INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

E-Discovery of Mobile Devices

C. Matthew Curtin, CISSP

Date: 2010-11-29 20:18:51

Mobile devices are increasingly common in adjudication ranging from criminal prosecution to corporate intellectual property litigation. This seminar discusses the use of electronic information in litigation broadly, with particular emphasis on data beyond documents.

After considering analytical possibilities with forensic analysis of non-document data, we focus on the issues unique to mobile devices. We start with an overview of the data available on mobile devices, how to find that mobile devices might have data of interest, and how to use mobile device data. We conclude with a case study involving intellectual property litigation centered around the use of BlackBerrys to transfer intellectual property from an old employer to a new one.

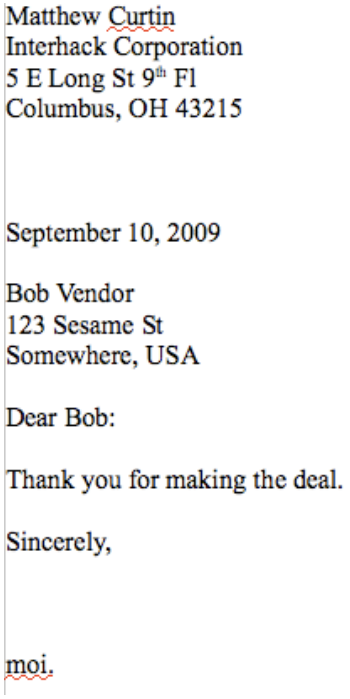
Use of Electronic Information in Litigation

Information in litigation is often best reconciled, allowing inconsistencies to be identified and explored. Historically this has required testing information against other documents or testimony. With electronic information, we have the additional ability to look for internal consistency.

Native Format: Was The Letter Backdated?

Let's consider the example of an electronic document, authored in *Word*. If we want to know the date of a document from its printout, we will typically look at a date that appears on the document and hope for the best. Such a letter might look like Figure 1.

When given access to the *Word* document itself in its *native format*, there may be additional information that is available to us. The *Word* file format is one that is designed to support the maintenance of a document, to keep track of its evolution from creation to the present. As part of meeting those design requirements, the file itself stores critical information that is not normally presented



Matthew Curtin
Interhack Corporation
5 E Long St 9th Fl
Columbus, OH 43215

September 10, 2009

Bob Vendor
123 Sesame St
Somewhere, USA

Dear Bob:

Thank you for making the deal.

Sincerely,

moi.

Figure 1: The Visible Text of an Electronic Letter

to a user unless looking specifically at document properties. There we can see information like date and time of the document's creation, when it was last printed, and when it was last modified. We can use such information to reconcile different dates and better assess the likelihood of a good printed date.

Compare the date from the visible text of our letter (shown again as Figure 2) with the dates shown in the electronic document properties (Figure 3).

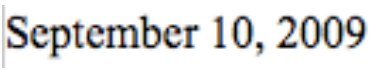


Figure 2: Date From the Visible Text

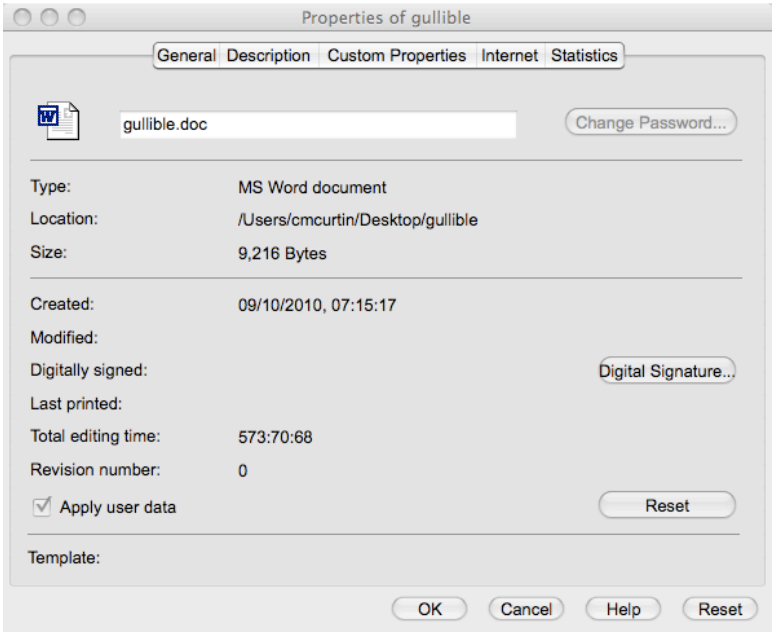


Figure 3: Document Properties of Our Letter

We can perform even more reconciliation if we are given access to the electronic mechanism used to store the *Word* document. In addition to the printed date on the document and the in-document metadata, we now have the ability to look to the *filesystem* of the storage unit. As shown in Figure 4, metadata that the filesystem maintains include the name of the file, as well as the time that the file was originally written to that place, when it was last modified, and when it was last accessed. Reconciliation of filesystem metadata with in-document metadata, and again with a printed date can help us to establish with more certainty the time of a document's creation.

In this case, we have a "printed" date of September 10, 2009, but both the electronic file and the computer storage unit place the earliest date as September 10, 2010. This may provide convincing support of the argument that the letter had been backdated.

```
  File: "gullible.doc"
  Size: 9216     FileType: Regular File
  Mode: (0644/-rw-r--r--)
                 Uid: (  501/cmcurtin)
                 Gid: (   20/   staff)
Device: 14,5   Inode: 1029258   Links: 1
Access: Sun Nov 21 17:25:41 2010
Modify: Fri Sep 10 07:40:32 2010
Change: Fri Sep 10 07:40:32 2010
```

Figure 4: Filesystem Properties of Electronic Document

Native Format: "Smoking Gun" Email?

Working with the native format of an email archive can be fruitful when looking for a message that might not be immediately visible. In many email systems, the act of "deleting" a message is merely *marking* the message in such a way that the software will not display it, except perhaps as "trash."

Additionally some "mailbox" formats (such as the Microsoft Outlook PST file) are really more than mailboxes. These are sometimes referred to as Personal Information Managers (PIM) and contain other information that can be useful especially in employment and domestic situations where contact details may be relevant.

In some cases, email or fragments of email can be recovered from working with the raw disk (or a forensic copy of the original raw disk) even when the mailbox file itself is not on the local system. These can be seen in the *unallocated* space on a storage device, as illustrated in Figure 5.

An expert will be able to work with the raw data using other tools that can retrieve and display information that might not otherwise be visible.

```
001a8970  73 73 61 67 65 20 69 6e  20 4d 49 4d 45 20 66 6f  |ssage in MIME fo|
001a8980  72 6d 61 74 2e 0a 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d  |rmat..----------|
001a8990  2d 2d 2d 2d 30 33 30 31  30 38 30 38 30 36 30 32  |----030108080602|
001a89a0  30 31 30 34 30 33 30 34  30 33 30 30 0a 43 6f 6e  |010403040300.Con|
001a89b0  74 65 6e 74 2d 54 79 70  65 3a 20 74 65 78 74 2f  |tent-Type: text/|
001a89c0  70 6c 61 69 6e 3b 20 63  68 61 72 73 65 74 3d 49  |plain; charset=I|
001a89d0  53 4f 2d 38 38 35 39 2d  31 3b 20 66 6f 72 6d 61  |SO-8859-1; forma|
001a89e0  74 3d 66 6c 6f 77 65 64  0a 43 6f 6e 74 65 6e 74  |t=flowed.Content|
001a89f0  2d 54 72 61 6e 73 66 65  72 2d 45 6e 63 6f 64 69  |-Transfer-Encodi|
001a8a00  6e 67 3a 20 37 62 69 74  0a 0a 4d 61 74 74 2c 20  |ng: 7bit..Matt, |
001a8a10  4e 69 63 6f 6c 65 2c 0a  0a 59 6f 75 72 20 63 6f  |Nicole,..Your co|
001a8a20  6e 66 69 67 20 69 73 20  72 65 61 64 79 20 2d 20  |nfig is ready - |
001a8a30  77 65 20 77 69 6c 6c 20  6e 65 65 64 20 61 62 6f  |we will need abo|
001a8a40  75 74 20 31 2f 32 20 68  6f 75 72 20 74 6f 20 63  |ut 1/2 hour to c|
001a8a50  6c 65 61 72 20 79 6f 75  72 20 72 6f 6f 6d 20 2d  |lear your room -|
001a8a60  20 0a 6d 61 6b 65 20 69  74 20 6e 69 63 65 2e 0a  | .make it nice..|
001a8a70  0a 50 6c 65 61 73 65 20  6c 65 74 20 6d 65 20 6b  |.Please let me k|
001a8a80  6e 6f 77 20 74 68 65 20  72 65 76 69 73 65 64 20  |now the revised |
001a8a90  73 74 61 72 74 20 64 61  74 65 20 61 73 20 73 6f  |start date as so|
001a8aa0  6f 6e 20 61 73 20 70 6f  73 73 69 62 6c 65 0a 0a  |on as possible..|
001a8ab0  54 68 61 6e 6b 73 2c 0a  0a 53 74 65 76 65 0a 0a  |Thanks,..Steve..|
001a8ac0  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 30 33  |--------------03|
001a8ad0  30 31 30 38 30 38 30 36  30 32 30 31 30 34 30 33  |0108080602010403|
```

Figure 5: "Hexdump" View of Raw Email Data Recovered from Unallocated Space

Native Format: What About That Picture?

Like documents, images have a primary purpose to be seen and interpreted by a human. Like electronic documents, electronic images often have additional information embedded in them.

Consider the photo in Figure 6. Clearly it's a picture of Huntington Park in downtown Columbus. What else can we determine about the picture? A look at the in-file metadata (Figure 7) shows additional information. We can see the make and model of the camera as well as the date and time that the picture was taken. In addition, this particular file also has the location encoded in the image.[1]

Figure 6: Photo From the Ballgame

[1] Location information comes from the camera phone's embedded Global Positioning System (GPS) reader. (See http://www.gps.gov/.) These are common in camera phones, and are increasingly common in other digital cameras from Nikon, Ricoh, Panasonic, Samsung, and others.

Date Time: 2010:04:30 19:30:22
Make: Research In Motion
Model: BlackBerry 8530
Orientation: 1 (Normal)
Resolution Unit: inches
Software: Rim Exif Version1.00a
X Resolution: 72
Y Resolution: 72
Altitude: 195 m (639.8 ft)
Latitude: 39° 58′ 9" N
Longitude: 83° 0′ 41.64" W
Speed: 0
Track: 340.66

Figure 7: Ballgame Photo In-File Metadata

Figure 8 shows the picture's coördinates on a map. Given altitude, latitude, and longitude, we can even determine from which seat I took the picture.

Working with reproductions of the pictures will allow for the content of the photo itself to be visible, but other information—potentially critical information—would be needlessly lost without bothering to look at the file in its native digital form.

Now that we have taken a look at several applications of digital information on computing systems generally, we can focus more specifically on mobile devices. In many ways, our understanding of digital information can be helpful, but mobile devices present a variety of unique opportunities and challenges.

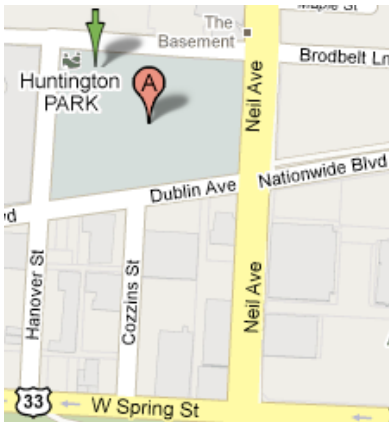


Figure 8: Location of Coördinates in Photo Map: Google Maps

Data on Mobile Devices

Before we can get to the data on mobile devices, we need to understand how mobile devices store information. We'll look first at the *hardware*, the physical mechanism for data storage, and how the data are formatted.

Hardware: Where Is This Stuff?

Components of mobile devices are much the same as in common computing devices. These are typically made up of input/output, computing, and storage. In this discussion we focus largely on storage.

We find a typical BlackBerry smartphone in Figure 9. We can see that the device has a camera visible in back, and a button to remove the back cover. Once we remove the back cover as in Figure 10 we reveal the battery. Removing the battery reveals the location for additional storage, known sometimes as the *memory card*, sometimes called a *media card*.

Memory cards come in a variety of capacities, interfaces, and sizes. Three sizes are depicted in Figure 11. From left to right, these are the CompactFlash (abbreviated as "CF"), Secure Digital (SD), and MicroSD. The MicroSD card is about the size of a fingernail.

The oldest of the formats is CF, and was designed for use in electronic devices such as digital cameras. More recent devices tend to use SD and MicroSD standards. The BlackBerry uses MicroSD.

Figure 9: The front and back of a typical BlackBerry.

Figure 10: Opening the BlackBerry.

Figure 11: Memory Cards
Photo: Evan Amos

Many devices use cards such as this, and may store information material to litigation. In addition to digital cameras and phones mentioned earlier, devices that use these memory cards include digital camcorders, computers, personal digital assistants (PDAs), portable media players, GPS readers, and video game consoles.

Mobile devices with access to mobile telephone networks may also have a removable card known as the Subscriber Identity Module (SIM). In addition to the identification and authentication information needed to use the mobile network, SIM cards can store information such as address books and text messages.

Figure 12 shows how opening another BlackBerry model and removing its battery reveals the SIM card. The top side shows manufacturer and identifying information. The underside is where the contacts are for interfacing with the device.

Figure 12: Finding the SIM Card in a BlackBerry

Common Properties of Data on Mobile Storage Media

In almost all cases, devices use these memory cards as they would a disk for storage: the media cards are formatted with a filesystem. That means not only do we have the files of interest, but the filesystem properties that we can associate with them, just as we did back when trying to assess whether a document was back-dated on page 2. Thus analysis of the storage can help us to understand things like when the device was in use.

Data not unique to mobile devices that are often found on them and could prove useful to analyze may come in many different formats. We describe some here. This list is not meant to be exhaustive, but to indicate some of the more common file formats, particularly for multimedia content that can be pertinent to an investigation but not easily "searchable" as documents.

JPEG Still image format, suitable for photos, by the Joint Photographic Experts Group.[2] These are typical on consumer digital cameras for still images. These allow for high color and high resolution, while also using *compression* to reduce the size of the corresponding file.

TIFF Still image format. This format allows for high resolution without compression.[3] Commonly available on higher-end digital cameras. Many of these cameras also offer a "raw" format for image storage, one that varies from one manufacturer to another.

[2] William B. Pennebaker and Joan L. Mitchell. *JPEG still image data compression standard*. Van Nostrand Reinhold, New York, NY, USA, 1992. ISBN 0-442-01272-1

[3] Adobe Developers Association. *TIFF Revision 6.0: Final*. Adobe Systems Incorporated, 1585 Charleston Road P.O. Box 7900 Mountain View, CA 94039-7900, June 1992. URL http://partners.adobe.com/asn/tech/tiff/specification.jsp;http://home.earthlink.net/~ritter/tiff/(TheUnofficialTIFFHomePage). Includes TIFF Specification Supplement 1 (enhancements for Adobe PageMaker 6.0) [14-Sep-1995] and TIFF Specification Supplement 2 (enhancements for Adobe Photoshop) [22-Mar-2002]. Hypertext linked for Web access

MPEG Format for multimedia applications including audio and video.[4]

QuickTime Apple's own multimedia standard, common on but not exclusive to Macintosh machines.[5]

Windows Media Microsoft's multimedia standard, common on but not exclusive to Windows machines.[6]

Specific capabilities of mobile devices and the data on them will vary wildly from one sort of device to another. We will consider several of the more common types of information.

Data Common to Mobile Phones

Some examples of datasets available on almost all phones irrespective of make and model include the *call log*, the *phone book*, and SMS data.

Call Log Mobile phones will typically keep a record of calls recently sent and received. These records can be incomplete and may be configured to store only the recent past, but that can be a start, and could also have just the information that you're looking for.

Phone Book Using the Phone Book to put names with numbers can be invaluable when attempting to understand how different parties are communicating with one another. Not only can names be put with numbers, but numbers can be associated together, showing someone's home and work numbers, for example.

SMS The short message service was developed originally to work with mobile telephone networks. The technology dates back to the mid 1980s and has been widely deployed along with the rest of mobile telephony infrastructure.[7] Thus these messages are often more native to the device than add-on application such as email. This tends to make SMS more common, as well as able to have its data stored in places that other data cannot be stored, such as on a SIM card.

[4] Didier Le Gall. MPEG: a video compression standard for multimedia applications. *Communications of the ACM*, 34(4):46–58, April 1991. ISSN 0001-0782. URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/103090.html

[5] Andrew W. Davis and Joe Burke. The Mac goes to the movies: A detailed look at Apple's QuickTime architecture. *Byte Magazine*, 18(2): 225–??, February 1993. ISSN 0360-5280

[6] Mingzhe Li, Mark Claypool, Robert Kinicki, and James Nichols. Characteristics of streaming media stored on the Web. *ACM Transactions on Internet Technology (TOIT)*, 5(4): 601–626, November 2005. ISSN 1533-5399

[7] F. Hillebrand, F. Trosby, K. Holley, and I. Harris. *Short Message Service (SMS): The Creation of Personal Global Text Messaging*. John Wiley & Sons, 2010. ISBN 9780470688656. URL http://books.google.com/books?id=YPgfNaoYHUsC

Additional Data

Once we get access to the data, we need to make sense of it. In many cases, assessment of the data is as simple as extracting the text from the data. In other cases, analysis of the data structure is necessary to determine how even to read the data.

How much additional information can be found will depend on the make and model of the phone, as well as the level of access the analyst has to it. If the storage unit can be removed from the phone, reading the unit in its entirety is straightforward—usually. More secure devices such as the BlackBerry have options for strong encryption of the data stored on such media.

Any time that cryptography is protecting data on a storage media, the *key* needed to "unlock" the data will be required. Typically the key is computed as a result of a passphrase or code controlled by the user of the device.

Finding Mobile Device Data

Intuition suggests that we cannot analyze devices that we do not have. In the most strict sense, this is true. Access to the device is the best way to perform analysis, giving us the ability to perform physical inspection of the unit; thus we can see if anything, such as a USB port is broken. In addition, of course, we can recover whatever data might be available on memory and SIM cards.

Finding these devices and their storage media is often just a matter of asking. As usual, though questions need to be precise and asked carefully.

Asking in interrogatories and deposition

Questions such as these will help to identify the scope of possibly-relevant devices for a particular person, and then provide insight on how the device might relate to the present legal action. Understanding the device's use can help us to understand the information most likely found there, thus focusing our attention on the best places to look to reduce waste and needless intrusion.

Explanatory text is *italicized* in this section; standard text indicates an interrogatory to be put before the device custodian.

1. *First, identify all possibly-relevant devices.*

   People tend to think about "computers" pretty consistently and can be expected to respond accordingly. Asking for a "mobile device" is unlikely to get the same consistency of response, so enumerating phones, BlackBerrys, iPhones, PDAs, tablet computers,

iPads, eBook readers, and so on can help to disambiguate. As these devices can frequently change, asking specific questions about duration of usage can help to identify which devices are most likely to have the needed information.

(a) Do you have a mobile phone? PDA? Tablet computer?
(b) What did you have before this device?
    i. Where is that device now?
(c) Do you use other devices that you use concurrently?

2. *Next, go through each device in the list to find out how it might be relevant.*

   Like computers, these systems have many functions. Understanding how they are used will go a long way toward helping to identify the relevant devices and the data likely to be encountered.

   (a) Are you the only one who uses the device?
   (b) What do you do with the device?
       i. How long have you had it?
       ii. Are you presently using the device?
       iii. How often do you use it?
       iv. Do you use it to communicate with others?
           A. Email?
              Email in particular can have many different configuration options. In some cases, the email will be stored on a central server, leaving little information on the device itself. In other cases, the entirety of the mailbox you need will be stored on the device. Best to ask how the email works, and where the messages are stored.
           B. Chat or Instant messages?
              There are many options for instant messages available. Google, Yahoo!, and AOL Instant Messager, for example, all have software that can run on smartphones that allow or real-time back-and-forth short messages. In addition, devices such as the BlackBerry will have their own instant message systems. Finally, in some corporate environments, there may be a central server where those messages are archived.
           C. Text messages?
              Most mobile phones now can work with text messages, also known as Short Message Service (SMS). Some phones also support an extension that allows for file transfer, Multimedia Message Service (MMS).

D. Voice?
Not all mobile devices are phones. But some devices that aren't phones can support voice communication through services such as Skype.

E. Video?
Some mobile devices can now support video conference service. Apple's iPhone has an application known as FaceTime, and Skype video is also available for some devices.

v. Is it on a mobile telephone network?
This might already be established through earlier responses but in any case we will want the additional detail.

A. Which provider?
At some level, a matter might require going back to a provider for records of calls or other communications. We will want to know which provider.

B. Has it always been on that provider?
The lifespan of a device might be greater than the lifespan of the service contract that keeps the system online. We might have several providers to subpœna for the right information.
If no, what process did you go through to change providers? Did you switch SIM cards? Where is the old SIM card now?

vi. Do you create content on it?
For many people these devices are "read-only." eBook readers, in particular, are designed for a reader, and offer little or no mechanism for annotation or other input. Some devices such as a BlackBerry anticipate more equal amounts of reading and writing. Tablet computers such as the iPad can comfortably handle both but may not be used that way. Understanding how the system is used (for reading, writing, or both) will help us quickly to eliminate from consideration devices that are unlikely to be fruitful.

A. Documents?
While full-scale documents might not be originally authored on the device, it's possible that they are annotated or edited on the device. There are various options for working with Word documents, for example.

B. Digital photos?
Photographic evidence as well as metadata showing usage may prove material.

C. Digital videos?
These can be like photos.
D. Pictures?
Other graphics may be created, e.g., drawn.
E. Music?
Many devices also function as digital music players.
F. Voice notes?
Devices such as the BlackBerry offer an option for the built-in microphone to be used to record voice notes. These can be useful when text annotation is impossible, when making a note between phone calls on the road.

Analysis of the physical unit is not the only option. In some cases, the device is not available, but we may be able to get some useful information by performing analysis of computer systems to which the mobile device has been connected.

Looking at other available data sources

When mobile devices like telephones are connected to computers, traces are often left behind. In some cases we can retrieve the information that the device presents to the operating system for identification—commonly make, model, and serial number. In other cases, we can get very detailed information, including specific content from the device, as if we had the device itself in-hand.

The most common case for connecting a mobile device is through a USB interface. When that connection is made in most computers, a record is made of the device being connected to the computer. Along with the identifying information is a date showing when the device was most recently connected to the machine. Thus, when looking to see how a mobile device might have been used to get access to data, we can begin our analysis at the computer where the device was most likely connected, such as a laptop or company-issued desktop computer. Obviously, performing this kind of analysis ahead of a deposition can be useful for ensuring that all devices and their usage is well-understood.

Even more information—a complete copy of all data available on a phone—may be available if the custodian uses an application like *BlackBerry Desktop Manager* to make a backup or to "sync" the computer data with the mobile device. We will focus on the BlackBerry in particular for this example to provide background to consider a case study later.

BlackBerry Desktop Manager offers several features to users who want to avoid losing their data in the event of loss of a device or

its function. The most critical of these are "backup" and "restore." The software is available for both Mac (Figure 13) and Windows (Figure 14) systems.

When the user makes a backup of the device, *BlackBerry Desktop Manager* identifies each of the databases on the device and downloads each one in turn to the local disk (Figure 15). All of the databases are stored in a single file that can be interpreted. In this particular case, this backup process is precisely the same as making a copy of the device using a utility for forensic analysis. Unless the user opts to encrypt the resulting backup file, all of the data on the phone is thus directly available for analysis as if the phone were available—though media files stored on the memory card will not be included.

Specifics of what is available will vary from case to case, but the copied data can be quite complete, including call log, SMS messages, address book, browsing history, email contents, calendar, chat messages, and history of applications for getting directions.

Figure 13: *BlackBerry Desktop Manager* for Macintosh

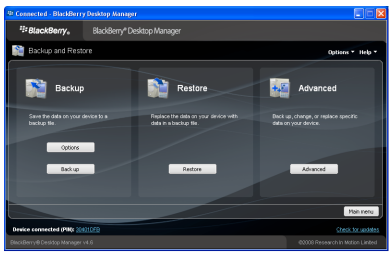


Figure 14: *BlackBerry Desktop Manager* for Windows

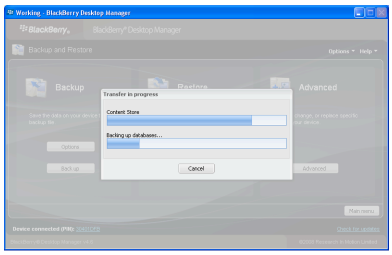


Figure 15: Making a Backup of a Phone With *BlackBerry Desktop Manager* for Windows

Using Mobile Device Data

With their relatively limited storage and processing capability, mobile devices are typically more subject to the volatility of temporal data. Simply stated, these devices can store less than larger computers, and consequently do not keep information as long as those computers. Thus, preservation of the data that might be material often has heightened urgency.

If mobile devices need to be brought into scope, they need to be identified quickly, preserved without delay, and preservation should take care to include whatever information could be deemed relevant. Taking the device into custody and holding it in a safe may not be sufficient—if a proceeding drags on for days, weeks, and months, the memory on a device that is not powered up can be lost.

Proper preservation might include duplication of the device itself, duplication of memory cards, and SIM cards. Options vary from one device to another, and needs vary from one case to another.

Due in part to the limited storage capacity of the smaller devices, extraction and production of data from those devices can be more straightforward. Data can often be formatted for review on a standard computer with no fancy or unusual software, though counsel will likely have to work with an expert to understand what can and cannot be properly read into the data.

One note of particular importance: some tools, even those for "forensic" purposes show only the data that they know how to interpret. Working with an expert who can tell you whether other sets of data are on the device may prove critical if applications related to the issues in the litigation are installed on the device. In some cases, we have extracted text from datasets of unknown format that can provide just the right piece of information for reconciliation with other datasets or for questioning in deposition.

Study of a case from my practice demonstrates how electronic discovery of mobile devices can lead to a powerful conclusion.[8]

[8] The case is real but identifying details have been changed as various agreements in the action are still in effect.

Case Study: Transfer of Intellectual Property

Mr. S was a sales agent for his firm, and a partial owner. When he resigned, the firm saw the need to ensure that its proprietary information, including customer list, remained under its control. When Mr. S joined a competitor the need became urgent. The firm had in its possession the computer he used while employed there as well as his BlackBerry, which the firm thought had been *wiped*.

I received the BlackBerry[9] and confirmed that it had been wiped—no information was available on the device. As is true on some mobile devices, the BlackBerry has a feature that will securely destroy the data on the device. This helps to keep the data safe even if the device is being sold to another party or is lost. The wipe can be activated either locally by selecting the option to do so from a menu, or in certain configurations from a central location such as a corporate IT department. In this case, the wipe Mr. S initiated also denied the firm the ability to review the last actions on the company-issued mobile device.

[9] We typically would seek to analyze the computer he used when employed by the plaintiff but we did not in this case due to technical specifics of the plaintiff's computing environment.

The firm initiated a lawsuit against the competitor, Mr. S and another former employee who followed Mr. S to the competitor. The firm sought a Temporary Restraining Order to prevent the former employees from using any of the firm's proprietary information for the benefit of the competitor. Counsel for the firm also issued a subpœna for Mr. S' home computer.

The TRO was granted. Counsel for the parties agreed upon a Protective Order wherein any of the defendants' information would be protected by requiring that I, as expert for the plaintiff, produce my findings first to defense counsel for any redaction before production to plaintiff's counsel.[10]

[10] This is a procedure we commonly suggest where there are competing interests in the data. Typically I will become party to the Protective Order and then follow the procedure such that opposing parties may be satisfied that their information is being protected from one another.

Mr. S was being deposed on Monday; on that afternoon we received his home computer for analysis. In the deposition, counsel discovered that Mr. S bought a new BlackBerry. We created an *image* of the computer's hard drive[11] and an inventory of the files on the drive on Tuesday. That inventory drew our attention to two files in particular, shown here in Figure 16.

[11] An exact duplicate of the disk, sometimes also known as "bit copy" or "forensic image."

```
Documents and Settings/Owner/My Documents/
    Backup-(2010-01-07).ipd
    Backup-(2010-03-09).ipd
```

Figure 16: Two BlackBerry Desktop Manager Backup Files Identified

We turned our attention to these backup files. The format of the file name, `Backup-(YYYY-MM-DD).ipd`, is consistent with the naming scheme used by the Windows edition of *BlackBerry Desktop Manager*. Comparison of the filesystem's attribute for storing time of file creation showed that the files were created on the dates indicated in the filenames.

Contacts databases for the backups seemed of particular interest.[12] The January backup had 145 entries in the Contacts database. March's backup had 4,241 entries in the Contacts database. Data extracted from the BlackBerry backup files were formatted for defense counsel's review.

[12] The BlackBerry Contacts database is different from the phone's Address Book.

Thursday morning, we produced the file inventory, extracted BlackBerry data, and our Initial Assessment Report of the hard drive to defense counsel for review, per the Protective Order. Friday afternoon, we received instructions for redaction from defense counsel: remove communications with counsel and passwords. We performed the redaction as instructed and sent the remainder of our findings along to plaintiff's counsel marked ATTORNEYS' EYES ONLY, per the Protective Order.

On the next Monday, we received Mr. S' new BlackBerry and analyzed it. Its Contacts database contained 4,226 entries. That extraction was also sent to defense counsel for review. On Tuesday we compared the Contacts database from the new BlackBerry with the Contacts database from the March backup and found 4,168 exact matches. Visual inspection of differences showed that many of the "non-matching" records were actually just corrections for items such as the format of a phone number.

We then turned our attention back to the March backup file—of which device? A personal BlackBerry? The work BlackBerry that had been wiped? BlackBerry devices are identified with a PIN—it's not a user's secret code, but something akin to the device's serial number. Helpfully, the Macintosh version of *BlackBerry Desktop Manager* provides this information in the backup filename itself,

but the Windows edition stores only a type of backup (full or partial) and a date, as shown in Figure 16 above.

In the March backup file we found a database supporting the *BlackBerry Messenger* application—a BlackBerry-specific instant messaging application. In that database was the PIN of the device from which the backup came. It was clearly different from Mr. S' new BlackBerry, so the contacts were on another BlackBerry before they were on the new device. Although the other BlackBerry had been wiped, we still had system information available and were thus able to compare the PIN of the old device to the March backup. *Voilà!*

With this, we were able to establish:

1. Mr. S maintained his contacts in his BlackBerry device, the one that had been wiped and rendered unreadable to his former employer;
2. Mr. S made a backup of his employer's BlackBerry on his home computer approximately one month before quitting his job and going to work for a competitor;
3. Mr. S used the backup of the data from his old employer's BlackBerry to load to his new BlackBerry; and
4. Mr. S continued to maintain and update the contacts database as seen on his new BlackBerry.

I drafted a Declaration on Tuesday and arrived in court Wednesday morning, prepared to testify at the preliminary injunction hearing. As I sat in the gallery with both phones and my documentation, the parties went into a settlement conference. Negotiations continued throughout the day, and the hearing was rescheduled for one week later. Negotiations still incomplete, I appeared again and waited to testify. This time, a settlement was reached.

Mr. S is prevented from using any of those contacts for a period of time, and all new contacts that he establishes must pass through an approval mechanism agreed by counsel for the parties to ensure that no contacts in the plaintiff's contact database are reached for a period of time.

Lessons Learned

Key lessons from this discussion include:

1. Electronic information contains more than meets the eye;
2. Unseen information, metadata, provide powerful tools for identifying and understanding relevant information;
3. Mobile devices present both challenges and opportunities in litigation;
4. Mobile devices may store information of interest in several places, including in its own memory and in cards that plug into the device;
5. Depositions and interrogatories can provide valuable information about how mobile devices are used and how their data should be understood;
6. The most effective analysis of mobile devices can include analysis of other devices and their interplay;
7. Through reconciliation and the tying together of loose ends what begins as a murky problem can have a clear and concise definition; and
8. Good technical analysis must be supported by good lawyering.

Bibliography

Adobe Developers Association. *TIFF Revision 6.0: Final*. Adobe Systems Incorporated, 1585 Charleston Road P.O. Box 7900 Mountain View, CA 94039-7900, June 1992. URL http://partners.adobe.com/asn/tech/tiff/specification.jsp;http://home.earthlink.net/~ritter/tiff/(TheUnofficialTIFFHomePage). Includes TIFF Specification Supplement 1 (enhancements for Adobe PageMaker 6.0) [14-Sep-1995] and TIFF Specification Supplement 2 (enhancements for Adobe Photoshop) [22-Mar-2002]. Hypertext linked for Web access.

Andrew W. Davis and Joe Burke. The Mac goes to the movies: A detailed look at Apple's QuickTime architecture. *Byte Magazine*, 18(2):225–??, February 1993. ISSN 0360-5280.

F. Hillebrand, F. Trosby, K. Holley, and I. Harris. *Short Message Service (SMS): The Creation of Personal Global Text Messaging*. John Wiley & Sons, 2010. ISBN 9780470688656. URL http://books.google.com/books?id=YPgfNaoYHUsC.

Didier Le Gall. MPEG: a video compression standard for multimedia applications. *Communications of the ACM*, 34(4):46–58, April 1991. ISSN 0001-0782. URL http://www.acm.org/pubs/toc/Abstracts/0001-0782/103090.html.

Mingzhe Li, Mark Claypool, Robert Kinicki, and James Nichols. Characteristics of streaming media stored on the Web. *ACM Transactions on Internet Technology (TOIT)*, 5(4):601–626, November 2005. ISSN 1533-5399.

William B. Pennebaker and Joan L. Mitchell. *JPEG still image data compression standard*. Van Nostrand Reinhold, New York, NY, USA, 1992. ISBN 0-442-01272-1.