

In Defense of the Defense: The Use of Computer Forensics in Child Pornography Cases

By Sharon Nelson, John Simek and Jesse Lindmar
© 2009 Sensei Enterprises, Inc.

Defending subjects charged with crimes involving the exploitation of children is challenging and technologically involved. Attorneys need to understand what can and can't be determined through computer forensic analysis in order to successfully represent their clients.

Pity the poor child pornography defendant? Maybe. These days, even battle-hardened, cynical types like the authors have some sympathy for these defendants and even more for the attorneys who represent them. It is not a level playing field for these defendants and they are regularly denied due process of law.

Author Nelson, a practicing attorney, keeps a copy of the Constitution in the right drawer of her desk. On a remarkable number of occasions, she has had reason to produce it when challenged for representing those charged with the production, possession or distribution of child pornography.

The Bill of Rights states in the Fifth Amendment: *No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.*

Likewise, the Fourteen Amendment applies the same due process right to the states.

Procedural due process has been held to be based on the principles of "fundamental fairness." Except, apparently, in the case of those accused of producing, possessing or distributing child pornography. We will step off our collective soapbox (we'll be back on it at the end of this article) to give this subject some scientific perspective, courtesy of forensic technologists John Simek and Jesse Lindmar (formerly a police officer).

In recent years, law enforcement entities world-wide have increased their search for and prosecution of groups and individuals involved with the production, distribution, transportation, and/or possession of child pornography and the online solicitation of minors. In all cases, those prosecuted are entitled to be vigorously defended, as they are considered innocent until proven guilty. In order to fully defend those being prosecuted, attorneys need to understand the rights and responsibilities of all parties involved and the limitations of computer forensics.

In many cases, law enforcement investigations are thorough and the located electronic evidence is direct and irrefutable. For example, law enforcement identifies a website as containing known child pornographic pictures and videos. Some pictures and videos are visually displayed on the site, while others are described and require they be manually downloaded. Through proper procedures, the site is shut down and a computer server is forensically seized, preserved and investigated.

An inventory of purported contraband is created either via a manual review of the data or through an automated comparison. During this process, unique hash values are generated for these items. A file's hash value can be likened to an individual's fingerprints or even DNA. These hash values are compared to a list of hash values for known contraband items in order to identify any items that have been previously determined to be genuine. Any items an investigator visually determines to be contraband, which do not appear in the known database, will require trained professionals to determine whether the items are actual; i.e. not virtual or containing adults.

Additionally, log files are located that indicate the Internet Protocol (IP) addresses of computer systems that previously connected to the website. Law enforcement identifies the Internet Service Provider (ISP) that allocated one of the logged IP addresses. They obtain and issue the ISP a subpoena asking them to provide subscriber information for the account holder assigned that IP address at the date and time the IP was logged on the seized computer server. The ISP responds with the name, address and telephone number of the account holder.

Law enforcement obtains a search warrant for computer systems and data storage devices located at the address provided by the ISP. Upon execution, one laptop computer is seized. The item is forensically preserved and investigated. During the course of investigation, several non-deleted picture and video files are located under a specific user account. The hash values of these files match those found on the previously seized computer server. It has already been determined these hash values are associated with known contraband.

Some of the files were found in locations that automatically cache information from visited websites; these files are consistent with those pictures and videos visually displayed on the website. Other files were found in non-default download locations inside user-created and user-named folders; these files are consistent with those pictures and videos requiring manual download. The file's names and the dates and times they were created in their respective locations are compared to the web-browser history; allowing the website source of the items (the previously shutdown website) to be identified. The dates and times the files were created are when a specific individual had access to the computer system and other file and web-site access can be directly linked to that user (e.g. access to password-protected files or visits to websites requiring login credentials).

The previous brief account is from what would be considered a relatively thorough computer forensic examination, however, in some cases, the evidence is not as conclusive. The converse to this investigation would be those led by inexperienced or over-burdened computer forensic examiners. For them, the mere presence of a picture or video they deem to be child pornography is typically where the investigation ends. The owner or primary user of the computer is typically charged. More often than not, their report consists of the automated output from the forensic software suite used to conduct their analysis, along with a listing of the purported contraband they've identified. We typically term this type of investigation as "point and click" forensics. No verification as to whether the file is known or if the victim is real is conducted. No explanation as to the origin of the alleged contraband is offered. The dates and times the files are created, modified or accessed are sometimes included, but not always. The files' unique hash values are not included. No attempt is made to identify the user of the computer during those times, understanding the most difficult part these investigations is to place a specific individual in front of the computer. Also, the verification of the setting for the computer clock is rarely documented. Conclusions as to when particular activity occurred may be based on totally inaccurate clock settings.

In many cases, the identification of true child pornography is obvious; if it takes more than a few seconds to recognize the subject as a child, it may not be. Many pictures and videos use individuals who may look

child-like and these items may need to be evaluated by a medical professional who can anatomically determine the possible age of the subject. Another method to determine whether a file or subject is real or “virtual” is to compare the uniqueness of the file to a database of items already deemed to be real. The National Center for Missing & Exploited Children (NCMEC) maintains such a database and law enforcement is urged, if not required, to submit alleged contraband for verification. It should be noted that access to the NCMEC database of hash values is not available to the private sector, further increasing the difficulty of computer forensic examinations for the defendants.

In the Child Pornography Prevention Act of 1996, Congress sought to prohibit images that are or appear to be “of a minor engaging in sexually explicit conduct” or are “advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.” In 2002, the Supreme Court struck down this legislative attempt to ban “virtual” child pornography in *Ashcroft v. The Free Speech Coalition*. It ruled that the expansion of the 1996 act to material that did not involve and thus harm actual children in its creation is an unconstitutional violation of free speech rights. The PROTECT Act of 2003 revisited the argument, prohibiting visual depictions of children engaged in sexual conduct regardless of whether the depicted minor actually exists.

Ultimately, defendants may claim that pornographic images are of “virtual” children, thus requiring the government to establish that the children shown in these digital images are real. Experts may render an opinion based upon their training and experience, they may compare the suspect files to a database of known files, or they may conduct a skin-tone analysis all in an attempt to verify the item’s status. Attorneys need to understand this is not a stand-alone defense. The reality is defendants will be prosecuted for items regardless of whether or not they’ve been evaluated and a judge or jury will make the final decision based upon the evidence presented.

Other defenses include the infamous “Trojan Defense” in which a computer is infected with “malware” (malicious software) that plants child pornography, provides access to a third-party to drop contraband or causes an unknown or unauthorized visit to site containing child pornography. A Trojan is a malicious program that pretends to be a benign application. When run, it can inconspicuously unload hidden programs, commands, or scripts that can cause system vulnerabilities, damage or unwanted activity. Examples can include the erasing or overwriting of data, corrupting files, uploading or downloading files, allowing remote access to the computer, or displaying pornographic websites.

To date, there is no known malware capable of directly placing child pornography on a computer system. That doesn’t mean it isn’t possible, however, none have been reported or encountered in the computer forensic community. For this defense to be successful, an analysis of the suspect computer must be conducted to determine if the system is infected, what malware is present and how did it arrive on the system, what are the capabilities and functions of the malware, were they active when the contraband was created on the system, and can they be directly tied to the contraband. Although this defense has been successful for a handful of cases, it is not recommended unless the majority of the above questions can be answered with evidence that supports the claim.

The equally infamous “Pop-Up Defense” allows for the contraband to have been created by a pop-up advertisement that occurred while the user was innocently surfing the Internet. With the advent of pop-up blocking capability in many of today’s web-browsers, coupled with the availability of anti-virus, anti-spyware, anti-adware, and firewall protection, this occurrence is less likely than it may have been four or more years ago. However, an in-depth review of the locatable web-browser history, as well as file activity analysis, could provide support to this claim or deflate it in a heart-beat.

The role of the defense computer forensic expert is to verify the prosecution's findings, locate potentially exculpatory information and opine as to how the data can be interpreted. Their focus is not to determine whether the identified items are contraband, but they may offer an opinion based upon their findings. In order for defense computer forensic experts to provide assistance they first need access to seized computer equipment or forensic images of the storage devices associated with the equipment. The Adam Walsh Child Protection and Safety Act of 2006 prevents defense experts from possessing any material containing the alleged contraband at their own facilities, therefore, any investigation and analysis will need to be conducted at a law enforcement facility.

A protocol must be established beforehand that allows the defense expert access to all electronic evidence in the matter, to conduct any analysis using their own equipment (hardware and software), and to conduct that analysis in a secure and private location. In order to quash any rebuttals stating that the defense expert cannot use their own equipment because they will transfer the contraband to their computer during analysis, the defense expert can and will configure the analysis machine to write activity to an external hard-disk drive. This hard-disk drive, which can be provided by law enforcement or the defense expert, will be securely erased of any written data at the conclusion of the analysis. This setup provides no limitations to the type of analyses that can be conducted and allows for any work product to remain confidential. Many law enforcement examiners and prosecutors do not believe it is possible to isolate any contraband "infection" and insist that law enforcement equipment be used. Most times this offered equipment is older and less powerful than the defense expert's equipment and does not contain the necessary forensic tools that are needed for a proper examination. In addition, usage of software on the law enforcement equipment typically is a violation of the license terms.

In the interest of time, only those analyses that need to be conducted onsite will be done. This could include generating file listings, extracting web-browser history, processing email/instant messages, manually reviewing pictures or videos, and extracting metadata. Files containing only textual data may be exported in order for additional laboratory analysis to be conducted offsite. Analysis may aid in determining if the evidence had been handled properly by law enforcement, the source of the contraband (e.g. the visited website containing the pictures or videos), users of the computer, the individual operating the computer at the time of the contraband's creation, patterns of activity, etc.

The typical, total cost of travel, analysis, reporting and testimony in these cases can range from \$10,000.00 to 15,000.00 when a single computer system is involved; the analysis cost will increase about \$1,000.00 for each additional computer system involved and may also increase the amount of time required onsite. It will usually take several days just to coordinate a date the onsite analysis can be conducted, as the opposing side may want to review and rebut the analysis protocol. A minimum of one, eight-hour day will be needed onsite; however, this may increase after the examiner assesses the evidence. After the onsite analysis is conducted, several more days will be needed to review the text-based evidence captured while onsite. When all of this is concluded, the examiner will be able to offer an opinion and draft an expert report if requested, but it will be riddled with qualifications that the examination is less than thorough due to time constraints and the inability to perform extended analysis in their own laboratories.

The overall goal of forensically examining evidence involved in these matters is to determine the truth and prosecute the individuals responsible for violating the law. Due to the vulgarity of the content, the tendency of these cases is to view any suspects as guilty until proven innocent. It is difficult to detach oneself from these investigations and remain unbiased, however, it is necessary in order to conduct a thorough investigation that represents the facts and supports the opinions.

.....

We are stepping back on our soapbox again. Remember, we are not representing the guilty. We are representing accused individuals presumed to be innocent until proven guilty. When a CP case comes through our doors, we are open-minded. We are dedicated to the truth. Should the evidence conclusively prove guilt, we will advise the attorney accordingly. The attorney generally encourages, in a forceful way, that the defendant accept a plea bargain.

As this is the most common result, we think of ourselves as ultimately assisting justice, by giving the defendant a full opportunity to demonstrate innocence, validating the work of the computer forensic technologists used by the prosecution, and then saving the taxpayers money and the courts time by having the defendant accept a plea. For both sides, all that should matter is the search for the truth.

Unfortunately, what we often find is that the prosecution and law enforcement are hell-bent on convicting these defendants and often unwilling to consider exonerating or ameliorating evidence. What is ameliorating evidence? A typical case might involve someone who downloaded a ton of adult pornography through usage of newsgroups. It is well documented that if you bulk download a lot of perfectly legal adult pornography, a few CP images may slip through unbeknownst to the user. Likewise, we've seen cases where an individual whose computer usage, searching, etc. shows no interest in child pornography suddenly and inexplicably takes a one-time walk on the dark side, perhaps fueled by alcohol, substance abuse or misplaced curiosity. There are, in fact, many defendants who are technically guilty where a lawyer has a very good argument to make to the court that this individual should be treated more leniently.

The new law makes it illegal for anyone other than law enforcement to possess child pornography, even defense counsel or their experts. This is where the principal of fundamental fairness is violated. The prosecution has usually had the evidence for months and months, to examine at their leisure. The beleaguered defense expert is forced, often by economics, to do whatever it is possible to do in one or two eight hours days. Frequently, the expert has to fight to use his/her own equipment and to work in privacy. The prosecution is not, of course, entitled to the work product of the attorney or the attorney's expert.

The excuse for all the obstacles that the expert faces is that law enforcement is trying to ensure that the expert is not leaving the federal or state facility with child pornography. As the reader could see from the scientific descriptions above, no competent computer forensics examiner ever could, or would, leave with contraband. However, it is frequently difficult to explain this to law enforcement personnel or prosecutors, who simply are not familiar enough with technology to understand that computer forensics can be safely done without any risk of leaving with contraband.

It seems to us that there is no fundamental fairness when the expert is constantly forced to make hard decisions based on money and time about how to proceed. Since the passage of The Adam Walsh Act, the costs of a forensic examination to defendants has rocketed skyward, as they must now pay for travel to the law enforcement facility and the expert, having no other work to perform at the facility, has no choice but to fully bill the time spent there, whereas the expert might well have let the computer run a script if the examination were done in the expert's lab while stopping the clock and working on someone else's case.

Additionally, the expert rarely believes that a full and adequate examination was done – there simply isn't enough time or money. The prosecution has a serious advantage and the defendant is greatly disadvantaged.

If all this were truly necessary to prevent the distribution of contraband, we would perhaps understand the need for special handling rules. The truth is, any competent computer forensics professional can safely examine child pornography in their own forensics lab, without any chance of having the contraband redistributed. The examiner uses an analysis machine, not network-connected, with temporary files written to a wipeable device, to perform the exam. The examiner wipes the temporary file repository when the examination is complete. As an alternative, a virtual machine may be used for the examination and additional steps may be taken to ensure any contraband is not permanently written to any device. The evidence itself is secured in a lab requiring dual authentication for access and is further secured within the lab in a dual-authentication safe. Before the Adam Walsh Act, we had constructed a forensics protocol specific to the examination of child pornography evidence – and that protocol had been accepted by numerous state and military courts.

Should we zealously pursue those who make victims of children? Of course. But at the expense of the Constitutional rights of the defendants? Absolutely not. We have seen innocent defendants. We have seen ameliorating evidence that properly should limit the length of prison sentences or warrant probation. And those defendants deserved the very best legal representation and expert examination that we could give them. As did the guilty, who all went to jail as part of a plea bargain or a trial. That is the American legal system. Unfortunately, in our zeal to convict those involved with child pornography, we have done harm to the Constitution. It is our hope that this harm will be recognized, and reversed, in accordance with the principles of fundamental fairness dictated by no less an authority than the Constitution of the United States.

The authors are the President , Vice President and Assistant Director of Sensei Enterprises, Inc., a computer forensics and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) sensei@senseient.com (e-mail), <http://www.senseient.com> (web)