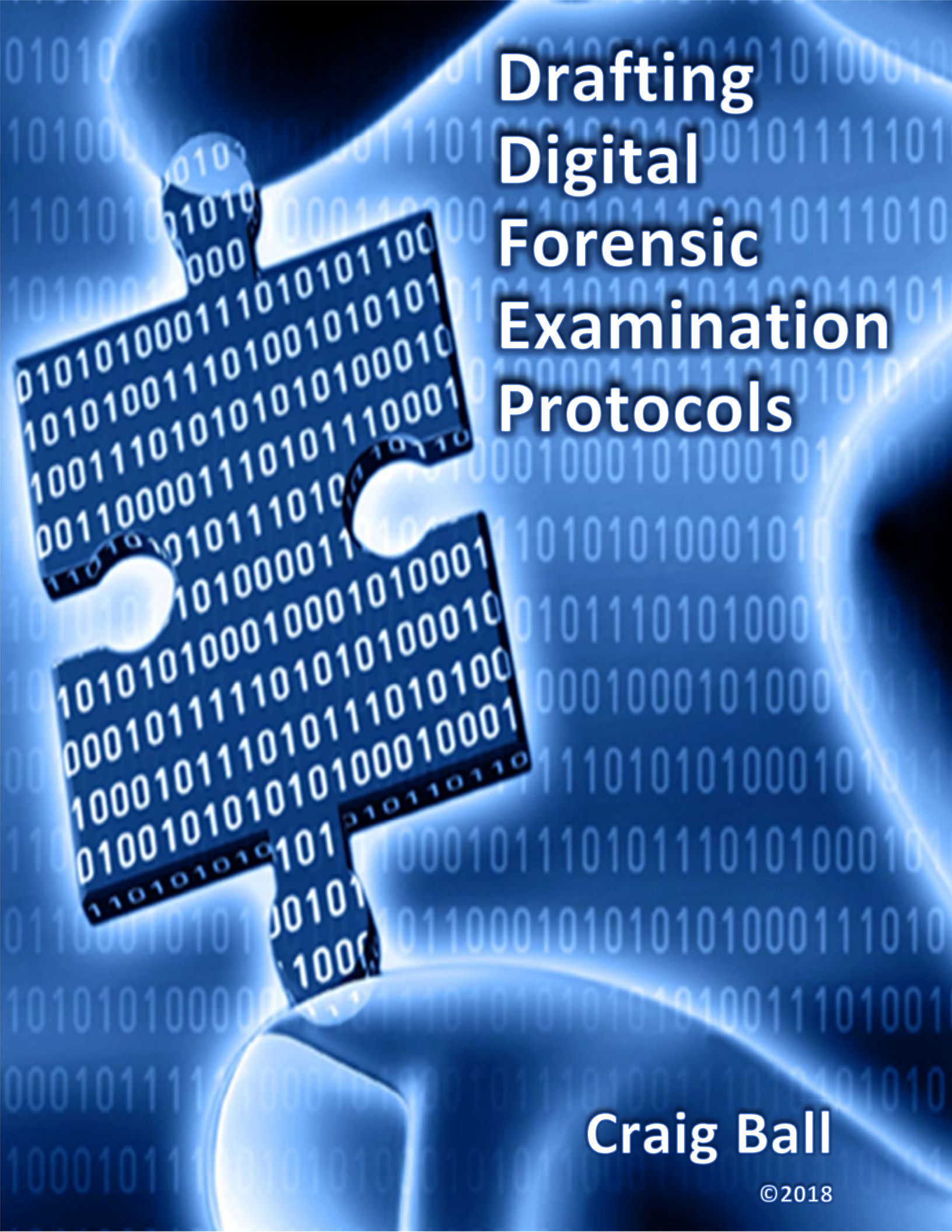
Drafting
Digital
Forensic
Examination
Protocols
Craig Ball
©2018

Drafting Digital Forensic Examination Protocols

By Craig Ball ©2018

A computer or smart phone under forensic examination is like a vast metropolis of neighborhoods, streets, buildings, furnishings and stuff--*loads* of stuff. It's customary for a single machine to yield over a million discrete information items, some items holding thousands of data points. Searching so vast a virtual metropolis requires a clear description of what's sought and a sound plan to find it.

In the context of electronic discovery and digital forensics, an examination protocol is an order of a court or an agreement between parties that governs the scope and procedures attendant to testing and inspection of a source of electronic evidence. Parties and courts use examination protocols to guard against compromise of sensitive or privileged data and insure that specified procedures are employed in the acquisition, analysis, and reporting of electronically-stored information (ESI).

A well-conceived examination protocol serves to protect the legitimate interests of all parties, curtails needless delay and expense and forestalls fishing expeditions. Protocols may afford a forensic examiner broad leeway to adapt procedures and follow the evidence, or a protocol may tightly constrain an examiner's discretion to defend against waiver of privilege or disclosure of irrelevant, prejudicial material. A good protocol helps an examiner know where to start his or her analysis, how to proceed and, crucially, when the job is done.

As a litigator for over 35 years and a computer forensic examiner for more than 25 years, I've examined countless devices and sources for courts and litigants. In that time, I've never encountered a forensic examination protocol of universal application. "Standard" procedures change over time, adapted to new forms of digital evidence and new hurdles--like full-disk encryption, solid-state storage and explosive growth in storage capacities and data richness. Without a protocol, a forensics examiner could spend months seeking to meet an equivocal examination mandate. The flip side is that poor protocols damn examiners to undertake pointless tasks and overlook key evidence.

Drafting a sensible forensic examination protocol demands a working knowledge of the tools and techniques of forensic analysis so counsel doesn't try to misapply e-discovery methodologies to forensic tasks. Forensic examiners deal in artifacts, patterns and configurations. The data we see is structured and encoded much differently than what a computer user sees. The significance and reliability of an artifact depends on its context. Dates and times must be validated against machine settings, operating system functions, time zones and corroborating events.

Much in digital forensics entails more than meets the eye; consequently, simply running searches for words and phrases "e-discovery-style" is far less availing than it might be in a collection of documents.

If you can conceive of taking the deposition of a computer or smart phone, crafting a forensic examination protocol is like writing out the questions in advance. Like a deposition, there are basic inquiries that can be scripted but no definitive template for follow-up questions. A good examiner--of people or computers--follows the evidence yet hews to relevant lines of inquiry and respects boundaries. A key difference is, good advocates fit the evidence to their clients' narrative where good forensic examiners let the evidence tell its own story.

If you've come here for a form examination protocol, you'll find it; but the "price" is learning a little about why forensic examination protocols require certain language and above all, why you must carefully adapt any protocol to the needs of your case.

Common Elements

Though each is unique, examination protocols share common elements. They should, *inter alia*:

- Identify the examiner (or the selection process) and the devices and media under scrutiny;
- set the scope of the exam, temporally and topically;
- Insure integrity of the evidence;
- Detail the procedures and analyses to be completed;
- Set deadlines and reporting responsibilities;
- Require cooperation; and,
- Assign payment duties.

Protocols typically set out the goals of the exam and articulate the rights sought to be protected. As needed, a protocol should address the who, what, when and where of access to devices or media and the conditions under which acquisition and examination will occur. A proper chain of custody is mandated, as well as who may be present when data is acquired or processed.

Identify the Examiner

If the parties or the Court haven't settled on who will conduct the examination, the protocol should detail the examiner's required qualifications and/or the selection process. The protocol should make clear whether the examiner is working for a party or serving as a neutral.

If a neutral will perform the exam, ideally the parties will agree upon a qualified person. When they cannot, the protocol might require each side to submit proposed candidates, including their *curriculum vitae* and a list of other matters in which the examiner candidates have served as court-appointed neutrals. The Court then reviews the CVs for evidence of training, experience, credible professional certification and other customary indicia of expertise in selecting its appointee.

> **Exemplar language:** *The parties have until [DATE] to agree upon a computer forensic examiner ("Examiner") who will inspect and analyze the electronic devices and media pursuant to this Protocol. If the parties fail to agree on an Examiner, they shall submit two names each to the Court with a summary of the proposed Examiners' qualifications and experience, not to exceed one page each, and each Examiner's fee structure. The Court will select an Examiner from among the candidates submitted. The Examiner will serve as an officer of the court, agree to submit to the jurisdiction of this Court and be bound by the terms of this Protocol.*

Identify the Devices and Media

A forensic examination protocol should clearly define what devices and media must be tendered for acquisition and analysis. Designations may be as specific as "*Dell Inspiron laptop computer Service Tag XYZ123*" or as broad as "*all computers, cell phones and electronic data storage devices (thumb drives, external hard drives and the like) in the care custody or control of John Doe*."

Forensic examinations routinely turn up evidence pointing to the existence of other potentially relevant devices and storage media. This triggers mistrust and charges of concealment or spoliation. Accordingly, the parties should discuss the potential for other devices to turn up and draft the examination protocol to address whether such items fall within the scope of the examination.

Set the Scope of Examination

As noted, there is no more a "standard" protocol applicable to every forensic examination than there is a "standard" set of deposition questions applicable to every matter or witness. In either circumstance, a skilled examiner tailors the inquiry to the case, follows the evidence as it develops and remains flexible enough to adapt to unanticipated discoveries. Consequently, it is desirable for a court-ordered protocol to afford the examiner some discretion to adapt to the evidence and apply their expertise.

In framing a forensic examination order, it's helpful to set out the goals to be achieved and the risks to be averted. By using an aspirational statement to guide the overall effort instead of directing the details of the expert's forensic activities, the parties and the court reduce the risk of a costly, wasteful exercise. To illustrate, a protocol might state: "*The computer forensic examiner should, as feasible, recover and produce from Smith's computer, phone and storage media tendered for examination all e-mail communications between John Smith and Jane Doe, but without revealing Smith's personal confidential information or the contents of privileged attorney-client communications to any person other than Smith's counsel.*"

The court issued a clear, succinct order in **Bro-Tech Corp. v. Thermax, Inc., 2008 WL 724627 (E.D. Pa. Mar. 17, 2008)**. Though it assumed some existing familiarity with the evidence (*e.g.*, referencing certain "Purolite documents"), an examiner should have no trouble understanding what was expected:

> *(1) Within three (3) days of the date of this Order, Defendants' counsel shall produce to Plaintiffs' computer forensic expert forensically sound copies of the images of all electronic data storage devices in Michigan and India of which Huron Consulting Group ("Huron") made copies in May and June 2007. These forensically sound copies are to be marked "CONFIDENTIAL--DESIGNATED COUNSEL ONLY";*
>
> *(2) Review of these forensically sound copies shall be limited to:*
> *(a) MD5 hash value searches for Purolite documents identified as such in this litigation;*
> *(b) File name searches for the Purolite documents; and*
> *(c) Searches for documents containing any term identified by Stephen C. Wolfe in his November 28, 2007 expert report;*
>
> *(3) All documents identified in these searches by Plaintiffs' computer forensic expert will be provided to Defendants' counsel in electronic format, who will review these documents for privilege;*
>
> *(4) Within seven (7) days of receiving these documents from Plaintiffs' computer forensic expert, Defendants' counsel will provide all such documents which are not privileged, and a privilege log for any withheld or redacted documents, to Plaintiffs' counsel. Plaintiffs' counsel shall not have access to any other documents on these images;*

(5) Each party shall bear its own costs;

Of course, this order keeps a tight rein on the scope of examination by restricting the effort to hash value, filename and keyword searches. Such limitations are appropriate where the parties are seeking a small population of well-known documents but would severely hamper a less-targeted effort. It bears mention that the *Bro-Tech* protocol was barely a forensic examination as it focused exclusively on active data, not forensic artifacts. As such, it's a poor template for a deeper inquiry.

Set the Temporal Scope

Parties routinely seek to impose time constraints on a forensic examination in terms of what data the examiner should search. While limiting an examiner to review of information in a relevant interval may seem wise, it's often infeasible and serves to frustrate the ends of the exam. No forensics tool can limit a search of unallocated clusters and forensic artifacts to a date range. There are few temporal guideposts for forensic artifacts because date information is usually absent or may be unreliable. Even for active data, there won't always be metadata in the master file table to support a reliable time limitation.

For example, log files contain information pertaining to dates other than the dates of the log files themselves. Excluding log files based on their file dates serves to prevent scrutiny of temporally-relevant log entries. Moreover, file metadata misleads those who don't fully understand its significance. A file's creation date often bears no relation to the date the file's contents were authored. A file's last modified date may relate to events outside a relevant interval although the contents of the file are precisely what the parties seek. An examiner can limit the date range only for items that have temporal data associated with them, but not otherwise.

So, be wary of language like, "*All searches are restricted to the time period from November 1, 2017 through May 23, 2018*." Interval limitations on search don't fly, and you won't know what you're missing.

A preferable approach in a protocol might be to specify that the examiner should not *produce* information to counsel if the examiner determines that the information falls outside of the relevant interval specified in the protocol. The distinction is that, while an examiner may not be able to limit a search to an interval, an examiner can often glean enough information about items found to make a reasonable assessment of their temporal relevance.

> **Exemplar Language:** *The parties intend that the scope of the examination be, as feasible, limited to the Relevant Interval: [Date 1] through [Date 2]. Except as otherwise specified herein, Examiner should make reasonable efforts to exclude from production the information that the Examiner determines falls outside of the Relevant Interval.*

Assess Evidence Integrity

If you're seeking a forensic exam, there's a good chance you suspect fraud or spoliation. It should come as no surprise to learn that evidence tendered for forensic examination is often swapped, fabricated, sterilized, reformatted, reimaged or otherwise corrupted. Why then, do so many lawyers framing examination protocols fail to explicitly require that the integrity of the evidence be assessed?

A threshold step in any forensic examination should include consideration of whether the evidence supplied is what it purports to be and if its contents have been wiped or manipulated to subvert the exam.

Exemplar Language: *The Examiner shall assess the integrity of the evidence by, e.g., checking Registry keys to investigate the possibility of drive swapping or fraudulent reimaging and looking at logs to evaluate BIOS clock manipulation. The Examiner may take other reasonable steps to determine if the data supplied is consistent with its stated origins, including but not limited to:*

a. *Looking at the dates of key system folders to assess temporal consistency with the device, operating system and events;*
b. *Looking for instances of applications employed to alter file metadata or erase/alter system cache and history data; and,*
c. *Noting the presence and nature of any recently installed applications and/or antiforensic "privacy" tools.*

The Examiner shall promptly report any irregularities concerning the integrity of the evidence to counsel for the parties.

Provide for Cooperation

Hardened device security has made it difficult for computer forensic examiners to forgo passwords and bypass encryption. Today, it's common that users must supply their access credentials to facilitate examination. A good examination protocol obliges parties to promptly supply same on request.

Exemplar Language: *The Parties shall cooperate with the Examiner insofar as promptly supplying non-privileged information and passwords and credentials required to access and decrypt data on the Image and accurately interpret same. No passwords or credentials obtained from the image or furnished by the parties will be used by the Examiner to access data other than found on the Image.*

Plot the Process

The most daunting feature of a forensic examination protocol is detailing the procedures and analyses to be completed. It's important to lay out these steps because forensic examiners use different tools, call things by different names and don't all possess the same grasp of forensic artifacts and their significance. The best way to ensure that the work gets done is to describe what's required in language the examiner will clearly understand and as steps the examiner has the tools and expertise to complete.

You can't do that by blindly borrowing language from a protocol in a different case.

Instead, read up on common forensic artifacts (I've written a lot on that subject elsewhere) or, better yet, consult a forensic examiner to lay out what needs to be done, describing the steps in enough detail that any examiner using one of the leading forensic tools will know what to do and where to look.

The single biggest mistake lawyers make in drafting forensic examination protocols is requiring examiners to do things they can't do. Forensic examiners can't always tell what files a user copied or what files were deleted. We can't always tell who logged in using another's password. Despite what you see on television, computers don't track everything, and they don't simply log all events, even in the event logs!

Forensics is a powerful tool; but, it's not magic. Most forensic artifacts on which examiners rely exist only by way of happy accidents.

You can roughly divide the evidence in a computer forensic examination between evidence generated or collected by a user (*e.g.,* an Excel spreadsheet or downloaded photo) and evidence created by the system, which serves to supply the context required to authenticate and weigh user-generated evidence. User-generated or -collected evidence tends to speak for itself without need of expert interpretation. In contrast, artifacts created by the system require expert interpretation, in part because such artifacts exist to serve purposes having nothing to do with logging a user's behavior for use as evidence in court. Most forensic artifacts arise because of a software developer's effort to supply a better user experience and improve system performance. Their probative value is a happy accident.

On Microsoft Windows systems, a forensic examiner may look to machine-generated artifacts called LNK files, prefetch records and Registry keys to determine what files and applications a user accessed and what storage devices a user attached to the system.

LNK files (pronounced "link" and named for their file extension) serve as pointers or "shortcuts" to other files. They are like shortcuts users create to conveniently launch files and applications; but, these LNK files aren't user-created. Instead, the computer's file system routinely creates them to facilitate access to recently used files and stores them in the user's RECENT folder. Each LNK file contains information about its target file that endures even when the target file is deleted, including times, size, location and an identifier for the target file's storage medium. Microsoft didn't intend that Windows retain evidence about deleted files in orphaned shortcuts; but, there's the happy accident–or maybe not so happy, if your client is caught in a lie because the computer was trying to better serve him.

Windows seeks to improve system performance by tracking the recency and frequency with which applications are run. If the system knows what applications are most likely to be run, it can "fetch" the programming code those applications need in advance and pre-load them into memory, speeding the execution of the program. Thus, records of the last 128 programs run are stored in series of so-called "prefetch" files. Because the metadata values for these prefetch files coincide with use of the associated program, by another happy accident, forensic examiners may attest to, say, the time and date a file wiping application was used to destroy evidence of data theft.

Two final examples of how much forensically-significant evidence derives from happy accidents are the USBSTOR and DeviceClasses records found in the Windows System Registry hive. The Windows Registry is the central database that stores configuration information for the system and installed applications—it's essentially everything the operating system needs to "remember" to set itself up and manage hardware and software. The Windows Registry is huge and complex. Each time a user boots a Windows machine, the registry is assembled from a group of files called "hives." Most hives are stored on the boot drive as discrete files and one—the Hardware hive—is created anew each time the machine inventories the hardware it sees on boot.

When a user connects an external mass storage device like a portable hard drive or flash drive to a USB port, the system must load the proper device drivers to enable the system and device to communicate.

To eliminate the need to manually configure drivers, devices have evolved to support so-called Plug and Play capabilities. Thus, when a user connects a USB storage device to a Windows system, Windows interrogates the device, determines what driver to use and—importantly—*records information about the device and driver pairing* within a series of keys stored in the ENUM/USBSTOR and the DeviceClasses "keys" of the System Registry hive. In this process, Windows tends to store the date and time of both the earliest and latest attachments of the USB storage device.

Windows is not recording the attachment of flash drives and external hard drives to enable forensic examiners to determine when employees attached storage devices to steal data! Presumably, the programmer's goal was to speed selection of the right drivers the next time the USB devices were attached; but, the happy accident is that the data retained for a non-forensic purpose carries enormous probative value when properly interpreted and validated by a qualified examiner.

Having said all this, the artifacts are different for different operating systems (Windows versus MacOS) and even for different releases of the same operating system. The artifacts are radically different on phones versus computers. It's complicated, and it changes…frequently.

If you will be suing a neutral examiner, draft the protocol to provide for the parties to confer with the examiner to establish the scope of work. Too often, examiners are saddled with unwieldy protocols poorly tailored to answering the parties' questions because the protocol was drafted without professional guidance.

What you should *not* expect to occur is your expert gaining direct access to your opponent's digital media. The more-likely result is a protocol laying out the steps to be followed by your *opponent's* expert or by a court-appointed neutral examiner.

Establish Who Pays

Though the forensic preservation of a desktop or laptop machine tends to cost no more than a short deposition, the cost of a forensic examination can vary widely depending upon the nature and complexity of the media under examination and the issues. Forensic examiners usually charge by the hour with rates ranging from approximately $200-$600 per hour according to experience, training, reputation and locale. Costs of extensive or poorly targeted examinations can quickly run into five and even six figures. Nothing has a greater influence on the cost than the scope of the examination. Focused examinations communicated via clearly expressed protocols tend to keep costs down. Searches should be carefully evaluated to determine if they are over- or under inclusive. The examiner's progress should be followed closely, and the protocol modified as needed. It's prudent to have the examiner report on progress and describe work yet to be done when either hourly or cost benchmarks are reached.

In all events, the examination protocol should make clear how, when and by whom the Examiner is compensated for professional time and reimbursed for expenses.

> **Exemplar Language:** *Charges for Examiner's professional time and time in transit shall be timely paid by Plaintiffs at the Examiner's customary rates, along with reasonable and customary expenses according to the terms of the rate sheet submitted before appointment. In the event Examiner's charges equal or*

exceed $_____, the Examiner shall report progress to the parties and project further charges expected to be incurred to completion.

Address Onsite Acquisition and Supervision

A party whose systems are being acquired and examined may demand to be present throughout the process. This may be feasible while the contents of a computer are being *acquired* (duplicated); otherwise, it's an unwieldy, unnecessary and profligate practice. Computer forensic examinations are commonly punctuated by the need to allow data to be processed or searched. Such efforts consume hours, even days, of "machine time," but not examiner time. Examiners sleep, eat and turn to other cases and projects until the process completes. However, if an examiner must be supervised during machine time operations, the examiner cannot jeopardize another client's expectation of confidentiality by turning to other matters. Thus, the "meter" runs all the time, without any commensurate benefit to either side except as may flow from the unwarranted inflation of discovery costs.

Demanding that forensically-sound acquisition occur on a client's premises versus in an examiner's lab can hugely inflate cost. On-site acquisition may be unavoidable for mission-critical systems like servers; but otherwise, I push back against demands to work on a party's premises versus in my own lab. In the lab, I can turn to other tasks and stop billing. Onsite acquisition and analysis run up the bill unnecessarily and require I be furnished a workspace that's suitable and secure, perhaps for days or longer.

Recovering Deleted Data

Although the goals of forensic examination vary depending on the circumstances justifying the analysis, a common aim is recovery of deleted data. One court ordered, "if the files…have been deleted or altered using a drive-wiping utility, [forensic examiner] will also recover all deleted files and file fragments." *Schreiber v. Schreiber*, 2010 WL 2735672 (N.Y. Sup. Ct. June 25, 2010). That's not such a good idea.

The Perils of "Undelete Everything"

Examination protocols shouldn't direct the examiner to, in effect, "undelete all deleted material and produce it." Though that sounds clear, it creates unrealistic expectations and invites excessive cost. Here's why:

A computer manages its hard drive in much the same way that a librarian manages a library. The files are the "books" and their location is tracked by an index. But there are two key differentiators between libraries and computer file systems. Computers employ no Dewey decimal system, so electronic "books" can be on any shelf. Further, electronic "books" may be split into chapters, and those chapters stored in multiple locations across the drive. This is called "**fragmentation**." Historically, libraries tracked books by noting their locations on index card in a card catalog. Computers similarly employ directories (called "**file tables**") to track files and fragmented segments of files.

When a user hits "Delete" in a Windows environment, nothing happens to the actual file targeted for deletion. Instead, a change is made to the master file table that keeps track of the file's location. Thus, akin to tearing up a card in the card catalogue, the file, like its literary counterpart, is still on the "shelf," but now—without a locator in the file table—the deleted file is a needle in a haystack, buried amidst millions of other unallocated clusters.

To recover the deleted file, a computer forensic examiner employs three principal techniques:

1. File Carving by Binary Signature

Because most files begin with a unique digital signature identifying the file type, examiners run software that scans each of the millions of unallocated clusters for file signatures, hoping to find matches. If a matching file signature is found and the original size of the deleted file can be ascertained, the software copies or "carves" out the deleted file. If the size of the deleted file is unknown, the examiner designates how much data to carve out. The carved data is then assigned a new name and the process continues.

Unfortunately, deleted files may be stored in pieces, as discussed above, so simply carving out contiguous blocks of fragmented data grabs intervening data having no connection to the deleted file and fails to collect segments for which the directory pointers have been lost. Likewise, when the size of the deleted file isn't known, the size designated for carving may prove too small or large, leaving portions of the original file behind or grabbing unrelated data. Incomplete files and those commingled with unrelated data are generally corrupt and non-functional. Their evidentiary value is also compromised.

File signature carving is frustrated when the first few bytes of a deleted file are overwritten by new data. Much of the deleted file may survive, but the data indicating what type of file it was, and thus enabling its recovery, is gone.

File signature carving requires that each unallocated cluster be searched for each of the file types sought to be recovered. When a court directs that an examiner "recover all deleted files," that's an exercise that could take excessive effort, followed by countless hours spent examining corrupted files. Instead, the protocol should, as feasible, specify the *particular* file types of interest based upon how the machine was used and the facts and issues in the case.

Notably, file carving of deleted information from unallocated clusters is fast becoming untenable by the emergence of solid state and encrypted media. Storage optimization techniques used by solid state drives serve to routinely overwrite once-recoverable data.

2. File Carving by Remnant Directory Data

In some file systems, residual file directory information revealing the location of deleted files may be strewn across the drive. Forensic software scans the unallocated clusters in search of these lost directories and uses this data to restore deleted files. Here again, reuse of clusters can corrupt the recovered data. A directive to "undelete everything" gives no guidance to the examiner respecting how to handle files where the metadata is known but the contents are suspect.

3. Search by Keyword

Where it's known that a deleted file contained certain words or phrases, the remnant data may be found using keyword searching of the unallocated clusters and slack space. Keyword search is a laborious and notoriously inaccurate way to find deleted files, but its use may be warranted when other techniques fail. When keywords are too short or not unique, false positives ("**noise hits**") are a problem. Examiners must painstakingly look at each hit to assess relevance and then manually carve out responsive data. This process can take days or weeks for a single machine.

Better Practice than "Undelete" is "Try to Find"

The better practice is to eschew broad directives to "undelete everything" in favor of targeted directives to use reasonable means to identify specified types of deleted files. To illustrate, a court might order, "*Examiner should seek to recover any deleted Word, Excel, PowerPoint and PDF files, as well as to locate potentially relevant deleted files or file fragments in any format containing the terms, 'explosion,' 'ignition' or 'hazard.'*"

Reporting and Deadlines

In the context of digital forensics, "reporting" means many things. As a lawyer-examiner, I create narrative reports setting forth in plain language what I'm seeing in the evidence and what my training and experience suggest it signifies. But, most forensic examiners regard reporting as a machine-generated process. It's common for a forensic "report" to consist of dozens or hundreds of pages of mostly-unintelligible gibberish spit out by software. So, it's smart to deal with that in the protocol. If the parties need specific questions answered in a narrative fashion, say so. If the analysis must be completed by a time certain, set deadlines for preliminary and final reporting and establish whether meeting those deadlines is feasible for the examiner (recognizing that the examiner has seen no evidence and probably has more questions than answers).

Forensic Acquisition versus Preservation

Parties and courts are wise to distinguish and apply different standards to requests for forensically-sound *acquisition* versus those seeking forensic *examination*. Forensically-sound acquisition of implicated media guards against spoliation engendered by continued usage of computers and by intentional deletion. It also preserves the ability to later conduct a forensic examination, if warranted.

Forensic *examination* and analysis of an opponent's ESI is both intrusive and costly, necessitating proof of egregious abuses before allowing one side to directly access the contents of the other side's computers and storage devices (something I caution courts against ordering). By contrast, forensically duplicating and preserving the *status quo* of electronic evidence costs little and can generally be accomplished without significant inconvenience or intrusion upon privileged or confidential material. Accordingly, courts should freely order forensic preservation upon a showing of good cause.

During the conduct of a forensically-sound acquisition:

1. Nothing on the evidence media is altered by the acquisition;
2. Everything on the evidence media is faithfully acquired; and,
3. The processes employed are authenticated to confirm success.

These standards cannot be met in every situation—notably, in the logical acquisition of a live server or physical acquisition of a phone or tablet device—but parties deviating from a "change nothing" standard should disclose and justify that deviation.

Exemplar Acquisition Protocol

An exemplar protocol for acquisition follows, adapted from the court's order in *Xpel Techs. Corp. v. Am. Filter Film Distribs*., 2008 WL 744837 (W.D. Tex. Mar. 17, 2008):

The motion is GRANTED and expedited forensic imaging shall take place as follows:

A. Computer forensic acquisition will be performed by _____ (the "Examiner").

B. Examiner's costs shall be borne by the Plaintiff.

C. Examiner must agree in writing to be bound by the terms of this Order prior to the commencement of the work.

D. Within two days of this Order or at such other time agreed to by the parties, Defendants shall make the specified computer(s) and other electronic storage devices available to Examiner to enable Examiner to make forensically-sound images of those devices, as follows:

i. Images of the computer(s) and any other electronic storage devices in Defendants' possession, custody, or control shall be made using hardware and software tools that create a forensically sound, bit-for-bit, mirror image of the original hard drives (*e.g.,* EnCase, FTK Imager, X-Ways Forensics or Linux dd). A bitstream mirror image copy of the media item(s) will be captured and will include all file slack and unallocated space.

ii. Examiner should document the make, model, serial or service tag numbers, peripherals, dates of manufacture and condition of the systems and media acquired.

iii. All images and copies of images shall be authenticated by cryptographic hash value comparison to the original media.

iv. The forensic images shall be copied and retained by Examiner in strictest confidence until such time the court or both parties request the destruction of the forensic image files.

v. Without altering any data, Examiner should, as feasible, determine and document any deviations of the systems' clock and calendar settings.

E. Examiner will use best efforts to avoid unnecessarily disrupting the normal activities or business operations of the Defendants while inspecting, copying, and imaging the computers and storage devices.

F. The Defendants and their officers, employees and agents shall refrain from deleting, relocating, defragmenting, overwriting data on the subject computers or otherwise engaging in any form of activity calculated to impair or defeat forensic acquisition or examination

Pulling It Together in an Exemplar Protocol

The following exemplar examination protocol was accepted by the Court in a case where the parties sought to determine what a user was doing on a laptop a laptop machine on a single day. As the machine was in a distant state, it was practical that the forensic image be acquired by another examiner and the image shipped to me.

Examination Protocol for Windows Laptop

I. **GOALS:** The purpose of Protocol is to guide, Craig Ball, Texas attorney and Certified Computer Forensic Examiner ("Examiner") in identifying and interpreting active and latent artifacts tending to shed light on the nature, extent and timing of usage, if any, of a Windows laptop machine

("Machine") during specified relevant intervals, as well as in assessing the integrity of the Machine and its contents for data loss, destruction and alteration during and following the relevant interval (*Date 1 through Date 2*).

II. **EVIDENCE:** This protocol assumes that Examiner will receive a forensically-sound, hash-authenticated bitstream image ("Image") of the Machine's data storage device(s) along with customary chain-of-custody information and baseline data establishing the accuracy or deviation of the Machine's system clock at the time of Image acquisition. Unless otherwise agreed by the parties and the Examiner, only a duly-certified Computer Forensic Examiner shall image the Machine and authenticate the chain-of-custody and baseline data.

III. **DUPLICATION:** The Examiner will make hash-authenticated working and archival copies of the Image. The Image supplied will not otherwise be used for analysis but will be secured until return or disposal.

IV. **COOPERATION AND CREDENTIALS:** The Parties shall cooperate with the Examiner insofar as promptly supplying non-privileged information and passwords and credentials required to access and decrypt data on the Image and accurately interpret same. No passwords or credentials obtained from the image or furnished by the parties will be used by the Examiner to access data other than found on the Image.

V. **AUTHORIZATION AND SCOPE:** The Examiner may:
   1. Load an authenticated working copy of the Image into an analysis platform or platforms and examine the file structures for anomalies.
   2. Assess the integrity of the evidence by, *e.g.*, checking Registry keys to investigate the possibility of drive swapping or fraudulent reimaging and looking at logs to evaluate BIOS clock manipulation. The Examiner may take other reasonable steps to determine if the data supplied is consistent with its stated origins.
   3. Look at the various creation dates of key system folders to assess temporal consistency with the machine, OS install and events.
   4. Look for instances of applications employed to alter file metadata or erase/alter usage cache and history data.
   5. Note recently installed applications and any antiforensic "privacy" tools.
   6. Refine the volume snapshot to, *e.g.,* identify relevant, deleted folders, applications and files, orphaned file records, Host Protected Areas, hidden partitions, inter-partition data and encrypted volumes.
   7. Further refine the volume snapshot to unpack compound files (e.g., compressed and container files), compare binary file signatures with file extensions, identify possible encrypted files using entropy testing, hash all files, extract application metadata and process contents of Volume Shadow Copies.
   8. Carve the unallocated clusters for file artifacts using binary signature analysis, seeking deleted files and deleted cache content, temp files, fragments and system artifacts.
   9. Locate and extract Registry hives for analysis.

10. Look at the LNK files, index files, TEMP directories, cookies, Registry MRUs, shellbags, jump lists, thumbnails, shadow copies and, as relevant, system and event logs and Windows prefetch area, to assess usage of applications, files and network accesses.
11. Generate and export complete file listings with associated file size, file path, hash and temporal metadata values (other metadata values as relevant and material).
12. If indicated, run keyword searches against the contents of all clusters (including unallocated clusters and file slack) seeking relevant data, then review same.
13. Sort the data chronologically for the relevant Modified, Accessed and Created (MAC) dates to assess the nature of activity within the relevant interval.
14. As feasible, generate a network activity report against, *inter alia*, index.dat and comparable network activity artifacts to determine, *inter alia,* if there has been web surfing web search, e-mail, texting, download or upload activity or research conducted at pertinent times concerning, *e.g.,* how to destroy or alter electronic evidence, conceal system and network usage and the like.
15. Filter for e-mail messaging formats (*e.g.,* PST, OST, NSF, DBX, MSG, EML, etc.), and extract messaging for processing in preferred application. Check OLK folders (Outlook attachment temp storage).
16. Examine container files for relevant email in the relevant interval(s). If web mail, look at cache data. If not found, carve UAC to reconstruct same.
17. Identify mobile device (*e.g.*, iTunes, Android) and Cloud (*e.g.,* DropBox) synch sources.
18. Gather the probative results of the efforts detailed above, assess whether anything else is likely to shed light on the documents and, if not, share conclusions as to what transpired.
19. Make recommendations for further lines of inquiry or sources of data, if any.

VI. **COST:** Charges for Examiner's professional time and time in transit shall be timely paid by Plaintiffs at the Examiner's customary rates, along with reasonable and customary expenses according to the terms of the Examiner's Engagement Agreement.

What's Missing?

Privilege and Confidentiality Concerns: The preceding protocol involved a matter where privileged and confidential material and communications weren't a concern; but, protocols more typically need to provide for non-waiver of privilege and for counsel's review of the examiner's reporting before it's seen by opposing counsel so that objections can be asserted to disclosure of privileged or protected content. A protocol should also address *ex parte* communications with the Examiner.

Exemplar Language: *To the extent the Examiner has direct or indirect access to information protected by the attorney-client privilege, such access will not result in a waiver of the attorney-client privilege. Unless counsel for all parties are included, there shall be no communications between any party or party's counsel aside from purely ministerial communications necessary to complete the tasks set out in this Protocol.*

All data and analyses governed by this Protocol are deemed protected material. Possession of such material is limited to the Examiner the attorneys of record in the captioned cause and their experts.

Counsel and their experts may not share or review the protected material in any manner with any other person, including their respective clients.

Any data or reporting resulting from the Examination will be produced by the Examiner to the attorney for the device/media owner for review. No data will be provided to opposing counsel until it has been reviewed and released by the attorney for the device/media owner. A listing of the data that was forwarded to counsel for the device/media owner will be included with the data. This index will include the file name, the date last modified and the file size, as feasible. Data not in the form of a file will be identified on the listing in a reasonably clear and practical manner. The attorney for the device/media owner will identify on the listing any items that will not be produced and the basis for withholding such items. Items not withheld shall be produced to the party or parties requesting the data along with the listing showing the items withheld and the basis for withholding such items.

Parties may object to withholding of any data, and counsel for the parties shall cooperate on procedures to resolve disputes about withheld data. If the parties cannot resolve a dispute as to the production of withheld data, then any party may move for protection or for an order to compel production.

Forms of Production: The protocol also doesn't address the challenge of delivering forensic artifacts to counsel in usable formats. Lawyers and courts are conditioned to expect "documents" and are rarely prepared for data. A crucial forensic artifact may be no more than a few bytes of encoded information bobbing in a sea of unallocated clusters. A handful of these can converted to a document-like format for review; but, what if there are hundreds of thousands of such instances to examine (as commonly occurs when running keyword searches against unallocated clusters)? Lawyers can't expect that the fruits of a forensic examination can be loaded into an e-discovery review platform and treated like documents. Too, lawyers can't expect to load native files into native software applications without altering the evidence. Native applications modify native files.

Skilled forensic examiners are experienced in working with lawyers to facilitate review of forensic artifacts in practical, scalable ways. Since it's not always practical or possible to provide for a form of production in advance of a forensic examination, a protocol should afford the examiner some leeway to supply deliverables in forms suited to assist the parties in their review (and the Court in any *in camera* review).

Ethical Boundaries

Unless the Court expressly permits, or the parties agree, a forensic examiner should never use the devices tendered for examination or information derived in the exam to access information beyond that stored on the physical devices and media when tendered for examination. Most examiners know this and will act ethically; however, a thorough protocol should make that restraint clear, so none need worry that an overeager examiner will abuse a booted clone device or a user's log in credentials.

Exemplar Language: *Examiner shall not use the devices and storage media tendered for examination, or any information or credentials derived from same, to access any electronic information not present on the devices and storage media when tendered for examination. This prohibition includes but is not limited to accessing private online or Cloud accounts, e-mail accounts or servers, private social media sites and banking and credit card accounts and transactions.*

Other Points to Ponder

A protocol may need to address topics such as disposition of evidence after analysis, data retention and destruction duties (including financial responsibility for same), amenability to discovery (deposition and subpoena), applicability of protective orders.

It's useful to empower the examiner to make recommendations for further lines of inquiry or sources of data. Certainly, the parties and the Court must be sensitive to suggestions that smack of make-work; but, a skilled, ethical examiner will often have the best ideas where to go to find other relevant electronic evidence.

Conclusion

Crafting a forensic examination protocol demands more than finding a good form to filch. It requires a clear sense of about what you seek to accomplish through an examination and the ability to express those goals with enough technical specificity to guide a diligent examiner to the artifacts that will answer your questions. There's often a tension between one side's wish to rein the examiner in and the others' to turn the examiner loose. A good protocol balances the two and affords the examiner just enough discretion to follow the electronic evidence and let it tell its tale.

About the Author

Craig Ball, of New Orleans is a court-appointed special master, Board-certified trial attorney (Texas), law professor and certified computer forensic examiner. More of Craig Ball's publications on computer forensics and electronic discovery are available at craigball.com and ballinyourcourt.com.