



MOBILE to the Mainstream

Preservation and Extraction of iOS Content
for E-Discovery

©2019

Craig Ball

Mobile to the Mainstream: Preservation and Extraction of iOS Content for E-Discovery

Craig Ball © 2019

The Need: Chances are you're reading this on your phone or tablet. If not, I'll bet your phone or tablet are at hand. 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 *average*. 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 to unseat e-mail as the Holy Grail of probative electronic evidence. *Mobile is where evidence lives now*; yet, mobile data remains "off the table" in discovery. It's infrequently preserved, searched or produced. That's inexcusable because:

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") and mobile content is diffuse; it's backed up and synched to laptops, desktops and online repositories like iCloud.

No one can say it's unduly burdensome. The goal is that you see for yourself that the 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*.

This guide comprises two sections:

Section I (pp. 3-8 and Appendices 1-3) addresses simple, scalable preservation of iPhone and iPad content, enabling litigants to meet the duty to preserve data in anticipation of civil litigation. It informs attorneys who aren't tech-savvy how to handle iOS-device preservation and explains why there's little burden or cost attendant to preserving iPhones and iPads.

Section II (pp. 17 *et seq.* and Appendix 4) looks at simple, low-cost approaches to extracting relevant mobile data to a standard e-discovery workflow and offers a Mobile Evidence Scorecard to promote consensus as to what forms of mobile content should be routinely collected and reviewed in e-discovery, giving due consideration to need, speed and expense.

SECTION I: PRESERVATION

Custodian-Directed Preservation of iPhone Content: Simple. Scalable. Proportional.

This Section and the exercises herein 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.

Three Principles

The following three principles underscore the need for efficient, defensible preservation of potentially-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 on the phone by, *e.g.*, sampling the contents of devices; but *merely having a policy that bars use of mobile devices to transmit or store relevant data is insufficient proof that such devices are not used that way*. Practice often belies policy, particularly for text messaging.
- Mobile preservation should be a routine 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* potentially-relevant mobile data, although such concerns often dictate how data is sequestered, processed, searched, reviewed and produced.

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 or guidance to succeed; and
- It doesn't deter custodians who seek to destroy or change inculpatory or embarrassing 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 initial impediment 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 threatened 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 or delete 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, nor do they need special tools or training;
- The backup process is speedy, easy to authenticate and lets custodians retain their phone;
- It's difficult to omit content from a backup and, once created, backups are hard to alter.
- It costs less than any alternative.

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, one- or two-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, falsely or naïvely claiming phones don't hold relevant data in the face of compelling contrary evidence and a dearth of supporting 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 method more than another. 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. Every 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. Some custodians may be on vacation and some may miss or ignore the request; however, these 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 apprehension or business interruption. It's speedy. It requires no special tools, cabling or software and no technical expertise. Moreover, the process poses little 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. If desired, remote screen-sharing handily facilitates 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.

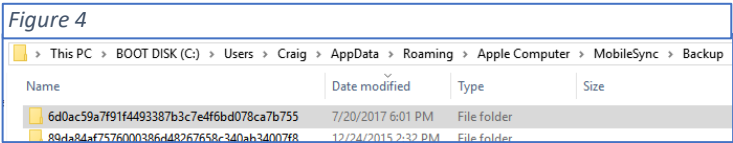
For an example of mobile backup instructions that might be directed to a custodian, look at Appendix 3. What’s asked of custodians serves as the step-by-step of the preservation exercise set out in Appendix 1.

Audit and Verification

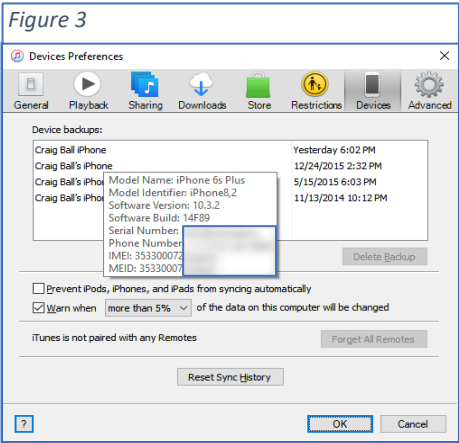
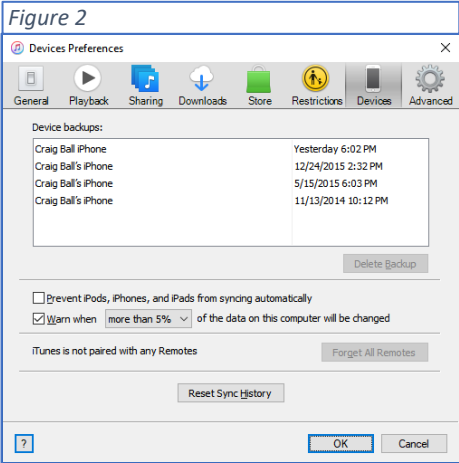
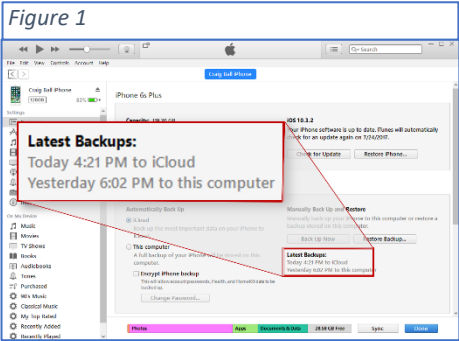
Sooner-or-later, experienced forensic examiners find an image acquired in the field to be incomplete or unusable back in the lab. It’s rare; but it happens. *There are always gremlins*. Custodial-initiated preservation benefits from oversight and audit, if only because the risk of gremlins *feels* greater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

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

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



ways to verify and audit a custodian-directed preservation Tailor the method to the potential for failure and the of a sponsoring witness to vouch for the integrity of the challenged. A proper audit trail could be as simple as the supplying a screenshot (ALT-Print Screen, then CTRL-V paste) details panel for the latest backup (as seen when one hovers 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-



can be the device latest under backed-up mouse about the serial **bottom.** containing There are several sensible effort. willingness process if custodian of the over

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
- Frequent Locations geolocation data

Why not use iCloud?

At some point, we probably 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 for storage and transmittal, and add efficiency, we compress and optionally encrypt the backup set using credentials chosen for the legal hold project, not each user's credentials.

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. Depending upon the composition of the data backed up, the compressed Zip file may be much reduced in size or hardly smaller at all. My phone's backup compresses by just 2%. Much of the data on my iPhone consists of JPEG photos already in a compressed format; so, 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 inadvertent overwriting of the data by a subsequent backup. 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 modern Windows or Mac machine can create compressed and encrypted Zip files.

A New Paradigm in Mobile Device Preservation: 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.

Appendices:

Appendix 1: Step-by-Step for iPhone/iPad Preservation Exercise

Appendix 2: Redirecting the iPhone Backup Files to External Media

Appendix 3: Exemplar iPhone Backup Instruction for Custodian-Directed Backup

Appendix 1: Step-by-Step for iPhone/iPad Preservation Exercise

It should not take more than about thirty minutes to complete this exercise. You can continue to use the phone during the backup process (*but don't disconnect the charge/sync cable*).

You will need:

1. A functioning laptop computer with **a working copy of iTunes installed and enough storage space on its boot drive (or redirected to an attached external drive per Appendix 2) to hold the backup;**
2. A **functioning iPhone (or iPad);** and
3. A **working data synch cable for the iPhone (or iPad) you will preserve.**

You *cannot* complete the exercise without all three of these. You *cannot* use an iPad to acquire an iPhone, and you *cannot* use a computer that's so locked-down it won't run iTunes or has its USB ports disabled.

Follow These Steps:

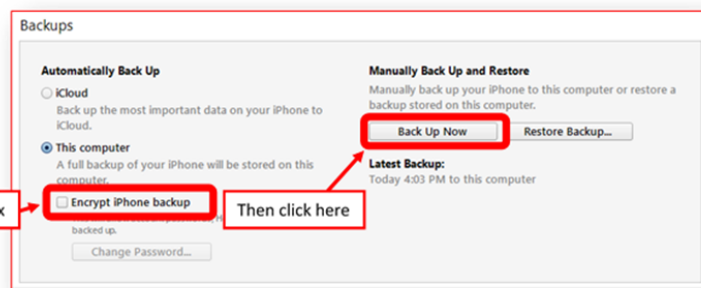
1. Open iTunes and check for updates (Help>Check for Updates). Install the latest version of iTunes if not installed.
2. Connect your iPhone/iPad to a USB 2.0 or 3.0 port on the computer using a USB charge/sync cable.
3. If a message asks for your device passcode or to Trust This Computer, follow the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

4. Select your iPhone when it appears in iTunes. the sidebar.



Click Summary in

5. In the Summary pane, be sure that "This Computer" is selected as the backup destination, uncheck "Encrypt iPhone Backup," then click "Back Up Now." You need not otherwise modify your Backup 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 a lock icon 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 a lock icon beside the name of your device.

7. You can now disconnect your phone from the computer.

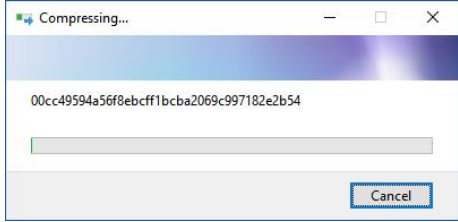
8. Locate the backup folder:

- **In 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.

- **In 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 (your backup file have a different name). **If there are multiple subfolders, identify the subfolder that has the last modified date and time that matches the time you started this backup.**

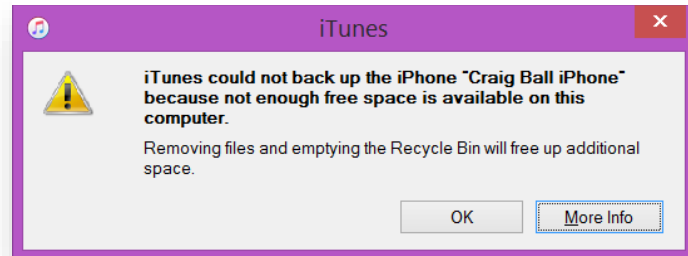
9. **Compress the contents of the subfolder:** In Windows, the subfolder just identified and select “**Send to>Compressed (zipped) folder.**” A progress panel like right should appear. On a Mac, right click on the and select “Compress.” Do not turn off your computer or reboot. *It could take up to an 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.]*

Appendix 2: Redirecting the iPhone Backup Files to External Media

Q. What if a custodian doesn't have enough space on their computer 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, an iPhone stores up to 512GB, 64 times as much. So, an iTunes backup may fail to complete because not enough free space is available on the computer performing the backup. A custodian may be able to resolve by, *e.g.*, emptying the Recycle Bin; but, if user simply can't garner enough space on boot drive where Apple stores the backup default, the custodian (or someone assisting) may need to "trick" the machine storing the backup on a sufficiently-sized alternate or external storage medium.

Figure 1



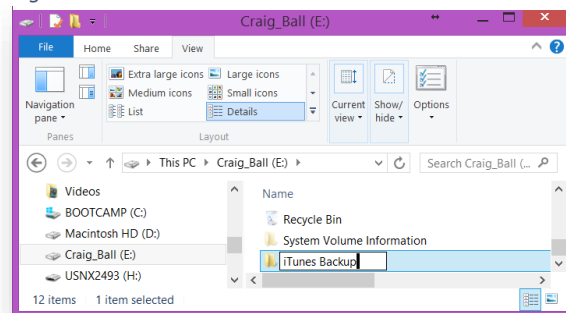
this
the
the
by
into

Storing on an external storage medium or to a network share offers another advantage: *it makes it easy to retrieve the data for processing and, with a little ingenuity and any free remote viewing (RDP) tool, e-discovery staff can handle much of the preservation process working with the custodian remotely.*

How to Redirect an iTunes Backup Location in Windows

Step 1. Create a new backup folder on a disk or network-attached medium with enough space to create your backup (roughly. twice the capacity of iPhone is ample). In Figure 2, I've created the new iTunes backup location on my E: drive (a 250GB thumb drive) and named it "iTunes_Backup:" You name yours anything you'd like.

Figure 2



your
can

Step 2. Rename the current iTunes backup folder

Using Windows File Explorer, navigate to your 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.

current

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 and **write down the full paths to the old and new backup folders.** *You must type both full paths correctly 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.

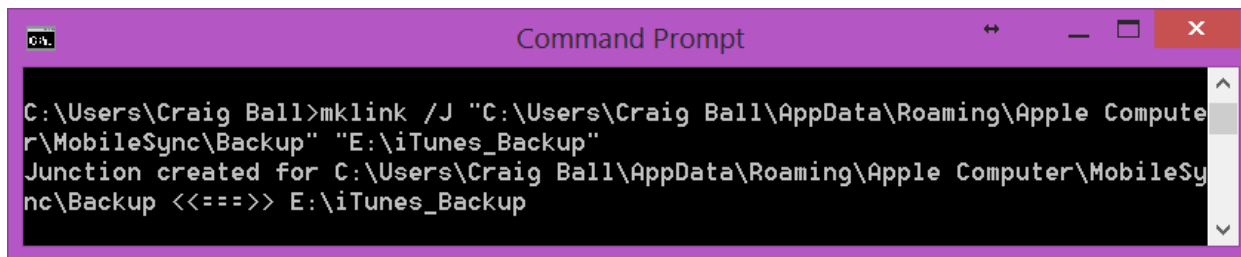
At the command line, carefully type the following command:

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 marks, as shown. Remember to substitute the paths you used for the quoted language. There’s a space after “mklink” and another space after “/J.”*

On my machine, the command and response looked like Figure 3:

Figure 3



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. 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. 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 4.

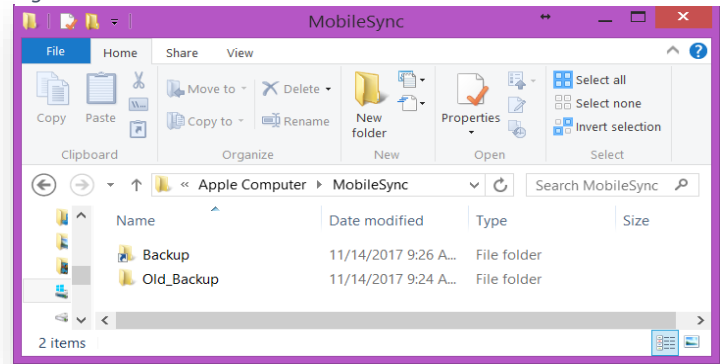
4. Optionally, Move your Old Backups

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 in the new backup folder you created.

Figure 4



To disable the directory junction, use the RMDIR command in the Windows command line interface and remove the backup directory created on the boot drive (NOT on the destination directory holding the backup).

Appendix 3: 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*, you 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:

11. Open iTunes and check for updates (Help>Check for Updates). Install the latest version of iTunes if not installed.
12. Connect your iPhone to a USB 2.0 or 3.0 port on the computer using a USB charge/sync cable.

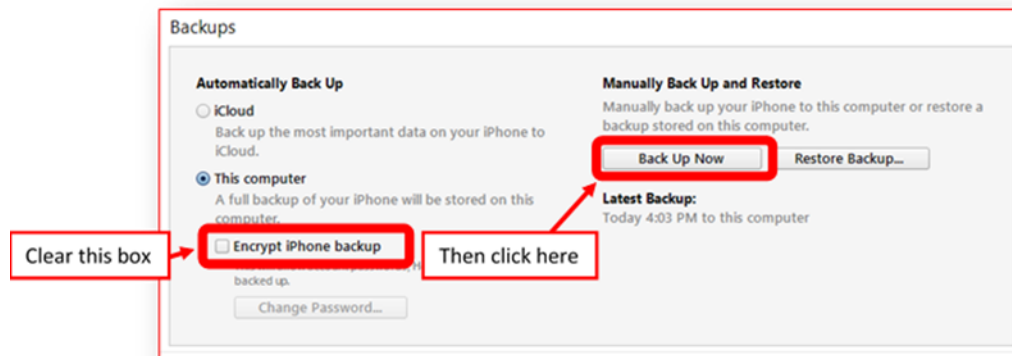
13. If a message asks for your device passcode or to Trust This Computer, follow the onscreen steps.

14. Select your iPhone when it appears in iTunes.



Click Summary in the sidebar.

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



16. 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 a lock icon 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 a lock icon beside the name of your device.

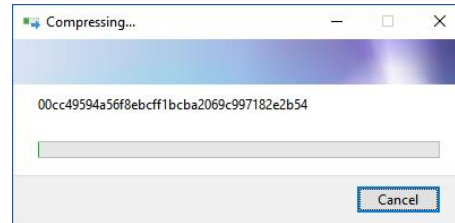
17. You can now disconnect your phone from the computer.

18. 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, identify the subfolder that has the last modified date and time that matches the time you started this backup.**

19. **Compress the contents of the subfolder:** In right click on the subfolder just identified and select **to>Compressed (zipped) folder.** A progress panel at right should appear. On a Mac, right click on the and select “Compress.” Do not turn off your 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.



Windows,
“Send
like the one
subfolder
computer or

20. 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.]*

21. 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.

SECTION II: EXTRACTION

Low-Cost Approaches to Mobile Data Extraction and Review

Once you've preserved the contents of a mobile device, how do you extract responsive in forms that are searchable and amenable to review? Most information items on mobile devices aren't "documents" that can be printed to a static format for review. Instead, much mobile content is fielded data that must retain a measure of structural integrity for intelligibility. This article looks at simple, low-cost approaches to getting relevant and responsive mobile data into a standard e-discovery review workflow and offers a Mobile Evidence Scorecard designed to start a dialogue leading to a consensus about what forms of mobile content should be routinely collected and reviewed in e-discovery, without the need for digital forensic examination.

In the last decade, the iPhone and other smart mobile devices have tethered us to apps and networks in powerful, unprecedented ways. Daily, the average user spends four hours on her phone spread over seventy-six sessions. For most users, smartphones are the first thing picked up in the morning and the last set down at night. Even when we aren't looking at them, smartphones receive communications, push and pull data, record our activities and broadcast our locations. Two-thirds of e-mail communications are sent and received using phones.

Over the last fifteen years, litigants have made strides in establishing defensible, repeatable procedures for preserving, collecting, processing, culling, reviewing and producing legacy paper documents, e-mail and productivity files residing on personal computers and servers, to the point that these functions have been brought in-house at many corporations and a few law firms. By contrast, few corporations and firms have acted to systemize the preservation and production of data from smartphones. Fewer still have a regime in place to address business data residing on employee-owned ("BYOD") devices. Despite being powerful, capacious computers, most lawyers and litigants treat mobile devices as if they only made phone calls. When addressed at all, smartphones are relegated to forensic examination by an expert rather than approached as a routine, repeatable process managed by e-discovery teams. Smartphones aren't "special" and, by virtue of enhanced security features on phones, there's little responsive content that can be collected through forensics that cannot also be gotten by e-discovery personnel or tech-savvy counsel. Smartphones are everyday tools that must be made a part of everyday, mainstream e-discovery.

Collection from computers could be routinized because there was consensus as to the types of information that should ordinarily be preserved, collected and reviewed. These included e-mail messages, photos, videos, and productivity formats like Word documents, Excel spreadsheets, PowerPoint presentations and PDFs. Contents of databases tended to be addressed on an *ad hoc* basis through negotiation between opposing parties.

No consensus exists as to what data must be routinely preserved and produced from mobile sources. Partly this stems from litigants' recalcitrance towards mobile evidence, and partly it's a consequence of the "special" forensic treatment accorded mobile sources. A forensic extraction seeks to recover everything: active data, latent data and deleted artifacts. "Get all you can get" is the *de facto* forensic standard, but often bears no proportionate relationship to the issues in the case. Forensic examiners endeavor to "get it all" because that's what we're trained to do, and what forensic tools are designed to do. Yet, "getting it all"—irrespective of relevance or materiality—is NOT what litigants or lawyers are obliged to do in e-discovery.

In the absence of circumstances prompting a need for digital forensics, e-discovery centers on active, readily-accessible data, not latent artifacts. Forensically-sound techniques are routinely sought to bear on

preservation; but, it's the rare matter that calls for forensic *analysis* of all sources. The cost would be unbearable were forensic analysis the norm.

So, what's our takeaway for smartphones? I'd argue that we must get the readily-accessible evidence on phones when it's relevant and responsive, but we must also strike a balance between what may be obtained through forensics versus what can be obtained using less-exacting but *reasonable and proportionate* methodologies. That is, not all we might want, but what's readily available, relevant and non-privileged considering the needs of the case.

Applying this principle, let's look at some of the data routinely found on a smartphone (and its backup) and consider potential relevance and burden issues. All the extractions and exports I'm about to describe were done using a \$50.00 program called iMazing (www.imazing.com) an easy-to-use tool that runs on both Windows and Mac machines. I like iMazing for these tasks, but there are other low-cost tools that perform admirably (See Appendix 4):

Files: Like a personal computer, phones hold word processed documents, spreadsheets, presentations and other files routinely responsive in e-discovery. Some of these items may be duplicative of other sources, but some may be unique to the phone. The burden of collecting files from mobile sources is not fundamentally different than collection from desktops, laptops, servers and cloud sources; so, unless it can be shown that documents on phones are merely duplicates of material collected elsewhere, there would seem to be no basis to eschew collection of files from mobile sources when potentially relevant.

Photos and Videos: Photographs and videos are some of the easiest items to collect from mobile sources, and phones have become the richest sources of photographic evidence. A phone may hold only a thumbnail-sized version of photos if the user, seeking to save space on the phone, configured the device to store photos in the cloud for download on demand. In that case, full resolution photos must either be downloaded to the phone before backup (if enough local storage is available) or independently collected from cloud storage. As iPhones now store photos in a High Efficiency Image File Format (with the file extension HEIC), parties collecting photos must weigh whether to collect in HEIC or convert to images JPEGs. Conversion entails loss of functionality for so-called "live" storing image sequences; but, many tools do not yet support the HEIC format.

Music and Ringtones: I've handled only two matters where a custodian's music collection was relevant to the issues in the case, and both were forensic investigations. Generally, music and ringtones won't be collected in e-discovery apart from the rare case where they have some unique relevance to the dispute. The burden to collect is small; but, the volume may be large, and music files are often rendered unusable by encryption.

Books: Like music, commercially-published books are rarely candidates for collection in discovery. Conceivably, references sources used by a key custodian and stored on the custodian's mobile device might be relevant, but that's not likely to occur with such frequency as to regard books as routine fodder for collection. Like music, books may be rendered unusable by encryption for copyright protection.

Messages: Messaging has eclipsed e-mail as the most common form of personal and business communication. Double-digit growth in messaging volume mirrors double-digit declines in e-mail usage. ***More than any other form of mobile evidence, messaging must become a source routinely scrutinized in e-discovery.*** The default message retention setting for the native messaging app on iPhones is to keep messages "forever;" so, it's

common to encounter many thousands of messages and dozens or hundreds of message threads on each device.

Messages are threaded according to the participants in the thread; consequently, you may have multiple threads including the same person in different groups of recipients as well as separate threads for the same person communicating from different devices or under different aliases (that is, by phone number or by contact name or nickname). The threading issues don't complicate collection, but they make review challenging. E-discovery veterans may note that the same challenges existed with e-mail and were solved once tools were purpose-built to deal with e-mail in discovery. Demand drove innovation for e-mail in ways that have yet to emerge for messaging.

There is little burden to collect threaded messaging stored on mobile devices, and it's trivial to export messaging in delimited formats like CSV files that can be viewed as spreadsheets. Attachments to messages can also be exported with ease, although the tools to do so may not neatly pair the attachment with its transmitting message and emoji may render as cryptic characters unless you change the encoding to Unicode UTF-8 when loading the file. It's also easy to export the threads as a text or PDF file, though so doing will severely limit the utility of the data in terms of reordering the contents of columns for sender, date, etc. Delimited formats are preferable unless the reviewer cannot use a spreadsheet or intends to (*shudder*) print the messages out. All forms will facilitate text search when ingested by an e-discovery review tool, unless the tool requires load files be generated to support even rudimentary text searches.

That last point underscores why messaging can be so simple to collect yet daunting to review: *too many review tools have failed to keep pace with important sources of electronic evidence* (like messaging or collaboration tools like Slack). It's not a preservation or collection problem. It's not even a processing problem. *All these are cheap and easy tasks*. The problem lies with culling and review.

The other big challenge to messaging is the variety of messaging channels in the marketplace. Though most people message from the native messaging app on their phones, many use proprietary and cross-platform apps like WhatsApp, Facebook Messenger, WeChat or Skype. Even Words with Friends supports texting between players!

Some of the low-cost apps capable of exporting messaging don't support specialized messaging apps as capably as they support native messaging capabilities or may not support them at all. These shortcomings don't auger for continuing to ignore messaging in discovery; however, it does require that expectations be calibrated to the limitations of the tools at your disposal and, crucially, to the reasonable expectations of the Court and opposing parties. The inability to get all the messages that may exist isn't reason to collect none but may require the use of more sophisticated tools and expert assistance to achieve quality and completeness.

Phone Call History: It's just a click or two to export a delimited file of an iPhone's call history, including contacts/phone numbers, call times, call directions (incoming/outgoing) and call durations. It's considerably less burdensome than it was to pull a paper phone call detail from a file, back when phone companies routinely supplied call details. It's far easier than logging into a cell provider's website and downloading a call history. Yet in e-discovery practice, phone call histories were only sought and produced when the call record was pertinent to a claim or defense in the cause; they weren't routinely sought simply because the information existed. Accordingly, mobile phone call history records aren't likely to be scrutinized absent a specific request and a plausible nexus between the data and the issues.

Voice Mail: Voice mail can be easily exported as a delimited CSV file showing time of call, duration, caller, number and, in some instances, a transcript of the message. The audio files for each message can also be exported in the .amr audio format, playable via QuickTime or iTunes. Unfortunately, the CSV file doesn't hyperlink to the audio files, making review a tedious process. Comparing mobile voicemail to its e-discovery antecedents, it's considerably easier to collect mobile voicemail, but it's just as challenging to review absent costly processing for message transcription or phonemic search.

Browser History and Bookmarks: Exporting browser history and bookmarks is far simpler for a mobile device as the task usually required expert assistance to collect from a personal computer but can be achieved with a few clicks from a phone backup. But, even if the data doesn't require expert intervention, is it likely to be relevant in enough matters to require routine collection? The jury is out on that, but the better approach is probably to require a specific request before routinely collecting and reviewing browser histories.

Calendar: Calendar entries for any selected interval can be exported to an iCal or CSV file format. If paper or Outlook calendars would have been reviewed in the past, then this data is easier to collect and ingest than processing a PST or photocopying years of paper calendars. The mobile calendar data is also much easier to redact.

Contacts: Another case- and custodian-specific determination as to collection and processing. All contacts or just selected contacts can be exported as a CSV file or as discrete VCards. Rudimentary text filtering before export is feasible, such as by including only contacts that include a relevant area- or zip code.

Notes: On iPhones, Notes is a no-frills word processing application akin to Windows Notepad. Some use it extensively; some not at all; but whether it holds user-generated documents relevant to the case should be routinely assessed. Single notes documents can be exported to PDF. Selected items or all Notes documents can be exported as discrete plain text files for each document, files named by date, time and first eight words of the Notes entry.

Voice Memos: As the name implies, the built-in Voice Memos app lets users record any audio to the iPhone. These can be exported, singly or collectively, as .M4A audio files and the exported files will retain the names of the source recordings. Like Voice Mail, Voice Memos are challenging to review without transcription or processing the audio for phonemic search; otherwise, there's no clear reason to distinguish a custodian's potentially responsive voice memos from memos made with Notes or other word processor in terms of preservation and collection.

Apps: Evidence that can be exported from individual apps varies as widely as the apps themselves. Although the data collected from apps comprise the customary JSON, PLIST and SQLITE files familiar to forensic examiners, apps also yield photos and documents in familiar productivity formats; the same files customarily collected when found on a user's laptop, desktop or network share. Any file can be exported easily; but, it's a manual process unaided by search or filtering features. As such, parsing all apps in this manner approaches the burden of a forensic examination without the benefit of an examiner's expertise. If a handful of apps are known to hold responsive files in intelligible formats, it's feasible and cost-effective to export potentially-responsive files one-by-one; else, it's not a scalable workflow.

File System: Though it's feasible to export most of the thousands of data and configuration files that make up the phone's file system, little of that data would be intelligible to counsel without further processing, expert

assistance and, sometimes, decryption of contents. As such, file system artifacts are probably best left to forensic investigations and won't be routinely collected and reviewed as part of routine e-discovery.

Geolocation Data: Geolocation data is relevant in many cases, even dispositive in some. Geolocation data is one of those peculiar sources of powerfully probative evidence (like e-mail stored on iPhones) that is readily accessible to a user via a few screen taps but enormously difficult to collect and review efficiently. By U.S. Federal law, any cell phone capable of making or receiving calls must broadcast its location in order to support 911 emergency response services. By default, an iPhone closely tracks a user's movements for months, recording locations visited and the times and durations of visits in its Significant Locations database. The latest version even records the length of the drive prior to arrival.

Any iPhone user can readily access their geolocation history via *Settings>Privacy>Location Services>System Services>Significant Locations*. It's trivial. But, the only way to collect this data without jailbreaking the phone and using specialized forensics software is to grab screenshots of the Significant Locations screens. That's because Apple protects this data and won't allow it to be exported. It's not backed up nor is it stored in iCloud. It's not difficult to acquire geolocation data by screenshots; it's just tedious, and data acquired by screenshots won't be text searchable or capable of being exported to mapping tools that would enhance its utility. To accomplish that, you need a digital forensics expert to acquire the recorded coordinates in a standard file format suited to geospatial data (e.g., Keyhole Markup or JSON files).

Scalability and Workflow Integration: An advantage of forensic tools is their scalability. Using X-Ways Forensics, Encase, FTK or one of the other tool suites, I can filter and search the data from dozens of hard- and thumb drive images in a single operation. I can export from some or all the images as easily and deliver the data in forms more-or-less suited for ingestion into a review platform. Phone forensics has never been scalable. I don't know of a production tool that's designed to manage simultaneous processing and analysis of dozens of phone images. If it exists, I doubt it's within the tool budgets of most forensic examiners.

The forty- or fifty buck consumer grade tools that accomplish the tasks I've just described do a mighty good job against a handful of phones and pads; but they don't scale--hardly a criticism considering that \$10,000 phone forensics tools don't either. As mobile enters mainstream discovery, the tools we employ must scale to support, not one or two devices, but dozens or hundreds of phones and pads. Still, we cannot wait for the perfect tool set to emerge. The evidence is here now, and no party should imagine a court will accept the excuse, "I didn't deal with any mobile evidence because I couldn't deal with all of it." Lawyers don't eliminate risk; we manage it. So, manage it.

The Mobile Evidence Scorecard: The information just shared are my opinions; however, they're based on experience and testing for each form of evidence listed. To distill these observations into a lay roadmap for collection and review of mobile content in e-discovery, I prepared the Mobile Evidence Scorecard. In it, I assess the burdens attendant to collection and review and the potential relevance of each source based upon existing standards in e-discovery and my years as a trial lawyer, e-discovery special master and forensic examiner. I invite different views of the criteria I used for the scorecard and conclusions I reached, asking only that the rationale for a different conclusion be shared, too. Please share better, cheaper and faster ways.



My goal is to foster consensus as to what data must be routinely preserved and produced from mobile sources. Messaging (be it called SMS, MMS, texting or instant messaging) must be every bit as mainstream and obligatory

as e-mail. Mobile photos and video must be considered in appropriate cases for both the probative value of the images and that of the embedded EXIF time and geolocation data.

We can't keep our heads in the sand on mobile simply because we've grown complacent with e-mail and documents. Evidence isn't documents anymore; it's data, and much of that evidence resides in those tiny, powerful computers in our pockets and purses. Notes content should be given a measure of the same scrutiny we devote to Word documents. Call logs, voice mail and calendar entries should all be collected and processed when they may bear on the issues. Relevant files are no less relevant because they've been stored in a pocket instead of on a server. If such evidence can be made ready for review with little skill and a fifty-dollar tool, where is the burden?

We've only to look around to see the changes wrought by mobile devices and the compelling reasons to move mobile to the mainstream of e-discovery. But honestly, who looks around anymore? We're all so busy staring at our phones.



Mobile Evidence Burden and Relevance Scorecard				
Mobile Data	Ease of Collection	Ease of Review	Potential Relevance	Routinely Collect?
 Files	Easy	Easy	Frequent	Yes
 Photos	Easy	Easy	Frequent	Yes
 Videos	Easy	Moderate	Frequent	Yes
 Music	Moderate	Difficult	Rare	No
 Ringtones	Easy	Moderate	Rare	No
 Books	Easy	Moderate	Rare	No
 Messages	Easy	Moderate	Frequent	Yes
 Phone	Easy	Easy	Case Specific	Yes
 Browser	Easy	Moderate	Rare	No
 Calendar	Easy	Easy	Case Specific	Yes
 Contacts	Easy	Moderate	Rare	No
 Notes	Easy	Easy	Frequent	Yes
 Voice Memos	Easy	Difficult	Frequent	Maybe
 Apps	Moderate	Difficult	Rare	No
 File System	Difficult	Difficult	Rare	No
 Geolocation	Difficult	Moderate	Case Specific	Maybe

Appendix 4: iPhone Backup Data Extraction Tools

There are many 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 exploration of these applications underscored that it's hard to discern which tools work well and which don't in advance of buying a license. Some promise "free evaluation copies" and "money back guarantees;" but, know that evaluation copies aren't terribly functional. The good news is, at \$30-\$50 on average for a lifetime license, you don't have to spend a lot to find a tool that meets your needs.

iMazing: \$39.99-\$279.96

The consumer-grade tool that impressed most 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 had no difficulty getting the content lawyers need most in e-discovery and, crucially, was adept at exporting the content in utile formats, including delimited CSV files for messaging and call histories.

Phone Rescue: \$49.99-\$69.99

Though slower than iMazing in my tests, Phone Rescue proved capable of doing the same tasks.

AnyTrans: \$39.99-\$59.99

You can view contents and export up to fifty items with a free trial version..

iBackup Viewer: \$39.95-\$499.95

The free version allows inspection, but you'll need to purchase a Pro license for export. A nice feature of iBackup Viewer is its ability to emulate the appearance of messages as they appear on an iPhone.

iPhone Backup Extractor: \$34.95-\$69.95

Though its interface wasn't as intuitive as iMazing's, the free "Lite" version of iPhone Backup Extractor permitted inspection of contents but, true-to-form for these tools, export required purchase of a license.

Fonepaw: \$29.95-\$99.95

FonePaw did a particularly good job on WhatsApp messaging.

These applications are just a few of the consumer-grade tools available to collect and export data from mobile devices. My testing didn't identify any one that was clearly superior to all others, and it should be noted that there were differences seen in, *e.g.*, the numbers of items identified in various categories. The key takeaway is this: ***tools capable of collecting and exporting iPhone content are plentiful, inexpensive and easy-to-use, and there are more and better options emerging all the time.***

About the Author



CRAIG BALL
ESI Special Master and Attorney
Computer Forensic Examiner
Author and Educator

3251 Laurel St.
New Orleans, LA 70115

Tel: 713-320-6066
E-mail: craig@ball.net
Web: www.craigball.com
Blog: ballinyourcourt.com

Craig Ball is a board-certified Texas trial lawyer, certified computer forensic examiner, law professor and electronic evidence expert. He's dedicated his career to teaching the bench and bar about forensic technology and trial tactics. After decades trying lawsuits, Craig limits his practice to service as a court-appointed special master and consultant in computer forensics and e-discovery. A prolific contributor to educational programs worldwide--having delivered over 2,000 presentations and papers--Craig's articles on forensic technology and electronic discovery frequently appear in the national media. For nine years, he wrote the award-winning column on computer forensics and e-discovery for American Lawyer Media called "Ball in your Court." Craig Ball has served as the Special Master or testifying expert on computer forensics and electronic discovery in some of the most challenging, front page cases in the U.S. (e.g., Enron, Madoff, In re: Seroquel, etc.).

EDUCATION

Rice University (B.A., 1979, triple major); University of Texas (J.D., with honors, 1982); Oregon State University (Computer Forensics certification, 2003); EnCase Intermediate Reporting and Analysis Course (Guidance Software 2004); WinHex Forensics Certification Course (X-Ways Software Technology 2005); Certified Data Recovery Specialist (Forensic Strategy Services 2009); Nuix Certified E-Discovery Specialist (2014); numerous other classes on computer forensics and electronic discovery.

SELECTED PROFESSIONAL ACTIVITIES

Law Offices of Craig D. Ball, P.C.; Licensed in Texas since 1982.

Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization 1988-2019

Certified Computer Forensic Examiner, Oregon State University and NTI

Certified Computer Examiner (CCE), International Society of Forensic Computer Examiners

Certified Data Recovery Specialist

Certified E-Discovery Specialist (Nuix)

Certified Cell Phone Data Recovery Specialist

Faculty, University of Texas School of Law, Adjunct Professor teaching Electronic Discovery & Digital Evidence

Faculty and Founder, Georgetown University Law Center, E-Discovery Training Academy

Admitted to practice U.S. Court of Appeals, Fifth Circuit; U.S.D.C., Southern, Northern and Western Districts of Texas.

Board Member, Georgetown University Law Center Advanced E-Discovery Institute and E-Discovery Academy

Board Member, International Society of Forensic Computer Examiners (*agency certifying computer forensic examiners*)

Member, Sedona Conference WG1 on Electronic Document Retention and Production

Member, Maryland Committee on Federal E-Discovery Guidelines, 2014- (civil and criminal committees)

Special Master, Electronic Discovery, numerous federal and state tribunals

Instructor in Computer Forensics and Electronic Discovery, United States Department of Justice

Lecturer/Author on Electronic Discovery for Federal Judicial Center and Texas Office of the Attorney General

Instructor, HTCIA Annual 2010, 2011 Cybercrime Summit, 2006, 2007; SANS Instructor 2009, PFIC 2010, CEIC 2011, 2012

Special Prosecutor, Texas Commission for Lawyer Discipline, 1995-96

Council Member, Computer and Technology Section of the State Bar of Texas, 2003-date; Chair 2015-2016

Chairman: Technology Advisory Committee, State Bar of Texas, 2000-02

President, Houston Trial Lawyers Association (2000-01); President, Houston Trial Lawyers Foundation (2001-02)

Director, Texas Trial Lawyers Association (1995-2003); Chairman, Technology Task Force (1995-97)

Member, High Technology Crime Investigation Association and International Information Systems Forensics Assn.

Member, Texas State Bar College

Member, Continuing Legal Education Comm., 2000-04, Civil Pattern Jury Charge Comm., 1983-94, State Bar of Texas

Life Fellow, Texas and Houston Bar Foundations

Adjunct Professor, South Texas College of Law, 1983-88

Recipient of Lifetime Achievement Awards from the State Bar of Texas Computer and Technology Section (2006) and the Association of

Certified E-Discovery Specialists (2016); LTN Consultant of the Year, 2009

Selected Publications available at www.craigball.com