Courtroom Considerations in Digital Image Forensics

H. T. Sencar and N. Memon (eds.), Digital Image Forensics, pp 313-326
DOI: 10.1007/978-1-4614-0757-7_11

Rebecca Mercuri, Ph.D.

Notable Software, Inc., P.O. Box 1166, Philadelphia, PA 19105
<www.notablesoftware.com>

Abstract The manner in which results of digital image forensic investigations are presented in the courtroom can be positively or adversely affected by case law, federal rules and legislative acts, availability of discovery materials, tools, and the use of exhibits. Issues pertinent to effective and successful testimony are addressed, along with suggestions for improvement of methods.

1 Computer Forensics

Computer forensic investigations, including those applied to all types of digital imagery, primarily deal with the analysis and reporting of evidence that is typically collected after (or possibly also during) an incident, with the intended goal of producing legally acceptable evidence for courtroom purposes. The forensic process thus necessarily differs from and involves considerably more effort than that which is required to perform simple data recovery and image restoration tasks. This is because one cannot merely present digital evidence materials to the court without also providing extensive accompanying documentation, detailing numerous salient aspects, especially those pertinent to establishing chain of custody, knowledgeable possession and control. The methods used by the forensic examiner must be well documented, as they may likely be subjected to scrutiny by attorneys, judges and other investigators. Forensic preparations, therefore, place a high emphasis on data authentication and report writing, and involve the use of tools that enhance the examiner's ability to perform these tasks.

The field of computer forensics, having evolved predominantly over the last decade, is relatively young, especially as compared to other forensic endeavors (such as those used by coroners or in ballistics) that have been performed for a

century or more. Presently there is no uniform certification process, training, degree, or license required in order to become a computer forensics or digital imaging examiner, and it is rare to find such an expert with a decade or more of court-related experience. Nor is any particular laboratory configuration specified for the performance of this work, although best practice recommendations are now beginning to appear. This lack of standardization is due, at least in part, to the rapid growth and ever-changing challenges of the computer field. New products are emerging constantly and commonly used forensic tools may not be able to handle certain items properly, or even at all, at the time when an examination is needed. For image forensics, software tools must be able to identify and display the various different types of digital picture and video formats. Hardware has to safely accommodate the changing array of media storage devices, such as SIM and other memory chips and cards, as well as drives and disks. To fill in the gaps, when needed, experts often supplement the commercially and publicly available tools with ones they have personally created or commissioned. Operating systems, programming languages, interfaces, and other aspects of the computational environment are also evolving and the examiner must stay informed in order to be able to properly assess and address the various and unique situations presented in each case.

The method of examination should not be unduly constrained by the forensic tools. Often it happens, though, that magnetic media (drives, disks, etc.) have been archived by an impounding facility using a process that results in a proprietary format (EnCase is one of these) that cannot be decoded without access to the specific software or a particular version thereof. This may impose additional and unnecessary time and cost on an examination facility, placing their client and legal team at a practical disadvantage. It is important that a court recognize the fact that each side should be allowed the same access to the data, preferably in the form that it was originally found, or at least a common and openly available one.

Of course, the volatility of electronic recording devices (especially those that can be written to or altered) comes into play. Individuals charged with the responsibility of collecting original evidence materials must ensure that their process does not damage or alter data in any way. Occasionally, evidence has been contaminated by over-zealous information technology staff who may scan a drive without first placing it into a write-protect bay, or file recovery tools may be erroneously employed that overwrite other data. The use of original digital media evidence must be limited to the minimal steps necessary for archiving and authentication. These archived materials should then be used to generate other forensic clones or derivative evidence to be provided for examination. Here again, there have been little or no controls or standards imposed or required, either for the collection, copying, or storage of these materials, and quality assurance has been observed to vary widely depending upon the type of facility involved. As an example, one would think it prudent to perform a hash value (authentication) calcula-

tion at the initial time of impounding, or minimally at the time the first copy is made, in order to ensure that no data has been altered, but this is rarely done.

2 Knowledge, Possession, Control

It is especially important to keep track of who has had access to the original evidence and establish timelines for possession. Once items have been impounded, they should be safeguarded under lock and key, such as in storage lockers, at all times when these materials are not in use. Chain of custody documents, where the individuals who have been responsible for the items are identified, along with access dates and times, should be maintained and made available for review as appropriate. This is true for derivative materials (data that has been copied from the originals) as well as the evidence itself. It is always preferable to hand courier these materials, especially originals, rather than risk damage, loss, or interception by using shipping services. If one must ship items, signatures, tracking, and insurance (if available) should be required.

Where child pornography digital imagery investigations are concerned, most laws refer to "knowing possession and control" which must be proven in order to convict. Federal law 18 U.S.C. § 2252A(a) prohibits certain activities relating to any visual depictions involving the use of a minor engaging in sexually explicit conduct, and makes it a felony to knowingly transport or ship in interstate or foreign commerce by any means including by computer or mail, or knowingly possess, receive or distribute such materials. Unfortunately, courts have quite often been persuaded by prosecutors to turn a blind eye to the aspects involving "knowledge" and "control" with the result being that mere possession is tantamount to guilt. Even though the law specifically refers to "sexually explicit conduct," the definition of this varies widely, even between counties in the same state. The photos of baby's first diaper change or cousins skinny-dipping in the lake, especially if genitalia are evident, could even be deemed explicit and used to constitute prurient interest. Some prosecutors and judges still use the "you know it when you see it" test for pornography, which can be flawed or deceiving when older but youthful-looking people are depicted.

Many computer users have no idea that when they try to delete files that have been accidentally downloaded, items may still persist in the "recycling bin" (or desktop "trash can") until perhaps the computer is turned off or rebooted, or after the trash is manually emptied via a file menu selection. This is also true of electronic mail, where deletion may only put the message into a trash folder that requires another action to empty it. As well, with electronic mail, attachments may be saved in a completely different folder in the computer's file system that users may not know about or is hard to find. Misleading and even preposterous comments have been made in grand jury testimony, and when obtaining search warrants, to the effect that "collectors" of contraband materials will deliberately place

these items in the trash to conceal them from other users of the computer, when clearly the accused recipient was actually trying to dispose of unwanted material.

Nor do many computer users realize that deletion, even from the "trash," typically only removes the name of the file from the active directory tree, and the file itself nevertheless continues to persist on the drive until the operating system overwrites it with other data. Given the proliferation of larger sized storage devices, it is common to find and recover a substantial percentage of the files that had ever existed on the system, in the unallocated space of the hard drives, some days, months or even years after the user(s) attempted and intended to delete them. Recovery tools have become more sophisticated too, such that even partial files for images and videos can be reconstructed out of existing fragments.

Certainly it is not illegal to possess or use programs that will effectively overwrite (with random characters or 1's or 0's) the unused (unallocated and slack) space of one's own magnetic media. This is often necessary for legitimate purposes (such as HIPAA compliance for health care records (Mercuri 2004)), but prosecutors are fond of making it seem that ownership of such tools constitutes intention to conceal contraband files. Nevertheless, many of these tools do not work properly, or are installed incorrectly, and individuals are often lulled into a false sense of confidence that their drives are being "wiped" of any evidence of possible misuse, when actually considerable data continues to persist.

In fact, whether a defendant actually opened and/or viewed a downloaded file that they deliberately downloaded may be considered irrelevant in terms of possession. An analogous situation is that one can certainly be charged with drug possession whether or not they are a user. The problem, especially with digital imagery, is that when multiple files are transmitted together in a group (such as in a zip file), the person requesting the file may be wholly unaware that contraband exists within the archive. When an archive is expanded, the contents typically are placed into a folder, which may never be opened for review. Here, a rapid-fire sequence of "last accessed" time stamps, within seconds of each other, is generally indicative of automatic file extraction without viewing.

File names can be highly misleading, since nondescriptive names (such as sequence numbers) are often used to aid in concealing contents from unsuspecting downloaders. A GAO study (United States General Accounting Office 2003) that performed searches on peer-to-peer networks using benign topics of interest to children or specific keywords, underscored the broad availability of such contraband materials while also noting problems with respect to the file names. Although their keyword search using words related to child pornography yielded file names indicating 42% child porn, 34% adult porn and 24% non porn, the actual images revealed the percentages to be 44% child porn, 13% child erotica, 29% adult porn, and 14% non porn, thus showing that a significant amount of material

is miscategorized based on naming. The statistical likelihood that someone using peer-to-peer networks for other purposes would unknowingly download felonious pictures or videos is therefore rather high.

Content identification is an area of imagery research that has seen more common use in recent years. Photo archives can allow keying of particular faces and objects to names, with automatic generation of labels as the database is developed. The rigor of such algorithms is not yet well understood, but it will certainly become another method of ferreting out contraband and pinpointing possible victims, likely with considerable false positives, in future investigations. With this, issues of privacy and censorship will need to be considered. Although it might be more reasonable for Internet Service Providers to monitor for content in imagery transmissions, these entities were provided with safe harbor in the United States of America under the Digital Millennium Copyright Act of 1998, with liability for misuse shifted to the end users, networks (such as peer-to-peer) and archivers (like YouTube). Other nations (Australia is a good example) do require the ISPs to perform some filtering. Such requirements (or lack thereof) may shift in the future as new laws and rulings are developed and instituted.

When attorneys and experts are able to successfully present the court with rationale that mere possession is not sufficient to demonstrate knowledge and control of contraband digital imagery, they must also be prepared to deal with evidence that can potentially corroborate allegations that the particular files were intentionally downloaded or actually seen. Such evidence typically involves the recorded timestamps on the files at issue, as well as data that can be extracted from system logs.

The trio of file time stamps, often referred to as “created,” “modified,” and “last accessed,” can be especially difficult to deal with. Recovery efforts, if not performed properly, may alter this data, and when overwritten on the original media, the earlier information is essentially unrecoverable. It should be noted that deleted files (after the trash can is emptied, but still existing in the unallocated space of the drive) will not show this associated data, since it is maintained by the file system and lost on deletion. The terminology referring to these three timestamps is rather misleading, since “created” does not necessarily (or even at all) pertain to when the file was actually generated, but rather it might be when it was placed into or taken out of an archive, or copied, or when operations are performed. The other two time stamps have the same properties, with “last accessed” being particularly unreliable because it often is routinely affected/updated by system operations (such as periodic virus scans). System time clocks may be altered or may not be reliable (especially if the computer is old and the battery has run down). There may also be confusion over the time zone of this information, especially when tools are used that reflect universal (Greenwich Mean) time, and do not account for Daylight Savings differences. Essentially, these dates and times

are not really reliable proof of particular user activities, although they are often held up as incontrovertible corroboratory evidence. This is not to say that the time stamps cannot also be used to provide exculpatory evidence, especially when there may be time or date intervals showing temporally when a defendant can demonstrate that he/she had no access whatsoever to the computer system.

System files are another area from which information can be harvested that appears to corroborate allegations. With respect to digital imagery, the Windows Media Player logs are often used to provide "proof" of viewing. For peer-to-peer situations, the Web browser software (such as Limewire) may use a slightly modified file name if the item is previewed during downloading, which can also be deemed to demonstrate proof of "knowing possession" especially if the modified name appears in a viewing log. That these logs occur in the background without the user's explicit authorization may seem to imply that their accuracy is unquestionable, but in fact, there is no true way to tie this information to any particular user, and it could also have resulted from malware (virus activity) or access by an unauthorized individual or distant computer. It is especially important to scan the system in order to determine if it may have been operating as a remotely controlled "bot" or was infected in a manner that may have enabled adverse activity to occur. Peer-to-peer situations are especially dangerous, in that if a contraband file is discovered in the file share folder, where it would normally reside following downloading, the charges against a defendant can include distribution as well as possession if the sharing feature has been turned on. Vigilante groups and special police task forces have been known to harvest the IP address information from file share browsers in an effort to identify possible contraband holders who will later be asked to provide their computers or will be served with search warrants in sting operations. The best way to prevent such problems from occurring is to avoid using peer-to-peer services, but many feel that this is an unfair constraint.

The thumbnail images that can be viewed when a directory is opened are also highly dubious as evidence. Some of these have been used to convict on the grounds of knowing possession and control, even when the original material has not been found to be present on the drive. The contention is that such thumbnails are only created when the related file has existed on the user's computer, but this is flatly untrue. When a folder is viewed in thumbnail mode, even after particular files are deleted, the thumbnail file (such as thumbs.db on the Windows operating system) still retains all of the individual thumbnails that previously were generated. Copying or moving an entire folder typically results in copying of the contained thumbnail file, which may not accurately reflect what pictures actually exist at the destination location. Hence, a folder copied from one user to another may contain concealed contraband that the recipient never knew about and could not see. This retention effect is difficult to demonstrate in court such that a jury or judge will understand that the appearance of a particular thumbnail in a system file does not at all constitute knowing possession or control, since the file is hidden by

default and specialized tools (such as the ones experts use in drive examinations) are required in order to extract and view any contents that are not also affiliated with the larger versions of pictures in the folder. Often the thumbnails are provided as discrete evidence elements in discovery without identifying them as being part of hidden system files, something that the defense expert needs to be careful to sort out in preparing their report. Although this tactic is becoming less common, individuals have certainly received convictions, with rejected appeals, on the basis of such thumbnails.

Digital image files will likely also contain header data that pertains to the time of creation and the equipment and settings used. This information can be readily modified, spoofed, or deleted, using publicly available tools. Recent scientific studies, though, have revealed subtle content within the image itself, allowing the particular digital camera that created the photo or video to be identified from others of the same model and type. Such analysis is still so new as to not have led to significant reported case law, but will likely become a factor in the future.

3 Expert Testimony

The court system is hierarchical in nature and, in formulating rulings, judges often look to the decisions of others, especially precedential decisions of higher courts within the same jurisdiction. It is thus in the best interest of all experts to try to avoid creating "bad law" where cases are "won" but the underlying expert theories are false. Image analysis could be one area where we may look back and see some matters whose outcome was based on expert testimony that was contrary to later-known facts. It is difficult to balance the need to move ahead with a demonstration that has not yet been fully vetted in the scientific community, with the desire to help a client as much as reasonably possible. Similar questions have been raised even with regard to the reliability of some common forensic tools, such that NIST has begun qualifying these via extensive examinations conducted in their Computer Forensics Tool Testing Project. We will likely see more of such tool validation in image analysis.

Differences in the manner in which expert testimony is handled by different courts, along with verification of scientific and forensic methods, is most evident when considering admissibility of evidence. The case of *Daubert v. Merrell Dow Pharmaceuticals, Inc.* 509 U.S. 579 (1993) dramatically altered the manner in which experts could present testimony. *Daubert* involved the claim that birth defects of children were related to the mothers' prenatal use of Bendectin, a prescription drug. Although testimony from eight experts concluded that Bendectin was responsible for birth defects on the basis of animal studies, chemical analyses, and an unpublished analysis of human statistical studies, the District Court in *Daubert* deemed that these methods of testing or analysis did not meet the "general acceptance" judicial test for expert opinion. The Court of Appeals for the 9th Circuit

agreed with this decision of the District Court, citing *Frye v. United States*, 293 F. 1013, 1014 (D.C. Cir. 1923).

At particular issue in *Daubert* were the Federal Rules of Evidence, which had been adopted by the United States Supreme Court on November 20, 1972 and enacted by the U.S. Congress on January 2, 1975. Confusingly, even though the Supreme Court reversed the lower courts' decisions in *Daubert* by trumping the earlier *Frye* standard with the newer Rules, this was only mandated for testimony in federal cases. Under Rule 702, scientific, technical or other specialized knowledge is only admissible if "(1) the testimony is based on sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case." (Morse and Gaugler 2007)

Where previously, under *Frye*, a level of "general acceptance" of the proffered testimony in the scientific community in which one claimed to have expertise was all that was necessary for admissibility, *Daubert* requires an independent judicial assessment of reliability of the testimony, even though a court may often be hard-pressed to provide such affirmations and often relies on the witness to say so themself. The phrase "I attest to this assertion with a high degree of scientific certainty" or "this opinion is stated within a reasonable degree of scientific probability or certainty" is used by experts in reports or during hearings in order to underscore the reliability of an opinion, but there is really no substantive proof demanded or required in order to support such claims. Although a blatant falsehood about an underlying fact relied upon for opinion might be considered perjurious, if such misinformation is pointed out an expert may still be able to claim "I believed this at the time, based on then-current methods and data."

For state court matters, some states have decided to use *Daubert* and adopted versions modeled on the federal rules, others are still using the earlier *Frye* test, some have developed their own tests of admissibility, and a number of states have not chosen to instantiate any particular method. Results in computational areas have occasionally failed to satisfy *Daubert* criteria because experts are often incapable of explaining the algorithms they have used to a non-technical audience. (Stevens) So, when delivering opinion, it is important for the expert to be familiar with and apply the appropriate testimony standards for the court one is appearing before. If there are any questions during pre-trial preparation, typically the attorneys working with the expert should advise.

The Federal Rules of Evidence are quite comprehensive and cut across diverse fields of forensics, such that computer experts have been able to adapt them to their investigations even though these were not even necessarily being considered (and computational devices barely existed) when Congress created this body of

law. Certain particular rules are especially important to consider when dealing with digital image forensics.

For example, Rule 1003 (Admissibility of Duplicates) states that "a duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Here, authentication for digital imagery is certainly a subject of contention. Law enforcement and prosecution is fond of referring to MD5 and SHA1 hash values as "digital fingerprints" while these are actually highly lossy and certainly not unique. Given that both of these hashes have been broken using collision search attack methods (Wang et al. 2005), one would think that more rigorous algorithms (such as SHA-256) would be encouraged, but the earlier methods are still commonplace, likely due to the toolsets being used and the time it takes to create the larger hash values.

That the smaller hashes have been compromised certainly comes into play when the values for contraband image files (such as those depicting child pornography) are used to identify such materials, possibly from remote locations via file sharing searches. Cracking has enabled files to be constructed such that hashes match those of common system files, so that when a hash-based search is done, numerous false positives are yielded.

Rule 1004 (Admissibility of Other Evidence of Contents) goes further with regard to duplicates, stating that "the original is not required" if it has been lost or destroyed, not obtainable, in possession of an opponent who has failed to produce it, or is not related to issues pertaining to control. Whereas in the law enforcement community, the MD5 and SHA1 hashes are still "generally accepted" as indicative of authenticity, under *Daubert* it might be possible to raise questions about the material (although proving this may be difficult) in an effort to have derivative evidence or copies excluded from trial use. As well, in police sting or honeypot (luring) operations, the full set of data collected during the investigation is rarely provided on the basis that such detail could potentially compromise other active cases. The introduction by prosecution of partial, out-of-context evidence (such as image or video fragments) may place defendants at risk, and attorneys may move a court to suppress such evidence.

Although Rule 601 states that "every person is competent to be a witness except as otherwise provided in these rules" the Rules have been used to provide a customary framework by which experts are validated by the court. Typically at the beginning of an expert's testimony, there is a review (voir dire) of the individual's qualifications by the attorney who has called them to the stand. The credentials, in the form of a curriculum vitae (CV) or résumé that includes publications as well as lists of cases in which the expert has previously testified or their opinion was made public, are given to the opposing side and the judge beforehand, providing

fuel for cross-examination. The questioning may be perfunctory if there are no objections, but is often rather extensive (for example, after publication, this chapter and even the entire book will likely be brought up in the qualification part of some hearings for this author when she provides expert testimony), with minute details used to try to impress (or malign) the level of expertise, or to point out potential areas of bias or prejudice, before the judge and jurors. Ultimately, it is the judge who determines whether the expert is deemed qualified and only then are they allowed to proceed to offer an opinion to the judge and jury on the case material. Rarely is an expert entirely disqualified, although an attorney may try to obtain numerous qualifications (such as for computer systems, computer forensics, and image forensics) some of which may be declined on the basis of the documentation and responses provided. Although part of a witness' CV may include a list of areas where judges have previously issued qualification, experts are only qualified for each particular case, requiring that this process occur in each litigation.

A problematic aspect of Rule 612 involves the use of notes when an expert is testifying. Basically, anything in writing can potentially be subject to subpoena by the opposition, so there may be instances where an expert should not create any documented record of discussions. Electronic messages and reports that are intended as drafts (not for distribution) are typically marked "ATTORNEY WORK PRODUCT PROTECTED" (or some variation thereof) because certain privileges recognized in the Rules of Evidence attach to preparation and collaboration with experts for reports and testimony. An expert's billing statements may often be perfunctory, leaving out details of what topics or individuals were involved, for similar reasons (although the hourly rate of remuneration may also be asked about during the expert's qualification). For the busy expert, subject to human frailty, who may not have a 100% precise memory of each case, many of which may be very similar in nature, the way around not bringing notes to the stand that could be required to be revealed, is that the attorney will mark the expert report as an exhibit at trial and then this document may be referred to and read from as a prompting vehicle for responses to questioning. As with the CV, typically the expert's written reports are disclosed in the discovery phase of litigation so that there will be no surprise at trial. Of course, all aspects of the report are subject to being picked apart by opposing counsel on cross-examination, so it is generally advisable to write just enough to make your points clear and go no further beyond that. This is generally a good rule of thumb for oral testimony as well.

4 Discovery

If the expert is retained early enough prior to trial, they may have an opportunity to assist with the discovery process. Although a novice might just rely on the hiring attorney or client to provide access to materials for review, the true value of an experienced expert, especially in the area of computer forensics, is often first seen in their ability to ascertain what additional discovery materials might be

available in the case. The expert should advise the attorney and client as to what they may be able to request, and will work with the impounding authority or opposition to obtain discovery materials in a format that best facilitates investigation. This is typically an iterative process, and may take months or even years to conclude. The good thing about being on the receiving end of discovery is that if you make your requests promptly, and the opposition is tardy in their responses, this can be called to the court's attention and should be helpful in obtaining continuances (extensions) on trial dates if additional time is required in order to perform the investigation and satisfy "due process."

When dealing with contraband digital imagery, the defense team is often held at a severe disadvantage by the customary belief that their expert cannot be allowed to examine a copy of the materials in their own laboratories for fear that they will be making and distributing copies of the alleged illicit data, despite the fact that doing so would likely constitute a felony and may even result in the loss of their business or occupation. Yet, even when court orders have been obtained requiring impounding agencies to provide contraband data to an examining laboratory on behalf of the accused defendant, requests have been denied on such grounds (especially since the enactment of the Adam Walsh Act in 2006). Defense has argued in numerous cases (sometimes successfully) that such discovery and investigation constraints provide an uneven playing field. One way of dealing with this is to use just the materials that have been released for off-site investigation, but occasionally it is not possible to perform an adequate job with only this data (particularly if photographs are provided in printed form and not as digital files). This type of discovery obstruction can also occur in civil cases where sides are unable to agree to the release of proprietary (trade secret) information.

If the forensic expert needs to be present at an opposition site to review data, typically they will be required to use (often substandard) equipment at that location, they may not have access to the same tool set that they are accustomed to using in their laboratory, their activities in performing the investigation may be monitored or even recorded (thus potentially revealing strategy), and subtle or overt harassment may even occur. In contrast, the holder of these materials essentially has 24-7 access to all of the evidence data, and can run exhaustive searches using whatever equipment they choose. Especially in public defender matters where fee ceilings are typically imposed and funding is limited, being required to repeatedly visit an unfamiliar lab to conduct investigations can unfairly increase litigation costs. The defense team will often not have access to the impounded discovery materials during the actual conduct of trial, so they cannot easily check items on a break or overnight when issues are raised in the immediacy of testimony. Prosecution investigators have been known to take advantage of their unlimited and easy access to the evidence (their office may even be located in another part of the building where the trial is taking place), and if they tip their hand to having performed additional mid-trial searches, the defense attorney must object to the intro-

duction of any new results, and request suppression of these, on the grounds of unfairness or surprise in discovery.

Since this type of restrictive investigation process often occurs with contraband cases, and since child pornography is increasingly at issue, especially with file sharing services, one would think that the defense lawyers and public defender offices would have joined together long before now (as prosecution did years ago with the FBI and state police in forming the various Regional Computer Forensic Laboratories around the country), in creating authorized settings where evidence examinations can be conducted without opposition calling the shots. Perhaps someday the gross inequities of this type of investigation will be challenged as a civil rights matter, and the situation will be rectified, but in the meanwhile it continues to hamper and prejudice the process.

The original intention of federal and state laws (as mentioned earlier) pertaining to possession and distribution of child pornography were to protect actual individuals from harm. This is why cartoons (such as South Park) depicting children engaged in sexual acts are not presently considered illegal, and also why the National Center for Missing and Exploited Children (NCMEC) maintains a database that identifies particular images and series with the people involved. (One should keep in mind that NCMEC is working for the prosecution, so defense access to their data and reports is typically prohibited or highly limited.)

With the subsequent enactment of Megan's Laws in all states, there has been an increased perception that individuals who happen to have obtained alleged child pornography, even if they came across it accidentally and are certainly not producing it, are actual pedophiles rather than just curious or foolish Web surfers. This has caused the pendulum to swing in the direction of considering some fabricated (i.e. computer generated or Photoshopped) images as contraband, even when no child was ever involved. States may also have bestiality laws, and imagery of this nature can be considered contraband, although it does not necessarily carry the same penalties as does a child porngraphy conviction, where lifelong residence registration is typically required even after all jail time and probation has been served. Note that the "sexting" phenomenon (where underage youth send nude or erotic photos of themselves to other youngsters) was not considered when this law was being devised. Megan's mother, Maureen Kanka, has indicated that prosecution of juveniles for such offenses was "harming the children more than helping them." (National Public Radio 2009)

For these many reasons and others (such as the authenticity and even the camera angles of the monitoring videos from police cars or shopping malls), it is important to enable digital image files to be analyzed for source and content. A vivid example is the air show footage of a jet that appears to be flying directly over the Golden Gate Bridge, actually considerably further away, with the FCC later re-

porting that objects were foreshortened through the camera angle and telephoto lens. (Myers and Doft 2010) As tools become more sophisticated in their ability to discern modifications (editing, morphing, etc.) or image distortions, defense will increasingly need the same type of 24-7 access to the data that prosecution now has, for analysis purposes. Experimentation and algorithm improvements can be done with benign files, but this also needs to be demonstrated with the actual charged items in order for results to be confirmed and for effective statements to be made, that will stand up to challenges, in reports and at trial.

The charges themselves also motivate the type of forensic analysis that should be used. Since time and funds are always a factor, a more focused investigation will typically yield stronger results than a scattershot approach. For example, if the charges do not include distribution or creation of images, then results pertaining to those issues may not need to be addressed. Especially in civil matters, it is helpful to understand the actual dispute in order to best select methods that will potentially yield beneficial data.

5 Exhibits

The manner in which digital images are displayed as exhibits at trial can also be problematic. Many courtrooms are now equipped with enormous display screens, where a movie or photograph can be shown some ten or more times larger than it would have appeared on a laptop computer. The shocking nature of this is often exploited with contraband imagery, whose deleterious effects defense attorneys should be cautious in ensuring are suppressed. Displays that are inappropriately oversized must not be allowed to unduly influence the judge or jury.

At the other extreme, the perceived prurient nature of an image can be used to provide a “peep show” at trial. In one instance, prosecution provided copies of two thumbnails of naked children (not engaged in sexual acts) to each juror in a manila folder. The jurors were informed that they should not open the folder until told to do so, and that what they would see they might find “shocking.” Unfortunately the defense attorney did not feel it appropriate to object to this presentation and the jury subsequently came back with a felony conviction, largely on the basis of these tiny, blurry images.

6 Concluding Thoughts

Courtroom issues involving the presentation of testimony related to digital image forensics create a balancing act for forensic experts, where the development and use of novel techniques must be weighed against the merits of the case and the ability to successfully introduce results into evidence. Digital image forensics is in its infancy, as is the field of computer forensics. As such, it is helpful to continue to gather insight from other forensic endeavors in an effort to establish good sci-

ence and good law. As well, the pace at which technology advances occur, far outstrips the ability of courts and legislatures to establish law that can reasonably address new situations. Judges and jurors may often have limited knowledge of how computers and the Internet work. The development of evidence and discovery rules have tended to be reactive rather than proactive, and these delays can adversely affect rulings. There are no simple answers to these problems, other than to attempt to create a level playing field where all parties can fairly review the evidence and present expert opinions in such fashion that justice will be able to be reasonably served.

7 Acknowledgements

The author would like to recognize Attorneys Anna M. Durbin and Michael W. Hoffman who provided salient feedback during the writing of this chapter. Clients and attorneys whom the author has worked with (or against!) on cases involving digital imagery, whose names have not been instantiated for reasons of privacy, are also thanked for the numerous insights they have provided. Dr. Norman Badler, director of the Center for Human Modeling and Simulation at the School of Engineering and Applied Science of the University of Pennsylvania is also acknowledged for his long-standing encouragement and support of research in computer graphics in general and this author in particular.

References

United States General Accounting Office (2003) Child Pornography is Readily Accessible over Peer-to-Peer Networks. GAO-03-537T, March 13, 2003.

Mercuri RT (2004) The HIPAA-potamus in Health Care Data Security. Security Watch, Communications of the Association for Computing Machinery, Volume 47, Number 7, July 2004.

National Public Radio (2009) 'Megan's Law' Mom Criticizes 'Sexting' Charges, March 26, 2009.

Stevens M Admissibility of Scientific Evidence under Daubert. http://faculty.ncwc.edu/mstevens/425/lecture03.htm Accessed October 22, 2010.

Morse MA Gaugler AC (2007) Daubert Challenges to Experts in Federal Criminal Cases: An Overlooked Defense. The National Association of Criminal Defense Lawyers Champion, July 2007.

Myers C Doft D (2010) Nothing wrong with jet's air show maneuver, FAA says. CNN, October 19, 2010.

Wang X Yin YL Yu H (2005) Finding Collisions in the Full SHA-1. Crypto 2005, LNCS 3621, pp. 17-36, 2005.