatically making an unencrypted backup or preserving what's required using iCloud. You must carefully follow the procedures set out below.*

What you will need:

- Your company-issued iPhone and its USB charge/sync cable;
- Your company-issued desktop or laptop computer with the iTunes program installed. The computer must have available (unused) storage space on its boot (C:) drive exceeding *twice* the storage capacity of the iPhone. That is, if you have a 128GB capacity iPhone, use a computer with at least 256GB of unused storage space on its C: drive. You can find the capacity of the iPhone in Settings>General>About>Capacity. You can find the available storage on your computer's boot (C:) drive using File Explorer on a Windows machine or Finder on a Mac.

Time Required: One to two hours (most of it unattended "machine" time)

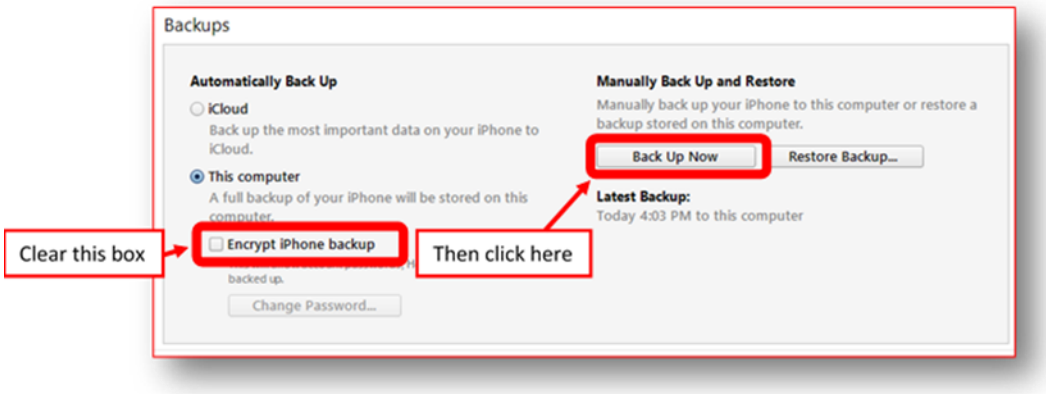
It will take about 10-15 minutes to follow these instructions, update iTunes, if needed, and begin the backup. The backup will complete in under 30 minutes, and you can continue to use the phone during the backup process (*but don't disconnect the charge/sync cable*). Then, it should take less than an hour to compress the data and 10 minutes or so to confirm successful compression and report on results. So long as the computer is secure and powered up

throughout the process, you do not need to supervise, or leave the iPhone connected once backup completes.

Follow These Steps:

1. Open iTunes and check for updates (Help>Check for Updates). Install the latest version of iTunes if not installed.
2. Connect your iPhone to a USB 2.0 or 3.0 port on the computer using a USB charge/sync cable.
3. If a message asks for your device passcode or to Trust This Computer, follow the onscreen steps.
4. Select your iPhone when it appears in iTunes. Click Summary in the sidebar.

5. In the Summary pane, be sure to uncheck "Encrypt iPhone Backup," then click "Back Up Now." You need not otherwise modify your Backups settings.



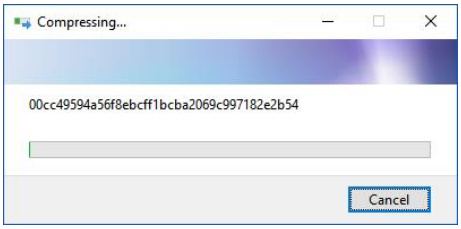
6. Monitor the progress of the backup at the top center of the iTunes window. After the process ends, see if your backup finished successfully. If you're using iTunes for Windows, choose Edit>Preferences>Devices from the menu bar at the top of the iTunes window. If you're using iTunes for Mac, go to iTunes Preferences>Devices. You should see the name of your device with the date and time that iTunes created the backup. If you see 🔒 beside the name of your device, you need to be certain you unchecked "Encrypt iPhone Backup" and repeat the process until you do not see 🔒 beside the name of your device.
7. You can now disconnect your phone from the computer.
8. Locate the backup folder:
    - **Windows:** Using File Explore, navigate to:

C:\Users*your account name*\AppData\Roaming\Apple Computer\MobileSync\Backup where "*your account name*" is the name of your Window's User ID on the machine.

- **Mac:** Using Finder, select Go>Go to Folder on the Finder menu and enter: **~/Library/Application Support/MobileSync/Backup/**

In both Windows and Mac, the Backup folder will contain one or more subfolders with 40-character names like *12da34bf5678900386c48267658d340eb34007f8*. **If there are multiple subfolders, i*dentify the subfolder that has the last modified date and time that matches the time you started this backup.***

9. **Compress the contents of the subfolder**: In Windows, right click on the subfolder just identified and select "***Send to>Compressed (zipped) folder***." A progress panel like the one at right should appear. On a Mac, right click on the subfolder and select "Compress." Do not turn off your computer or reboot. Allow the compression process to complete. It could take less than an hour to finish depending upon the type and volume of data backed up.



10. Once compression has completed, Windows users should again navigate to the backup folder (see step 8 above) to confirm the presence of a file with the same name as the subfolder you identified but with the file extension .zip. Record the name, date/time and size of the zip file. *[If you cannot see file extensions on your Windows machine, open "My Computer," click "Tools" and click "Folder Options" or click "View" and then "Options" depending on your version of Windows. In the Folder Options window, click the "View" tab. Uncheck the box that says, "Hide file extensions for known file types." This should make file extensions visible.]*

11. By reply e-mail, send the **name, date/time and size of the zip file you just created**. *Do not delete or open this file. It must be preserved without alteration until further notice.*

Your supervisor is copied here to insure you are afforded the time, oversight and support needed to comply in a timely way. Thank you for your cooperation. Call me at _____ with any questions.