

Defense Forensics and Child Pornography

Images depicting minors engaged in sex acts or appearing in sexually provocative positions are the subject of an ever increasing number of criminal cases involving computers. A survey of the cases handled by the RCFL (Regional Computer Forensic Laboratories) shows that child pornography constitutes the highest percentage of their investigations.

While the decision about what constitutes child pornography appears to be a sociopolitical football with the Supreme Court ruling in the [Ashcroft v. The Free Speech Coalition](#) case, striking down the ban on virtual porn; currently, the U.S. government's position on child pornography is defined by the PROTECT Act, also known as the Amber Alert Bill. The PROTECT Act, signed into law in by George Bush in 2003, bans images that are *indistinguishable from photographs of minors engaged in sex acts*. Current graphic technologies allow for some very realistic appearing images, but a reasonable person would most likely be able to tell that these "drawn" images were not of real children. This is not necessarily the case where actual photos of adults have been modified to appear like minors. If a reasonable person can not tell that the photos were not of minors, there will be legal problems with the images. This latter test of legality has opponents of the PROTECT Act wondering where the victim is if the images are of adults.

The real issue with the possession of child pornography has less to do with the images themselves, and how they were created, or who is depicted in them, and more to do with control over the images. Today's operating systems, in particular the Windows operating system, is so insecure that it is impossible to say that any one individual was in control of their computer. Even savvy computer users can not truly claim to be in complete control of their computers. Rather, they are more likely to know when someone else has "owned" their computer and take actions to mitigate damage, theft, or in some cases, the planting of illegal digital material, later to be known as digital evidence.

The number of viruses, worms, spyware, key loggers and other types of computer vulnerabilities is endless. The abilities of these "malware" programs range from destroying the actual computer hardware to merely making copies of themselves and sending themselves on to the next desktop. Making changes to programs, capturing information such as passwords, or leaving behind files,

like child pornography, falls into a mid-range capability.

There are viruses that plant kiddie porn images on a hard drive and then send e-mail to the computer owner claiming that a program has detected child porn on their computer and here is the proof, showing evidence of what the virus had planted. Claiming that these images are only some of the images that can be found, claims that for a fee (extortion) they (whoever they are) will clean the offending images from the hard drive.

A less harmful virus, but equally capable of putting child pornography on the hard drive is one that changes the start page of the Web browser. When a computer user starts the Web browser on a computer infected with this virus, the Web browser can be directed to a Web page containing illegal images. Even with the best efforts of the computer user to eradicate the virus, erasing the browser cache, where temporary copies of the images are stored, the images will still exist in the unallocated sector space of the computer's hard drive. Many, if not most of the images presented as evidence of child porn possession come from the unallocated sectors of hard drives. Unallocated sectors are those portions of the hard drive that once contained files that were erased. Files on a computer are not actually erased, only references to the files are removed, while their data remains until overwritten by another file, or erased using a file eradicator such as Evidence Eliminator.

Not only is it not possibly, most of the time not even forensically, to tell who had access to a computer over the Internet, it is even less possible to tell who had access to a computer by sitting down in front of the keyboard. A case in San Diego was a good example of how important this point is. In the San Diego case it was learned that the child pornography was downloaded the day after the defendant was removed from his home by a restraining order, and had no physical or network access to his computer. Therefore, it was not possible for him to have downloaded the images he was being accused of possessing.

Until there is a definitive and forensically sound way of identifying exactly who is in front of the keyboard most digital evidence should be considered as the most tenuous circumstantial evidence. Where the prosecution has the burden of proof, they must prove that the digital evidence being used to convict a person is the result of the actions taken by the accused and not by a hacker, either remotely over a network, or a person physically using the

computer. It is difficult to prove who is in front of the keyboard. In a Riverside, CA case it was possible to tell when the accused was not in front of the keyboard by referring to his truck driver log book. Because he was physically not present it was possible to see that images for which he was being accused were actually downloaded by someone else. Interestingly, partly because of the emotional nature of the crime, it has become the responsibility of the accused to prove innocence of possession, where the burden of proof seems to require no more than insinuation. This would be tantamount to claiming someone guilty of possessing a firearm because it was found in a public restroom frequented by the accused. Information security professionals have relied for the last fifteen years on the [two factor authentication](#) scheme to provide greater assurance that the person at the computer is who they say they are. The same principle can be applied in the field of computer forensics. It should be a required part of sound forensic methodology to require at least two identification factors to be used when authenticating the author, owner, possessor of digital evidence. Because we are all at risk for such accusations we should certainly expect sound methodology to be used to identify data with its proper owner when accusing someone of a crime.

While free speech and civil liberties argue over the finer points of what defines "prurient interest" and what images are objectionable, and what exactly is virtual porn, it is fairly clear that in most of the cases involving child pornography, the evidence is hardly worth the hard drive on which it was imaged. While government investigators can weave wild tails around what they find on a computer hard drive, when put to the task of carrying the burden of proof, providing convincing evidence that no one else in the world, other than the accused could have possibly put the images on the computer, they won't be able to do it. They can not, beyond a reasonable doubt, claim, in most cases, that the accused downloaded, viewed, or was in any way in control or had knowledge of the images he is accused of possessing.